Z2 : 01 – the actual used level

Z3-Z4 : Country / Currency Code - packed BCD.
The packed BCD country / currency code of the reader can be sent in two different forms depending on the value of the left most BCD digit.

If the left most digit is a 0, the International Telephone Code is used to indicate the country that the reader is set-up for. For example, the USA code is 00 01H (Z3 = 00 and Z4 = 01).

If the left most digit is a 1, the latest version of the ISO 4217 numeric currency code is used (see Appendix A1). For example, the code for the US dollar is 18 40H (Z2 = 18 and Z3 = 40) and for the Euro is 1978 (Z3 = 19 and Z4 = 78). Use FFFFh if the country code in unknown.

For level 3 cashless readers, it is mandatory to use the ISO 4217 numeric currency code (see Appendix A1).

Z5 : Scale Factor.
The multiplier used to scale all monetary values transferred between the VMC and the reader.

Z6 : Decimal Places.
The number of decimal places used to communicate monetary values between the VMC and the age verification device.

All pricing information sent between the VMC and the Age Verification Device is scaled using the scale factor and decimal places. This corresponds to:

$$\text{ActualPrice} = P \cdot X \cdot 10^{-Y}$$

where P is the scaled value send in the price bytes, and X is the scale factor, and Y is the number of decimal places. For example if there are 2 decimal places and the scale factor is 5, then a scaled price of 7 will mean an actual of 0.35.

Z7 : Application Maximum Response Time - seconds.
The maximum length of time a reader will require to provide a response to any command from the VMC. The value reported here supersedes the payment reader's default NON-RESPONSE time defined in section 7.5 if the value reported here is greater.

Z8 : Miscellaneous Options – xxxxyyyy

11.4.3 Poll

POLL (6AH)

The POLL command is used by the VMC to obtain information from the verification device. In addition to an ACK, the VMC may receive the following POLL responses from the verification device.

Reader responses:

Just Reset (00H)
Z1

Z1 : JUST RESET
Indicates the device has been reset.
Note: the difference between ACK and JUST RESET responses is:
00H 00H* =JUST RESET
00H* =ACK
*mode bit=1

Reader Config Info (01H)	Reader Feature Level	Country Code High	Country Code Low	Scale Factor	Decimal Places	Application Maximum Response Time	Miscellaneous Options
Z1	Z2	Z3	Z4	Z5	Z6	Z7	Z8

Display Request (02H)	Display Time	Display Data
Z1	Z2	Z3-Z34

Z1 : DISPLAY REQUEST
The Age Verification Device is requesting a message to be displayed on the VMC's display.

Z2 : Display Time - 0.1 second units
The requested display time. Either the VMC or the Age Verification Device may overwrite the message before the time has expired.

Peripheral ID (09H)	Manufacturer Code	Serial Number	Model Number	Software Version	Optional Feature bits
Z1	Z2-Z4	Z5-Z16	Z17-Z28	Z29-Z30	Z31 - Z34

Z1 : PERIPHERAL ID
Age Verification Device is sending peripheral ID information.

Z2 - Z4 : Manufacturer Code - ASCII
Identification code for the equipment supplier. Currently defined codes are listed in the **EVA** document entitled "***European Vending Association Data Transfer Standard***" (**EVA-DTS**), the Audit Data
Lists section, sub-section 2, "Manufacturer Codes".

Z5-Z16 : Serial Number – ASCII
Factory assigned serial number.

Z17-Z28 : Model Number - ASCII
Manufacturer assigned model number.

Z29-Z30 : Software Version - packed BCD
Current software version.

Z31- Z34 Optional Feature Bits. Each of the 32 bits indicate an optional feature availability. Bits should be sent in descending order, i.e. bit 31 is sent first and bit 0 is sent last. Options **must be enabled by the VMC** using the Expansion Optional Feature Bit Enable (17H-04H) command and **all features are disabled after a reset**. Currently defined options are:

b0 - File Transport Layer supported

b1 to b31 not used (should be set to 0)

Malfunction / Error (0AH) Z1	Error Code Z2

Z1 : MALFUNCTION/ERROR
The Age Verification Device is reporting a malfunction or error.

Z2 : Error Code - xxxxyyyy

Transient Error Handling
The error will be reported to the VMC until it has been ACKnowledged. The error state will be cleared in the age verification device, and normal operations will continue.

Non-transient Error Handling
The error will be reported to the VMC at each POLL as long as it exists. If the Age Verification Device is still functional, multi-message responses will allow normal responses in addition to the error report.

Time/Date Request (11H)

Z1

Z1 : TIME DATE REQUEST
In certain circumstances it will be necessary to synchronize the real time clock of the Age Verification Device with real time clock of the VMC. The Age Verification Device will respond with TIME/DATE REQUEST to a POLL command of the VMC. The VMC will follow with the EXPANSION-WRITE TIME/DATE FILE to the age verification device.

11.4.4 Expansion commands (request ID)

	Request	Manufacturer	Serial	Model	Software
Expansion	ID	Code	Number	Number	Version
(6FH)	(00H)				
	Y1	Y2-Y4	Y5-Y16	Y17-Y28	Y29-Y30

Y1 : REQUEST ID
The VMC is requesting Age Verification Device identification information. The information included above (Y2-Y30) provides the Age Verification Device with VMC identification information.

Y2-Y4 : Manufacturer Code - ASCII
Identification code for the equipment supplier. Currently defined codes are listed in the EVA document entitled "The Data Transfer Standard EVA-DTS" document, the Audit Data Dictionary section, chapter 4, "Manufacturer Codes".

Y5-Y16 : Serial Number - ASCII
Factory assigned serial number.

Y17-Y28 : Model Number - ASCII
Manufacturer assigned model number.

Y29-Y30 : Software Version - packed BCD
Current software version.

Age Verification Device response:

Peripheral	Manufacture	Serial	Model	Software	Optional
ID	Code	Number	Number	Version	Feature Bits
(09H)					
Z1	Z2-Z4	Z5-Z16	Z17-Z28	Z29-Z30	Z31-Z34

11.4.5 EXPANSION - Write Time/Date File

Expansion (6FH)	Write Time/ Date File (03H) Y1	Time Date Y2-Y11

Y1 : WRITE TIME/DATE FILE
The VMC requests to write the Time/Date file.

Y2- Y11: Time/Date to synchronize the Age Verification Device real time clock. The date bytes are BCD encoded.

Y2 = Years (Range: 00..99)
Y3 = Months (Range: 01..12)
Y4 = Days (Range: 01..31)
Y5 = Hours (Range: 00..23)
Y6 = Minutes (Range: 00..59)
Y7 = Seconds (Range: 00..59)
Y8 = Day of Week (Range: 01..07, Monday = 1..Sunday = 7)
Y9 = Week Number (Range: 01..53)
Y10 = Summertime (Range: 00..01, Summertime = 1)
Y11 = Holiday (Range: 00..01, Holiday = 1)

If any item of the time/date is not supported use FFH instead.

11.4.6 EXPANSION - Diagnostics

Expansion (6FH)	Diagnostics (FFH) Y1	User Defined Data Y2-Yn

Y1 : DIAGNOSTICS.
Device manufacturer specific instruction for implementing various manufacturing or test modes.

Y2-Yn : User Defined Data.
The data portion of this command is defined by the manufacturer and is not part of this document.

Age Verification Device response:

Diagnostics Response (FFH) Z1	User Defined Z2-Zn

Z1 : DIAGNOSTICS RESPONSE.
Z2-Zn : User Defined Data.
The data portion of this response is defined by the manufacturer and is not part of this document.

11.5 Age Verification Device Non-Response Time

The default maximum non-response time for the Age Verification Device is 5 seconds. This is the maximum time for which an Age Verification Device will not respond to a command or a POLL with ACK, NAK or a message. The "Application Maximum Response Time" reported in byte Z7 of the Age Verification Device Configuration Data supersedes this default value if Z7 is greater.

.

11.6 Age Verification Device Power Requirements

The current draw for any Age Verification Device must fall within the following limits. All measurements are at the minimum VMC Voltage Output.

Idle mode = 300 mA. (avg.) continuous

Transport or Read/Write cycle = 1.5 A @ 50% maximum duty cycle up to 5 seconds.

Appendix 1

Currency Codes

A1.1 Information

The following **Tables of Codes for the Representation of Currencies and Funds** are provided by the Secretariat of ISO 4217 MA. It is provided here to be used for the MDB currency code information sent between the credit peripherals and the VMC.

Table A.1 Currency and Funds Code List (English alphabetical order by entity)

Table A.2 Funds Codes Registered with the Maintenance Agency

Table A.3 Codes for Historic Denominations of Currencies and Funds

A1.2 MDB/ICP Use

As stated in the individual credit device sections, the two byte, packed BCD country / currency code of the coin changer, bill validator, and card reader devices can be sent in two different forms depending on the value of the left most BCD digit.

If the left most digit is a 0, the International Telephone Code is used to indicate the country that the reader is set-up for.

> For example, the USA telephone code is 001 which translates into the MDB code as **00 01**h (Zx = **00**h and Zy = **01**h).

If the left most digit is a 1, the latest version of the ISO 4217 numeric currency code is used as listed in this Appendix.

> For example, the code for the US dollar is 840 which translates into the MDB code as **18 40**h (Zx = **18**h and Zy = **40**h).
>
> The code for the Euro is 978 which translates into the MDB code as **1978**h (Zx = **19**h and Zy = **78**h).
>
> **FFFF**h should be used if the country code in unknown (Zx = **FF**h and Zy = **FF**h).

Note that for level 3 cashless readers, it is mandatory to use the_the ISO 4217 numeric currency code.

Table A.1 Currency and Funds Code List (English alphabetical order by entity)

ENTITY	Currency	Code Alphabetic	 Numeric	Decimal Position
AFGHANISTAN	Afghani	AFA	004	2
ALBANIA	Lek	ALL	008	2
ALGERIA	Algerian Dinar	DZD	012	2
AMERICAN SAMOA	US Dollar	USD	840	2
ANDORRA	Spanish Peseta	ESP	724	0
	French Franc	FRF	250	2
	Andorran Peseta	ADP	020	0
ANGOLA	New Kwanza	AON	024	2
	Kwanza Reajustado	AOR	982	2
ANGUILLA	East Caribbean Dollar	XCD	951	2
ANTARCTICA	No universal currency			
ANTIGUA AND BARBUDA	East Caribbean Dollar	XCD	951	2
ARGENTINA	Argentine Peso	ARS	032	2
ARMENIA	Armenian Dram	AMD	051	2
ARUBA	Aruban Guilder	AWG	533	2
AUSTRALIA	Australian Dollar	AUD	036	2
AUSTRIA	Schilling	ATS	040	2
AZERBAIJAN	Azerbaijanian Manat	AZM	031	2
BAHAMAS	Bahamian Dollar	BSD	044	2
BAHRAIN	Bahraini Dinar	BHD	048	3
BANGLADESH	Taka	BDT	050	2
BARBADOS	Barbados Dollar	BBD	052	2
BELARUS	Belarussian Ruble	BYB	112	0
	Belarussian Ruble	BYR	974	0
BELGIUM	Belgian Franc	BEF	056	0
BELIZE	Belize Dollar	BZD	084	2
BENIN	CFA Franc BCEAO+	XOF	952	0
BERMUDA	Bermudian Dollar (customarily known as Bermuda Dollar)	BMD	060	2
BHUTAN	Indian Rupee	INR	356	2
	Ngultrum	BTN	064	2

+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de l'Afrique de l'Ouest.

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	Position
BOLIVIA	Boliviano	BOB	068	2
	Mvdol*	BOV	984	2
BOSNIA & HERZEGOVINA	Convertible Marks	BAM	977	2
BOTSWANA	Pula	BWP	072	2
BOUVET ISLAND	Norwegian Krone	NOK	578	2
BRAZIL	Brazilian Real	BRL	986	2
BRITISH INDIAN OCEAN TERRITORY	US Dollar	USD	840	2
BRUNEI DARUSSALAM	Brunei Dollar	BND	096	2
BULGARIA	Lev	BGL	100	2
	Bulgarian LEV	BGN	975	2
BURKINA FASO	CFA Franc BCEAO+	XOF	952	0
BURUNDI	Burundi Franc	BIF	108	0
CAMBODIA	Riel	KHR	116	2
CAMEROON	CFA Franc BEAC#	XAF	950	0
CANADA	Canadian Dollar	CAD	124	2
CAPE VERDE	Cape Verde Escudo	CVE	132	2
CAYMAN ISLANDS	Cayman Islands Dollar	KYD	136	2
CENTRAL AFRICAN REPUBLIC	CFA Franc BEAC#	XAF	950	0
CHAD	CFA Franc BEAC#	XAF	950	0
CHILE	Chilean Peso	CLP	152	0
	Unidades de fomento*	CLF	990	0
CHINA	Yuan Renminbi	CNY	156	2
CHRISTMAS ISLAND	Australian Dollar	AUD	036	2
COCOS (KEELING) ISLANDS	Australian Dollar	AUD	036	2
COLOMBIA	Colombian Peso	COP	170	2
COMOROS	Comoro Franc	KMF	174	0

+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de l'Afrique de l'Ouest.

CFA Franc BEAC; Responsible authority: Banque des Etats de l'Afrique Centrale.

• Funds code [See table A.2(E) for definitions of funds types].

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	Position
CONGO	CFA Franc BEAC#	XAF	950	0
CONGO, THE DEMOCRATIC REPUBLIC OF	Franc Congolais	CDF	976	2
COOK ISLANDS	New Zealand Dollar	NZD	554	2
COSTA RICA	Costa Rican Colon	CRC	188	2
COTE D'IVOIRE	CFA Franc BCEAO+	XOF	952	0
CROATIA	Kuna	HRK	191	2
CUBA	Cuban Peso	CUP	192	2
CYPRUS	Cyprus Pound	CYP	196	2
CZECH REPUBLIC	Czech Koruna	CZK	203	2
DENMARK	Danish Krone	DKK	208	2
DJIBOUTI	Djibouti Franc	DJF	262	0
DOMINICA	East Caribbean Dollar	XCD	951	2
DOMINICAN REPUBLIC	Dominican Peso	DOP	214	2
EAST TIMOR	Timor Escudo	TPE	626	0
	Rupiah	IDR	360	2
ECUADOR	US Dollar	ESD	840	2
EGYPT	Egyptian Pound	EGP	818	2
EL SALVADOR	El Salvador Colon	SVC	222	2
EQUATORIAL GUINEA	CFA Franc BEAC#	XAF	950	0
ESTONIA	Kroon	EEK	233	2
ERITREA	Nakfa	ERN	232	2
ETHIOPIA	Ethiopian Birr	ETB	230	2
FAEROE ISLANDS	Danish Krone	DKK	208	2
FALKLAND ISLANDS (MALVINAS)	Falkland Islands Pound	FKP	238	2

CFA Franc BEAC; Responsible authority: Banque des Etats de l'Afrique Centrale.

+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de l'Afrique de l'Ouest.

* Funds code [see Table A.2 (E) for definitions of funds types].

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	Position
FIJI	Fiji Dollar	FJD	242	2
FINLAND	Markka	FIM	246	2
FRANCE	French Franc	FRF	250	2
FRENCH GUIANA	French Franc	FRF	250	2
FRENCH POLYNESIA	CFP Franc	XPF	953	0
FRENCH SOUTHERN TERRITORIES	French Franc	FRF	250	2
GABON	CFA Franc BEAC#	XAF	950	0
GAMBIA	Dalasi	GMD	270	2
GEORGIA	Lari	GEL	981	2
GERMANY	Deutsche Mark	DEM	276	2
GHANA	Cedi	GHC	288	2
GIBRALTAR	Gibraltar Pound	GIP	292	2
GREECE	Drachma	GRD	300	2
GREENLAND	Danish Krone	DKK	208	2
GRENADA	East Caribbean Dollar	XCD	951	2
GUADELOUPE	French Franc	FRF	250	2
GUAM	US Dollar	USD	840	2
GUATEMALA	Quetzal	GTQ	320	2
GUINEA	Guinea Franc	GNF	324	0
GUINEA-BISSAU	Guinea-Bissau Peso	GWP	624	2
	CFA Franc BCEAO+	XOF	952	0
GUYANA	Guyana Dollar	GYD	328	2
HAITI	Gourde	HTG	332	2
	US Dollar	USD	840	2
HEARD AND MCDONALD ISLANDS	Australian Dollar	AUD	036	2
HONDURAS	Lempira	HNL	340	2

CFA Franc BEAC; Responsible authority: Banque des Etats de l'Afrique Centrale.

+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de l'Afrique de l'Ouest.

Table A.1 (Continued)

ENTITY	Currency	Code Alphabetic	 Numeric	Decimal Point
HONG KONG	Hong Kong Dollar	HKD	344	2
HUNGARY	Forint	HUF	348	2
ICELAND	Iceland Krona	ISK	352	2
INDIA	Indian Rupee	INR	356	2
INDONESIA	Rupiah	IDR	360	2
INTERNATIONAL MONETARY FUND (IMF)**	SDR	XDR	960	N.A.
IRAN (ISLAMIC REPUBLIC OF)	Iranian Rial	IRR	364	2
IRAQ	Iraqi Dinar	IQD	368	3
IRELAND	Irish Pound	IEP	372	2
ISRAEL	New Israeli Sheqel*	ILS	376	2
ITALY	Italian Lira	ITL	380	0
JAMAICA	Jamaican Dollar	JMD	388	2
JAPAN	Yen	JPY	392	0
JORDAN	Jordanian Dinar	JOD	400	3
KAZAKHSTAN	Tenge	KZT	398	2
KENYA	Kenyan Shilling	KES	404	2
KIRIBATI	Australian Dollar	AUD	036	2
KOREA, DEMOCRATIC PEOPLE'S REPUBLIC OF	North Korean Won	KPW	408	2
KOREA, REPUBLIC OF	Won	KRW	410	0

* Currency name was effective 4th September 1985

** This entry is not derived fron ISO 3166, but is included here in alphabetic sequence for convenience.

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	Point
KUWAIT	Kuwaiti Dinar	KWD	414	3
KYRGYZSTAN	Som	KGS	417	2
LAO PEOPLE'S DEMOCRATIC REPUBLIC	Kip	LAK	418	2
LATVIA	Latvian Lats	LVL	428	2
LEBANON	Lebanese Pound	LBP	422	2
LESOTHO	Rand	ZAR	710	2
	(financial Rand)*	ZAL	991	2
	Loti	LSL	426	2
LIBERIA	Liberian Dollar	LRD	430	2
LIBYAN ARAB JAMAHIRIYA	Libyan Dinar	LYD	434	3
LIECHTENSTEIN	Swiss Franc	CHF	756	2
LITHUANIA	Lithuanian Litas	LTL	440	2
LUXEMBOURG	Luxembourg Franc	LUF	442	0
MACAU	Pataca	MOP	446	2
MACEDONIA, THE FORMER YUGOSLAV REPUBLIC OF	Denar	MKD	807	2
MADAGASCAR	Malagasy Franc	MGF	450	0
MALAWI	Kwacha	MWK	454	2
MALAYSIA	Malaysian Ringgit	MYR	458	2
MALDIVES	Rufiyaa	MVR	462	2
MALI	CFA Franc BCEAO+	XOF	952	0
MALTA	Maltese Lira	MTL	470	2
MARSHALL ISLANDS	US Dollar	USD	840	2
MARTINIQUE	French Franc	FRF	250	2
MAURITANIA	Ouguiya	MRO	478	2
MAURITIUS	Mauritius Rupee	MUR	480	2
MEXICO	Mexican Peso	MXN	484	2
	Mexican Unidad de Inversion (UDI)*	MXV	979	2
MICRONESIA	US Dollar	USD	840	2
MOLDOVA, REPUBLIC OF	Moldovan Leu	MDL	498	2
MONACO	French Franc	FRF	250	2

* Funds code [See table A.2(E) for definitions of funds types].

+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de l'Afrique de l'Ouest.

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	Point
MONGOLIA	Tugrik	MNT	496	2
MONTSERRAT	East Caribbean Dollar	XCD	951	2
MOROCCO	Moroccan Dirham	MAD	504	2
MOZAMBIQUE	Metical	MZM	508	2
MYANMAR	Kyat	MMK	104	2
NAMIBIA	Rand	ZAR	710	2
	Namibia Dollar**	NAD	516	2
NAURU	Australian Dollar	AUD	036	2
NEPAL	Nepalese Rupee	NPR	524	2
NETHERLANDS	Netherlands Guilder	NLG	528	2
NETHERLANDS ANTILLES	Netherlands Antillian Guilder	ANG	532	2
NEW CALEDONIA	CFP Franc	XPF	953	0
NEW ZEALAND	New Zealand Dollar	NZD	554	2
NICARAGUA	Cordoba Oro	NIO	558	2
NIGER	CFA Franc BCEAO+	XOF	952	0
NIGERIA	Naira	NGN	566	2
NIUE	New Zealand Dollar	NZD	554	2
NORFOLK ISLAND	Australian Dollar	AUD	036	2
NORTHERN MARIANA ISLANDS	US Dollar	USD	840	2
NORWAY	Norwegian Krone	NOK	578	2
OMAN	Rial Omani	OMR	512	3
PAKISTAN	Pakistan Rupee	PKR	586	2
PALAU	US Dollar	USD	840	2

+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de l'Afrique de l'Ouest.

The lowest unit of recorded value for the Iraqi Dinar is the Dirham (1 Iraqi Dinar = 20 Dirhams).

** The Namibia Dollar becomes effective September 15th 1993

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	Point
PANAMA	Balboa	PAB	590	2
	US Dollar	USD	840	2
PAPUA NEW GUINEA	Kina	PGK	598	2
PARAGUAY	Guarani	PYG	600	0
PERU	Nuevo Sol	PEN	604	2
PHILIPPINES	Philippine Peso	PHP	608	2
PITCAIRN	New Zealand Dollar	NZD	554	2
POLAND	Zloty	PLN	985	2
PORTUGAL	Portuguese Escudo	PTE	620	0
PUERTO RICO	US Dollar	USD	840	2
QATAR	Qatari Rial	QAR	634	2
REUNION	French Franc	FRF	250	2
ROMANIA	Leu	ROL	642	2
RUSSIAN FEDERATION	Russian Ruble	RUR	810	2
	Russian Ruble	RUB	643	2
RWANDA	Rwanda Franc	RWF	646	0
ST HELENA	St Helena Pound	SHP	654	2
ST KITTS - NEVIS	East Caribbean Dollar	XCD	951	2
SAINT LUCIA	East Caribbean Dollar	XCD	951	2
ST PIERRE AND MIQUELON	French Franc	FRF	250	2
SAINT VINCENT AND THE GRENADINES	East Caribbean Dollar	XCD	951	2
SAMOA	Tala	WST	882	2
SAN MARINO	Italian Lira	ITL	380	0
SAO TOME AND PRINCIPE	Dobra	STD	678	2
SAUDI ARABIA	Saudi Riyal	SAR	682	2

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal
		Alphabetic	Numeric	Point
SENEGAL	CFA Franc BCEAO+	XOF	952	0
SEYCHELLES	Seychelles Rupee	SCR	690	2
SIERRA LEONE	Leone	SLL	694	2
SINGAPORE	Singapore Dollar	SGD	702	2
SLOVAKIA	Slovak Koruna	SKK	703	2
SLOVENIA	Tolar	SIT	705	2
SOLOMON ISLANDS	Solomon Islands Dollar	SBD	090	2
SOMALIA	Somali Shilling	SOS	706	2
SOUTH AFRICA	Rand	ZAR	710	2
SPAIN	Spanish Peseta	ESP	724	0
SRI LANKA	Sri Lanka Rupee	LKR	144	2
SUDAN	Sudanese Dinar	SDD	736	2
SURINAME	Surinam Guilder	SRG	740	2
SVALBARD AND JAN MAYEN ISLANDS	Norwegian Krone	NOK	578	2
SWAZILAND	Lilangeni	SZL	748	2
SWEDEN	Swedish Krona	SEK	752	2
SWITZERLAND	Swiss Franc	CHF	756	2
SYRIAN ARAB REPUBLIC	Syrian Pound	SYP	760	2
TAIWAN, PROVINCE OF CHINA	New Taiwan Dollar	TWD	901	2
TAJIKISTAN	Tajik Ruble	TJR	762	0

+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de l'Afrique de l'Ouest.

Table A.1 (Continued)

ENTITY	Currency	Code		Decimal Point
		Alphabetic	Numeric	
TANZANIA, UNITED REPUBLIC OF	Tanzanian Shilling	TZS	834	2
THAILAND	Baht	THB	764	2
TOGO	CFA Franc BCEAO+	XOF	952	0
TOKELAU	New Zealand Dollar	NZD	554	2
TONGA	Pa'anga	TOP	776	2
TRINIDAD AND TOBAGO	Trinidad and Tobago Dollar	TTD	780	2
TUNISIA	Tunisian Dinar	TND	788	3
TURKEY	Turkish Lira	TRL	792	0
TURKMENISTAN	Manat	TMM	795	2
TURKS AND CAICOS ISLANDS	US Dollar	USD	840	2
TUVALU	Australian Dollar	AUD	036	2
UGANDA	Uganda Shilling ++	UGX	800	0
UKRAINE	Hryvnia	UAH	980	2
UNITED ARAB EMIRATES	UAE Dirham	AED	784	2
UNITED KINGDOM	Pound Sterling	GBP	826	2
UNITED STATES	US Dollar	USD	840	2
	(Same day)*	USS	998	2
	(Next day)*	USN	997	2
UNITED STATES MINOR OUTLAYING ISLANDS	US Dollar	USD	840	2

+ CFA Franc BCEAO; Responsible authority: Banque Centrale des Etats de l'Afrique de l'Ouest.

++ The Uganda Shilling was denominated as from 18 May 1987.

* Funds code [See table A.2(E) for definitions of funds types].

Table A.1 (Continued)

ENTITY	Currency	Code Alphabetic	 Numeric	Decimal Point
URUGUAY	Peso Uruguayo	UYU	858	2
UZBEKISTAN	Uzbekistan Sum	UZS	860	2
VANUATU	Vatu	VUV	548	0
VATICAN CITY STATE (HOLY SEE)	Italian Lira	ITL	380	0
VENEZUELA	Bolivar	VEB	862	2
VIETNAM	Dong	VND	704	2
VIRGIN ISLANDS (BRITISH)	US Dollar	USD	840	2
VIRGIN ISLANDS (U.S.)	US Dollar	USD	840	2
WALLIS AND FUTUNA ISLANDS	CFP Franc	XPF	953	0
WESTERN SAHARA	Moroccan Dirham	MAD	504	2
YEMEN	Yemeni Rial	YER	886	2
YUGOSLAVIA	New Dinar	YUM	891	2
ZAMBIA	Kwacha	ZMK	894	2
ZIMBABWE	Zimbabwe Dollar	ZWD	716	2

Table A.1 (Continued)

ENTITY	**Currency**	**Code**		**Decimal**
		Alphabetic	**Numeric**	**Position**
Entity not applicable	Gold	XAU	959	N.A.
	Bond Markets Units			
	European Composite Unit (EURCO)	XBA	955	N.A.
	European Monetary Unit (E.M.U.-6)***	XBB	956	N.A.
	European Unit of Account 9 (E.U.A.- 9)	XBC	957	N.A.
	European Unit of Account 17 (E.U.A.- 17)	XBD	958	N.A.
	Palladium	XPD	964	N.A.
	Platinum	XPT	962	N.A.
	Silver	XAG	961	N.A.

*** E.M.U.-6 is sometimes known as the European Currency Unit. This should not be confused with the settlement unit of the European Monetary Cooperation Fund (E.M.C.F.) which has the same name (see entry for 'European Monetary Cooperation Fund' in this table).

Table A.1 (Continued)

ENTITY	Currency	Code Alphabetic	 Numeric	Decimal Position
Entity not applicable	Special settlement currencies			
	UIC-Franc	XFU	Nil	N.A.
	Gold-Franc	XFO	Nil	N.A.
	Codes specifically reserved for testing purposes	XTS	963	N.A.
	The codes assigned for transactions where no currency is involved are:	XXX	999	N.A.
	euro*	EUR*	978	2

* On 1 January 1999, the euro will become the currency of those Member States of the European Union which adopt the single currency in accordance with the Treaty establishing the European Community. This code has been issued now so that technical preparations can be started. The code element "EU" has been reserved by the ISO 3166 Maintenance Agency for use within ISO 4217 where "R" has been appended to make an acceptable mnemonic code.

Table A.2 Funds Codes Registered with the Maintenance Agency

CURRENCY AUTHORITY	Currency	Fund Type	Code Alphabetic	Code Numeric	Decimal Position
BOLIVIA		Mvdol	BOV	984	2
CHILE		Unidades de Fomento	CLF	990	0
MEXICO		Mexican Unidad de Inversion (UDI)	MXV	979	2
UNITED STATES	US Dollar	Same day	USS	998	2
		Next day	USN	997	2

Definitions of the fund types listed above

BOV: For indexation purposes and denomination of certain finacial instruments (ex. treasury bills). The Mvdol is set daily by the Central Bank of Bolivia based upon the official USD/BOB rate.

CLF: This development unit has been approved by the Chilean government for use in insurance transactions (with effect from 10 April 1980).

ECV: A daily indexation mechanism set by the Ecuadorian Central Bank. The UVC is set according to the variation of the Consumer price Index (Urban), as compiled by the National Census and Statistics Institute (INEC).

MXV : The UDI is an inflation adjusted mechanism set by the Central Bank of Mexico according to the variation in the Mexican Consumer Price Index. The value of the UDI is expressed in terms of Mexican Pesos per UDI. It is used to denominate mortgage loans, some bank deposits with maturities of 3 month or more and Government bonds (UDIBONOS).

USN: "Next day" funds are immediately available for transfer in like funds, and subject to settlement, available the next business day for same day funds transfer or withdrawal in cash.

USS: "Same day" funds are immediately available for transfer today or for withdrawal in cash, subject to the settlement of the transaction through the payment mechanism used.

(USD designates the US Dollar, the currency designator when an accumlation of amounts contains more than one funds type.)

Table A.3 Codes for Historic Denomination of Currencies and Funds

ENTITY	Historic Currencies	Code	Numeric	WD
ALBANIA	Old Lek	ALK *	-	12/89
ANGOLA	Kwanza	AOK	-	03/91
ARGENTINA	Peso Argentino	ARP	-	07/85
	Austral	ARA	-	01/92
	Peso	ARY*	-	1989/1990
BELGIUM	Convertible Franc	BEC	993	03/90
	Financial Franc	BEL	992	03/90
BOLIVIA	Peso	BOP	-	02/87
BOSNIA & HERZEGOVINA	Dinar	BAD	070	09/97
BRAZIL	Cruzeiro	BRB	-	03/86
	Cruzado	BRC	-	02/89
	New Cruzado	BRN	-	03/90
	Cruzeiro	BRE	076	08/93
	Cruzeiro Real	BRR	987	07/94
BULGARIA	Lev A/62	BGK*	-	1989/1990
	Lev A/52	BGJ*	-	1989/1990
BURMA#	N/A	BUK	-	02/90
CHINA	Peoples Bank Dollar	CNX*	-	12/89
CROATIA	Dinar	HRD	-	01/95
CZECHOSLOVAKIA	Krona A/53	CSJ*	-	1989/1990
	Koruna	CSK	200	03/93
ECUADOR	Sucre	ECS	218	9/00
	Unidad del Valor constante (UVC)*	ECV	983	9/00
EQUATORIAL GUINEA	Ekwele	GQE	226	06/86
	Ekwele	EQE*	-	12/89

* Non ISO code
Change in country name

Table 3 (Continued)

ENTITY	Historic Currencies	Code	Numeric	WD
EUROPEAN MONETARY COOPERATION FUND (EMCF)**	European Currency Unit (E.C.U)	XEU	954	01/99
GERMAN DEMOCRATIC REPUBLIC	Mark der DDR	DDM	278	07/90 to 09/90
GEORGIA	Georgian Coupon	GEK	268	10/95
GUINEA	Syli	GNS	-	02/86
	Syli	GNE*	-	12/89
GUINEA BISSAU	Guinea Escudo	GWE	-	Between 1978-1981
ICELAND	Old Krona	ISJ*	-	1989/1990
ISRAEL	Old Shekel	ILR*	-	1989/1990
	Pound	ILP	-	Between 1978-1981
LESOTHO	Maloti	LSM	-	05/85
LAO	Kip Pot Pol	LAJ*	-	12/89
LATVIA	Latvian Ruble	LVR	-	12/94
LITHUANIA	Talonas	LTT	-	07/93
LUXEMBOURG	Convertible Franc	LUC	989	03/90
	Financial Franc	LUL	988	03/90
MALDIVES	Maldive Rupee	MVQ*	-	12/89
MALI	Mali Franc	MAF*	-	12/89
		MLF	446	11/84
MALTA	Maltese Pound	MTP	-	06/83
MEXICO	Mexican Peso	MXP	-	01/93

* Non ISO code

Table 3 (Continued)

ENTITY	Historic Currencies	Code	Numeric	WD
MOZAMBIQUE	Mozambique Escudo	MZE	-	Between 1978-1981
NICARAGUA	Cordoba	NIC	-	10/90
PERU	Sol	PES	-	02/86
	Inti	PEI	-	07.91
	Sol	PEH*	-	1989/1990
POLAND	Zloty	PLZ	616	01/97
ROMANIA	Leu A/52	ROK*	-	1989/1990
SOUTH AFRICA	Financial Rand	ZAL	991	03/95
SOUTHERN RHODESIA#	Rhodesian Dollar	RHD	-	Between 1978-1981
SPAIN	Spanish Peseta ("A" Account)	ESA	996	Between 1981-1983
	(convertible Peseta Accounts)	ESB	995	12/94
SUDAN	Sudanese Pound	SDP	-	06/98
UNION OF SOVIET SOCIALIST REPUBLICS#	Rouble	SUR	-	12/90
YEMEN, DEMOCRATIC OF	Yemeni Dinar	YDD	720	09/91
UGANDA	Uganda Shilling	UGS	-	05/87
	Old Shilling	UGW*	-	1989/1990
UKRAINE	Karbovanet	UAK	804	09/96

* Non ISO code
Change in country name.

Table 3 (Continued)

ENTITY	Historic Currencies	Code	Numeric	WD
URUGUAY	Old Uruguay Peso	UYN*	-	12/89
	Uruguayan Peso	UYP	-	03/93
VIETNAM	Old Dong	VNC*	-	1989/1990
YUGOSLAVIA	New Yugoslavian Dinar	YUD	-	01/90
	Yugoslavian Dinar	YUN	890	11/95
ZAIRE	Zaire	ZRZ	-	02/94
	New Zaire	ZRN	180	06/99
ZIMBABWE	Rhodesian Dollar	ZWC*	-	12/89
ENTITY AND CURRENCY NOT APPLICABLE	RINET Funds Code	XRE	N/A	11/99

* Non ISO code

ANNEX

INFORMATION TO BE PROVIDED BY THOSE MAKING APPLICATION FOR THE ISSUE OF NEW CODES, AMENDMENTS AND DELETIONS.

Applications for additions or changes to the code lists are acceptable from any source. However, on order to ensure rapid processing by the Secretaries, the information required from applicants has been laid down as follows:

(a) Name of entity

(b) Name of currency

(c) The institution responsible for the currency (name and place of operation).

(d) Requirements:

(1) Whether currency or funds code: if funds code, give definition and proposed use;

(2) If new code, make proposal;

(3) If revision, state existing code and make proposal;

(4) If deletion, indicate code to be deleted;

(e) Reason for application;

(f) Evidence of support (currency code only);

(g) Date of implementation (indicate if special conditions of urgency apply);

(h) Application submitted by (name, address, telephone, telex numbers, etc, of applicant);

(i) Date of application.

Applications should be addressed to

Miss A M Wadsworth Tel. (0181) 996 7466 National
Secretariat for ISO4217MA +44 181 996 7466 International
BSI
389 Chiswick High Road Fax (0181) 996 7466 National
London +44 181 996 7466 International
W4 4AL United Kingdom

Appendix 2

Battery Operated Card Reader

A2.1 Special Application

The Battery Operated Card Reader described below is a special application of the MDB/ICP specification (non-standard) and is not sanctioned by NAMA. It is provided here to document an application that exists in use today.

A2.2 Extension to MDB/ICP – Card Reader Using Standby Feature

Some Vending machines use battery operated equipment. According to this feature, these machines and all devices used within these machines must provide a standby operating mode.

During standby operation - necessary for saving battery power while the machine is not in use - all devices shall consume a minimum standby current. Any device is equipped with some hardware wake-up mechanism. Both standby current and wake-up mechanism is to be defined in the device related hardware specification.

After wake-up, a device uses normal operating current, until a defined shutdown sequence is established and the device enters standby mode again.

The following specification shows the extensions and procedures for a normal MDB/ICP card reader and VMC-controller necessary to do wake-up and shut down sequences. The hardware specification related to wake-up is a separate BDTA-document. To understand the following details, it is necessary to know, that a separate bi-directional wake-up pin is applied to the card-reader. Pulling the wake-up line (from the card-reader while a card is inserted), both card-reader and VMC will be brought to normal operation mode.

A2.3 Extension to MDB/ICP – SETUP Config Data

SETUP (11H)	Config Data (00H) Y1	VMC Feature Level Y2	Columns on Display Y3	Rows on Display Y4	Display Info Y5

Y1 : Configuration data.
VMC is sending its configuration data to reader.

Y2 : VMC Feature Level.
Indicates the feature level of the VMC. The available feature levels are:

<u>01</u> - The VMC is not capable or will not perform the advanced features as specified in <u>Table 1: COMMANDS & RESPONSES</u> following Section 7.3.2. The reader will not provide advanced information to the VMC, but can do the advanced features internally (transparently to the VMC). The reader has no revaluation capability.

<u>02</u> - The VMC is capable and willing to perform the advanced features as specified in <u>Table 1: COMMANDS & RESPONSES</u> following Section 7.3.2. The reader will provide advanced information to the VMC (if possible) and will not do the advanced features internally.

<u>03</u> - The VMC is able to support level 02, but also supports some or all of the optional features listed in the EXPANSION ID command (i.e., file transfer, 32 bit credit, multi-currency / language features, negative vend, and / or data entry).

81H: VMC is Level 01, but battery operated.
82H: VMC is Level 02, but battery operated.
83H: VMC is Level 03, but battery operated.

Y3 : Columns on Display. The number of columns on the display. Set to 00H if the display is not available to the reader.

Y4 : Rows on Display.
The number of rows on the display.

Y5 : Display Information - xxxxxyyy

xxxxx =	Unused
yyy =	Display type
000 :	Numbers, upper case letters, blank and decimal point.
001 :	Full ASCII
010-111:	Unassigned

Reader Config Data (01H) Z1	Reader Feature Level Z2	Country / Currency Code High Z3	Country / Currency Code Low Z4	Scale Factor Z5	Decimal Places Z6	Application Maximum Response Time Z7	Miscellaneous Options Z8

Z1 : READER - Configuration data.
Indicates the payment media reader is responding to a SETUP - Configuration data request from the VMC.

Z2 : Reader Feature Level.
Indicates the feature level of the reader. Currently feature levels are:

01 - The reader is not capable or will not perform the advanced features as specified in Table 1. COMMANDS & RESPONSES following Section 7.3.2. The reader will not provide advanced information to the VMC, but can do the advanced features internally (transparently to the VMC). The reader has no revaluation capability.

02 - The reader is capable and willing to perform the advanced features as specified in Table 1. COMMANDS & RESPONSES following Section 7.3.2. The reader will provide advanced information to the VMC (if possible) and will not do the advanced features internally.

03 - The reader is able to support level 02, but also supports some or all of the optional features listed in the EXPANSION ID command (i.e., file transfer, 32 bit credit, multi-currency / language features, negative vend, and / or data entry).

80H: This bit is additionally set, if the reader is capable to work in battery operation mode and should be compared with the VMC against its own working mode. This is also done from the reader against the VMCs request in Y2.

Z3-Z4 : Country / Currency Code - packed BCD.
The packed BCD country / currency code of the changer can be sent in two different forms depending on the value of the left most BCD digit.

If the left most digit is a 0, the International Telephone Code is used to indicate the country that the changer is set-up for. For example, the USA code is 00 01H (Z3 = 00 and Z4 = 01).

If the left most digit is a 1, the latest version of the ISO 4217 numeric currency code is used (see Appendix A1). For example, the code for the US dollar is 18 40H (Z2 = 18 and Z3 = 40) and for the Euro is 1978 (Z3 = 19 and Z4 = 78). Use FFFFh if the country code in unknown.

For level 3 cashless readers, it is mandatory to use the ISO 4217 numeric currency code (see Appendix A1).

Z5 : Scale Factor.

The multiplier used to scale all monetary values transferred between the VMC and the reader.

Z6 : Decimal Places.
The number of decimal places used to communicate monetary values between the VMC and the payment media reader.

All pricing information sent between the VMC and the payment media reader is scaled using the scale factor and decimal places. This corresponds to:

$$\mathrm{ActualPrice} = P \cdot X \cdot 10^{-Y}$$

where P is the scaled value send in the price bytes, and X is the scale factor, and Y is the number of decimal places. For example if there are 2 decimal places and the scale factor is 5, then a scaled price of 7 will mean an actual of 0.35.

Z7 : Application Maximum Response Time - seconds.
The maximum length of time a reader will require to provide a response to any command from the VMC. The value reported here supercedes the payment reader's default NON-RESPONSE time defined in section 7.5 if the value reported here is greater.

Z8 : Miscellaneous Options - xxxxyyyy

xxxx: Unused (must be set to 0)

yyyy: Option bits

b0=0: The payment media reader is NOT capable of restoring funds to the user's payment media or account. Do not request refunds.

b0=1: The payment media reader is capable of restoring funds to the user's payment media or account. Refunds may be requested.

b1=0: The payment media reader is NOT multivend capable. Terminate session after each vend.

b1=1: The payment media reader is multivend capable. Multiple items may be purchased within a single session.

b2=0: The payment media reader does NOT have a display.

b2=1: The payment media reader does have its own display.

b3=0: The payment media reader does NOT support the VEND/CASH SALE subcommand.

b3=1: The payment media reader does support the VEND/CASH SALE subcommand.

b4-b7=0 Any future options must be covered by the EXPANSION COMMAND option bits.

Note: The following changes are the only changes to upgrade to battery operated readers:

If a VMC is battery operated, it signals the card reader with the flag 80H to work in battery operation mode. Within byte Z2 the reader also sets the flag to 80H to signal standby feature capability.

If only one of both is in standby capability, this results in an configuration error and the manufacturers should deal with handling of this condition. Assume that at least one device will not enter standby mode and therefore battery lifetime is dramatically reduced!

A2.4 VMC-Reader Operation Sequences

The VMC and the Reader should operate during battery mode in the following way:

After wake-up, the VMC starts with the normal sequences:

Reset
Setup/Config
MAX/MIN-price
Identify
Enable
Poll

During these sequences, the VMC has two possibilities to signal the Card-Reader, not to enter standby-mode again:

Pulling the wake-up pin to low level
Running poll sequences in continuos timing.

If neither the wake-up pin is driven low, nor any command is further sent to the card reader, the reader enters standby state after its Application Maximum Response Time (normally defined to 5 sec in ICP, but sent in byte Z7 of status response)

During card operation, the sequences continue normally with

Begin Session
Vend Request
Vend Accepted
Vend Success
Cancel Session/Session Complete

Whenever a cancel session or session complete command is received, the reader should stop all internal work after a defined timeout period (Application Maximum Response Time) is finished after the last command sequence and after the wake-up pin is not pulled low.

The VMC should stop polling after the cancel session or session complete command and additionally should no longer pull wake-up pin.

If even the reader or the VMC may wish any further communication (i.e. for additionally trailing display messages or multi vend purposes or etc.) the reader can use any non idle answer to the poll command (i.e. the display message) whereas the VMC can continue polling or pulling the wake-up pin.

Note that the wake-up pin may not be used from the reader to hold on operation, cause dynamic system consideration and of course holding more devices within the system in normal operation mode is not a good job.

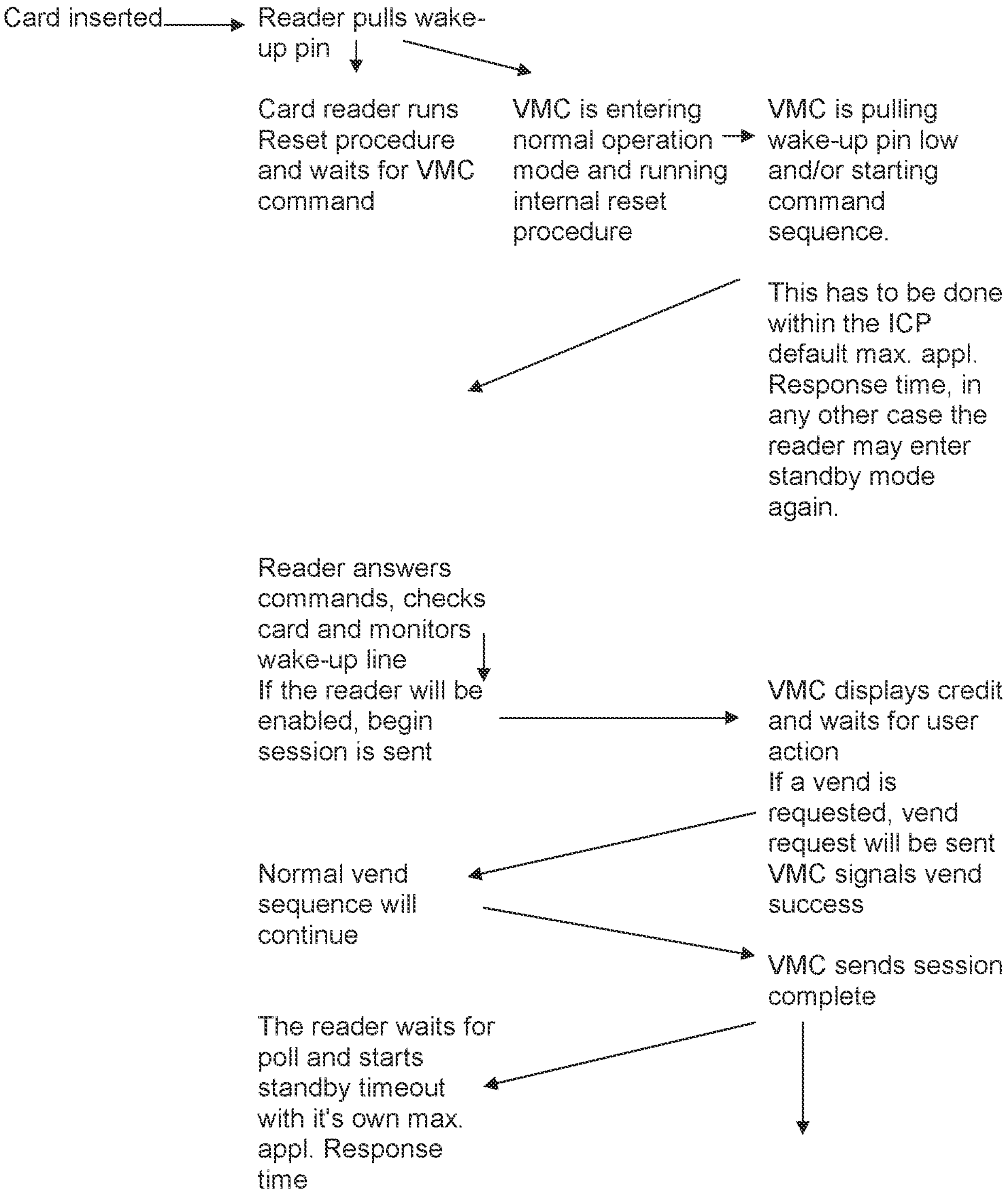
The reader should be in a power saving mode after this timeout period where power consumption is less than 10 uA.

To allow the reader holding VMC operating, at least 5 poll have to be sent, after the cancel session or session complete. If any one of these polls is answered different with only a ACK, 5 polls have to be sent again. Note, that if a display message is sent, display time is added!

If the reader entered standby state, and a new card is inserted, the procedure starts a again.

Whenever during this next session, the reader should avoid all unnecessary work, i.e. display messages like „reader xyz, Software version 99.4711“ or „checking RAM“ and so on should be avoided. While in battery operation, the user has inserted a card and is waiting for display of his fund, to continue with a vend and is not interested in service related messages.

A2.5 Session Example



Card inserted

Reader pulls wake-up pin

Card reader runs Reset procedure and waits for VMC command

VMC is entering normal operation mode and running internal reset procedure

VMC is pulling wake-up pin low and/or starting command sequence.

This has to be done within the ICP default max. appl. Response time, in any other case the reader may enter standby mode again.

Reader answers commands, checks card and monitors wake-up line

If the reader will be enabled, begin session is sent

VMC displays credit and waits for user action

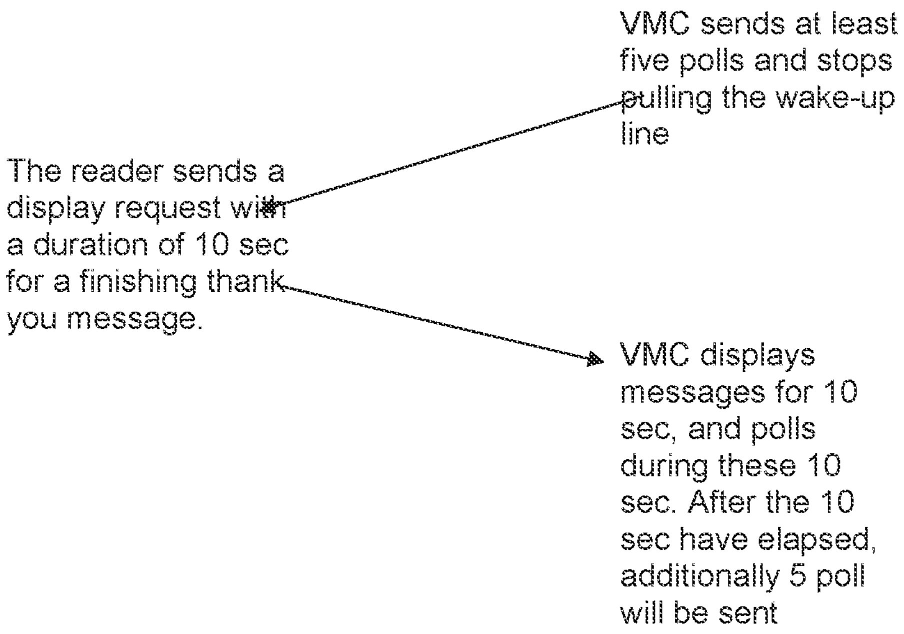
If a vend is requested, vend request will be sent

Normal vend sequence will continue

VMC signals vend success

VMC sends session complete

The reader waits for poll and starts standby timeout with it's own max. appl. Response time



VMC sends at least five polls and stops pulling the wake-up line

The reader sends a display request with a duration of 10 sec for a finishing thank you message.

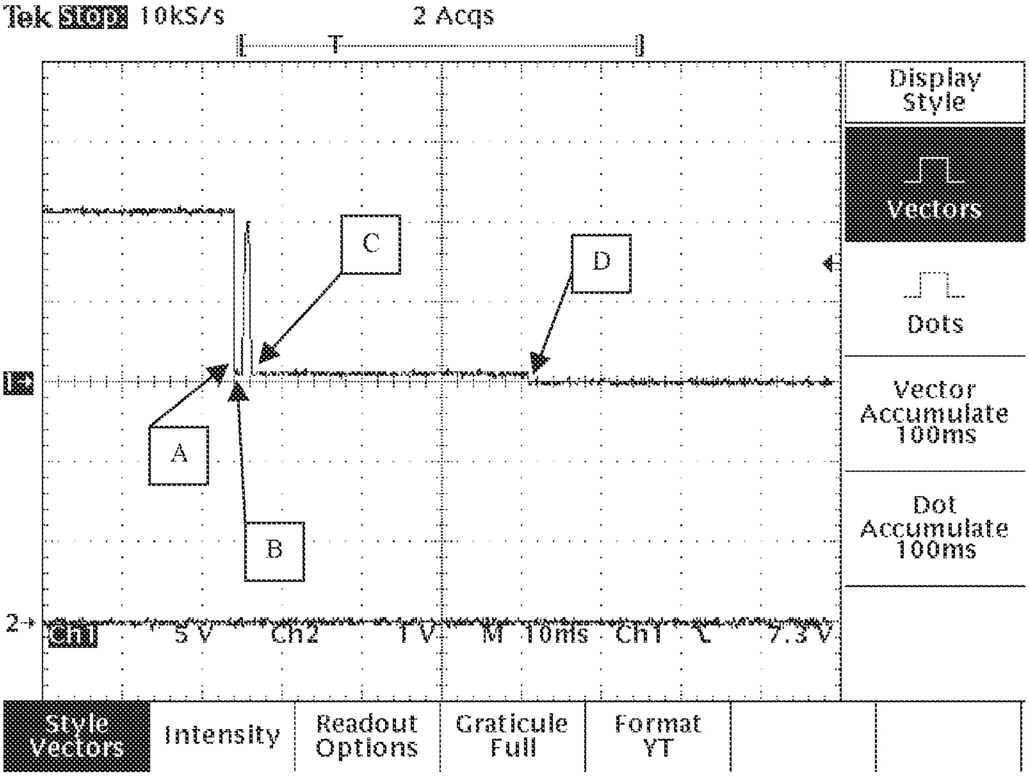
VMC displays messages for 10 sec, and polls during these 10 sec. After the 10 sec have elapsed, additionally 5 poll will be sent

A2.6 Hardware Considerations

Hardware Considerations

Within this special battery operation, the pin 3 of MDB/ICP connector is used as a wake-up signal. Refer to special BDTA-hardware specification.

To show an example of the timing for this pin, refer to the following diagram, which gives an example of all special timing problems related to more than one wake-up condition.



Position A: mechanical switch on VMC is pulling pin 3 low (i.e. door switch)
Position B: mechanical switch is released
Position C: card reader has finished reset routines and pulls pin 3 low
Position D: VMC has finished reset routines and pulls pin 3 low too.

If a card is inserted first, pin 3 may be pulled low first at position B.
If VMC is waked up via other means, maybe card reader is waked up at position D first.

In any case, this is a good example to clarify different waveform conditions on pin 3. Please note that any device may release pin 3 after a short duration (<1ms) cause pin 3 should work as dynamically wake-up. Holding pin 3 permanently low may prevent other devices from wake-up, i.e. after all devices ran into timeout and one is still holding pin 3, the other can no longer enter ready state (Note i.e. to door-switches etc.)

(this page intentionally left blank)

Appendix 3

MDB Recommended "Best Practices"

The following sections make recommendations that are intended to help reduce compatibility issues. Note that when developing a device you should not assume other devices or VMCs will follow these recommendations. Your device or VMC must meet the full MDB specifications!

1. **Physical Connections (Power/Voltage/Connection)**
2. **Timing Considerations (Lowest Level/Time-out)**
3. **Commands, Repetition, ACK, NAK**
4. **Logical Level, Processing**

1. Physical Connections (Power/Voltage/Connection)

Voltage specification (General)

Verify that the VMC meets the min MDB voltage at max load with the min input line voltage.

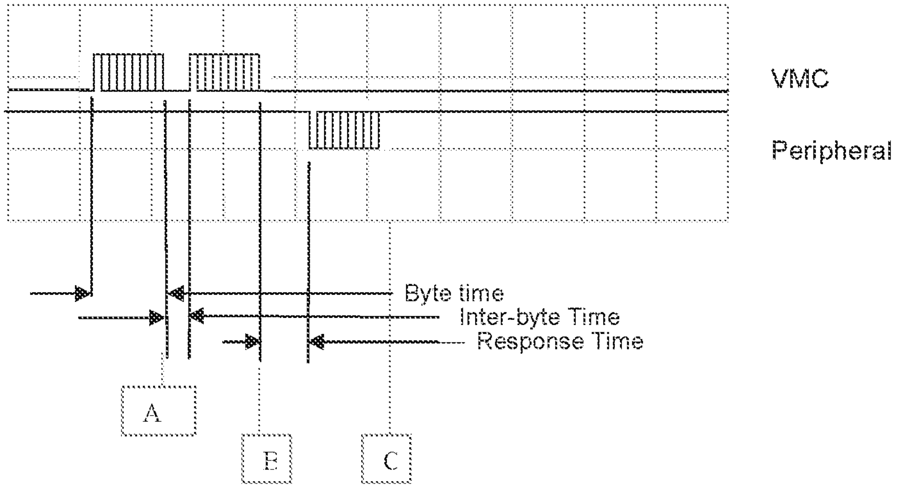
2. Timing Considerations (Lowest Level/Time-out)

Timing Considerations (General)

To avoid timing issue (Section 3.1 Timing Definitions) it is recommended that you allow for some margin in your design. See table below:

Item	MDB Specification	Tolerated values
Communication startup	200ms	500ms
Communication response time (when waiting for a response)	5ms max	20ms*
Communication response time (when sending a response)	5ms max	4ms
Interbyte time (when receiving data)	1ms max	5ms*
Interbyte time (when sending data)	1ms max	0.8ms
Non-Response time (the time the device may be busy performing other processes. I.e., validating coins)	Varies per device	Plus the time between polls
Application Non-Response time (time that can be reprogrammed to be different from the default Non-Response time.	Varies per device	Plus the time between polls

*Using the tolerated values will provide compatibility with older equipment manufactured under the EVMMA version of the MDB specification that had the Communication response time at 20ms and Interbyte time at 5ms. The transmitting device must always use the values of the MDB specification.



Please note, that the receiving device at the bus (master or slave) will get a receive interrupt (using standard UART devices) only after the byte is fully transmitted. These are the positions A, B, and C in the above diagram.

Therefore, the receiving device needs to set a higher value for the interbyte timeout, because it needs to add at least the transmission time for one byte (which is 1 start bit + 9 data bits + 1 stop bit at a rate of 9600 baud equal 1.2 ms). The same happens for the response timeout, because the response is first detected, while the first byte is fully received.

Another common implementation error is checking the response timeout after the whole response message is received. This will never work because if, for example, the response is more than 5 bytes, the transmission time for 5 bytes will be more than 5 ms and will always timeout.

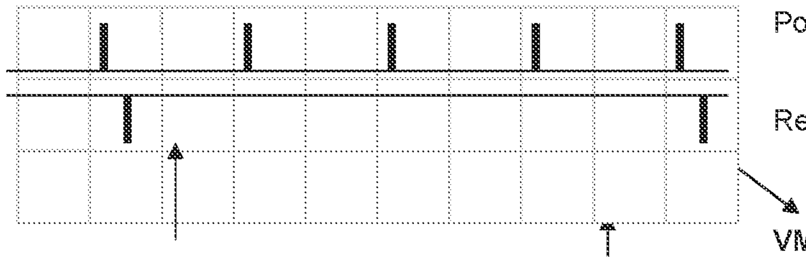
POLL Frequency (General)
Section 2.4.3 states, "Each peripheral should be polled every 25-200 milliseconds." However, the VMC is likely to stop communication during a vend or at other times when it does not need to communicate with the peripherals. Note that this may cause the peripheral(s) to RESET, see "Non-communication Time-out"-section in this document.

Because of this, poll frequency is not as important as many people think it is.

While not specifically prohibited, polling at a high rate while waiting for a response will usually delay the response, as the peripheral will have to service the POLL. Polling at a very low frequency, however may decrease coin or bill acceptance rate.

For all devices, the recommended VMC POLL frequency is 125ms - 200ms.

Example for a cashless device card acceptance:



VMC has received the begin session!

Card inserted, reader begins checking it and is no longer able to respond

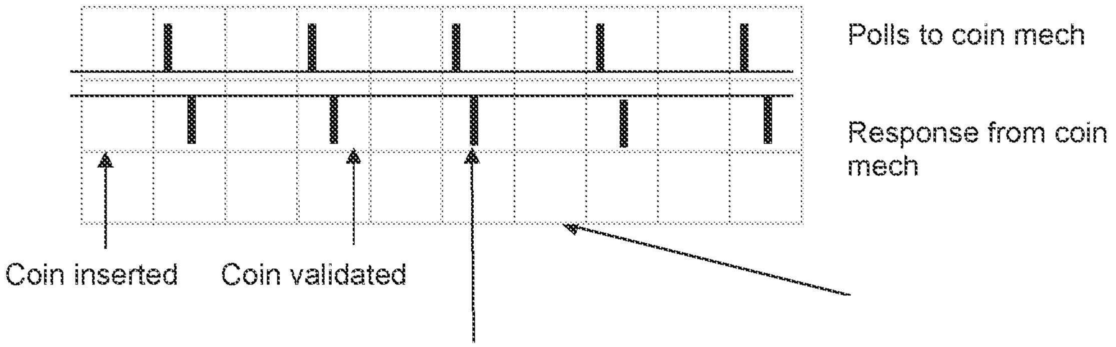
Card validated, reader is able to respond with begin session, but has to wait for the next poll.

As shown in the above diagram, the time from card insertion to credit being displayed on the vending machine is not specifically related to the polling rate. After the card is inserted, the card reader validates the card. During this time, some card readers are no longer able to answer the poll, others answer with an ACK only.

When card validation is finished, the reader is ready to send the begin session, which will result in the balance of the card being displayed on the VMC. Obviously, this and only this depends on polling frequency. The time to the next poll has to be added to the validation time to get the maximum time before the credit is displayed.

Please note that some readers may need significant processing time to answer the polls. If a developer increases the polling frequency, this would extend the validation time instead of getting a faster reaction with begin session.

Example for a coin acceptor:



Coin Accepted message sent to VMC, coin mech re-enables acceptance.

Note that some coin acceptors can send more than one coin message in response to a poll. The VMC must be able to parse multiple coin messages from one poll response.

General Data Response Timeout

Unless otherwise specified, a VMC should wait at least 30 seconds for a response to commands that require data to be returned. This does not infer that the device is not ACKing POLL commands, but rather the VMC is waiting for data pertaining to the command. I.e., for a PAYOUT VALUE command, the coin mech should respond to each PAYOUT VALUE POLL within 30 seconds.

Non-communication Timeout (General)
If a peripheral does not communicate with the VMC for an extended period of time, that peripheral should take care of any relevant house-keeping and then RESET. This time should be of sufficient length to guarantee that communications with the VMC have been completely lost. The recommendation is to wait at least 10 times the max response time for a device.

If the VMC does not successfully communicate with a peripheral for the 'application maximum response time', it should attempt to RESET that peripheral once every 10 seconds (Section 2.4.3 POLLing) and continue operations (if possible) with the other MDB peripheral(s) that are still responsive.

Poll Responses covered by note 1 -Sent once each occurrence (Coin Mech)
Some devices send this response each time the changer detects the condition. For example, the changer sees the gate open so it sends the escrow request, if the next time it checks it see the gate open it will send the escrow request again. Other devices will only send it once until the gate returns to the normal position.

It is recommended to send it only once.

3. 3. Commands, Repetition, ACK, NAK

NAK and RET (Section 2.2 Block Format)
The purpose of a NAK is ONLY to indicate a message has been received with a bad checksum. NAK is never intended to be used for a command that is understood, but not executable.

Since the error may be caused by the corruption of the address byte (shown in the following example), it is not recommended to use the NAK, but rather to not response. The 5ms non-response timeout will be treated as if it were a NAK (Section 2.2 Block Format/Master-to-Peripheral, Peripheral-to-Master and Response Codes).

RET is a VMC-only response that is sent to a peripheral to force it to retransmit its previous (and presumably good) response. (Section 2.2 Block Format/Response Codes).

Example of NAK or 'no NAK' with an error in the address byte:

The following example shows how you can get in trouble with a simple RESET COMMAND sent to a cashless device. Whereas the cashless device itself receives the command without error, the bill validator in the system sees a voltage transient (corruption) of the address byte.

VMC sends	**Cashless received**	**Billval received**	**Cashless response**	**Bill validator response**	
POLL to cashless	POLL valid CRC	command to other address			
			Sends a JUST RESET	Sends nothing	
Sends ACK to previous received just reset	ACK	ACK			
			Nothing	Nothing	
RESET to cashless	RESET valid Checksum	Instead of command to its address, receives command to address 30H with Checksum 10H (because the destination 10H address byte was modified by transient voltage)			
			Sends ACK after 4ms	Sends NAK after 1 ms	*
			Sends ACK after 1ms	Sends NAK after 4 ms	**
			Sends ACK after 3ms	Sends nothing	***

As is shown, with only a single bit toggled (10h is modified to 30h). Three different reactions are possible:

* 1st Example (shown in Blue):
The VMC receives a NAK first, but 3ms later, an ACK would arrive. If the VMC immediately sends a different command after the NAK the further answer of the next device would collide with the ACK of the cashless and cause a second failure.

** 2nd Example (shown in Red):
The VMC receives the correct ACK first and continues immediately (if it is using a very fast polling rate). The NAK of the bill validator will collide in any case with the next message and cause further errors!

*** Last example (shown in Green):
The VMC receives the correct ACK first and continues immediately (if it is using a very fast polling rate). The bill validator will not cause any further errors, because it sends nothing. In this, and only this case, if the cashless device has a checksum

error too, both devices would not answer. The VMC would then repeat the command after 5 ms, because it would interpret the timeout as an NAK.

Recommendations from here:

Newer peripherals should never send a NAK, to avoid further handling errors.

Newer VMCs should never try to increase the polling rate if they receive a NAK from a peripherals, instead they should wait for the full timeout period to expire (and skip) further ACK's and NAK's from other peripherals. Please note that if you have four peripherals on the bus, the VMC may receive at least four ACK's and/or NAK's in or out of sequence!

To improve system reliability you should implement the bit counting method defined in the note of page 2-4 of the MDB specification.

Command Repetition (General)
VMC commands which are not ACKed should be repeated for the duration of the non-response time-out. If the command is not a POLL it is recommended that the command should alternate with a POLL. This does not mean that the VMC cannot communicate with other peripherals on the bus, but it should continue to communication with any non-responsive peripheral until it can reliably conclude that it is offline. At that point, it should start trying to RESET that peripheral once every 10 seconds. (Section 2.4.3 POLLing). When it receives a response to the RESET the VMC will need to re-initialize the peripheral.

Command Repetition (special commands)
VMC commands which are not ACKed should be repeated for the duration of the non-response time-out. Please note, that this is a general guideline, which in some circumstances may not be a "successful" implementation.

<u>Condition 1 (coin mech dispense)</u>
If a dispense command is not ACKed, this may be
a) a misunderstanding by the peripheral
b) a corrupted bus signal
c) another peripheral corrupting the bus

If the command itself did not arrive at the coin mech, repetition is ok. If the command arrived at the coin mech, but the VMC did not see the ACK, repetition obviously leads into multiple coin dispense!!!

In this situation, it is recommended not to re-send the command multiple times, although the choice is ultimately down to the system designer, and to wait for a while before restarting communications. This will allow any noise on the bus to dissipate.

<u>Condition 2 (bill validator or coin mech acceptance)</u>
If a bill validator accepts a bill or a coin mech accepts a coin, this is reported during the next poll to the VMC. This message is then ACK'ed by the VMC.
If this ACK is not detected by the bill validator or coin mech, for whatever reason, the peripheral repeats the message (this means, the same coin or bill value is sent again).

If the bill or coin value message did not arrive at VMC, repetition is ok. However, if the command arrived at the VMC, but the bill validator or coin mech did not see the ACK, repetition obviously leads into increasing credit!!!

Recommendation to minimize this effect especially for bill validators with high denomination values:
Whenever a VMC receives a bill (or coin) message, it should send the ACK, process the bill (or coin), wait for the recommended maximum response timeout (20ms) and send an additional poll.
If the VMC receives the same bill (or coin) message again after 20ms, (instead of receiving an ACK only) this can be assumed to be a repetition due to non-received ACK. If nothing is reported or a different value is sent, the ACK was understood or a new bill (or coin) has arrived.
This solution assumes, that bill (or coin) insertion is much slower than 20ms (which obviously is true especially for bill vals)

Command Order (General)
In most cases the VMC can send any command at any time in any order. Note the Cashless device spec is the only peripheral that defines the sequence of commands.

Command Out-Of-Sequence (Cashless Payment Device)
If the VMC receives a Command Out-Of-Sequence from a cashless payment device, it is a clear indication that the state of the cashless payment device is no longer in synch with the VMC. The VMC should take care of any relevant house-keeping and then issue a RESET to the cashless payment device. This will put both parties in a known state of operation.

4. Logical Level, Processing

Maintaining MDB Level Compatibility (General)
In a system where the peripheral supports a higher level MDB protocol than the VMC, the peripheral should revert to the lower level MDB protocol to communicate with the VMC. (Section 1.3.1 Levels and Section 2.4.4 Levels)
In a system where the VMC supports a higher level MDB protocol than a peripheral, it is the responsibility of the VMC to revert to the lower level MDB protocol when communicating with the peripheral. (Section 1.3.1 Levels and Section 2.4.4 Levels)

Response data length (General)
Note that some responses for peripherals can be variable length (tube status, poll, etc.). For example, a peripheral can send multiple messages in response to a poll command. Note that the 9th mode bit should be set on the last byte of the data being received (see section 2.5 Typical Session Examples)

Scale Factors (General)
The VMC needs to be able to handle devices with different scaling factors. The VMC needs to determine the least common dominator and adjust the values from each device.

Decimal point (General)
The decimal point information is only used to set the position on a credit display (it doesn't adjust the values).

Country Codes (General)
Do not require devices to have the same country code. In July 2000 the spec changed to use the ISO4217 numeric currency codes. Devices before that date used the international telephone codes.

Just Reset (General)
If a device sends a just reset response, the VMC should re-initialize the device (request setup information, re-enable the device, etc.). Don't send a reset command.

Multiple Coin Reporting
The VMC must take into account that coin mechs can send the value of more than one coin in one poll response.

Multiple Bill Reporting
The VMC must take into account that bill validators can send the value of more than one bill in one poll response.

Power-Up Sequence (Cashless Payment Device)
The following sequence is recommended as the power-up process for cashless payment devices. Post-RESET ACKs are not explicitly listed and are implied.

Send RESET until ACKed.
POLL until JUST RESET response.
Send SETUP/CONFIG command.
POLL until READER CONFIG response.
Send MAX/MIN PRICE command.
Send EXPANSION ID REQUEST.
POLL until PERIPHERAL ID response.

Send READER ENABLE command when ready.

Cashless Payment Device Enable/Disable (Cashless Payment Device)
While it is specifically allowed for "grandfather" reasons, a VMC should never need to disable a cashless payment device during a session. However, if this does occur, the cashless payment system should complete the session-in-progress normally (Section 7.4.12 READER – Disable), and subsequently refuse to start any new sessions with the VMC until enabled.

Level 2 BEGIN SESSION Command (Cashless Payment Device)
The description of Byte Z8 of the Level 02/03 BEGIN SESSION message (Section 7.4.4 POLL) appears to match the EVA-DTS Standard v.5.0, App. A.1 Definitions. All NAMA MDB specification references in this document are based on Version 3.0 (Draft 1), dated March 26, 2003, always refer to the latest EVA-DTS version.

Cashless Payment Device Discounting (Cashless Payment Device)
The VMC should not make any financial decision(s) based on the BEGIN SESSION balance. Some cashless peripherals support various types of discounting. Consequently, the VMC should not terminate a session if the reported balance is less than the minimum price or refuse to issue a VEND REQUEST when the list price of a selected item exceeds the reported balance of funds.

Similarly, if a cashless payment device reports a starting balance of 0xFFFF in the BEGIN SESSION message, the VMC should proceed normally i.e., permit a product selection. A BEGIN SESSION balance of 0xFFFF means that the available fund balance is not currently known and/or should not be displayed. It is not meant to suggest that the balance is insufficient for operation. An appropriate message for the customer should be displayed instead of the balance – i.e. "Please make a selection".

Revalue Limit Requests (Cashless Payment Device)
Similar to discounting, some cashless devices are capable of granting "bonus" credit to users (i.e., giving $6.00 credit for a $5.00 bill). There may also be cases where a cashless device pre-deducts sales tax resulting in a credit that is less than the amount in the REVALUE command. Finally, most cashless devices that store credit on the media have a maximum allowable credit.

Consequently, the VMC should issue a REVALUE LIMIT REQUEST prior to determining which fund sources (e.g. note values) are applicable to a user. In a multivend environment, this means the VMC must issue multiple REVALUE LIMIT REQUESTs.

If a cashless device cannot accept credit, either because the operation is not acceptable at this time or because the current media has reached its maximum credit limit, the device should respond to a REVALUE LIMIT REQUEST with a REVALUE DENIED not a REVALUE LIMIT of $0.00. The REVALUE DENIED response clearly signals that revalue is not an acceptable operation.

Balance Display (Cashless Payment Device)
For VMCs that opt to show the available funds, it is important to consider the following:
Cashless payment devices with active discounts will deduct less than the VEND REQUEST amount. The displayed balance in the VMC must reflect the difference between starting balance and the amount in the VEND APPROVED message (not the VEND REQUEST). This assures that the displayed balance on the VMC is correct, and (where applicable) matches the cashless payment device's display.

Because the REVALUE APPROVED message does not contain an amount field like VEND APPROVED, the VMC is not capable of tracking card balance correctly in a "bonusing" environment.

Multi-Vend (Cashless Payment Device)
Multi-vending is the practice of vending multiple products within a single session. While multi-vending is a function of the VMC, it should only be attempted when the multivend bit (b1) of the Miscellaneous Options byte (Section 7.4.2 Setup- Config Data/ Byte Z8) of the cashless device's configuration data is set (b1=1).

If a VEND DENIED scenario occurs during a multi-vend session, the VMC has the option to terminate or continue the vend session. It may be that the user tried to buy something that cost more than his balance. If the VMC has less expensive goods to vend, continuing the session would give the user an opportunity to select something affordable.

If a VEND FAILURE scenario occurs during a multi-vend session, the VMC should always issue a VEND FAILURE to the cashless payment device. The VMC has the option to terminate or continue the vend session. It may be that the user selected an empty column, and another selection will be successfully vended.

Display Messages (Cashless Payment Device)
If Byte Y3 (Columns) and/or Y4 (Rows) of the SETUP/CONFIG message are zero, VMC display is not available for use by the cashless payment device (Section 7.4.2 SETUP – Config Data).
If the display is available, a Display Request message can be sent anytime after the power-up sequence has been completed. In practice, there are only a few conditions under which the cashless payment device should make a Display Request:

1. Immediately after the power-up sequence is completed to display the cashless payment system's software revision number. This should not create significant problems because it only happens at power-up.
2. Anytime the cashless device is out of service.
3. In the enabled state to indicate an error accessing the media (e.g. busy signal for a credit card reader). This should not create a conflict because a) it is transient, and b) the user should be concentrating on the purchase process.
4. In the enabled state to prompt the user (e.g. for a PIN). This should not create a conflict because a) it is transient, and b) the user should be concentrating on the purchase process.
5. In the enabled state to inform the user of the funds available for purchase. This should not create a conflict because a) it is transient, and b) the user should be concentrating on the purchase process.
6. During session idle (e.g. after a VEND DENIED to indicate the reason for the refusal). This should not create a conflict because a) it is transient, and b) the user should be concentrating on the purchase process.

If the VMC reports itself to support Full ASCII (Y5 = xxxx001b) then it will support all printable ASCII characters (0x20 thru 0x7F). If values outside this range are used, the results are dependent upon the actual display controller chip. This is strongly discouraged.

Selected Number (Item Number or Product Code?) (Cashless Payment Device)
The selected number should be the vending machines selection number, which is normally the product key index. If the VMC i.e. has a two digit input, where one is alphanumerical, ("A-1" or "C-6" or ..), it has to convert it in a appropriate way to a number. To be compatible to all versions of card-readers and DTS-versions, ensure the number is in the range of 1-n. The maximum of n depends on the level used and options (1-255 or 1-65535).

The conversion method and the maximum selection number should be published by the VMC vendor to ensure the correct settings of the cashless device. Vice-versa, the cashless device vendor should publish the maximum usable numbers of selection, and the default action, if a selection number out of this range is sent.

Normally, this default action should result in a simple conversion to the maximum number and accepting the price from the vending machine, skipping all internal discounts etc.

Combining a VMC and a cashless device which do not have compatible maximum selection numbers is not an issue MDB has to solve, but is an application setup error.

Bill Stacking/Escrowing (Cashless Payment Device)
As a general practice, the VMC should escrow any bills tendered for credit to a cashless payment device until it has verified that the cashless payment medium can accept the full credit amount. This is done via the REVALUE LIMIT REQUEST command/response sequence. Once the value has been deemed acceptable, the VMC should stack/secure the bill prior to issuing the REVALUE REQUEST to the cashless payment device. This provides maximum protection against theft attempts. (Section 7.4.16 Revalue)

Mixed Tender Transactions (Cashless Payment Device)
Historically, this practice has been avoided by the VMC disabling the other peripherals when one becomes active (i.e., if someone inserts a bill into the validator, the VMC will disable the cashless payment device). If mixed tender transactions are to be supported, we must determine which fund source has priority for purchases, as well as for dispensing change.

There are two issues here:

1. If revalue is permitted, always revalue first, and then any purchase(s) should be from the card.
2. If revalue is not allowed, use cash first, and then deduct remaining funds from card.

Example: A mixed-tender VMC accepts $1.00 bill and a user inserts a $5.00 card.

Revalue Permitted: The $1.00 bill is stacked and a REVALUE REQUEST for $1.00 is sent to the cashless payment device. Once approved, any purchases should come from the $6.00 card balance.

Revalue Not Permitted: The $1.00 remains in escrow. The user selects a $1.50 item. The VMC sends a VEND REQUEST for $0.50 to the cashless payment device. If and only if it gets a 'vend approved', it will use/stack the $1.00 in escrow and sell the product. If it cannot stack it, the vend will be aborted and a vend failure will be sent. (Note: The cashless payment device will assume a $0.50 product was sold even though the Item Number may have been sold previously for $1.50.)

Obviously, this combination of settings causes more problems than the "non stacking" combination.

First: if the cashless gives a discount, the discount may reduce the price to a value less than the vend request (because the calculation uses the $1.50 value). This would result in stacking less than the whole bill, which is not possible! In this case, a vend denied should be sent. This method would temporarily disable the mixed payment.

Second: if refund is not possible, aborting of a vend will result in a credit loss situation. The VMC should use the opposite vend procedure – i.e. first stack the bill and then send the vend request. But, if in this case a 'vend denied' is received, the VMC needs to give change for at least the bill value!

MDB does not specify handling procedures for all these combinations – the operator needs to check the VMC and/or cashless capabilities as this is not an issue with the standards but a "market feature" problem.

Fund handling with a VEND FAILURE (Cashless Payment Device)
Normally funds are the responsibility of the fund source, (i.e., the cashless payment device). If a VEND FAILURE occurs the funds in question can be handled as follows:

NOTE: To prevent double refunds where the cashless payment device provides a process for refunds, the cashless device must indicate that the media supports refunds, regardless of whether or not it can actually transfer the lost funds back to the payment media.

The correct handling for vend failure is always, that no credit should be converted i.e. cash credit is escrowed, card credit is refunded. Card credit will never be transformed to cash!!

If the cashless device is not capable of refunding, for whatever reason, the VMC, and maybe the cashless device, may produce a log file or a statistic to ensure this is recorded. However, the credit balance in this case is always lost and may only be refunded to the customer by manual intervention (hotline, etc.)

If the cashless device is capable of refunding, nothing else is necessary. Sometimes, if a special card is used or the card is no longer present, refunding is not possible. In this case the same procedure as described above must be followed.

If the system allows the card refund amount to be transformed to cash, the following should be taken into account:

a. The VMC can make a record of the lost funds and remove them from escrow.
b. The VMC can retain the credit and allow it to be used as part of a cash purchase.
c. The VMC CANNOT dispense the funds as change. In the case of a credit card charge or where the original source of funds was a credit card transaction, this constitutes a cash advance, all be it small.
d. Please note further, that the VMC may have problems dealing with a discount amount.
e. Please note further, that the cashless payment scheme may not allow this behaviour.

Fund Handling with a Negative Vend Failure
After a vend is approved, it is up to the cashless device how it handles the negative vend value

State Machine (Cashless Payment Device)
The defined state machine within the standard is information for both VMC and cashless programmers of the logical steps required to run the device.

In any case, the state machine should never be used as medium to swap the Master-/Slave device functions. In MDB, the VMC is always the Master device. This results in a unspecified sequence of commands for the VMC (as for all other devices). i.e. even if the device has reached the begin session state, the VMC is allowed to send, for example, an FTL command. If the cashless is not able to support this command in the current state, it may send the applicable response (i.e. FTL denied), but will continue in the reached state!!

Further examples of this are multiple "Vend Session Complete" or similar commands. Because the cashless device enters the inactive state with the first vend session complete, further repeated commands will never produce any problems and may simply be ignored.

A lot of cashless devices use the "out of sequence" message in this case. This may be appropriate in terms of "educating the VMC programmer", but will never solve the issue. The "out of sequence" message usually causes the VMC to send a reset command to re-sync the devices. This is not a problem for the VMC, but can cause the cashless device to run into problems - mainly because the reset sequence of a lot of cashless devices can take many seconds, during which the customer is unable to use their cards. This obviously can lead to complaints.

The "Out of sequence" message should be the last resort for a cashless device, to be used only if it is unable to solve state machine problems any other way. Unfortunately, due to the polling mechanism with a finite polling frequency, the loss of synchronisation between the VMC and the cashless state is unavoidable.

An example of this is as follows:
After a card insertion we get a begin session.
Both devices enter the session idle state.
The customer presses the escrow lever and takes the card out simultaneously.
The VMC would send a Reader Cancel command, whereas the cashless would like to transmit an end session (because its session ended when the card was taken out).

The situation then arises that the cashless device is in the inactive state (no card present), but cannot send the message to the VMC (no poll available, instead a wrong command for this state).

The VMC, on the other hand, believes it is sending the correct command, as it is still in the session idle state. Hence, it would repeat the cancel session, until it is answered. It would then get a totally unnecessary "out of sequence", and maybe an additional "end session".

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/956,741	04/18/2018	Paresh K. Patel	104402-5033-US	9837

24341 7590 02/27/2023
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER
POE, KEVIN T

ART UNIT	PAPER NUMBER
3692	

NOTIFICATION DATE	DELIVERY MODE
02/27/2023	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

donald.mixon@morganlewis.com
padocketingdepartment@morganlewis.com

Office Action Summary	**Application No.** 15/956,741	**Applicant(s)** Patel, Paresh K.	
	Examiner KEVIN T POE	**Art Unit** 3692	**AIA (FITF) Status** Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 6/27/2022.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-20 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-20 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date ______.

3) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date ______.

4) ☐ Other: ______.

DETAILED ACTION

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA. This office action is in response to applicant's communication of August 16, 2022. The rejections are stated below. Claims 1-20 are pending and have been examined.

2. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Response to Amendment/Arguments

3. Applicant's arguments concerning 35 U.S.C. 103 have been considered and are persuasive so therefore the rejection has been withdrawn.

Claim Interpretation

4. In the interest of compact prosecution, Applicant should be aware that there is claim language that does not serve to differentiate the claims from the prior art and/or or provide an additional element that can be a consideration for eligibility[1]. *See* MPEP 2103(c).

[1] *See* MPEP 2106.04(d)(2) ("Examiners should keep in mind that in order to qualify as a "treatment" or "prophylaxis" limitation for purposes of this consideration, the claim limitation in question must affirmatively recite an action that effects a particular

Intended Use

5. Intended use language is generally not given patentable weight. *See* MPEP 2114(II) ("A claim containing a 'recitation with respect to the manner in which a claimed apparatus is intended to be employed does not differentiate the claimed apparatus from a prior art apparatus' if the prior art apparatus teaches all the structural limitations of the claim. *Ex parte Masham*, 2 USPQ2d 1647 (Bd. Pat. App. & Inter. 1987)."); *see also* MPEP 2103(C). Examples of claim limitations that are often found to precede intended use include "adapted to," "capable of," "sufficient to," "whereby," and "for."

6. Claim 1 recites "memory… the one or more programs comprising instructions for: broadcasting…". The limitation of "broadcasting"…etc. represent the intended use of the instructions and do not have patentable weight". Claims 2-5 and 16-18, also

Claim Rejections - 35 USC § 112(a)

The following is a quotation of the first paragraph of 35 U.S.C. 112(a):

> (a) IN GENERAL.—The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

7. Claims 1-14 and 16-17 are rejected under 35 U.S.C. 112(a) or 35 U.S.C. 112 (pre-AIA), first paragraph, as failing to comply with the written description requirement.

treatment or prophylaxis for a disease or medical condition. An example of such a limitation is a step of "administering amazonic acid to a patient" or a step of "administering a course of plasmapheresis to a patient." If the limitation does not actually provide a treatment or prophylaxis, *e.g.,* it is merely an intended use of the claimed invention or a field of use limitation, then it cannot integrate a judicial exception under the "treatment or prophylaxis" consideration. For example, a step of "prescribing a topical steroid to a patient with eczema" is not a positive limitation because it does not require that the steroid actually be used by or on the patient, and a recitation that a claimed product is a "pharmaceutical composition" or that a "feed dispenser is operable to dispense a mineral supplement" are not affirmative limitations because they are merely indicating how the claimed invention might be used.")

The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor or a joint inventor, or for applications subject to pre-AIA 35 U.S.C. 112, the inventor(s), at the time the application was filed, had possession of the claimed invention.

Lack of Algorithm

8. Claims 1 and 9 each recite "An electronic communication module comprising: …an interface that couples the communication module with an article of manufacture …". Applicant's electronic communication module is described in 0307 and 0321-0326 of Applicant's specification. Paragraphs 0321-0326 mirror the claims and do not describe what the interface is. Paragraph 0307 while stating "devices are each supported by a single payment module/communication module, which is a substantial extension of communication capabilities of an offline device configured with a payment/communication module as described herein". It too fails to describe what the claimed "interface" is. Finally, with respect to "references made to a 'payment module' in particular are equally applicable to a 'communication module' in general" (paragraph 0326), to one of ordinary skill, while all "payment modules" can be a "communication module", not all "communication modules" are "payment modules", and it is these communication modules in which the interface is not sufficiently described. Therefore, the claim lacks written description as it has been held "[the] written description requirement is not necessarily met when the claim language appears in ipsis verbis in the specification. 'Even if a claim is supported by the specification, the language of the specification, to the extent possible, must describe the claimed invention so that one

skilled in the art can recognize what is claimed. The appearance of mere indistinct words in a specification or a claim, does not necessarily satisfy that requirement. Dependent claims 2-8 and 10-14 do not remedy the deficiency of claims 1 and 9 stand rejected on the same grounds. (Enzo Biochem, Inc. v. Gen-Probe, Inc., 323 F.3d 956, 968, 63 USPQ2d 1609, 1616 (Fed. Cir. 2002) (MPEP 2163.03 V)).

9. Claim 2 recites "<u>facilitating</u> the first service for the first mobile device; and while facilitating the … ". Paragraph 0323 of PgPub while stating "the communication module facilitates the first service by way of the first packets, while concurrently continuing to broadcast second packets indicating presence of the second device". However, the specification does not provide details on what "facilitating", comprises. Therefore Applicant does not provide the algorithms or steps/procedures taken to perform the function with sufficient details so that one of ordinary skill in the art would understand how the inventor intended the functions to be performed. Claim 3, 10-11, 16, and 17 are also rejected as each recites similar language "facilitating". (MPEP 2161 01 I).

10. Claim 5 recites "including in each of the first packets information necessary to decode or reconstruct respective packets <u>independently</u> of information from any of the second packets; and including in each of the second packets information <u>necessary decode or reconstruct respective packets independently</u> …". Paragraph 0253 uses the word "independent", however this is directed to "pulses" ("the amount and number of pulses are dissociated and be in any number independent of the value of pulse").

Therefore, Applicant has not provided one of ordinary skill in the art with sufficient details as to how Applicant the function is to be performed. (MPEP 2161 01 I).

Claim Rejections - 35 USC § 112

The following is a quotation of 35 U.S.C. 112(b):

> (b) CONCLUSION.—The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention.

11. Claims 1-8 are rejected under 35 U.S.C. 112, second paragraph or 35 U.S.C. 112(b), as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Unclear Scope

12. Claim 1 recites "An electronic communication module comprising: ... an interface that couples the communications module ...". Therefore, it is unclear as to whether the communication module comprises a transceiver, an interface, or additionally one or more processors, memory storing one or more programs ... comprising instructions for". Dependent claims 2-8 do not remedy the deficiency of claim 1 and stand rejected on the same grounds.

Claim Rejections – 35 USC 102

13. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the rejections under this section made in this Office action.

> A person shall be entitled to a patent unless -

> (a)(2) the claimed invention was described in a patent issued under section 151, or in an application for patent published or deemed published under section 122(b), in which the patent or application, as the case may be, names another inventor and was effectively filed before the effective filing date of the claimed invention.

14. **Claims 1-8** are rejected under 35 U.S.C. 102(a)(2) as being anticipated by **Khan et al. [US Pub No. 2004/0029569 A1]**.

15. Regarding **claim 1**, Khan discloses an electronic communication module comprising:

a transceiver (Figure 3 items 304, 306; paragraphs 0031, 0044 and 0099);

an interface (Figure 3 item 340; paragraphs 0041, 0049 and 0101) that couples the communication module (paragraphs 0045) with an article of manufacture (Figure 19 item 120),

one or more processors (Figure 3 items 300, 308; paragraphs 0031, 0032 and 100), and

memory storing one or more programs (paragraph 0100) to be executed by the one or more processors (Figure 3 item 308; paragraphs 0031 0032, and 0042).

With respect to “the one or more programs comprising instructions for: broadcasting from the transceiver…; wherein each of the first packets…; … ; … wherein the first and second packets are transmitted in an alternating pattern.” This represents the mere intended use of the one or more programs and it has been held that intended use limitations will not differentiate the claimed structure from the prior art (MPEP 2103. I C).

16. Regarding **claims 2-5**, each recite the language "the electronic communication module of claim 1, ... further comprising instructions for" therefore each claim is directed to intended use of the of the instructions and will not differentiate the claim structure from the prior art module of Khan (Figure 3; paragraph 0100). (MPEP 2103. I C). Regarding **claim 6**, "wherein broadcasting..." also does not have patentable weight as it merely further describes the intended use of the instructions of claim 1 specifically "memory... comprising instructions for: broadcasting from the transceiver..."

17. Regarding **claims 7-8,** as the "first service", "the second service", "article of manufacture", "payment service", "data transfer service" and "configuration service" are not components of the "electronic communication module" neither will not differentiate the claims from the prior art module of Khan (Figure 3; paragraph 0100).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KEVIN T POE whose telephone number is (571)272-9789. The examiner can normally be reached on **Monday-Friday 9:30am through 6pm EST**.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **Calvin Hewitt** can be reached on 571-272-6709. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see https://ppair-my.uspto.gov/pair/PrivatePair. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/K.T.P/
Examiner, Art Unit 3692
/KEVIN T POE/

/CALVIN L HEWITT II/
Supervisory Patent Examiner, Art Unit 3692

Notice of References Cited	Application/Control No. 15/956,741	Applicant(s)/Patent Under Reexamination Patel, Paresh K.
	Examiner KEVIN T POE	Art Unit 3692
		Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-7965693-B2	06-2011	Jiang; James	H04L63/102	370/338
*	B	US-8514775-B2	08-2013	Frecassetti; Mario Giovanni	H04W28/0231	370/328
*	C	US-8856045-B1	10-2014	Patel; Paresh K.	G06Q20/326	705/79
*	D	US-20040029569-A1	02-2004	Khan, Mohammad A.	G07F7/0886	455/410
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Dialog®

STIC
Scientific and Technical
Information Center

Report Information from Dialog

July 25 2023 22:46

Table of contents

USA Technologies Announces Cashless Solution to Be Offered by Blackboard Inc

Publication info: Business Wire 18 July 2007: NA.
ProQuest document link

Abstract (English): Students Use ID, Debit and Credit Cards to Purchase from Vending Machines Nationwide
MALVERN, Pa. -- USA Technologies (NASDAQ:USAT) announced today that Blackboard Inc. has begun offering its cashless payment technology to customers of the Blackboard Commerce Suite[TM] to allow students to make cashless payments at campus vending machines.
The cashless technology is imbedded in Blackboard's FlexVend reader and supports a suite of both wired and wireless applications that enable one-card transactions on-campus, off-campus and online for cashless payment, identification and security.
The new FlexVend readers allow students to pay for products from vending machines with their Blackboard campus card, all major credit cards, as well as contactless 'touch and go' payment systems, such as MasterCard's PayPass.

Full text: Students Use ID, Debit and Credit Cards to Purchase from Vending Machines Nationwide
MALVERN, Pa. -- USA Technologies (NASDAQ:USAT) announced today that Blackboard Inc. has begun offering its cashless payment technology to customers of the Blackboard Commerce Suite[TM] to allow students to make cashless payments at campus vending machines.
The cashless technology is imbedded in Blackboard's FlexVend reader and supports a suite of both wired and wireless applications that enable one-card transactions on-campus, off-campus and online for cashless payment, identification and security.
The new FlexVend readers allow students to pay for products from vending machines with their Blackboard campus card, all major credit cards, as well as contactless 'touch and go' payment systems, such as MasterCard's PayPass.
USA Technologies reported that Blackboard already offers its e-Suds[TM] laundry service where students go online to check the availability of college laundry washers and dryers, swipe their Blackboard transaction card to activate and pay for the service, and are notified electronically when the laundry is done.
"Our goal is to provide students with the most efficient, high-tech solutions to meet their every-day needs and wants," said Russ Carlson, President of the Blackboard Commerce Group. "FlexVend provides Blackboard cardholders the ultimate in payment convenience, and the cost is automatically deducted from their Blackboard account."
Blackboard is a leading provider of software and services to the education industry.
"The expanded relationship we now share with Blackboard combines the best leading-edge technology and service from both Blackboard and USA Technologies to bring a quality payment solution to campuses nationwide," said Wendy Jenkins, Vice President, Marketing, USA Technologies. "We are excited that Blackboard has added USA Technologies cashless technology to its portfolio of offerings for students, and we welcome the Federal Reserve Board's recent decision to eliminate the need for receipts for debit card purchases under $15 which will make cashless from vending machines on campus even more popular," she said.
The online reporting capability of the FlexVend reader also allows for improved auditing of vending machines, resulting in greater efficiency, productivity and security for vending machine operators.
About USA Technologies:
USA Technologies is a leader in the networking of wireless non-cash transactions, associated financial/network

services and energy management. USA Technologies provides networked credit card and other non-cash systems in the vending, commercial laundry, hospitality and digital imaging industries. The Company has marketing agreements with AT&T, Honeywell, Blackboard, MasterCard and others. For further information on USA Technologies, please visit www.usatech.com.

About Blackboard Inc:

Blackboard Inc. is a leading provider of enterprise software applications and related services to the education industry. Founded in 1997, Blackboard enables educational innovations everywhere by connecting people and technology. Millions of people use Blackboard everyday at academic institutions around the globe, including colleges, universities, K-12 schools and other education providers, as well as textbook publishers and student-focused merchants that serve education providers and their students. Blackboard is headquartered in Washington, D.C., with offices in North America, Europe, Australia and Asia.

Statement under the Private Securities Litigation Reform Act:

With the exception of the historical information contained in this release, the matters described herein contain forward-looking statements that involve risk and uncertainties that may individually or mutually impact the matters herein described, including but not limited to, the ability of the Company to increase revenues in the future due to the developing and unpredictable markets for its products, the ability to achieve a positive cash flow, the ability to obtain orders for its energy management products , the ability to obtain new customers and the ability to commercialize its products, which could cause actual results or revenues to differ materially from those contemplated by these statements.

Subject: Computer industry;Computer services industry;Information technology services industry; Microcomputer industry

Location: United States

Company / organization: Blackboard Inc.; USA Technologies Inc.

Identifier (keyword): Trade

SIC classification: 7370: Computer and Data Processing Services;3571: Electronic computers

Publication title: Business Wire

Pagination: NA

Publication date: Jul 18, 2007

Publisher: Business Wire

Journal subject: Business, Business, international

Journal code: 0EIN

Source type: Newswire

Language of publication: English

Document type: Magazine/Journal

Source attribution: Gale PROMT, © Publisher specific

Accession number: 166521527

Document URL: https://dialog.proquest.com/professional/docview/673610549?accountid=131444

Date created: 2010-04-28

First available: 2010-07-25

Database: Gale Group PROMT® (1972 - current)

Bibliography

Citation style: APA 6th - American Psychological Association, 6th Edition

USA technologies announces cashless solution to be offered by blackboard inc. (2007, Jul 18). Business Wire Retrieved from https://dialog.proquest.com/professional/docview/673610549?accountid=131444

THE COMMODITY VENDING MACHINE

Article · February 2005

1 author:

Susanne Gruber
Association for Research in Commodity Science - Forschungsverein für Warenlehre und angewandte Naturwissenschaften
38 PUBLICATIONS **10** CITATIONS

THE COMMODITY VENDING MACHINE

Susanne GRUBER, Renate BUBER, Bernhart RUSO, Johannes GADNER

Univ.-Ass. Dr. Susanne Gruber, Institute of Technology and Sustainable Product Management, University of Economics and Business Administration Vienna, Augasse 2 - 6, A-1090 Vienna, Austria, susanne.gruber@wu-wien.ac.at

Ass. Prof. Dr. Renate Buber, Institute of Retailing and Marketing, University of Economics and Business Administration Vienna, Augasse 2 - 6, A-1090 Vienna, Austria, renate.buber@wu-wien.ac.at

Dr. Bernhart Ruso, Institute of Knowledge Organisation, Lange Gasse 63/15, A-1080 Wien, Austria, bernhart@ruso.at

Dr. Johannes Gadner, Institute of Knowledge Organisation, Lange Gasse 63/15, 1080 Vienna, Austria, johannes.gadner@iwo.at

Abstract

This paper describes the groups of players in the vending market and introduces a typology of vending machines. From a commodity perspective, vending includes the discussion of the types of vending machines and their technical demands for storing and preparing goods and services and for installing the vending machine at a certain location. From a marketing perspective, vending is defined as the distribution and selling of goods and services by a vending machine. In addition, a vending machine is seen as a distribution channel of a retailer. In the vending market, four groups of players can be differentiated: (1) the producers of the vending machines and the accessories as well as the goods; or the service providers; (2) the site lessors; (3) the operators, merchandisers and maintenance people; and (4) the customers.

The different types of vending machines can be categorized into product-oriented and service-oriented machines. Product-oriented vending machines offer both cold and hot food as well as non-food items. Service-oriented vending machines offer different kinds of services, e.g. entertainment (jukeboxes, slot machines) and non-entertainment (telephones or scales). In addition, from packaging refund machines the customer can get the packaging deposit back.

Keywords: vending, vending machine, distribution, operator, site lessor

Introduction

The first vending machine was constructed by Heron of Alexandria (Mechanicus, about 100 BC). After inserting a coin, holy water was dispensed.[1] For more than 100 years people have been able to buy goods and services from vending machines. The first commercial vending machines were built at the end of the 80's of the 19th century.[2] On 13 March 1908, the first stamp and postcard-vending machine of the world was installed in front of the Hotel des Postes.[3]

Vending machines are used in different markets, in the retail trade for the selling of food and non-food items as well as convenience products. Selling cold and hot drinks was the predominant business in the past, but at present, the variety of goods and services marketed with vending machines is steadily increasing. Vending Associations in different countries define vending differently.

Basically, vending is defined as the selling of products through vending machines[4], which are "coin operated machines for the sale of small articles"[5]. Additionally, vending machines can be designed for the sale of large quantities of various products, e.g. in Japan, one can buy ten-kilo bags of rice from a vending machine[6]. Furthermore, for a couple of years, it has been possible to pay for goods and services by credit card which has to be put in the vending machine's slot for cards.

The American Association NAMA (National Automatic Merchandising Association) states that "vend is the delivery of a single unit of merchandise"[7]. In the US, vending is highly connected with the slogan "Coffee, Candy, Cola"[8]. “Coffee" symbolises the sale of hot drinks like coffee, hot chocolate, tea, but also soups; the term "Candy" represents sweats, and "Cola" replaces the enumeration of different soft drinks. In the very beginning, the vending industry started with the 4-Cs-concept, coffee, cup soda, candy and cigarettes, and later on the range grew to almost 8 Cs - coffee, candy or confections, chips, cold drinks, canned drinks, cigarettes, cold cup and commissary.[9]

In Europe vending includes a wider range of products (EVA, European Vending Association)[10]. The Vending Association in Germany (BDV, Bundesverband der Deutschen Vending Automaten-Wirtschaft e.V.) defines vending as the selling of everyday essentials, especially food and drinks through vending machines. Producers of machines, operators and different associations use the term vending for all kinds of food and drinks, but they include non-food products as well.

The Austrian Association (ÖVV, Österreichische Verkaufsautomaten Vereinigung) defines all machines that sell goods, including food, drinks, photos, parking-tickets as vending machines; but copying-machines, telephones, lockers, washing-machines, pin balls, slot machines, etc. are also included.[11] The BDV excludes machines which offer amusement features from the vending industry.[12]

From a marketing point of view, vending machines are defined as a store format of the retail trade industry with an automatic selling procedure – the customer has to select the product, to take it with him/her and to pay for it, everything is done by him-/herself.[13],

In the US, a vending machine utilizes a full glass front to merchandise the product selection inside the machine. Most often the product is delivered via spirals and is dispensed to a delivery pan located at the bottom of the machine.[14]

Summarising, in this article vending is defined as the selling of goods or services by a vending machine at which the customer has to administer the selection of the product or the service, to pick up the product and carry it away and to pay for the product or service on the spot – either in cash, by credit card or by means of other electronically available kinds of payment, e.g. text messaging.

The Vending Market

In the vending market, four groups of players can be differentiated:

- the producers of the vending machines, the accessories and the goods, as well as the service provider,
- the site lessors,
- the operator (the merchandisers and maintenance people), and
- the customers (see figure 1).

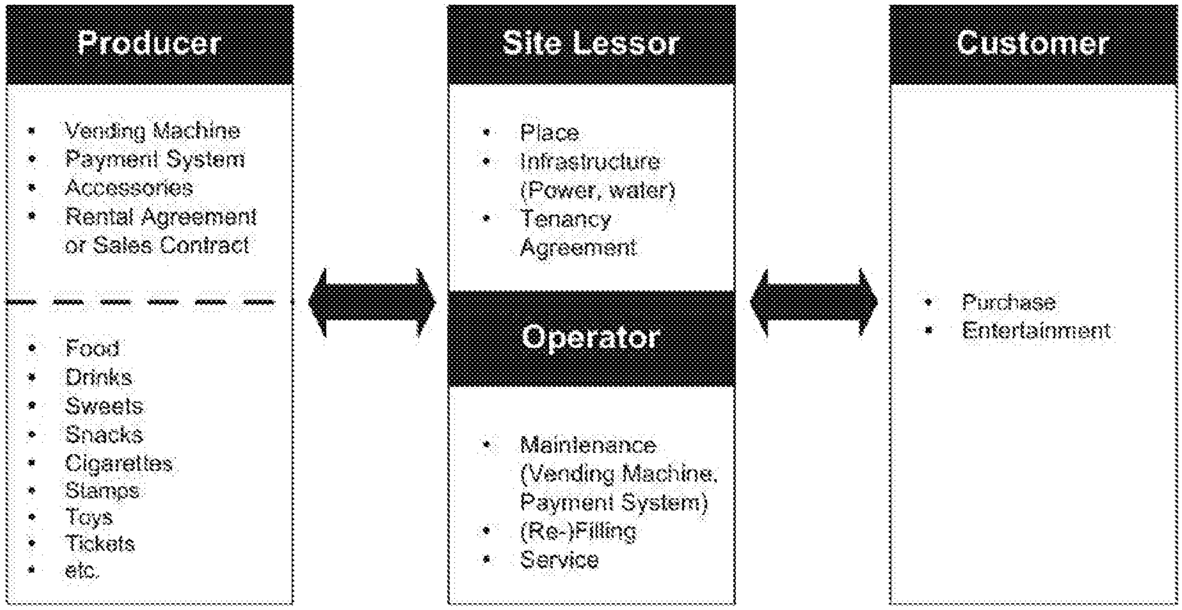


Figure 1: Vending Market Players

The Producer of the Vending Machine

Besides the technical functions (power, water supply, distribution and payment unit), marketing-relevant aspects (e.g. accessories like spoons, cups, serviettes) have to be considered for the design of the vending machines. Due to both the high costs of the maintenance and the strong influence of the functional efficiency on customer satisfaction, the technical equipment and the payment system as well as the distribution comfort are very important. Therefore, the handling features must be designed carefully, particularly to protect the vending machines against vandalism or technical breakdowns.

The Producer of the Merchandise

Goods and accessories must serve both the technical demands of the vending machines (size, durability, handling) and the needs of the customers (attractiveness, simple opening to pick up selected goods, etc.). The packaging must guarantee that the goods do not break, and do not stick in the spiral when selected and delivered.

The Operator

The operator has to look after the (re-)filling, the cleaning and the functional efficiency of the vending machine as well as the cost-, and benefit-efficiency of the housing.[15] Usually, the operator assembles the assortment and decides about the payment system (cash, credit card, internet, text messaging, etc.).

The operator has to know the needs, wants and attitudes of the customers. Without any data about customer profiles, who buys when, what, in which quantity, one cannot conclude from turnover to the actual customers′ wishes and needs[16]. This lack of information is one of the main problems of the vending business. Thus, the customer is left alone when buying from the vending machine, and the operator very often does not know too much about the motives and attitudes of the customer. In general, it can be stated that from the point of view of the customer, the image of this distribution channel should be improved.

The Site Lessor

The site lessor is the owner or tenant of the place where a vending machine is installed. He/she lets the place to the operator and gets paid for it. Usually, vending machines can be found in three different markets:

- the business market (office, factory, surgery, etc.),
- the catering market (restaurant, cafe, kiosk, etc.),
- the public market (public building, school, university, shopping mall, sports centre, railway station, airport, street, etc.).

The Customer and the Buying Situation

The customer selects goods from the vending machine, pays for them either in cash, by credit card or by other means and takes the goods from the delivery unit, either for immediate or later consumption.

Purchasing from a vending machine can be seen as a particular buying situation. The customer cannot ask for any help, and he/she is doing the purchase by him-/herself without any advice from a shop assistant. If the vending procedure works well, the customer is served quite quickly. In the case of a problem, he/she has to find out how to deal with the situation. Usually, the operator’s phone number is written on a sign that is affixed to the vending machine. That is, the customer has to make and to pay for the phone call and ideally the problem can be solved immediately. If the customer wants to complain about the goods’ quality, the handling comfort of the delivery unit or anything else, first he/she has to figure out how she/he can get in touch with the contact person. The buying situation is characterised by indirect communication, the active search for information, and the customer’s risk of leaving with the problem unsolved. On the other hand, the particular buying situation can also be seen positively. The customer can select, pick up the product, and pay without being disrupted or manipulated by a shop-assistant[*].

[*] On the other hand, the reasons for customers not to buy goods from a vending machine are manifold. Some people prefer to be served. Moreover, in a study by Buber, R. et al. the customers argued that self-service is not as attractive and the service as well as the ambience of a cafe are more appealing (Buber, R./Ruso, B./Gadner, J./Gruber, S./Atzwanger, K. (2004): Measuring Consumer Behavior in Recreational and Sales Areas of Shopping Malls. Band 52 der Schriftenreihe Handel und Marketing (ed. by Schnedlitz, P.), Wien (interview 11, line 78).

Types of Vending Machines

Product-oriented and Service-oriented Vending Machines

The silent shop assistant is part of our life. 24 hours a day he/she offers different goods, e.g. photos for passports, business cards, parking tickets, condoms, cigarettes, sweets, food, hot and cold drinks. On other machines you can play a videogame, make copies, wash your clothes, make a phone call, gamble, etc.[17]

Vending machines can be categorized into product-oriented and service-oriented machines. Product-oriented vending machines are machines that offer both cold and hot food as well as non-food goods. This category includes packaging refund machines where the customer gets the bottle deposit back.

Service-oriented vending machines offer different kinds of services, entertainment (e.g. jukeboxes, slot machines) and non-entertainment (e.g. telephone or scales).

Figure 2 gives an overview of the different types of vending machines.

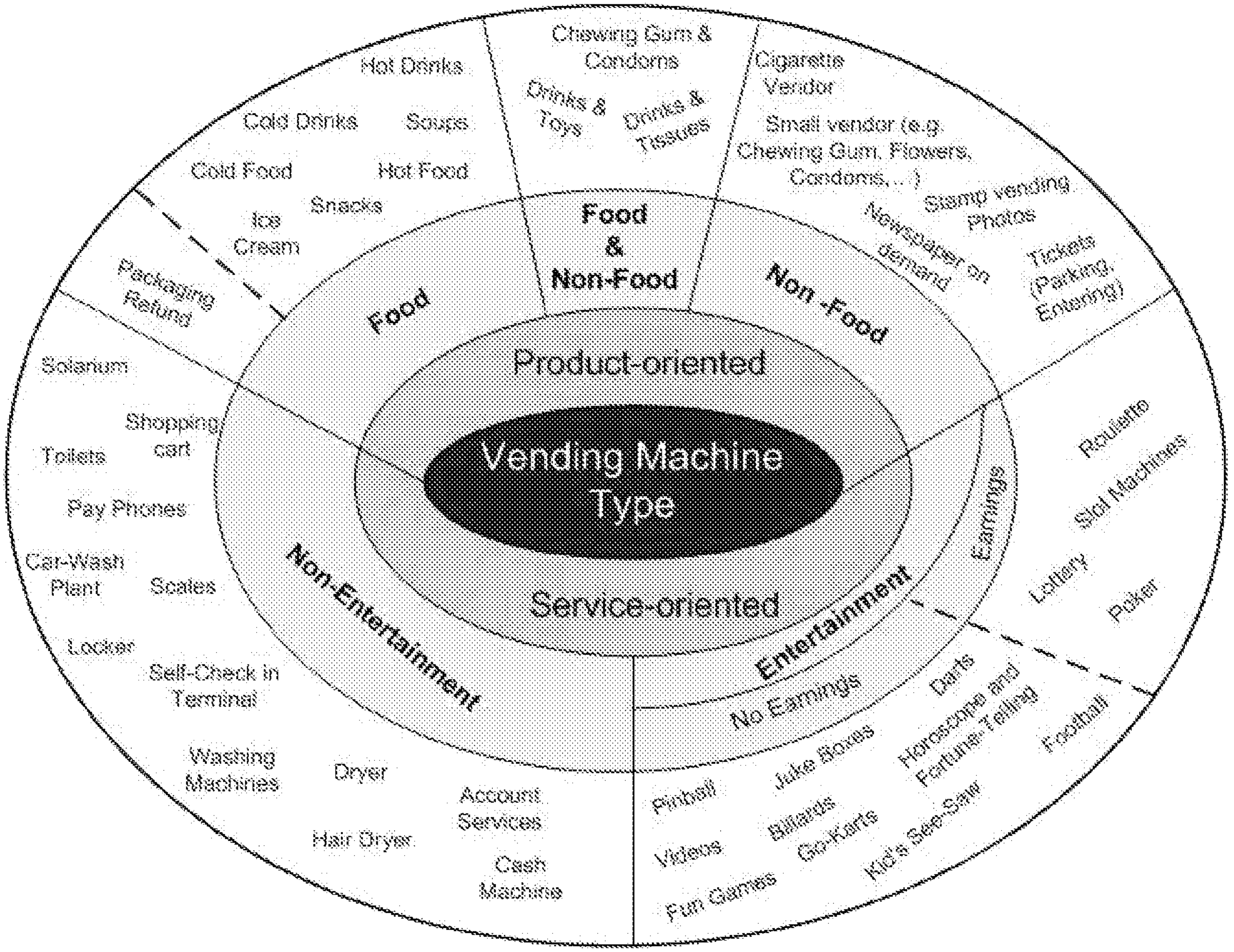


Figure 2: Types of Vending Machines and Typical Examples

Usage of Vending Machines

Vending Machines for Food

A food vending machine can offer either only one type of food or different kinds of food. Especially, if there is little space, combined vending machines with food (cold and hot) and drinks (cold and hot) in one machine are installed.

Vending machines for food offer:

- cold food: sandwiches, fruits, vegetables,
- hot food: fried food, pastries,
- soups,
- hot drinks: coffee, cocoa, tea, milk,
- cold drinks: ice tea, fresh juices, soft drinks, iced coffee,
- snacks: biscuits, chocolate, sweets, chewing gum, crackers, peanuts,
- ice cream.

The technical equipment for vending machines for food includes:

- Power: for all types of food,
- Water supply or water tank: for machines that offer coffee, tea, cocoa, milk, soups or fresh drinks,
- Cooling system: to cool drinks, food and ice cream,
- Heating system: to prepare hot food and keep food warm,
- Waste tanks: for the used coffee and tea powder,
- Selection panel: choice of goods
- Display: as a manual for customers
- Distribution unit: spiral rows, boxes, taps,
- Payment system: slots for coins and cards, etc.

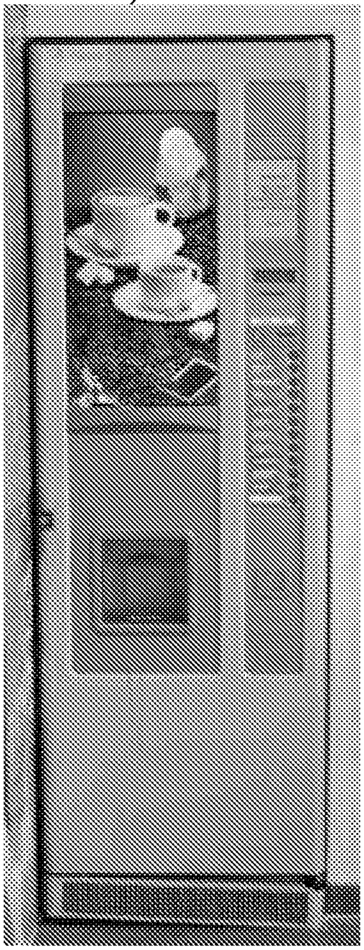


Figure 3: Vending Machine for Hot Drinks

Vending Machines for Non-Food

Figure 4 shows a typical vending machine for cigarettes and illustrates the usual applications of non-food vending machines in general.

Usually, vending machines for non-food offer the following items:

- cigarettes,
- flowers,
- condoms,
- toiletries (soap, towel, handkerchief, tampon, sanitary towel),
- stamps,
- photos,
- tickets: parking, entering,
- newspapers,
- toys: cars, puppets,
- small articles: jewelleries, stones, stories.

The technical equipment for vending machines for non-food items includes:

- Power: for lighting and cooling equipment if necessary,
- Cooling system: to keep goods fresh,
- Selection panel: choice of goods,
- Display: as a manual for customers,
- Handing out system: spiral rows, boxes, slots,
- Payment system: slots for coins and cards.

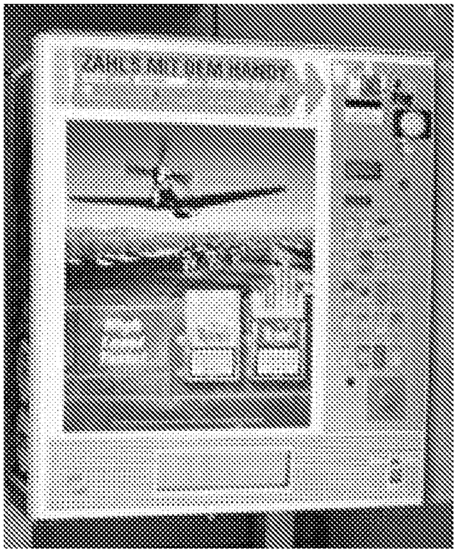
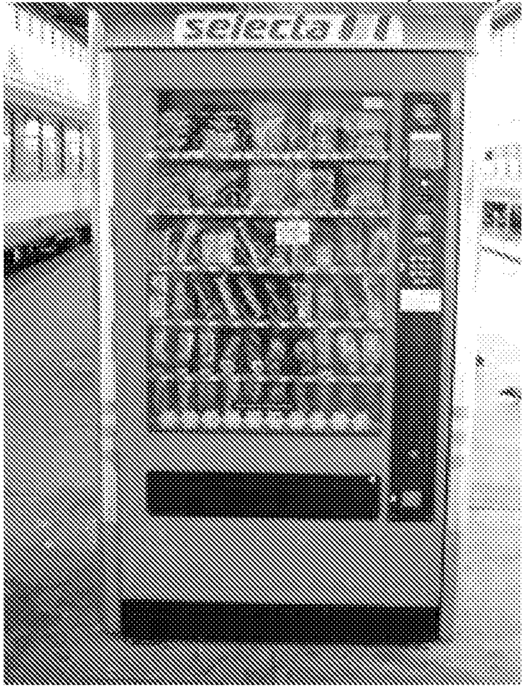


Figure 4: A Typical Vending Machine for Non-food Items

Vending Machines for Food and Non-Food Items

Figure 5 depicts a typical vending machine installed on platforms in Austrian railway stations. These machines are filled with snacks, sweets, cold drinks, and tissues.



The technical equipment for vending machines for food and non-food includes:

- Power,
- Water supply or water tank,
- Cooling system,
- Heating system,
- Waste tanks,
- Selection panel,
- Display,
- Distribution unit,
- Payment system.

Figure 5: Example of a Combined Vending Machine for Food and Non-Food Items

Vending Machines for Packaging Refund

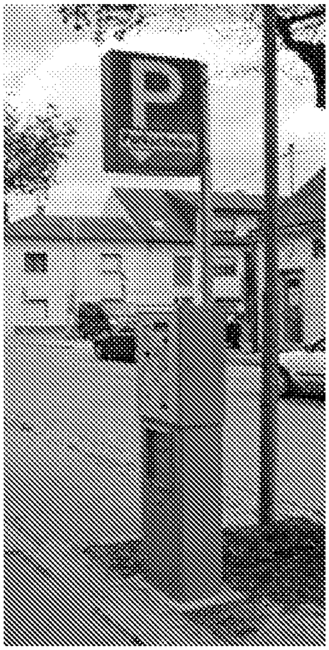
Vending machines for packaging refund scan and register packaging like bottles, jars, cans, and boxes. The refund is paid to the customer by cash or the customer gets a ticket, which he/she has to present to the cashier.

The technical equipment for vending machines for packaging refund includes:

- Power: for scanning system, delivery unit,
- Scanning system: for scanning and identify the packaging,
- Handing in system: boxes, slots,
- Display,
- Printing and handing out system: printing the ticket and slots for handing out prouducts,
- Payment system: for refund.

Figure 6: Example of a Packing Refund Machine

Vending Machines for Non-Entertainment Services



Vending machines for non-entertainment are:

- scales,
- horoscopes and fortune-telling,
- parking and entering,
- pay phones,
- toiletries and solarium,
- shopping carts,
- banking service: foreign exchange, cash withdrawal, account services,
- lockers, safe deposits,
- check in: on airports, at railway stations,
- car service: car-wash plant, self service vacuum cleaner.

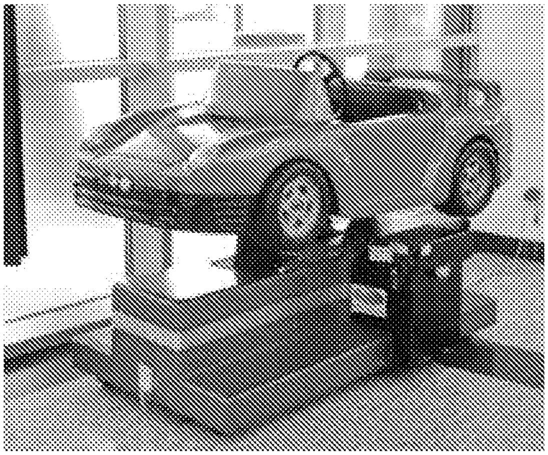
The technical equipment for vending machines for non-entertainment depends on the demands:

- Power,
- Scanning system: for check in and banking service functions,
- Display,
- Printing system: printing tickets and slots for handing out,
- Payment system:

Figure 7: Example of a Non-Entertainment Vending Machine

Vending Machines for Entertainment – No Earnings

If the customer has inserted the coins the vending machine starts; it ends after a fixed time or after the game is over. It can be started once again. These machines sell entertainment.



Vending machines for entertainment and no earnings are:

- sports machines: football, darts, billards,
- fun games: pinball, video games,
- videos: on TV, in video cabins,
- jukeboxes,
- karts: go-karts for adults and children.
- automatic see-saw: animals, cars, fantasy figures.

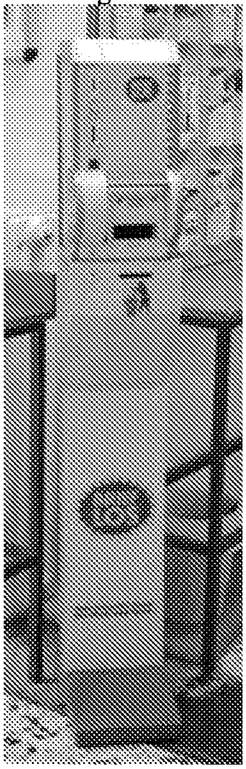
The technical equipment for vending machines for entertainment without earnings includes:

- Power: for the payment system and the engine,
- Engine: for movement,
- Display,
- Payment system.

Figure 8: Example of an Entertainment Vending Machine (No Earnings Possible): Automatic See-Saw

Vending Machines for Entertainment with Earnings

Vending machines for entertainment with earnings are slot machines, roulette, poker, lottery, etc. These vending machines sell the game and if the customer is successful, he/she can win cash.



A vending machine for entertainment with earnings has to be equipped with the following technical items:

- Power: for the payment system and the engine,
- Engine: for movement,
- Product selection,
- Payment system: slots,
- Handing out system.

Figure 9: Example of An Entertainment Vending Machine with Earnings

Installation

When selecting the vending machine's location one has to consider both the technical infrastructure and customer-related issues, e.g. visitor frequency, lighting, security.

Table 1 illustrates the technical demand for installing the different vending machines.

Types of Vending machines		Power 1)	Phone or Internet supply	Water supply	Cooling system	Heating system	Waste tank	Scanning system	Display	Selection panel	Distribution unit					Engine	Payment system
											Spiral rows	Boxes	Slots	Dispenser	Accessories		
Food	Cold Food	X	(X)		X				(X)	X	c	c			c		X
	Hot Food	X	(X)			X			(X)	X	c	c			c		X
	Soups	X	(X)	X		X	X		(X)	X				X	X		X
	Hot drinks	X	(X)	X		X	X		(X)	X				X	X		X
	Cold drinks - juices, milk, water	X	(X)	(X)	X		X		(X)	X				X	X		X
	Cold drinks - canns, bottles	X	(X)		X				(X)	X	X	X					X
	Snacks	X	(X)						(X)	X	X	X					X
	Ice cream	X	(X)	X	X		X		(X)	X				X	X		X
	Ice - packet	X	(X)		X				(X)	X	X	X					X
Non-Food	Cigarettes	X	(X)						(X)	X	c	c					X
	Flowers	X	(X)		X				(X)	X		X					X
	Condoms	X	(X)						(X)	X	c	c					X
	Toilette articles	X	(X)						(X)	X	c	c					X
	Stamps	X	(X)						(X)	X	c	c	c				X
	Photos	X	(X)						(X)	X		c	c				X
	Tickets	X	(X)						(X)	X		c	c				X
	Newspapers	X	(X)						(X)	X	c	c	c				X
	Toys	X	(X)						(X)	X	c	c					X
	Small articles	X	(X)						(X)	X	c	c					X
Packaging refund		X						X	(X)			c	c				X
Non-entertainment	Scales	(X)	(X)						X	(X)							X
	Parking and Entering	X	(X)						(X)	(X)		c	c				X
	Pay phones	X	X						(X)	(X)							X
	Toilettes																X
	Solaries	X	(X)						(X)	X							X
	Shopping carts																X
	Banking service	X	(X)					(X)	(X)	X			X				X
	Lockers, safe deposits	(X)	(X)						(X)	(X)							X
	Check in	X	(X)					(X)	(X)	(X)			X				X
	Car service	X	(X)	(X)					(X)	(X)							X
Entertainment - No earnings	Sports machines	X	(X)						(X)	(X)						(X)	X
	Fun games	X	(X)						(X)	(X)						(X)	X
	Videos	X	(X)						(X)	(X)							X
	Jukeboxes	X	(X)						(X)	(X)						(X)	X
	Karts	X														X	X
	Automatic See-saw	X														X	X
	Horoscopes and fortune telling	X	(X)						(X)	(X)							X
Entertainment - Earnings	Slot machines	X	(X)						(X)	(X)						(X)	X
	Roulette	X	(X)						(X)	(X)						(X)	X
	Poker	X	(X)						(X)	(X)							X
	Lottery	X	(X)						(X)	(X)							(X)

1 Electricity for electric operated equipment
c one or more of the given possibilities

X is needed
(X) depends on demands

Table 1: The Technical Equipment of Vending Machines

Future Prospects

The spectrum of vending machines is astonishingly wide: From ice-cream to hot coffee, from cigarettes to parking tickets and from train tickets to horoscopes. Further technological developments in the vending market are to be expected. Prototypes of fully automated shops, where the customers' credit cards are debited according to the goods in their trolleys at the cash point, without the help of a cashier, are already in use. These shops are, in a manner of speaking, huge vending machines and the shop assistants' tasks are reduced to merely servicing the machines. The rapid development of vending machines and the reduction of the social contact between seller and buyer mirrors two types of changes in our society. On the one hand, the technical achievements, which allow for new types of products to be offered and ensure security for both the seller and the customer. On the other hand, the customers' needs are changing. Today, on many occasions customers prefer to buy anonymously, without any personal commitment and without any time limit - twenty-four hours a day. Furthermore, as wages and rental fees are steadily increasing, shop facilities without the traditional shop assistant can be run at a more competitive price. As the customer gets more and more hybrid, he/she satisfies her/his needs by purchasing in different shop formats (from a discount store to a speciality shop) at different price levels. The customers' behavior changes dramatically, and it has to be questioned in what direction the development of purchases from vending machines will go in the future.[18]

REFERENCES

[1] Heron von Alexandria, in: www.wikipedia.org, August 8, 2005, CET 13:33

[2] Verkaufsautomaten, in: www.wikipedia.org, August 8, 2005, CET 13:33

[3] Tageschronik 0313, in: www.chronikverlag.de, August, 8, 2005, CET 13:49

[4] BDV (Bundesverband Deutscher Verpflegungs- und Vending-Unternehmen e. V.) (2001): Press information, 2001, p. 1

[5] Oxford University Press (1994): The Oxford English Reader's Dictionary, Berlin – Munich, p. 568

[6] Photoman: Japan, in: www.photoman.com, July 14’ 2004, CET 14:40

[7] NAMA Vision/Industry Definitions, in: www.vending.org, August 3, 2005, CET 12:19

[8] o. V. (1999): Coffee, Candy, Cola, in: Gewerbe-Report 3/99, p. 17ff

[9] NAMA Vision/Industry Definitions, in: www.vending.org/nama_vision/index.php?page=definitions, August 8, 2005, CET 16:47

[10] EVA, European Vending Association: www.eva.be, August 3, 2005, CET 11:13

[11] ÖVV, Österreichische Verkaufsautomaten Vereinigung: www.ovv.at, June 16, 2005, CET 14:07

[12] BDV, Bundesverband der Deutschen Vending Automaten-Wirtschaft e.V.: www. bdv-online.de, June 16, 2005, CET 13:54

[13] DILLER, H. (2001): Vahlens Großes Marketinglexikon, Verlag C. H. Beck, Munich 2001, p. 1830

[14] NAMA Vision/Industry Definitions, in: www.vending.org, August 3, 2005, CET 12:19

[15] MONSSEN, N. (1999): Vending – Ein Markt mit Zukunft. BDV (Bundesverband Deutscher Verpflegungs- und Vending-Unternehmen e. V.) (Hrsg.), Köln

[16] JUNGBLUTH, H. M. (2002): High-Tech contra Anonymität. In: gv-praxis Nr. 9, 4 September 2002, p. 64 (translated by authors)

[17] OVV: http://www.ovv.at, July 14, 2004, CET 16:20

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

ADMINISTRATIVE ORDER 2021-33

IN RE: CORONAVIRUS PUBLIC EMERGENCY
______________________________________/

NINTH ORDER CONCERNING JURY TRIALS AND OTHER PROCEEDINGS

This Order is issued in conjunction with Administrative Orders 2021-12, 2020-76, 2020-53, 2020-41, 2020-33, 2020-24, 2020-21 and 2020-18 which limited in-court appearances and continued all jury matters.

THEREFORE, the United States District Court for the Southern District of Florida hereby issues the following order:

1. All persons entering any federal courthouse facility within the Southern District of Florida **must** wear a face mask at all times unless otherwise directed by the Court. Face masks may not contain exhalation valves or vents. The only exceptions to the face mask requirement are for a medical condition that precludes an individual from wearing a face mask and children under two (2) years of age.

2. All persons entering any federal courthouse facility within the Southern District of Florida **must** maintain a social distance of at least 6' apart unless they are members of the same household.

3. All persons entering any federal courthouse facility within the Southern District of Florida may be subject to screening.

4. All persons using the elevators in any federal courthouse facility within the Southern District of Florida shall abide by social distancing signage posted at the elevator entrance unless the individuals in the elevator are members of the same household.

5. The United States Courthouses in Miami, Fort Lauderdale, West Palm Beach, Fort Pierce, and Key West, including Bankruptcy Court and Probation, will remain open for business, with reduced staffing, to a level to maintain essential operations, consistent with Administrative Order 2020-20 and subject to the following limitations.

6. Jury trials in the Southern District of Florida scheduled to begin on or after March 30, 2020, are continued until July 6, 2021, excluding preselected Pilot jury trials which will proceed as scheduled by the presiding Judge. The Court may issue other Orders concerning future continuances as necessary and appropriate.

7. All trial-specific deadlines in criminal cases scheduled to begin before July 6, 2021, are continued pending further Order of the Court. Individual judges may continue trial-specific deadlines in civil cases in the exercise of their discretion.

8. Individual judges presiding over criminal proceedings may take such actions consistent with this Order as may be lawful and appropriate to ensure the fairness of the proceedings and preserve the rights of the parties.

9. The Court is cognizant of the right of criminal defendants to a speedy and public trial under the Sixth Amendment, and the particular application of that right in cases involving defendants who are detained pending trial. Any motion by a criminal defendant seeking an exception to this Order in order to exercise that right should be directed to the District Judge assigned to the matter in the first instance; provided, however, that no such exception may be ordered without the approval of the Chief Judge after consultation with the Court.

10. The time period of any continuance entered as a result of this Order shall be excluded under the Speedy Trial Act, 18 U.S.C. § 3161(h)(7)(A), as the Court finds that the ends of justice served by taking that action outweigh the interests of the parties and the public in a speedy trial. Absent further Order of the Court or any individual judge, the period of

exclusion shall be from March 30, 2020, to July 6, 2021. The Court may extend the period of exclusion as circumstances may warrant. This Order and period of exclusion are incorporated by reference as a specific finding pursuant to 18 U.S.C. § 3161(h)(7)(A) in the record of each pending case where the Speedy Trial Act applies. *See Zedner v. United States*, 547 U.S. 489, 506–07 (2006). The period of exclusion in this Court's prior Administrative Orders on this subject (2021-12, 2020-76, 2020-53, 2020-41, 2020-33, 2020-24, 2020-21 and 2020-18) are likewise incorporated by reference as a specific finding pursuant to 18 U.S.C. § 3161(h)(7)(A) in the record of each pending case where the Speedy Trial Act applies.

11. Individual judges may continue to hold hearings, conferences, and bench trials in the exercise of their discretion, consistent with this Order.

12. Judges are strongly encouraged to conduct court proceedings by telephone or video conferencing where practicable.

13. Criminal matters before Magistrate Judges, such as initial appearances, arraignments, detention hearings, and the issuance of search warrants, shall continue to take place in the ordinary course.

14. All grand jury sessions in the Southern District of Florida resumed on November 16, 2020, with no more than two grand jury sessions per week. The U.S. Attorney's Office and Clerk of Court will continue to safely convene no more than two grand jury sessions per week until further Order. The Court may issue other Orders concerning future continuances, or additional grand jury sessions, as necessary and appropriate.

15. This Court's most recent Administrative Order on the Coronavirus pandemic (2021-12) states that, although the Speedy Trial Act requires an information or indictment charging an individual with the commission of an offense to be filed within thirty (30) days from the

date on which such individual was arrested or served with a summons in connection with such charges, the period from March 26, 2020, until July 6, 2021, is excluded pursuant to 18 U.S.C. § 3161(h)(7)(A) and (B)(iii). The Court is cognizant of the right of criminal defendants to a speedy and public trial under the Sixth Amendment, and the particular application of that right in cases involving defendants who are detained pending trial. Nonetheless, this Court found that the ends of justice served by excluding this time outweighed the interests of the parties and the public in a speedy trial because the absence of grand jury sessions made it unreasonable to expect the return and filing of an indictment within the period set forth in 18 U.S.C. § 3161(b). Likewise, the Court finds that the ends of justice are served by extending again this period of exclusion, and outweigh the interests of the parties and the public in a speedy trial. As stated above, this Court has authorized the resumption of only two grand jury sessions per week; ordinarily, according to the U.S. Attorney's Office, there are eleven. Additionally, according to the U.S. Attorney's Office, it must present approximately 150 matters to a grand jury for indictment, plus new arrests. Given the limited availability of grand jury resources and continued exigent circumstances created by the pandemic, the Court finds that it remains generally unreasonable to expect the return and filing of an indictment within the period set forth in 18 U.S.C. § 3161(b), and an additional period of exclusion will promote the safe and orderly administration of justice. The additional period of exclusion shall be for the period from March 15, 2021, until July 6, 2021. The Court may shorten or extend the period of exclusion as circumstances warrant. Any individual judge may enter an Order modifying this additional period of exclusion for any particular case, including upon motion by any party. This Order and period of exclusion are incorporated by reference as a specific finding pursuant to 18 U.S.C. § 3161(h)(7)(A) in the record of each pending case where the Speedy Trial Act applies. *See Zedner v. United*

States, 547 U.S. 489, 506–07 (2006).

16. All judicial naturalization ceremonies in the Southern District of Florida will be held remotely or by video conference.

17. The Clerk's Office, Probation, the Bankruptcy Court, and all other Court services shall remain open with reduced staffing, at a level to maintain essential operations, consistent with Administrative Order 2020-20.

This Order shall remain in effect until further Order of the Court.

DONE AND ORDERED in Chambers at Miami, Miami-Dade County, Florida, this 6th day of April, 2021.

K.M.Moore

K. MICHAEL MOORE
CHIEF UNITED STATES DISTRICT JUDGE

c: Honorable William H. Pryor, Jr., Chief Judge, Eleventh Circuit
All Southern District Judges, Bankruptcy and Magistrate Judges
James Gerstenlauer, Circuit Executive, Eleventh Circuit
Juan Antonio Gonzalez, Acting United States Attorney
Gadyaces Serralta, United States Marshal
Michael Caruso, Federal Public Defender
Angela E. Noble, Court Administrator • Clerk of Court
Joe Falzone, Clerk, Bankruptcy Court
Consuelo Irimia, Chief Probation Officer
Library

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

24341 7590 08/17/2022
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
HAMILTON, MATTHEW L	
ART UNIT	PAPER NUMBER
3682	

DATE MAILED: 08/17/2022

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/681,673	11/12/2019	Paresh K. Patel	104402-5038-US	1077

TITLE OF INVENTION: Method and System for Asynchronous Mobile Payments for Multiple In-Person Transactions Conducted in Parallel

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	11/17/2022

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

24341 7590 08/17/2022

Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/681,673	11/12/2019	Paresh K. Patel	104402-5038-US	1077

TITLE OF INVENTION: Method and System for Asynchronous Mobile Payments for Multiple In-Person Transactions Conducted in Parallel

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	11/17/2022

EXAMINER	ART UNIT	CLASS-SUBCLASS
HAMILTON, MATTHEW L	3682	705-071000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1____________________

2____________________

3____________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual □ Corporation or other private group entity □ Government

4a. Fees submitted: □Issue Fee □Publication Fee (if required) □Advance Order - # of Copies ________________

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

□ Electronic Payment via EFS-Web □ Enclosed check □ Non-electronic payment by credit card (Attach form PTO-2038)

□ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. __________

5. **Change in Entity Status** (from status indicated above)

□ Applicant certifying micro entity status. See 37 CFR 1.29

□ Applicant asserting small entity status. See 37 CFR 1.27

□ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature ____________________ Date ____________________

Typed or printed name ____________________ Registration No. ____________________

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
16/681,673	11/12/2019	Paresh K. Patel	104402-5038-US	1077

24341 7590 08/17/2022

Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
HAMILTON, MATTHEW L	
ART UNIT	PAPER NUMBER
3682	

DATE MAILED: 08/17/2022

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	**Application No.** 16/681,673	**Applicant(s)** Patel et al.	
	Examiner MATTHEW L HAMILTON	**Art Unit** 3682	**AIA (FITF) Status** Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.☑ This communication is responsive to June 24, 2022.

□ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2.□ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3.☑ The allowed claim(s) is/are 1-20 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4.□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) □All b) □ Some* c) □ None of the:

1. □ Certified copies of the priority documents have been received.
2. □ Certified copies of the priority documents have been received in Application No. _____ .
3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5.□ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

□ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6.□ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1.☑ Notice of References Cited (PTO-892)

2.□ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.

3.□ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.

4.□ Interview Summary (PTO-413), Paper No./Mail Date. _____.

5. ☑ Examiner's Amendment/Comment

6. ☑ Examiner's Statement of Reasons for Allowance

7. ☑ Other Examiner's Amendment.

/MATTHEW L HAMILTON/
Primary Examiner, Art Unit 3682

DETAILED ACTION

Response to Amendment

This action is in response to the amendment filed on June 24, 2022. Claims 1-4, 6-11, 13-17, and 19-20 have been amended. Claims 1-20 have been examined and are currently pending.

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Inventorship

This application currently names joint inventors. In considering patentability of the claims the examiner presumes that the subject matter of the various claims was commonly owned as of the effective filing date of the claimed invention(s) absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and effective filing dates of each claim that was not commonly owned as of the effective filing date of the later invention in order for the examiner to consider the applicability of 35 U.S.C. 102(b)(2)(C) for any potential 35 U.S.C. 102(a)(2) prior art against the later invention.

EXAMINER'S AMENDMENT

Claims 1-20 are allowed subject to the examiner's amendment described below. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in an interview with Douglas J. Crisman, Reg. 39,951 on July 27, 2022.

The application has been amended as follows: Please amend claims 1, 3, 8, 10, 14, and 16.

1. (Currently Amended) A method, comprising:

at a consumer device including a display, one or more processors, a communications unit, and memory, performing by an application executing on the consumer device:

identifying a first merchant device in proximity to the consumer device based at least in part on broadcasted information transmitted by the first merchant device, wherein the broadcasted information includes a first identifier corresponding to the first merchant device;

transmitting via the communications unit of the consumer device the first identifier to a server and, in response to transmitting the first identifier to the server, receiving from the server an electronic communication including:

first merchant identification information of a first merchant associated with the first merchant device, wherein the first merchant identification information includes one or more of a name, logo, picture, address, phone, or email of the first merchant; and

first merchant transaction information identifying a proposed in-person transaction between the consumer device and the first merchant, wherein the first merchant transaction information includes [[a]] one or more merchant-specified preset transaction amounts each associated with a product or service;

displaying on the display of the consumer device the first merchant identification information;

receiving from a user of the consumer device selection of the first merchant identification information;

in response to receiving the selection of the first merchant identification information:

displaying the first merchant transaction information;

receiving from the user of the consumer device first supplemental transaction information, wherein the first supplemental transaction information is a selection of the one or more merchant-specified preset transaction amounts each associated with a product or service; and

transmitting the first supplemental transaction information to the server; and

in response to transmitting the first supplemental transaction information to the server, receiving confirmation from the server that the proposed in-person transaction between the consumer device and the first merchant has been completed.

3. (Currently Amended) The method of claim 1, further comprising:

identifying by the application executing on the consumer device a second merchant device in proximity to the consumer device based at least in part on broadcasted information transmitted by the second merchant device, wherein the broadcasted information includes a second identifier corresponding to the second merchant device; and

transmitting via the communications unit of the consumer device the second identifier to the server;

wherein the electronic communication received from the server further includes:

second merchant identification information of a second merchant associated with the second merchant device, wherein the second merchant identification information includes one or more of a name, logo, picture, address, phone, or email of the second merchant; and

second merchant transaction information identifying a proposed in-person transaction between the consumer device and the second merchant, wherein the second merchant transaction information includes [[a]] one or more merchant-specified preset transaction amounts each associated with a product or service; and

wherein displaying on the display of the consumer device the first merchant identification information further includes simultaneously displaying on the display of the consumer device the first merchant identification information and the second merchant identification information.

8. (Currently Amended) A consumer device, comprising:

a display;

one or more processors; and

memory storing one or more programs to be executed by the one or more processors, the one or more programs comprising instructions for:

at a consumer device including a display, one or more processors, a communications unit, and memory, performing by an application executing on the consumer device:

identifying a first merchant device in proximity to the consumer device based at least in part on broadcasted information transmitted by the first merchant device, wherein the broadcasted information includes a first identifier corresponding to the first merchant device;

transmitting via the communications unit of the consumer device the first identifier to a server and, in response to transmitting the first identifier to the server, receiving from the server an electronic communication including:

first merchant identification information of a first merchant associated with the first merchant device, wherein the first merchant identification information includes one or more of a name, logo, picture, address, phone, or email of the first merchant; and

first merchant transaction information identifying a proposed in-person transaction between the consumer device and the first merchant, wherein the first merchant transaction information includes [[a]] one or more merchant-specified preset transaction amounts each associated with a product or service;

displaying on the display of the consumer device the first merchant identification information;

receiving from a user of the consumer device selection of the first merchant identification information;

in response to receiving the selection of the first merchant identification information:

displaying the first merchant transaction information;

receiving from the user of the consumer device first supplemental transaction information, wherein the first supplemental transaction information is a selection of the one or more merchant-specified preset transaction amounts each associated with a product or service; and

transmitting the first supplemental transaction information to the server; and

in response to transmitting the first supplemental transaction information to the server, receiving confirmation from the server that the proposed in-person transaction between the consumer device and the first merchant has been completed.

10. (Currently Amended) The consumer device of claim 8, further comprising instructions for:

identifying by the application executing on the consumer device a second merchant device in proximity to the consumer device based at least in part on broadcasted information transmitted by the second merchant device, wherein the broadcasted information includes a second identifier corresponding to the second merchant device; and

transmitting via the communications unit of the consumer device the second identifier to the server;

wherein the electronic communication received from the server further includes:

second merchant identification information of a second merchant associated with the second merchant device, wherein the second merchant identification information includes one or more of a name, logo, picture, address, phone, or email of the second merchant; and

second merchant transaction information identifying a proposed in-person transaction between the consumer device and the second merchant, wherein the second merchant transaction information includes [[a]] one or more merchant-specified preset transaction amounts each associated with a product or service; and

wherein displaying on the display of the consumer device the first merchant identification information further includes simultaneously displaying on the display of the consumer device the first merchant identification information and the second merchant identification information.

14. (Currently Amended) A non-transitory computer readable storage medium storing one or more programs configured for execution by a computer system, the one or more programs including instructions for:

at a consumer device including a display, one or more processors, a communications unit, and memory, performing by an application executing on the consumer device:

identifying a first merchant device in proximity to the consumer device based at least in part on broadcasted information transmitted by the first merchant device, wherein the broadcasted information includes a first identifier corresponding to the first merchant device;

transmitting via the communications unit of the consumer device the first identifier to a server and, in response to transmitting the first identifier to the server, receiving from the server an electronic communication including:

first merchant identification information of a first merchant associated with the first merchant device, wherein the first merchant identification information includes one or more of a name, logo, picture, address, phone, or email of the first merchant; and

first merchant transaction information identifying a proposed in-person transaction between the consumer device and the first merchant, wherein the first merchant transaction information includes [[a]] one or more merchant-specified preset transaction amounts each associated with a product or service;

displaying on the display of the consumer device the first merchant identification information;

receiving from a user of the consumer device selection of the first merchant identification information;

in response to receiving the selection of the first merchant identification information:

displaying the first merchant transaction information;

receiving from the user of the consumer device first supplemental transaction information, wherein the first supplemental transaction information is a selection of the one or more merchant-specified preset transaction amounts each associated with a product or service; and

transmitting the first supplemental transaction information to the server; and

in response to transmitting the first supplemental transaction information to the server, receiving confirmation from the server that the proposed in-person transaction between the consumer device and the first merchant has been completed.

16. (Currently Amended) The non-transitory computer readable storage medium of claim 14, further comprising instructions for:

identifying by the application executing on the consumer device a second merchant device in proximity to the consumer device based at least in part on broadcasted information transmitted by the second merchant device, wherein the broadcasted information includes a second identifier corresponding to the second merchant device; and

transmitting via the communications unit of the consumer device the second identifier to the server;

wherein the electronic communication received from the server further includes:

second merchant identification information of a second merchant associated with the second merchant device, wherein the second merchant identification information includes one or more of a name, logo, picture, address, phone, or email of the second merchant; and

second merchant transaction information identifying a proposed in-person transaction between the consumer device and the second merchant, wherein the second merchant transaction information includes [[a]] one or more merchant-specified preset transaction amounts each associated with a product or service; and

wherein displaying on the display of the consumer device the first merchant identification information further includes simultaneously displaying on the display of the consumer device the first merchant identification information and the second merchant identification information.

Klingen US Publication 20160092859 A1 System and Method for Facilitating a Purchase Transaction Using Beacon Equipped Devices

Klingen discloses a purchase transaction between a merchant and a customer, a merchant device sends transaction information to a payment gateway and sends a beacon signal containing a transaction identifier to a customer mobile device. The customer mobile device sends the transaction identifier and payment information corresponding to a customer payment account to the payment gateway. The payment gateway applies the transaction identifier to access the transaction information received from the merchant device and sends purchase information based on the transaction information to the customer mobile device. The customer mobile device displays the purchase information to the customer, obtains an indication of customer assent to pay for the item and sends a confirmation of customer assent to the payment gateway. Upon receiving the confirmation of customer assent from the customer mobile device, the payment gateway processes the purchase transaction based on the payment account information.

Dhurka et al. US Publication 2017013478 A1 Checkout Kiosk Connected to a Mobile Payment Application for Expedited Transaction Processing

Dhurka discloses systems and methods for a checkout kiosk connected to a mobile payment application for expedited transaction processing. A user may visit a merchant location for a merchant and select one or more items for purchase from the merchant. A payment provider used to provide payments to the merchant may establish a kiosk at the merchant location. The user may utilize the kiosk to perform transaction processing instead of utilizing a checkout line by entering the items selected for purchase using a mobile device and payment application for the payment provider. A device at the kiosk may provide the payment application to the mobile device, and may assist the user in establishing a payment account with the payment provider. The kiosk may further provide matching of items in the transaction to items in possession of the user to prevent fraud or theft of items.

Fiore et al. US Publication 20130275303 A1 Method and System for Two Stage Authentication with Geolocation

Fiore discloses geographical location information provided by a mobile device is used to assist in providing a first authentication for payment transactions against a payment account number of a user. Mobile device identification is associated with a payment account number of the user such that the user is provided a first authentication for payment transactions against the payment account number when the mobile device has entered a premises of a merchant.

The present invention discloses a mobile consumer device with a display, processor(s), and memory: identifies a merchant device in proximity to the consumer device based on broadcasted information transmitted by the first merchant device, the broadcasted information including a first identifier corresponding to the first merchant device; transmits the first identifier to a server and receives from the server an electronic communication including identification and transaction information associated with the merchant; displays the identification information, receives user selection of the merchant identification information; and in response, displays the merchant transaction information, receives supplemental user information, and transmits the supplemental transaction information to the server for completion of the transaction.

Claim 1 is allowed because the prior art of record of Klingen, Dhurka, and Fiore alone or in combination, fails to teach or suggest or otherwise make obvious, all the limitations comprising:

first merchant transaction information identifying a proposed in-person transaction between the consumer device and the first merchant, wherein the first merchant transaction information includes one or more merchant-specified preset transaction amounts each associated with a product or service;

displaying the first merchant transaction information;

receiving from the user of the consumer device first supplemental transaction information, wherein the first supplemental transaction information is a selection of the one or more merchant-specified preset transaction amounts each associated with a product or service;

Independent claims 8 and 14 are allowed based on a similar rationale. Dependent claims 2-7, 9-13, and 15-20 are allowable based on the same rationale as the claims they depend.

Objections to claims 1-4, 8-11, and 14-17 have been withdrawn.

The Examiner notes the applicant's invention is directed to patentable eligible subject matter under 35 U.S.C. 101. The applicant's invention provides an improvement over past systems, the applicant's specification discloses, "Traditional electronic payment systems for in-person transactions are one-to-one such that there is one merchant and one consumer conducting one transaction at a time. The process requires a captive, exclusive interaction between the merchant and consumer, and typically neither party may disengage from the process until the payment has completed or has been cancelled." (paragraph 0007), "Additionally, other consumers who want to make a payment to the same merchant must wait until the current transaction has completed processing. Consumers interact with the merchant sequentially and wait their turn." (paragraph 0008), "This system is acceptable in traditional retail situations where one consumer is purchasing a good or service and needs the merchant to perform "check out" tasks. In such electronic payment systems, the payment transaction is first initiated by the merchant (e.g., requesting a consumer pay a certain amount). These electronic payment systems do not work well when there are multiple consumers needing to pay a single merchant at approximately the same time, or when the merchant is not able to initiate the payment process." (paragraph 0009), "Implementations described herein provide methods and systems for enabling electronic payments via a mobile device such that multiple consumers can initiate overlapping in-person payments to a single merchant at the same time, or substantially the same time. Moreover, in some implementations, the consumer has the option to send payment to a merchant without the merchant having to request payment first." (paragraph 0011), "There are numerous use cases for such a system, some of which are currently only handled by cash payments (since existing electronic payment systems do not address the need to have multiple parties sending payments to a single merchant). One example use case involves payments to a street performer, who would traditionally put out a box, hat, or an open guitar case (collectively referred to as collection box) for audience payments. As he or she is performing, any number of audience members can drop cash into the collection box to pay the performer." (paragraph 0012) and "Notably, the performer (or in different contexts, a merchant) is not required to initiate the payment with each consumer and does not need to stop doing what he or she is doing. A plurality of consumers can also pay the performer/merchant without needing to wait for each transaction to finish. The transaction is asynchronous as the performer/merchant need not acknowledge the transaction before the next payment and may not acknowledge the payment at all. Methods and systems described herein allow this and similar in-person payment scenarios to be handled via electronic payments managed via mobile electronic devices associated with a merchant/performer and one or more customers." (paragraph 0013).

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Greiner et al. US Patent 10217151 B1 Systems and Methods for Proximity Based Communication

Greiner discloses a system may transmit a signal originating from a BLUETOOTH low energy (“BLE”) beacon at a merchant location. The signal may include a first identifier associated with the merchant location and a merchant device. A customer device may receive the signal within a predetermined distance of the BLE beacon. The system may receive a transmission sent by the customer device in response to the signal from the BLE beacon. The transmission may include a second identifier associated with the user. The system may identify the user associated with the customer device based on the second identifier. The user may be at the merchant location.

Apriva LLC Awarded Patent for System and Method for Facilitating a Purchase Transaction using a Customer Device Beacon, June 7, 2017, Global IP News (Year: 2017)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW L HAMILTON whose telephone number is (571)270-1837. The examiner can normally be reached Monday-Thursday 9:30-5:30 pm EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Waseem Ashraf can be reached on (571)270-3948. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MATTHEW L HAMILTON/
Primary Examiner, Art Unit 3682

Notice of References Cited	Application/Control No. 16/681,673	Applicant(s)/Patent Under Reexamination Patel et al.	
	Examiner MATTHEW L HAMILTON	Art Unit 3682	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-10217151-B1	02-2019	Greiner; Hans-Jurgen	H04W4/80	1/1
	B					
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Apriva LLC Awarded Patent for System and Method for Facilitating a Purchase Transaction using a Customer Device Beacon, June 7, 2017, Global IP News (Year: 2017)
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

BLUETOOTH DOC	Date / Year-Month-Day 2005-11-25	Approved Adopted	Revision V10r00	Document No HFP1.5_SPEC
Prepared Car Working Group	e-mail address car-feedback@bluetooth.org			N.B.

HANDS-FREE PROFILE 1.5

Abstract

The Hands-Free Profile (HFP) 1.5 specification defines the minimum set of functions such that a Mobile Phone can be used in conjunction with a Hands-Free device (e.g. installed in the car or represented by a wearable device such as a headset), with a *Bluetooth*® Link providing a wireless means for both remote control of the Mobile Phone by the Hands-Free device and voice connections between the Mobile Phone and the Hands-Free device.

Compliance with this specification assures interoperability between a Bluetooth enabled Hands-Free device and any Bluetooth equipped Mobile Phone supporting this profile.

Revision History

Revision Number	Date	Comments
RC10.50	01-01-2912-11-2003	Hands-Free Profile 0.50 published1st draft for SubWG12 Review
RC21.00m VD	22-11-200403-14-03	CR document derived from FIPD07r04Additional comments from BTI/BQRB reviews
D10r08	16-02-2005	Editing for Prototyping Specification standards
D12r00	19-03-2005	Incorporated Prototyping Specifications
D12r01	22-04-2005	Errata and corrections from IOP.
D12r02	28-04-2005	HFP 1.0 Errata- 13, 261, 317, 549, 550, 575, 586, 635, 706, 731, 746
D15r03	13-05-2005	Correct formatting problems and comments from review.
D15r04	27-05-2005	Errata 819, 820, 821, 822
D15r05	07-06-2005	Edits from BARB Review. Errata 823.
D15r06	07-18-2005	Changes from BARB review. Editorial changes for language and readability.
D15r07	08-01-2005	Comments from BTI/BARB review.
D15r08	09/02/2005	Comments from BTI review.
D15r09	09/22/2005	Comments from BTI review
D15r09	09/26/2005	Add 3GPP 27.07 version and remove reference to Call Waiting for AT+CHUP
D15r10-11	10/04/2005	BTI Comments
D15r12	10/05/2005	Editorial changes
D15r13	10/07/2005	Prepare for publication
V10r00	11/25/2005	Adopted by the *Bluetooth* Board of Directors

Contributors

Name	Company
Aaron WEINFIELD	Denso
Basam MASRI	Denso
Don LIECHTY	Extended Systems
Stephen RAXTER	Johnson Controls
Vartika AGARWAL	Motorola
Leonard HINDS	Motorola
Burch SEYMOUR	Motorola
Stephane BOUET	Nissan
Jamie MCHARDY	Nokia
Jurgen SCHNITZLER	Nokia
Guillaume POUJADE	Parrot
Dmitri TOROPOV	Siemens
Erwin WEINANS	Sony Ericsson
Tim REILLY	Stonestreet One
Akira MIYAJIMA	Toyota
Ryan BRUNER	Visteon
Scott WALSH	Plantronics
Patrick CLAUBERG	Nokia
Neil MACMULLEN	CSR
Michael BUNTSCHECK	BMS
Florencio CEBALLOS	Visteon
Bill BERNARD	Visteon

Disclaimer and Copyright Notice

The copyright in this specification is owned by the Promoter Members of *Bluetooth*® Special Interest Group (SIG), Inc. (“*Bluetooth* SIG”). Use of these specifications and any related intellectual property (collectively, the “Specification”), is governed by the Promoters Membership Agreement among the Promoter Members and *Bluetooth* SIG (the “Promoters Agreement”), certain membership agreements between *Bluetooth* SIG and its Adopter and Associate Members (the “Membership Agreements”) and the *Bluetooth* Specification Early Adopters Agreements (1.2 Early Adopters Agreements) among Early Adopter members of the unincorporated *Bluetooth* SIG and the Promoter Members (the “Early Adopters Agreement”). Certain rights and obligations of the Promoter Members under the Early Adopters Agreements have been assigned to *Bluetooth* SIG by the Promoter Members.

Use of the Specification by anyone who is not a member of *Bluetooth* SIG or a party to an Early Adopters Agreement (each such person or party, a “Member”), is prohibited. The legal rights and obligations of each Member are governed by their applicable Membership Agreement, Early Adopters Agreement or Promoters Agreement. No license, express or implied, by estoppel or otherwise, to any intellectual property rights are granted herein.

Any use of the Specification not in compliance with the terms of the applicable Membership Agreement, Early Adopters Agreement or Promoters Agreement is prohibited and any such prohibited use may result in termination of the applicable Membership Agreement or Early Adopters Agreement and other liability permitted by the applicable agreement or by applicable law to *Bluetooth* SIG or any of its members for patent, copyright and/or trademark infringement.

THE SPECIFICATION IS PROVIDED “AS IS” WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, SATISFACTORY QUALITY, OR REASONABLE SKILL OR CARE, OR ANY WARRANTY ARISING OUT OF ANY COURSE OF DEALING, USAGE, TRADE PRACTICE, PROPOSAL, SPECIFICATION OR SAMPLE.

Each Member hereby acknowledges that products equipped with the *Bluetooth* technology ("*Bluetooth* products") may be subject to various regulatory controls under the laws and regulations of various governments worldwide. Such laws and regulatory controls may govern, among other things, the combination, operation, use, implementation and distribution of *Bluetooth* products. Examples of such laws and regulatory controls include, but are not limited to, airline regulatory controls, telecommunications regulations, technology transfer controls and health and safety regulations. Each Member is solely responsible for the compliance by their *Bluetooth* Products with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for their *Bluetooth* products related to such regulations within the applicable jurisdictions. Each Member acknowledges that nothing in the Specification provides any information or assistance in connection with securing such compliance, authorizations or licenses. **NOTHING IN THE SPECIFICATION CREATES ANY WARRANTIES, EITHER EXPRESS OR IMPLIED, REGARDING SUCH LAWS OR REGULATIONS.**

ALL LIABILITY, INCLUDING LIABILITY FOR INFRINGEMENT OF ANY INTELLECTUAL PROPERTY RIGHTS OR FOR NONCOMPLIANCE WITH LAWS, RELATING TO USE OF THE SPECIFICATION IS EXPRESSLY DISCLAIMED. BY USE OF THE SPECIFICATION, EACH MEMBER EXPRESSLY WAIVES ANY CLAIM AGAINST *BLUETOOTH* SIG AND ITS PROMOTER MEMBERS RELATED TO USE OF THE SPECIFICATION.

Bluetooth SIG reserve the right to adopt any changes or alterations to the Specification as it deems necessary or appropriate.

Contents

1 Introduction

1.1 Scope

This document defines the protocols and procedures that shall be used by devices implementing the Hands-Free Profile. The most common examples of such devices are in-car Hands-Free units used together with cellular phones, or wearable wireless headsets.

The profile defines how two devices supporting the Hands-Free Profile shall interact with each other on a point-to-point basis.

An implementation of the Hands-Free Profile typically enables a headset, or an embedded Hands-Free unit to connect, wirelessly, to a cellular phone for the purposes of acting as the cellular phone's audio input and output mechanism and allowing typical telephony functions to be performed without access to the actual phone.

1.2 Profile Dependencies

In Figure 1.1, the Bluetooth profile structure and the dependencies of the profiles are depicted. A profile is dependent upon another profile if it re-uses parts of that profile, by explicitly referencing it. Dependency is illustrated in the figure below.

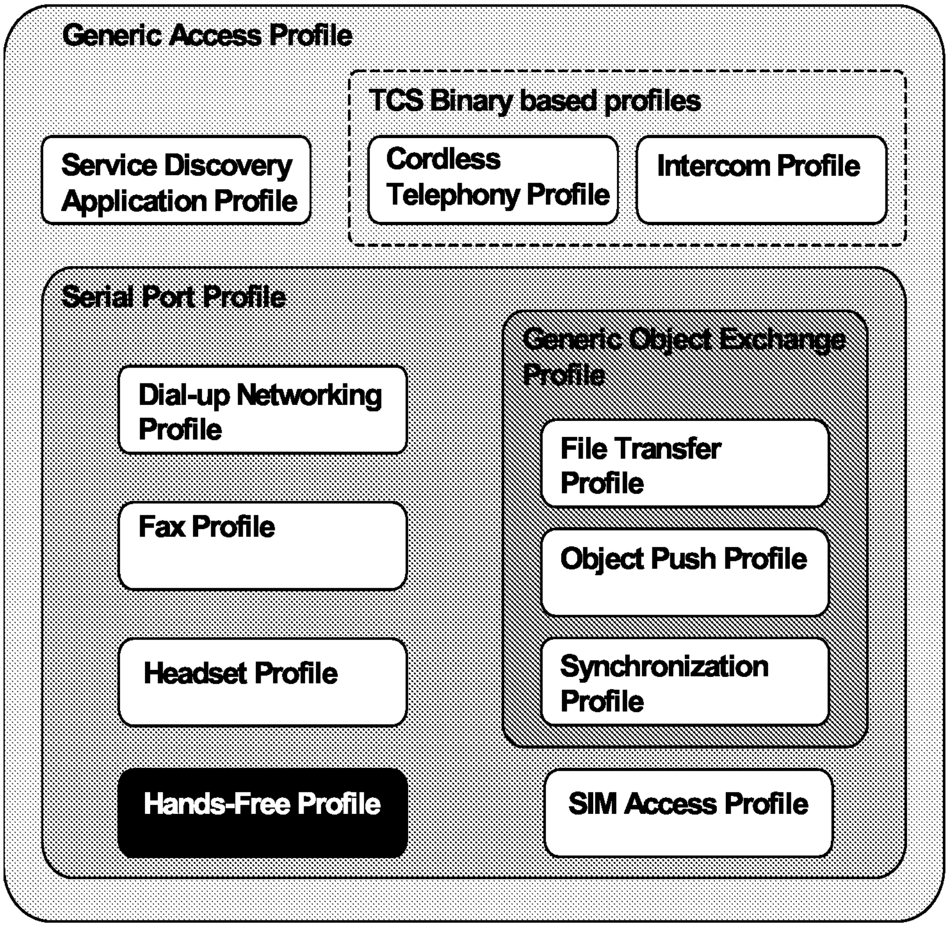


Figure 1.1: Bluetooth Profiles

As indicated in the figure, the Hands-Free Profile is dependent upon both the Serial Port Profile [5] and the Generic Access Profile [4]. Details are provided in Sections 5 (Serial Port Profile) and 6 (Generic Access Profile).

1.3 Symbols and Conventions

1.3.1 Requirement Status Symbols

In this document, the following symbols are used:

- "M" for mandatory to support
- "O" for optional to support
- "X" for excluded (used for capabilities that may be supported by the device, but the Hands-Free Profile shall not use these capabilities)

- "C" for conditional to support
- "N/A" for not applicable (in the given context this capability is not defined)

Some capabilities or features (identified as “X”), mandated according to the relevant Bluetooth specifications, are excluded with respect to this profile because they may degrade the operation of devices in the particular use case. Therefore, features or capabilities labeled “X” shall never be activated while operating in a use case where they are labeled as such.

1.3.2 Naming Conventions

In this document, the following naming conventions are used:

- Where “Core Specification” is said it refers to the Bluetooth Core Specification 1.1 or later adopted by the Bluetooth® SIG.
- Where “LMP link” is said, it means a Link Manager (LM) level link over which only Link Manager Protocol (LMP) commands are conveyed.
- Where “RFCOMM connection” is said, it means the presence of a virtual serial port as specified in [5].
- Where “Service Level Connection” is said, it means a synchronized high-level protocol connection involving a portion of the protocol stack. In this specific case, it refers to the presence of a RFCOMM connection, and assumes that the HF has synchronized itself to the state of the AG using the specified Service Level Connection initialization procedure.
- Where “Service Level Connection initialization” is said, it means the execution of the set of AT commands and responses specified by the profile necessary to synchronize the state of the HF with that of the AG.
- Where “Service Level Connection establishment” is said, it means the combined process of establishing the RFCOMM connection, as well as the necessary device synchronization using Service Level Connection initialization.
- Where “Synchronous Connection” is said, it means a SCO or eSCO logical link intended for supporting a full duplex Audio Connection.
- Where “Audio Connection” is said, it means a Synchronous Connection including the means to provide a complete audio path between two devices assuming roles within this profile.
- Where “incoming call” is said, it means a call connection in the direction “Phone Network=>AG”, such that it is initiated by the Network to which the AG is attached.
- Where ‘outgoing call’ is said, it means a call connection in the direction ”AG=>Phone Network”, such that it is initiated by the AG towards the Network to which it is attached.

1.3.3 Signaling Diagram Conventions

The signaling diagrams in this specification are informative only. Within the diagrams, the following conventions are used to describe procedures:

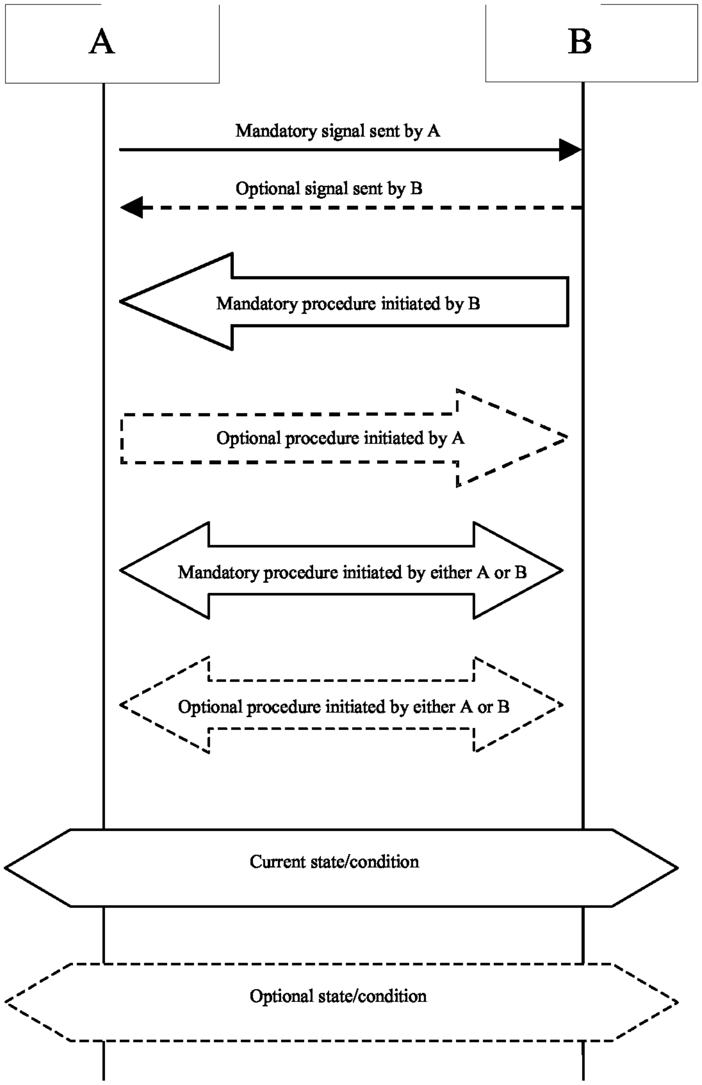

A
B
Mandatory signal sent by A
Optional signal sent by B
Mandatory procedure initiated by B
Optional procedure initiated by A
Mandatory procedure initiated by either A or B
Optional procedure initiated by either A or B
Current state/condition
Optional state/condition

Figure 1.2: Conventions used in signaling diagrams

2 Profile Overview

2.1 Protocol Stack

The figure below shows the protocols and entities used in this profile.

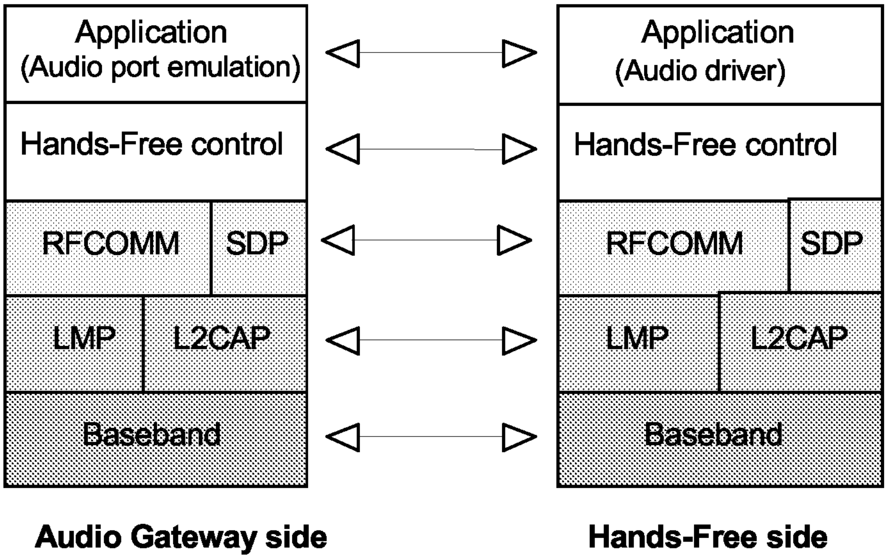


Figure 2.1: Protocol stack

The Baseband, LMP and L2CAP are the OSI layer 1 and 2 Bluetooth protocols. RFCOMM is the Bluetooth serial port emulation entity. SDP is the Bluetooth Service Discovery Protocol. See [1] for more details on these topics.

Compatibility to v1.1 or later Core Specification is required.

Hands-Free control is the entity responsible for Hands-Free unit specific control signaling; this signaling is AT command based.

Although not shown in the model above, it is assumed by this profile that Hands-Free Control has access to some lower layer procedures (for example, Synchronous Connection establishment).

The audio port emulation layer shown in Figure 2.1 is the entity emulating the audio port on the Audio Gateway, and the audio driver is the driver software in the Hands-Free unit.

For the shaded protocols/entities in Figure 2.1, the Serial Port Profile [5] is used as the base standard. For these protocols, all mandatory requirements stated in the Serial Port Profile apply except in those cases where this specification explicitly states deviations.

2.2 Configuration and Roles

Figure 2.2 below shows typical configurations of devices for which the Hands-Free Profile is applicable:

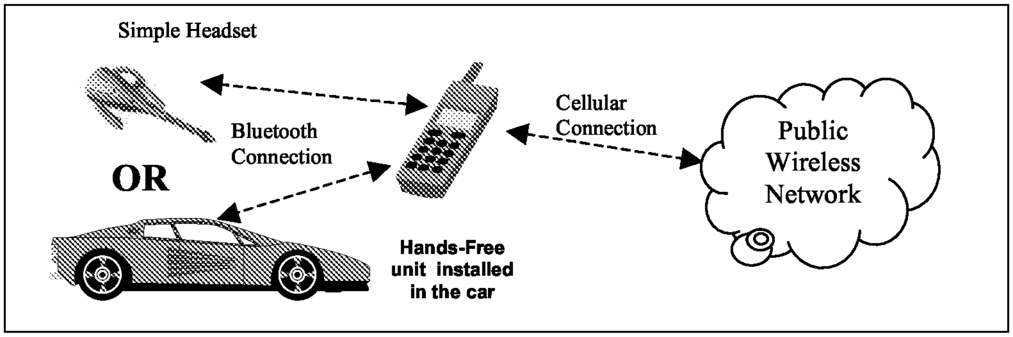


Figure 2.2: Typical Hands-Free Use

The following roles are defined for this profile:

Audio Gateway (AG) – This is the device that is the gateway of the audio, both for input and output. Typical devices acting as Audio Gateways are cellular phones.

Hands-Free unit (HF) – This is the device acting as the Audio Gateway's remote audio input and output mechanism. It also provides some remote control means.

These terms are used in the rest of this document to designate these roles.

2.3 User Requirements and Scenarios

The following rules apply to this profile:

a) The profile states the mandatory and optional features when the "Hands-Free Profile" is active in the Audio Gateway and the Hands-Free unit.

b) The profile mandates the usage of CVSD for transmission of audio (over the Bluetooth link). The resulting audio is monophonic, with a quality that, under normal circumstances, does not have perceived audio degradation.

c) Between the Hands-Free unit and the Audio Gateway, only one Audio Connection per Service Level Connection at a time is supported.

d) Both the Audio Gateway and the Hands-Free unit may initiate Audio Connection establishment and release. Valid speech data shall exist on the Synchronous Connection in both directions after the Audio Connection is established.

e) Whenever an "Audio Connection" exists, a related "Service Level Connection" shall also exist.

f) The presence of a "Service Level Connection" shall not imply that an "Audio Connection" exists. Releasing a "Service Level Connection" shall also release any existing "Audio Connection" related to it.

2.4 Profile Fundamentals

Baseband authentication and encryption is optional for both the Hands-Free unit and the Audio Gateway. If both devices support authentication and encryption, the application on either device may require its use.

A Hands-Free unit may be able to use the services of the Audio Gateway without the creation of a secure connection. It is implementation specific whether the Hands-Free unit provides or supports security enforcement for the user.

Whenever baseband authentication and/or encryption is used, the two devices shall create a secure connection using the GAP authentication procedure as described in Section 5.1 of the Generic Access Profile [4]. This procedure may include entering a Bluetooth PIN code and creation of proper link keys. In cases when the UI of the Hands-Free unit is limited, a fixed Bluetooth PIN code may be used during the GAP authentication procedure.

If a LMP link is not already established between the Hands-Free unit and the Audio Gateway, the LMP link shall be set up before any other procedure is performed.

There are no fixed master of slave roles in the profile.

The Audio Gateway and Hand-Free unit provide serial port emulation. For the serial port emulation, RFCOMM (see [1]) is used. The serial port emulation is used to transport the user data including modem control signals and AT command from the Hands-Free unit to the Audio Gateway. The AT commands are parsed by the Audio Gateway and responses are sent to the Hands-Free unit via the Bluetooth serial port connection.

2.5 Conformance

If conformance to this profile is claimed, all capabilities indicated as mandatory for this profile shall be supported in the specified manner (process mandatory). This also applies for all optional and conditional capabilities for which support is indicated. All mandatory, optional and conditional capabilities, for which support is indicated, are subject to verification as part of the Bluetooth Qualification Program.

3 Application layer

This section describes the feature requirements for units complying with Hands-Free Profile.

Table 3.1 below shows the feature requirements for this profile.

	Feature	Support in HF	Support in AG
1.	Connection management	M	M
2.	Phone status information	M$^{\text{(note 1)}}$	M
3.	Audio Connection handling	M	M
4	Accept an incoming voice call	M	M
5.	Reject an incoming voice call	M	O
6.	Terminate a call	M	M
7.	Audio Connection transfer during an ongoing call	M	M
8.	Place a call with a phone number supplied by the HF	O	M
9.	Place a call using memory dialing	O	M
10.	Place a call to the last number dialed	O	M
11.	Call waiting notification	O	M
12.	Three way calling	O$^{\text{(note 2)}}$	O$^{\text{(note 3)}}$
13.	Calling Line Identification (CLI)	O	M
14.	Echo canceling (EC) and noise reduction (NR)	O	O
15.	Voice recognition activation	O	O
16.	Attach a Phone number to a voice tag	O	O
17.	Ability to transmit DTMF codes	O	M
18.	Remote audio volume control	O	O
19.	Respond and Hold	O	O
20.	Subscriber Number Information	O	M
21a.	Enhanced Call Status	O	M
21b.	Enhanced Call Controls	O	O

Note 1: The HF shall support at least the two indicators "service" and "call".

Note 2: If "Three way calling" is supported by the HF, it shall support AT+CHLD values 1 and 2. The HF may additionally support AT+CHLD values 0,3 and 4.

Note 3: If "Three way calling" is supported by the AG, it shall support AT+CHLD values 1and 2. The AG may additionally support AT+CHLD values 0,3 and 4.

Table 3.1: Application layer procedures

Table 3.2 below maps each feature to the procedures used for that feature. All procedures are mandatory if the feature is supported.

	Feature	Procedure	Ref.
1.	Connection management	Service Level Connection establishment	4.2
		Service Level Connection release	4.3
2.	Phone status information	Transfer of Registration Status Transfer of Signal Strength Indication Transfer of Roaming Status Indication Transfer of Battery Level Indication Query of Operator Selection Extended Audio Gateway Error Codes Transfer of Call, Call Setup and Call Held Status	4.4 4.5 4.6 4.7 4.8 4.9 4.10
3.	Audio Connection handling	Audio Connection set up Audio Connection release	4.11 4.12
4.	Accept an incoming voice call	Answer an incoming call	4.13
5.	Reject an incoming voice call	Reject an incoming call	4.14
6.	Terminate a call	Terminate a call process	4.15
7.	Audio Connection transfer during an ongoing call	Audio Connection transfer towards the HF Audio Connection transfer towards the AG	4.16 4.17
8.	Place a call with the phone number supplied by the HF	Place a call with the phone number supplied by the HF	4.18
9.	Place a call using memory dialing	Memory dialing from the HF	4.19
10.	Place a call to the last number dialed	Last number re-dial from the HF	4.20
11.	Call waiting notification	Call waiting notification activation	4.21
12.	Three way calling	Three way call handling	4.22
13.	Calling Line Identification (CLI)	Calling Line Identification (CLI) notification	4.23
14.	Echo canceling (EC) and noise reduction (NR)	HF unit requests turning off the AG's EC and NR	4.24
15.	Voice recognition activation	Voice recognition activation	4.25
16.	Attach a phone number to a voice tag	Attach a voice tag to a phone number	4.26
17.	Ability to transmit DTMF codes	Transmit DTMF code	4.27

	Feature	Procedure	Ref.
18.	Remote audio volume control	Remote audio volume control Volume level synchronization	4.28
19.	Response and Hold	Query response and hold status Put an incoming call on hold from HF Put an incoming call on hold from AG Accept a held incoming call from HF Accept a held incoming call from AG Reject a held incoming call from HF Reject a held incoming call from AG Held incoming call terminated by caller	4.29 4.29 4.29 4.29 4.29 4.29 4.29 4.29
20.	Subscriber Number Information	Subscriber Number Information	4.30
21a.	Enhanced Call Status	Query Call List Indication of Held Call Status	4.31 4.31
21b.	Enhanced Call Control	Release Specified Call Private Consult Mode	4.32 4.32

Table 3.2: Application layer feature to procedure mapping

4 Hands-Free Control Interoperability Requirements

4.1 Introduction

The interoperability requirements for the Hands-Free Control entity are completely contained in this section. Sections 4.2 through 4.28 specify the requirements for the procedures directly related to the application layer features.

The procedures listed in this section are primarily based on the use of a minimum set of AT commands as the control protocol. Section 4.33 specifies these AT commands and their result codes.

Section 4.2 specifies how Service Level Connections are handled in general and specifically states how the layers beneath the Hands-Free Control entity are used to establish and release a Service Level Connection.

4.2 Service Level Connection Establishment

Upon a user action or an internal event, either the HF or the AG may initiate a Service Level Connection establishment procedure.

A Service Level Connection establishment requires the existence of a RFCOMM connection, that is, a RFCOMM data link channel between the HF and the AG.

Both the HF and the AG may initiate the RFCOMM connection establishment. If there is no RFCOMM session between the AG and the HF, the initiating device shall first initialize RFCOMM.

The RFCOMM connection establishment shall be performed as described in Section 7.3 of Generic Access Profile [4] and Section 3 of Serial Port Profile [5].

4.2.1 Service Level Connection Initialization

When an RFCOMM connection has been established the Service Level Connection Initialization procedure shall be executed.

First in the initialization procedure the HF shall send the AT+BRSF=<HF supported features> command to the AG to both notify the AG of the supported features in the HF, as well as to retrieve the supported features in the AG using the +BRSF result code.[1]

After having retrieved the supported features in the AG, the HF shall determine which indicators are supported by the AG, as well as the ordering of the supported indicators. This is because, according to the 3GPP 27.007 specification [2], the AG may support additional indicators not provided for by the Hands-Free Profile, and because the ordering of the indicators is implementation specific. The HF uses the AT+CIND=? Test command to retrieve information about the supported indicators and their ordering.

[1] Audio Gateways supporting the 0.96 version of Hands-Free Profile will return ERROR as a response to AT+BRSF

Once the HF has the necessary supported indicator and ordering information, it shall retrieve the current status of the indicators in the AG using the AT+CIND? Read command.

After having retrieved the status of the indicators in the AG, the HF shall then enable the "Indicators status update" function in the AG by issuing the AT+CMER command, to which the AG shall respond with OK. As a result, the AG shall send the +CIEV unsolicited result code with the corresponding indicator value whenever a change in service, call, or call setup status occurs. When an update is required for both the call and call setup indicators, the AG shall send the +CIEV unsolicited result code for the call indicator before sending the +CIEV unsolicited result code for the call setup indicator. The HF shall use the information provided by the +CIEV code to update its own internal and/or external indications.

Once the "Indicators status update" function has been enabled, the AG shall keep the function enabled until either the AT+CMER command is issued to disable it, or the current Service Level Connection between the AG and the HF is dropped for any reason.

After the HF has enabled the “Indicators status update” function in the AG, and if the “Call waiting and 3-way calling” bit was set in the supported features bitmap by both the HF and the AG, the HF shall issue the AT+CHLD=? test command to retrieve the information about how the call hold and multiparty services are supported in the AG. The HF shall not issue the AT+CHLD=? test command in case either the HF or the AG does not support the "Three way calling" feature.

The HF shall consider the Service Level Connection fully initialized, and thereby established, in either of the following cases:

- After the HF has successfully retrieved information about how call hold and multiparty services are supported in the AG using the AT+CHLD command, if and only if the “Call waiting and 3-way calling” bit was set in the SupportedFeatures attribute of the SDP records for both HF and AG.
- After the HF has successfully enabled the “Indicator status update” using the AT+CMER command, if and only if the “Call waiting and 3-way calling” bit was not set in the SupportedFeatures attribute of the SDP records for either the HF or the AG.

If the HF receives an indication from the AG that a call is currently active, the HF may determine if an unanswered call is currently on hold by querying the Response and Hold state of the AG (see section 4.29.1).

The AG shall consider the Service Level Connection to be fully initialized, and thereby established, in either of the following cases:

- After that the AG has successfully responded with information about how call hold and multiparty services are supported in the AG using +CHLD as well as responded OK, if and only if the “Call waiting and 3-way calling” bit was set in the supported features bitmap for both HF and AG.

- After the AG has successfully responded with OK to the AT+CMER command (to enable the “Indicator status update” function), if and only if the “Call waiting and 3-way calling” bit was not set in the supported features bitmap for either the HF or the AG.

Refer to Section 4.33 for more information on the AT+CIND, AT+CMER, AT+CHLD and AT+BRSF commands and the +CIEV unsolicited result code.

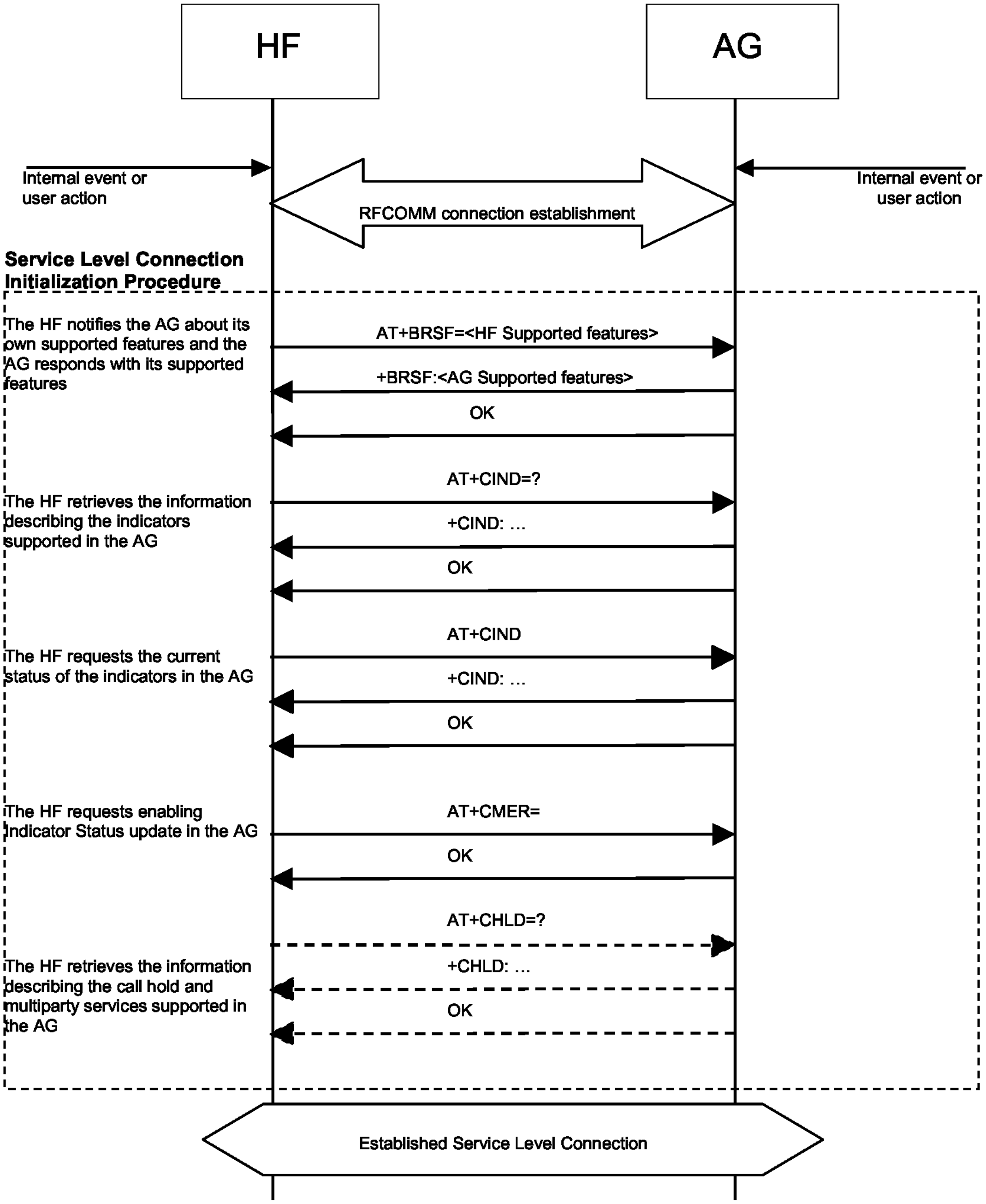

HF
AG
Internal event or user action
Internal event or user action
RFCOMM connection establishment
Service Level Connection Initialization Procedure
The HF notifies the AG about its own supported features and the AG responds with its supported features
AT+BRSF=<HF Supported features>
+BRSF:<AG Supported features>
OK
AT+CIND=?
The HF retrieves the information describing the indicators supported in the AG
+CIND: ...
OK
AT+CIND
The HF requests the current status of the indicators in the AG
+CIND: ...
OK
The HF requests enabling Indicator Status update in the AG
AT+CMER=
OK
AT+CHLD=?
The HF retrieves the information describing the call hold and multiparty services supported in the AG
+CHLD: ...
OK
Established Service Level Connection

Figure 4.1: Service Level Connection establishment

4.2.2 Link Loss Recovery

This section addresses the link loss recovery from a HF unit. The HF unit may reconnect with the AG whenever there is loss of Bluetooth link.

When a Service Level Connection is disconnected due to explicit termination at one end (using the "Service connection release" as described in Section 4.3), then both devices (AG and HF unit) shall wait for an explicit user action before an attempt is made to re-establish the Service Level Connection.

If the HF unit determines that the Service Level Connection was disconnected due to a link supervision timeout, then the HF unit may execute the "Service Level Connection establishment" procedure as described in Section 4.2 to establish a new Service Level Connection to the AG. Following a link loss due to link supervision timeout, the HF unit shall not assume that the service level connection state from the previous connection is valid (such as Call Status, Service Status).

4.3 Service Level Connection Release

This section describes the procedure for releasing a Service Level Connection.

The disconnection of a Service Level Connection shall result in the immediate removal of the corresponding RFCOMM data link channel between the HF and the AG. Also, an existing audio connection has to be removed as consequence of the removal of the Service Level Connection. The removal of the L2CAP and link layers is optional.

An established Service Level Connection shall be released using a “Service Level Connection removal” procedure.

- Either the HF or AG shall initiate the “Service Level Connection release” procedure due to an explicit user request.
- The “Service Level Connection release” procedure shall be initiated if the Bluetooth functionality is disabled in either the HF or AG.
- The “Service Level Connection release” procedure may be initiated if an “Audio Connection transfer towards the AG”, as stated in section 4.12, is performed during an ongoing call in the AG. In the case that the Service Level Connection is removed, the AG shall attempt to re-establish the Service Level Connection once the call is dropped.

As pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist.

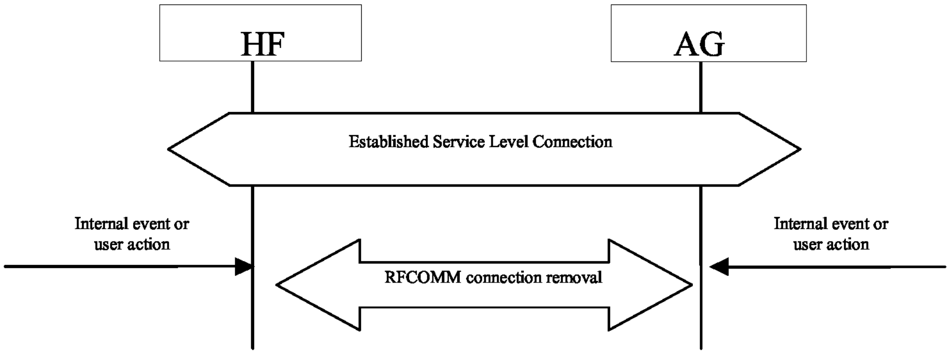

HF
AG
Established Service Level Connection
Internal event or user action
Internal event or user action
RFCOMM connection removal

Figure 4.2: Service Level Connection removal

4.4 Transfer of Registration Status

The AT+CMER command, as described in Section 4.2, enables the "Registration status update" function in the AG. When this function is enabled, the AG shall send the +CIEV unsolicited result code with the corresponding service indicator and value whenever the AG's registration status changes. The HF unit shall be capable of interpreting the information provided by the +CIEV result code to determine the service availability status as listed in Section 4.33.2.

As pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the AG shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.

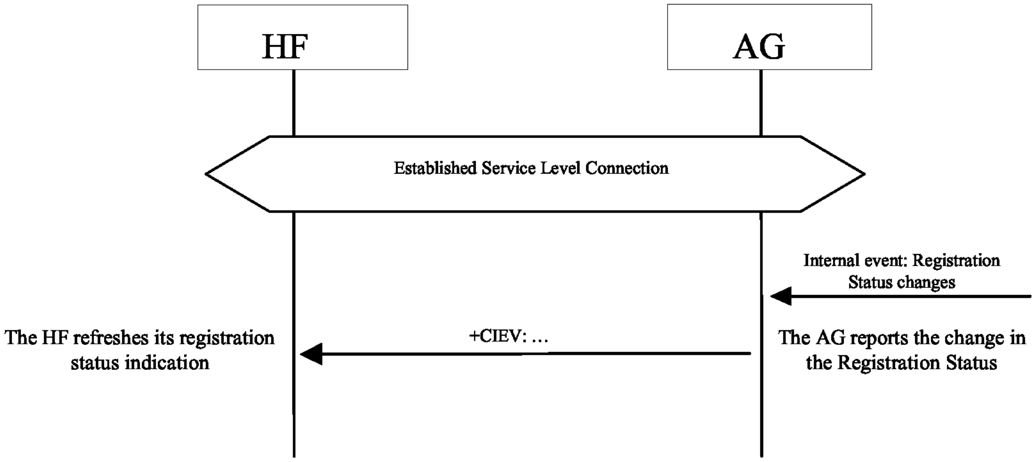

HF
AG
Established Service Level Connection
Internal event: Registration Status changes
The HF refreshes its registration status indication
+CIEV: ...
The AG reports the change in the Registration Status

Figure 4.3: Typical Registration Status update

4.5 Transfer of Signal Strength Indication

This procedure enables the AG to send to HF unsolicited result codes with the signal strength values.

The following pre-condition applies for this procedure:

- An ongoing connection between the AG and the HF shall exist. If this connection does not exist, the AG shall establish a connection using "Service Level Connection set up" procedure described in section 4.2.

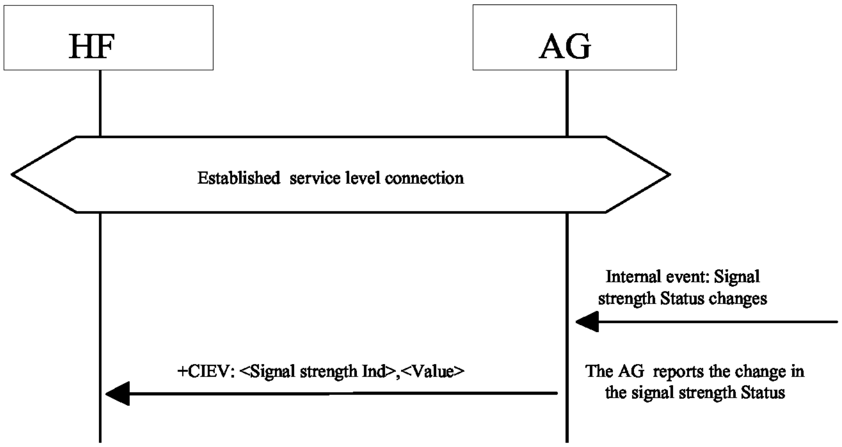

HF
AG
Established service level connection
Internal event: Signal strength Status changes
+CIEV: <Signal strength Ind>,<Value>
The AG reports the change in the signal strength Status

Figure 4.4: Transfer of Signal strength indication

- As a result, the AG shall send the +CIEV unsolicited result code with the corresponding signal strength value whenever its signal strength changes.

4.6 Transfer of Roaming Status Indication

This procedure enables the HF to know the "Roaming Status" of the AG.

The AT+CMER command, as described in Section 4.24.2, enables the "Roaming status Indication" in the AG. As a result, the AG shall send the +CIEV unsolicited result code with the corresponding indicator values whenever its roaming status changes.

As pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the HF shall establish the Service Level Connection using the proper procedure as described in Section 4.2.

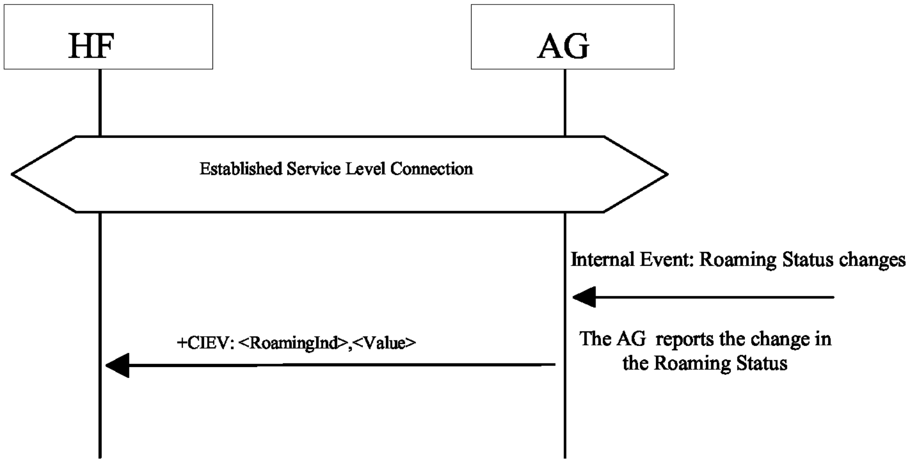

HF
AG
Established Service Level Connection
Internal Event: Roaming Status changes
+CIEV: <RoamingInd>,<Value>
The AG reports the change in the Roaming Status

Figure 4.5: Transfer of Roaming Status Indication

4.7 Transfer of Battery Level Indication of AG

This procedure allows the HF to know the battery level of the AG.

The AT+CMER command, as described in Section 4.24.2, enables the “Battery level update” in the AG. As a result, the AG shall send the +CIEV unsolicited result code with the corresponding battery level values whenever its level changes.

The following pre-condition applies for this procedure:

- An ongoing connection between the AG and the HF shall exist. If this connection does not exist, the AG shall establish a connection using “Service Level Connection set up” procedure described in Section 4.2.

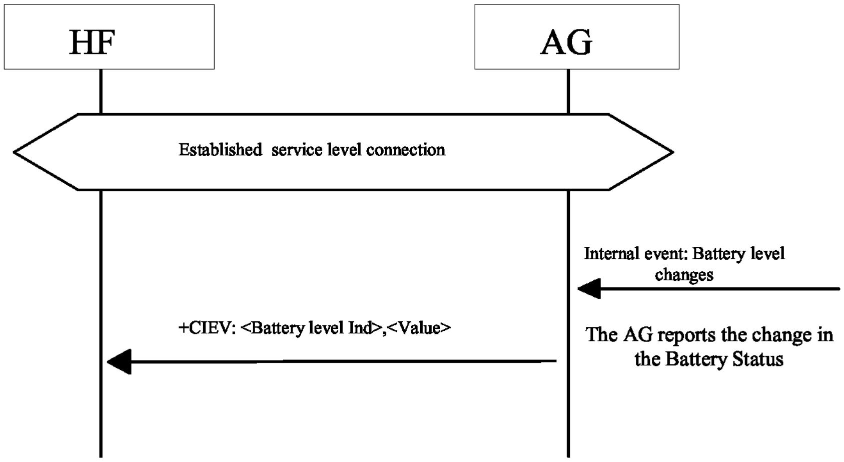

HF
AG
Established service level connection
Internal event: Battery level changes
+CIEV: <Battery level Ind>,<Value>
The AG reports the change in the Battery Status

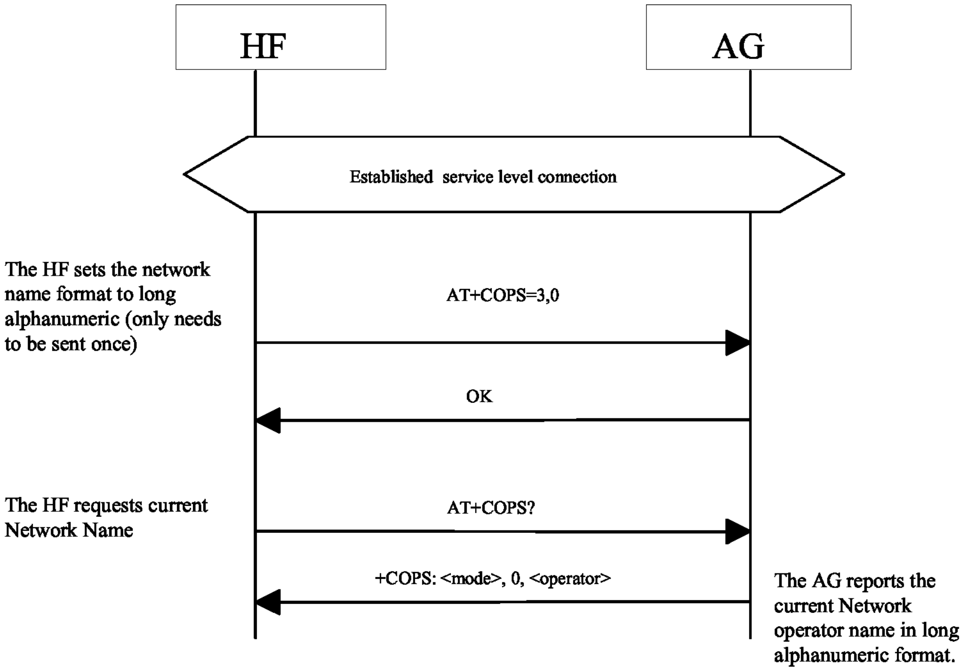
Figure 4.6: Transfer of Battery level indication

4.8 Query Operator Selection

The HF shall execute this procedure to find out the name of the currently selected Network operator by AG.

The following pre-condition applies for this procedure:

- An ongoing connection between the AG and the HF shall exist. If this connection did not exist, the AG shall establish a connection using “Service Level Connection set up” procedure described in Section 4.2.


HF
AG
Established service level connection
AT+COPS=3,0
OK
AT+COPS?
+COPS: <mode>, 0, <operator>

The HF sets the network name format to long alphanumeric (only needs to be sent once)

The HF requests current Network Name

The AG reports the current Network operator name in long alphanumeric format.

Figure 4.7: Query currently selected Network operator

- HF shall send AT+COPS=3,0 command to set name format to long alphanumeric. Long alphanumeric is defined as a maximum of 16 characters. The value of 3 as the first parameter indicates that this command is only affecting the format parameter (the second parameter). The second parameter, 0, is the value required to set the format to "long alphanumeric."
- Upon an internal event or user-initiated action, HF shall send the AT+COPS? (Read) command to find the currently selected operator.
- AG shall respond with +COPS response indicating the currently selected operator. If no operator is selected, <format> and <operator> are omitted.

4.9 Report Extended Audio Gateway Error Results Code

The HF shall execute this procedure to enable/disable Extended Audio Gateway Error result codes in the AG.

The following pre-condition applies for this procedure:

- An ongoing connection between the AG and the HF shall exist. If this connection did not exist, the AG shall establish a connection using "Service Level Connection set up" procedure described in section 4.2.

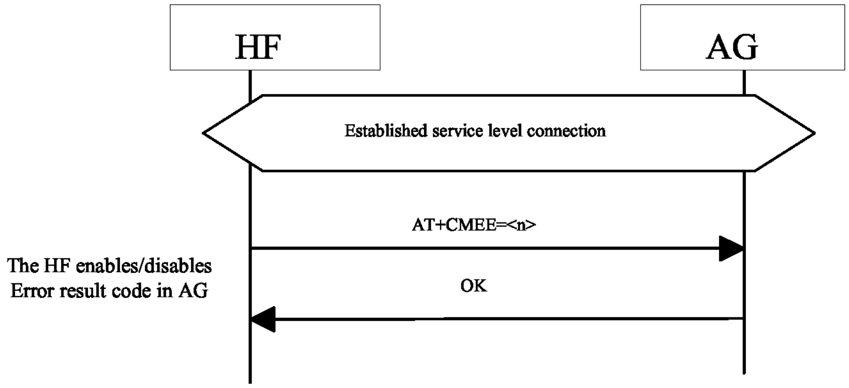

HF
AG
Established service level connection
AT+CMEE=<n>
The HF enables/disables Error result code in AG
OK

Figure 4.8: Enable/Disable AG Error result code

- The HF shall issue the AT+CMEE command to enable/disable the “Extended Audio Gateway Error Result Code” in the AG. The parameter <n> controls the activation/deactivation of the “Extended Error result code” notification.
- Whenever there is an error relating to the functionality of the AG as a result of AT command, the AG shall send +CME ERROR: <err> response to the HF.

4.10 Transfer of Call, Call Setup and Held Call Status

The AT+CMER command, as described in Section 4.2, enables the “Call Status indicators update” function in the AG. When this function is enabled, the AG shall issue a +CIEV unsolicited result code with the corresponding call indicator and value whenever the AG's current call status changes. Likewise, the AG shall issue a +CIEV unsolicited result code with the corresponding callsetup indicator and value whenever the AG's current call setup status changes. The AG shall also issue a +CIEV unsolicited result code with corresponding callheld indicator and value whenever the AG’s current held call status changes.

The HF unit shall be capable of interpreting the information provided by the +CIEV result code to determine the call status as listed in Section 4.33.2.

Furthermore, the HF unit may also be capable of interpreting the optional callsetup state information provided by the +CIEV result code as listed in Section 4.33.2.

The HF unit shall be able to accept unknown indicators provided by the +CIEV result code. The HF unit may ignore unknown indicators provided by the +CIEV result code.

Note: Although the HF unit is required to parse the +CIEV result codes, the HF unit is not required to provide User Interface indicators for the +CIEV result codes.

4.11 Audio Connection Setup

Upon a user action or an internal event, either the HF or the AG shall initiate the establishment of an Audio Connection whenever necessary. Further internal actions may be needed by the HF or the AG to internally route the audio paths.

An Audio Connection set up procedure always means the establishment of a Synchronous Connection and it is always associated with an existing Service Level Connection.

In principle, setting up an Audio Connection by using the procedure described in this section is not necessarily related to any call process.

Once an Audio Connection between the HF and the AG exists, the AG shall utilize the HF as its primary audio port. The AG shall keep the audio paths, call related or not, routed towards HF for all the operations (e.g. voice, alert, key press tones) involving presence of audio.

As pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the initiator of the procedure shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.

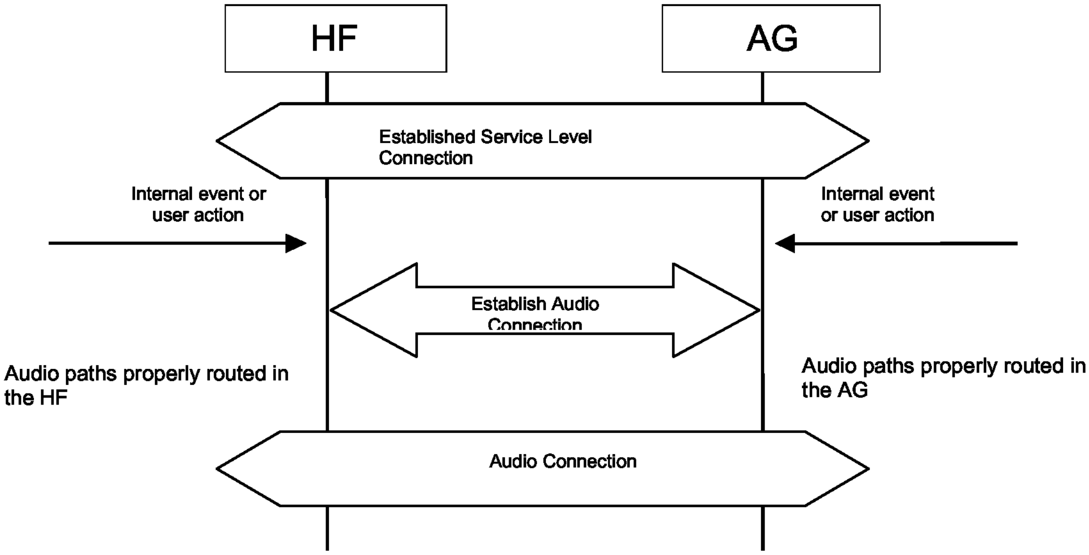

HF
AG
Established Service Level Connection
Internal event or user action
Internal event or user action
Establish Audio Connection
Audio paths properly routed in the HF
Audio paths properly routed in the AG
Audio Connection

Figure 4.9: Audio Connection set up

Both the initiator and the acceptor shall notify the presence of the new Audio Connection.

4.12 Audio Connection Release

Upon a user action or an internal event, either the HF or the AG shall release an existing Audio Connection whenever necessary.

As pre-condition for this procedure, an ongoing Audio Connection between the AG and the HF shall exist.

An Audio Connection removal always means the disconnection of its corresponding Synchronous Connection.

When the audio connection is released, the audio path shall be routed to the AG.[2]

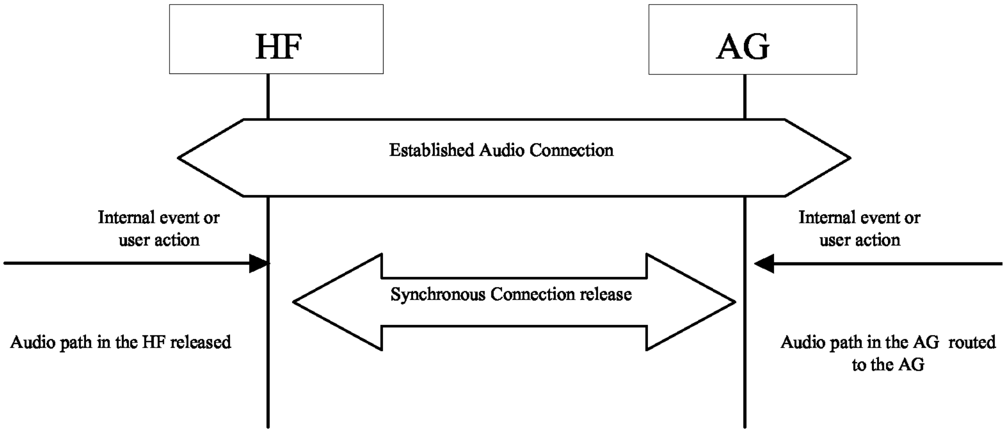

HF
AG
Established Audio Connection
Internal event or user action
Internal event or user action
Synchronous Connection release
Audio path in the HF released
Audio path in the AG routed to the AG

Figure 4.10: Audio Connection release

4.13 Answer an Incoming Call

Upon an incoming call, the AG shall send a sequence of unsolicited RING alerts to the HF. The RING alert shall be repeated for as long as the call acceptance is pending, or until the incoming call is interrupted for any reason.

The HF shall produce a local alerting in reaction to the RING.

If the AG's SDP record (or +BRSF message) indicates "In-band ring tone" is supported, the AG shall send in-band ring tones unless subsequently changed using procedures defined in Section 4.13.4.

The AG may abort the incoming call when necessary. It shall then stop sending the RING alert to the HF.

4.13.1 Answer Incoming Call from the HF – In-Band Ringing

Optionally, the AG may provide an in-band ring tone.

This case is described in Figure 4.11 below and implies, as pre-condition, that an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the AG shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.

As the figure below shows, if an in-band ring tone is used, the AG shall send the ring tone to the HF via the established Audio Connection.

[2] In principle, removing an Audio Connection by using the procedure described in this section is not necessarily related to any call process.

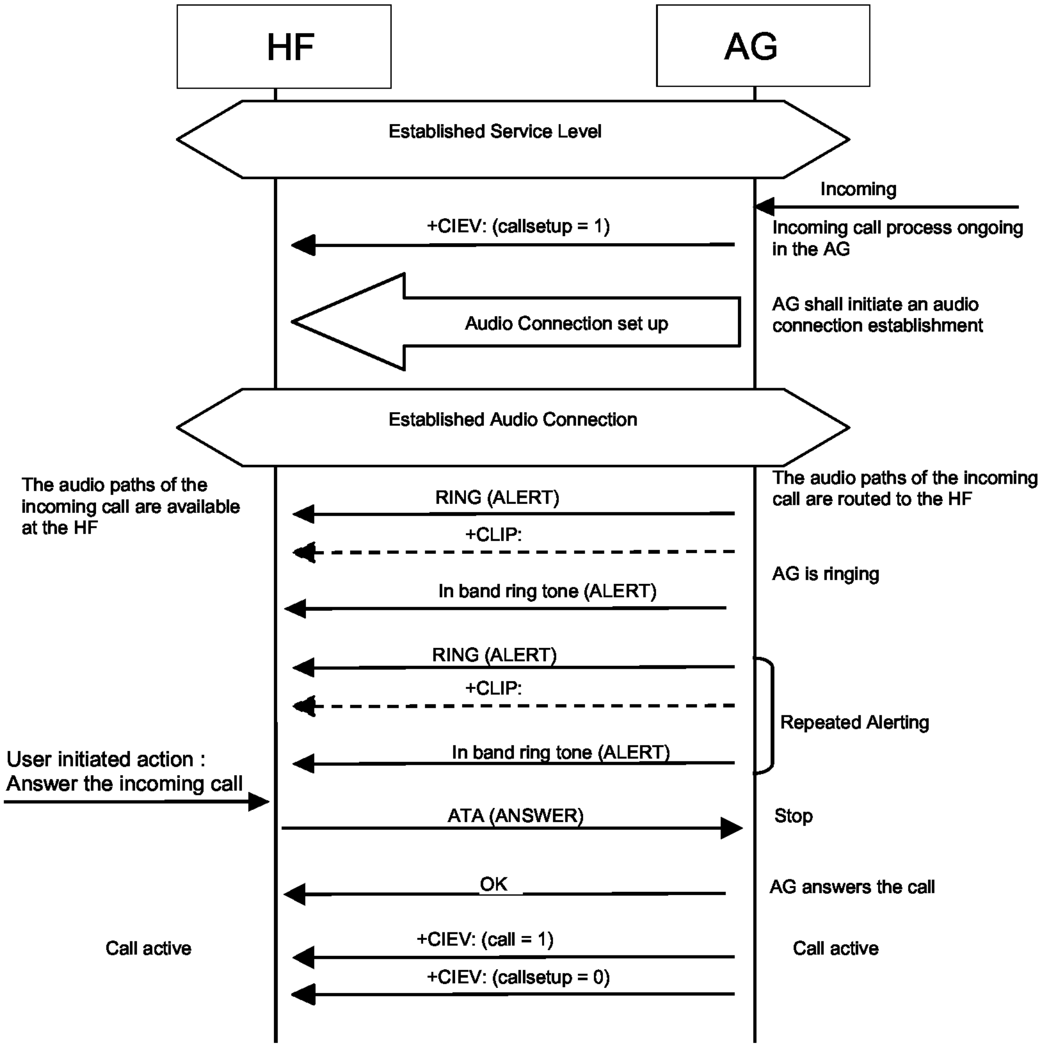

HF
AG
Established Service Level
Incoming
+CIEV: (callsetup = 1)
Incoming call process ongoing in the AG
Audio Connection set up
AG shall initiate an audio connection establishment
Established Audio Connection
The audio paths of the incoming call are available at the HF
RING (ALERT)
The audio paths of the incoming call are routed to the HF
+CLIP:
AG is ringing
In band ring tone (ALERT)
RING (ALERT)
+CLIP:
Repeated Alerting
User initiated action : Answer the incoming call
In band ring tone (ALERT)
ATA (ANSWER)
Stop
OK
AG answers the call
Call active
+CIEV: (call = 1)
Call active
+CIEV: (callsetup = 0)

Figure 4.11: Answer an incoming call from the HF – in-band ring tone

The user accepts the incoming voice call by using the proper means provided by the HF. The HF shall then send the ATA command (see Section 4.33) to the AG. The AG shall then begin the procedure for accepting the incoming call.

If the normal incoming call procedure is interrupted for any reason, the AG shall issue the +CIEV result code, with the value indicating (callsetup=0) to notify the HF of this condition (see also Section 4.14.2).

4.13.2 Answer Incoming Call from the HF – No In-Band Ringing

As pre-condition, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the AG shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.

As the figure below shows, if no in-band ring tone is used and an Audio Connection does not exist, the AG shall set up the Audio Connection and route the audio paths to the HF upon answering the call.

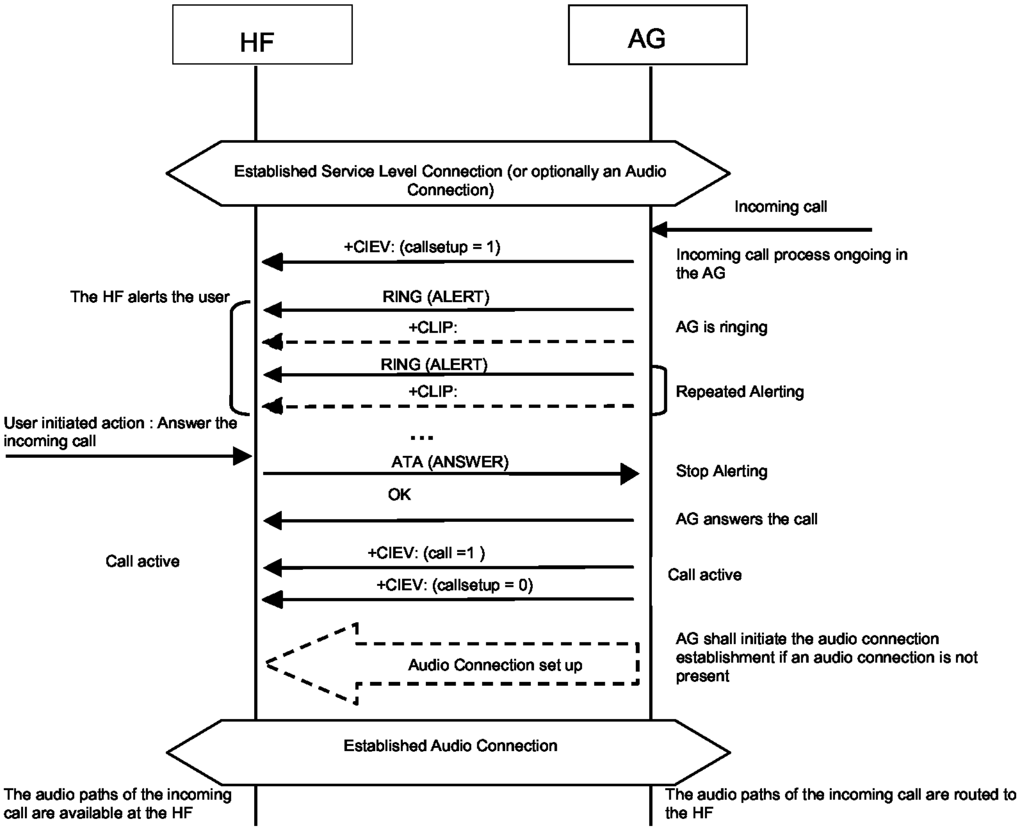

HF
AG
Established Service Level Connection (or optionally an Audio Connection)
Incoming call
+CIEV: (callsetup = 1)
Incoming call process ongoing in the AG
The HF alerts the user
RING (ALERT)
+CLIP:
AG is ringing
RING (ALERT)
+CLIP:
Repeated Alerting
User initiated action : Answer the incoming call
...
ATA (ANSWER)
Stop Alerting
OK
AG answers the call
Call active
+CIEV: (call =1)
+CIEV: (callsetup = 0)
Call active
Audio Connection set up
AG shall initiate the audio connection establishment if an audio connection is not present
Established Audio Connection
The audio paths of the incoming call are available at the HF
The audio paths of the incoming call are routed to the HF

Figure 4.12: Answer an incoming call from the HF – no in-band ring tone

The user accepts the incoming voice call by using the proper means provided by the HF. The HF shall then send the ATA command (see Section 4.33) to the AG, and the AG shall start the procedure for accepting the incoming call and establishing the Audio Connection if an Audio Connection does not exist (refer to Section 4.11).

If the normal incoming call procedure is interrupted for any reason, the AG shall issue the +CIEV result code, with the value indicating (callsetup=0) to notify the HF of this condition (see also Section 4.14.2).

4.13.3 Answer Incoming Call from the AG

The following pre-conditions apply for this procedure:

- As a pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist.
- The AG shall alert the HF using either of the two procedures described in Sections 4.13.1 and 4.13.2.
- The HF shall alert the user.

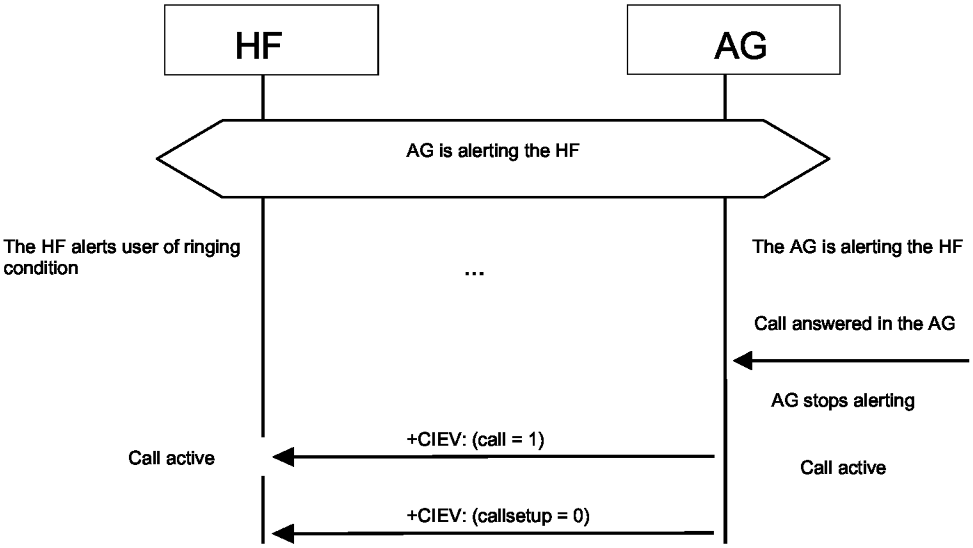


Figure 4.13: Answer an incoming call from the AG

The user accepts the incoming call by using the proper means provided by the AG.

If the normal incoming call procedure is interrupted for any reason, the AG shall issue the +CIEV result code, with the value indicating (callsetup=0) to notify the HF of this condition (see also Section 4.14.2).

4.13.4 Change the In-Band Ring Tone Setting

The SDP record entry “In-band ring tone” of the “Supported features” record (see table 5.4) informs the HF if the AG is capable of sending an in-band ring tone or not. If the AG is capable of sending an in-band ring tone, it shall send the in-band ring tone by default. The AG may subsequently change this setting.

In case the AG wants to change the in-band ring tone setting during an ongoing service level connection, it shall use the unsolicited result code +BSIR (Bluetooth Set In-band Ring tone) to notify the HF about the change. See Figure 4.14 for details.

Refer to Section 4.33 for more information on the +BSIR unsolicited result code.

The in-band ring tone setting may be changed several times during a Service Level Connection.

As pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the AG shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.

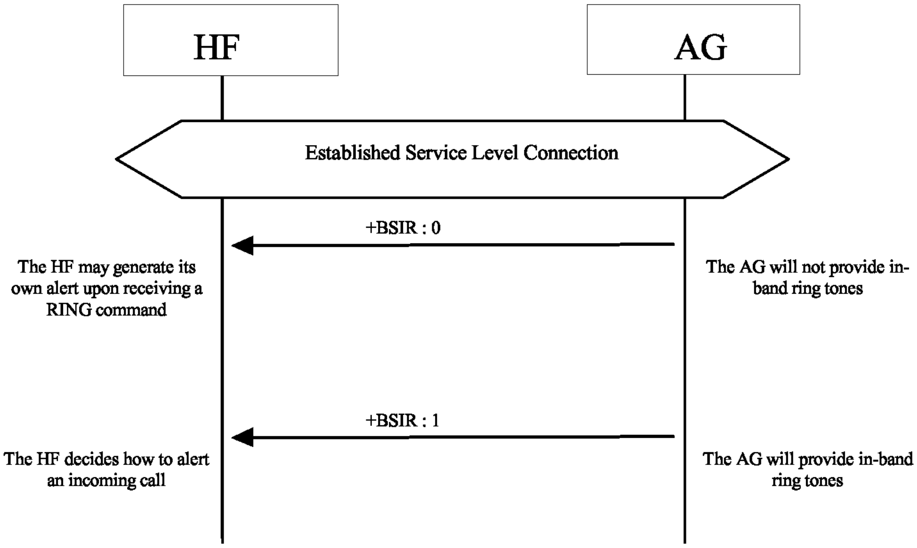

HF
AG
Established Service Level Connection
+BSIR : 0
The HF may generate its own alert upon receiving a RING command
The AG will not provide in-band ring tones
+BSIR : 1
The HF decides how to alert an incoming call
The AG will provide in-band ring tones

Figure 4.14: Change of the in-band ring tone setting initiated by the AG

In case the HF does not want to use the AG's in-band ring tone, it may mute the Audio Connection after it has received +CIEV:(callsetup=1). The HF shall un-mute the Audio Connection upon receiving the +CIEV:(callsetup=0) indication.

4.14 Reject an Incoming Call

In case of an incoming call, the AG shall alert the HF by either one of the two procedures described in Sections 4.13.1 and 4.13.2.

Instead of answering the call, the user may reject the incoming call process by user action at the HF or the AG. These two procedures are described in the following sections.

4.14.1 Reject an Incoming Call from the HF

As a precondition to this procedure, the AG shall alert the HF using either of the two procedures described in Sections 4.13.1 and 4.13.2.

The user rejects the incoming call by using the User Interface on the Hands-Free unit. The HF shall then send the AT+CHUP command (see Section 4.33) to the AG. This may happen at any time during the procedures described in Sections 4.13.1 and 4.13.2.

The AG shall then cease alerting the HF of the incoming call and send the OK indication followed by the +CIEV result code, with the value indicating (callsetup=0).

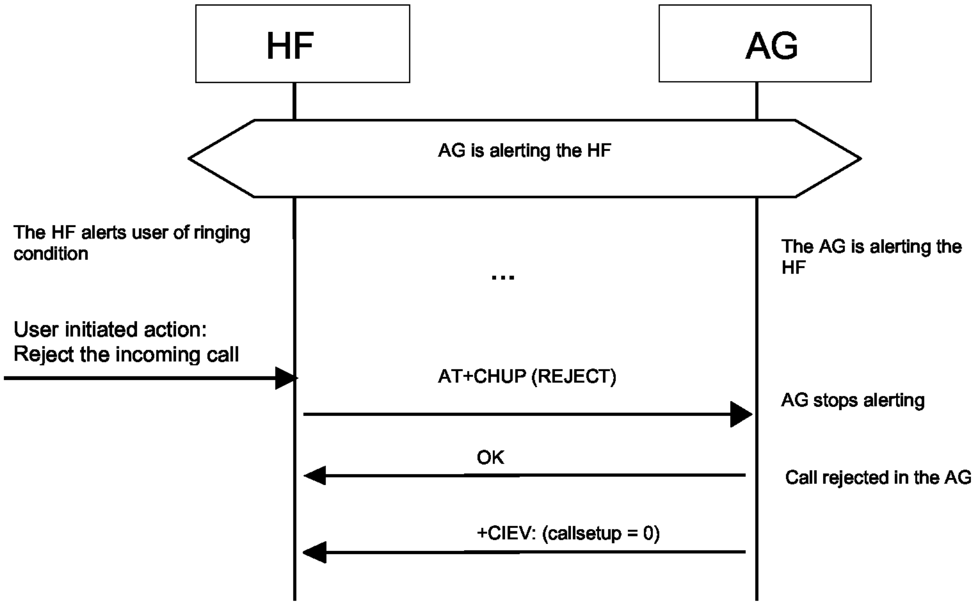

HF
AG
AG is alerting the HF
The HF alerts user of ringing condition
...
The AG is alerting the HF
User initiated action: Reject the incoming call
AT+CHUP (REJECT)
AG stops alerting
OK
Call rejected in the AG
+CIEV: (callsetup = 0)

Figure 4.15: Reject an incoming call from the HF

4.14.2 Rejection/Interruption of an Incoming Call in the AG

As a precondition to this procedure, the AG shall alert the HF using either of the two procedures described in Sections 4.13.1 and 4.13.2.

The user rejects the incoming call by using the User Interface on the AG. Alternatively the incoming call process may be interrupted in the AG for any other reason.

As consequence of this, the AG shall send the +CIEV result code, with the value indicating (callsetup=0). The HF shall then stop alerting the user.

This may happen at any time during the procedures described in Sections 4.13.1 and 4.13.2.

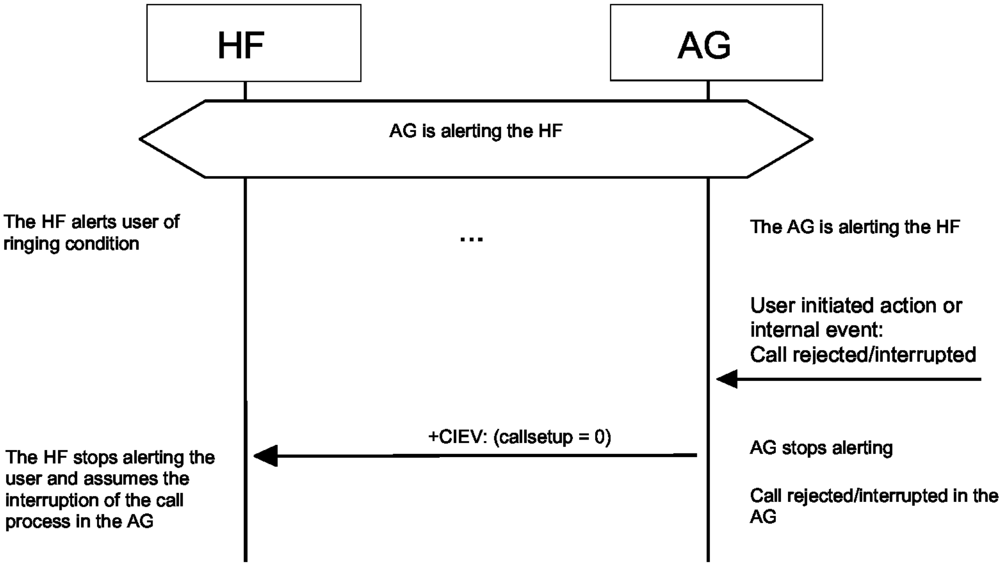

HF
AG
AG is alerting the HF
The HF alerts user of ringing condition
...
The AG is alerting the HF
User initiated action or internal event: Call rejected/interrupted
+CIEV: (callsetup = 0)
AG stops alerting
The HF stops alerting the user and assumes the interruption of the call process in the AG
Call rejected/interrupted in the AG

Figure 4.16: Rejection/interruption of an incoming call in the AG

4.15 Terminate a Call Process

An ongoing call process may be terminated by either the HF or the AG by means of a user action or any other event.

4.15.1 Terminate a Call Process from the HF

The following pre-conditions apply for this procedure:

- An ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the HF shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.
- A call related process is ongoing in the AG.

Although not required for the call termination process, an Audio Connection is typically present between the HF and AG.

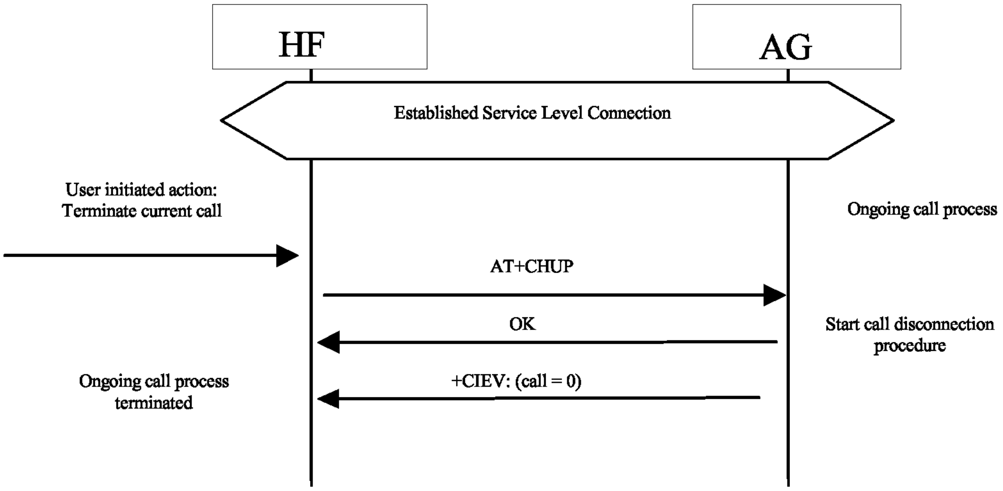


Figure 4.17: Terminate ongoing call - HF initiated

The user may abort the ongoing call process using whatever means provided by the Hands-Free unit. The HF shall send AT+CHUP command (see Section 4.33) to the AG, and the AG shall then start the procedure to terminate or interrupt the current call procedure. The AG shall then send the OK indication followed by the +CIEV result code, with the value indicating (call=0).

Performing a similar procedure, the AT+CHUP command described above may also be used for interrupting a normal outgoing call set-up process.

4.15.2 Terminate a Call Process from the AG

The following pre-conditions apply for this procedure:

- An ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the AG shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.
- A call related process is ongoing in the AG.

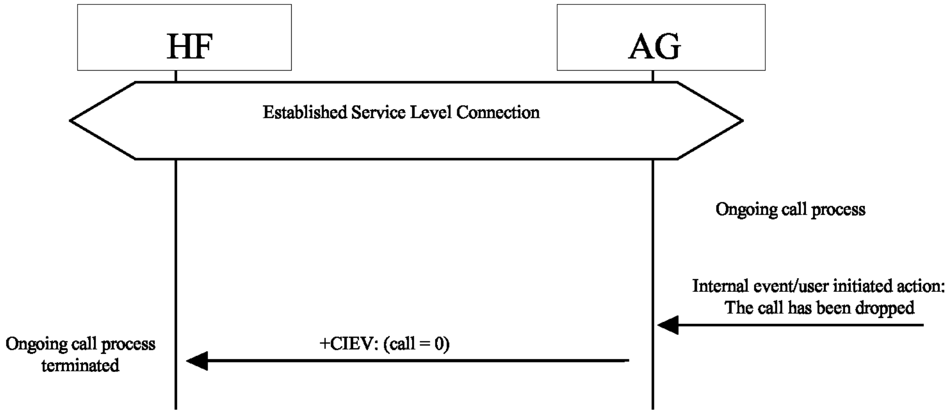

HF
AG
Established Service Level Connection
Ongoing call process
Internal event/user initiated action:
The call has been dropped
Ongoing call process
terminated
+CIEV: (call = 0)

Figure 4.18: Terminate ongoing call - AG initiated

This procedure is fully applicable for cases in which an ongoing call process is interrupted in the AG for any reason.

In this case the AG shall send the +CIEV result code, with the value indicating (call=0).

4.16 Audio Connection Transfer Towards the HF

The audio paths of an ongoing call may be transferred from the AG to the HF. This procedure represents a particular case of an “Audio Connection set up” procedure, as described in Section 4.11.

The call connection transfer from the AG to the HF is initiated by a user action either on the HF or on the AG side. This shall result in either the HF or the AG, respectively, initiating an “Audio Connection set up” procedure with the audio paths of the current call being routed to the HF.

This procedure is only applicable if there is no current Audio Connection established between the HF and the AG. In fact, if the Audio Connection already exists, this procedure is not necessary because the audio path of the AG is assumed to be already routed towards the HF.

The following pre-conditions apply for this procedure:

- An ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the initiator of the “Audio Connection transfer towards the HF” procedure shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.
- An ongoing call exists in the AG, with the audio paths routed to the AG means.

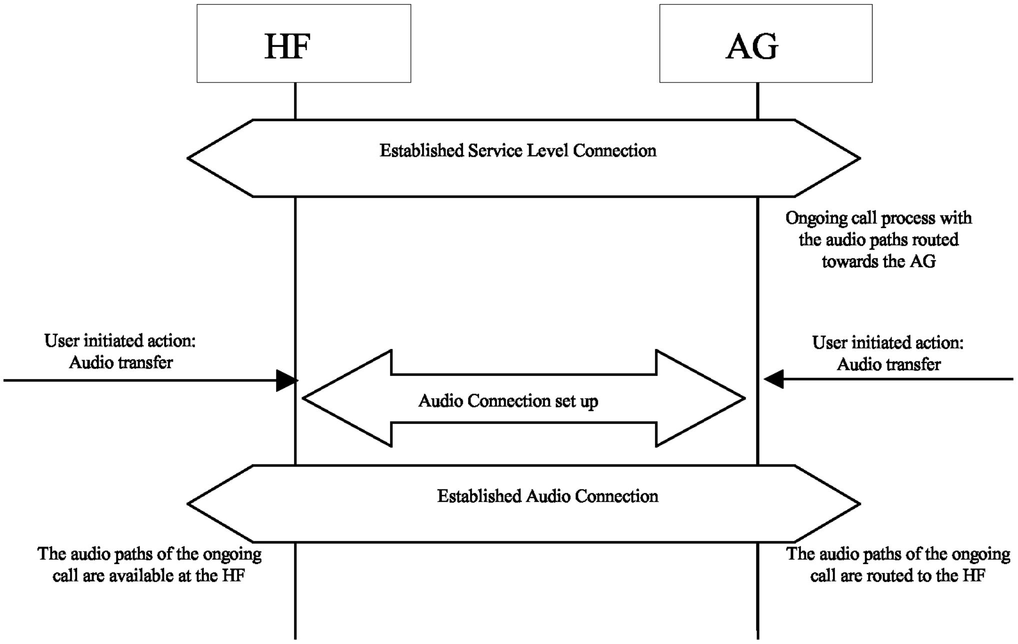

HF
AG
Established Service Level Connection
Ongoing call process with the audio paths routed towards the AG
User initiated action: Audio transfer
User initiated action: Audio transfer
Audio Connection set up
Established Audio Connection
The audio paths of the ongoing call are available at the HF
The audio paths of the ongoing call are routed to the HF

Figure 4.19: Audio Connection transfer to the HF

4.17 Audio Connection Transfer Towards the AG

The audio paths of an ongoing call may be transferred from the HF to the AG. This procedure represents a particular case of an “Audio Connection release” procedure, as described in Section 4.12.

The call connection transfer from the HF to the AG is initiated by a user action in the HF or due to an internal event or user action on the AG side. This results in an “Audio Connection release” procedure being initiated either by the HF or the AG respectively, with the current call kept and its audio paths routed to the AG.

If as a consequence of an HF initiated “Audio Connection transfer towards the AG” procedure, the existing Service Level Connection is autonomously removed by the AG, the AG shall attempt to re-establish the Service Level Connection once the current call ends.

As pre-condition for this procedure, an ongoing call process shall exist in the AG. The audio paths of the ongoing call shall be available in the HF via an Audio Connection established between the AG and the HF.

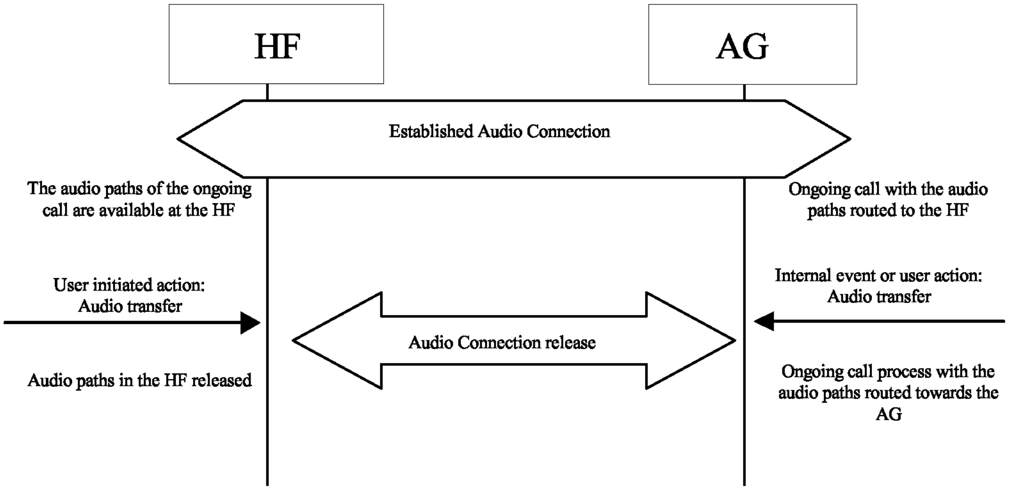

HF
AG
Established Audio Connection
The audio paths of the ongoing call are available at the HF
Ongoing call with the audio paths routed to the HF
User initiated action: Audio transfer
Internal event or user action: Audio transfer
Audio Connection release
Audio paths in the HF released
Ongoing call process with the audio paths routed towards the AG

Figure 4.20: Audio Connection transfer to the AG

4.18 Place a Call With the Phone Number Supplied by the HF

The HF may initiate outgoing voice calls by providing the destination phone number to the AG. To start the call set-up, the HF shall initiate the Service Level Connection establishment (if necessary) and send a proper ATDdd…dd; command to the AG. The AG shall then start the call establishment procedure using the phone number received from the HF and issues the +CIEV result code, with the value (callsetup=2) to notify the HF that the call set-up has been successfully initiated.

Refer to Section 4.33 for more information on the ATDdd…dd; command.

As pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the HF shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.

If an Audio Connection is not established the AG shall establish the proper Audio Connection and route the audio paths of the outgoing call to the HF immediately following the commencement of the ongoing call set up procedure.

Once the AG is informed that the alerting of the remote party has begun, the AG shall issue the +CIEV result code, with the value indicating (callsetup=3). If the wireless network does not provide the AG of an indication of alerting the remote party, the AG may not send this indication.

Upon call connection the AG shall send issue the +CIEV result code, with the value indicating (call=1).

If the normal outgoing call establishment procedure is interrupted for any reason, the AG shall issue the +CIEV result code, with the value indicating (callsetup=0), to notify the HF of this condition (see Section 4.15.2).

If the AG supports the “Three-way calling” feature and if a call is already ongoing in the AG, performing this procedure shall result in a new call being placed to a third party with the current ongoing call put on hold. For details on how to handle multiparty calls refer to Section 4.22.2.

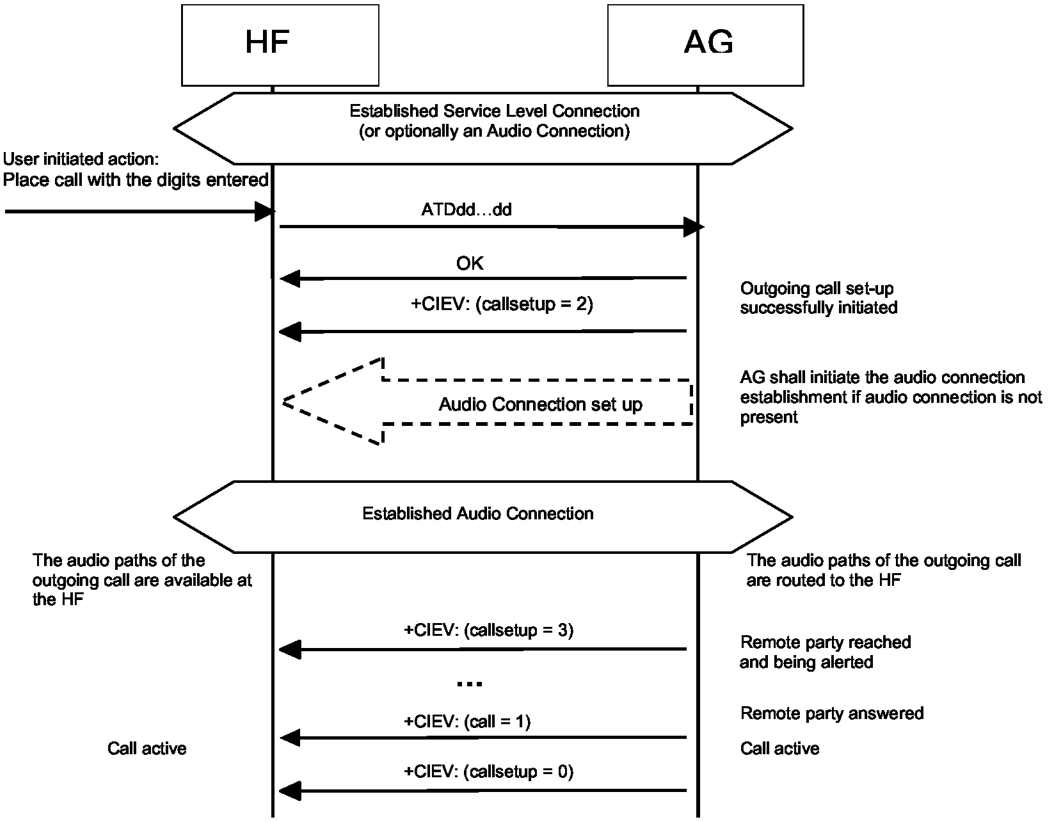

HF
AG
Established Service Level Connection
(or optionally an Audio Connection)
User initiated action:
Place call with the digits entered
ATDdd…dd
OK
+CIEV: (callsetup = 2)
Outgoing call set-up successfully initiated
Audio Connection set up
AG shall initiate the audio connection establishment if audio connection is not present
Established Audio Connection
The audio paths of the outgoing call are available at the HF
The audio paths of the outgoing call are routed to the HF
+CIEV: (callsetup = 3)
Remote party reached and being alerted
…
+CIEV: (call = 1)
Remote party answered
Call active
Call active
+CIEV: (callsetup = 0)

Figure 4.21: Place an outgoing voice call with the digits entered in the HF

4.19 Memory Dialing from the HF

The HF may initiate outgoing voice calls using the memory dialing feature of the AG. To start the call set-up, the HF shall initiate the Service Level Connection establishment (if necessary) and send an ATD>nnn…; command to the AG. The AG shall then start the call establishment procedure using the phone number stored in the AG memory location given by nnn…; and issue the +CIEV result code, with the value (callsetup=2) to notify the HF that the call set-up has been successfully initiated.

Refer to Section 4.33 for more information on the ATD>nnn… command.

As pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the HF shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.

If an Audio Connection is not established, the AG shall establish the proper Audio Connection and route the audio paths of the outgoing call to the HF immediately following the commencement of the ongoing call set up procedure.

Once alerting of the remote party begins, the AG shall issue the +CIEV result code, with the value indicating (callsetup=3).

Upon call connection the AG shall send issue the +CIEV result code, with the value indicating (call=1).

If the normal outgoing call establishment procedure is interrupted for any reason, the AG shall issue the +CIEV result code, with the value indicating (callsetup=0), to notify the HF of this condition (see Section 4.15.2).

If the AG supports the "Three-way calling" feature and if a call is already ongoing in the AG, performing this procedure shall result in a new call being placed to a third party with the current ongoing call put on hold. For details on how to handle multiparty calls refer to Section 4.22.2.

If there is no number stored for the memory location given by the HF, the AG shall respond with ERROR.

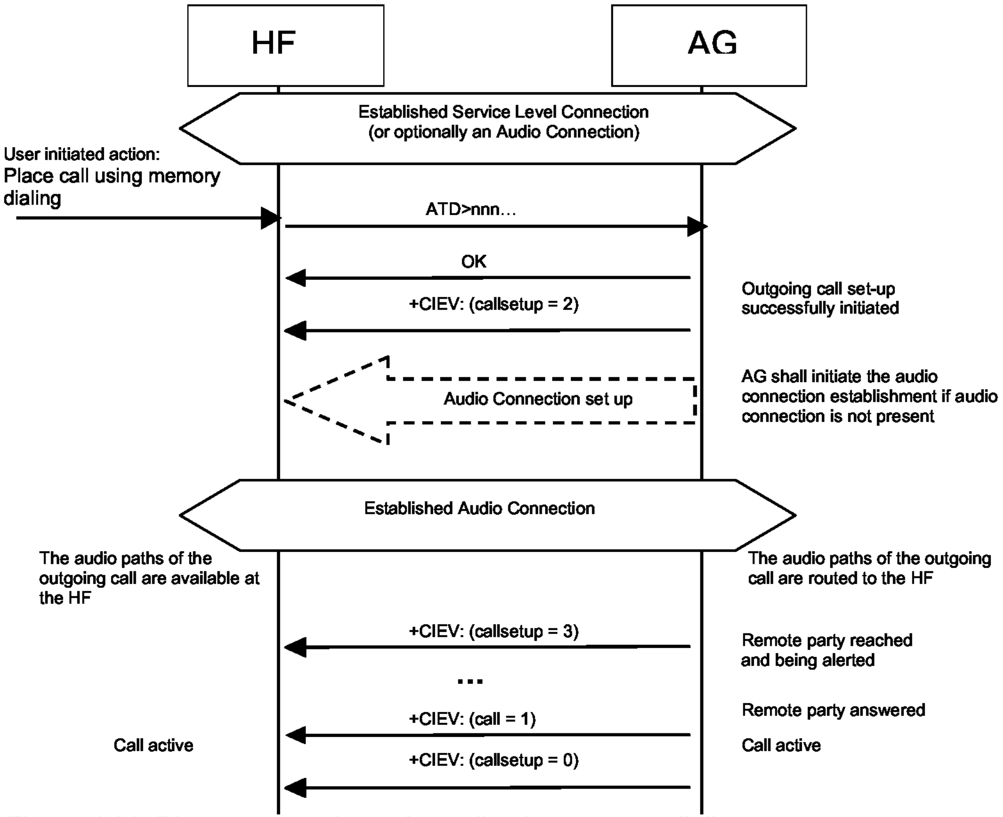

HF
AG
Established Service Level Connection
(or optionally an Audio Connection)
User initiated action:
Place call using memory dialing
ATD>nnn...
OK
+CIEV: (callsetup = 2)
Outgoing call set-up successfully initiated
Audio Connection set up
AG shall initiate the audio connection establishment if audio connection is not present
Established Audio Connection
The audio paths of the outgoing call are available at the HF
The audio paths of the outgoing call are routed to the HF
+CIEV: (callsetup = 3)
Remote party reached and being alerted
...
Remote party answered
+CIEV: (call = 1)
Call active
Call active
+CIEV: (callsetup = 0)

Figure 4.22: Place an outgoing voice call using memory dialing

4.20 Last Number Re-Dial from the HF

The HF may initiate outgoing voice calls by recalling the last number dialed by the AG. To start the call set-up, the HF shall initiate the Service Level Connection establishment (if necessary) and send an AT+BLDN command to the AG. The AG shall then start the call establishment procedure using the last phone number dialed by the AG, and issues the +CIEV result code, with the value (callsetup=2), to notify the HF that the call set-up has been successfully initiated.

Refer to Section 4.33 for more information on the AT+BLDN command.

As pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the HF shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.

If an Audio Connection is not established, the AG shall establish the proper Audio Connection and route the audio paths of the outgoing call to the HF immediately following the commencement of the ongoing call set up procedure.

Once alerting of the remote party begins, the AG shall issue the +CIEV result code, with the value indicating (callsetup=3).

Upon call connection the AG shall send issue the +CIEV result code, with the value indicating (call=1).

If the normal outgoing call establishment procedure is interrupted for any reason, the AG shall issue the +CIEV result code, with the value indicating (callsetup=0), to notify the HF of this condition (see Section 4.15.2).

If the AG supports the "Three-way calling" feature and if a call is already ongoing in the AG, performing this procedure shall result in a new call being placed to a third party with the current ongoing call put on hold. For details on how to handle multiparty calls refer to Section 4.22.2.

If there is no number stored for the memory location given by the HF, the AG shall respond with ERROR.

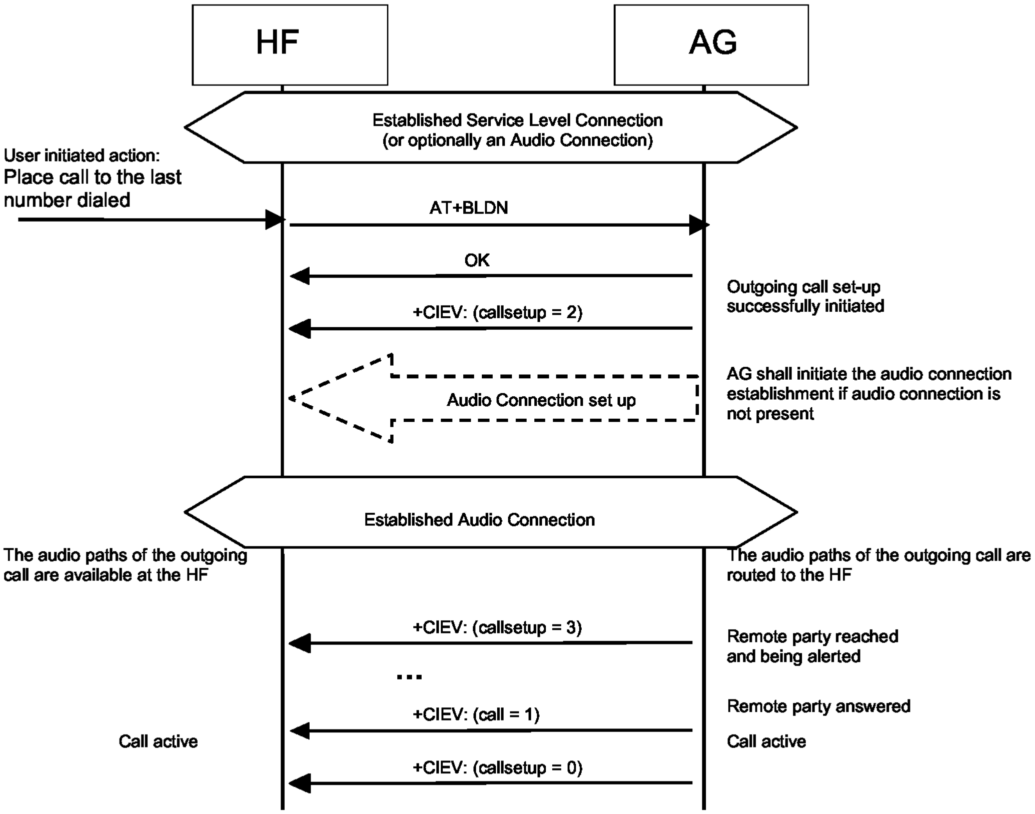

HF
AG
Established Service Level Connection
(or optionally an Audio Connection)
User initiated action:
Place call to the last number dialed
AT+BLDN
OK
+CIEV: (callsetup = 2)
Outgoing call set-up successfully initiated
Audio Connection set up
AG shall initiate the audio connection establishment if audio connection is not present
Established Audio Connection
The audio paths of the outgoing call are available at the HF
The audio paths of the outgoing call are routed to the HF
+CIEV: (callsetup = 3)
Remote party reached and being alerted
...
+CIEV: (call = 1)
Remote party answered
Call active
Call active
+CIEV: (callsetup = 0)

Figure 4.23: Place an outgoing voice call with the last number dialed

4.21 Call Waiting Notification Activation

The HF may issue the AT+CCWA command to enable the “Call Waiting notification” function in the AG. Once the “Call Waiting notification” is enabled, the AG shall send the corresponding +CCWA unsolicited result code to the HF whenever an incoming call is waiting during an ongoing call. It is always assumed that the “call waiting” service is already active in the network.

Once the HF issues the AT+CCWA command, the AG shall respond with OK. It shall then keep the “Call Waiting notification” enabled until either the AT+CCWA command is issued to disable “Call Waiting notification,” or the current Service Level Connection between the AG and the HF is dropped for any reason.

Refer to Section 4.33 for more information on the AT+CCWA command.

As pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the HF shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.

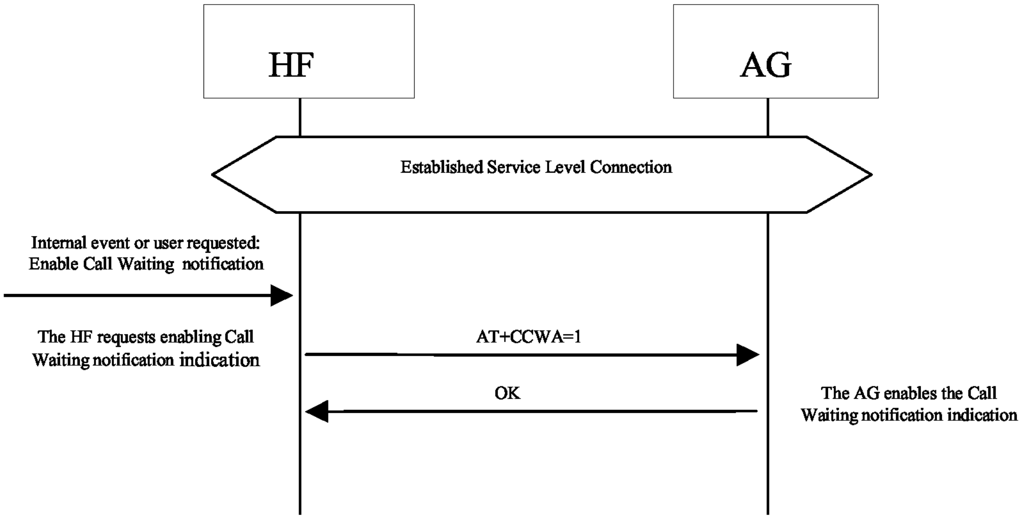

HF
AG
Established Service Level Connection
Internal event or user requested: Enable Call Waiting notification
The HF requests enabling Call Waiting notification indication
AT+CCWA=1
OK
The AG enables the Call Waiting notification indication

Figure 4.24: Activation of Call waiting notification

4.22 Three Way Call Handling

Proper management of several concurrent calls shall be accomplished by performing the procedures described in [2] but with some limitations stated in this specification. For more details, refer to Section 4.33.

The HF device cannot always assume that the "call hold and/or multiparty" services are available in the network. If the AG determines that a requested action by the HF device cannot be performed due to the inability of the network to support that feature or lack of subscriber subscription, the AG shall return a +CME error.

There are two +CME ERROR codes that are used to indicate network related failure reasons to the HF :

30 - No Network Service. Indicates that an AT+CHLD command cannot be implemented due to network limitations.

31 - Network Timeout. Indicates that an AT+CHLD command cannot be implemented due to network problems.

In general, when the user deals with multiple concurrent calls, the HF shall issue the corresponding AT+CHLD command as a result of user actions. This command allows the control of multiple concurrent calls and provides means for holding calls, releasing calls, switching between two calls, and adding a call to a multiparty conference.

When this feature is supported, the HF and AG are only mandated to implement the “basic Three Way calling” commands AT+CHLD = 1 and 2.

This section covers two cases. In one case the third party call is received in the AG, and notification is sent to the HF via a Call Waiting notification. In the second case, the third party call is placed from the HF.

Refer to Section 4.33 for more information on the AT+CHLD command.

The following pre-conditions apply for these procedures:

- As pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the initiator of the procedure shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.
- An ongoing call in the AG shall exist.

4.22.1 Three Way Calling—Call Waiting Notification

In addition to the two previously stated preconditions, the Call Waiting notification to the HF shall already be enabled in the AG (that is, the procedure stated in Section 4.21 has been performed).

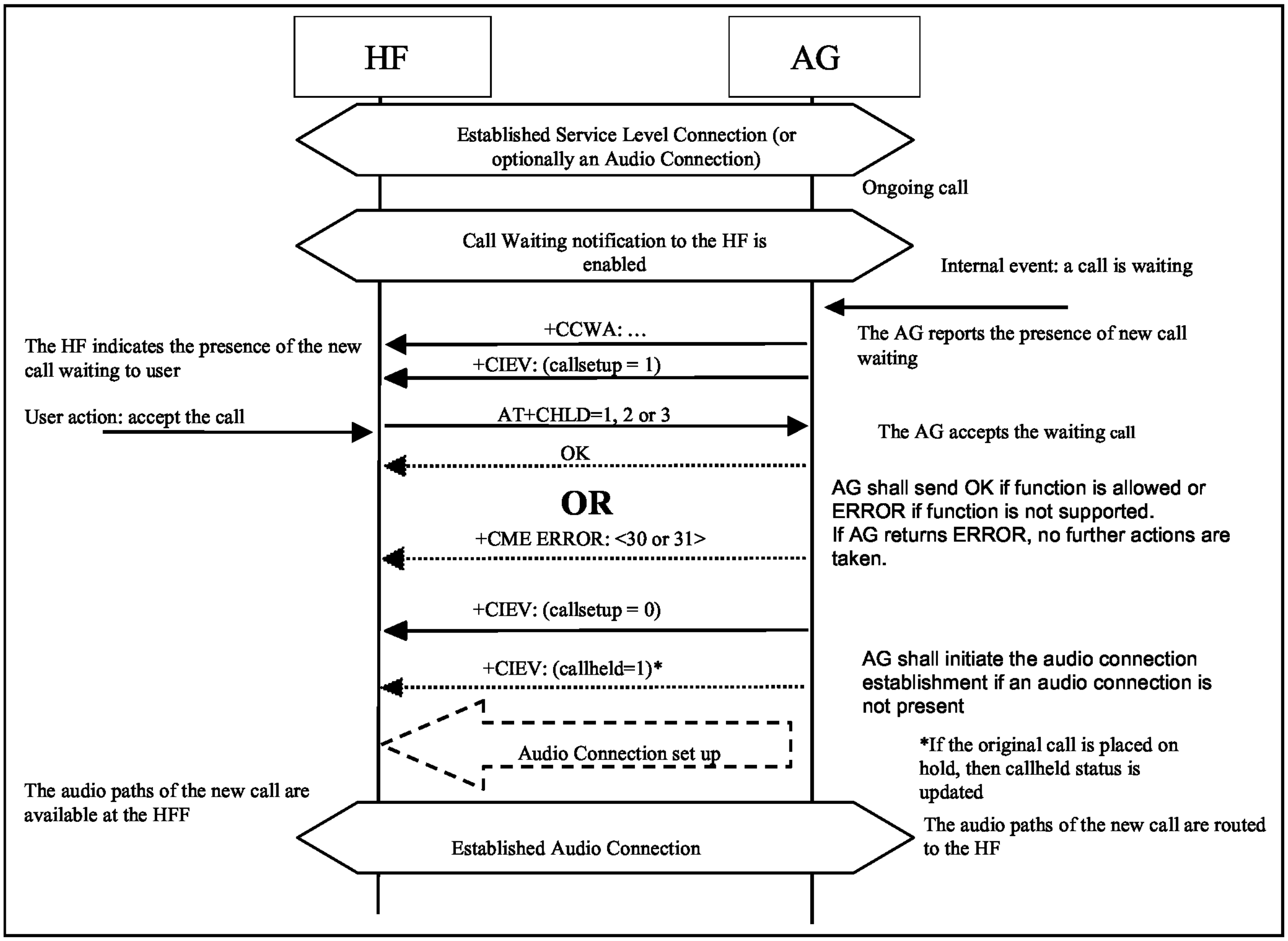

HF
AG
Established Service Level Connection (or optionally an Audio Connection)
Ongoing call
Call Waiting notification to the HF is enabled
Internal event: a call is waiting
+CCWA: ...
The HF indicates the presence of the new call waiting to user
+CIEV: (callsetup = 1)
The AG reports the presence of new call waiting
User action: accept the call
AT+CHLD=1, 2 or 3
The AG accepts the waiting call
OK
OR
AG shall send OK if function is allowed or ERROR if function is not supported.
If AG returns ERROR, no further actions are taken.
+CME ERROR: <30 or 31>
+CIEV: (callsetup = 0)
+CIEV: (callheld=1)*
AG shall initiate the audio connection establishment if an audio connection is not present
Audio Connection set up
*If the original call is placed on hold, then callheld status is updated
The audio paths of the new call are available at the HFF
Established Audio Connection
The audio paths of the new call are routed to the HF

Figure 4.25: Typical Call Waiting indication followed by a three way call set up process

If the AG receives a third party call, it shall send the call waiting notification +CCWA and +CIEV result code, with the value indicating (callsetup=1), to the HF. If the user accepts the call at the HF, it shall send the AT+CHLD with parameter 1, 2 or 3 to the AG. The AG shall then accept the waiting call and respond with OK, and issue the +CIEV result code with the value indicating (callsetup=0). If the HF elects to send AT+CHLD=2 (placing the original call on hold), then the AG shall send the +CIEV result code with the value indicating a held call (callheld=1).

Optionally, the HF may then use the AT+CHLD command, in order to change the status of the held and active calls.

If the normal incoming call procedure is interrupted for any reason, the AG shall issue the +CIEV result code, with the value indicating (callsetup=0), to notify the HF of this condition (see Section 4.14.2).

4.22.2 Three Way Calls – Third Party Call Placed from the HF

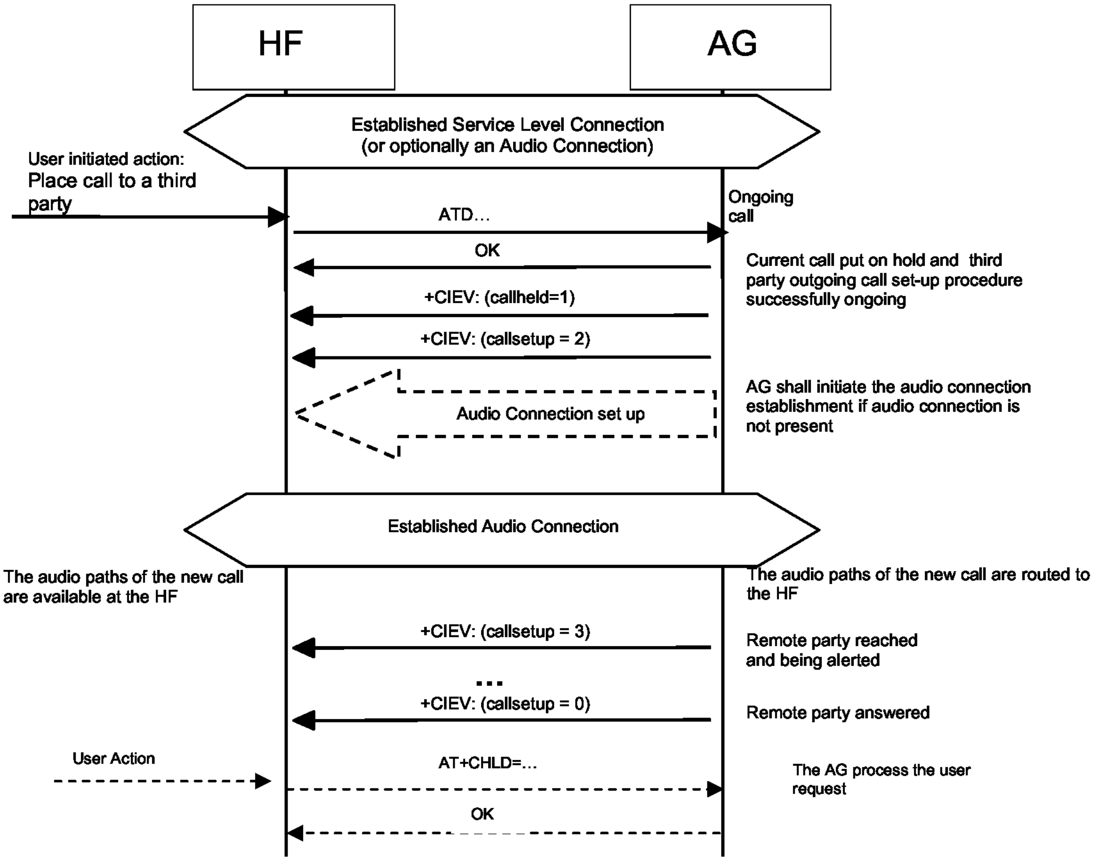

HF
AG
Established Service Level Connection
(or optionally an Audio Connection)
User initiated action:
Place call to a third party
ATD…
Ongoing call
OK
Current call put on hold and third party outgoing call set-up procedure successfully ongoing
+CIEV: (callheld=1)
+CIEV: (callsetup = 2)
Audio Connection set up
AG shall initiate the audio connection establishment if audio connection is not present
Established Audio Connection
The audio paths of the new call are available at the HF
The audio paths of the new call are routed to the HF
+CIEV: (callsetup = 3)
Remote party reached and being alerted
...
+CIEV: (callsetup = 0)
Remote party answered
User Action
AT+CHLD=...
The AG process the user request
OK

Figure 4.26: Three way call handling when the third party call is placed from the HF

If a third party call is placed from the HF using the ATD command, the AG shall send the OK indication and +CIEV result code, with the value indicating (callsetup=2), to the HF. The AG shall then place the active call in hold status in order to establish the new call.

Once the AG is informed that the alerting of the remote party has begun, the AG shall issue the +CIEV result code, with the value indicating (callsetup=3). If the wireless network does not provide the AG of an indication of alerting the remote party, the AG may not send this indication.

If the remote party answers the call, the AG shall issue the +CIEV result code with the value indicating (callsetup=0).

Optionally, the HF may then use the AT+CHLD command in order to change the status of the held and active calls. If the AT+CHLD command results in the change in a held call status the AG shall provide the status indication using the +CIEV result code with the value indicating the call held status (callheld=<0,1,2>).

If the normal outgoing call procedure is interrupted for any reason, the AG shall issue the +CIEV result code, with the value indicating (callsetup=0), to notify the HF of this condition (see Section 4.15.2).

4.23 Calling Line Identification (CLI) Notification

The HF may issue the AT+CLIP command to enable the “Calling Line Identification notification” function in the AG.

If the calling subscriber number information is available from the network, the AG shall issue the +CLIP unsolicited result code just after every RING indication when the HF is alerted in an incoming call. See Section 4.13 for more details.

Once the HF issues the AT+CLIP command, the AG shall respond with OK. The AG shall then keep the “Calling Line Identification notification” enabled until either the AT+CLIP command is issued by the HF to disable it, or the current Service Level Connection between the AG and the HF is dropped for any reason.

Refer to Section 4.33 for more information on the AT+CLIP command.

As pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the HF shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.

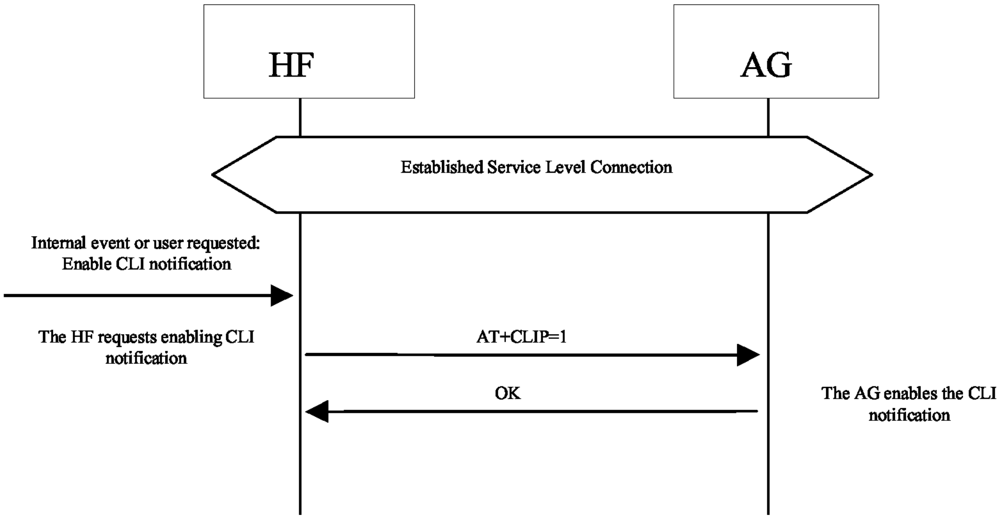

HF
AG
Established Service Level Connection
Internal event or user requested: Enable CLI notification
The HF requests enabling CLI notification
AT+CLIP=1
OK
The AG enables the CLI notification

Figure 4.27: Activation of CLI notification

4.24 The HF Requests Turning Off the AG’s EC and NR

The HF may disable the echo canceling and noise reduction functions resident in the AG via the AT+NREC command.

If the HF supports embedded EC and/or NR functions it shall support the AT+NREC command as described in the procedures in this section. Moreover, if the HF has these functions enabled, it shall perform this procedure before any Audio Connection between the HF and the AG is established.

By default, if the AG supports its own embedded echo canceling and/or noise reduction functions, it shall have them activated until the AT+NREC command is received. From then on, and until the current Service Level Connection between the AG and HF is dropped for any reason, the AG shall disable these functions every time an Audio Connection between the HF and the AG is used for audio routing.

If the AG does not support any echo canceling and noise reduction functions, it shall respond with the ERROR indicator on reception of the AT+NREC command.

Refer to Section 4.33 for more information on the AT+NREC command.

As pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the HF shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.

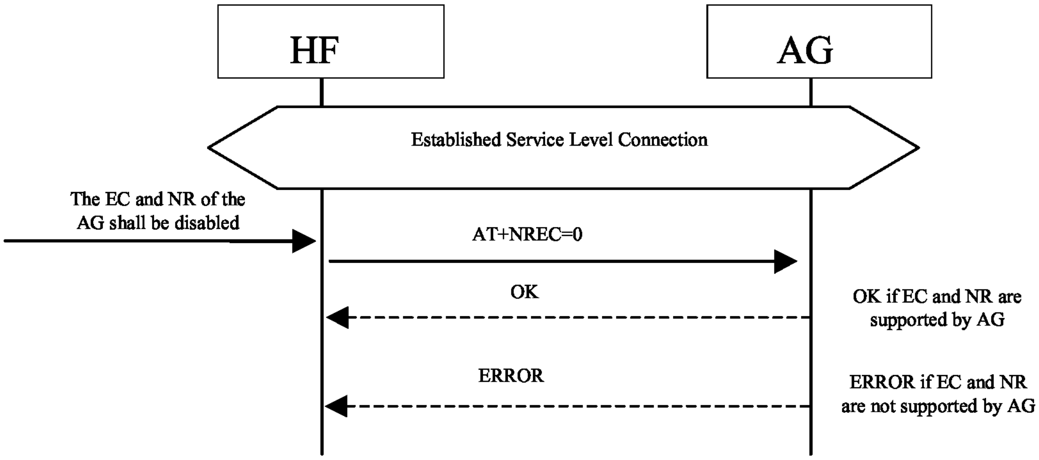

HF
AG
Established Service Level Connection
The EC and NR of the AG shall be disabled
AT+NREC=0
OK
OK if EC and NR are supported by AG
ERROR
ERROR if EC and NR are not supported by AG

Figure 4.28: NR and EC functions available in the AG

The HF sends the AT+NREC command and AG confirms with either OK or ERROR indication.

4.25 Voice Recognition Activation

The HF, via the AT+BVRA command, or the AG autonomously, may activate/deactivate the voice recognition function resident in the AG. Beyond the audio routing and voice recognition activation capabilities, the rest of the voice recognition functionality is implementation dependent.

Whenever the AG supports a voice recognition function it shall support the AT+BVRA command as described in the procedures in this section.

If the HF issues the AT+BVRA command, the AG shall respond with the OK result code if it supports voice recognition, then initiate an Audio Connection to the HF (if the Audio Connection does not already exist) and begin the voice input sequence.

If the AG does not support voice recognition, the AG shall respond with the ERROR indication.

When the voice recognition function is activated from the AG, it shall inform the HF via the +BVRA: 1 unsolicited result code and the AG shall initiate an Audio Connection to the HF (if the Audio Connection does not already exist) and begin the voice input sequence.

Once activated, depending upon the voice recognition implementation, the AG shall then keep the voice recognition function enabled:

- For the duration of time supported by the implementation ("momentary on" voice recognition implementation). In this case, the AG shall notify the HF by sending a +BVRA: 0 unsolicited result code.
- Or until the AT+BVRA command is issued to disable voice recognition from the HF.
- Or until the current Service Level Connection between the AG and the HF is dropped for any reason.

Refer to Section 4.33 for more information on the AT+BVRA command and the +BVRA result code.

As pre-condition for these procedures, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the initiator of the procedure shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.

4.25.1 Voice Recognition Activation – HF Initiated

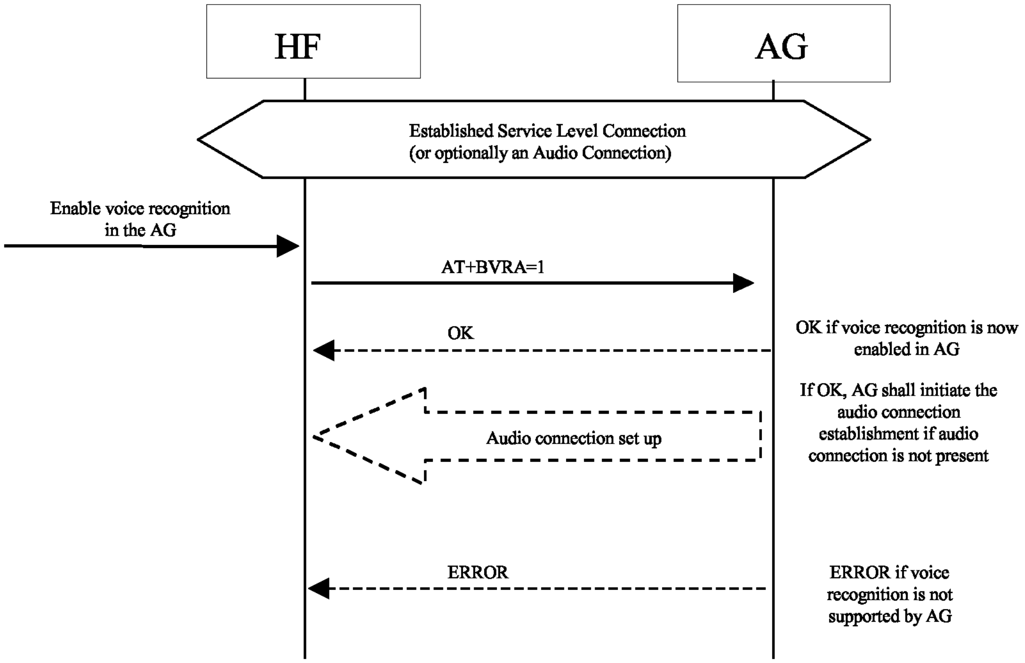


Figure 4.29: Voice recognition activation – HF initiated

4.25.2 Voice Recognition Activation – AG Initiated

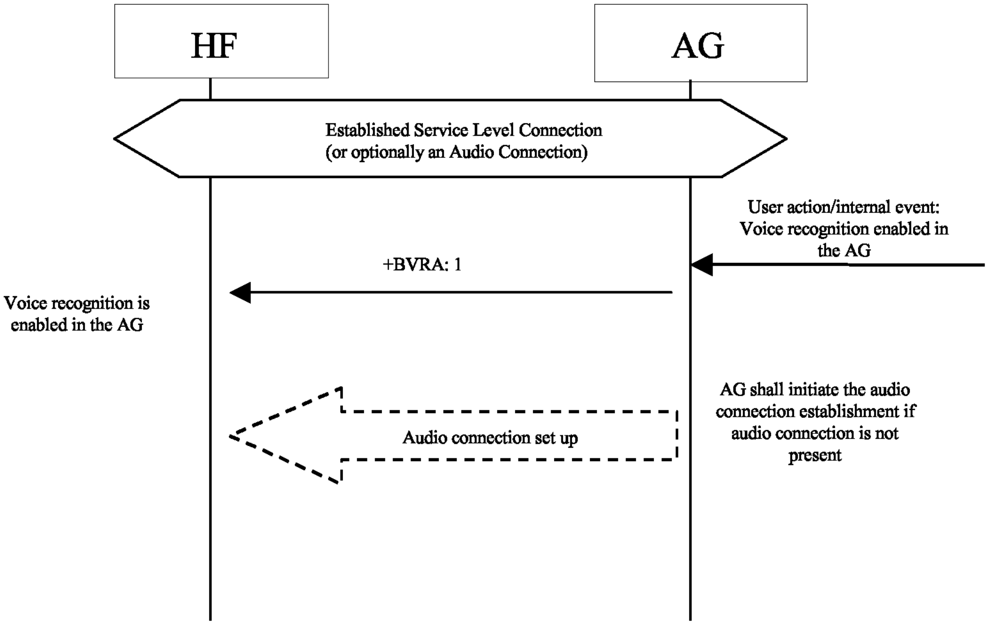

HF
AG
Established Service Level Connection
(or optionally an Audio Connection)
User action/internal event:
Voice recognition enabled in
the AG
+BVRA: 1
Voice recognition is
enabled in the AG
Audio connection set up
AG shall initiate the audio
connection establishment if
audio connection is not
present

Figure 4.30: Voice recognition activation – AG initiated

4.25.3 Voice Recognition Deactivation

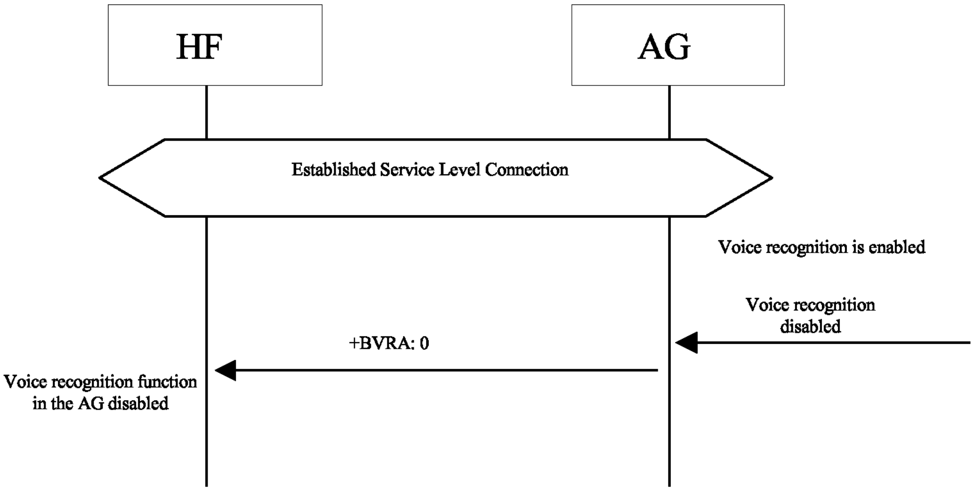

HF
AG
Established Service Level Connection
Voice recognition is enabled
Voice recognition
disabled
+BVRA: 0
Voice recognition function
in the AG disabled

Figure 4.31: Voice recognition deactivation – "momentary on" approach

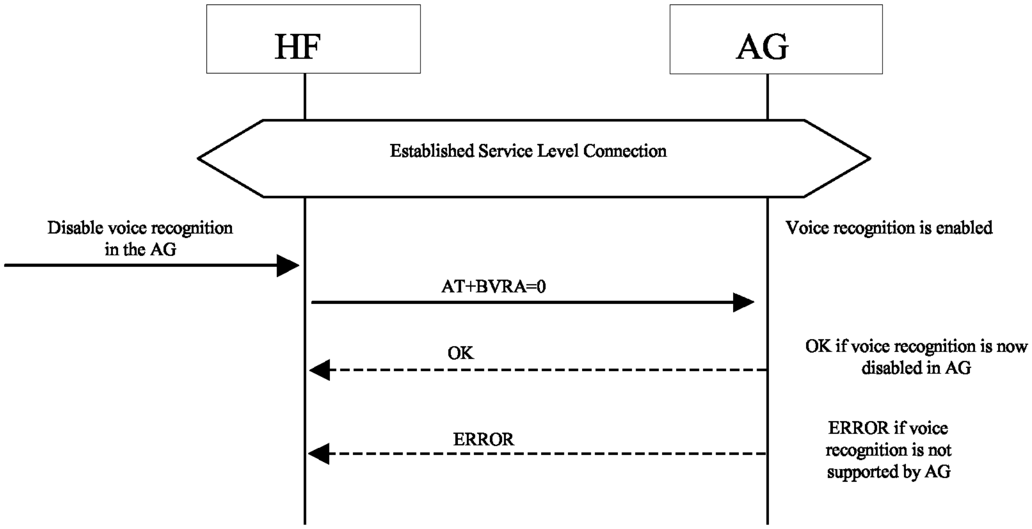

HF
AG
Established Service Level Connection
Disable voice recognition in the AG
Voice recognition is enabled
AT+BVRA=0
OK
OK if voice recognition is now disabled in AG
ERROR
ERROR if voice recognition is not supported by AG

Figure 4.32: Voice recognition deactivation from the HF

4.26 Attach a Phone Number to a Voice Tag

This procedure is applicable to HF units supporting internal voice recognition functionality. It provides a means to read numbers from the AG for the purpose of creating a unique voice tag and storing the number and its linked voice tag in the HF unit's memory. The HF unit may then use its internal Voice Recognition to dial the linked phone numbers when a voice tag is recognized by using the procedure "Place a call with the phone number supplied by the HF" described in Section 4.18.

Upon an internal event or user action, the HF may request a phone number from the AG by issuing the AT+BINP=1 command. Depending on the current status of the AG, it may either accept or reject this request.

If the AG accepts the request, it shall obtain a phone number and send the phone number back to the HF by issuing the +BINP response.

If the AG rejects the request from the HF, it shall issue the ERROR result code to indicate this circumstance to the HF.

When this procedure is executed multiple times (to retrieve multiple AG phone numbers to be linked to voice tags), it is the responsibility of the AG to provide the next phone number to be passed to the HF each time the procedure is executed.

Refer to Section 4.33 for more information on the AT+BINP command and the +BINP response.

As pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the HF shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.

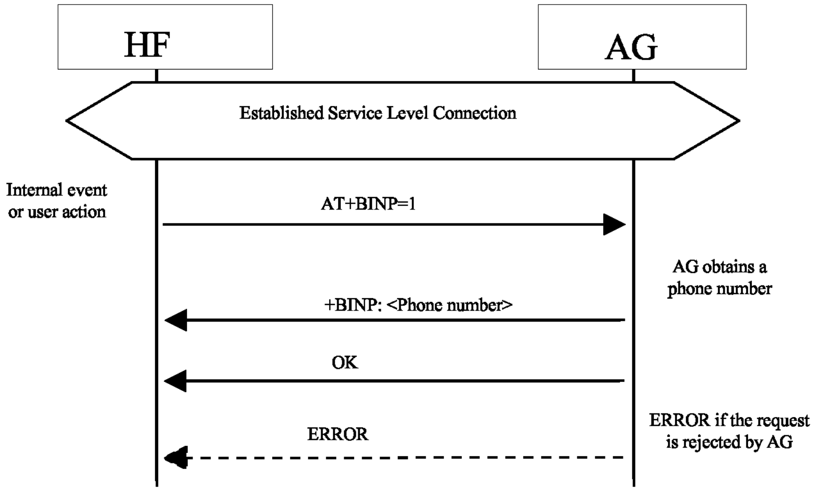

HF
AG
Established Service Level Connection
Internal event or user action
AT+BINP=1
AG obtains a phone number
+BINP: <Phone number>
OK
ERROR
ERROR if the request is rejected by AG

Figure 4.33: Request phone number to the AG

4.27 Transmit DTMF Codes

During an ongoing call, the HF transmits the AT+VTS command to instruct the AG to transmit a specific DTMF code to its network connection.

Refer to Section 4.33 for more information on the AT+VTS command.

The following pre-conditions apply for this procedure:

- An ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the HF shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.
- An ongoing call in the AG exists.

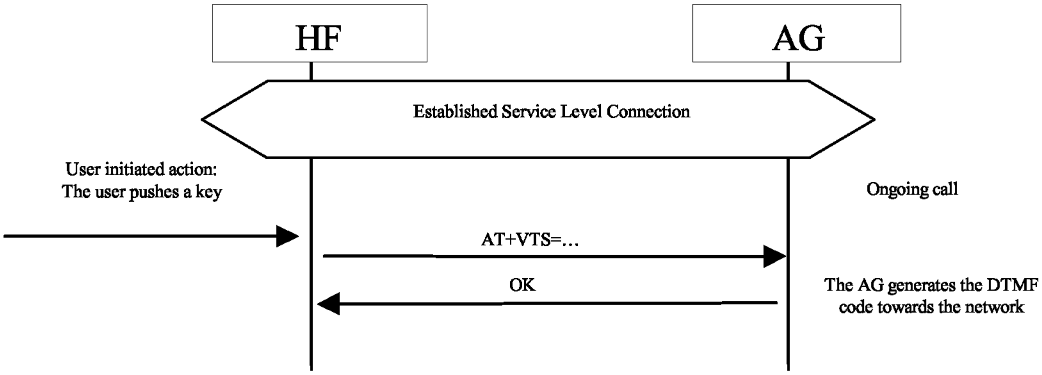

HF
AG
Established Service Level Connection
User initiated action: The user pushes a key
Ongoing call
AT+VTS=...
OK
The AG generates the DTMF code towards the network

Figure 4.34: Transmit DTMF code

4.28 Remote Audio Volume Control

4.28.1 Audio Volume Control

This procedure enables the user to modify the speaker volume and microphone gain of the HF from the AG.

The AG may control the gain of the microphone and speaker of the HF by sending the unsolicited result codes +VGM and +VGS respectively. There is no limit in the amount and order of result codes.

If the remote audio volume control feature is supported in the HF device, it shall support at least remote control of the speaker volume.

As pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the AG shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.

An audio connection is not a necessary pre-condition for this feature.

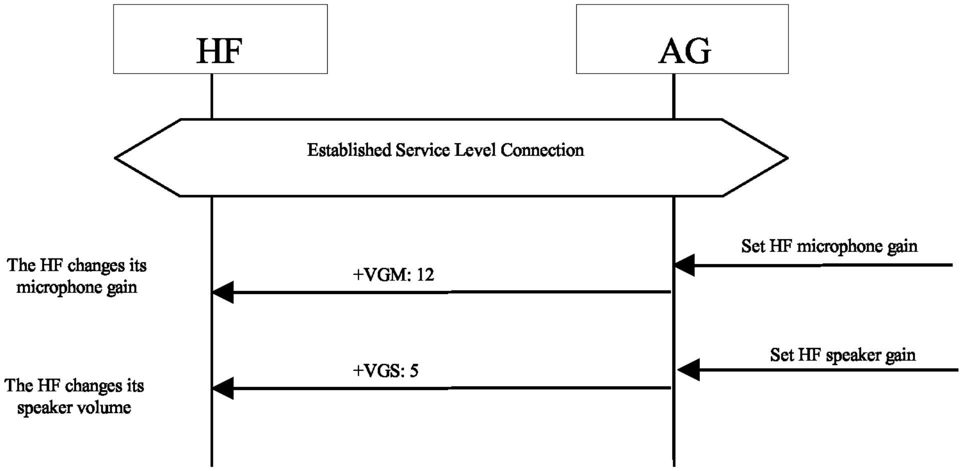

HF
AG
Established Service Level Connection
Set HF microphone gain
The HF changes its microphone gain
+VGM: 12
Set HF speaker gain
+VGS: 5
The HF changes its speaker volume

Figure 4.35: Typical example of audio volume control

Both the speaker and microphone gains are represented as parameter to the +VGS and +VGM, on a scale from 0 to 15. The values are absolute values, and relate to a particular (implementation dependent) volume level controlled by the HF.

Refer to Section 4.33 for more information on these commands and unsolicited result codes.

4.28.2 Volume Level Synchronization

This procedure allows the HF to inform the AG of the current gain settings corresponding to the HF's speaker volume and microphone gain.

On Service Level Connection establishment, the HF shall always inform the AG of its current gain settings by using the AT commands AT+VGS and AT+VGM.

If local means are implemented on the HF to control the gain settings, the HF shall also use the AT commands AT+VGS and AT+VGM to permanently update the AG of changes in these gain settings.

In all cases, the gain settings shall be kept stored, at both sides, for the duration of the current Service Level Connection. Moreover, if the Service Level Connection is released as a consequence of an HF initiated “Audio Connection transfer towards the AG”, as stated in Section 4.17, the HF shall also keep the gain settings and re-store them when the Service Level Connection is re-established again.

The HF is only mandated to support microphone gain synchronization when it supports remote microphone gain control.

As pre-condition for this procedure, an ongoing Service Level Connection between the AG and the HF shall exist. If this connection does not exist, the HF shall autonomously establish the Service Level Connection using the proper procedure as described in Section 4.2.

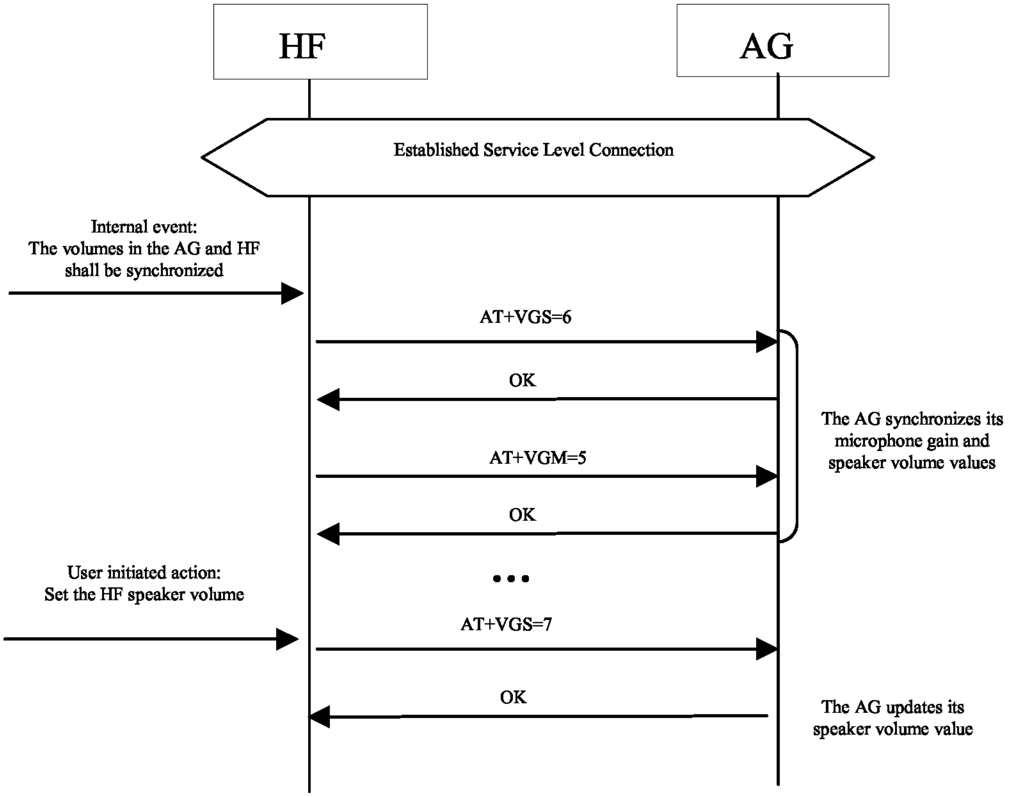


Figure 4.36: Typical example of volume level synchronization

Refer to Section 4.33 for more information on these commands and unsolicited result codes.

4.29 Response and Hold

This procedure allows the user to put an incoming call on hold and then accept or reject the call from the HF or AG. This feature is specific to the limited markets where PDC and CDMA networks support this function.

4.29.1 Query Response and Hold Status

The HF shall execute this procedure to query the status of the "Response and Hold" state of the AG.

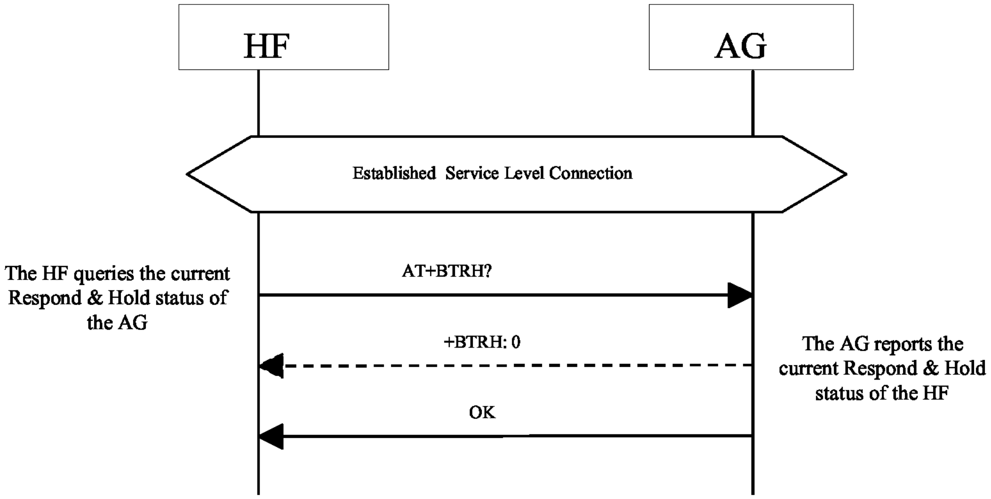

HF
AG
Established Service Level Connection
The HF queries the current Respond & Hold status of the AG
AT+BTRH?
+BTRH: 0
The AG reports the current Respond & Hold status of the HF
OK

Figure 4.37: Query Response and Hold State of AG

- The HF shall issue AT+BTRH? command to query the current "Response and Hold" state of the AG.
- If the AG is currently in any of the Response and Hold states, then the AG shall send a +BTRH: Response with the parameter set to 0. If the AG is not in the Response and Hold states, then no response shall be sent.
- The AG shall send OK response to signal completion of the AT+BTRH? command.

4.29.2 Put an Incoming Call on Hold from HF

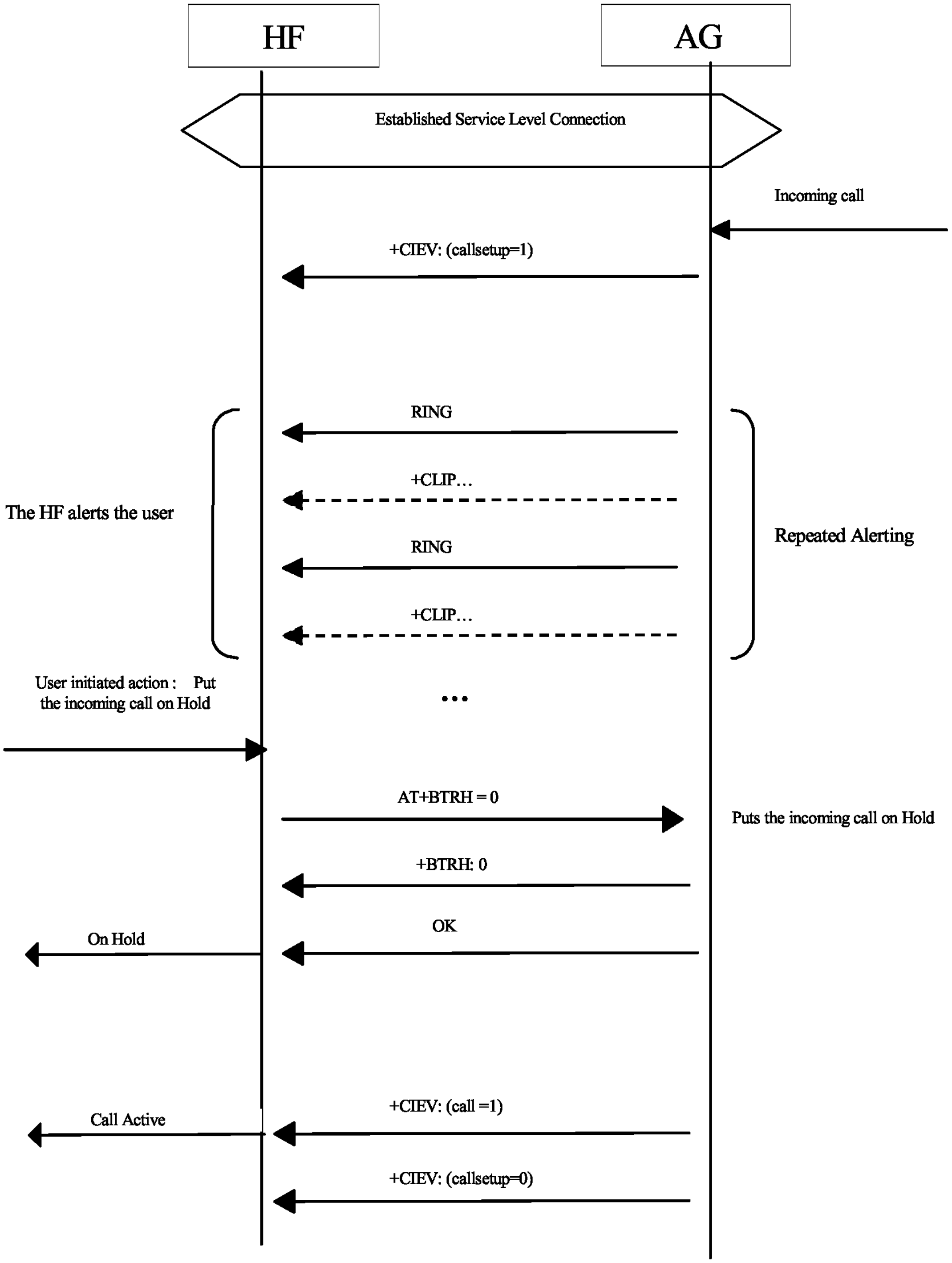


Figure 4.38: Put an incoming call on Hold from HF

- As a pre-condition to this procedure, the AG shall not have an active call or a call on hold.
- The AG shall send a sequence of unsolicited RING alerts to the HF. The RING alert shall be repeated until the HF accepts the incoming call or until the incoming call is interrupted for any reason.

- If the HF has enabled the Calling Line Identification [CLI], the AG shall send a +CLIP Response to HF.
- The user may put the incoming voice call on hold by using the proper means provided by the HF unit. The HF shall then send the AT+BTRH command with the parameter <n> set to 0. The AG shall then begin the procedure for putting the incoming call on hold.
- The AG shall send +BTRH Response with the parameter set to 0 as soon as the incoming call is put on hold.
- The AG shall send the +CIEV Response with the call status set to 1.
- The AG shall send the +CIEV Response with the callsetup status set to 0.

4.29.3 Put an Incoming Call on Hold from AG

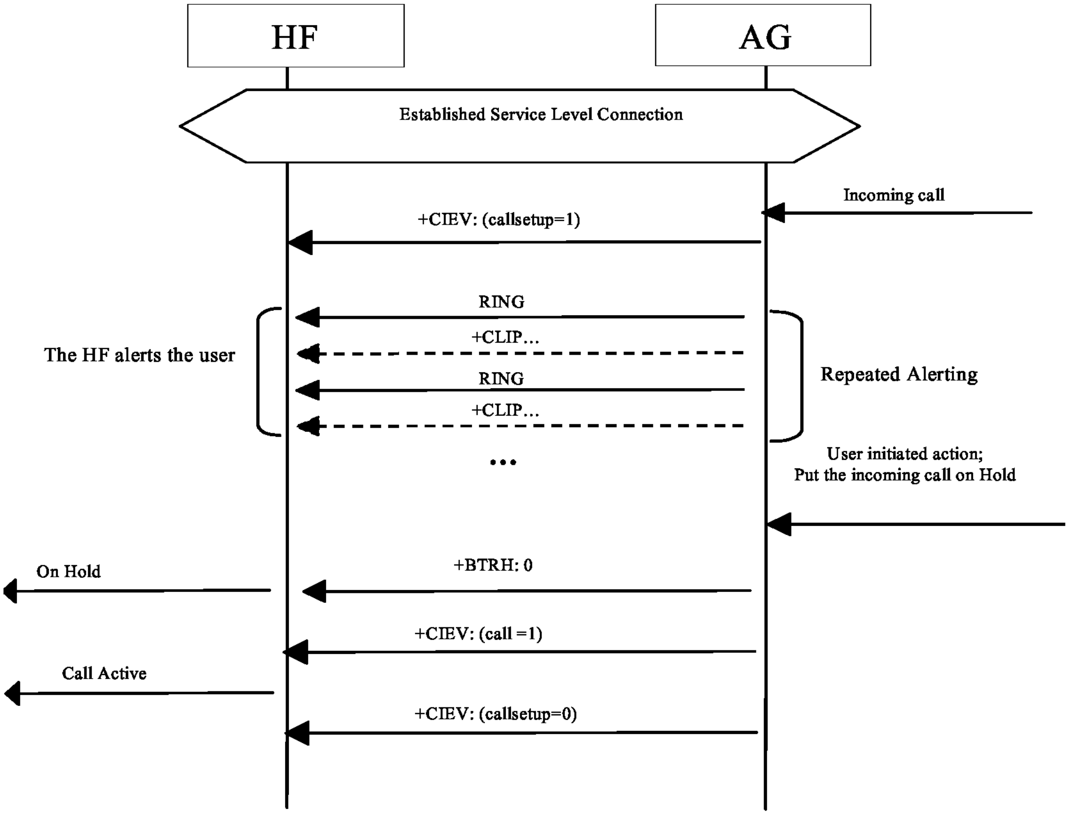


Figure 4.39: Put an incoming call on Hold from AG

As a pre-condition to this procedure, the AG shall not have an active call or a call on hold.

- The AG shall send a sequence of unsolicited RING alerts to the HF. The RING alert shall be repeated until the HF accepts the incoming call or until the incoming call is interrupted for any reason.
- If the HF has enabled the Calling Line Identification [CLI], the AG shall send a +CLIP Response to the HF.
- The user may put the incoming voice call on hold by using the proper means provided by the AG unit. The AG shall then send +BTRH Response with the parameter <n> set to 0 to indicate that the incoming call is on hold.
- Depending on whether in band ringing is enabled or disabled, there may or may not be a synchronous connection established between the HF and AG. The synchronous connection state (enabled or disabled) shall not be changed when an incoming call is placed on hold.
- The AG shall send the +CIEV Response with the call status set to 1.
- The AG shall send the +CIEV Response with the callsetup status set to 0.

4.29.4 Accept a Held Incoming Call from HF

The following additional pre-condition applies to this procedure:

- An incoming call was put on hold.

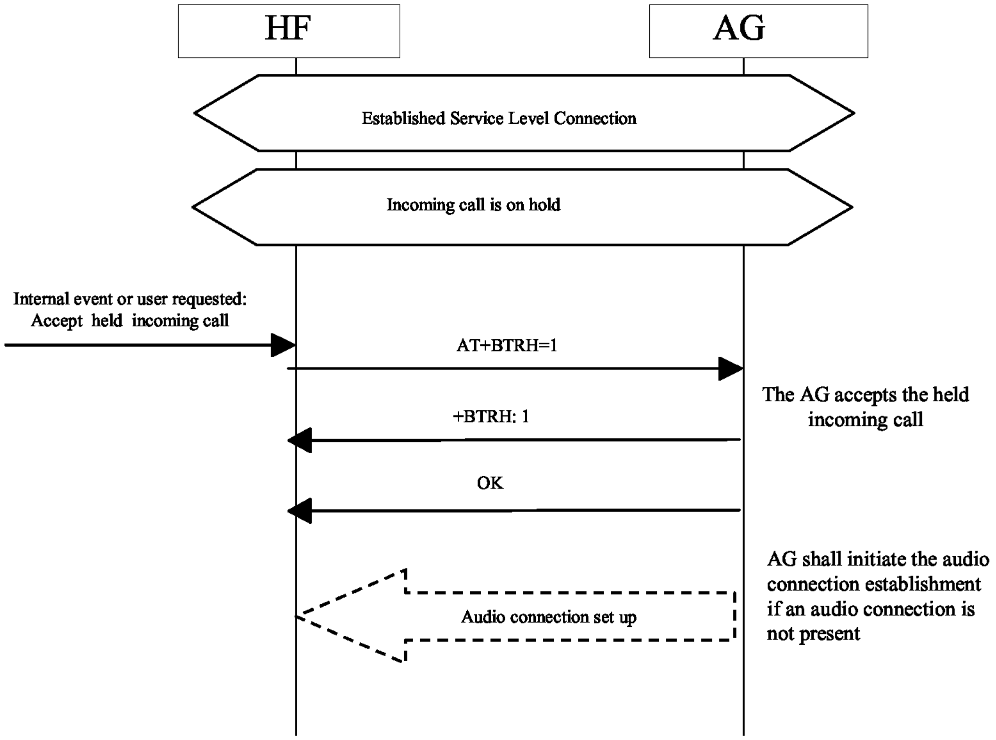

HF
AG
Established Service Level Connection
Incoming call is on hold
Internal event or user requested:
Accept held incoming call
AT+BTRH=1
+BTRH: 1
The AG accepts the held incoming call
OK
Audio connection set up
AG shall initiate the audio connection establishment if an audio connection is not present

Figure 4.40: Accept a held incoming call from HF

- The user may accept the incoming voice call on hold by using the proper means provided by the HF unit. The HF shall then send the AT+BTRH command with the parameter <n> set to 1. The AG shall then begin the procedure for accepting the incoming call that was put on hold.

- The AG shall then send +BTRH Response with the parameter <n> set to 1 to notify HF that the held incoming call was accepted.
- The AG shall start the procedure for establishing the audio connection and route the audio paths to the HF only if the audio connection was not established.

4.29.5 Accept a Held Incoming Call from AG

The following additional pre-condition applies to this procedure:

- An incoming call was put on hold.

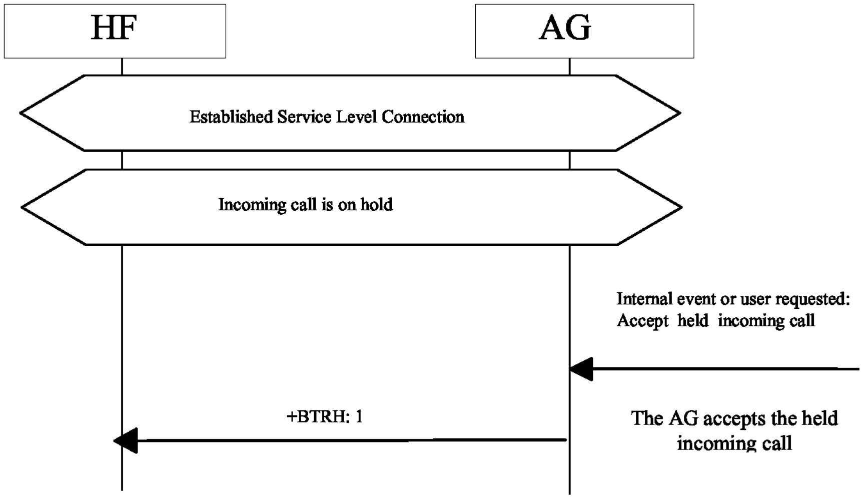

HF
AG
Established Service Level Connection
Incoming call is on hold
Internal event or user requested:
Accept held incoming call
+BTRH: 1
The AG accepts the held incoming call

Figure 4.41: Accept a held incoming call from AG

- The user may accept the incoming voice call on hold by using the proper means provided by the AG unit. The AG shall then send +BTRH Response with the parameter <n> set to 1 to notify the HF that the held incoming call was accepted.

4.29.6 Reject a Held Incoming Call from HF

The following additional pre-condition applies to this procedure:

- An incoming call was put on hold.

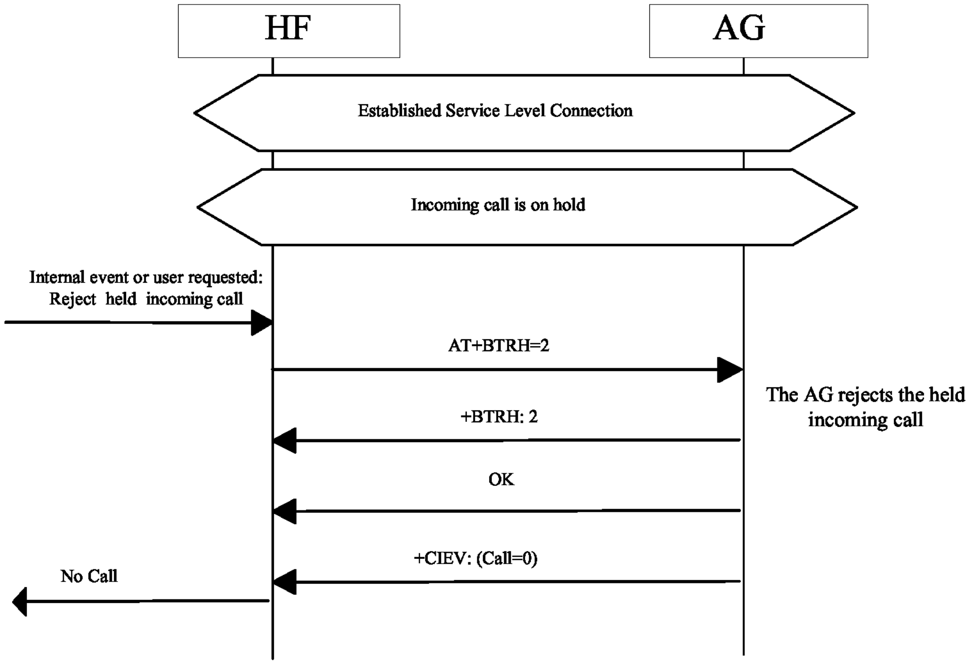

HF
AG
Established Service Level Connection
Incoming call is on hold
Internal event or user requested: Reject held incoming call
AT+BTRH=2
The AG rejects the held incoming call
+BTRH: 2
OK
+CIEV: (Call=0)
No Call

Figure 4.42: Reject a held incoming call from HF

- The user may reject the incoming voice call on hold by using the proper means provided by the HF unit. Either of the following two sequences shall be permissible by the HF and AG:
  - The HF may send the AT+BTRH command with the parameter <n> set to 2. The AG shall then begin the procedure for rejecting the incoming call that was put on hold. The AG shall send +BTRH Response with the parameter <n> set to 2 to notify the HF that the held incoming call was rejected.
  - The HF may send the AT+CHUP command to reject the held incoming call. The AG shall reject the held call and send the OK indication to the HF.
- The AG shall send the +CIEV Response with the call status set to 0.

4.29.7 Reject a Held Incoming Call from AG

The following additional pre-condition applies to this procedure:

- An incoming call was put on hold.

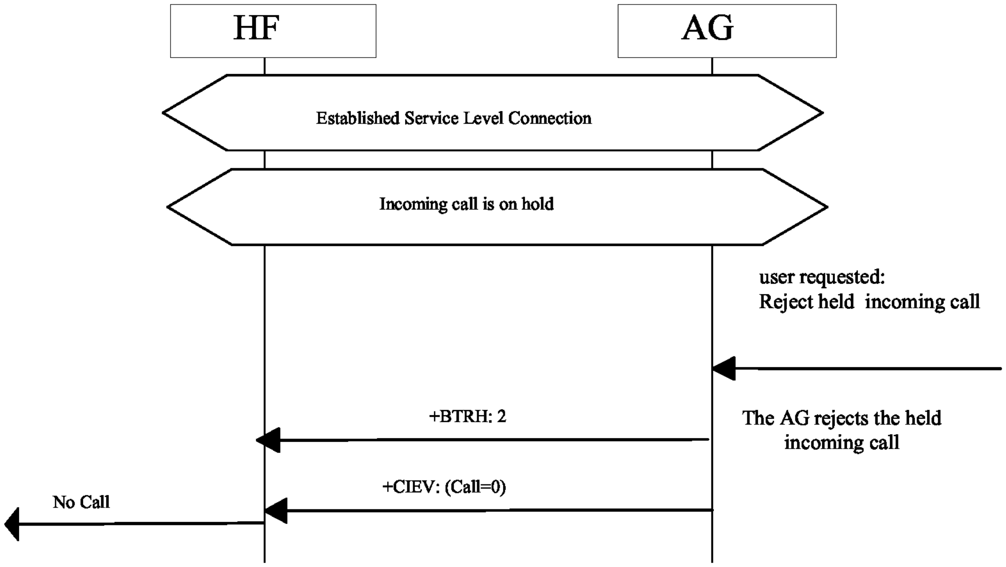

HF
AG
Established Service Level Connection
Incoming call is on hold
user requested:
Reject held incoming call
+BTRH: 2
The AG rejects the held incoming call
+CIEV: (Call=0)
No Call

Figure 4.43: Reject a held incoming call from AG

- The user may reject the incoming voice call on hold by using the proper means provided by the AG unit. The AG shall then send +BTRH Response with the parameter <n> set to 2 to notify HF that the held incoming call was rejected.
- The AG shall also send the +CIEV Response with the call status parameter set to 0 to indicate that the AG is currently not in a call.

4.29.8 Held Incoming Call Terminated by Caller

The following additional pre-condition applies to this procedure:

- An incoming call was put on hold.

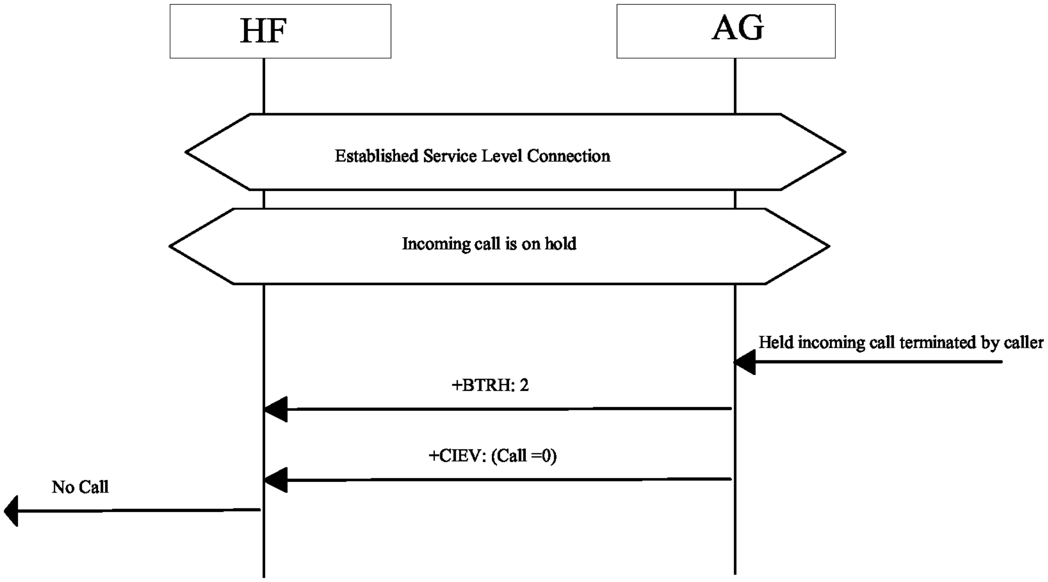

HF
AG
Established Service Level Connection
Incoming call is on hold
Held incoming call terminated by caller
+BTRH: 2
+CIEV: (Call =0)
No Call

Figure 4.44: Held incoming call terminated by caller

- The caller may terminate the held incoming call. The AG shall then send +BTRH Response with the parameter <n> set to 2 to notify the HF that the held incoming call was terminated.
- The AG shall send the +CIEV Response with the Call status parameter set to 0 to indicate that the AG is currently not in a call.

4.30 Subscriber Number Information

This procedure allows HF to query the AG subscriber number.

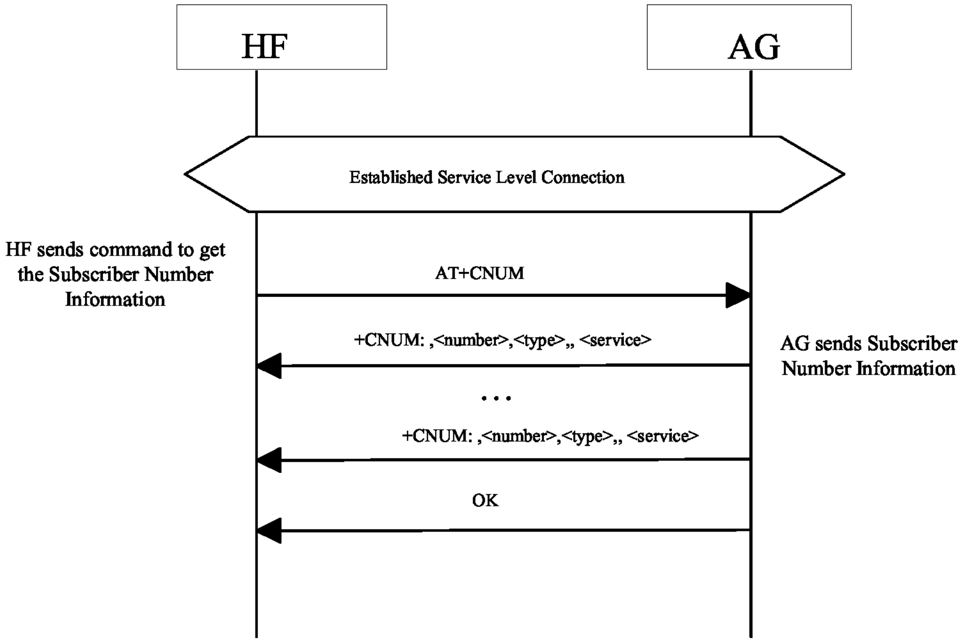

HF
AG
Established Service Level Connection
HF sends command to get the Subscriber Number Information
AT+CNUM
+CNUM: ,<number>,<type>,, <service>
AG sends Subscriber Number Information
...
+CNUM: ,<number>,<type>,, <service>
OK

Figure 4.45: Query Subscriber Number Information of AG

This procedure illustrates AG response to the query of an empty subscriber number.

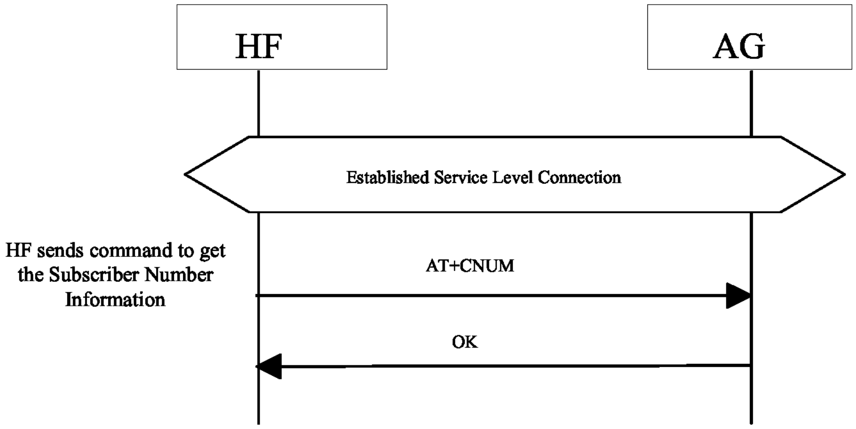

HF
AG
Established Service Level Connection
HF sends command to get the Subscriber Number Information
AT+CNUM
OK

Figure 4.46: Empty Subscriber Number Information from AG

The following pre-condition applies for this procedure:

- An ongoing Service Level Connection between the HF and AG shall exist. If this connection does not exist, the HF shall establish a connection using the "Service Level Connection set up" procedure described in Section 4.2.
- The HF shall send the AT+CNUM command to query the AG subscriber number information.

- If the subscriber number information is available, the AG shall respond with the +CNUM response. If multiple numbers are available, the AG shall send a separate +CNUM response for each available number.
- The AG shall signal the completion of the AT+CNUM action command with an OK response. The OK will follow zero or more occurrences of the +CNUM response. (See figures 4.45 and 4.46).

4.31 Enhanced Call Status Indications

4.31.1 Query List of Current Calls in AG

The HF shall execute this procedure to query the list of current calls in AG.

The following pre-condition applies for this procedure:

- A SLC must exist between the AG and HF devices. If no current SLC exists, the HF shall first initiate a SLC.

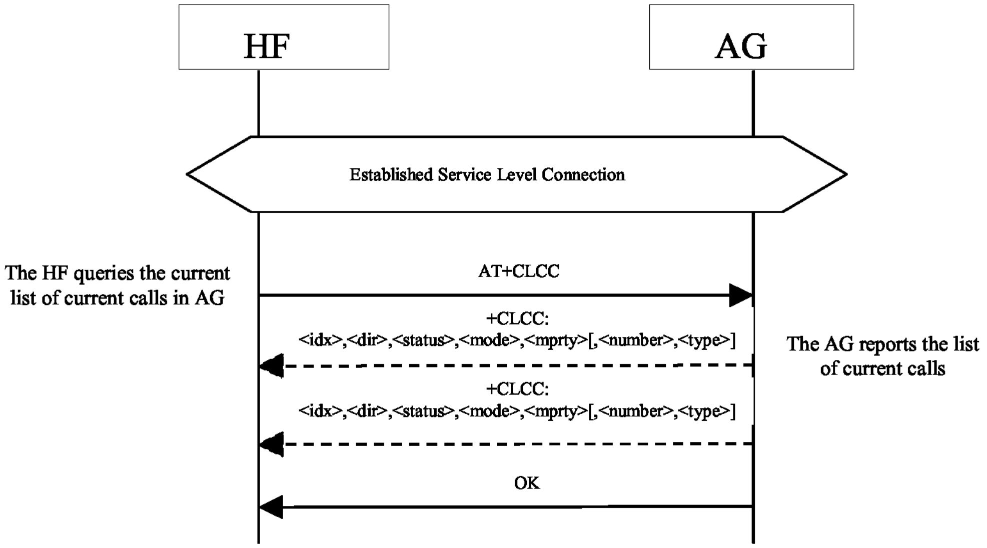

HF
AG
Established Service Level Connection
The HF queries the current list of current calls in AG
AT+CLCC
+CLCC: <idx>,<dir>,<status>,<mode>,<mprty>[,<number>,<type>]
The AG reports the list of current calls
+CLCC: <idx>,<dir>,<status>,<mode>,<mprty>[,<number>,<type>]
OK

Figure 4.47: Query List of Current Calls

- HF shall find out the list of current calls in AG by sending the AT+CLCC command.
- If the command succeeds and if there is an outgoing (Mobile Originated) or an incoming (Mobile Terminated) call in AG, AG shall send a +CLCC response with appropriate parameters filled in to HF.
- If there are no calls available, no +CLCC response is sent to HF.
- The AG shall always send OK response to HF.

4.31.2 Indication of Status for Held Calls

Upon the change in status of any call on hold in the AG, the AG shall execute this procedure to advise the HF of the held call status. The values for the callheld indicator are:

0= No calls held

1= Call is placed on hold or active/held calls swapped
(The AG has both and active AND a held call)
2= Call on hold, no active call

The following pre-condition applies for this procedure:

- The HF shall have enabled the Call Status Indicators function in the AG.
- A SLC shall exist between the AG and HF devices.

Whenever an active call is placed on hold such that the AG now has both an active and held call or the active/held call positions swapped by a request from the HF or by action on the AG the AG shall issue a +CIEV unsolicited result code with the callheld indicator value of “1”.

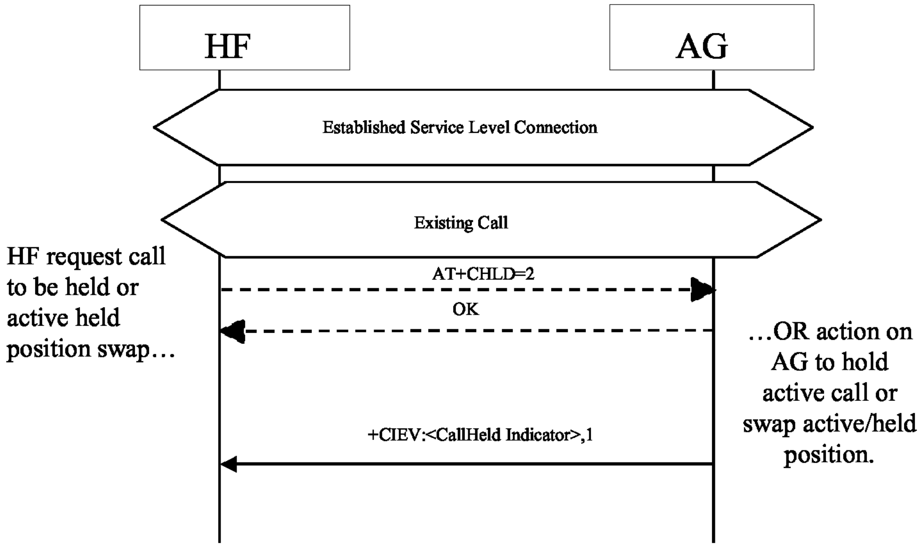

HF
AG
Established Service Level Connection
Existing Call
HF request call to be held or active held position swap…
AT+CHLD=2
OK
…OR action on AG to hold active call or swap active/held position.
+CIEV:<CallHeld Indicator>,1

Figure 4.48: Call Held or Active/Held Position Swap

Consequently, upon the release of any call on hold by the HF, the AG or by network event, or actions by the HF or AG to retrieve a held call, the AG shall issue a +CIEV unsolicited result code with the callheld indicator value of “0”.

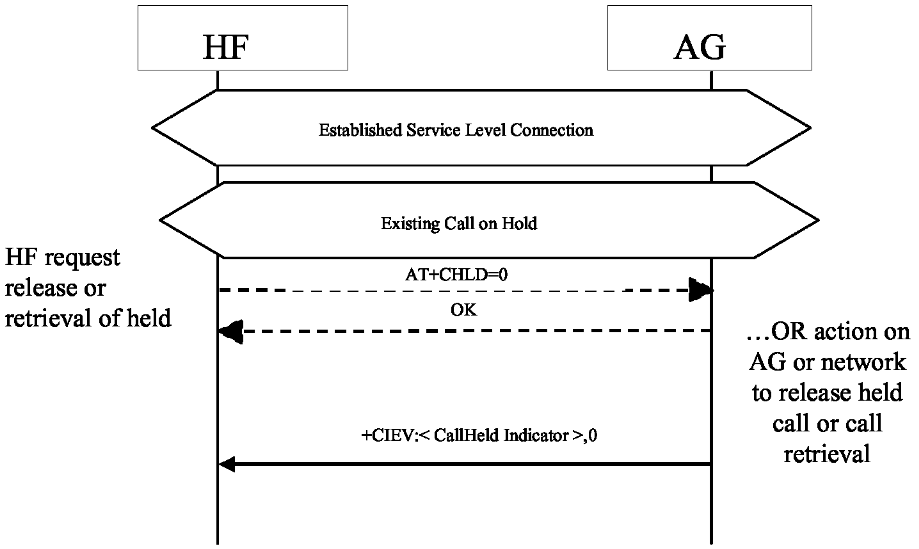

HF
AG
Established Service Level Connection
Existing Call on Hold
HF request release or retrieval of held
AT+CHLD=0
OK
…OR action on AG or network to release held call or call retrieval
+CIEV:< CallHeld Indicator >,0

Figure 4.49: Held Call Release

If a call is still on hold when an active call is terminated or a single active call is put on hold, the AG shall issue a +CIEV unsolicited result code with the callheld indicator value of “2”.

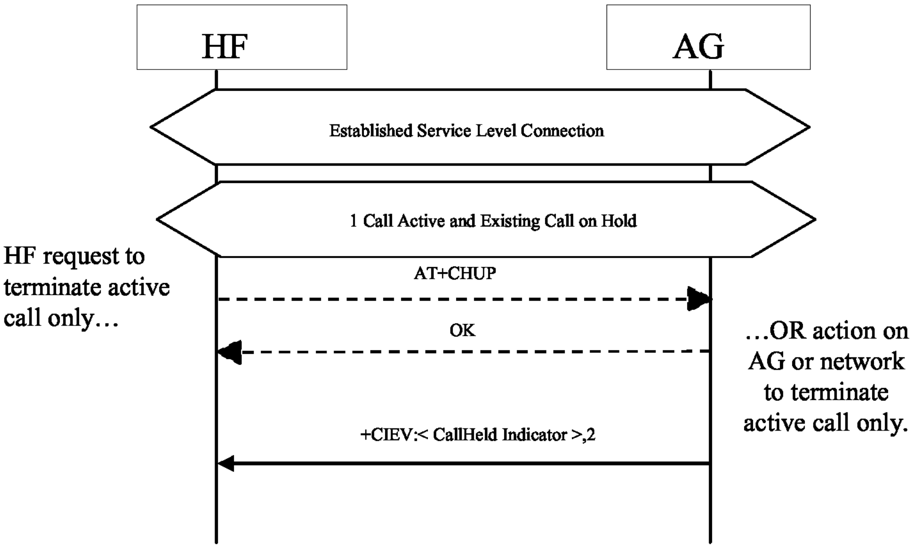

HF
AG
Established Service Level Connection
1 Call Active and Existing Call on Hold
HF request to terminate active call only…
AT+CHUP
OK
…OR action on AG or network to terminate active call only.
+CIEV:< CallHeld Indicator >,2

Figure 4.50: Active Call Terminated/Call Remains Held

4.32 Enhanced Call Control Mechanisms

As stated earlier, the Enhanced Call Control mechanism is simply an extension of the current AT+CHLD command. These extensions are defined as additional arguments to the AT+CHLD command. The new arguments for this command include an index of a specific call as indicated in the +CLCC response.

4.32.1 Release Specified Call Index

The HF shall execute this procedure to release a specific call in the AG.

The following pre-condition applies for this procedure:

- A SLC must exist between the AG and HF devices. If no current SLC exists, the HF shall first initiate a SLC.

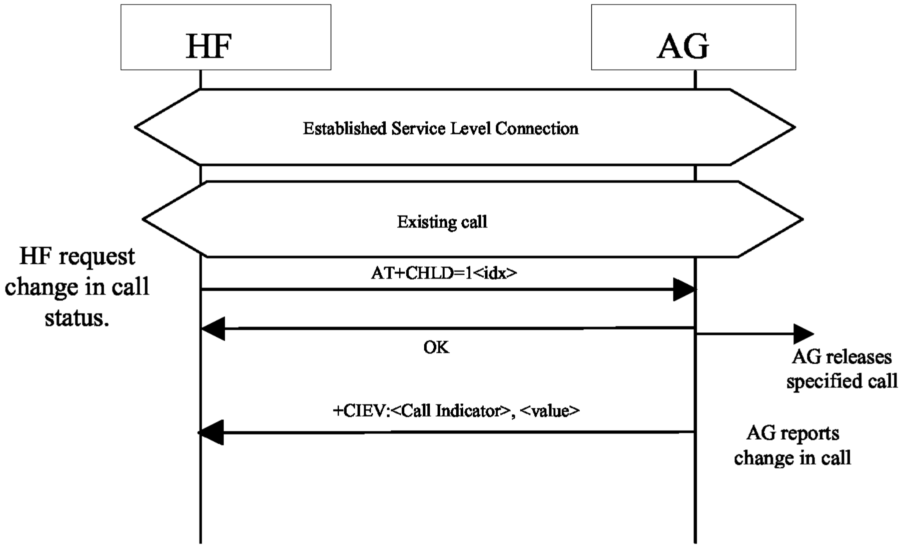

HF
AG
Established Service Level Connection
Existing call
HF request change in call status.
AT+CHLD=1<idx>
OK
AG releases specified call
+CIEV:<Call Indicator>, <value>
AG reports change in call

Figure 4.51: Release Specified Active Call

- The HF shall send the AT+CHLD=1<idx> command to release a specific active call.
- The AG shall release the specified call.
- If the released call was an active call and a call is currently held, the AG shall retrieve the held call.
- In the event that there are multiple held calls the AG shall retrieve the call associated with the lowest call index.
- The AG shall report the change in call status.

If the index (<idx>) is not valid, the AG shall report the proper error code.

4.32.2 Private Consultation Mode

The HF shall execute this procedure to place all parties of a multiparty call on hold with the exception of the specified call.

The following pre-condition applies for this procedure:

- A SLC must exist between the AG and HF devices. If no current SLC exists, the HF shall first initiate a SLC.
- Existing multiparty call is active in AG.

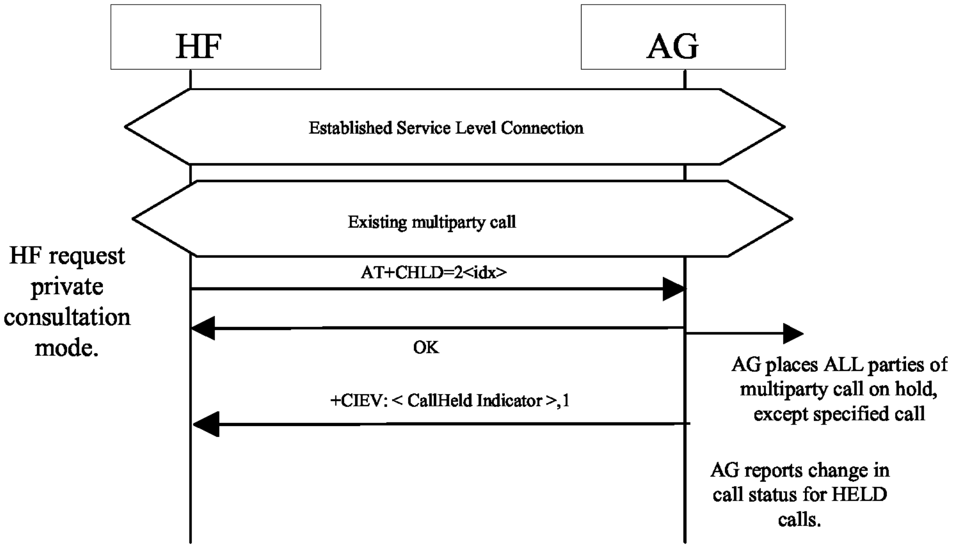

HF
AG
Established Service Level Connection
Existing multiparty call
HF request private consultation mode.
AT+CHLD=2<idx>
OK
+CIEV: < CallHeld Indicator >,1
AG places ALL parties of multiparty call on hold, except specified call
AG reports change in call status for HELD calls.

Figure 4.52: Request Private Consultation Mode

- HF shall send the AT+CHLD=2<idx> command to request private consultation mode.
- AG shall place all other parties of call on hold.
- AG shall report the change in status of the held parties.
- If the index (<idx>) is not valid, the AG shall respond with the proper error code.

4.33 AT Command and Results Codes

4.33.1 General

For the exchange of the commands and unsolicited results codes, the format, syntax and procedures of 3GPP 27.007 [2] shall be taken as reference. The following rules specifically apply for the HFP specification:

- Only one command (or unsolicited result code) per command line needs to be expected.
- The AG, by default, shall not echo the command characters.
- The AG shall always transmit result codes using verbose format.

- The characters below shall be used for AT commands and result codes formatting:

  <cr> corresponds to the *carriage return (0/13)* as stated in [6]

  <lf> corresponds to the *line feed (0/10)* as stated in [6]
- The format of an AT command from the HF to the AG shall be:

  <AT command><cr>
- The format of the OK code from the AG to the HF shall be:

  <cr><lf>OK<cr><lf>
- The format of the generic ERROR code from the AG to the HF shall be:

  <cr><lf>ERROR<cr><lf>
- The format of an unsolicited result code from the AG to the HF shall be:

  <cr><lf><result code><cr><lf>

The Hands-Free Profile uses a subset of AT commands and result codes from existing standards; these are listed in Section 4.33.2. Section 4.33.3 lists the new Bluetooth defined AT commands and result codes not re-used from any existing standard.

In general, the AG shall use the OK code, as described in Section 4.33.2, for acknowledgement of the proper execution of a command and respond with the proper error indication to any unknown command received from the HF.

It is mandatory for the AG to properly respond to any error condition and for the HF to properly process the corresponding error indication code received from the AG. The code ERROR, as described in Section 4.33.2, shall be used as error indication for this purpose.

The HF shall always ignore any unknown or unexpected indication code received from the AG. The only exception is the case in which the AG issues a "Mobile Equipment Error" indication using the +CME ERROR: result code (see [2]). In this case, the HF shall interpret this result code in the same way as if it was a generic ERROR code.

As a general rule, when an AT command or result code of this specification is implemented, support for the associated parameters "covered" in this specification, and all their corresponding possible values, shall be considered mandatory unless otherwise explicitly stated in each particular case.

4.33.2 AT Capabilities Re-Used from GSM 07.07 and 3GPP 27.007

The re-used AT commands and unsolicited result codes for implementing the functionality described in this specification are listed below:

As a convention, if a parameter of an AT command or result code is not "covered" in this specification, it shall not be present in the corresponding AT command, and the HF shall ignore the parameter whenever it is received in a result code.

- **ATA**

  Standard call answer AT command. Refer to Annex G in [2].

- **ATDdd…dd;**

  Standard AT command intended for placing a call to a phone number. Only voice calls are covered in this specification. Refer to Section 6.2 in [2].

- **ATD>nnn...;**

Extension of the standard ATD command, intended for memory dialing. Only voice calls are covered in this specification. Refer to Section 6.3 in [2].

- **ERROR**

  Standard error indication code. It shall be issued on detection of any syntax, format or procedure error condition. The “Mobile Equipment Error” report code “+CME ERROR:” is covered below. Refer to Annex B in [2].

- **OK**

  Standard acknowledgement to the execution of a command. Refer to Annex B in [2].

- **NO CARRIER, BUSY, NO ANSWER, DELAYED, BLACKLISTED**

  Extended response indication codes for AT commands. These codes shall be issued from the AG to the HF as responses to AT commands from the HF to the AG or from the AG as unsolicited result codes. These are in addition to the +CME ERROR: responses.

- **RING**

  Standard “incoming call” indication. Refer to Annex B in [2].

- **AT+CCWA**

  Standard “Call Waiting notification” AT command. Within the AT+CCWA=[<n>[,<mode>[,<class>]]]command, only enabling/disabling of the Call Waiting notification unsolicited result code +CCWA , using the <n> parameter, is covered in this specification. Refer to Section 7.12 in [2].

- **+CCWA**

  Standard “Call Waiting notification” unsolicited result code.

  In the +CCWA result code only <number> and <type> parameters are covered in this specification. Other parameters are not considered relevant in this specification and shall be ignored by the HF.

  The <number> parameter shall be a text string and shall always be contained within double-quotes.

  The <type> field specifies the format of the phone number provided, and can be one of the following values:

  - values 128-143: The phone number format may be a national or international format, and may contain prefix and/or escape digits. No changes on the number presentation are required.

- values 144-159: The phone number format is an international number, including the country code prefix. If the plus sign ("+") is not included as part of the number and shall be added by the AG as needed.
- values 160-175: National number. No prefix nor escape digits included.
- Refer to Section 7.12 in [2].

- **AT+CHLD**

  Standard call hold and multiparty handling AT command. In the AT+CHLD=<n> command, this specification only covers values for <n> of 0, 1, 1<idx>, 2, 2<idx>, 3 and 4, where:

  0 = Releases all held calls or sets User Determined User Busy (UDUB) for a waiting call.
  1 = Releases all active calls (if any exist) and accepts the other (held or waiting) call.
  1<idx> = Releases specified active call only (<idx>).
  2 = Places all active calls (if any exist) on hold and accepts the other (held or waiting) call.
  2<idx> = Request private consultation mode with specified call (<idx>). (Place all calls on hold EXCEPT the call indicated by <idx>.)
  3 = Adds a held call to the conversation.
  4 = Connects the two calls and disconnects the subscriber from both calls (Explicit Call Transfer). Support for this value and its associated functionality is optional for the HF.

  The test command AT+CHLD=? may be used for retrieving information about the call hold and multiparty services available in the AG (refer to Section 4.2.1).

  Refer to Section 7.13 in [2] and Section 4.5.5.1 in [8] for details.

- **AT+CHUP**

  Standard hang-up AT command. Execution command causes the AG to terminate the currently active call. This command shall have no impact on the state of any held call. Refer to Section 6.5 in [2].

  AT+CHUP is also used as the command to reject any incoming call prior to answer.

- **AT+CIND**

  Standard indicator update AT command. Only read command AT+CIND? and test command AT+CIND=? are required in this specification.

  The AT+CIND? read command is used to get current status of the AG indicators.

  The AT+CIND=? test command is used to retrieve the mapping between each indicator supported by the AG and its corresponding range and order index. It shall be issued at least once before any other command related to these indicators (AT+CIND? or AT+CMER) is used.

  The following indicators are covered in this specification:

- service: Service availability indication, where:

  <value>=0 implies no service. No Home/Roam network available.

  <value>=1 implies presence of service. Home/Roam network available.

- call: Standard call status indicator, where:

  <value>=0 means no call active.

  <value>=1 means a call is active.

- callsetup: Bluetooth proprietary call set up status indicator[3]. Support for this indicator is optional for the HF. When supported, this indicator shall be used in conjunction with, and as an extension of the standard call indicator. Possible values are as follows:

  <value>=0 means not currently in call set up.

  <value>=1 means an incoming call process ongoing.

  <value>=2 means an outgoing call set up is ongoing.

  <value>=3 means remote party being alerted in an outgoing call.

Refer to Section 8.9 in [2].

- callheld: Bluetooth proprietary call hold status indicator. Support for this indicator is mandatory for the AG, optional for the HF. Possible values are as follows:

  0= No calls held
  1= Call is placed on hold or active/held calls swapped
  (The AG has both and active AND a held call)
  2= Call on hold, no active call

- signal: Signal Strength indicator, where:

  <value>= ranges from 0 to 5

- roam: Roaming status indicator, where:

  <value>=0 means roaming is not active

  <value>=1 means a roaming is active

- battchg: Battery Charge indicator of AG, where:

  <value>=ranges from 0 to 5

- **+CIND**

  Standard list of current phone indicators. Refer to section 8.9 in [2].

- **AT+CLCC**

  Standard list current calls command. Refer to section 7.18 in [2].

- **+CLCC**

  Standard list current calls result code. Refer to section 7.18 in [2].

[3] This status indicator is not defined in the GSM 07.07 specification

Supported parameters are as follows:

- ❖ idx= The numbering (starting with 1) of the call given by the sequence of setting up or receiving the calls (active, held or waiting) as seen by the served subscriber. Calls hold their number until they are released. New calls take the lowest available number.
- ❖ dir= 0 (outgoing), 1 (incoming)
- ❖ status= 0 = Active
  1 = Held
  2 = Dialing (outgoing calls only)
  3 = Alerting (outgoing calls only)
  4 = Incoming (incoming calls only)
  5 = Waiting (incoming calls only)
- ❖ mode= 0 (Voice), 1 (Data), 2 (FAX)
- ❖ mpty= 0 (Not Multiparty), 1 (Multiparty)
- ❖ number (optional)
- ❖ type (optional)

- **AT+COPS**

The AT+COPS=3,0 shall be sent by the HF to the AG prior to sending the AT+COPS? command. AT+COPS=3,0 sets the format of the network operator string to the long format alphanumeric.

The AT+COPS? command is used for reading network operator. This profile shall only support the "reading" of the name of the network operator. The response to this command from the AG shall return a +COPS:<mode>,<format>,<operator> where:

<mode> contains the current mode and provides no information with regard to the name of the operator.

<format> specifies the format of the <operator> parameter string, and shall always be 0 for this specification.

<operator> specifies a quoted string in alphanumeric format representing the name of the network operator. This string shall not exceed 16 characters. Refer to Section 7.3 in [2].

- **AT+CMEE**

Standard AT command used to enable the use of result code +CME ERROR: <err> as an indication of an error relating to the functionality of the AG.

The set command AT+CMEE=1 is covered in this specification.

- **+CME ERROR**

This is the Extended Audio Gateway Error Result Code response. Format of the response is: +CME ERROR: <err>. The format of <err> shall be numeric in this specification. The possible values for <err> covered in this specification are described below. These error codes may be provided instead of the standard ERROR response code to provide additional information to the HF. The ERROR response code is still allowed while using the Extended Audio Gateway Error Result Codes.

+CME ERROR: 0 – AG failure
+CME ERROR: 1 – no connection to phone
+CME ERROR: 3 – operation not allowed
+CME ERROR: 4 – operation not supported
+CME ERROR: 5 – PH-SIM PIN required
+CME ERROR: 10 – SIM not inserted
+CME ERROR: 11 – SIM PIN required
+CME ERROR: 12 – SIM PUK required
+CME ERROR: 13 – SIM failure
+CME ERROR: 14 – SIM busy
+CME ERROR: 16 – incorrect password
+CME ERROR: 17 – SIM PIN2 required
+CME ERROR: 18 – SIM PUK2 required
+CME ERROR: 20 – memory full
+CME ERROR: 21 – invalid index
+CME ERROR: 23 – memory failure
+CME ERROR: 24 – text string too long
+CME ERROR: 25 – invalid characters in text string
+CME ERROR: 26 – dial string too long
+CME ERROR: 27 – invalid characters in dial string
+CME ERROR: 30 – no network service
+CME ERROR: 32 – Network not allowed – Emergency calls only

- **AT+CLIP**

  Standard “Calling Line Identification notification” activation AT command. It enables/disables the Calling Line Identification notification unsolicited result code +CLIP. Refer to Section 7.6 in [2].

- **+CLIP**

  Standard “Calling Line Identification notification” unsolicited result code.

  In the +CLIP: <number>, type> [,<subaddr>,<satype> [,[<alpha>] [,<CLI validity>]]] result code. Only <number> and <type> parameters are covered in this specification. Other parameters are not considered relevant in this specification and shall be ignored by the HF.

  The <number> parameter shall be a text string and shall always be contained within double-quotes.

  The <type> field specifies the format of the phone number provided, and can be one of the following values:

  - values 128-143: The phone number format may be a national or international format, and may contain prefix and/or escape digits. No changes on the number presentation are required.

- values 144-159: The phone number format is an international number, including the country code prefix. If the plus sign ("+") is not included as part of the number and shall be added by the AG as needed.
- values 160-175: National number. No prefix nor escape digits included.

  Refer to Section 7.11 in [2].

- **AT+CMER**

  AT+CMER

  Standard event reporting activation/deactivation AT command.

  In the AT+CMER=[<mode>[,<keyp>[,<disp>[,<ind> [,<bfr>]]]]] command, only the <mode>, and <ind> parameters are relevant for this specification. Only their values <mode>=(0,3) and <ind>=(0,1) are covered in this specification. Refer to Section 8.10 in [2].

  The following examples show how the AT+CMER command may be used for activating or deactivating the “indicator events reporting” result code:

  AT+CMER=3,0,0,1 activates “indicator events reporting”.

  AT+CMER=3,0,0,0 deactivates “indicator events reporting”.

- **+CIEV**

  Standard “indicator events reporting” unsolicited result code.

  In the +CIEV: <ind>,<value> result code, only the indicators stated in the AT+CIND command above are relevant for this specification where:

  - <ind>: Order index of the indicator within the list retrieved from the AG with the AT+CIND=? command. The first element of the list shall have <ind>=1.
  - <value>: current status of the indicator.

  If the HF receives any unknown indicator or value, it shall ignore it.

  Refer to Section 8.10 in [2].

- **AT+VTS**

  Standard DTMF generation AT command. Only the AT+VTS=<DTMF> command format is covered in this specification.

  Refer to Annex C.2.11 in [2].

- **AT+CNUM**

  Syntax: AT+CNUM (Retrieve Subscriber Number Information)
  AT+CNUM=? (Test Subscriber Number Information – Not Implemented)

  Description:

  Command issued by HF for the “Subscriber Number Information” feature in the AG.

  Only the action command AT+CNUM format is used.

- **+CNUM**

Syntax: +CNUM: [<alpha>],<number>, <type>,[<speed>] ,<service> (Response for AT+CNUM)

Description:

Standard Response used for sending the “Subscriber Number Information” from AG to HF.

The AG shall send the +CNUM: response for the AT+CNUM from the HF.

Values:

-<alpha>: This optional field is not supported, and shall be left blank.

-<number>: Quoted string containing the phone number in the format specified by <type>.

-<type> field specifies the format of the phone number provided, and can be one of the following values:

- values 128-143: The phone number format may be a national or international format, and may contain prefix and/or escape digits. No changes on the number presentation are required.

- values 144-159: The phone number format is an international number, including the country code prefix. If the plus sign ("+") is not included as part of the number and shall be added by the AG as needed.

- values 160-175: National number. No prefix nor escape digits included.

-<speed>: This optional field is not supported, and shall be left blank.

-<service>: Indicates which service this phone number relates to. Shall be either 4 (voice) or 5 (fax).

Example:

+CNUM: ,"5551212",129,,4

Refer to section 7.1 in [2].

4.33.3 Bluetooth Defined AT Capabilities

The GSM 07.07 [2] format and syntax rules shall be taken as the reference for these commands.

The new Bluetooth specific AT capabilities are listed below:

- **AT+BINP** *(Bluetooth INPut)*

  Syntax: AT+BINP=<datarequest>

  Expected response: +BINP: <dataresp$_1$>…<dataresp$_n$>

  Description:

  Command used for requesting some specific data input from the AG[4]. On reception of this command the AG shall perform the proper actions such that the requested information is sent back to the HF using the +BINP response.

  The type of data the HF shall expect in the <dataresp> parameter returned by the AG depends on the information requested in each case.

  Only support for execution command is mandated. Neither the read nor test commands are mandatory.

  Values:

  <datarequest>: 1, where

  1 = Phone number corresponding to the last voice tag recorded in the HF.

  <dataresp$_{1..n}$>: Data parameters returned by the AG. Their contents depends on the value of the <datarequest> parameter as follows:

<datarequest> value	<dataresp> parameters
1	<Phone number>: Phone number string (max. 32 digits). The format (type of address) of the phone number string shall conform with the rules stated in [7], sub-clause 10.5.4.7, for a value (in integer format) of the *type of address octet* of 145, if dialing string includes international access code character "+", and for a value of 129 otherwise.

- **AT+BLDN** *(Bluetooth Last Dialed Number)*

  Syntax: AT+BLDN

  Description:

[4] AT+BINP was created with future extensibility in mind. While the Hands-Free Profile only specifies a <datarequest> value of 1 (i.e. phone number), future profiles may choose to add values for <datarequest> to support the retrieval of additional data from the AG.

Command used for calling the last phone number dialed. On reception of this command, the AG shall set up a voice call to the last phone number dialed.

Only support for execution command is mandated. Neither the read nor test commands are mandatory.

- **AT+BVRA** *(Bluetooth Voice Recognition Activation)*

  Syntax: AT+BVRA=<vrec>

  Description:

  Enables/disables the voice recognition function in the AG.

  Only support for execution command is mandated. Neither the read nor test commands are mandatory.

  Values:

  <vrec>: 0, 1, entered as integer values, where

  0 = Disable Voice recognition in the AG

  1 = Enable Voice recognition in the AG

- **+BVRA** *(Bluetooth Voice Recognition Activation)*

  Syntax: +BVRA: <vrect>

  Description:

  Unsolicited result code used to notify the HF when the voice recognition function in the AG is activated/deactivated autonomously from the AG.

  The unsolicited +BVRA:1 result code shall not be sent by the AG to the HF if the corresponding voice recognition activation has been initiated by the HF. Likewise, the unsolicited +BVRA:0 result code shall not be sent by the AG to the HF if the corresponding voice recognition deactivation has been initiated by the HF, regardless of which side initiated the voice recognition activation.

  Values:

  <vrect>: 0, entered as integer value, where

  0 = Voice recognition is disabled in the AG

  1 = Voice recognition is enabled in the AG

- **AT+BRSF** *(Bluetooth Retrieve Supported Features)*

  Syntax: AT+BRSF=<HF supported features bitmap>

  Description:

  Notifies the AG of the supported features available in the HF, and requests information about the supported features in the AG. The supported features shall be represented as a decimal value.

  Values:

<HF supported features bitmap>: a decimal numeric string, which represents the value of a 32 bit unsigned integer. The 32 bit unsigned integer represents a bitmap of the supported features in the HF as follows:

Bit	Feature
0	EC and/or NR function
1	Call waiting and 3-way calling
2	CLI presentation capability
3	Voice recognition activation
4	Remote volume control
5	Enhanced call status
6	Enhanced call control
7-31	Reserved for future definition

The reserved bits [7-31] shall be initialized to Zero.

- **+BRSF** *(Bluetooth Retrieve Supported Features)*

Syntax: +BRSF: <AG supported features bitmap>

Description:

Result code sent by the AG in response to the AT+BRSF command, used to notify the HF what features are supported in the AG. The supported features shall be represented as a decimal value.

Values:

<AG supported features bitmap>: a decimal numeric string, which represents the value of a 32 bit unsigned integer. The 32 bit unsigned integer represents a bitmap of the supported features in the AG as follows:

Bit	Feature
0	Three-way calling
1	EC and/or NR function
2	Voice recognition function
3	In-band ring tone capability
4	Attach a number to a voice tag
5	Ability to reject a call
6	Enhanced call status
7	Enhanced call control
8	Extended Error Result Codes
9-31	Reserved for future definition

The reserved bits (9-31) shall be initialized to Zero.

- **AT+NREC** *(Noise Reduction and Echo Canceling)*

Syntax: AT+NREC=<nrec>

Description:

Command issued to disable any Echo Canceling and Noise Reduction functions embedded in the AG.

Only support for execution command is mandated. Neither the read nor test commands are mandatory.

Values:

<nrec>: 0, entered as integer value, where

0 = Disable EC/NR in the AG

- **AT+VGM** *(Gain of Microphone)*

Syntax: AT+VGM=<gain>

Description:

Command issued by the HF to report its current microphone gain level setting to the AG. <gain> is a decimal numeric constant, relating to a particular (implementation dependent) volume level controlled by the HF. This command does not change the microphone gain of the AG; it simply indicates the current value of the microphone gain in the HF.

Only support for execution command is mandated. Neither the read nor test commands are mandatory.

Values:

<gain>: 0 -15, entered as integer values, where

0 = Minimum gain

15 = Maximum gain

- **AT+VGS** *(Gain of Speaker)*

Syntax: AT+VGS=<gain>

Description:

Command issued by the HF to report its current speaker gain level setting to the AG. <gain> is a decimal numeric constant, relating to a particular (implementation dependent) volume level controlled by the HF. This command does not change the speaker gain of the AG; it simply indicates the current value of the speaker volume in the HF.

Only support for execution command is mandated. Neither the read nor test commands are mandatory.

Values:

<gain>: 0 -15, entered as integer values, where

0 = Minimum gain

15 = Maximum gain

- **+VGM** *(Gain of Microphone)*

Syntax: +VGM:<gain>

Description:

Unsolicited result code issued by the AG to set the microphone gain of the HF. <gain> is a decimal numeric constant, relating to a particular (implementation dependent) volume level controlled by the HF.

Due to the small inconsistency between the GSM standard ([2]) and the current Headset specification ([3]), the HF shall also accept the "**=**" symbol, in place of "**:**", as a valid separator for this unsolicited result code.

Values:

<gain>: 0 -15, integer values, where

0 = Minimum gain

15 = Maximum gain

- **+VGS** *(Gain of Speaker)*

Syntax: +VGS:<gain>

Description:

Unsolicited result code issued by the AG to set the speaker gain of the HF. <gain> is a decimal numeric constant, relating to a particular (implementation dependent) volume level controlled by the HF.

Due to the small inconsistency between the GSM 07.07 standard ([2]) and the current Headset specification ([3]), the HF shall also accept the "**=**" symbol, in place of "**:**", as valid separator for this unsolicited result code.

Values:

<gain>: 0 -15, integer values, where

0 = Minimum gain

15 = Maximum gain

- **++BSIR** *(Bluetooth Setting of In-band Ring tone)*

Syntax: +BSIR: <bsir>

Description:

Unsolicited result code issued by the AG to indicate to the HF that the in-band ring tone setting has been locally changed. The HF may react accordingly by changing its own alert method.

Values:

<bsir>: 0 = the AG provides no in-band ring tone

1 = the AG provides an in-band ring tone

- **AT+BTRH (Bluetooth Response and Hold Feature)**

Syntax: AT+BTRH=<n> (Set command)
AT+BTRH? (Read Current Status)

Description:

Command issued by the HF for the "Response and Hold" feature in the AG.
This specification defines the use of the set and read command. The AT+BTRH? command shall be used by the HF to query the current "Response and Hold" state of the AG.

Values:

<n>: 0, 1, 2 entered as integer values, where
0 = Put Incoming call on hold
1 = Accept a held incoming call
2 = Reject a held incoming call

- **+BTRH (Bluetooth Response and Hold Feature)**

Syntax: +BTRH: <n> (Response for AT+BTRH)

Description:

Result code used to notify the HF when-ever the incoming call is either put on hold or accepted or rejected. The AG shall also respond back with this response for the AT+BTRH? command from the HF.

Values:

<n>: 0,1,2 entered as integer value, where
0 = Incoming call is put on hold in the AG
1 = Held incoming call is accepted in the AG
2 = Held incoming call is rejected in the AG

5 Serial Port Profile

This profile requires compliance to the Serial Port Profile [5]. The following text together with the associated sub-clauses defines the requirements with regard to this profile in addition to the requirements as defined in the Serial Port Profile.

For the Hands-Free Profile, both the AG and the HF may initiate connection establishment. Therefore, for the purposes of reading the Serial Port Profile [5], both the AG and the HF may assume the role of Device A or B.

5.1 RFCOMM Interoperability Requirements

For the RFCOMM layer, no additions to the requirements as stated in the Serial Port Profile [5] Section 4 apply.

5.2 L2CAP Interoperability Requirements

For the L2CAP layer, no additions to the requirements as stated in the Serial Port Profile [5] Section 5 apply.

5.3 SDP Interoperability Requirements

The following service records are defined for the Hands-Free Profile. There is one service record applicable to the Hands-Free unit and another for the Audio Gateway.

The attribute “SupportedFeatures” states the features supported in each device. This attribute is not encoded as a data element sequence; it is simply a 16-bit unsigned integer. The set of features supported in each case is bit-wise defined in this attribute on a yes/no basis. The mapping between the features and their corresponding bits within the attribute is listed below in Table 5.2 for the HF and in Table 5.4 for the AG. If a device indicates support for a feature, then it shall support that feature in the manner specified by this Profile, and be subject to verification as part of the Bluetooth Qualification Program.

The codes assigned to the mnemonics used in the Value column, as well as the codes assigned to the attribute identifiers (if not specifically mentioned in the AttrID column), are listed in the Bluetooth Assigned Numbers (see URL [9]).

The values of the “SupportedFeatures” bitmap given in Table 5.2 shall be the same as the values of the Bits 0 to 4 of the AT-command AT+BRSF (see Section 4.33.3).

Item		Definition	Type	Value	Status	Default
ServiceClassIDList					M	
	ServiceClass0		UUID	Hands-Free	M	
	ServiceClass1		UUID	Generic Audio	M	
ProtocolDescriptorList					M	
	Protocol0		UUID	L2CAP	M	

Item	Definition	Type	Value	Status	Default
Protocol1		UUID	RFCOMM	M	
ProtocolSpecificParameter 0	Server Channel	Uint8	N=server channel #	M	
BluetoothProfileDescriptorList				M	
Profile0	Supported Profiles	UUID	Hands-Free	M	Hands-Free
Param0	Profile Version	Uint16	0x0105[5]	M	
ServiceName	Display-able Text name	String	*Service-provider defined*	O	“Hands-Free unit”
SupportedFeatures	Features supported	Uint16	*Device dependent*	M	0x0000

Table 5.1: Service Record for the HF

Bit position (0=LSB)	Feature	Default in HF
0	EC and/or NR function (yes/no, 1 = yes, 0 = no)	0
1	Call waiting and three way calling(yes/no, 1 = yes, 0 = no)	0
2	CLI presentation capability (yes/no, 1 = yes, 0 = no)	0
3	Voice recognition activation (yes/no, 1= yes, 0 = no)	0
4	Remote volume control (yes/no, 1 = yes, 0 = no)	0

Table 5.2: “SupportedFeatures” attribute bit mapping for the HF

The "Network" attribute states, if the AG has the capability to reject incoming calls[6]. This attribute is not encoded as a data element sequence; it is simply an 8-bit unsigned integer. The information given in the “Network” attribute shall be the same as the information given in Bit 5 of the unsolicited result code +BRSF (see Section 4.33.3). An attribute value of 0x00 is translated to a bit value of 0; an attribute value of 0x01 is translated to a bit value of 1.

The values of the “SupportedFeatures” bitmap given in Table 5.4 shall be the same as the values of the Bits 0 to 4 of the unsolicited result code +BRSF (see Section 4.33.3).

[5] Indicating version HFP 1.5.
[6] In previous versions of the Hands-Free Profile, the attribute values were called "GSM like" and "others".

Item	Definition	Type	Value	Status	Default
ServiceClassIDList				M	
ServiceClass0		UUID	AG Hands-Free	M	
ServiceClass1		UUID	Generic Audio	M	
ProtocolDescriptorList				M	
Protocol0		UUID	L2CAP	M	
Protocol1		UUID	RFCOMM	M	
ProtocolSpecificParameter0	Server Channel	Uint8	N=server channel #	M	
BluetoothProfileDescriptorList				M	
Profile0	Supported Profiles	UUID	Hands-Free	M	Hands-Free
Param0	Profile Version	Uint16	0x0105[7]	M	
ServiceName	Display-able Text name	String	*Service-provider defined*	O	"Voice gateway"
Network		Uint8	0x01 – Ability to reject a call 0x00 – No ability to reject a call	M	
SupportedFeatures	Features supported	Uint16	*Device dependent*	M	0x0009

Table 5.3: Service Record for the AG

Bit position (0=LSB)	Feature	Default in AG
0	Three-way calling (yes/no, 1 = yes, 0 = no)	1
1	EC and/or NR function (yes/no, 1 = yes, 0 = no)	0
2	Voice recognition function (yes/no, 1 = yes, 0 = no)	0
3	In-band ring tone capability (yes/no, 1 = yes, 0 = no)	1
4	Attach a phone number to a voice tag (yes/no, 1 = yes, 0 = no)	0

Table 5.4: "SupportedFeatures" attribute bit mapping for the AG

[7] Indicating version HFP 1.5

5.3.1 Interaction with Hands-Free Profile Rev 0.96 Implementations

HF implementations, which are according to the Hands-Free Profile specification Rev. 0.96, will not send the AT+BRSF command. Likewise, AG implementations, which are according to the Hands-Free Profile specification Rev. 0.96, will not be able to respond to AT+BRSF with the +BRSF unsolicited result code. Instead they will respond with ERROR.

In order to retrieve the “SupportedFeatures” information from an HF, which does not send AT+BRSF, Service Discovery should be used by the AG implementation. Whenever the “SupportedFeatures” attribute is not present in the HF service record, or if the AG does not perform the Service Discovery procedure, default values as stated in Table 5.2 shall be assumed.

In order to retrieve the “SupportedFeatures” and “Network” information from an AG, which does not send +BRSF, Service Discovery should be used by the HF implementation. Whenever the “SupportedFeatures” attribute is not present in the AG service record, or if the HF does not perform the Service Discovery procedure, default values as stated in Table 5.4 shall be assumed.

5.4 Link Manager (LM) Interoperability Requirements

The profile adopts the requirements for the Link Manager as stated in the “Serial Port Profile” [5].

Additionally this profile mandates that both the AG and HF devices shall support synchronous logical transports, subject to the requirements in Section 5.6.

5.5 Link Control (LC) Interoperability Requirements

Table 5.5 shows the changes from Link Controller requirements in the Serial Port Profile [5].

Table 5.5: Link Controller requirements

	Capability	Support in AG	Support in HF
1.	Inquiry		O
2.	Inquiry scan	O	
7	Voice CODEC		
C	CVSD	M	M

5.5.1 Class of Device

A device implementing the HF role of HFP shall set the "Audio" bit in the Service Class field. Optionally, if the HF intends to be discovered as a "Hands-Free", it may use the following values in the Class of Device field:

1. Indicate "Audio" as Major Device class.
2. Indicate “Hands-Free” as the Minor Device class.

An inquiring AG may use this information to filter the inquiry responses.

5.6 Synchronous Connection Interoperability Requirements

Synchronous connections may be realized by a SCO or by an eSCO logical transport. Only the support for SCO logical transports is mandated.

The remainder of this section relates to devices supporting eSCO logical transports. Here, “initiating” and “responding” refers to the initiating and responding (i.e. accept or reject) role in setting up the synchronous connection.

Table 5.6 defines eSCO configuration parameter sets S1, S2 and S3. HCI level parameters are given as a reference. On systems not incorporating HCI, values for LMP level eSCO parameters T_{eSCO}, W_{eSCO} and packet length shall be associated that correspond to these HCI parameters and fall into the mandatory parameter ranges for these packet types as given in the LMP specification, and the Voice Setting parameter translates into the air mode parameter of LMP.

eSCO parameter set	**S1** **“Safe Settings”**	**S2**	**S3**
Packet type	EV3	2-EV3	2-EV3
Transmit/Receive Bandwidth	8000	8000	8000
Voice_Setting (air coding)	CVSD	CVSD	CVSD
Max_Latency	0x0007 (7 ms)	0x0007 (7 ms)	0x000A (10ms)
Retransmission_Effort	0x01	0x01	0x01

Table 5.6: eSCO synchronous connections (HCI Reference parameters)

The following requirements apply to the support and use of eSCO logical transports and are based on parameter sets S1, S2 and S3:

- The device starting the request for a Synchronous Connection is known as the Initiator, the device receiving the request from the Initiator is known as the Responder. The Responder is able to accept or reject a request for eSCO transport. The Responder shall always accept a request for SCO transport.
- If support for eSCO logical transports is indicated at the Controller level, the Initiator may request the setup of an eSCO logical transport instead of SCO.
- The Initiators request for an eSCO transport may involve any configuration parameters matching the bidirectional throughput requirements of the voice codec (see section 5.5). If an HCI is supported on this device, the request for setting up a synchronous connection may include single or multiple packet types masked within the same request.
- The Responder may choose to accept or reject the request from the Initiator. It may reject the request for an eSCO transport, or may accept it with parameters that do not match the requested parameters. In this case the Initiator may retry the Synchronous Connection setup with different configuration parameters.

- If one or subsequent requests for an eSCO logical transport fails, the Initiator shall not abandon the setup of an eSCO transport without having requested eSCO using the “safe settings” S1.
- Only for HCI-based devices: if the Responder does not reject the request for an eSCO transport, the response shall include the parameters corresponding to the “safe settings” S1 when accepting a request. The Responder shall not request eSCO parameters that would inhibit the ability of the Initiator to negotiate the S1 settings.
- If the Initiator fails to establish an eSCO transport with the S1 settings, the Initiator shall request the setup of a SCO transport.
- Only for HCI-based devices: the Responder shall include the parameters for a SCO transport when accepting a request for a Synchronous Connection.

The following requirements apply if a device supports both eSCO logical transports and Enhanced Data Rate (as of Bluetooth core specification v2.0 + EDR or later).

- The Controller shall support the packet type 2-EV3, hence mandatory eSCO parameters ranges as given in the LMP specification and contained in settings S2 and S3.
- On an HCI-Responder, at least the settings S2 shall be included in the list of acceptable parameters.

6 Generic Access Profile

This section defines the support requirements for the capabilities as defined in the “Generic Access Profile” of the Core Specification.

6.1 Modes

The table shows the support status for GAP Modes in this profile.

Procedure	**Support in HF**
General discoverable mode	M
Procedure	**Support in AG**
Pairable mode	M

Table 6.1: Modes

6.2 Security Aspects

There are no changes to the security requirements as stated in the Generic Access Profile.

6.3 Idle Mode Procedures

Table 6.2 shows the support status for Idle mode procedures within this profile.

Procedure	**Support in AG**
Initiation of general inquiry	M
Initiation of general bonding	O
Initiation of dedicated bonding	O

Table 6.2: Idle mode procedures

7 References

[1] "Specification of the Bluetooth System; Core, v1.1 or later"

[2] 3GPP 27.007 v6.8.0 now supersedes and replaces ETS 300 916, "Digital cellular telecommunications system (Phase 2+); AT command set for GSM Mobile Equipment (ME) (GSM 07.07 version 7.5.0)"

http://www.3gpp.org/ftp/Specs/html-info/27007.htm

[3] "Specification of the Bluetooth System; Profiles, v1.1 or later, Headset Profile"

[4] "Specification of the Bluetooth System; Core, v1.1 or later, Generic Access Profile"

[5] "Specification of the Bluetooth System; Profiles, v1.1 or later, Serial Port Profile"

[6] "ITU-T50, Terminal Equipment and Protocols for telematic services: International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 IA5). Information technology – 7-Bit coded character set for information interchange"

[7] "Digital cellular telecommunication system (Phase 2+); Mobile radio interface layer 3 specification", (GSM 04.08 version 6.11.0)

[8] "GSM 02.30 (version 7.1.0): Digital cellular telecommunications system (Phase 2+); Man-Machine Interface (MMI) of the Mobile Station (MS)"

[9] Bluetooth Assigned Number URL is https://www.bluetooth.org/foundry/assignnumb/document/assigned_numbers

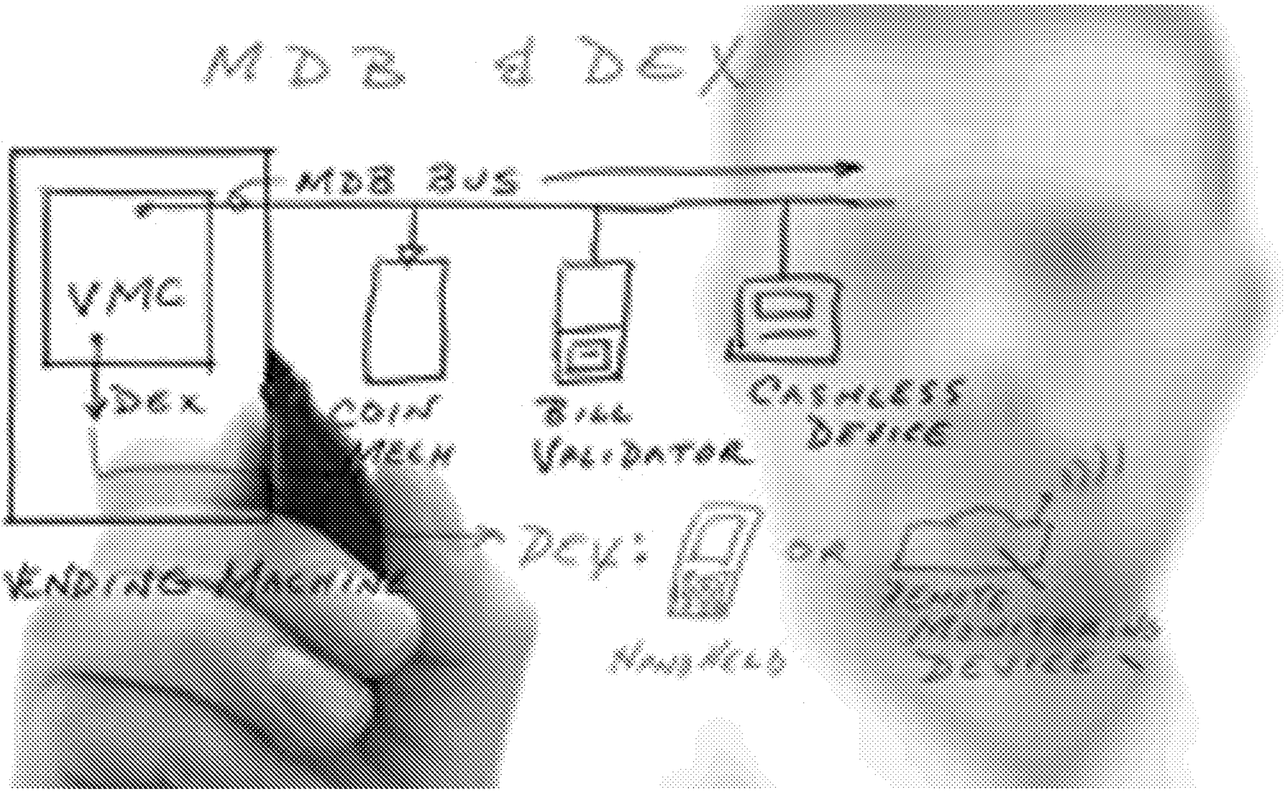
8 List of Acronyms and Abbreviations

Abbreviation or Acronym	**Meaning**
AG	Audio Gateway
AT	Attention
CLI	Calling Line Identification
CODEC	COder DECoder
CVSD	Continuous Variable Slope Delta modulation
DTMF	Dual Tone Multi-Frequency
EC	Echo Cancellation
EDR	Enhanced Data Rate
eSCO	Extended Synchronous Connection Oriented
GAP	Generic Access Profile
GSM	Global System for Mobile communication
HF	Hands-Free unit
L2CAP	Logical Link Control and Adaptation Protocol
LMP	Link Manager Protocol
NR	Noise Reduction
OSI	Open System Interconnection
PIN	Personal Identification Number
RFCOMM	Serial port transport protocol over L2CAP
SCO	Synchronous Connection Oriented
SDP	Service Discovery Protocol
UI	User Interface
UUID	Universally Unique Identifier

9 List of Figures

10 List of Tables

Vending MARKETWATCH



DEX and MDB: A Primer For Vendors

Technology Basics 101: Both technologies are important but serve different functions.

Feb 7th, 2008

Two of the most oft-mentioned and misunderstood technologies in our industry are MDB (multi-drop bus) and DEX (digital exchange). It amazes me how frequently I hear people confuse MDB and DEX, as if they are related. Allow me to end that rumor right here. The only correlation between DEX and MDB is that they are two separate and distinct technologies that happen to reside in modern day vending machines.

DEX BRINGS IMPROVED AUDIT

DEX was brought to the industry in the late 1980s to provide better audit capabilities. The bottlers brought DEX, a uniform commercial code set up across many industries, to vending when they implemented DEX for communications between a route handheld and a grocery store's computer system. Since many bottler route drivers performed direct store delivery (DSD) as well as service of can/bottle machines, it made sense for their handheld to communicate with the vending machines they serviced as well as the stores. As often happened due to their size, resources and commitment to implementing technology, the bottlers took the leadership position, and the National Automatic Merchandising Association Technology Committee (made up mostly of engineers and industry suppliers) followed suit, adopting DEX as our industry standard.

VENDING USAGE INFORMATION

So what is DEX? DEX is our standard for an ASCII code-based electronic audit file, a way to communicate information such as sales, cash in bill validators, coins in coin boxes, sales of units by selection, pricing, door openings, and much more. It is created either locally by the VMC (Vending Machine Controller often called the "brain" of an electronic machine) or created by a retrofit DEX device in older electromechanical (dip switch) machines.

DEX is the result of the VMC storing information on an interval basis (the interval of time since the last DEX reading) and cumulative basis (since the VMC was first installed or the machine went into service). The VMC accumulates the data and transmits it in DEX format (see sidebar) over the DEX port when requested.

DEX data is quite useful and extensive. It eliminates the need for route people to write what they loaded into a machine on a route card. It also makes it unnecessary to manually input this information into a handheld. But the feature of DEX that gets most companies excited and starting to "DEX" their machines is the accuracy of cash accountability. There is no more second guessing what was to be collected out of the machine.

DEX IMPROVES ROUTE ACCOUNTING

DEX data is downloaded to a handheld device or transmitted via a remote monitoring device over to software that can parse the information into useful reports. DEX is downloaded using a 0.25-inch stereo plug (exactly like the one with your old stereo headphones from the 70s). When downloaded to a handheld, DEX is parsed and compared to planogram information unique to that machine that was stored in the handheld. This informs the route driver how many units of each product he/she has to load back into the machine to bring it back up to par.

Remote monitoring devices (wireless, LAN or telephone) can forward DEX, usually via the Internet, to a central computer where the software performs the same tasks as the handheld, but from the headquarters. This gives vendors the opportunity to pre-assemble items for locations before drivers leave and efficiently pack route trucks with only the necessary products.

Approximately 60 to 70 percent of the machines currently deployed have "native" DEX, meaning the machines come with a VMC that produces DEX. Sometimes a newer version of firmware for the VMC and a DEX download cable are required to be added to enable DEX.

Older electronic and electromechanical machines not equipped with DEX can be retrofitted with either a new VMC that provides DEX (and many of the features found in new machines) or with a retrofit DEX audit device.

DEX File Interpretation Chart - View this chart in PDF format.

MULTI DROP BUS RELATES TO PAYMENT

MDB (multi drop bus) relates to the different payment systems interfacing together. When vending machines were electromechanical (using dip switches), bill validators and cashless systems had to run through the coin mechanisms. There were a slew of different connectors to interface to all the different types of coin mechs on the market, and it was very confusing since there was no industry standard. Even early electronic machines, which had VMC, didn't have standard connections. They used a serial interface (such as MicroMech), but additional devices, like bill validators or cashless systems, still had to be connected to and emulate the coin mechanisms.

If it wasn't for the NAMA and European Vending Association (EVA) getting together in the 1990s and working in a cooperative spirit to write the MDB specification, we would probably still be struggling through proprietary interfaces and the nightmare of connectors. MDB is an international standard co-authored by NAMA and EVA, and is present in almost every vending machine worldwide except for the Far East, which has its own standards.

MDB = ELECTRICAL BUS FOR INTERFACING

MDB was the first attempt by the industry to come up with a standard interface for all transactional electronic devices (i.e., coin mechanism, bill validator or cashless system) to be able to interface through an electrical bus to the VMC. This electrical bus provides one standard male and female connector, both of which are found on all MDB vending transactional electronic devices. An MDB device should have a y-MDB connection, providing for a piggyback connection from one MDB device to another.

I typically like to compare MDB to the USB port on a personal computer (PC). USB is an international electrical bus standard which supplies an electrical connection and protocol for connecting peripheral devices (such as a mouse) to a PC. Likewise, the MDB is the vending industry's international standard for providing an electrical connection with protocol for peripheral devices (in this case, an example would be a coin mech) to the VMC.

The one thing MDB does that USB doesn't do is that MDB provides sufficient power to operate the transactional device. (USB can power very low draw devices, but it wasn't designed to power most PC peripheral devices.)

When an MDB device is connected to an MDB machine, the device identifies itself to the machine as to the type of device it is (coin mech, bill validator or cashless system) and the currency for which the MDB device is programmed to receive. The VMC recognizes and enables the MDB device for operation, after which the MDB device and VMC communicate constantly.

The dialogue establishes that a machine is active for taking in currency or cashless, transmitting each activity that occurs with the MDB device, such as each occurrence of a coin being accepted into a coin mechanism; a bill being accepted into a bill validator; or a credit card, tap-and-go device or keyfob being accepted by a cashless system). The machine establishes a monetary credit and shows the credit on the display.

Since the VMC is the brains of the machine, it determines if enough credit is present in the machine to enable a vend. When a vend occurs, the VMC communicates back to the transactional device MDB to complete the transaction. For a coin mech, it means pay back change; for a bill validator, stack the bill from escrow; for a cashless device, it means transmit the vend price and transactional information over to the processor or local card server (college); and for a stored value cashless system, it means writing new stored value back to the magnetic card or smart token or keyfob.

ERROR MESSAGE COMMUNICATION

One of the very nice features of MDB is that MDB devices communicate status to the VMC. This means if there is a problem with a device, the device communicates a message to the VMC indicating the error. Examples of this are bill jams, bill stacker capacity status, coin mech problems, etc. This feature is particularly useful when used with remote data collection systems, where error messages can be forwarded to field service personnel via text messages or email.

TRACKING VENDING ACTIVITY THROUGH MDB

When MDB was originally conceived, MDB communications was limited to transaction device identification and operational communications between the device and the VMC. Information such as vend selection was not available, mainly because it is internal to the VMC and does not need to be transmitted on the MDB.

Eventually, cashless device suppliers lobbied NAMA/EVA to change the specifications for the MDB to accommodate transmission of selection information on the MDB, so that information is now available.

Some cashless and remote data communication providers choose to bypass DEX and derive audit information from MDB communications. While it is possible to derive sales and selection choices, the information produced by MDB is not as detailed as DEX, because it was never intended to be.

DEX and MDB are clearly distinct technologies. DEX allows product auditing, cash accountability and possible pre-kitting, while MDB is the means in which various transactional devices operate and communicate with the brains of the vending machine. DEX is used with a handheld unit or remote monitoring, of which the MDB is an internal component. Both DEX and MDB were meant to make it easier to deploy useful technology in vending equipment.

Source URL: https://www.vendingmarketwatch.com/home/article/10272928/dex-and-mdb-a-primer-for-vendors

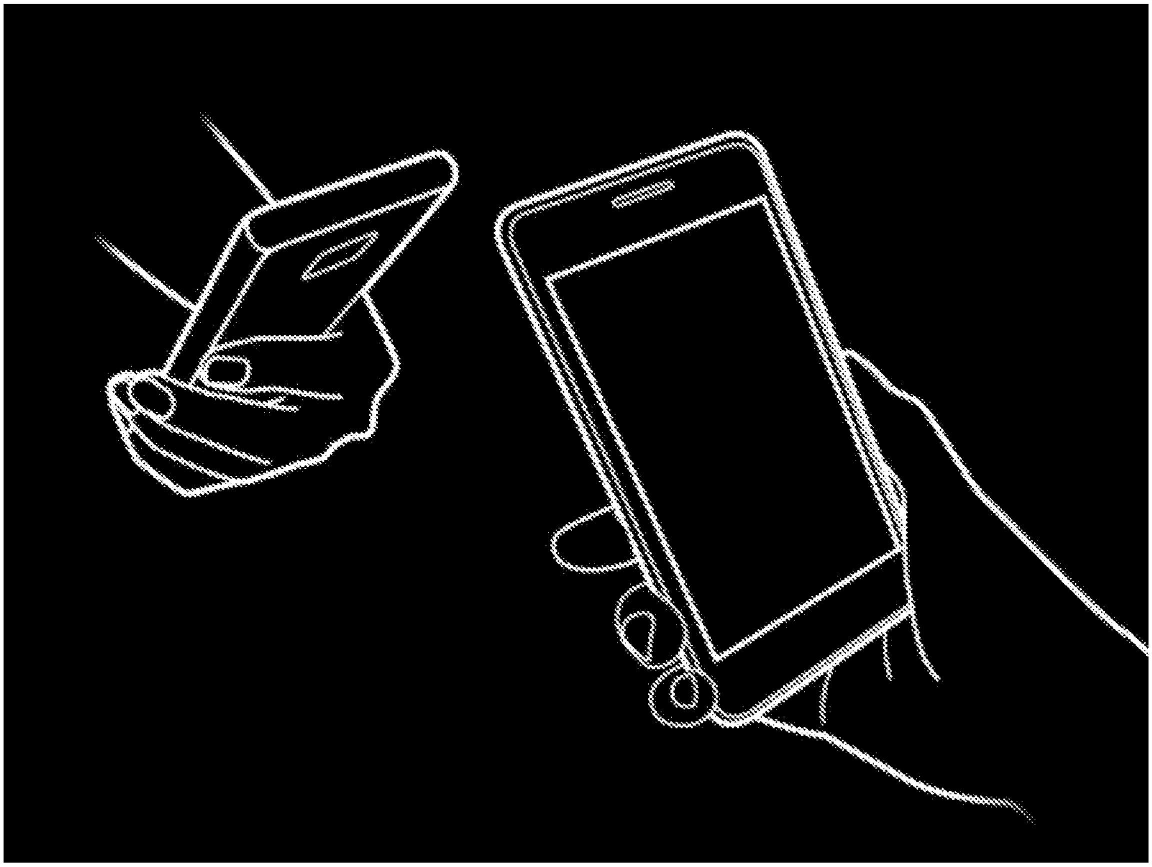
Apple TV 4K Eurovision 2021 NBA Playoffs Apple Watch 3 World's largest iceberg break free in Antarctica

BEST RE

How to use S Beam on your Samsung Galaxy S3

If you want to send large image, video or song files from one Galaxy S3 to another, Samsung has come up with S Beam. Here's how to use it.

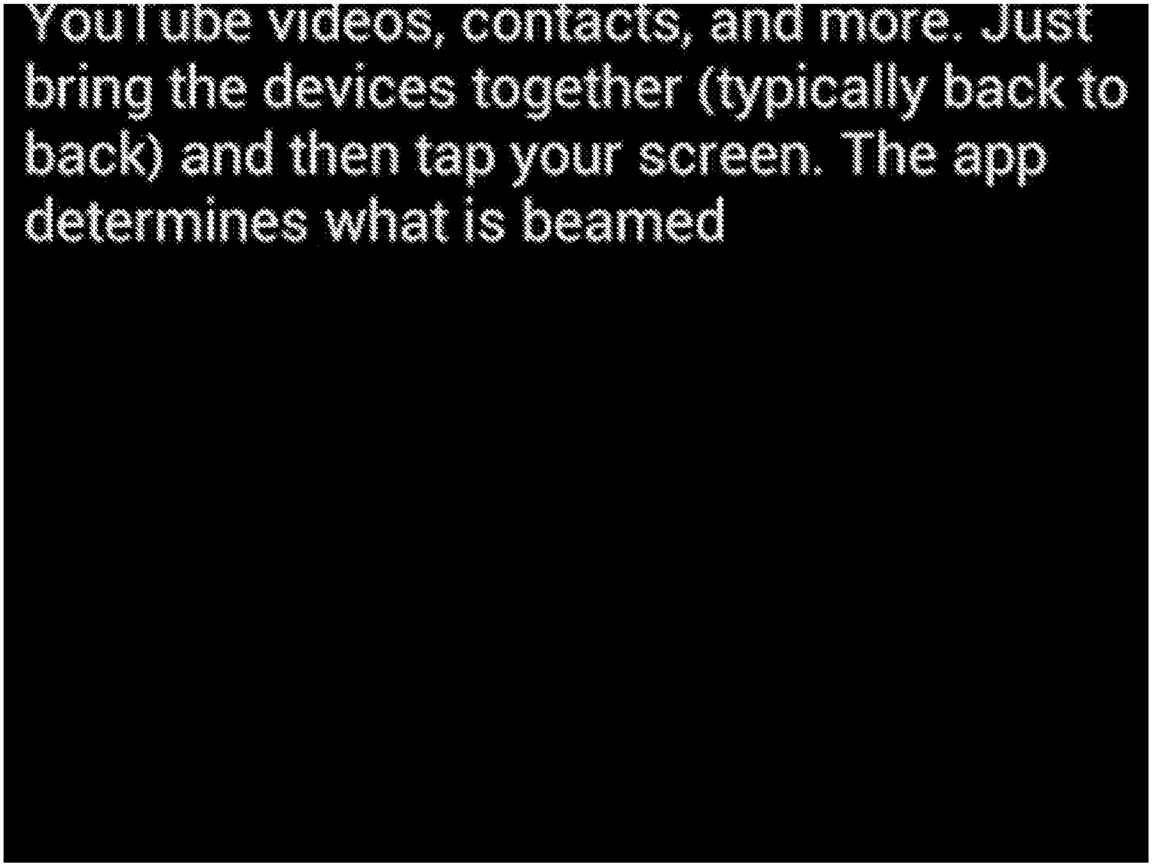
John Thompson June 21, 2012 2:07 a.m. PT



over NFC to transmit information such as contact details and browser pages from one mobile to another. But it doesn't use Wi-Fi Direct so it's impractical for larger files.

By combining NFC and Wi-Fi Direct, S Beam is capable of sending larger files between phones, such as images, videos and music tracks. The transfer is initiated by NFC and the actual file transfer is handled using Wi-Fi Direct. This means you can expect transfer speeds of up to 300MBps.

How to enable S Beam

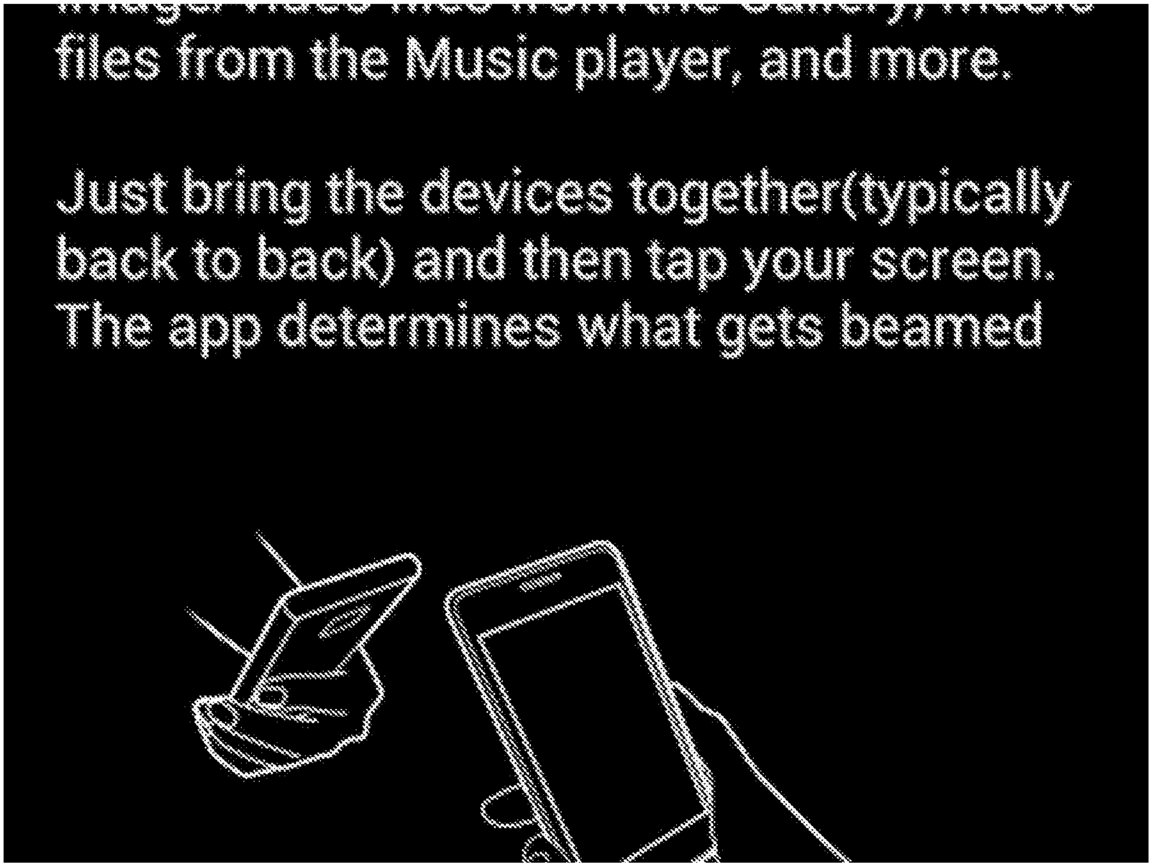


YouTube videos, contacts, and more. Just bring the devices together (typically back to back) and then tap your screen. The app determines what is beamed

You can activate both Android Beam and S Beam through the Settings app on your Galaxy S3. To do this, go to Settings > More settings, and you will see separate entries for both. Tap on each of them to ensure that they are activated.

You will need to enable NFC in the same settings window as well, as this allows the phone to transfer information with other NFC-enabled devices.

How to transfer files using S Beam



files from the Music player, and more.

Just bring the devices together(typically back to back) and then tap your screen. The app determines what gets beamed

Transferring a file between two phones couldn't be simpler. You simply navigate to the image, video or music track that you want to send and hold the back of your phone against the back of another S Beam-capable device. Your phone will tell you to 'tap to beam', and the file transfer will begin.

As the transfer uses Wi-Fi Direct, you can then take the phones away from each other and the transfer will continue uninterrupted. You don't need to be connected to the same network for this -- it all happens automatically between the phones.

At the moment, S Beam is only available on the Galaxy S3, although as Samsung continues to release more Android 4.0 devices, you will be able to transfer files in this way between more models. You can use the Android Beam functionality with any phone running Android 4.0 or later that has NFC capabilities.

Mobile Apps

How To

PRESS RELEASE
September 10, 2013

Apple Announces iPhone 5s—The Most Forward-Thinking Smartphone in the World

iPhone 5s Features 64-bit A7 chip, All-New 8 Megapixel iSight Camera with True Tone Flash & Introduces Touch ID Fingerprint Sensor

CUPERTINO, California—September 10, 2013—Apple® today announced iPhone® 5s, the most forward-thinking iPhone yet, featuring an all-new A7 chip, making iPhone 5s the world's first smartphone with 64-bit desktop-class architecture for blazing fast performance in the palm of your hand. iPhone 5s redefines the best smartphone experience in the world with amazing new features all packed into a remarkable thin and light design, including an all-new 8 megapixel iSight® camera with True Tone flash and introducing Touch ID™, an innovative way to simply and securely unlock your phone with just the touch of a finger. iPhone 5s comes with iOS 7, the most significant iOS update since the original iPhone, engineered for 64-bit technology and featuring hundreds of great new features, including Control Center, Notification Center, improved Multitasking, AirDrop®, enhanced Photos, Safari®, Siri® and iTunes Radio℠.

"iPhone 5s is the most forward-thinking smartphone in the world, delivering desktop class architecture in the palm of your hand," said Philip Schiller, Apple's senior vice president of Worldwide Marketing. "iPhone 5s sets a new standard for smartphones, packed into its beautiful and refined design are breakthrough features that really matter to people, like Touch ID, a simple and secure way to unlock your phone with just a touch of your finger."

The all-new A7 chip in iPhone 5s brings 64-bit desktop-class architecture to a smartphone for the first time. With up to twice the

CPU and graphics performance, almost everything you do on iPhone 5s is faster and better than ever, from launching apps and editing photos to playing graphic-intensive games—all while delivering great battery life. Apple also engineered iOS 7 and all the built-in apps to maximize the performance of the A7 chip. iPhone 5s is the best mobile gaming device with access to hundreds of thousands of games from the App Store℠, the A7 chip's 64-bit architecture and support for OpenGL ES version 3.0. iPhone 5s delivers incredibly rich and complex visual effects, previously only possible on Macs, PCs and gaming consoles.

Every iPhone 5s includes the new M7 motion coprocessor that gathers data from the accelerometer, gyroscope and compass to offload work from the A7 for improved power efficiency. Developers can also access new CoreMotion APIs that take advantage of M7, so they can create even better fitness and activity apps that go well beyond what other mobile devices offer. The M7 motion coprocessor continuously measures your motion data, even when the device is asleep, and saves battery life for pedometer or other fitness apps that use the accelerometer all day.

iPhone 5s introduces Touch ID, an innovative way to simply and securely unlock your iPhone with just the touch of a finger. Built into the home button, Touch ID uses a laser cut sapphire crystal, together with the capacitive touch sensor, to take a high-resolution image of your fingerprint and intelligently analyze it to provide accurate readings from any angle. Setting up Touch ID to recognize your fingerprint is easy, and every time you use it, it gets better. The Touch ID sensor recognizes the touch of a finger so the sensor is only activated when needed, preserving battery life. All fingerprint information is encrypted and stored securely in the Secure Enclave inside the A7 chip on the iPhone 5s; it's never stored on Apple servers or backed up to iCloud®. Touch ID can also be used as a secure way to approve purchases from the iTunes Store®, App Store or iBooks Store℠.

iPhone 5s makes it even easier to take great photos with the world's most popular camera. The all-new 8 megapixel iSight camera features a larger f/2.2 aperture and a new, larger sensor with 1.5µ pixels for better sensitivity and low-light performance, resulting in better pictures. These improvements, along with the Apple-designed image signal processor in the A7 chip and the new Camera app in iOS 7, provide up to two-times faster auto-focus, faster photo capture, automatic image and video stabilization, and better dynamic range. iPhone 5s introduces the new True Tone flash—the world's first for any camera—that variably adjusts color and intensity for over 1,000 combinations, so photos taken with a flash appear more natural. iPhone 5s also includes a new Burst Mode, Slo-Mo video with 120 fps, a new FaceTime® HD camera for better low-light performance and audio-only FaceTime calls with iOS 7.

iPhone 5s features a remarkable thin and light, precision-crafted design that customers around the world love, including an anodized aluminum body with diamond cut chamfered edges, a stunning 4-inch Retina® display and glass inlays. iPhone 5s is available in three gorgeous metallic finishes including gold, silver and space gray. To complement iPhone 5s, Apple designed premium leather cases in six rich colors—beige, black, blue, brown, yellow and (RED)—with soft, color-matched microfiber lining.

iPhone 5s makes it even easier to connect to high-speed networks with support for up to 13 LTE[1] wireless bands, more than any other smartphone in the world. With download speeds up to 100 Mbps[2], you can browse, download and stream content even faster. iPhone 5s includes dual-band 802.11 a/b/g/n Wi-Fi support for up to 150 Mbps[2] and Bluetooth 4.0. iPhone 5s delivers an amazing 10 hours of talk time on 3G networks, up to 10 hours of web browsing on Wi-Fi and LTE networks and up to 8 hours on 3G networks, and up to 10 hours of video playback and up to 40 hours of audio playback.[3]

iPhone 5s comes with iOS 7, the most significant iOS update since the original iPhone, engineered to support the A7 chip's 64-bit architecture, the new iSight camera and Touch ID fingerprint sensor. iOS 7 features a stunning new user interface, completely redesigned with an elegant color palette, distinct, functional layers and subtle motion that make it feel more alive. iOS 7 has hundreds of great new features, including Control Center, Notification Center, improved Multitasking, AirDrop, enhanced Photos, Safari, Siri and introduces iTunes Radio, a free Internet radio service based on the music you listen to on iTunes®.[4]

iPhone 5s customers have access to the revolutionary App Store, which offers more than 900,000 apps to iPhone, iPad® and iPod touch® users in 155 countries around the world. More than 50 billion apps have been downloaded from the App Store to date, offering customers an incredible range of apps in 23 categories, including newspapers and magazines in Newsstand, games and entertainment, business, news, sports, health and fitness and travel.

Designed specifically for iOS, iPhoto®, iMovie®, Pages®, Numbers® and Keynote® are among the most popular apps in the App Store and are now available as free downloads with the purchase of iPhone 5s. iPhoto and iMovie enable you to do more than you ever thought possible with your photos and movies, and with Pages, Numbers and Keynote you can create, edit and share stunning documents, spreadsheets and presentations on your iPhone, iPad or iPod touch.

Pricing & Availability
iPhone 5s comes in gold, silver or space gray, and will be available in the US for a suggested retail price of $199 (US) for the 16GB model and $299 (US) for the 32GB model and $399 (US) for the 64GB

model.[5] iPhone 5s will be available from the Apple Online Store (www.apple.com), Apple's retail stores, and through AT&T, Sprint, T-Mobile, Verizon Wireless and select Apple Authorized Resellers. iPhone 5s cases will be available in beige, black, blue, brown, yellow and (RED) for a suggested retail price of $39 (US) through the Apple Online Store (www.apple.com), Apple's retail stores and select Authorized Apple Resellers. iPhone 5s will be available in the US, Australia, Canada, China, France, Germany, Hong Kong, Japan, Puerto Rico, Singapore and the UK on Friday, September 20. A new iPhone 4S 8GB model will also be available for free.[5] iOS 7 will be available as a free software update starting on Wednesday, September 18 for iPhone 4 and later, iPad 2 and later, iPad mini and iPod touch (fifth generation). Some features may not be available on all products.

[1] LTE is available through select carriers. Network speeds are dependent on carrier networks, check with your carrier for details.
[2] Based on theoretical speeds, actual speeds may vary.
[3] Battery life depends on device settings, usage and other factors. Actual results vary.
[4] iTunes Radio will be available with the launch of iOS 7 in the US.
[5] For qualified customers.

Apple designs Macs, the best personal computers in the world, along with OS X, iLife, iWork and professional software. Apple leads the digital music revolution with its iPods and iTunes online store. Apple has reinvented the mobile phone with its revolutionary iPhone and App Store, and is defining the future of mobile media and computing devices with iPad.

Press Contacts:
Teresa Brewer
Apple
tbrewer@apple.com
(408) 974-6851

Natalie Kerris
Apple
nat@apple.com
(408) 974-6877

 Newsroom

The latest news and updates, direct from Apple.

Read more >

 > Newsroom > Apple Announces iPhone 5s—The Most Forward-Thinking Smartphone in the World

Shop and Learn

Mac

iPad

iPhone

Watch

TV

Music

AirPods

HomePod

iPod touch

Accessories

Gift Cards

Services

Apple Music

Apple TV+

Apple Fitness+

Apple News+

Apple Arcade

iCloud

Apple One

Apple Card

Apple Books

App Store

Account

Manage Your Apple ID

Apple Store Account

iCloud.com

Apple Store

Find a Store

Shop Online

Genius Bar

Today at Apple

Apple Camp

Apple Store App

Refurbished and Clearance

Financing

Apple Trade In

Order Status

Shopping Help

For Business

Apple and Business

Shop for Business

For Education

Apple and Education

Shop for K-12

Shop for College

For Healthcare

Apple in Healthcare

Health on Apple Watch

Health Records on iPhone

For Government

Shop for Government

Shop for Veterans and Military

Apple Values

Accessibility

Education

Environment

Inclusion and Diversity

Privacy

Racial Equity and Justice

Supplier Responsibility

About Apple

Newsroom

Apple Leadership

Job Opportunities

Investors

Events

Contact Apple

More ways to shop: Find an Apple Store or other retailer near you. Or call 1-800-MY-APPLE.

Privacy Policy | Terms of Use | Sales and Refunds | Legal | Site Map United States

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

24341 7590 10/06/2022
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
POINVIL, FRANTZY	
ART UNIT	PAPER NUMBER
3698	

DATE MAILED: 10/06/2022

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/147,305	01/12/2021	Paresh K. Patel	104402-5046-US	8393

TITLE OF INVENTION: METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	01/06/2023

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

24341 7590 10/06/2022

Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/147,305	01/12/2021	Paresh K. Patel	104402-5046-US	8393

TITLE OF INVENTION: METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	01/06/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
POINVIL, FRANTZY	3698	705-044000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1________________________

2________________________

3________________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual □ Corporation or other private group entity □ Government

4a. Fees submitted: □ Issue Fee □ Publication Fee (if required) □ Advance Order - # of Copies ________________

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

□ Electronic Payment via EFS-Web □ Enclosed check □ Non-electronic payment by credit card (Attach form PTO-2038)

□ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. __________

5. **Change in Entity Status** (from status indicated above)

□ Applicant certifying micro entity status. See 37 CFR 1.29

□ Applicant asserting small entity status. See 37 CFR 1.27

□ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature ________________________ Date ________________________

Typed or printed name ________________________ Registration No. ________________________

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/147,305	01/12/2021	Paresh K. Patel	104402-5046-US	8393

24341 7590 10/06/2022
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
POINVIL, FRANTZY	
ART UNIT	PAPER NUMBER
3698	

DATE MAILED: 10/06/2022

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	**Application No.** 17/147,305	**Applicant(s)** Patel, Paresh K.	
	Examiner FRANTZY POINVIL	**Art Unit** 3698	**AIA (FITF) Status** Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.☑ This communication is responsive to the response filed 9/15/2022.

□ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2.□ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3.☑ The allowed claim(s) is/are 2-29 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4.□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) □All b) □ Some* c) □ None of the:

1. □ Certified copies of the priority documents have been received.
2. □ Certified copies of the priority documents have been received in Application No. _____ .
3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5.□ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

□ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6.□ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1.☑ Notice of References Cited (PTO-892)

2.☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 8/30/2022; 9/22/2022.

3.□ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.

4.□ Interview Summary (PTO-413), Paper No./Mail Date. _____.

5. □ Examiner's Amendment/Comment

6. ☑ Examiner's Statement of Reasons for Allowance

7. ☑ Other IDS 8/17/2022.

/FRANTZY POINVIL/
Primary Examiner, Art Unit 3698

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Allowable Subject Matter

2. The following is an examiner's statement of reasons for allowance:

Claims 2-29 are allowable over the art of record.

The prior art taken alone or in combination failed to teach or suggest:

"detecting one or more payment accepting units in proximity to the mobile device, including detecting predefined radio transmissions broadcast by the one or more payment accepting units, wherein the one or more payment accepting units are payment operated machines that accept payment for dispensing of products and/or services, and displaying a user interface of a mobile payment application on the display of the mobile device, the user interface being configured to display a visual indication of the one or more payment accepting units and accept user input to (i) receive selection by a user of the mobile device of an available payment accepting unit of the one or more payment accepting units and (ii) trigger payment by the mobile payment application for a transaction initiated by the user of the mobile device with the available payment accepting unit of the one or more payment accepting units" as recited in independent claims 2, 16 and 23.

The above recited limitations provide meaningful limitations that transforms the abstract idea into patent eligible. Each of the independent claims as a whole effects an improvement to another technology or technical field. These limitations in combination provide meaningful limitations beyond generally linking the use of the abstract idea to a practical application.

Aument (US Patent No. 11182794 B1) discloses a payment reader and a POS terminal to communicate over a wireless connection. The methods and systems include monitoring one or more parameters corresponding to a payment reader and another device in proximity to the payment reader. The first device, through a set of customized instructions, determines whether behavior of the second device substantially corresponds to the first device, in order to detect suspected hardware or software intrusion associated with the secure first device. On successful detection of a suspected intrusion, the first device generates an alert for a user of the first device if illegal intrusion is suspected by the processor.

Silva et al (US 20160098690 A1) disclose a wireless-enabled kiosk system and associated method for recycling and performing other processes with mobile phones and other electronic devices are described herein. In various embodiments, the present technology includes systems and methods for wirelessly connecting a consumer-operated kiosk with an electronic device to facilitate processing (e.g., purchasing) the device. In some embodiments, the present technology includes using a wireless link to identify a device, evaluate a device, resolve device issues to enable purchase of the device, locate a device, etc. Various other aspects of the present technology are described herein.

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to FRANTZY POINVIL whose telephone number is (571)272-6797. The examiner can normally be reached M-Th 7:00AM to 5:30PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Anderson can be reached on 571-270-0508. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/fp/

/FRANTZY POINVIL/
Primary Examiner, Art Unit 3698

September 20, 2022

Notice of References Cited	Application/Control No. 17/147,305	Applicant(s)/Patent Under Reexamination Patel, Paresh K.
	Examiner FRANTZY POINVIL	Art Unit 3698 Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-11182794-B1	11-2021	Aument; Todd A.	G06Q20/3278	1/1
*	B	US-20200387881-A1	12-2020	Smith; Lincoln	G07C9/37	1/1
*	C	US-20180315271-A1	11-2018	Gharabegian; Armen Sevada	F03G6/001	1/1
*	D	US-20160098690-A1	04-2016	Silva; John	H04W4/80	705/21
*	E	US-9272713-B1	03-2016	Dvoskin; Daniel	B60K28/02	1/1
*	F	US-20130087050-A1	04-2013	Studor; Charles F.	A47J31/525	99/279
*	G	US-20070159994-A1	07-2007	Brown; David L.	H04W12/02	370/324
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Kumar, "Amazon gets Indian patent for auto authentication of mobile transactions", ProQuest document Id: 2433007646, Financial Express, !3 August (Year: 2020).
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				**Electronically filed December 6, 2023**	
				Application Number	18/197,071
				Filing Date	May 14, 2023
				First Named Inventor	Paresh K. Patel
				Art Unit	3698
				Examiner Name	Frantzy POINVIL
Sheet	1	of	17	Attorney Docket Number	104402-5075-US

U.S. PATENT DOCUMENTS

Examiner Initials	Cite No.	Document Number	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Number - Kind Code			
		4,374,557 A	2/22/1983	Sugimoto et al.	
		5,479,602 A	12/26/1995	Baecker et al.	
		5,844,808 A	12/1/1998	Konsmo et al.	
		5,854,994 A	12/29/1998	Canada et al.	
		5,880,733 A	3/9/1999	Horvitz et al.	
		5,892,900 A	4/6/1999	Ginter et al.	
		5,955,718 A	9/21/1999	Levasseur	
		6,056,194 A	5/2/2000	Kolls	
		6,390,269 B1	5/21/2002	Billington	
		6,462,644 B1	10/8/2002	Howell	
		6,505,095 B1	1/7/2003	Kolls	
		6,584,309 B1	6/24/2003	Whigham	
		6,594,759 B1	7/15/2003	Wang	
		6,743,095 B2	6/1/2004	Cole et al.	
		6,793,134 B2	9/21/2004	Clark	
		6,810,234 B1	10/26/2004	Rasanen	
		6,840,860 B1	1/11/2005	Okuniewicz	
		7,085,556 B2	8/1/2006	Offer	
		7,110,954 B2	9/19/2006	Yung et al.	
		7,127,236 B2	10/24/2006	Khan et al.	
		7,131,575 B1	11/7/2006	Kolls	
		7,455,223 B1	11/25/2008	Wilson	
		7,458,510 B1	12/2/2008	Zhou	
		7,464,867 B1	12/16/2008	Kolls	
		7,493,288 B2	2/17/2009	Biship et al.	
		7,672,680 B1	3/2/2010	Lee et al.	
		7,690,495 B1	4/6/2010	Kolls	
		7,721,958 B2	5/25/2010	Belfer et al.	
		7,848,980 B2	12/7/2010	Carlson	
		7,962,369 B2	6/14/2011	Rosenberg	
		7,965,693 B2	6/21/2011	Jiang et al.	
		7,983,670 B1	7/19/2011	Elliott	
		8,020,763 B1	9/20/2011	Kowalchyk	
		8,059,101 B2	11/15/2011	Westerman	
		8,157,167 B2	4/17/2012	Cost et al.	
		8,255,323 B1	8/28/2012	Casey et al.	
		D669,899 S	10/30/2012	Cheng et al.	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Substitute for Form 1449-PTO

Electronically filed December 6, 2023	
Application Number	18/197,071
Filing Date	May 14, 2023
First Named Inventor	Paresh K. Patel
Art Unit	3698
Examiner Name	Frantzy POINVIL
Attorney Docket Number	104402-5075-US

Sheet	2	of	17

		8,346,670 B2	1/1/2013	Hasson et al.	
		8,356,754 B2	1/22/2013	Johnson et al.	
		8,376,227 B2	2/19/2013	Hammad et al.	
		8,396,589 B2	3/12/2013	Katzenstein Garibaldi	
		8,412,626 B2	4/2/2013	Hirson et al.	
		8,438,066 B1	5/7/2013	Yuen	
		8,479,190 B2	7/2/2013	Sueyoshi et al.	
		8,489,140 B2	7/16/2013	Weiner et al.	
		8,514,775 B2	8/20/2013	Frecassetti et al.	
		8,517,766 B2	8/27/2013	Golko et al.	
		8,548,426 B2	10/1/2013	Smith	
		8,577,734 B2	11/5/2013	Treyz	
		8,583,496 B2	11/12/2013	You et al.	
		8,600,899 B1	12/2/2013	Davis	
		8,596,528 B2	12/3/2013	Fernandes et al.	
		8,596,529 B1	12/3/2013	Kolls	
		8,606,702 B2	12/10/2013	Ruckart	
		8,615,445 B2	12/24/2013	Dorsey et al.	
		8,645,971 B2	2/4/2014	Carlson et al.	
		8,700,530 B2	4/15/2014	Smith	
		8,707,276 B2	4/22/2014	Hill et al.	
		8,712,893 B1	4/29/2014	Brandmaier	
		8,761,809 B2	6/24/2014	Faith et al.	
		8,769,643 B1	7/1/2014	Ben Ayed	
		8,788,341 B1	7/22/2014	Patel	
		8,794,734 B2	8/5/2014	Drummond	
		8,810,430 B2	8/19/2014	Proud	
		8,819,659 B2	8/26/2014	Ramer et al.	
		8,831,677 B2	9/9/2014	Villa-Real	
		8,838,481 B2	9/16/2014	Moshfeghi	
		8,850,421 B2	9/30/2014	Proud	
		8,856,045 B1	10/7/2014	Patel et al.	
		8,881,975 B1	11/11/2014	Matthews	
		8,898,620 B2	11/25/2014	Eizenman et al.	
		8,903,737 B2	12/2/2014	Cameron et al.	
		8,958,846 B2	2/17/2015	Freeny, Jr.	
		9,001,047 B2	4/7/2015	Forstall	
		9,037,492 B2	5/19/2015	White	
		9,092,768 B2	7/28/2015	Breitenbach et al.	
		9,098,961 B1	8/4/2015	Block et al.	
		9,210,247 B2	12/8/2015	Vance et al.	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Substitute for Form 1449-PTO

Electronically filed December 6, 2023			
Application Number	18/197,071		
Filing Date	May 14, 2023		
First Named Inventor	Paresh K. Patel		
Art Unit	3698		
Examiner Name	Frantzy POINVIL		
Attorney Docket Number	104402-5075-US		

Sheet	3	of	17

		9,262,771 B1	2/16/2016	Patel	
		9,272,713 B1	3/1/2016	Dvoskin et al.	
		9,395,888 B2	7/19/2016	Schiplacoff et al.	
		9,424,603 B2	8/23/2016	Hammad	
		9,483,763 B2	11/1/2016	Van Os	
		9,547,859 B2	1/17/2017	Patel	
		9,875,473 B2	1/23/2018	Patel	
		9,898,884 B1	2/20/2018	Arora et al.	
		10,121,318 B2	11/6/2018	LeMay et al.	
		10,163,292 B1	12/25/2018	Romero	
		10,210,501 B2	2/19/2019	Low et al.	
		10,217,151 B1	2/26/2019	Greiner et al.	
		10,304,057 B1	5/28/2019	Powell	
		10,380,573 B2	8/13/2019	Lin et al.	
		10,410 194 B1	9/10/2019	Grassadonia	
		10,423,949 B2	9/24/2019	Lyons et al.	
		10,824,828 B2	11/3/2020	Ostri	
		10,977,642 B2	4/13/2021	Khan	
		11,010,759 B1	5/18/2021	Maeng	
		11,042,852 B1	6/22/2021	Wadhwa	
		11,074577 B1	7/27/2021	Soccorsy et al.	
		11,182,794 B1	11/23/2021	Aument	
		11,227,275 B2	1/18/2022	Van Heerden et al.	
		11,308,462 B2	4/19/2022	Berman et al.	
		11,373,147 B1	6/28/2022	Moore	
		2002/0016740 A1	2/7/2002	Ogasawara	
		2002/0164953 A1	11/7/2002	Curtis	
		2003/0009385 A1	1/9/2003	Tucciarone	
		2003/0089767 A1	5/15/2003	Kiyomatsu	
		2003/0101096 A1	5/29/2003	Suzuki et al.	
		2003/0110097 A1	6/12/2003	Lei	
		2003/0130902 A1	7/10/2003	Athwal	
		2003/0158891 A1	8/21/2003	Lei et al.	
		2003/0191811 A1	10/9/2003	Hashem	
		2003/0206542 A1	11/6/2003	Holder	
		2003/0236872 A1	12/25/2003	Atkinson	
		2004/0029569 A1	2/12/2004	Khan et al.	
		2004/0049454 A1	3/11/2004	Kanno et al.	
		2004/0117262 A1	6/17/2004	Berger et al.	
		2004/0122685 A1	6/24/2004	Bunce et al.	
		2004/0133653 A1	7/8/2004	Defosse	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Substitute for Form 1449-PTO

Sheet	4	of	17

Electronically filed December 6, 2023	
Application Number	18/197,071
Filing Date	May 14, 2023
First Named Inventor	Paresh K. Patel
Art Unit	3698
Examiner Name	Frantzy POINVIL
Attorney Docket Number	104402-5075-US

		2005/0021459 A1	1/27/2005	Bell	
		2005/0043011 A1	2/24/2005	Murray	
		2005/0080510 A1	4/14/2005	Bates	
		2005/0101295 A1	5/12/2005	Rupp	
		2005/0177798 A1	8/11/2005	Thomson et al.	
		2005/0181804 A1	8/18/2005	Misikangas et al.	
		2005/0232421 A1	10/20/2005	Simons et al.	
		2005/0234776 A1	10/20/2005	Jacoves	
		2006/0043175 A1	3/2/2006	Fu et al.	
		2006/0052157 A1	3/9/2006	Walker et al.	
		2006/0123335 A1	6/8/2006	Sanchez et al.	
		2007/0050083 A1	3/1/2007	Signorelli et al.	
		2007/0083287 A1	4/12/2007	Defosse et al.	
		2007/0095901 A1	5/3/2007	Illingworth	
		2007/0119680 A1	5/31/2007	Saltsov et al.	
		2007/0159994 A1	7/12/2007	Brown et al.	
		2007/0186105 A1	8/9/2007	Bailey	
		2007/0187491 A1	8/16/2007	Godwin et al.	
		2007/0227856 A1	10/4/2007	Gopel	
		2007/0255653 A1	11/1/2007	Tumminaro	
		2008/0010193 A1	1/10/2008	Rackley III. et al.	
		2008/0033880 A1	2/7/2008	Fiebiger et al.	
		2008/0040265 A1	2/14/2008	Rackley III. et al.	
		2008/0126213 A1	5/29/2008	Robertson et al.	
		2008/0141033 A1	6/12/2008	Ginter et al.	
		2008/0154727 A1	6/26/2008	Carlson	
		2008/0154735 A1	6/26/2008	Carlson	
		2008/0163257 A1	7/3/2008	Carlson et al.	
		2008/0167017 A1	7/10/2008	Wentker et al.	
		2008/0167991 A1	7/10/2008	Carlson, et al.	
		2008/0183480 A1	7/31/2008	Carlson, et al.	
		2008/0201226 A1	8/21/2008	Carlson, et al.	
		2008/0208762 A1	8/28/2008	Arthur et al.	
		2008/0249658 A1	10/9/2008	Walker	
		2008/0254853 A1	10/16/2008	Wright et al.	
		2008/0255947 A1	10/16/2008	Friedman	
		2008/0319913 A1	12/25/2008	Wiechers	
		2009/0037284 A1	2/5/2009	Lewis et al.	
		2009/0076896 A1	3/19/2009	Dewitt	
		2009/0099961 A1	4/16/2009	Ogilvy	
		2009/0106160 A1	4/23/2009	Skowronek	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				**Electronically filed December 6, 2023**
			Application Number	18/197,071
			Filing Date	May 14, 2023
			First Named Inventor	Paresh K. Patel
			Art Unit	3698
			Examiner Name	Frantzy POINVIL
Sheet	5	of	17	Attorney Docket Number 104402-5075-US

		2009/0119190 A1	5/7/2009	Realini	
		2009/0171682 A1	7/2/2009	Dixon et al.	
		2009/0306818 A1	12/10/2009	Slagley et al.	
		2009/0306819 A1	12/10/2009	Insolia	
		2009/0303982 A1	12/10/2009	Blachman et al.	
		2009/0313132 A1	12/17/2009	Kenna et al.	
		2009/0327089 A1	12/31/2009	Kanno et al.	
		2010/0061294 A1	3/11/2010	Proctor Jr	
		2010/0082485 A1	4/1/2010	Lin et al.	
		2010/0094456 A1	4/15/2010	Simpkins et al.	
		2010/0198400 A1	8/5/2010	Pascal	
		2010/0227671 A1	9/9/2010	Laaroussi et al.	
		2010/0276484 A1	11/4/2010	Banerjee	
		2010/0280956 A1	11/4/2010	Chutorash	
		2010/0312692 A1	12/9/2010	Teicher	
		2010/0320266 A1	12/23/2010	White	
		2010/0329285 A1	12/30/2010	Stanton	
		2011/0029405 A1	2/3/2011	Cronin	
		2011/0040686 A1	2/17/2011	Carlson	
		2011/0125561 A1	5/26/2011	Marcus	
		2011/0153436 A1	6/23/2011	Krampe	
		2011/0153442 A1	6/23/2011	Krampe	
		2011/0153495 A1	6/23/2011	Dixon et al.	
		2011/0172848 A1	7/14/2011	Breitenbach et al.	
		2011/0178883 A1	7/21/2011	Granbery	
		2011/0225067 A1	9/15/2011	Dunwoody	
		2011/0238476 A1	9/29/2011	Carr	
		2011/0244799 A1	10/6/2011	Roberts et al.	
		2011/0251892 A1	10/13/2011	Laracey	
		2011/0251910 A1	10/13/2011	Dimmick	
		2011/0276636 A1	11/10/2011	Cheng et al.	
		2011/0289023 A1	11/24/2011	Forster et al.	
		2012/0011024 A1	1/12/2012	Dorsey et al.	
		2012/0016731 A1	1/19/2012	Smith et al.	
		2012/0029691 A1	2/2/2012	Mockus et al.	
		2012/0030047 A1	2/2/2012	Fuentes	
		2012/0036045 A1	2/9/2012	Lowe et al.	
		2012/0066096 A1	3/15/2012	Penide	
		2012/0078735 A1	3/29/2012	Bauer et al.	
		2012/0108173 A1	5/3/2012	Hahm et al.	
		2012/0136478 A1	5/31/2012	Anand	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Substitute for Form 1449-PTO

Sheet 6 of 17

Electronically filed December 6, 2023	
Application Number	18/197,071
Filing Date	May 14, 2023
First Named Inventor	Paresh K. Patel
Art Unit	3698
Examiner Name	Frantzy POINVIL
Attorney Docket Number	104402-5075-US

		2012/0150742 A1	6/14/2012	Poon et al.	
		2012/0158172 A1	6/21/2012	Wencslao	
		2012/0158528 A1	6/21/2012	Hsu et al.	
		2012/0160912 A1	6/28/2012	Laracey	
		2012/0197740 A1	8/2/2012	Grigg et al.	
		2012/0203666 A1	8/9/2012	Torossian et al.	
		2012/0231844 A1	9/13/2012	Coppinger	
		2012/0246074 A1	9/27/2012	Annamalai et al.	
		2012/0253852 A1	10/4/2012	Pourfallah	
		2012/0254631 A1	10/4/2012	Skillman et al.	
		2012/0255653 A1	10/11/2012	Chin	
		2012/0258773 A1	10/11/2012	Alvarez Rivera	
		2012/0276845 A1	11/1/2012	Wikander	
		2012/0290472 A1	11/15/2012	Mullen et al.	
		2012/0296826 A1	11/22/2012	Bergdale et al.	
		2012/0303528 A1	11/29/2012	Weiner et al.	
		2012/0316963 A1	12/13/2012	Moshfeghi	
		2012/0330844 A1	12/27/2012	Kaufman	
		2012/0330764 A1	12/27/2012	Nahidipour	
		2013/0030931 A1	1/31/2013	Moshfeghi	
		2013/0054016 A1	2/28/2013	Canter et al.	
		2013/0054336 A1	2/28/2013	Graylin	
		2013/0054395 A1	2/28/2013	Cyr et al.	
		2013/0067365 A1	3/14/2013	Shrufi et al.	
		2013/0085835 A1	4/4/2013	Horowitz	
		2013/0087050 A1	4/11/2013	Studor et al.	
		2013/0100886 A1	4/25/2013	Cherian	
		2013/0110296 A1	5/2/2013	Khoo	
		2013/0117490 A1	5/9/2013	Harriman	
		2013/0117738 A1	5/9/2013	Livingston et al.	
		2013/0124289 A1	5/16/2013	Fisher	
		2013/0126607 A1	5/23/2013	Behjat	
		2013/0143498 A1	6/6/2013	Niemi	
		2013/0166448 A1	6/27/2013	Narayanan	
		2013/0185150 A1	7/18/2013	Crum	
		2013/0191789 A1	7/25/2013	Calman	
		2013/0217333 A1	8/22/2013	Sprigg et al.	
		2013/0246171 A1	9/19/2013	Carapelli	
		2013/0246364 A1	9/19/2013	Bhavith	
		2013/0267121 A1	10/10/2013	Hsu	
		2013/0267176 A1	10/10/2013	Hertel et al.	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				**Electronically filed December 6, 2023**	
				Application Number	18/197,071
				Filing Date	May 14, 2023
				First Named Inventor	Paresh K. Patel
				Art Unit	3698
				Examiner Name	Frantzy POINVIL
Sheet	7	of	17	Attorney Docket Number	104402-5075-US

		2013/0275303 A1	10/17/2013	Fiore	
		2013/0275305 A1	10/17/2013	Duplan	
		2013/0278622 A1	10/24/2013	Sun et al.	
		2013/0282590 A1	10/24/2013	Rajarethnam et al.	
		2013/0297422 A1	11/7/2013	Hunter et al.	
		2013/0311379 A1	11/21/2013	Smith	
		2013/0311382 A1	11/21/2013	Fosmark et al.	
		2013/0331985 A1	12/12/2013	Felique	
		2013/0332293 A1	12/12/2013	Ran	
		2013/0346305 A1	12/26/2013	Mendes	
		2014/0006451 A1	1/2/2014	Mullis et al.	
		2014/0012414 A1	1/9/2014	Pérez et al.	
		2014/0019367 A1	1/16/2014	Khan et al.	
		2014/0025958 A1	1/23/2014	Calman	
		2014/0032413 A1	1/30/2014	Low	
		2014/0032410 A1	1/30/2014	Georgiev et al.	
		2014/0040117 A1	2/2/2014	Jain	
		2014/0040028 A1	2/6/2014	King et al.	
		2014/0052524 A1	2/20/2014	Andersen	
		2014/0064116 A1	3/6/2014	Linde et al.	
		2014/0067542 A1	3/6/2014	Everingham	
		2014/0074714 A1	3/13/2014	Melone et al.	
		2014/0074723 A1	3/13/2014	Kamat	
		2014/0085046 A1	3/27/2014	Shin et al.	
		2014/0085109 A1	3/27/2014	Stefik	
		2014/0089016 A1	3/27/2014	Smullin	
		2014/0100977 A1	4/10/2014	Davis	
		2014/0122298 A1	5/1/2014	Oyer	
		2014/0136301 A1	5/15/2014	Valdes	
		2014/0136411 A1	5/15/2014	Cho	
		2014/0143055 A1	5/22/2014	Johnson	
		2014/0143074 A1	5/22/2014	Kolls	
		2014/0143137 A1	5/22/2014	Carlson	
		2014/0172179 A1	6/19/2014	Baudin	
		2014/0180852 A1	6/26/2014	Kamat	
		2014/0188708 A1	7/3/2014	Govindarajan et al.	
		2014/0108108 A1	7/17/2014	Artman	
		2014/0201066 A1	7/17/2014	Roux et al.	
		2014/0249995 A1	9/4/2014	Ogilvy	
		2014/0278989 A1	9/18/2014	Calman	
		2014/0279008 A1	9/18/2014	Calman	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				**Electronically filed December 6, 2023**
				Application Number	18/197,071
				Filing Date	May 14, 2023
				First Named Inventor	Paresh K. Patel
				Art Unit	3698
				Examiner Name	Frantzy POINVIL
Sheet	8	of	17	Attorney Docket Number	104402-5075-US

		2014/0279101 A1	9/18/2014	Duplan et al.	
		2014/0279556 A1	9/18/2014	Priebatsch	
		2014/0279537 A1	9/18/2014	Cicoretti	
		2014/0289047 A1	9/25/2014	Yee	
		2014/0317611 A1	10/23/2014	Wojcik et al.	
		2014/0324627 A1	10/30/2014	Haver	
		2014/0337235 A1	11/13/2014	Van Heerden et al.	
		2014/0351099 A1	11/27/2014	Zhu	
		2014/0361872 A1	12/11/2014	Garcia et al.	
		2014/0378057 A1	12/25/2014	Ramon et al.	
		2015/0006421 A1	1/1/2015	Pearson	
		2015/0051977 A1	2/19/2015	Lyman	
		2015/0073980 A1	3/12/2015	Griffin et al.	
		2015/0081462 A1	3/19/2015	Ozvat et al.	
		2015/0088698 A1	3/26/2015	Ackerman	
		2015/0100152 A1	4/9/2015	Trevino et al.	
		2015/0105901 A1	4/16/2015	Joshi et al.	
		2015/0120546 A1	4/30/2015	Fernandes	
		2015/0120555 A1	4/30/2015	Jung	
		2015/0149992 A1	5/28/2015	Wade et al.	
		2015/0154579 A1	6/4/2015	Teicher	
		2015/0154579 A1	6/4/2015	Teicher	
		2015/0169312 A1	6/18/2015	Patel	
		2015/0170131 A1	6/18/2015	Patel	
		2015/0170132 A1	6/25/2015	Patel	
		2015/0170136 A1	6/25/2015	Patel	
		2015/0178702 A1	6/25/2015	Patel	
		2015/0220381 A1	8/6/2015	Horagan et al.	
		2015/0235202 A1	8/20/2015	Zabala	
		2015/0235202 A1	8/20/2015	Zabala	
		2015/0278811 A1	10/1/2015	Lalchandani	
		2015/0287085 A1	10/8/2015	Windmueller	
		2015/0302377 A1	10/22/2015	Sweitzer	
		2015/0302411 A1	10/22/2015	Bondesen et al.	
		2015/0317720 A1	11/5/2015	Ramaratnam	
		2015/0332029 A1	11/19/2015	Coxe	
		2015/0346994 A1	12/3/2015	Chanyontpatanakul	
		2015/0373537 A1	12/24/2015	Toksvig	
		2016/0012465 A1	1/14/2016	Sharp	
		2016/0019604 A1	1/21/2016	Kobayashi	
		2016/0063476 A1	3/3/2016	Baldie	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				**Electronically filed December 6, 2023**	
				Application Number	18/197,071
				Filing Date	May 14, 2023
				First Named Inventor	Paresh K. Patel
				Art Unit	3698
				Examiner Name	Frantzy POINVIL
Sheet	9	of	17	Attorney Docket Number	104402-5075-US

		2016/0086145 A1	3/24/2016	Tsutsui	
		2016/0092859 A1	3/31/2016	Klingen	
		2016/0098690 A1	4/7/2016	Silvia et al.	
		2016/0132870 A1	5/12/2016	Xu et al.	
		2016/0196220 A1	7/7/2016	Perez et al.	
		2016/0232515 A1	8/11/2016	Jhas	
		2016/0292469 A1	10/6/2016	Ianni	
		2016/0335620 A1	11/17/2016	Lyons et al.	
		2016/0350744 A1	12/1/2016	Tang et al.	
		2017/0006656 A1	1/5/2017	Nacer et al.	
		2017/0193508 A1	1/13/2017	Patel et al.	
		2017/0193478 A1	7/6/2017	Dhurka	
		2017/0193479 A1	7/6/2017	Kamat	
		2017/0330164 A1	11/16/2017	Suelberg et al.	
		2018/0005220 A1	1/4/2018	Laracey	
		2018/0165908 A1	6/14/2018	Patel et al.	
		2018/0197167 A1	7/12/2018	Ganesan et al.	
		2018/0240096 A1	8/23/2018	Patel	
		2018/0276674 A1	9/27/2018	Ramatchandirane et al.	
		2018/0315271 A1	11/1/2018	Gharabegian et al.	
		2019/0236586 A1	8/1/2019	Mei et al.	
		2019/0244205 A1	8/8/2019	Fieglein	
		2019/0244465 A1	8/8/2019	Saunders et al.	
		2020/0387881 A1	12/10/2020	Smith et al.	
		20210/158309 A1	5/27/2021	Mcginlay et al.	
		2021/0357932 A1	11/18/2021	Patel	
		2023/0222506 A1	7/13/2023	Patel et al.	
		2023/0274274 A1	8/31/2023	Patel	
		2023/0289811 A1	9/14/2023	Patel et al.	
		2023/0297987 A1	9/21/2023	Patel	

FOREIGN PATENT DOCUMENTS

Examiner Initials	Cite No.	Foreign Patent Document	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		CN105139196A	12/9/2015	Shenzhen Shenruo Tech Co Ltd	
		EP1571607A2	9/7/2005	France Telecom	
		EP2061001A1	5/20/2009	Kummernuss	
		JP2002-183812A	6/28/2002	Sanyo Electric Co	
		JP2003-242401A	8/29/2003	Yoshida Sadao	
		JP2003-323662A	11/14/2003	Miyaoka Akira	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				**Electronically filed December 6, 2023**	
				Application Number	18/197,071
				Filing Date	May 14, 2023
				First Named Inventor	Paresh K. Patel
				Art Unit	3698
				Examiner Name	Frantzy POINVIL
Sheet	10	of	17	Attorney Docket Number	104402-5075-US

		JP2004-252640A	9/9/2004	Fuji Electric Retail Systems	
		JP2005-526325T	9/2/2005	Yeo Tae-Soon	
		JP2009-259226A	11/5/2009	Fuji Electric Retail Systems	
		JP2012-504273T	2/16/2012	Apple Inc.	
		WO2003/098561A1	11/27/2003	Yeo Tae-Soon	
		WO2007/015610A1	2/8/2007	Baek	
		WO2008/083022A1	7/10/2008	Visa USA Inc.	
		WO2008/083025A2	7/10/2008	Visa USA Inc.	
		WO2008/083078A2	7/10/2008	Visa USA Inc.	
		WO2008/083089A1	7/10/2008	Visa USA Inc.	
		WO2008/083105A2	7/10/2008	Visa USA Inc.	
		WO2008/083115A1	7/10/2008	Visa USA Inc.	
		WO2008/083119A1	7/10/2008	Visa USA Inc.	
		WO2009/070430A2	6/4/2009	Suridx, Inc.	
		WO2013/132995A1	9/12/2013	Sony	
		WO2013/177416A2	11/28/2013	Bush et al.	
		WO2014/093857A1	6/19/2014	Anderson et al.	
		WO2016/123545A1	8/4/2016	PayRange Inc.	
		WO2017/010936A1	1/19/2017	Tourego Global Pte Ltd	
		WO2017/143079A1	8/24/2017	PayRange Inc.	
		WO2006/020692A2	2/23/2006	Walker Digital, Llc	
		JP2010528716A	8/26/2010	CFPH, L. El. C.	
		KR20130138637A	12/19/2013	Lian Digital Co., Ltd.	
		WO2016158748A1	10/6/2016	NEC Corporation	
		CN106803175A	6/6/2017	Visa International Service Association	
		CN108352094A	9/7/2021	K. E. Pischick	
		JPH1125320A	1/29/1999	Fujitsu Ltd	
		JP2004310740A	11/4/2004	Kirin Beverage Corp, Kirin Brewery Co Ltd, Fuji Electric Retail Systems Co Ltd	
		JP4586607B2	11/24/2010	Oki Electric Industry Co Ltd	
		CN1561508A	1/5/2005	Swivel Secure Ltd.	
		EP3901880A1	10/27/2021	PayRange Inc.	
		WO2017010936A1	1/19/2017	Tie Wee TAN	

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Substitute for Form 1449-PTO

Electronically filed December 6, 2023	
Application Number	18/197,071
Filing Date	May 14, 2023
First Named Inventor	Paresh K. Patel
Art Unit	3698
Examiner Name	Frantzy POINVIL
Attorney Docket Number	104402-5075-US

Sheet	11	of	17

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published
		@RobocopyEs, posted 11OCT2014, retrieved 13FEB2018, <URL:https://twitter.com/robocopyes> 2 pgs.
		Adams, How can stationary kiosks thrive in a mobile world?, American Banker, 2012
		Balan et al., mFerio: the design and evaluation of a peer-to-peer mobile payment system, JUN2009, 14 pgs
		Balfe et al., "e-EMV: emulating EMV for internet payments with trusted computing Technologies, OCT2008, 12 pgs
		Bing, Bing Images Search: "dongle", http://www.bing.com/images/search?q=dongle&amp;FORM+HDRSC2, 05DEC2013, 8 pgs
		Carlson, Specification, US 60/871,898, 26DEC2006, 169 pgs.
		Frolick, Assessing M-Commerce Opportunities, Auerbach Publications Inc., Information Systems Management, Spring 2004
		Google, Chromecast, htttp://www.google.com/intl/devices/chromecast/, 12DEC2013, 4 pgs
		How to Pay the New Way, youtube, 05APR2018, 4 pgs.
		How will Apple's new mobile wallet Passbook impact other mobile wallets?, posted 13JUN2012, retrieved 13FEB2018 from <URL:https://www.quora.com/How-will-Apples-new-mobile-wallet-Passbook-impact-other-mobile-wallets>, 5 pgs.
		Kadambi et al., Near-Field Communication-based Secure Mobile Payment Service, AUG2009, 10 pgs.
		When the Future Feels Worse Than the Past: A Temporal Inconsistency in Moral Judgment, 15 pgs. (Year: 2010) https://citeseerx.ist.psu.edu/viewdoc/ download?doi=10.1.1.675.3584&rep=repl&type=pdf
		Novotny, Applying RFID technology in the retail industry-benefits and concerns from the consumer's perspective, Institute of Economic Science, Eszterhazy Karoly College, Eger, Hungary, Retail Technologies for the 21 Century, innovation and competitiveness in the retail industry, 2015
		Nurel, "Recent Developments in Wireless Network Systems", Izmir Institute of Technology, September 2001, 280 pages (Year: 2001).
		Patel, Office Action, US14/320,534, 02MAR2018, 26 pgs.
		Patel, Final Office Action, US14/320,534, 16APR2015, 21 pgs.
		Patel, Final Office Action, US14/320,534, 30NOV2016, 24 pgs.
		Patel, Final Office Action, US14/321,717, 18JUN2015, 22 pgs.
		Patel, Final Office Action, US14/321,724, 08OCT2015, 19 pgs.
		Patel, Final Office Action, US14/321,724, 13DEC2017, 22 pgs.
		Patel, Final Office Action, US14/321,733, 14NOV2014, 11 pgs.

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				**Electronically filed December 6, 2023**	
				Application Number	18/197,071
				Filing Date	May 14, 2023
				First Named Inventor	Paresh K. Patel
				Art Unit	3698
				Examiner Name	Frantzy POINVIL
Sheet	12	of	17	Attorney Docket Number	104402-5075-US

		Patel, Final Office Action, US14/335,762, 09JUN2016, 15 pgs.
		Patel, Final Office Action, US14/456,683, 08JUN2015, 14 pgs.
		Patel, Final Office Action, US14/458,192, 16SEP2015, 26 pgs.
		Patel, Final Office Action, US14/458,199, 24JUN2015, 8 pgs.
		Patel, Final Office Action, US14/641,236, 11MAR2016, 16 pgs.
		Patel, Final Office Action, US14/968,703, 12FEB2019, 22 pgs.
		Patel, Final Office Action, US15/435,228, 02OCT2020, 24 pgs.
		Patel, Final Office Action, US15/893,514, 22JUL2021, 12 pgs.
		Patel, Final Office Action, US15/956,741, 02OCT2020, 12 pgs.
		Patel, Notice of Allowance, US14/214,644, 10JUN2014, 9 pgs.
		Patel, Notice of Allowance, US14/321,733, 22JUN2015, 8 pgs.
		Patel, Notice of Allowance, US14/321,733, 27FEB2015, 9 pgs.
		Patel, Notice of Allowance, US14/335,762, 03OCT2016, 8 pgs.
		Patel, Notice of Allowance, US14/335,762, 30MAR2015, 9 pgs.
		Patel, Notice of Allowance, US14/456,683, 08OCT2015, 15 pgs.
		Patel, Notice of Allowance, US14/458,192, 12OCT2017, 8 pgs..
		Patel, Notice of Allowance, US14/458,199, 20JAN2017, 9 pgs.
		Patel, Notice of Allowance, US14/611,065, 26MAR2018, 18 pgs.
		Patel, Notice of Allowance, US14/614,336, 11DEC2015, 8 pgs.
		Patel, Notice of Allowance, US14/614,336, 25NOV2015, 13 pgs.
		Patel, Notice of Allowance, US14/968,703, 27JUN2019, 10 pgs..
		Patel, Notice of Allowance, US15/406,492, 11MAR2020, 10 pgs.
		Patel, Notice of Allowance, US15/435,228, 12AUG2021, 9 pgs.
		Patel, Notice of Allowance, US15/603,400, 18DEC2019, 9 pgs.
		Patel, Notice of Allowance, US15/603,400, 18JUN2020, 5 pgs.
		Patel, Notice of Allowance, US15/878,352, 23OCT2020, 9 pgs.
		Patel, Notice of Allowance, US16/029,483, 23DEC2020, 23 pgs.
		Patel, Notice of Allowance, US16/748,727, 09MAY2022, 18 pgs.
		Patel, Notice of Allowance, US16/748,727, 20JAN2022, 17 pgs.

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				**Electronically filed December 6, 2023**	
				Application Number	18/197,071
				Filing Date	May 14, 2023
				First Named Inventor	Paresh K. Patel
				Art Unit	3698
				Examiner Name	Frantzy POINVIL
Sheet	13	of	17	Attorney Docket Number	104402-5075-US

		Patel, Notice of Allowance, US16/750,477, 26JAN2022, 17 pgs.
		Patel, Notice of Allowance, US16/934,933, 31MAR2021, 9 pgs.
		Patel, Notice of Allowance, US16/681,673, 17AUG2022, 22 pgs.
		Patel, Notice of Allowability, US16/934,392, 28SEP2022, 2 pgs.
		Patel, Notice of Allowance, US17/529,111, 22SEP2022, 10 pgs.
		Patel, Notice of Allowance, US17/654,732, 16SEP2022, 9 pgs.
		Patel, Non-Final Office Action, US14/320,534, 08APR2016, 21 pgs.
		Patel, Non-Final Office Action, US14/320,534, 29OCT2014, 18 pgs.
		Patel, Non-Final Office Action, US14/321,717, 19DEC2014, 16 pgs.
		Patel, Non-Final Office Action, US14/321,724, 13MAR2017, 21 pgs.
		Patel, Non-Final Office Action, US14/321,724, 15MAY2015, 19 pgs.
		Patel, Non-Final Office Action, US14/321,733, 21AUG2014, 9 pgs.
		Patel, Non-Final Office Action, US14/335,762, 10DEC2014, 7 pgs.
		Patel, Non-Final Office Action, US14/335,762, 18SEP2015, 13 pgs.
		Patel, Non-Final Office Action, US14/456,683, 02JAN2015, 10 pgs.
		Patel, Non-Final Office Action, US14/458,192, 23MAR2017, 26 pgs.
		Patel, Non-Final Office Action, US14/458,192, 30JAN2015, 24 pgs.
		Patel, Non-Final Office Action, US14/458,199, 05JAN2015, 7 pgs.
		Patel, Non-Final Office Action, US14/458,199, 28MAR2016, 8 pgs.
		Patel, Non-Final Office Action, US14/611,065, 03OCT2016, 19 pgs.
		Patel, Non-Final Office Action, US14/611,065, 13JUN2017, 17 pgs.
		Patel, Non-Final Office Action, US14/614,336, 27MAY2015, 17 pgs.
		Patel, Non-Final Office Action, US14/641,236, 07FEB2018, 19 pgs.
		Patel, Non-Final Office Action, US14/641,236, 29MAY2015, 10 pgs.
		Patel, Non-Final Office Action, US14/968,703, 07AUG2018, 31 pgs.
		Patel, Non-Final Office Action, US15/406,492, 25JUL2019, 17 pgs.
		Patel, Non-Final Office Action, US15/435,228, 26MAR2020, 21 pgs.
		Patel, Non-Final Office Action, US15/603,400, 12JUN2019, 11 pgs.
		Patel, Non-Final Office Action, US15/878,352, 24JAN2020, 13 pgs.

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				**Electronically filed December 6, 2023**	
				Application Number	18/197,071
				Filing Date	May 14, 2023
				First Named Inventor	Paresh K. Patel
				Art Unit	3698
				Examiner Name	Frantzy POINVIL
Sheet	14	of	17	Attorney Docket Number	104402-5075-US

		Patel, Non-Final Office Action, US15/893,514, 29OCT2020, 17 pgs.
		Patel, Non-Final Office Action, US15/956,741, 22APR2020, 10 pgs.
		Patel, Non-Final Office Action, US15/956,741, 27DEC2021, 10 pgs.
		Patel, Non-Final Office Action, US16/029,483, 27APR2020, 28 pgs.
		Patel, Non-Final Office Action, US16/681,673, 24DEC2021, 21 pgs.
		Patel, Non-Final Office Action, US16/934,933, 28OCT2020, 10 pgs.
		Patel, Non-Final Office Action, US17/216,399, 08APR2022, 15 pgs.
		Patel, Non-Final Office Action, US15/893,514, 30SEP2022, 8 pgs.
		PayRange Inc., Communication Pursuant to Article 94(3), EP14828617.2, 19DEC2017, 6 pgs.
		PayRange Inc., Communication Pursuant to Article 94(3), EP16706931.9, 29JUN2018, 8 pgs.
		PayRange Inc., Communication Pursuant to Rules 161(1) and 162, EP14828617.2, 21SEP2016, 2 pgs.
		PayRange Inc., Communication Pursuant to Rules 161(1) and 162, EP16706931.9, 21SEP2017, 2 pgs.
		PayRange Inc., Communication under Rule 71(3) EPC, EP14828617.2, 19NOV2020, 7 pgs.
		PayRange Inc., Communication under Rule 71(3) EPC, EP17708929.9, 12JUN2020, 7 pgs.
		PayRange Inc., European Search Report, EP20203134.0, 01MAR2021, 7 pgs.
		PayRange Inc., European Search Report, EP21165692.1, 14SEP2021, 10 pgs.
		PayRange Inc., IPRP, PCT/US2014/071284, 21JUN2016, 6 pgs.
		PayRange Inc., IPRP, PCT/US2016/015763, 01AUG2017, 7 pgs.
		PayRange Inc., IPRP, PCT/US2017/015676, 31JUL2018, 9 pgs.
		PayRange Inc., IPRP, PCT/US2017/018194, 21AUG2018, 17 pgs.
		PayRange Inc., IPRP, PCT/US2019/060777, 11MAY2021, 7 pgs.
		PayRange Inc., ISR/WO, PCT/US2014/071284, 25MAR2015, 9 pgs.
		PayRange Inc., ISR/WO, PCT/US2016/015763, 08APR2016, 9 pgs.
		PayRange Inc., ISR/WO, PCT/US2017/015676, 18APR2017, 11 pgs.
		PayRange Inc., ISR/WO, PCT/US2017/018194, 12APR2017, 10 pgs.
		PayRange Inc., ISR/WO, PCT/US2019/060777, 06FEB2020, 11 pgs.
		PayRange Inc., ISR/WO, PCT/US2021/042632, 17NOV2021, 11 pgs.
		PayRange Inc., Notice of Reasons for Rejection, JP2017527886, 29AUG2019, 10 pgs.

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				**Electronically filed December 6, 2023**	
				Application Number	18/197,071
				Filing Date	May 14, 2023
				First Named Inventor	Paresh K. Patel
				Art Unit	3698
				Examiner Name	Frantzy POINVIL
Sheet	15	of	17	Attorney Docket Number	104402-5075-US

		PayRange Inc., Notice of Reasons for Rejection, JP2018-543707, 04SEP2020, 4 pgs.
		PayRange Inc., Notice of Reasons for Rejection, JP2020-101558, 07OCT2021, 4 pgs.
		PayRange Inc., Summons to Attend Oral Proceedings, EP14828617.2, 02APR2020, 12 pgs.
		PayRange New Product Launch, posted at youtube.com 27JUN2015, © 2016 YouTube, LLC, [online], [site visited 02MAR2016]. Available from Internet, <URL: https://www.youtube.com/watch?v=NTvvV03XFeg., 1 pg.
		Smart Vending Machine Demo at TechCrunch Disrupt 2013, posted at youtube.com 03DEC2013, © 2016 YouTube, LLC, [online], [site visited 02MAR2016]. Available from internet, URL: https://www.youtube.com/watch?v=XEz1H-gxLj8>
		Square Mobile Credit Card Processing for iPhone, iPod, iPad, posted at youtube.com, posting date 30APR2011, © 2016 YouTube, LLC, [online], [site visited 02MAR2016]. Available from internet, <URL: https://www.youtube.com/watch?v=v6sKb3CFSKw>
		Kanapaka et al., A Stochastic Game Theoretic Model for Expanding ATM Services. Https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7395687, 2015, 8 pgs.
		Patel, Notice of Allownce, US17/147,305, 06OCT2022, 9 pgs.
		Hoffman et al., "New options in Wireless payments", Internet World 7.7:37 Penton Media Inc., Penton Business Media, Inc. and their subsidiaries. (Year: 2001) 5 pgs.
		Carton et al., "Framework for Mobile Payments Integration', Electronic Journal of Information Systems Evaluation, 15.1: 14-24, Academic Conferences International Limited, January. (Year: 2012), 14 pgs.
		Apriva LLC Awarded Patent for System and Method for Facilitating a Purchase Transaction using a Customer Device Beacon, June 7, 2017, Global IP News (Year: 2017), 5 pgs.
		Kumar, "Amazon gets Indian patent for auto authentification of mobile transactions", ProQuest document Id:2433007646, Financial Express, 13 August (Year:2020), 2 pgs.
		Patel, Non-Final Office Action, US17/443,802, 23DEC2022, 14 pgs.
		Patel, Non-Final Office Action, US15/956,741, 27FEB2023, 11 pgs.
		Patel et al., Notice of Allowance, US15/893,514, 10APR2023, 13 pgs.
		Heimerl et al., “Community sourcing: Engaging Local Crowds to Perform Expert Work Via Physical Kiosks”, CHI '12: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, May 2012, Pages 1539–1548, 10 pgs. https://doi.org/10.1145/2207676.2208619
		Patel, Notice of Allowance, US17/443,802, 28JUN2023, 8 pgs.
		Patel, Corrected Notice of Allowability, US17/443,802, 10JUL2023, 5 pgs.
		Patel, Notice of Allowance, US17/983,311, 28JUN2023,10 pgs.
		EIC 3600 Search Report, STIC, Scientific & Technical Information Center, Date Completed 06/12/2023, 5 pgs.

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				**Electronically filed December 6, 2023**	
				Application Number	18/197,071
				Filing Date	May 14, 2023
				First Named Inventor	Paresh K. Patel
				Art Unit	3698
				Examiner Name	Frantzy POINVIL
Sheet	16	of	17	Attorney Docket Number	104402-5075-US

		Patel et al., Notice of Allowance, US15/893,514, 12JUL2023, 13 pgs.
		Patel et al., Notice of Allowance, US17/973,506, 26JUL2023, 13 pgs.
		Katy Jacob, "Are mobile payments the smart cards of the aughts?", Scientific and Technical Information Center, Report Information from Dialog, July 14, 2023 – 11:33, ProQuest, Publication Info: Chicago Fed Letter 240: 1-4. Federal Reserve Bank of Chicago. (Jul 2007), 9 pgs.
		Patel et al., Notice of Allowance, US17/963,170, 04AUG2023, 16 pgs.
		USA Technologies Announces Cashless Solution to Be Offered by Blackboard Inc., Scientific and Technical Information Center, Report Information from Dialog, July 25, 2023, ProQuest, Publication Info: Business Wire 18 July 2007: NA, 6 pgs.
		Hossain et al., " COMPREHENSIVE STUDY OF BLUETOOTH SIGNAL PARAMETERS FOR LOCALIZATION", Department of Electrical & Computer EngineeringNational University of Singapore, 5 pgs. Email: {g0500774, weeseng}@nus.edu.sg,
		HANDS-FREE PROFILE 1.5, Doc. No. HFP1.5_SPEC, 2005-11-25, 93 pgs.
		DEX and MDB: A Primer For Vendors | Vending Market Watch, Feb 7th, 2008, 5 pgs. https://www.vendingmarketwatch.com/print/content/10272928
		MDB Protocol V4.2 – Multi-Drop Bus – Internal Communication Protocol, MDB / ICP, Version 4.2, February 2011, 313 pgs.
		Gruber et al., "THE COMMODITY VENDING MACHINE", FORUM WARE INTERNATIONAL 2005/02, 11 pgs.
		Michael L. Kasavana, Innovative VDI Standards: Moving an Industry Forward, The Journal of International Management, Volume 4, Number 3, December 2009, 10 pgs.
		SDFL Administrative Order 2021-33, April 6, 2021, 5 pgs.
		The New York Times by David Poque, In Arrived of 2 iPhones, 3 Lessons, Sept. 17, 2013, 4 pgs. https://www./nytime.com/2013/09/18/technology/personaltech/In-Arrived-of-2-iPhones-3-Lessons.html
		Cnet, John Thompson, How to use S Beam on your Samsung Galaxy S3, June 21, 2012, 5 pgs. https://www.cnet.com/how-to/how-to-use-s-beam-on-your-samsung-galaxy-s3/
		iPhone, User Guide For iOS 6.1 Software, 156 pgs.
		Apple Reports Fourth Quarter Results, October 28, 2013, 4 pgs.
		Apple Announces iPhone 5s—The Most Forward - Thinking Smartphone in the World, September 10, 2013, 5 pgs.
		cNet, by Marguerite Reardon, Motion sensing comes to mobile phones, June 11, 2007, 4 pgs.
		Multi-Drop Bus – Internal Communication Protocol, MDB / ICP, Version 3, March 26, 2003, 270 pgs.

Examiner Signature		Date Considered	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Substitute for Form 1449-PTO				**Electronically filed December 6, 2023**	
				Application Number	18/197,071
				Filing Date	May 14, 2023
				First Named Inventor	Paresh K. Patel
				Art Unit	3698
				Examiner Name	Frantzy POINVIL
Sheet	17	of	17	Attorney Docket Number	104402-5075-US

		Weidong Kou, Payment Technologies for E-Commerce, University of Hong Kong Pokfulam Road, Hong Kong, ACM Subject Classification (1998): H.4, K.4.4, J.l, 339 pgs.
		Specification for RFID Air Interface, EPC™ Radio-Frequency Identity Protocols, Class-1 Generation-2 UHF RFID, Protocol for Communications at 860 MHz – 960 MHz, Version 1.2.0, EPCglobal Inc., 23 October 2008, 108 pgs.
		Baier et al., "Principles of Model Checking", The MIT Press Cambridge, Massachusetts, London, England, 2008, 994 pgs.
		Patel, Notice of Allowance, US17/983,311, 04OCT2023,11 pgs.
		Patel, Non-Final Office Action, US18/197,070, 27SEP2023, 8 pgs.

Examiner Signature		Date Considered	

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

24341 7590 09/22/2022
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
HOLLY, JOHN H	
ART UNIT	PAPER NUMBER
3696	

DATE MAILED: 09/22/2022

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/529,111	11/17/2021	PARESH K. PATEL	104402-5056-US	6900

TITLE OF INVENTION: SYSTEMS AND METHODS FOR DETERMINING ELECTRIC PULSES TO PROVIDE TO AN UNATTENDED MACHINE BASED ON REMOTELY-CONFIGURED OPTIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	12/22/2022

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to:
Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

24341 7590 09/22/2022

Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/529,111	11/17/2021	PARESH K. PATEL	104402-5056-US	6900

TITLE OF INVENTION: SYSTEMS AND METHODS FOR DETERMINING ELECTRIC PULSES TO PROVIDE TO AN UNATTENDED MACHINE BASED ON REMOTELY-CONFIGURED OPTIONS

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$600	$0.00	$0.00	$600	12/22/2022

EXAMINER	ART UNIT	CLASS-SUBCLASS
HOLLY, JOHN H	3696	705-044000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1____________________________

2____________________________

3____________________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual □ Corporation or other private group entity □ Government

4a. Fees submitted: □Issue Fee □Publication Fee (if required) □Advance Order - # of Copies ____________________

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

□ Electronic Payment via EFS-Web □ Enclosed check □ Non-electronic payment by credit card (Attach form PTO-2038)

□ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. __________

5. **Change in Entity Status** (from status indicated above)

□ Applicant certifying micro entity status. See 37 CFR 1.29

□ Applicant asserting small entity status. See 37 CFR 1.27

□ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature ____________________________________ Date ________________________________

Typed or printed name ____________________________________ Registration No. __________________________

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/529,111	11/17/2021	PARESH K. PATEL	104402-5056-US	6900

24341 7590 09/22/2022

Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
HOLLY, JOHN H	

ART UNIT	PAPER NUMBER
3696	

DATE MAILED: 09/22/2022

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	**Application No.** 17/529,111	**Applicant(s)** PATEL, PARESH K.	
	Examiner JOHN H HOLLY	**Art Unit** 3696	**AIA (FITF) Status** Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.☑ This communication is responsive to Amendment filed August 19,2022.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2.☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3.☑ The allowed claim(s) is/are 2-31 . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4.☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) ☐All b) ☐ Some* c) ☐ None of the:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5.☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6.☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1.☑ Notice of References Cited (PTO-892)

2.☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date August 19, 2022.

3.☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.

4.☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.

5. ☐ Examiner's Amendment/Comment

6. ☑ Examiner's Statement of Reasons for Allowance

7. ☐ Other _____.

/John H. Holly/
Primary Examiner, Art Unit 3696

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

DETAILED ACTION

This communication is in response to an Amendments filed August 19, 2022.

Continued Examination Under 37 C.F.R. §1.114

A request for continued examination ("RCE") under 37 C.F.R. §1.114, including the fee set forth in 37 C.F.R. §1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 C.F.R. §1.114, and the fee set forth in 37 C.F.R. §1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on August 19, 2022 has been entered.

. Information Disclosure Statement

The Information Disclosure Statement (IDS) submitted on August 19, 2022 was filed in compliance with the provisions of 37 CFR 1.97. Accordingly, this Information Disclosure Statement is being considered by the Examiner.

Allowable Subject Matter

Claims 2 – 31 are allowed over prior art of record.

Reasons for Allowance

The following is an examiner's statement of reasons for allowance:
The prior art of record neither anticipates nor renders obvious the claimed subject matter of the instant application as a whole either taken alone or in combination, in particular, prior art of record does not teach “detecting a selection of a first user interface object that corresponds to a first option in the first set of remotely-configured options; after detecting the selection of the first user interface object, receiving, from the server, pulse information specifying a count, amplitude, shape, or interval of electric pulses to be provided to the control unit of the unattended machine by the pulse-providing device in accordance with the first option; in accordance with a determination that a trigger condition has been satisfied, sending the pulse information to the pulse-providing device; and at the pulse-providing device: receiving the pulse information; determining based on the received pulse information a signal sequence of electrical pulses to output to the control unit of the unattended machine in order to initiate a cashless operation of the unattended machine, wherein the signal sequence of electrical pulses emulates an analog signal generated by a coin receiving switch of the unattended machine, and wherein the signal sequence is characterized by the count, amplitude, shape, or interval of electric pulses specified by the pulse information; and causing the unattended machine to initiate the cashless operation by issuing the signal sequence of electrical pulses to the control unit.”.

The following prior art references have been deemed most relevant to the allowed claim(s):

The closest prior art Mordechai Teicher (Pub. # US 2010/0312692 A1) teaches a compact payment terminal for operating upon a purchase made by a customer at a retail device is provided. The customer carries a mobile communication device that includes a payment module and a communication module. The compact payment terminal includes a first interface for interfacing with the retail device, a second interface for interfacing with the mobile communication device of the customer and a processing unit connected to the first and second interface. The compact payment terminal is configured to receive, via the first interface, a payment request from the retail device, cooperate, via the second interface, with the payment module of the mobile communication device for initiating a payment transaction respective to the payment request, and selectably conduct, via the second interface and the communication module of the mobile communication device, a communication session between the processing unit and at least one server.

The closest prior art Jonathan L. Lei et al. (Pub. # US 2003/0158891 A1) teaches a wireless network system includes a server system connected to a network. An electronic device is provided having a wireless transceiver adapted to communicate via at least one of light transmission and radio frequency (RF) transmission. A portable wireless device is provided having a wireless connection to the network. The portable wireless device is adapted to communicate wirelessly with the electronic device. The electronic device communicates with the server system over the network through the portable wireless device. The electronic device may conduct real-time and/or non-real-time transactions with the server system by utilizing the portable wireless device as a communication proxy.

.

.

The arguments presented by the Applicant along with the combination of elements, such as, "determining based on the received pulse information a signal sequence of electrical pulses to output to the control unit of the unattended machine in order to initiate a cashless operation of the unattended machine, wherein the signal sequence of electrical pulses emulates an analog signal generated by a coin receiving switch of the unattended machine, and wherein the signal sequence is characterized by the count, amplitude, shape, or interval of electric pulses specified by the pulse information.".
The claimed solution is necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks and recite significantly more than an abstract idea.

Conclusion

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to John H. Holly whose telephone number is 571.270.3461. The examiner can normally be reached on MON. - FRI 10 AM - 8 PM p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Namrata Boveja can be reached on (571)-272-8105. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

/John H. Holly/
Primary Examiner, Art Unit 3696

Notice of References Cited	Application/Control No. 17/529,111	Applicant(s)/Patent Under Reexamination PATEL, PARESH K.	
	Examiner JOHN H HOLLY	Art Unit 3696	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-20100312692-A1	12-2010	TEICHER; MORDECHAI	G06Q20/3278	455/414.1
*	B	US-20030158891-A1	08-2003	Lei, Jonathan L.	G06Q20/327	709/203
	C					
	D					
	E					
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
*	U	ProQuestDialogNPL Search History
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
17/443,802	07/27/2021	Paresh K. Patel	104402-5053-US	7874

24341 7590 12/23/2022
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
HASSAN, AURANGZEB	

ART UNIT	PAPER NUMBER
2184	

NOTIFICATION DATE	DELIVERY MODE
12/23/2022	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

donald.mixon@morganlewis.com
padocketingdepartment@morganlewis.com

Office Action Summary	Application No. 17/443,802	Applicant(s) Patel, Paresh K.	
	Examiner AURANGZEB HASSAN	Art Unit 2184	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 7/27/21.
□ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)□ This action is **FINAL.** 2b) ☑ This action is non-final.

3)□ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-20 is/are pending in the application.
5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) □ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1,6-9,14-17 and 20 is/are rejected.

8) ☑ Claim(s) 2-5,10-13 and 18-19 is/are objected to.

9) □ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)□ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 7/27/21 is/are: a)☑ accepted or b)□ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
Certified copies:
a)□ All b)□ Some** c)□ None of the:
1.□ Certified copies of the priority documents have been received.
2.□ Certified copies of the priority documents have been received in Application No. _____.
3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☑ Notice of References Cited (PTO-892)

2) ☑ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b)
Paper No(s)/Mail Date 8/17/2022.

3) ☑ Interview Summary (PTO-413)
Paper No(s)/Mail Date 12/12/22.

4) □ Other: ______.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Double Patenting

2. A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process... may obtain a patent therefor..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the claims that are directed to the same invention so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

Claim 4 is rejected under 35 U.S.C. 101 as claiming the same invention as that of claim 1 of prior U.S. Patent No. 11,074,580. This is a statutory double patenting rejection.

Claim 12 is rejected under 35 U.S.C. 101 as claiming the same invention as that of claim 7 of prior U.S. Patent No. 11,074,580. This is a statutory double patenting rejection.

3. *The nonstatutory double patenting rejection* is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the “right to exclude” granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on nonstatutory double patenting provided the reference application or patent either is shown to be commonly owned with the examined application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement. See MPEP § 717.02 for applications subject to examination under the first inventor to file provisions of the AIA as explained in MPEP § 2159. See MPEP § 2146 *et seq.* for applications not subject to examination under the first inventor to file provisions of the AIA. A terminal disclaimer must be signed in compliance with 37 CFR 1.321(b).

The USPTO Internet website contains terminal disclaimer forms which may be used. Please visit www.uspto.gov/patent/patents-forms. The filing date of the application in which the form is filed determines what form (e.g., PTO/SB/25, PTO/SB/26, PTO/AIA/25, or PTO/AIA/26) should be used. A web-based eTerminal Disclaimer may be filled out completely online using web-screens. An eTerminal Disclaimer that meets all requirements is auto-processed and approved immediately upon submission. For more information about eTerminal Disclaimers, refer to www.uspto.gov/patents/process/file/efs/guidance/eTD-info-I.jsp.

Claim 1 is rejected on the ground of nonstatutory double patenting as being unpatentable over claim 1 of U.S. Patent No. 11,074,580. Although the claims at issue are not identical, they are not patentably distinct from each other because the patented claim contain all of the elements seen in the instant application and has additional details of receiving a first command at the slave interface, sending an acknowledgement and relaying the command. Broadening of claims in a child application dictates obviousness.

Claim 9 is rejected on the ground of nonstatutory double patenting as being unpatentable over claim 7 of U.S. Patent No. 11,074,580. Although the claims at issue are not identical, they are not patentably distinct from each other because the patented claim contain all of the elements seen in the instant application and has additional details of receiving a first command at the slave interface, sending an acknowledgement and relaying the command. Broadening of claims in a child application dictates obviousness.

Claim 17 is rejected on the ground of nonstatutory double patenting as being unpatentable over claim 13 of U.S. Patent No. 11,074,580. Although the claims at issue are not identical, they are not patentably distinct from each other because the patented claim contain all of the elements seen in the instant application and has additional details of receiving a first command at the slave interface, sending an acknowledgement and relaying the command. Broadening of claims in a child application dictates obviousness.

Instant Application	11074580
Claim 1	Claim 1 teachings of slave interface coupled via MDB Host interface Wireless transceiver Processor handling electronic device interaction with machine controller, peripheral device, mobile device; Validating a peripheral device request and send associated commands therein
Claim 9	Claim 7 teachings of slave interface coupled via MDB Host interface Wireless transceiver Processor handling electronic device interaction with machine controller, peripheral device, mobile device;

	Validating a peripheral device request and send associated commands therein
Claim 17	Claim 13 teachings of slave interface coupled via MDB Host interface Wireless transceiver Processor handling electronic device interaction with machine controller, peripheral device, mobile device; Validating a peripheral device request and send associated commands therein

Claim Objections

4. Claim 9 is objected to because of the following informalities: line 7 should be corrected to disclose what MDB represents. Appropriate correction is required which should be written as “a multi-drop bus (MDB)”.

Claim 17 is objected to because of the following informalities: line 7 should be corrected to disclose what MDB represents. Appropriate correction is required which should be written as “a multi-drop bus (MDB)”.

Claim Rejections - 35 USC § 103

5. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 1, 6 – 9, 14 – 17, and 20 are rejected under 35 U.S.C. 103 as being unpatentable over Ran (US Publication Number 20130332293) in view of Kolls (US Publication Number 2014/0143074).

7. As per claims 1, 9, and 17, Ran teaches an electronic device, method and medium for retrofitting a machine to provide external access to one or more electronic peripheral devices of the machine, the electronic device (212, figure 3) comprising: a slave interface (414, figure 4) configured to couple the electronic device to a machine controller (314, figure 4) of the machine via a multi-drop bus (MDB); a host interface (412, figure 4, handles the communication mechanism between the connected elements) configured to couple the electronic device to a first peripheral device (peripheral device, 318, paragraph 44) of the one or more electronic peripheral devices

of the machine, wherein the first peripheral device is configured to communicate and is decoupled from the MDB of the machine (peripheral can handle virtual tokens where not necessarily connected to the machine, paragraph 44 – 45); a wireless transceiver; one or more processors (410, figure 4); and non-transitory memory (424, figure 4) storing one or more programs to be executed by the one or more processors (310, figure 4), the one or more programs comprising instructions for: registering the electronic device as a slave to the machine controller (paragraph 44, registering the possible objects the electronic device can handle); registering the first peripheral device as a slave to the electronic device (paragraph 44, peripheral device connectivity is handled by the driver, wherein registering is seen and initiating connectivity); receiving, from a mobile device via the wireless transceiver (wireless communication with a wireless receiver requires a transceiver on the sending side, paragraphs 26 and 27), a request to access signals generated by the first peripheral device (token management received by UPOS service, paragraph 44); validating the request (paragraph 40), wherein validation of the request indicates that the mobile device is authorized, by a remote server, to access the signals generated by the first peripheral device (validating the authorization of a connected device with respect to the server); and sending a first reset command to the first peripheral device via the host interface (resetting the token upon completion event, 120, figure 1), wherein the first reset command includes a directive to update a signal destination address (step 110, figure 1) of the first peripheral device from a controller address (114, figure 1) of the machine controller to a device address of the electronic device (initialization and handling of addressing of interfaced devices to gain access to the pos system, paragraphs 22 – 25).

Ran does not explicitly disclose the MDB functionality with explicitly characterizing and registering a device as a slave.

However, Kolls teaches coupling the electronic device to the machine controller via a multi-drop bus (MDB); wherein the first peripheral device is configured to communicate via MDB protocol and is decoupled from the MDB of the machine; registering the electronic device as a slave to the machine controller; registering the first peripheral device as a slave to the electronic device (slaves characterized with MDB functionality, paragraph 166).

Ran and Kolls are analogous art because they are from the same field of endeavor of sale-based systems.

It would have been obvious to one of ordinary skill in the art before the effective filing date of the claimed invention, having the teachings of Ran and Kolls before him, to modify the characterization of Ran with that of Kolls as it would further allow for enhance connectivity and identification. The motivation for doing so would have been to enhance efficiency in the system (paragraphs 14 – 16). Therefore, it would have been obvious to combine Kolls with Ran to obtain the invention as specified in the instant claims.

8. Ran modified by the teachings of Kolls as seen in claim 1 above, as per claim 6, 14, and 20, Ran teaches a device, method, medium, wherein the instructions for registering the electronic device as a slave to the machine controller comprise instructions for: identifying the electronic device to the machine controller as the first

peripheral device; and accepting registration of the electronic device as the first peripheral device (token handling, paragraph 18, 22 – 24).

9. Ran modified by the teachings of Kolls as seen in claim 1 above, as per claim 7 and 15, Kolls teaches a device and method, wherein the first peripheral device is a coin acceptor (506, figure 5), a bill acceptor (506, figure 5), or a payment card reader (526, figure 5), and the first signal is a payment received signal (to 502, figure 5,payment management).

10. Ran modified by the teachings of Kolls as seen in claim 1 above, as per claim 8 and 16, Kolls teaches a device and method, wherein the machine is a vending machine, a parking meter, a toll booth, a laundromat washer or dryer, an arcade game, a kiosk, a photo booth, a toll booth, or a transit ticket dispensing machine (different machine functionality seen in paragraph 87).

Allowable Subject Matter

11. Claims 2 – 5, 10 – 13, 18 and 19 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Wang/Bell/Fu/Biship/Villa have teachings of mobile device payment handling and authentication with respect to a pos system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to AURANGZEB HASSAN whose telephone number is (571)272-8625. The examiner can normally be reached 7 AM to 3 PM.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Henry Tsai can be reached on 571-272-4176. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of published or unpublished applications may be obtained from Patent Center. Unpublished application information in Patent Center is available to registered users. To file and manage patent submissions in Patent Center, visit: https://patentcenter.uspto.gov. Visit https://www.uspto.gov/patents/apply/patent-center for more information about Patent Center and https://www.uspto.gov/patents/docx for information about filing in DOCX format. For additional questions, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AH

/HENRY TSAI/
Supervisory Patent Examiner, Art Unit 2184

Examiner-Initiated Interview Summary	**Application No.** 17/443,802	**Applicant(s)** Patel, Paresh K.		
	Examiner AURANGZEB HASSAN	**Art Unit** 2184	**AIA (First Inventor to File) Status** Yes	**Page** **1 of 1**

All Participants (applicant, applicants representative, PTO personnel)	**Title**	**Type**
AURANGZEB HASSAN	Examiner	Telephonic
Benjamin Pezzner	Attorney	

Date of Interview: 12 December 2022

Issues Discussed:

Other

Examiner and Applicant briefly discussed the PTAB proceedings with respect to the parent of the instant application US Patent No. 11,074580 (attached) , different art cited along with relevance, and the most recent decision by the Board to deny the petition request on 12/6/2022. Examiner noted that the decision with respect to the parent case would be considered in any claims of the instant application having the same elements therein.

☑ Attachment

/AURANGZEB HASSAN/ Examiner, Art Unit 2184	

Applicant is reminded that a complete written statement as to the substance of the interview must be made of record in the application file. It is the applicants responsibility to provide the written statement, unless the interview was initiated by the Examiner and the Examiner has indicated that a written summary will be provided. See MPEP 713.04
Please further see:
MPEP 713.04
Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews, paragraph (b)
37 CFR § 1.2 Business to be transacted in writing

Applicant recordation instructions: It is not necessary for applicant to provide a separate record of the substance of interview.

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Notice of References Cited	Application/Control No. 17/443,802	Applicant(s)/Patent Under Reexamination Patel, Paresh K.	
	Examiner AURANGZEB HASSAN	Art Unit 2184	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-6594759-B1	07-2003	Wang; Ynjiun P.	G06Q20/327	713/172
*	B	US-20050021459-A1	01-2005	Bell, John David	G07F7/08	705/40
*	C	US-20060043175-A1	03-2006	Fu; Rong Yao	G06Q20/3276	235/383
*	D	US-7493288-B2	02-2009	Biship; Fred	G07F7/0833	705/50
*	E	US-8831677-B2	09-2014	Villa-Real; Antony-Euclid C.	G07F7/0886	455/552.1
	F					
	G					
	H					
	I					
	J					
	K					
	L					
	M					

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Espacenet

Bibliographic data: CN1561508 (A) — 2005-01-05

Code identification method and system

Inventor(s): DONALD KEECH WINSTON [GB] + (KEECH WINSTON DONALD)

Applicant(s): SWIVEL TECHNOLOGIES LTD [GB] + (SWIVEL TECHNOLOGIES LTD)

Classification:
- international: ***G06Q20/00; G07F7/10; H04L9/32;*** (IPC1-7): G07F19/00; G07F7/10; H04L9/18
- cooperative: **G06F17/00 (KR); G06Q20/02 (EP, US); G06Q20/04 (EP, US); G06Q20/10 (EP, US); G06Q20/12 (EP, US); G06Q20/32 (EP, KR, US); G06Q20/322 (EP, US); G06Q20/347 (EP, US); G06Q20/382 (EP, US); G06Q20/385 (EP, US); G06Q20/388 (EP, US); G06Q20/4014 (EP, US); G06Q20/425 (EP, US); G07F7/10 (EP, US); G07F7/1075 (EP, US)**

Application number: CN20018012009 20010907

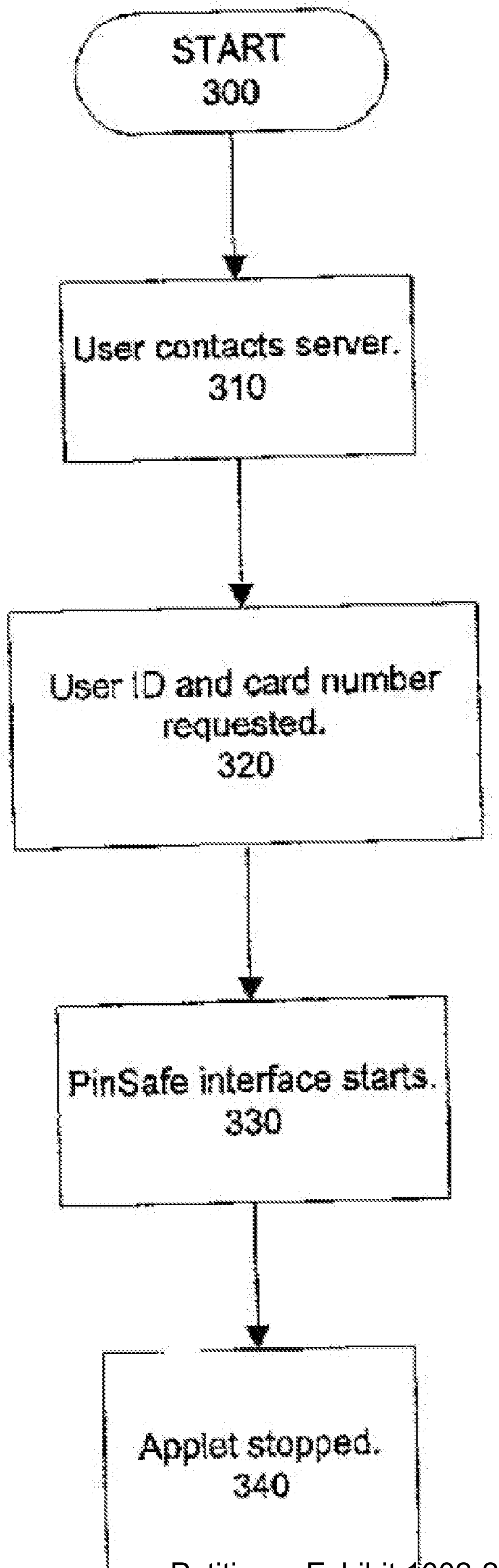
Priority number(s): GB20000021964 20000907 ; US20000663281 20000915 ; US20010915271 20010727

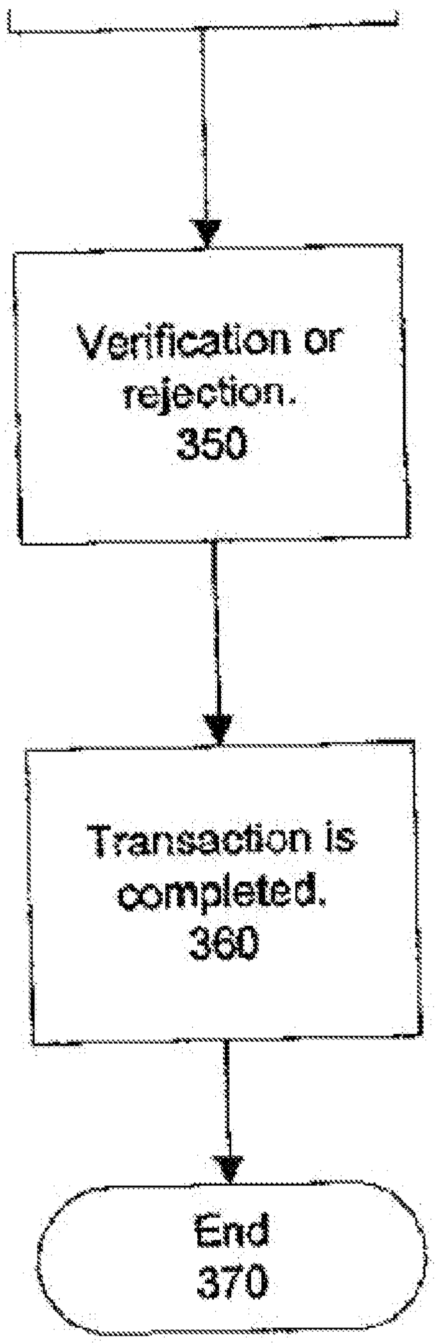
Also published as: AU2005100466 (A4) AU2005100466 (B4) AU8784701 (A) BR0113887 (A) CA2421495 (A1) CN1279498 (C) CY1113961 (T1) DK1316076 (T3) EA004422 (B1) EA200300263 (A1) EP1316076 (A2) EP1316076 (B1) ES2403039 (T3) JP2004508644 (A) KR20030036766 (A) MXPA03002050 (A) NO20030982 (L) NZ524391 (A) PT1316076 (E) US2002029342 (A1) US2002059146 (A1) US7392388 (B2) WO0221463 (A2) WO0221463 (A3) less

Abstract not available for CN1561508 (A)
Abstract of corresponding document: US2002029342 (A1)

A method and system for secure identification of a person in an electronic communications environment, wherein a host computer is adapted to be able to communicate with a plurality of electronic devices operated by the user. The user is issued with a user code, known only to the user and stored in the host computer. When the user is required to identify themselves to the host computer, the host computer generates a pseudo-random security string and applies the user code to the pseudo-random security string to generate a transaction code. The host computer also transmits the pseudo-random security string to one of the electronic devices which is

displayed by the electronic device to the user. The user applies their known user code to the displayed pseudo-random security string and determines the transaction code. The user enters the transaction code into an electronic device and the entered transaction code is then transmitted back to the host computer. Positive identification is achieved when the host computer determined transaction code matches the transaction code entered by the user. In addition, the system could employ a secure user code entry interface which would allow secure input of the user code.




Verification or rejection.
350
Transaction is completed.
360
End
370

Espacenet

Description: CN1561508 (A) — 2005-01-05

Code identification method and system

Description not available for CN1561508 (A)
Description of corresponding document: US2002029342 (A1)

A high quality text as facsimile in your desired language may be available amongst the following family members:

AU2005100466 (B4) CA2421495 (A1) DK1316076 (T3) EA200300263 (A1) ES2403039 (T3) JP2004508644 (A) KR20030036766 (A) MXPA03002050 (A) NZ524391 (A) PT1316076 (E) US2002029342 (A1) WO0221463 (A2) US2002059146 (A1)

The EPO does not accept any responsibility for the accuracy of data and information originating from other authorities than the EPO; in particular, the EPO does not guarantee that they are complete, up-to-date or fit for specific purposes.

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] The present application is a continuation-in-part of U.S. patent application Ser. No. 09/663,281, filed Sep. 15, 2000 which claims priority from U.K. Patent Application Number GB 0021964.2, filed Sep. 7, 2000, both of which are incorporated herein by reference in their entirety.

FIELD OF THE INVENTION

[0002] The present invention relates to the field of secure transactions and more specifically to the verification of a user's identity for conducting transactions.

BACKGROUND OF THE INVENTION

[0003] The present invention relates to a system and method for identifying a user or device and, optionally, for conducting transactions between the user or device and a third party, for example, by way of a telephone connection or an electronic computer system such as the Internet.

[0004] Various systems are know for conducting electronic transactions in a more or less secure manner over a telecommunications link or the like. One well known system is known as electronic funds transfer at point-of-sale (EFTPOS), in which a user is issued with a credit or debit card bearing a unique identification number, usually embossed on the card in human-readable form and also encoded on a machine-readable magnetic strip on the reverse of the card. For further identification purposes, the card typically includes a space for a user permanently to include his or her signature. In use, when a user wishes to make a purchase in, for example, a retail store, he or she presents the debit or credit card to a store employee. The card is then swiped through a card reader, and information relating to the identity of the card, the identity of the retail store and the value of the goods or services being purchases is transmitted by way of a telephone connection to a remote computer server operated by the card issuer (normally a bank or suchlike). The remote computer server checks that the user's card account contains sufficient funds or credit to cover the proposed transaction, checks that the user's card account is currently operational (for example, to check that the card has not been reported stolen), and then issues a confirmation signal back to the card reader to indicate that the transaction may be authorized. The store employee must then obtain a specimen of the user's signature and compare this with the signature on the reverse of the card so as to check the identity of the user. If the signatures appear to match, the store employee operates the card reader to complete the transaction, and the funds required to cover the transaction are then electronically transferred from the user's card account to the retail store. If the signatures do not appear to match, then the store employee may request additional proof of identification before authorizing the transaction, or may simply refuse the transaction and retain the user's card, which may have been stolen, thereby preventing any unauthorized transfer of funds. This system is open to fraudulent abuse, since it is possible for a card to be stolen and for a thief to forge the signature of an authorized user.

[0005] In a development of this system, a card user may be issued with a personal identification number (PIN), which is usually a four digit code, and which is theoretically known only to the user and to the card issuer. Instead of or in addition to providing a specimen of his or her signature at the point-of-sale, the card user is required to enter his or her PIN into the card reader, and this information is transmitted to the remote computer server together with the card and retail store identification data and data regarding the value of the transaction. By providing an extra identification check by way of the PIN, this system helps to prevent fraud by forgery of signatures, but is still not completely secure because the PIN does not change between transactions, and may therefore be intercepted together with card identification data when being transmitted between the card reader and the remote server. Furthermore, it is possible for a thief to observe a user entering his or her PIN into a card reader and to remember the PIN. If the thief is also able to obtain card identification details, for example, from a discarded till receipt or through conspiracy with the store employee, it is a simple matter to produce a fake card including all the appropriate identification information for later fraudulent use, or even to rob the authorized card user of his or her card.

[0006] The Protocol of the present invention is currently the only identity verification solution available that can be used across all platforms, using a common user interface. A number of other attempts to solve the problem of identity verification are currently available and include Public Key Infrastructure (PKI), SMART Cards, and biometrics.

[0007] A Public Key Infrastructure is a combination of hardware and software products, policies and procedures. PKI provides the basic security required to carry out electronic business so that users, who do not know each other, or are widely distributed, can communicate securely through a chain of trust. PKI is based on digital IDs known as 'digital certificates' which act like 'electronic passports' and bind the user's digital signature to his or her public key. The PKI approach is only applicable for Internet or other transactions that use a computer because the complexity of the software at the users' end of the transaction requires significant computing resources. The PKI approach is not well suited to high volume transaction processing because of this complexity.

[0008] Smart Cards are a response to the problem of credit/debit card fraud. Smart Cards are cards that have a microchip embedded within the card which enables personal details about the cardholder to be stored securely on the card, which can then be used to verify the identity of the person using the card. The Smart Card system relies upon there being a Smart Card reading apparatus at the point of sale. Currently, few high street merchants have invested in such equipment, and recent industry estimates expect a hybrid smart card/magnetic strip environment for the next 10-15 years. In addition, smaller or independent retailers find the cost of such equipment is a deterrent to uptake. Few Smart Card systems address the problem of "card not present" fraud such as e-commerce, m-commerce, interactive TV and telephone order unless the consumers invest in Smart-Card readers for the home. Similarly, any Smart Card can be copied ("skimmed/cloned") and can subsequently be used fraudulently in card not present situations. Most major card issuers have plans to roll out such Smart Cards within the next few years, although the costs of the equipment, the cards themselves and the availability of the chips may delay this process. The present invention has been designed to be able to act as a security overlay to such Smart Card systems and can make any transaction as secure as those for which the Smart Cards are designed.

[0009] A number of companies are currently developing biometric solutions to the problem of cardholder verification. The Biometric systems can use fingerprints, voice recognition, retinal scans or tissue samples to positively identify the cardholder. Similar to smart cards these biometric systems would require complex and costly equipment at the point of sale and would not provide any protection against fraud in card not present situations.

BRIEF SUMMARY OF THE INVENTION

[0010] According to a first aspect of the present invention, there is provided a coded identification system, the system comprising an electronic computer, a specific electronic communications device that is operable to be in communication with the electronic computer, and at least one electronic communications device that is operable to be in communication with the electronic computer, wherein the electronic computer includes data relating to the specific electronic communications device, including a permanent identification code, a mask code and an identification code enabling electronic communication between the electronic computer and the specific electronic communications device, and wherein the permanent identification code is input to the at least one electronic communications device and transmitted to the electronic computer, the electronic computer generates a pseudo-random string and transmits this to the specific electronic communications device, the mask code is applied to the pseudo-random string so as to generate a volatile identification code in accordance with predetermined rules, the volatile identification code is transmitted back to the electronic computer by the specific electronic communications device or the at least one electronic communications device, the electronic computer checks the volatile identification code transmitted thereto against a volatile identification code obtained by applying the mask code to the pseudo-random string in accordance with the predetermined rules, and in which a positive identification is made when the volatile identification codes are found to match by the electronic computer.

[0011] According to a second aspect of the present invention, there is provided a method for identifying a specific electronic communications device or user thereof to an electronic computer having stored therein data relating to the specific electronic communications device or user thereof, including a permanent identification code, a mask code and an identification code enabling communication between the electronic computer and the specific electronic communications device, wherein the permanent identification code is input to at least one electronic communications device and transmitted thereby to the electronic computer, the electronic computer associates the permanent identification code with the identification code enabling communications there between and the specific electronic communications device and generates a pseudo-random string before transmitting this to the specific electronic communications device, the mask code is applied to the pseudo-random string in accordance with predetermined rules so as to generate a volatile identification code, the volatile identification code is input to the specific electronic communications device or at least one electronic communications device and transmitted to the electronic computer where it is compared with a volatile identification code generated therein by applying the mask code to the pseudo-random string, and a positive identification is made when the volatile identification codes match.

[0012] The specific electronic communications device may be a separate device from the at least one electronic communications device, or may be the same device. For example, the specific electronic communications device may be a mobile telephone, a pager, a land-line telephone, a personal digital assistant or a computer which may be owned or specifically operated by a given person. The at least one electronic communications device may be an electronic funds transfer (EFT) or electronic funds transfer at point-of-sale (EFTPOS) terminal, or may be the same mobile telephone, pager, land-line telephone, personal digital assistant or computer which may be owned or specifically operated by the person as hereinbefore described.

[0013] The permanent identification code may be supplied to a user in the form of a card bearing human and/or machine-readable data.

[0014] The identification code enabling electronic communication between the electronic computer and the specific electronic communications device may be a mobile telephone or pager number where the specific electronic communications device is a mobile telephone, pager or personal digital assistant, or may be an e-mail address or similar code allowing specific communication with a given specific electronic communications device.

[0015] Where the specific electronic communications device is a mobile telephone or the like, the pseudo-random string may be transmitted in the form of a text message under the short messaging service (SMS) protocol. Other well-known communications protocols may be employed where appropriate, depending on the nature of the specific electronic communications device.

[0016] Embodiments of the present invention provide additional security of identification in a number of ways. Firstly, in addition to requiring the person to have access to the permanent identification code, the system requires the person to be in possession of an appropriate specific electronic communications device. Secondly, because the system requires the user to cause his or her mask code to operate on the pseudo-random string so as to generate a volatile identification code in accordance with the predetermined rules, without the mask code being electronically transmitted together with the permanent identification code, it is difficult for an unauthorized person to intercept communications between the electronic computer, the specific electronic communications device and/or the at least one electronic communications device so as to determine the mask code and the permanent identification code.

[0017] It will be appreciated that the present invention extends to situations where it is required to establish a secure identification of a specific electronic communications device rather than of a person as such. For example, the present invention may be used as part of a secure "hand-shaking" protocol between remote computers, serving positively and securely to identify the specific electronic communications devices, which may itself be an electronic computer, to the electronic computer. Both the electronic computer and the specific electronic communications device will have the mask code stored within their memories but will not communicate the mask code between each other except by way of a secure connection, ideally entirely separate from their normal means of communication.

[0018] The mask code may take various forms. In a currently preferred embodiment, a person is issued with or selects a four digit numerical string, for example, 3928, analogous to the well known PIN codes currently used when operating automated teller machines (ATMs). However, different lengths of mask code may be used as appropriate. The pseudo-random string (which may be numeric, alphanumeric or any other combination of characters) transmitted to the specific electronic communications device in response to a signal sent by the at least one electronic communications device is displayable thereon in a predetermined form, with the characters making up the pseudo-random string being displayed preferably as a linear array. The person operating the specific electronic communications device then takes the first digit of his or her mask code, in this example 3, and notes the character in third position (say from left to right) along the pseudo-random string. The person then takes the second digit of his or her mask code, in this example 9, and notes the character in ninth position along the pseudo-random string, and so on for the digits 2 and 8 of the mask code. The characters selected from the pseudo-random string form the volatile identification code which is then input into the at least one electronic communications device and transmitted to the electronic computer for verification. Alternatively, the volatile identification code may be transmitted to the electronic computer by way of the specific electronic communication device. If the volatile identification code received by way of the electronic computer corresponds to an expected volatile identification code calculated by the electronic computer applying the mask code to the pseudo-random string, a positive identification is take to have been made. The prime security feature is that the mask code is never transmitted between the electronic computer, the specific electronic communications device or the at least one electronic communications device, and is thus safe from interception by unauthorized third parties. The secondary security feature is that a person must be in possession of his or her own specific electronic communications device, since the electronic computer will transmit the pseudo-random strong only thereto.

[0019] For additional security, after the volatile identification code has been transmitted to the electronic computer for verification and found to match a volatile identification code generated by the electronic computer, the electronic computer may transmit a message to the specific electronic communications device requesting that the person confirms that the identification is correct. Only when the person responds affirmatively to the message by transmitting a confirmatory message from the specific electronic communications device to the electronic computer so the identification process finally completed.

[0020] In some embodiments of the present invention, it is not necessary for a person operating the specific electronic communications device to view the pseudo-random string and to apply the mask code manually thereto. Instead, a computer program may be provided in a memory of the specific electronic communications device which allows the person to enter his or her mask code when prompted, and which then applies the mask code automatically to the pseudo-random string, returning the appropriate volatile identification code for input into the specific electronic communications device or the at least one electronic communications device.

[0021] In a further development, at least one position in the pseudo-random strong may be chosen to contain a character representative of a predetermined parameter or condition. Advantageously, the position of the character and its representational meaning are know only to the electronic computer and the person operating the specific electronic communications device. For example where the electronic computer is operated by a bank and the permanent identification code is the person's bank account number, then one of the positions in the pseudo-random string, say the seventh, may be chosen to be representative of a balance of the person's bank account, with 0 for example indicating zero funds and 9 indicating a balance over [pound]1000, with FIGS. 1 to 8 being representative of balances there between on a linear scale. Alternatively, for greater security, the at least one position in the pseudo-random strong may be chosen to contain a flag character, with say any one of the digits 1 to 5 indicating a balance below [pound]500 and any one of the digits 6 to 9 indicating a balance above [pound]500. It will be apparent that many other representational schemas may be applied so as to convey information in the pseudo-random string. Because the position and meaning of the at least on representative character in the pseudo-random strong is preferably selectable by the person rather than following a set format which may become known to unauthorized third parties, it remains difficult to extract meaningful information should the pseudo-random string be intercepted during transmission. Furthermore, the person may be required to identify the position and/or meaning of the at least one representative character after receiving the pseudo-random string, thereby providing an additional layer of security in the identification process.

[0022] It will be apparent that in the embodiment described hereinabove, the pseudo-random string must be at least ten characters long, since a mask code made up of the numbers 0 to 9 requires at least ten positions along the pseudo-random string to be functional. However, a person of ordinary skill will appreciate that different mask codes and string lengths may be used as required by selecting appropriate coding schemas. It is to be emphasized that the pseudo-random string issued by the electronic computer in response to an identification request from the at least one electronic communications device will be different for each request, and that it will therefore be extremely difficult to determine a given mask code given a series of potentially interceptable pseudo-random strings and volatile identification codes. Indeed, in embodiments where the specific electronic communications device is a separate device from the at least one electronic communications device, for example, a mobile telephone and an EFTPOS terminal respectively, then the pseudo-random string and the volatile identification code are never transmitted along the same route, for example, a given temporary telephone connection. In embodiments where the specific electronic communications device is the at least one electronic communications device, for example, a remote computer terminal adapted for secure connection to the electronic computer, then the pseudo-random string may be transmitted along the same route, but not together at the same time. In the latter embodiment, an initial request to log on to the electronic computer may only be considered if it emanates by way of a direct modem link from a predetermined telephone number associated with the person, the pseudo-random string is then transmitted back along the modem link to the remote terminal and the volatile identification code transmitted to the electronic computer by way of the same direct modem connection.

[0023] In a particularly preferred embodiment, the electronic computer is operated by a debit or credit card issuer, the specific electronic communications device is a mobile telephone, the at least one electronic communications device is an EFTPOS terminal operated by a retailer, the permanent identification code is a person's debit or credit card account number, the mask code is a four digit number as described above, the identification code enabling electronic communications between the electronic computer and the specific electronic communications device is a telephone number of the mobile telephone. It is to be understood that the debit or credit card issuer may be a bank which issues standard debit cards enabling purchases to be made against funds in the person's current account or standard credit cards enabling purchases to be made against a credit account, or may alternatively be a specialist service provider issuing dedicated debit cards to subscribers, where the subscribers must arrange for funds to be transferred to the service provider as requires so as to keep at least a minimum positive balance associated with their dedicated debit card accounts.

[0024] When a person first applies for an account from the card issuer, he or she is issued with an account number and a card which bears the account number and name of the account holder in the usual way, for example by way of embossing the card with human-readable indicia and by way of providing machine-readable data on a magnetic strip on a reverse portion of the card. The person must supply the usual details, such as name and home address, to the card issuer, together with his or her mobile telephone number. It is also necessary for the mask code to be issued to the card issuer or to be agreed between the card issuer and the person. The mask code is preferably issued separately from the card, for example by way of separate postal deliveries, and is never transmitted together with the account number and/or telephone number. When the person wishes to make a purchase using the debit or credit card, he or she presents the card to a retailer. The retailer then swipes the card through the EFTPOS terminal, which then contacts a main computer operated by the card issuer.

[0025] The card/account number is transmitted to the main computer by way of a modem link, together with transaction details including the price of the purchase being made. The main computer then correlates the card/account number with the person's mobile telephone number and, if there are sufficient funds in the account to cover the intended purchase, generates a pseudo-random string which is transmitted to the mobile telephone by way, for example of and SMS message over a cellular telecommunications link. The person applies the mask code to the pseudo-random string as hereinbefore described, and then gives the volatile identification code thus generated to the retailer. The retailer, in turn, enters the volatile identification code into the EFTPOS terminal, which then transmits this data back to the main computer where it is correlated with the person's account details and compared with a volatile identification code temporarily stored in the main computer and generated therein by applying the mask code to the pseudo-random string independently of the person. If the volatile identification codes match, the main computer transmits a confirmation message to the EFTPOS terminal authorizing the transaction, and the necessary funds to cover the purchase are then transferred automatically to the retailer and debited from the person's card account.

[0026] In the event that there are insufficient funds in the person's account to cover the cost of the purchase, the main computer may issue a signal to the EFT terminal that the transaction is not authorized, and may issue a message to the mobile telephone advising the person to add finds to the account. In the event that the volatile identification codes are found not to match, then the main computer may issue a signal to the EFTPOS terminal so as to inform the retailer, who may then ask the person to check that the correct volatile identification code has been generated and to provide the correct code for transmission to the main computer. If the person gives the wrong volatile code more than a predetermined number of times, for example three times, then the main computer may suspend that person's account temporarily for reasons of suspicion of fraudulent use. The authentic card holder must then apply to the card issuer, together with suitable verification of his or her identity, before the account is reactivated and/or a new account and card is issued.

[0027] In some embodiments, the person may communicate with the central computer directly by way of his or her mobile telephone. This is possible because transmissions from a mobile telephone include details of the number of telephone number of the mobile telephone, and because the main computer is able to correlate mobile telephone numbers with card accounts. One useful feature that may be provided is an emergency account lock that may be activated in the event that the credit or debit card or even the mobile telephone is stolen. Such a lock may be activated by transmitting a predetermined lock code, for example 9999, to the main computer. Alternatively, or in addition, a lock code may be issued in mask code format, which is useful in the event that a person is robbed and threatened with violence so as so hand over his or her card and mobile telephone, together with his or her mask code.

[0028] A further useful security feature may be provided wherein, after the volatile identification code has been transmitted to the electronic computer for verification and found to match a volatile identification code generated by the electronic computer, the electronic computer may transmit a message to the mobile telephone requesting that the person confirms that the transaction is authorized. The message may be sent in SMS or voicemail format, and may include details of the transaction. Only when the person responds affirmatively to the message by transmitting a confirmatory message from the mobile telephone to the electronic computer is the transaction finally authorized.

[0029] The credit or debit card of this embodiment of the present invention may also be used to make secure purchases over the Internet. In this scenario, the at least one electronic communications device may be a computer server operated by an Internet retailer. When a person wishes to make a secure purchase, he or she submits the account number to the server, by way of e-mail or through the retailer's website, and the server then transmits the account details and purchase details to the main computer operated by the card issuer as before. An SMS message containing the pseudo-random string is then transmitted to the person's mobile telephone, and the person then causes a volatile identification code to be generated and then submitted to the retailer's server from where it is transmitted to the main computer for verification before the transaction is authorized and funds released.

[0030] A person may have more than one account with the card issuer, and may accordingly select or be assigned more than one mask code, one for each account. Alternatively or in addition, more than one mask code may be assigned to each account, and the main computer may indicate by way of one or more characters in the pseudo-random string that it is expecting the person to apply a particular mask code, selected from a plurality of prearranged mask codes, to the pseudo-random string, thus providing an additional level of security.

[0031] It is to be appreciated that the present invention is not limited to credit or debit card transaction, but provides a secure method and system of identification in a wide variety of situations. For example, access to a building or vehicle may be controlled by providing a central computer holding details of all people authorized to enter the building or vehicle, and a swipe card bearing a unique identification number or code in magnetically-coded format may be issued to each person authorized to enter the building or vehicle. At entrances to the building or vehicle, electronic locks linked to card scanners and electronic keypads may be provided, the card scanners and keypads allowing communication with the central computer. When an authorized person wishes to enter the building or vehicle, he or she swipes the swipe card through the card scanner, which then transmits the unique identification number or code to the central computer. The central computer correlates the unique identification number or code with personal details of the person, including a predetermined mask code, and then transmits a pseudo-random string to the keypad for display on a display provided thereon. The person must then apply his or her mask code to the pseudo-random string and enter the volatile identification code thus generated into the keypad, which then transmits the volatile identification code to the central computer for comparison with a volatile identification code generated in the central computer as hereinbefore described. If the volatile identification codes match, then the central computer issues a signal to unlock the electronic lock. Such a system provides a significant advantage over existing electronic locks operated by keying in a predetermined code, because each time a person enters the building or vehicle, he or she will have to enter a different volatile identification code. This means that a potential thief of the like will not be able to gain access to the building or vehicle merely by observing an authorized person keying in an entry code and subsequently entering the same entry code.

[0032] Furthermore, it is not necessary to provide a swipe card to each person authorized to enter the building or vehicle. Instead, each person is issued with a unique and memorable permanent identification number or code, which may be input by way of the electronic keypad when access to the building or vehicle is required. The unique permanent identification number or code is then correlated in the central computer with the appropriate mask code and a pseudo-random string transmitted to the electronic keypad for display on a display thereof as before.

[0033] It will be appreciated that in the above embodiments, the electronic keypad and optional card scanner form the at least one electronic communications device as well as the specific electronic communications device. For added security, albeit involving additional inconvenience, persons authorized to enter the building or vehicle may be provided with mobile telephones as specific electronic communications devices, with the pseudo-random string being transmitted to the mobile telephone rather than to a display on the electronic keypad.

[0034] Alternative uses for the system and method of the present invention include any situation where secure identification of a person in an electronic communications environment is required. For example, the system and method maybe employed for a secure remote log-in to a computer and secure telecommunications in general (e.g. business-to-business e-commerce transactions, air traffic control communications, etc.). The system and method may also be implemented in the context of a vehicle immobilizer and/or alarm, whereby an authorized user of a vehicle is requested to apply a mask code to a pseudo-random string so as to deactivate the immobilizer or alarm.

[0035] A further use for the present invention is a secure ticketing system. A supplier of travel tickets, concert tickets, cinema and theater tickets and tickets for sporting events, among others, may issue a "virtual" ticket in the form of a permanent customer identification code and a pseudo-random string transmitted from a host computer to a specific electronic communications device. Upon arrival at a venue or upon request by a ticket inspector, a person to whom the "virtual" ticket has been issued may be required to apply his or her mask code to the pseudo-random string and to provide the virtual identification code generated thereby, together with the permanent customer identification code, to the ticket inspector. The ticket inspector may be provided with an electronic communications device by way of which this information may be transmitted back to the host computer for verification, and to which a verification signal may be sent by the host computer in the event that the person is positively identified as an authorized ticket holder.

[0036] Yet another use of the present invention is in a parcel or postal depot, such as a post office, or a catalog store or a warehouse or the like, where people visit to pick up parcels, post or other articles and it is necessary to positively identify a person before handing over the parcels, post or other articles. A person picking up an article will have been issued with a pseudo-random string and, upon collection, is asked to supply a volatile identification code generated by the application of his or her mask code to the pseudo-random string.

[0037] According to another aspect of the present invention, there is provided an identity verification secure transaction system comprising a host computer for storing a user code associated with a user and for supplying a pseudo-random security string for a transaction. The host computer determines a one time transaction code by applying the user code to the pseudo-random security string. There is at least one electronic device in electronic communication with the host computer used for administering and completing the transaction by receiving and displaying the pseudo-random security string. The user determines the transaction input code by applying their user code to the pseudo-random security string displayed on the electronic device. The user enters the transaction input code in the electronic device displaying the pseudo-random security string, or in a device in communication with the host computer. The entered user transaction code is sent to the host computer for verification with the one time transaction code. The pseudo-random security string may be displayed and user entry of the transaction code may entered in any combination of devices including an Electronic Funds Transfer Point of Sale (EFT/POS) device, a wireless device associated with the user, a user computer connected via the Internet with the host computer or any device capable of communicating electronically with the host computer. Further, the host computer may transmit the one time transaction code for display on an electronic device, the system may be used to complete a transaction with a merchant through a merchant computer or web site which is in electronic communication with the host computer and a user computer or device. The system may be used to provide security or regulated access to a database or account information.

[0038] The present invention also provides a method for verifying an identity for conducting secure transactions in which the system stores information about a user pin associated with a host computer; generates a pseudo-random security string, determines a transaction code by applying the user pin to the pseudo-random security string, and transmits the pseudo-random security string to an electronic device. The electronic device displays the pseudo-random security string so that the user can determine a user transaction input code by applying their user code to the pseudo-random security string. The user enters the transaction input code on the same or a different electronic device in electronic communication with the host computer. The user entered transaction code is transmitted to the host computer for verification that the host computer determined transaction code matches the user entered transaction input code. The system of the present invention completes the transaction, allows access to a database or account information when the host computer determined transaction code matches the user entered transaction input code.

[0039] Another aspect of the present invention includes a secure user code entry interface system which is comprised of a secure user code entry interface. The user code entry interface is stored and running on an electronic device where the electronic device has a display. Viewable on the display if the secure user code entry interface which contains at least one active display for entry, by the user, of one digit of the user code per cycle of the interface. The active display of the interface illuminates at least one display digit on the interface and the user keys any key of a keypad or mouse or touches any area of a touch sensitive screen when the illuminated digit matches the digit to be entered in their user code. A random run on time is added to time when the user enters the keystroke so that the active display remains active and therefore information relating to the number entered can not be determined. The secure user interface contains one cycle for each digit of a user code.

[0040] According to a still further aspect of the present invention, there is provided an identity verification secure transaction system comprising a host, at least one electronic device, and a secure user interface. The host computer stores information about the user which includes account and user code information. The at least one electronic device is in electronic communication with the host computer and displays the secure user input interface for entry of the user code. The at least one electronic device has at least a display and a user input device. The secure user code entry interface contains at least one cycle for each digit of the user code and contains an active display for entry of the user code. The user enters each digit of the user code by a response through a user input device at a response time when a display digit which corresponds with the appropriate digit of the user code is illuminated in the active display of the interface. After entry of each digit within a cycle is entered a random run on time is added to the time when the user responded in order to extend each cycle of the active display so that the anyone could not determine which digit was selected by viewing the user interface. After entry of the entire user code the entered code is transmitted to the host computer for verification with the host computer stored user code. The user may enter their response by keying any key on a keyboard or mouse or by touching any area of a touch sensitive display.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0041] For a further understanding of the nature, objects, and advantages of the present invention, reference should be had to the following detailed description, read in conjunction with the following drawings, wherein like reference numerals denote like elements and wherein:

[0042] FIG. 1 is a schematic diagram showing a preferred embodiment of the present invention.

[0043] FIG. 2 is a schematic diagram showing a preferred embodiment of the dual channel schema.

[0044] FIG. 3 is a process flow diagram showing the steps a user would take while interacting with the system of the present invention.

[0045] FIG. 4 is a schematic diagram showing a preferred embodiment of the single channel schema of the present invention.

[0046] FIG. 5 is a schematic diagram showing an additional embodiment of the single channel schema of the present invention.

[0047] FIG. 6 is a schematic diagram of an additional embodiment of the single channel schema of the present invention.

[0048] FIG. 7 is a schematic diagram of an additional embodiment of the single channel schema of the present invention.

[0049] FIG. 8 is a schematic diagram showing an additional embodiment incorporating various aspects and features of the present invention.

[0050] FIG. 9 is a schematic diagram showing a secured database access system of the present invention.

[0051] FIG. 10 is a schematic diagram of a secure system for retrieving bank account information.

[0052] FIG. 11 is a representation of pseudo-random string.

[0053] FIG. 12 is a schematic diagram showing the modification and integration process of the user's temporary or transactional.

[0054] FIG. 13a is a graphical representation of the user interface of the present invention.

[0055] FIG. 13b is a graphical representation of the user interface of the present invention.

[0056] FIG. 13c is a graphical representation of the user interface of the present invention.

[0057] FIG. 13d is a graphical representation of the user interface of the present invention.

[0058] FIG. 13e is a graphical representation of the user interface of the present invention.

[0059] FIG. 13f is a graphical representation of the user interface of the present invention.

[0060] FIG. 13g is a graphical representation of the user interface of the present invention.

[0061] FIG. 13h is a graphical representation of the user interface of the present invention.

[0062] FIG. 14 is a graphical representation of the start screen of the PIN Safe interface of the present invention.

[0063] FIG. 15a is a graphical representation of the first cycle of the PIN Safe user interface.

[0064] FIG. 15b is a graphical representation of the second cycle of the PIN Safe user interface.

[0065] FIG. 15c is a graphical representation of the third cycle of the PIN Safe user interface.

[0066] FIG. 15d is a graphical representation of the fourth cycle of the PIN Safe user interface.

[0067] FIG. 15e is a graphical representation of the PIN Safe user interface using symbols or characters instead of numbers.

[0068] FIG. 16 is a schematic diagram showing features of the present invention utilized in a database access system via the Internet.

[0069] FIG. 17 is a schematic diagram containing features of the present invention utilized in the access of multiple databases via the Internet.

[0070] FIG. 18 is a schematic diagram illustrating various features and components of the present invention communicating via the Internet.

[0071] FIG. 19 is a schematic diagram illustrating various features and components of the present invention communicating via the Internet.

[0072] FIG. 20 is a schematic diagram of various features and components of the present invention communicating via the Internet.

[0073] FIG. 21 is a schematic diagram illustrating the access and data channels of an additional embodiment of the present invention.

[0074] FIG. 22 represents a schematic diagram displaying a generic server gateway schema incorporating various aspects of the present invention.

[0075] FIG. 23 shows a schematic diagram illustrating a generic integration platform of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0076] FIG. 1 shows a host computer 1 operated by a credit/debit card issuer, a user 2 having a mobile telephone 3, and an EFTPOS terminal 4. The user 2 is issued with a card (not shown) having a unique 16-digit account number embossed and magnetically encoded thereon, this 16-digit account number being correlated in the host computer 1 with account details relating to the user as well as a 4-digit mask code selected by or assigned to the user 2 upon initial registration with the credit/debit card issuer and a unique telephone number of the mobile telephone 3. The 16-digit account number is chosen for a compatibility with existing credit/debit card protocols, and the 4-digit mask code for compatibility with existing PIN protocols. When the user 2 wishes to make a purchase from a retailer (not shown) operating the EFTPOS terminal 4, he or she presents the card, which is then scanned by the EFTPOS terminal 4. Details regarding a purchase are also entered into the EFTPOS terminal 4 by the retailer, and these are transmitted, together with the account number, to the host computer 1 by way of a modem link 5. The host computer 1 then correlates the account number with details of the user 2, including the telephone number of the mobile telephone 3, and generates a 13-digit pseudo-random string which is transmitted to the mobile telephone 3 by way of an SMS or voicemail protocol 6. The first three digits of the pseudo-random string are not random and are reserved to indicate to the user that a received SMS message is from the host computer. For example, the first three digits may be "T1:" or "T2:" or the like, so as to indicate that the host computer 1 is expecting the user 2 to apply a first or a second mask code to the pseudo-random string. The next 10-digits of the pseudo-random string provide sufficient redundancy for any 4-digit mask code to operate thereupon in the manner hereinbefore described. By choosing a string length of 13 digits for the pseudo-random string, compatibility with existing mobile telephone displays and EAN13 (European Article Number) barcode protocols is ensured.

[0077] Upon reception of the pseudo-random string by the mobile telephone 3, the user 2 must apply the mask code thereto as hereinbefore described so as to generate a volatile identification code, which is then passed 8 to the retailer and entered into the EFTPOS terminal 4 for transmission to the host computer 1. Alternatively, the volatile identification code may be returned by the user 2 to the host computer 1 by way of the mobile telephone 3. When the host computer 1 receives the volatile identification code, it compares this with a volatile identification code generated within the host computer 1 by applying the mask code to the pseudo-random string and, if the volatile identification codes are found to match, issues a signal to the EFTPOS terminal 4 so as to authorize the purchase and to transfer necessary funds to the retailer. Optionally, before authorizing the transfer of funds, the host computer 1 may send a message to the mobile telephone 3, for example in SMS or voicemail format 6, preferably including details of the transaction, and requesting that the user 2 return a signal 7 so as finally to confirm the transaction. This may provide added peace-of-mind for unusually large transactions and may alert a user 2 in the event that fraudulent use is being made of his or her card.

[0078] The present invention may be implemented in both a single and dual channel schema which are disclosed and discussed in relation to FIGS. 2-10.

[0079] The Dual Channel protocol is appropriate for all users who own a G2 mobile phone. The types of transaction might include: (1) Electronic Funds Transfer at the Point of Sale (EFT/POS) and (2) Telephone orders. EFT/POS are transactions where the user would make a purchase at a merchant in the normal way and when the credit/debit card is swiped through the card reader, the merchant would be prompted to ask for the customer's transaction affirmation code (TAC) or mask code. The user remembers a their four digit PIN number which is used to determine the TAC from the pseudo-random string, which is given at the point of sale. If the user intends to make multiple purchases within a short space of time or in an area where mobile phone reception is poor the user can elect in advance to use the same TAC for a single day. A telephone order transaction would essentially use the same method as above with the exception that the merchant physically enters the card details in the usual manner before being prompted for the TAC.

[0080] Additional features of the dual channel schema are that the customer will be able to choose alternative user-friendly methods of identifying the TAC from the pseudo-ramndom security string. such as an Enigma interface or voice recognition system. An Enigma Interface would include minor modifications to a SIM card in a phone or pager during manufacture but customers could avoid any calculation of the TAC themselves. Users will be able to key in their PIN and by pressing an additional key of their choice, the phone or pager will automatically compute the resultant TAC, without the customer even seeing the Security String. This computation would be a completely internal, ensuring that only the TAC is displayed, and the PIN is not retained in the mobile phone or pager. A voice recognition interface could be implemented in voice activated phones and be able to compute the appropriate TAC on the simple command "TAC!" from an approved voice.

[0081] Customers could also have the option of choosing, when applying for an enabled card, a geometric shape, as will be discussed in more detail below, in which the security string will always be delivered. The customer would simply register their chosen geometric shape to be displayed on screen and then visually apply their PIN pattern to determine the corresponding resultant TAC. This display can be interfaced by a WAP mobile phone, a G3 mobile phone, an Internet site display prompt or a secondary dedicated terminal placed at the point of sale.

[0082] The protocol of the present invention may be 'bolted-on' to an existing database server and can at least run on unmodified EFT/POS hardware such as: (1) AMEX; (2) Split dial EPOS; and (3) VISA AVS3. In addition, the dual channel protocol can be used to upgrade the security of Mondex systems (these already use a 4-PIN digit at POS).

[0083] The dual demand schema may use a standard G2 mobile phone, G3, and WAP device to receive the security string. If these devices include a modified SIM card interface for this security string the device may also include a GUI or an Enigma interface to simplify the derivation of the TAC.

[0084] FIG. 2 represents a diagram showing the protocol for the present invention applied to a point of sale environment. FIG. 2 displays the main components and steps for this transaction and displays two different options. The first option utilizes a split dial electronic funds transfer point of sale machine (EFT/POS), where the details of the transaction are directly sent via the Authorization Server 207. The second option utilizes the merchant acquirer's network.

[0085] In the direct dial scenario, the user 201 receives a security string 210 from the Authorization Server 207 which resides on the device 202. The security string 210 resides on the device 202, such as a mobile phone, until the user is ready to make a purchase. When the user 201 is ready to make a purchase they hand over, in step 220, their enabled credit card 204 to a merchant 205 to conduct the electronic funds transfer or point of sale (EFT/POS). The card 204 is swiped as usual at the merchant's 205 EFT/POS terminal. The user 201 reviews the security string 210 residing on their device 202 and determines their TAC for that particular sale. The four digit TAC 230 is provided to the merchant 205 by the user 201. The user 201 may provide the TAC verbally, by entering it into the POS terminal, or by entering the number on the mobile device 202. The credit card 204, TAC 230, and transaction amount are then sent, via the direct dial network 240, to the Authorization Server 207. The Authorization Server 207 confirms with the card issuer 209 that the account has sufficient funds in the account and that the TAC corelates with the user's PIN number and the issued security string 210. In the event that the account number, transaction amount, and TAC are verified the Authorization Server 207 allows the transaction to proceed.

[0086] In the second scenario, referred to as the merchant acquirer network scenario, the same initial steps apply. The user 201 receives a security string 210 which resides on the device 202, such as a mobile phone, and that when the user 201 is ready to purchase an item from the merchant 205 they, in step 220, present the merchant 205 with the registered credit or debit card 204. The card 204 is swiped at the EFT/POS terminal and again the user 201 determines their four digit TAC 230, via the security string 210 residing on their mobile phone or device 202. In this scenario, the transaction information including the account number of the card 200 and amount of purchase are routed via path 250 to scheme 252. The standard credit card transaction details and the pre-authorized PIN are sent to the card issuing host server 209. The scheme 252 sends the card 204 information and pre-authorization PIN to the card issuer host 209 via communications path 256. At the same time, the scheme 252 communicates with the Authorization Server 207 and verifies that the pre-authorized PIN correlates to the user's PIN. The card issuer 209 proceeds with the transaction and upon verification allows the transaction to proceed.

[0087] In addition to the dual channel schema described above, the present invention also allows for a single channel schema whereby a user would be able to use the present invention for such transactions as online purchasing via internet websites. The single channel schema and protocol is conducted via either a computer, a WAP device, Smart Card, Proprietary System or a G3 mobile phone, where the security string is received and the TAC transmitted on the same device. This protocol does not require a secondary channel to conduct a secure transaction.

[0088] The single channel protocol runs via an applet downloaded by the user onto their computer, WAP device or G3 mobile phone. The security string and the TAC can only be received by an enabled server and transmitted via an SSL link. The present invention is resistant to 'ghost' sites, where the user is unaware that the site they are dealing with is not certified, because the merchant (whether certified or not) would only be in possession of the users 'User name or card ID' and not the relevant TAC.

[0089] The single channel solution solves the problem encountered by transmitting the relevant TAC and security string over the Internet by instructing the users ISP (Web browser) to transmit only the user name to the merchant and the relevant TAC to the enabled server/database.

[0090] FIG. 3 shows each step along the process a user would take to register and use the single channel schema. The process is started in step 300 and in step 310 the user contacts the server host of the present invention through a single channel device such as a personal computer, an internet connected hand held device, a cell phone or wireless phone, or any device that may support a web browser via a single communication channel. Upon contact with the server or host of the present invention a log on web page containing the interface applet is sent to the user's device. In step two 320 the user is requested to input their user ID and preauthorized credit card or debit card number through an appropriate entry method. The user interface may include on screen drop down menus or other various user friendly applications to enhance the entry process of the user ID and credit card or debit card number. The user ID is sent to the server for verification. If the server verifies the user's identity a security string is sent to the client web page using the low processing overhead protocol (LPO protocol) with a prompt to initiate the applet. The applet is used to abstract and repack the TAC code according to the LPO protocol and start the Pin Safe interface.

[0091] In step 330 the Pin Safe interface is started enabling safe user entry of a PIN or TAC. The LPO protocol extraction is carried out using an automatic System Identification Digit (SID) and System Outgoing Digit (SOD) generation. As will be described in more detail below, the TAC code is pulled from the security string and repacked according to the LPO protocol and sent to the server host for verification. In step 340 the applet is stopped and destroyed, all values are zeroed and the security string residing on the device is cleared. The user sees an interface which identifies that the device is awaiting a response from the server. In step 350 the log on to the server is verified or rejected according to the user ID and TAC code response. If verified, confirmation is sent to the client browser followed by requested service access or transaction. In step 360 the session or transaction is finished allowing the user to close the session or the process or the session may be automatically closed triggered by some length of time of inactivity. The user's information with the single channel schema is terminated at step 370.

[0092] FIG. 4 displays the main components for a preferred embodiment of the single channel schema of the present invention. The user 401 would visit the server 407 of the present invention and the server 407 would provide applets 470 for downloading to the user's device 403. The user 401 downloads an applet 470 via path 421 which is then stored on the device 403 as the customer applet 422. The web merchant 405 would also visit the Authorization Server 407 via path 450 and download the an applet 470 via path 451 which is stored on the merchant site 405 as merchant applet 452. The user 401 using the device 403 visits the web merchant site 405 via path 430 and selects items they wish to purchase by placing them in the basket 406 and selecting the appropriate credit or debit card for use 407. The merchant site 405 then accumulates the items in the basket 406, information about the card 407, and utilizing the merchant applet 452 routes the information along path 431 to the Authorization Server 407.

[0093] The Authorization Server 407 starts the verification process and using communications path 432 routes the appropriate information back through the merchant applet 452 to the customer applet 422 resident on the user's device 403. The user 401 is requested to enter the TAC. Once the user has entered the TAC, the TAC is sent along path 433 through the merchant back to the Authorization Server 407 to validate the response. In addition, the Authorization Server 407, at step 434, validates that there are sufficient funds in the account and in step 435 verifies that the information about the card 407, TAC, and account funds availability are verified. The Authorization Server 407 sends an "accept" notice along path 436 to the merchant site 405 which is then relayed, via path 437, to the users device 403.

[0094] FIGS. 5-7 also relate to single channel schemas utilizing different aspects and security protocols. In FIG. 5, the user 501 visits a merchant internet site 505 and would select various items for purchase. Upon checkout, payment is demanded via path 510 from the merchant site 505 to the user 501. The personal computer or device 503 contains an applet 522 which communicates with the site 505 and includes the proper software or applet 522 to notify, along path 520, the Authorization Server 507 that a transaction authorization is needed. The merchant domain name, transaction amount, user ID, and Transaction Authorization Code (TAC) are transferred from the user's device 503, along path 530, to the Authorization Server 507. Already present on the personal computer or user's device 503 is the security string for the user to determine their TAC code.

[0095] The Authorization Server 507 communicates with the merchant internet site 505, via path 540, to certify the card and transaction amount information. The Authorization Server 507 also forwards a transaction ID via path 541 to the user 501 through the user's personal computer 503. The transaction ID is forwarded to the merchant's internet site, along path 542, from the user's personal computer 503. The Authorization Server 507 certifies that the amount of purchase, the card information, and TAC are appropriate and sends the card details and amount along path 550 to the merchant internet site 505. The transaction details are sent from the merchant internet site 505 to the card issuer 509, via path 560, and ultimately the card issuer 509 sends payment via path 570 to the merchant internet site 505.

[0096] The single channel schema displayed in FIG. 6 is similar to the single channel schema displayed in FIG. 5 except that a wireless device 604 is included to remove the security string from the user's personal computer 603. In the schema illustrated in FIG. 6, the security string is omitted and simply the four digit TAC 620 for that transaction is transmitted from the Authorization Server 607 to the user's wireless device 604.

[0097] FIG. 7 is a single channel schema similar to the single channel schemas disclosed in FIGS. 5 and 6 except that instead of the four digit TAC being transmitted from the Authorization Server 707 to the wireless device 704, as described above in relation to FIG. 6, a thirteen digit security string 720 is sent to the wireless device 704. The schema disclosed in FIG. 7 discloses that as the user 701 selects items to be purchased from the merchant internet site 705 the payment demand along path 710 is sent to the user via the user's personal computer 703. The applet 722 then prompts the user to enter the TAC code, which the user determines from the security string 720 sent from the Authorization Server 707 to the wireless device 704. The applet 722 forwards the merchant domain name, transaction amount, user ID, and TAC to the Authorization Server 707 along path 730. The Authorization Server 707 certifies the transaction, along path 740, and forwards the user account number and amount along path 750 to the merchant internet site 705 . The transaction details are sent from the merchant internet site 705 to the card issuer 709, along path 760, and payment is then forwarded from the card issuer 709 to the merchant internet site 705 along path 770.

[0098] In the various online merchant scenarios employing the single or dual channel schema, as seen in FIGS. 2-7, there may be instances when the merchant does not have a particular item in stock and therefore can not process or complete the entire transaction immediately. In these instances, the merchant typically does not complete the transaction until the merchandise is dispatched. However, the user may have already input their TAC and the system would want to send the user a new pseudo-random security string.

[0099] The present invention overcomes this hurdle by having the Authorization Server receive the payment request and the active TAC. The merchant's server typically would transmit the order request to the authorisation server within a nominal 1-minute time out. However, if the merchant has received a purchase order for goods not in stock that order request will be delayed. The delayed order request will not be sent to the authorisation server until the goods have been received and are ready to be dispatched to the customer. Upon reception of the user's TAC and transaction details and the absence of the merchant's transmission of the order within the 1-minute timeframe the authorisation server will default to a deferred payment program.

[0100] The deferred payment program will hold the active TAC at the Authorization Server and is proof that the user has ordered the goods. A new security string can then be issued to the user for use during the next transaction. The authorisation server program will immediately send an email to the user stating details of the goods that he has requested from the merchant. Every week, or some other predetermined time interval, the Authorization Server will remind the user of his order request. The user is therefore informed of any pending transactions that will be eventually cleared through his account.

[0101] When the goods arrive at the merchant's depot and are ready to dispatch, the merchant details are then transmitted to the Authorization Server and the transaction is completed. If by this time the user has insufficient funds to cover the transaction amount the transaction would be declined, as typical in a standard credit card transaction.

[0102] FIG. 8 represents an additional schema utilizing features of the present invention in which a user has a pre-authorized or debit account 804. The user would see a live device 805, such as a vending machine, and would select items via path 810 thereby triggering the live device 805 to demand payment. The payment demand would be routed through the preauthorized liquid account 804 which is done by swiping the pre-authorized account 804, such as a credit or debit card, in step 840 through a card swipe device 806. In addition the micro payment demand would also notify the card swipe device 806 that a TAC would be requested. The user may have a personal device 803, such as a wireless phone, which would contain either a TAC or security string whereby the user would determine the TAC and enter the TAC 830 into the card swipe device 806. Alternatively, the user could enter the TAC 830 into the wireless device 803 which would wirelessly transmit the TAC 830 to the card swipe device 806 or Authorization Server 807. The details of the transaction are sent along path 850 from the card swipe device 806 to the Authorization Server 807. The Authorization Server 807 contains the information on the liquid account and if verified would notify a micro payment host 808 along path 860 to authorize payment. The micro payment host 808 then transfers payment along path 870 to the live device 805.

[0103] FIG. 9 represents a data control schema whereby elements of the present invention can be used to add a security overlay and pre-authorization into a database for controlling access to a database. In FIG. 9 the user 901 through their computer or laptop 903 wants access to a database 909. Access is requested along path 910 from the Authorization Server 907. A security string is sent from the Authorization Server 907 to the computer 903, via path 920, whereby the user determines their TAC. The user inputs the TAC which is transmitted to the Authorization Server 907 along path 930. Provided the TAC matches the appropriate PIN verified for the user 901 the Authorization Server 907 allows access to the database 909 along path 940. Further, the system can simply transmit the TAC, instead of the security string. The access data is then transmitted to the user's computer 903 through the Authorization Server 907 via path 950. In addition, the security string can be sent to the user 901 via an alternate path 921 such as through use of a wireless device 904.

[0104] FIG. 10 represents a remote bank balance inquiry schema whereby a user can check the balance of an account. In the schema presented in FIG. 10, the user 1001 through use of a cell phone, pager, or wireless device 1004 can request the balance of an account located in a bank 1008. The user is provided with a security string or TAC, via path 1010, which is resident on the wireless device 1004. The user determines their TAC code and either presents their TAC code through a bank teller (not shown) or inputs it into the wireless device 1004. The TAC code is sent to the Authorization Server 1007 which verifies that the TAC code is appropriate for the security string and corresponds with the user's PIN. The Authorization Server 1007 then communicates with the bank 1008 along path 1020 to retrieve the account information thereby providing the user with the requested information.

[0105] Two important aspects of the present invention which are utilized in the dual and single channel schemas described in relation to FIGS. 2-10 are the low processing overhead protocol and the security string operation. Certain wireless devices, such as web devices, cannot run high level encrypted programs due to their low processing overhead. The present invention incorporates a low processing overhead protocol which enables such devices to run highly secured transactions or downloads without using a large memory foot print. An additional benefit of the low processing overhead protocol is that existing transaction data issuing servers could also process information quicker than traditionally encrypted systems. The low processing overhead protocol evades the possibility of a correlation between the TAC and security string by simultaneously using multiple security strings. Only one of the multiple security strings is actually relevant and the remaining strings are used to hide the relevant string. The security strings contain identical digits but are arranged in different random orders. The user's applet receives the multiple security strings and distinguishes which string is relevant by using a system identifying digit (SID). The system identifying digit knows which of the security strings is genuine and instantly dumps the irrelevant strings and processes only the correct and relevant string. As an example, if the identifying digit value was 4, the present invention would identify that the fourth security string was the relevant security string.

[0106] During a transaction, as will be described in conjunction with FIGS. 11 and 12, the user inputs their PIN and the TAC is internally calculated on the applet of the wireless device, personal computer EFT/POS, or as seen in FIG. 11, a thirteen digit security string 1100 would be sent from the Authorization Server to the user; device identifying a string of random digits, in this instance thirteen (13). The security string 1100 may come with a two letter identifying prefix 101 which identifies which server has issued the security string 1100. For example in FIG. 11, if the user's PIN was 2468 and the user applies that PIN number to the digit locations in the security string 1100. The user would look at the number in the second spot, the fourth spot, the sixth spot and the eighth spot to determine their transaction affirmation code or TAC for that particular transaction. In this instance, the user's PIN of 2468 would yield a TAC of 7693. Therefore, the user would input 7693 as the TAC to notify the Authorization Server to continue with the verification process.

[0107] Further explanation of the manner in which the TAC is secured within the transmitted secure security strings is explained in conjunction with FIG. 12. As seen in FIG. 12, the user, or customer 1201 has a known PIN 1202 (i.e. 1234). Stored on the user's device and downloaded from the server 1207 is the thirteen digit pseudorandom string 1203. In this instance, the customer's PIN value of 1234 as it relates to the pseudo string 1203 indicates a TAC code 1204 of '6891.' When the user is asked to verify or input the TAC 1204 to authorize the server 1207 to verify that the customer 1201 is in fact the authorized and registered customer the TAC 1204 may be manipulated and reversed in a myriad of ways to protect the code during transfer along the communications path to the server 1207. One method for providing a security overlay to the customer's PIN 1202 and the TAC code 1204 is to incorporate the TAC code into one thirteen digit string of a multitude of strings as previously described.

[0108] To identify the appropriate string the applet running on the customer's device would identify the relevant string through a system identifying digit 1205. The SID 1205 is used to identify which of the security strings is relevant. The SID 1205 may be determined in a myriad of ways including using certain numbers or combination of numbers of the user's PIN 1202, having the user set the SID 1205, and having the system server set the SID 1205. In the example shown in FIG. 12, the system set the SID value equal to 3. Therefore, the third string of nine strings is the relevant string. The nine (9) strings of thirteen (13) digits are sent via a data connect, such as a data stream 1230, to the user or customer's 1201 device. The applet on the device knows the SID 1205 value and extracts the relevant string 1203.

[0109] The customer reviews the relevant string 1203 resident on their device and determines their TAC 1204. The TAC 1204 is then intertwined into an outgoing relevant string which is grouped with eight (8) non-relevant strings. The outgoing data stream 1240 contains nine outgoing strings of thirteen digits. The location of the relative outgoing string is identified by a system outgoing digit (SOD) 1209 which can also be determined in a myriad of ways such as using or adding certain numbers of a customer's PIN 1202 or having the customer or system server select the SOD 1209.

[0110] In this example, the system set the system outgoing digit (SOD) 1209 value at 2. Therefore, the TAC 1204 will be integrated into the second of nine strings in the data stream of strings 1240. The TAC code 1204 may also be inversed, manipulated, have an automatic number added to it (i.e. each number is increased by one), or any other manner in which the PIN number can be modifed prior to transmission. In the example shown in FIG. 12, the TAC code 1204, is inversed to determine the location of the TAC numbers within the relevant outgoing string. For example, since the TAC 1204 in this example had a value of '6891' the inverse value of '1986' would dictate that in the first spot is the first digit of the TAC code, in the ninth spot is the second digit of the TAC and so forth until the TAC is integrated into the relevant security string.

[0111] The data stream of outgoing security strings 1240 containing the nine strings of thirteen digits is sent to the server 1207 which has an applet for verification. The server 1207 has an applet which knows the SOD 1209 value and can identify the relevant outgoing security string for verification of the user's PIN. Therefore, the applet on server the server 1207 knows the customer's PIN 1202 is '1234' and can determine that based upon the protocol established can determine that the SOD 1209 value was 2 and therefore the relevant string is the second string. The server 1207 will analyze the second string in relation to the user's stored PIN and expected response to verify that the response matches the TAC 1204 code from the initial string 1230.

[0112] Upon receiving the nine carrier strings, the server 1207 knows the outgoing digit position of the relevant TAC carrier string and instantly dumps the irrelevant strings and processes the correct selected TAC carrying string. The verification process at the server 1207 then matches the correct TAC with the issued security string and user's PIN number. If all three correlate, the authorization is completed and a new security string is transmitted to the user's applet.

[0113] Although in this example the number has been limited to nine lines of thirteen digits plus three (3) system digits per line (totaling 144 digits). It is not meant to limit the number of lines or digits that can be used. The nine lines of thirteen digits totaling 144 digits is intentionally less than the total global packet standard for many devices of 160 characters. Therefore, keeping the digit size below 160 keeps the processing overhead at a minimum allowing for low processing capability in WAP applications and wireless devices. In addition, this low processing overhead results in extremely fast verification times. The verification process also employs a filtering step followed by a single dimension array process which is not an intensive arithmetic computation system which would require more processing time.

[0114] In addition to the various single and dual channel schemas, the low processing overhead protocol, and use of the multiple security string security overlay the present invention may also provide a security overlay within the user interface. FIGS. 13a-13h represent various user interface examples to which a user may be provided for inputting a user's TAC. In the examples provided in 13a-13h the user would remember their personal PIN as a pattern rather than a numerical sequence. As an example, if the user had chosen to use the shape 1301 and shown display in FIG. 13e, they would only have to remember that they created a PIN which creates a small box 1303 inside of the shape 1301 disclosed in FIG. 13c. When the display is populated with random numbers then user applies their chosen design (i.e. small box 1303). In this example, the user's PIN from box 1303 would be '2389'. Therefore, knowing the PIN of '2389' and viewing the randomly generated numbers within the random display 1302 the user would see that the numbers '7538' correspond with their PIN number location. Therefore, the user's TAC for completing such a transaction or entry into the database, would be '7538'. The user interfaces disclosed in FIGS. 13a-h are merely exemplary and numerous displays, as well as colors and graphic symbols could be incorporated into the user interface. Therefore, the user would be able to create a graphic representation of their PIN without the need to remember the four digit PIN number.

[0115] Another feature of the present invention which deals with the user interface of the system involves the use of a Pin Safe deterrent interface. Any device with a keyboard or touch sensitive interface which may be connected to a network or which is otherwise capable of downloading data or machine code may have the integrity of a password or key entry security system comprised. One way in which the system may be comprised is through the use of a Trojan program. A Trojan program is a small program which collects keyboard information for latter use. An additional program can also collect password or key entry information but fanes an unsuccessful logon attempt at the last digit of the logon entry and attempts to continue the logon with the real user unaware, by guessing the last digit (this is known as a "sniffer" program). Both of these techniques require actual data from a device keyboard or key pad or other input device. Whereas data may, by encryption or other means, be delivered and resent securely right up to and from the actual process occurring in the devices processing unit, if the security system requires meaningful user data entry to access or operate the security system that data may be intercepted and relayed greatly reducing the security of the system.

[0116] Although keyboard or small amounts of other input data may be redirected or stored with little or no user indication or system performance impact the same cannot be said for the device's graphical display, where the output is high throughput and device specific. Screen grabbing, or screen capturing, is possible but system resource intensive and therefore quite likely to be discovered by a user, especially on a device of comparatively low processing power. A good level of resistance could therefore be offered by an interface that provides information to a security system that is only meaningful to that system within the scope of its own time interface parameters and where any captured keyboard information has no external meaning. Similarly, any possible screen grabbed or screen captured information should not compromise the system's logon security.

[0117] The inputting of a Username, Password or PIN number in a computer, PDA, 2.5G or 3G mobile device is currently flawed for the following reasons: (1) the User can be seen from onlookers entering their PIN number into the device (called 'shoulder surfing'); (2) the keyboard could contain a 'Trojan' program that records the inputted Username, Password or PIN number (Trojans are downloaded without the knowledge of the User onto a computer and can reside there indefinitely); (3) PKI Certificates authenticate that the transaction was conducted on a certified computer, but they do not effectively authenticate the User behind the computer; and (4) computers running Microsoft Windows have a problem because Windows remembers the Username, Password or PIN number which creates a situation where the device stores the I/D of the User within the computer.

[0118] The "radar" deterrent or Pin Safe user interface of the present invention achieves a positive user I/D because the user has to be present during every transaction. The Pin Safe user interface is Trojan resistant because any key can be used to input a PIN or TAC which renders any Trojan key intercept information useless, as does the displayed information on screen.

[0119] In addition, the user interface is shoulder surfing resistant because there is nothing that could be gleaned from looking either at the screen or the keyboard input, rendering shoulder surfing a pointless exercise. Further, the system is resistant to PIN interception when using the Dual and Single channel (Applet) protocol. The protocol of the present invention is unique because it transmits a volatile TAC every time a transaction is made. A successful attempt to intercept/decrypt this information could not result in the user's real PIN being compromised.

[0120] Another feature of the present invention is that it is a multi-platform system. The PIN Safe user interface works on a wide variety of computers and applications because of its low memory footprint and simple generic user interface. The protocol and system as a whole is non device-specific and can run on any device such as a public use computer. The system does not have to run on a trusted computer system where the program history is known. With no digital certificate required for the computer the User could conduct a transaction on any computer worldwide.

[0121] Further, the user interface is easy to use because the user need know nothing about the protocol, TAC's and Security Strings. The PIN Safe user would merely input their unchanging PIN via the Pin Safe user interface. Further, the Pin Safe user interface is "tempest" proof because the interface does not display the users PIN or TAC (Pseudo PIN) on screen, and therefore is not subject to Electro-magnetic emissions from the VDU that could be the subject of surveillance via Tempest technologies. The strong protection gained by using the Pin Safe user interface of the present invention allows safe single PIN usage on a variety of accounts with differing security architectures which can be achieved by using a central PIN Authorization Server. Even if the security string resides on the device it is not a problem because the present invention does not require a digital certificate and therefore there is nothing in the memory of the computer that compromises the Users I/D if it falls into the wrong hands.

[0122] The Pin Safe user interface involves a unique method of inputting a PIN number into a computer, ATM, PDA, 2.5G or 3G Mobile Device. FIGS. 14 and 15a-15e are representative examples of the Pin Safe user interface screens. When a user wishes to conduct an online transaction, the Pin Safe applet will activate which will provide the "Start" user interface displayed in FIG. 14. Pressing any key on the user's computer screen TAC or PIN then activates the entry interface screen. The interface can be activated by using the keyboard, mouse, or a touch screen display.

[0123] As seen in FIGS. 15a-15e, the Pin Safe interface will now start to display (in this example in a clockwise manner) 12 digits in sequence (starting with 1 and ending in 12). During the display cycle, the User simply registers his PIN or TAC by pushing any key on their keyboard, mouse or any spot on the touch screen display when the digit they wish to register is illuminated. The Pin Safe display will rotate 4 times, once for every digit of a 4 PIN number.

[0124] At the 12thposition there is a dwell time to allow customer response for the starting of the next cycle accurately. When the first cycle for the first PIN number has finished the display will start again with another cycle. The cycles can also be identified by changing the illumination color. This process is repeated 4 times until all 4 digits are inputted to make up the User's 4 digit PIN.

[0125] For example, as seen in FIGS. 15a-15d, if the user's PIN was '2468' then on the first cycle the keyboard would be pressed when the 2<nd >digit was illuminated, see FIG. 15a. On the second cycle the keyboard would be pressed when the 4thdigit was illuminated (see FIG. 15b), on the third cycle the keyboard would be pressed when the 6thdigit was illuminated (see FIG. 15c), and on the fourth cycle the keyboard would be pressed when the 8thdigit was illuminated (see FIG. 15d). Only one display is seen at any one time on the screen preventing an onlooker from determining which PIN is being inputted. Further, the changing colors of the display background and the digits displayed can be pseudo-random.

[0126] After the User presses the keyboard to register the first PIN TAC digit a random run on period of time is activated. The run on process prevents shoulder surfers from seeing exactly which digit was registered. For example, as seen in conjunction with FIG. 15a, when the User wishes to register the first digit, as number 2, they would press any key on the keyboard when the number 2 or second digit is highlighted, however the display continues illuminating the numbers or digits after 2 around the cycle. The system may also illuminate only a portion of the numbers after the selected number, such as between 0 to 4 digits after the selected number, before speeding up the illumination of all numbers until completion of the cycle. A shoulder surfer would see the cycle speed up after the numbers 2, 3, 4, 5 or 6 were illuminated and would not be able to determine which digit had been registered. After the run on period, the system may increase the cycle speed to complete the cycle so that the user does not have to sit through the full cycle time to aide quick PIN entry. The run on period is normally less than the point in elapsed time from the key press to the time when the user would start to question whether a positive selection had been made. For short term visual memory, of a human, this is a maximum of around three seconds.

[0127] The run on period and increased cycle speed may be applied on all 4 cycles or displays. The dwell time between the digits being illuminated and the change in cycles is pseudo-random to prevent Trojan programs from determining which digit was inputted by correlating the display with the keyboard and the user's computer clock speed.

[0128] As seen in FIG. 15e, the Pin Safe user interface can also use characters, letters, or symbols instead of numbers on the display which would allows the user's code or pin to be any group of symbols or letters which spell a word. In addition, as previously discussed, in relation to FIG. 9, the present invention can be used for the remote access of data using either the Dual or Single Channel schema or protocol and the PIN Safe interface.

[0129] Enabling an existing database with the PIN Safe interface of the present invention can be done by providing an authentication server computer that registers the Users PIN number, issues and stores security strings, and correlates the received TAC to authenticate the user's identification.

[0130] In addition, the Pin Safe or Radar Interface can work within a computers own processor, within a LAN configuration, and over the Internet. Operating within a computers own processor the Pin Safe interface could act as a hack proof screensaver which means that when a user first started their computer they will be presented with the interface. The user must input their PIN accordingly and if the user decided to leave the computer for a short time, where there is the opportunity for criminal use of his computer, the user could press a function key which would activate the Pin Safe interface. Upon returning to the their computer they would simply click on their mouse or any key and enter their PIN via the Pin Safe interface.

[0131] In addition, if a user fails to input their PIN digit during any of the 4 sweep cycles, the present invention will allow the input of the PIN digit during any sweep (providied they are in the correct sequence). This means that a 'Reset' button will not require pushing unless the user has made a conscious mistake.

[0132] Additional schemas for employing the security features, measures, protocols, interfaces, and overlays of the present invention are discussed in connection with FIGS. 16-23.

[0133] As seen in FIG. 16, the Authorization Server 1607 is connected directly to a

Client's, Host Gateway Server 1609. The Host Gateway Server 1609 is the database's 1611 connection to the Internet 1613 and it is placed outside the firewall 1615 that surrounds the host database 1611 (this is to ensure that any hacking activity cannot occur inside the database 1611). The remote data access configuration may also employ the Pin Safe interface 1623 in conjunction with the user 1601 and the user's device 1604. The system may also employ a backup server or database 1630.

[0134] The Authorization Server 1607 can be configured to act as dual or single channel system. Its architecture allows the Host Gateway Server 1609 to allow access to the database 1611 either via the present invention or via it's existing access procedure. This means that after installation, the enabled access trials can be conducted without affecting the original configuration.

[0135] FIG. 17 shows how multiple Clients 1740, 1750 can be accessed from one User 1701, using one PIN number. This is achieved by installing a Central PIN Authorization Server 1707 which consolidates the received TAC's with the issued security strings from any enabled Client 1740, 1750.

[0136] The Pin Safe interface can be applied various ways including the dual channel, single channel: Thin Client and single channel Applet embodiments. In the dual channel application as seen in FIG. 18, the User's TAC is inputted via the Pin Safe interface 1823 and it is sent directly to the Authorization Server 1807 through the Internet 1813. With the dual channel application no security string is sent to the Users computer 1822 and instead it is sent to the mobile device 1804 via SMS.

[0137] As seen in FIG. 18, the Security String is sent from authorization computer 1807 to the User's mobile device 1804. The user inputs the TAC via the Pin Safe interface 1823 and the Authorization Server 1807 receives the TAC via the Internet 1813.

[0138] In the single channel Thin Client application, as seen in FIG. 19, the Pin Safe interface applet 1923 resides on the Authorization Server 1907. The User 1901 accesses this applet 1923 remotely from any computer 1922 and does not need to 'set up' the computer 1922 by pre-downloading any form of program beforehand. As seen in FIG. 19, the User accesses the Authorization Server 1907 and applet 1923 via the Internet 1913. The User 1901 inputs their PIN, which is correlated at the source or Authorization Server 1907.

[0139] In the single channel Applet application, as seen in FIG. 20, the Pin Safe interface applet 2023 resides on the users computer 2022. The applet 2023 needs downloading only once and would be automatically sent to the user's computer 2022 during the registration process. The Pin Safe interface has been specifically designed with an extremely small memory footprint making the process of downloading and use very fast.

[0140] As seen in FIG. 20, the User accesses the Authorization Server 2007 via the Internet 2013. The user 2001 inputs their PIN, which the applet 2023 converts into a TAC (it does this automatically using the volatile security string resident in the applet 2023) and then sends, via the Internet 2013, for correlation at the Authorization Server 2007.

[0141] FIG. 21, shows a typical data access application where an Authorization Server 2107 has been fitted to a Gateway Server 2109 accessing a Database 2111. FIG. 21 assumes that the user 2101 has registered with the system and has the Pin Safe Interface applet 2123 on their computer. To access information from the Database 2111 the Authorization Server 2107 sends a new security string to the user's computer or G2 mobile phone 2104 via the Internet 2113 or through a wireless connection 2151. The security string 2151 resides on the device 2104 until the user 2101 wishes to access the Database 2111.

[0142] The User 2101 sends his volatile TAC to the Authorization Server 2107 to confirm his/her identity. In the dual channel scenario the user obtains their TAC from the G2 mobile device 2104 via either visual extraction (using their PIN as a sequencer) or Smart PIN or SIMM extraction where the User 2101 enters their PIN into the device 2104 and the relevant TAC digits are displayed on the device 2104 screen. The TAC is then inputted into the user's computer (not shown). In the single channel scenario the user simply inputs their PIN into the Pin Safe interface 2123. The PIN is then converted into a TAC within the applet 2123 and transmitted via path 2120 to the Authorization Server 2107.

[0143] Only when the user's identification is positively confirmed, by correlating the received TAC to the user's PIN and previously issued security String is the request 2130 for data, via the Gateway Server 2109, initialized via path 2130. The requested data can now be routed via path 2140 to the user's computer.

[0144] The Pin Safe interface is not required if the security string delivery and TAC extraction are conducted on a second device such as through the dual channel protocol. Using a G2 mobile phone a user can receive a security string and extract the TAC independent of the data accessing computer. This means that the TAC can be entered into the data accessing computer without the requirement of the Pin Safe interface because a TAC is inherently secure against shoulder surfing, Trojans, Tempest technologies and online user identification theft.

[0145] FIG. 22 displays a generic Server/Gateway Schema incorporating various aspects of the present invention. The generic secure server schema may also incorporate UPS (Uninterruptible Power Supply), Dual Redundancy, Disk Mirrored, Linux Web Server 2245 and Internal Firewall 2215, the Pin Safe applet 2223, a user database 2207 and an internal maintenance any reporting function 2211.

[0146] FIG. 23 shows the Generic Integration Platform which displays the Authorization Server 2307 inside a firewall 2215. The Authorization Server 2307 is connected to a Net Server 2317 and a host database 2311. The host database 2311 may also be inside it's own firewall 2316.

[0147] Additionally the authorization process identifies the user via a response rather than an identifying account and its parameters which negates the so called "Friendly Fraud" from misuse of online fraud guarantees. An added benefit is that there is also an audit trail for database files access.

[0148] Any reference herein to a computer means any personal computer, ATM, PDA, G2.5 Mobile Device, G3 Mobile Device, or any device with a CPU. Any reference herein to a transaction means any financial transaction, remote Data Access procedure, or any interface transaction between a user and a system. The numbers on the various user interfaces and displays are merely exemplary and the use of characters, letters, colors and such may be used individually or in combination and still fall within the intended scope of the present invention.

[0149] While the preferred embodiment and various alternative embodiments of the invention have been disclosed and described in detail herein and by way of example, it will be apparent to those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope thereof, and that the scope of the present invention is to be limited only by the following claims.

Espacenet

Claims: CN1561508 (A) — 2005-01-05

Code identification method and system

Claims not available for CN1561508 (A)
Claims of corresponding document: US2002029342 (A1)

A high quality text as facsimile in your desired language may be available amongst the following family members:

AU2005100466 (B4) CA2421495 (A1) DK1316076 (T3) ES2403039 (T3) JP2004508644 (A) KR20030036766 (A) MXPA03002050 (A) NZ524391 (A) PT1316076 (E) US2002029342 (A1) WO0221463 (A2) US2002059146 (A1)

- Original claims
- Claims tree

The EPO does not accept any responsibility for the accuracy of data and information originating from other authorities than the EPO; in particular, the EPO does not guarantee that they are complete, up-to-date or fit for specific purposes.

1. An identity verification secure transaction system comprising:
a host computer for storing a user code associated with a user, for supplying a pseudo-random security string for a transaction, wherein said host computer determines a one time transaction code by applying said user code to said pseudo-random security string; and
at least one electronic device in electronic communication with said host computer for administering said transaction by receiving and displaying said pseudo-random security string and for receiving a user transaction input code, wherein said user transaction input code is determined by applying said user code to said pseudo-random security string displayed on said at least one electronic device and said user transaction input code is sent to said host computer;
wherein said host computer verifies that said user input code matches said one time transaction code.

2. The system of claim 1, wherein said at least one electronic device is an Electronic Funds Transfer Point of Sale (EFT/POS) device.

3. The system of claim 1, wherein said at least one electronic device is comprised of an electronic Funds Transfer Point of Sale (EFT/POS) device for administering said transaction and receiving said user transaction input code and a wireless device associated with said user for receiving and displaying said pseudo-random security string.

4. The system of claim 3, where said one time transaction code is received and

displayed by said wireless device instead of said pseudo-random security string.

5. The system of claim 1, wherein said at least one electronic device is a wireless device associated with said user.

6. The system of claim 5, wherein said one time transaction code is sent to said wireless device instead of said pseudo-random security string.

7. The system of claim 1, wherein said at least one electronic device is comprised of:
a user computer, in electronic communication with said host computer, for receiving and displaying said pseudo-random security string and receiving said user transaction input code; and
a merchant computer, in electronic communication with said user computer and said host computer, for administering said transaction, wherein one of said at least one electronic device relays said user transaction input code to said host computer for user identity verification.

8. The system of claim 7, wherein said user computer and said merchant computer communicate via the Internet.

9. The system of claim 7, wherein said one time transaction code is received and displayed by said user computer instead of said pseudo-random security string.

10. The system of claim 1, wherein said at least one electronic device is comprised of:
a wireless device associated with said user for receiving and displaying said pseudo-random security string,
a user computer, in electronic communication with said host computer, for receiving said user transaction input code; and
a merchant computer, in electronic communication with said user computer and said host computer, for administering said transaction, wherein one of said at least one electronic device relays said user transaction input code to said host computer for user identity verification.

11. The system of claim 10, wherein said one time transaction code is received and displayed by said wireless device instead of said pseudo-random security string.

12. The system of claim 1, wherein said host computer upon verification allows completion of said transaction.

13. The system of claim 1, wherein said host computer upon verification allows access to a database.

14. The system of claim 1, wherein said host computer upon verification allows access to account information.

15. A method of verifying an identity for conducting secure transactions comprising the steps of:
storing information about a user pin associated with a host computer;
generating a pseudo-random security string by said host computer;
determining a transaction code by applying said user pin to said pseudo-random security string;
transmitting said pseudo-random security string to at least one electronic device,
displaying said pseudo-random security string on said at least one electronic device for use by said user to determine a user transaction input code by applying said user code

to said pseudo-random security string;
inputting said user transaction input code on said at least one electronic device;
transmitting said user transaction input code from said at least one electronic device to said host computer; and
determining, by said host computer, whether said transaction code and said user transaction input code match.

16. The method of claim 15, further including the step of completing a transaction when said transaction code and said user transaction input code match.

17. The method of claim 16, further including the step of providing access to a database when said transaction code and said user transaction input code match.

18. The method of claim 16, further including the step of providing access to account information when said transaction code and said user transaction input code match.

19. The method of claim 15, further including the step of transmitting and displaying said pseudo-random security string on an Electronic Funds Transfer Point of Sale (EFT/POS) device.

20. The method of claim 15, further including the step of transmitting and displaying said pseudo-random security string on a wireless device associated with said user.

21. The method of claim 15, further including the step of transmitting and displaying said pseudo-random security string on a user computer wherein said user computer is in electronic communication with said host computer.

22. The method of claim 21, further including the step of communicating between the said host computer and said user computer via the Internet.

23. The method of claim 15, further including the step of transmitting and display said transaction code to said at least one electronic device.

24. A secure user code entry interface system comprising:
a secure user code entry interface for entry of a user code on an electronic device wherein said electronic device has a display; wherein said secure user code entry interface contains at least one active display for entry of at least one digit of said user code by a user; wherein said active display illuminates at least one display digit within said active display and said user enters said at least one digit of said user code by a response through an input device at a response time when said at least one display digit which corresponds with said at least one digit of said user code is illuminated in said active display; and
a random run on time is added to said response time to extend said at least one active display.

25. The secure user code entry interface system of claim 24, wherein said response is entered by keying any one of a plurality of keys of a keyboard.

26. The secure user code entry interface system of claim 24, wherein said response is entered by keying any one of a plurality of keys of a mouse.

27. The secure user code entry interface system of claim 24, wherein said response is entered through any area of a touch sensitive display.

28. The secure user code entry interface system of claim 24, wherein said secure user code entry interface program contains a plurality of cycles of said at least one active displays for entry of each digit of said user code.

29. The secure user code entry interface system of claim 24, wherein said random run on time is less than three (3) seconds.

30. An identity verification secure transaction system comprising:
a host computer for storing a user code associated with a user;
an electronic device in electronic communication with said host computer, wherein said electronic device has a display and a user input device; and
a secure user code entry interface viewable on said display of said at least one electronic device for entry of said user code, wherein said secure user code entry interface contains at least one cycle with an active display for entry of said user code;
wherein said user enters at least one user code digit of said user code by a response through said user input device at a response time when a display digit which corresponds with said at least one user code digit of said user code is illuminated in said active display, and
wherein said each digit of said at least one user code digit if entered in each cycle of said at least one cycle and a random run on time is added to said response time to extend each cycle of said at least one cycle; and
wherein the entered said user code is transmitted to said host computer for verification with the stored said user code.

31. The identity verification secure transaction system of claim 30, wherein said response is entered by keying any one of a plurality of keys of a keyboard.

32. The identity verification secure transaction system of claim 30, wherein said response is entered through any area of a touch sensitive display.

[19] 中华人民共和国国家知识产权局

[51] Int. Cl^7
G07F 19/00
G07F 7/10 H04L 9/18

[12] 发明专利申请公开说明书

[21] 申请号 01812009.1

[43] 公开日 2005 年 1 月 5 日

[11] 公开号 CN 1561508A

[22] 申请日 2001.9.7 [21] 申请号 01812009.1
[30] 优先权
[32] 2000. 9. 7 [33] GB [31] 0021964.2
[32] 2000. 9.15 [33] US [31] 09/663,281
[32] 2001. 7.27 [33] US [31] 09/915,271
[86] 国际申请 PCT/GB2001/004024 2001.9.7
[87] 国际公布 WO2002/021463 英 2002.3.14
[85] 进入国家阶段日期 2003.3.7

[71] 申请人 斯维沃安全有限公司
地址 英国北约克郡
[72] 发明人 温斯顿·唐纳德·基奇

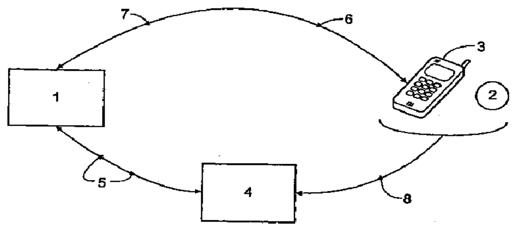
[74] 专利代理机构 北京英赛嘉华知识产权代理有限责任公司
代理人 余 朦 陈宇萱

权利要求书 9 页 说明书 32 页 附图 24 页

[54] 发明名称 代码识别方法及系统

[57] 摘要

一种用于在电子通信环境中安全识别个人的系统和方法，其中一台计算机主机被改造成能与由个人操作的一个特定电子通信设备进行通信。 个人被配备了一个掩码，该掩码只为个人所知并且保存在计算机主机中，但是从来不在个人与计算机主机之间电子传送。 当个人需要使其自身被计算机主机识别出来的时候，计算机主机向特定电子通信设备发送一个伪随机字串，而掩码则必须根据预定规则被应用于该伪随机字串，用以产生一个易失性识别码，该易失性识别码随后被回送到计算机主机。当该易失性识别码与计算机主机中通过将其中保存的掩码应用于伪随机字串所得到易失性识别码相匹配时，计算机主机将会获得一个肯定的识别结果。这样，个人的掩码从未被电子传送，由此避免被截取，并且对每个不同的伪随机字串来说，易失性识别码各不相同，由此使通过欺诈截获的通信变得毫无意义。



ISSN 1008-4274

1. 一种代码识别系统，该系统包括一台电子计算机，一个特定电子通信设备，该设备可被操作而与电子计算机通信，以及至少一个电子通信设备，该设备可被操作用于与电子计算机进行通信，其中，所述电子计算机包含涉及所述特定电子通信设备的数据，该数据包括一个永久识别码、一个掩码和一个允许实现电子计算机与特定通信设备之间电子通信的识别码，其中所述永久识别码被输入至所述少一个电子通信设备并被发送到所述电子计算机，所述电子计算机产生一个伪随机字串并将其发送到所述特定电子通信设备，所述掩码被应用于所述伪随机字串，以便根据预定规则产生一个易失性识别码，所述易失性识别码由所述特定电子通信设备或所述至少一个电子通信设备被回送给所述电子计算机，所述电子计算机通过将所述掩码根据预定规则应用于所述伪随机字串，从而获取一个易失性识别码，并对照该易失性识别码来检查发送到其自身的易失性识别码，其中，在所述电子计算机发现这两个易失性识别码相互匹配时，它将产生一个肯定的识别结果；该方法的特征在于：

i）所述伪随机字串包含一个由字符组成的第一线性阵列，在该第一阵列中，每个字符都具有一个指定的数字位置（第一、第二、第三等等）；

ii）所述掩码包含一个由数字组成的第二线性阵列，在该第二阵列中，每个数字都具有一个指定数字位置（第一、第二、第三等等）；以及

iii）用于将所述掩码应用于所述伪随机字串以产生所述易失性识别码的预定规则根据所述第二阵列中的数字按照位置顺序依次选择所述第一阵列中的数子位置，并且顺序地返回由所述第一阵列中选出的字符以形成一个第三线性阵列，该第三线性阵列形成了所述易失性识别码。

2. 如权利要求1所述的系统，其特征在于，所述特定电子通信设备和所述至少一个电子通信设备是同一设备。

3. 如权利要求1所述的系统，其特征在于，所述特定电子通信设备和所述至少一个电子通信设备是单独的设备。

4. 如上述权利要求中的任意一项权利要求所述的系统，其特征在于，所述特定电子通信设备是移动电话、寻呼机或个人数字助理。

5. 如权利要求3或从属于权利要求3的权利要求4所述的系统，其特征在于，所述至少一个电子通信设备是一个EFTPOS终端或类似设备。

6. 如上述权利要求中的任意一项权利要求所述的系统，其特征在于，所述永久识别码以带有个人和/或机器可读的标记的形式而被提供。

7. 一种用于将一特定电子通信设备或是其用户识别给电子计算机的方法，所述电子计算机上存有涉及所述特定电子通信设备或其用户的数据，该数据包括一个永久识别码、一个掩码和一个允许实现所述电子计算机与所述特定通信设备之间的电子通信的识别码，其中所述永久识别码被输入给至少一个电子通信设备并由此被发送到所述电子计算机，所述电子计算机将所述永久识别码与允许实现电子计算机与特定电子通信设备之间通信的所述识别码相关联，并且在将该识别码被发送到特定电子通信设备之前产生一个伪随机字串，所述掩码根据预定规则而被应用于该伪随机字串，用以产生一个易失性识别码，该易失性识别码被输入给所述特定电子通信设备或所述至少一个电子通信设备，并被传送给所述电子计算机，在所述电子计算机中，所述易失性识别码被与所述电子计算机中通过将所述掩码根据预定规则应用于伪随机字串而产生的一个易失性识别码进行比较，当这两个易失性识别码匹配时，所述计算机将产生一个肯定的识别结果；该方法的特征在于：

i）所述伪随机字串包含一个由字符组成的第一线性阵列，在该第一阵列中，每个字符都具有一个指定的数字位置（第一、第二、第三等等）；

ii）所述掩码包含一个由数字组成的第二线性阵列，在该第二阵列中，每个数字都具有一个指定的数字位置（第一、第二、第三等等）；以及

iii）用于将所述掩码应用于所述伪随机字串以产生所述易失性识别码的预定规则根据所述第二阵列中的数字按照位置顺序依次选择所述第

一阵列中的数字位置，并且顺序地返回由所述第一阵列中选出的字符以形成一个第三线性阵列，该第三线性阵列形成了所述易失性识别码。

8. 如权利要求7所述的方法，其特征在于，所述伪随机字串包含至少一个字符，该字符代表的是涉及个人的数据的某个条件。

9. 如权利要求7或8所述的方法，其特征在于，所述特定电子通信设备和所述至少一个电子通信设备是同一设备。

10. 如权利要求7或8所述的方法，其特征在于，所述特定电子通信设备和所述至少一个电子通信设备是单独的设备。

11. 如权利要求9或10所述的方法，其特征在于，所述特定电子通信设备是移动电话、寻呼机或是个人数字助理。

12. 如权利要求10或从属于权利要求10的权利要求11所述的方法，其特征在于，所述至少一个电子通信设备是一个EFTPOS终端或类似设备。

13. 一种身份验证安全交易系统，包括：

i）一台计算机主机，用于存储与用户关联的用户代码，用于为交易提供一个伪随机安全字串，其中，所述计算机主机通过将所述用户代码应用于所述伪随机安全字串来确定一个一次性交易代码；

ii）至少一个电子设备，该设备通过接收并显示所述伪随机安全字串与用于管理交易的所述计算机主机进行电子通信，并且用于接收一个用户交易输入代码，其中，所述用户交易输入代码是通过将所述用户代码应用于显示在所述至少一个电子设备上的所述伪随机安全字串来确定的，并且所述用户交易输入码被发送到所述计算机主机；其中：

iii）所述计算机主机验证所述用户输入代码与所述一次性交易码相匹配。

14. 如权利要求13所述的系统，其特征在于，所述至少一个电子通信设备是一个交易点资金电子过户（EFT/POS）设备。

15. 如权利要求13所述的系统，其特征在于，所述至少一个电子通信设备包括一个用于管理所述交易并接收所述用户交易输入代码的交易点资金电子过户（EFT/POS）设备，以及一个与所述用户关联并用于接收和显示所述伪随机安全字串的无线设备。

16. 如权利要求15所述的系统，其特征在于，所述无线设备接收和显示的是所述一次性交易码，而不是所述伪随机安全字串。

17. 如权利要求13所述的系统，其特征在于，中所述至少一个电子设备是一个与所述用户关联的无线设备。

18. 如权利要求17所述的系统，其特征在于，发送到所述无线设备的是所述一次性交易码，而不是所述伪随机安全字串。

19. 如权利要求13所述的系统，其特征在于，所述至少一个电子设备包括：

i）一台用户计算机，它与所述计算机主机进行电子通信，用于接收和显示所述伪随机安全字串，并且接收所述用户交易输入代码码；以及

ii）一台商家计算机，它与所述用户计算机和所述计算机主机进行电子通信，用于管理所述交易，其中，所述至少一个电子设备中的一个设备将所述用户交易输入代码转达给所述计算机主机，以便进行用户身份验证。

20. 如权利要求19所述的系统，其特征在于，所述用户计算机和所述商家计算机通过互联网通信。

21. 如权利要求19或20所述的系统，其特征在于，所述用户计算机接收和显示的是所述一次性交易码，而不是所述伪随机安全字串。

22. 如权利要求13所述的系统，其特征在于，所述至少一个电子设备包括：

i）一个与所述用户关联的无线设备，用于接收和显示所述伪随机安全字串；

ii）一台用户计算机，它与所述计算机主机进行电子通信，用于接收所述用户交易输入代码；以及

iii）一台商家计算机，它与所述用户计算机和所述计算机主机进行电子通信，用于管理所述交易，其中，所述至少一个电子设备中的一个设备将所述用户交易输入代码转达给所述计算机主机，以便进行用户身份验证。

23. 如权利要求22所述的系统，其特征在于，所述无线设备接收和显示的是所述一次性交易码，而不是所述伪随机安全字串。

24. 如权利要求13到23中的任一权利要求所述的系统，其特征在于，所述计算机主机基于验证来允许完成所述交易。

25. 如权利要求13到24中的任一权利要求所述的系统，其特征在于，所述计算机主机基于验证来允许访问一数据库。

26. 如权利要求13到25中的任一权利要求所述的系统，其特征在于，所述计算机主机基于验证来允许访问一账户信息。

27. 一种用于通过验证身份以实施安全交易的方法，包括以下步骤：

i）保存与一计算机主机有关的用户 pin 的信息；

ii）由所述计算机主机产生一个伪随机安全字串；

iii）通过将所述用户 pin 应用于所述伪随机安全字串来确定一个交易

代码;

iv）将所述伪随机安全字串传送给至少一个电子设备;

v）将所述伪随机安全字串显示在所述至少一个电子设备上，以便由所述用户通过将所述用户代码应用于所述伪随机安全字串来确定一个用户交易输入代码;

vi）在所述至少一个电子设备上输入所述用户交易输入代码;

vii）将所述用户交易输入代码从所述至少一个电子设备发送到所述计算机主机; 以及

viii）由所述计算机主机确定所述交易代码是否与所述用户交易输入代码相匹配。

28. 如权利要求27所述的方法，其特征在于还包括以下步骤: 当所述交易代码和所述用户交易输入代码相匹配时，完成交易。

29. 如权利要求27或28所述的方法，其特征在于还包括以下步骤: 当所述交易代码和所述用户交易输入代码相匹配时，提供对一数据库的访问。

30. 如权利要求27到29中的任一权利要求所述的方法，其特征在于还包括以下步骤: 当所述交易代码和所述用户交易输入代码相匹配时，提供对账户信息的访问。

31. 如权利要求27到30中的任一权利要求所述的方法，其特征在于还包括以下步骤: 在一个交易点资金电子过户（EFT/POS）设备上传送和显示所述伪随机安全字串。

32. 如权利要求27到30中的任一权利要求所述的方法，其特征在于还包括以下步骤: 在一个与所述用户关联的无线设备上传送和显示所述伪随机安全字串。

33. 如权利要求27到30中的任一权利要求所述的方法，其特征在于还包括以下步骤：在一用户计算机上传送和显示所述伪随机安全字串，其中，所述用户计算机与所述计算机主机进行电子通信。

34. 如权利要求33所述的方法，其特征在于还包括以下步骤：所述计算机主机和所述用户计算机之间通过互联网进行通信。

35. 如权利要求15所述的方法，其特征在于还包括以下步骤：将所述交易代码发送给所述至少一个电子设备，并在所述至少一个电子设备上显示该交易代码。

36. 一种安全的用户代码输入界面系统，包括：

i）一个安全的用户码输入界面，用于在一电子设备上输入用户代码，其中所述电子设备具有一个显示器；其中所述安全的用户码输入界面包含至少一个发光显示，用于使所述用户输入所述用户代码中的至少一位数字；其中所述发光显示照明或加亮所述发光显示中的至少一位显示数字，并且，当符合所述用户代码中至少一位数字的所述至少一位显示数字在所述发光显示上被照明或加亮的时候，所述用户在应答时间通过一个输入设备做出一个应答以输入所述用户代码中的至少一位数字；并且其中

ii）一个随机的连续时间被添加到所述应答时间中，以便延长所述至少一个发光显示。

37. 如权利要求36所述的安全的用户代码输入界面系统，其特征在于，所述响应是通过点击一个键盘上多个按键中的任意一个按键而被输入的。

38. 如权利要求36所述的安全的用户代码输入界面系统，其特征在于，所述响应是通过点击一鼠标的多个按键中的任意一个而被输入的。

39. 如权利要求36所述的安全的用户代码输入界面系统，其特征在于，所述响应是通过一触摸显示上的任意区域而被输入的。

40. 如权利要求36到39中的任一权利要求所述的安全的用户代码输入界面系统，其特征在于，所述安全的用户代码输入界面程序包含所述至少一个发光显示的多个循环，用以输入所述用户代码中的各位数字。

41. 如权利要求36到40中的任一权利要求所述的安全的用户代码输入界面系统，其特征在于，所述随机的连续时间少于三（3）秒钟。

42. 一种身份验证安全交易系统，包括：

i）一台计算机主机，用于保存一个与用户关联的用户代码；

ii）一个电子设备，它与所述计算机主机进行电子通信，其中，所述电子设备具有一个显示器和一个用户输入设备；以及

iii）一个安全的用户代码输入界面，它在所述至少一个电子设备的用于输入所述用户代码的所述显示器上是可视的，其中，所述安全的用户代码输入界面包含至少一个具有用于输入所述用户代码的发光显示的循环；其中，当符合所述用户代码中所述至少一个用户代码数字的显示数字在所述发光显示中被照明或是被加亮的时候，所述用户在应答时间使用所述用户输入设备做出一个响应以输入所述用户代码中至少一个用户码数字；

iv)其中所述至少一位用户代码数字中的所述各位数字是在所述至少一个循环的各个循环中被输入的，并且一个随机的连续时间被添加到所述应答时间，以延长所述至少一个循环的每个循环；以及

v）其中，输入的所述用户代码被发送到所述计算机主机，以便用保存的所述用户代码来加以验证。

43. 如权利要求42所述的身份验证安全交易系统，其特征在于，所述响应通过点击一键盘上多个按键中的任意一个而被输入。

44. 如权利要求42所述的身份验证安全交易系统，其特征在于，所述响应是通过一触摸显示上的任意区域而被输入的。

代码识别方法及系统

本发明涉及一种用于识别用户或设备的系统和方法，这种系统和方法还能够被可选地用于例如经由电话连接或是互联网这类电子计算机系统在用户或设备与第三方之间进行交易。

各种系统由于在电信链路或其他链路上使用程度不同的安全方式来执行电子交易而闻名。一种有名的系统称为销售点资金电子过户（EFTPOS），在这种系统中，用户获得一张带有唯一识别代码的信用卡或借记卡，该识别代码通常以个人可读的形式印在卡上，并且还被编码在卡背面的机器可读磁条中。出于进一步识别的目的，卡上通常还包含有使用户在其中永久包含他或她的签名的空间。在使用中，例如用户希望在零售店购买物品时，他或她把借记卡或信用卡交给商店雇员。然后该卡由一个读卡器刷取，涉及卡身份、零售店身份和所购买商品或服务价格的信息通过电话连接被发送到由发卡方（通常是银行或类似机构）操作的远程计算机服务器上。远程计算机服务器证实用户卡账户包含足以支付所提出的交易的资金或信用，并且检查用户卡账户当前是可以使用的（举例来说，检查卡没有被挂失），然后，远程计算机服务器向读卡器发回一个证实信号，指示可以允许交易。之后，商店雇员必须获取用户签名样本，并将其与磁卡背面的签名比较，以便检查用户身份。如果签名看上去匹配，那么商店雇员操作读卡器来完成交易，然后，支付交易费用所需要的资金被从用户卡账户电子过户到零售店。如果签名看上去不匹配，那么在许可交易之前，商店雇员可以要求附加的证据鉴定，也可以简单地直接拒绝交易并且保留可能是被盗的用户卡，由此防止了任何未经许可的资金过户。这个系统很容易受到欺诈性滥用，因为对失窃卡和窃贼来说，有可能伪造授权用户的签名。

在一个对上述系统的改进方案中，持卡用户可被分配一个个人识别号（PIN），该识别号通常是一个四位编码，并且理论上只有用户和发卡

方知道这个识别号。代替在销售点提供他或她的签名样本，或是除了在销售点提供他或她的签名样品之外，持卡用户还需要将其PIN输入读卡器，这个信息与卡和零售店识别数据以及涉及交易价格的数据一起被发送到远程计算机服务器。通过使用PIN来提供附加的识别验证，这个系统有助于防止通过伪造签名实施的欺诈行为，但是该系统仍然不是完全安全的，因为PIN在几次交易之间并未改变，因此，当PIN在读卡器与远程服务器之间被传送时，PIN有可能与卡识别数据一起被截取。此外，对窃贼来说，有可能看到用户将他或她的PIN输入读卡器并记住PIN。如果窃贼也能通过例如丢弃的现金收据、或是与商店雇员合谋而得到卡识别资料、或者甚至抢劫已授权卡的用户的卡，那么制造一张包含所有适当识别信息的伪造卡以用于以后的欺诈性使用将是一件非常简单的事情。

根据本发明的第一方面，它提供了一种经过编码的识别系统，该系统包括一台电子计算机；一个特定电子通信设备，该设备可被操作而与电子计算机通信；以及至少一个电子通信设备，该设备可被操作而与电子计算机通信，其中，电子计算机包含与所述特定电子通信设备有关的数据，该数据包括一个永久识别码、一个掩码以及一个允许实现所述电子计算机和所述特殊通信设备之间电子通信的识别码，其中永久识别码被输入至少一个电子通信设备并被发送到电子计算机，电子计算机产生一个伪随机字串并将其发送到所述特定电子通信设备，所述掩码被应用于该伪随机字串以便根据预定规则产生一个易失性识别码，该易失性识别码由所述特定电子通信设备或是至少一个电子通信设备回送到电子计算机，电子计算机根据预定规则将掩码应用于伪随机字串，从而获取一个易失性识别码，并对照该易失性识别码来检查发送到其自身的易失性识别码，其中，当这两个易失性识别码相互匹配的时，电子计算机将做出一个肯定的识别结果。

根据本发明的第二方面，它提供了一种用于将特定电子通信设备或是其用户识别给电子计算机的方法，该电子计算机中保存有与所述特定电子通信设备或是其用户有关的信息，其中包括一个永久识别码、一个掩码和一个允许实现电子计算机和特定电子通信设备之间通信的识别码，其中，所述永久识别码被输入至少一个电子通信设备，由此被传送

到电子计算机，电子计算机将永久识别码与允许实现电子计算机与特定电子通信设备之间通信的识别码相关联，并且在将该识别码发送到所述特定电子通信设备之前产生一个伪随机字串，掩码根据预定规则而被应用于所述伪随机字串，以便产生一个易失性识别码，该易失性识别码被输入所述特定电子通信设备或至少一个电子通信设备，并被传送到电子计算机，在电子计算机中，所述易失性识别码被与一个通过将掩码应用于伪随机字串而产生的易失性识别码进行比较，当这两个易失性识别码相互匹配时，电子计算机将得出一个肯定的识别结果。

所述特定电子通信设备可以是一个独立于所述至少一个电子通信设备的设备，也可以是同一设备。举例来说，该特定电子通信设备可以是移动电话、寻呼机、陆线电话、个人数字助理或是由特定人员拥有或专门操作的计算机。所述至少一个通信设备可以是一个资金电子过户(EFT)终端或是一个销售点资金电子过户（EFTPOS）终端，也可以是与上面相同，是移动电话、寻呼机、陆线电话、个人数字助理或是由特定人员拥有或专门操作的计算机。

所述永久识别码可以按照持卡人和/或机器可读数据的卡的形式提供给用户。

在所述特定电子通信设备是移动电话、寻呼机或个人数字助理的情况下，实现电子计算机和特定电子通信设备之间电子通信的识别码可以是移动电话号码或寻呼机号码，识别码还可以是电子邮件地址或是任何允许与给出的特定电子通信设备之间进行特定通信的类似代码。

在特定电子通信设备是移动电话或类似设备的情况下，伪随机字串可以按照基于短信服务（SMS）协议的文本消息形式发送。根据特定电子通信设备的性质，在合适情况下，也可以采用其它公知的通信协议。

本发明的实施例以多种方式提供了附加的识别安全性。首先，除了要求个人使用永久识别码之外，系统还要求个人拥有一个适当的特定电子通信设备。其次，由于系统需要用户将其掩码作用于伪随机字串以在不同时传送掩码以及永久识别码的情况下根据预定规则产生一个易失性识别码，因此，对非授权人员来说，要对电子计算机、特定电子通信设备和/或至少一个电子通信设备之间的通信进行截取以确定掩码和永久识

别码将是非常困难的。

可以预见，本发明能够扩展到这样一种情况，其中有必要建立特定电子通信设备的安全识别，而不是个人安全识别。举例来说，本发明可被用作远程计算机之间安全“握手”协议的一部分，确实并可靠地用于将特定电子通信设备识别给电子计算机，其中特定电子通信设备自身就可能是一台电子计算机。电子计算机和特定电子通信设备都把掩码保存在自己的存储器中，但是除了经由安全连接之外，它们不会相互交换掩码，理论上，安全连接与它们的正常通信装置是完全分离的。

掩码可以采用多种形式。在一个当前的优选实施例中，一个人被配备或选择一个四位数字串，例如 3928，该数字串类似于当前在操作自动柜员机（ATM）时使用的公知 PIN 码。不过，如果恰当的话，也可以使用不同长度的掩码。响应于至少一个电子通信设备发送的信号而被发送到特定电子通信设备的伪随机字串（可以是数字、字母或是其它任意字符组合）能以预定形式被显示出来，其中组成伪随机字串的字符最好被显示成一个线性阵列。然后，操作特定电子通信设备的个人选取其掩码的第一位数字，本实例中为 3，并将该字符记录在伪随机字串的第三个位置上（假定从左往右）。之后，该人员选取掩码中的第二位数字，在本实例中为 9，并将该字符记录在伪随机字串的第九个位置上，依此类推再记录掩码中的数字 2 和 8。从伪随机字串中选出的字符形成了易失性识别码，该易失性识别码随后被输入至少一个电子通信设备，并被发送到电子计算机进行验证。另外，该易失性识别码也可以通过特定电子通信设备被发送到电子计算机。如果电子计算机接收的易失性识别码与电子计算机通过将掩码应用于伪随机字串而计算出来的一个预期的识别码相对应，则一个肯定的识别结果将被产生。这种机制的主要安全特征在于，掩码从未在电子计算机、特定电子通信设备或是至少一个电子通信设备之间被传送，由此防止了未授权第三方的截取。其辅助安全特征在于，人员必须拥有他或她自己的特定电子通信设备，因为电子计算机只向该设备发送伪随机字串。

对于其它的安全性来说，在易失性识别码被发送到电子计算机进行验证并且被发现与电子计算机生成的易失性识别码相互匹配之后，电子

计算机可以向特定电子通信设备发送一个消息，要求个人确认识别是正确的。只有当个人从特定电子通信设备向电子计算机发送一个确认消息以对该消息做出肯定的应答时，验证过程才最终结束。

在本发明的某些实施例中，对操作特定电子通信设备的人员来说，没有必要查看伪随机字串以及手动将掩码应用于该字串。取而代之的是，可以在特定电子通信设备的存储器中配备一个计算机程序，该程序能使个人在被提示的时候输入他或她自己的掩码，然后自动将掩码应用于伪随机字串，并返回恰当的易失性识别码，从而将该易失性识别码输入特定电子通信设备或是至少一个电子通信设备。

在另一个改进中，伪随机字串中至少一个位置可被选择以用于包含一个代表预定参数或是条件的字符。比较有利的是，该字符的位置和它所代表的意义仅仅为电子计算机和操作特定电子通信设备的个人所知。例如，在电子计算机由银行操作并且永久识别码是个人银行账号的情况下，伪随机字串中的一个位置，假设是第七位，该位置可被选择用于代表个人银行账户的余额，例如 0 表示资金为零，9 表示余额超过 1000 英镑，数字 1 到 8 表示其间呈线性比例的余额。另外，为了实现更好的安全性，伪随机字串中至少有一个位置可被选择用于包含一个标记字符，该字符假定数字 1 到 5 中的任意一个表示低于 500 英镑的余额，而数字 6 到 9 则代表余额超过 500 英镑。很明显，其它许多代表性模式也可被采用以用来传送伪随机字串中的信息。由于伪随机字串中至少一个代表性字符的位置和意义最好能由个人选择，而不是遵循一种可能被非授权第三方得知的固定格式，因此，在传送过程中，要想提取伪随机字串中的有意义的信息，那将是非常困难的。此外，在接收到伪随机字串之后，可以要求个人识别至少一个代表性字符的位置和/或意义，由此在识别处理中提供了一个附加的安全层。

很明显，在上文描述的实施例中，伪随机字串必须达到至少十个字符的长度，因为由数字 0 到 9 组成的掩码要求伪随机字串中至少有十个位置是有用的。然而，普通技术人员可以了解，通过选择恰当的编码模式，不同的掩码和字串长度可以根据需要而被选择。需要强调的是，电子计算机响应于一个来自至少一个电子通信设备的识别请求而给出伪随

机字串，对每个请求来说，伪随机字串各不相同，因此，要想对一连串有可能被截取的伪随机字串和易失性识别码的给定掩码加以确定，这将是极为困难的。实际上，在特定电子通信设备独立于至少一个通信设备的实施例中，例如它们分别是移动电话和 EFTPOS 终端，伪随机字串和易失性识别码永远不会沿着相同路由（例如一个指定的临时电话连接）发送。在特定电子通信设备与至少一个电子通信设备是同一设备的实施例中，例如适于安全连接到电子计算机的远程计算机终端，伪随机字串可以沿着相同路由发送，但是不会在同一时间发送。在以后的实施例中，可以只对一个用于登录到电子计算机的初始请求加以考虑，如果该请求从关联个人的预定电话号码经由直接调制解调器链路发出，那么伪随机字串将沿着该调制解调器链路回送到远程终端，易失性识别码也经由相同的直接调制解调器连接传送到电子计算机。

在一个特别优选的实施例中，电子计算机由借记卡或信用卡的发卡方操作，特定通信设备是一个移动电话，至少一个电子通信设备是一个由零售商操作的 EFTPOS 终端，永久识别码是个人借记卡或信用卡账号，掩码是一个如上所述的四位数字，用于实现电子计算机和特定电子通信设备之间电子通信的识别码是一个移动电话的电话号码。需要理解的是，借记卡或信用卡的发卡方可以是一个银行，它发行能以个人当前账户资金来购买物品的标准借记卡，也发行能以信用账户来购买物品的信用卡，发卡方还可以是一个向用户发行专用借记卡的专家服务提供商，在这种情况下，用户必须准备资金，根据需要将其过户到服务提供商，从而保持与其专用借记卡账户关联的最小正平衡。

当个人首次从发卡方申请一个账户时，他或她将被分配一个账号和一张卡，卡上以通常方式记有持卡人的账号和姓名，例如将个人可读的标记印在卡上并在卡背面的磁条上提供机器可读的数据。个人必须向发卡方提供普通资料，例如姓名和家庭住址，以及他或她的移动电话号码。发卡方还有必要提供掩码或者就掩码与个人达成一致。掩码最好与卡分开发行，例如通过单独的邮政递送，并且掩码永远不与账号和/或电话号码一起传送。当个人希望使用借记卡或信用卡购买物品时，他或她把卡交给零售商。零售商通过 EFTPOS 终端刷卡，该终端然后与发卡方操作

的一台主机接通。卡/账户号以及包含购买价格的交易资料经由调制解调器链路发送到主机。然后，主机将卡/账户代码与个人的移动电话号码相关联，如果账户中有足以支付预期购买的资金，那么主机产生一个伪随机字串，该字串在蜂窝电信链路上经由例如SMS消息发送到移动电话。如前文所述，个人将掩码应用于伪随机字串，然后把由此产生的易失性识别码交给零售商。接下来，零售商将该易失性识别码输入EFTPOS终端，然后，该终端把这个数据返回至主机。在主机中，该数据被与个人的账户资料相关联，并与主机中产生并临时保存的一个易失性识别码相比较，该临时保存的识别码是通过将掩码应用于与个人无关的伪随机字串而产生的。如果这两个易失性识别码匹配，那么主机将一个确认信息发送到EFTPOS终端以授权交易，然后，支付购买所需要的资金被自动过户到零售商，并从个人卡的账户中记入借方。

在个人账户上的资金不足以支付购买所需要的费用的情况下，主机将向EFT终端发出一个交易未被批准的信号，并且可以向移动电话发送一个建议个人向账户中添加资金的消息。如果发现易失性识别码不匹配的情况下，主机可以向EFTPOS终端发送一个信息，以便通知零售商，然后零售商可以要求个人检查正确的易失性识别码已被生成，并提供正确的易失性识别码以便传送到主机。如果个人给出错误易失码的次数超出了预定次数，例如三次，那么主机可以因为怀疑盗用而临时中止个人的账户。然后，在账户被重新激活和/或发行新账号及新卡之前，个人必须携带其身份的适当证明来向发卡方提出申请。

在某些实施例中，个人可以通过他或她的移动电话而与中心计算机直接通信。这么做是有可能的，因为移动电话的传输中包含了移动电话的电话号码资料，并且主机能够将电话号码与卡的账号相关联。由此可以提供的一个有用特征，即，在信用卡或借记卡乃至移动电话被盗的情况下，可以激活一个紧急账户锁定。这种锁定可以通过向主机发送一个预定的锁定码来激活，例如9999。作为替换或是附加，锁定码也可以用掩码格式来发布，这在个人遭到抢劫或是被用暴力威胁，以至于要交出其卡号、电话号码以及掩码的情况下是非常有用的。

还有一个更为有用的安全特征可以被提供，其中，在易失性识别码

发送到电子计算机进行验证并被发现它与电子计算机产生的易失性识别码相匹配之后，电子计算机可以向移动电话发送一个消息，请求个人确认该交易是被认可的。这个消息可以采用SMS或语音邮件形式发送，并且可以包含交易资料。只有当个人用移动电话向电子计算机发送一个确认消息以对电子计算机发送的消息做出肯定应答的时候，交易才最终得到授权。

根据本发明这个实施例所述的信用卡或借记卡也可被用于在互联网上进行安全采购。在这种情况下，至少一个电子通信设备可以是互联网零售商操作的计算机服务器。当个人希望进行安全采购时，他或她借助电子邮件或是通过零售商网站向服务器提交账号，然后如先前那样，服务器将账户资料以及采购资料发送到发卡方操作的主机。之后，包含伪随机字串的SMS消息被发送到个人的移动电话，随后，个人产生一个易失性识别码并把它提交给零售商服务器，在许可交易和放出资金之前，该易失性识别码被从零售商服务器传送到主机进行验证。

个人在发卡方也可以具有不止一个账户，并且由此可以选择或被分配以一个以上的掩码，每个账户都有一个掩码。作为替换或是附加，每个账户可以被分配以一个以上的掩码，主机可以通过伪随机字串的一个或多个字符来指示它期待个人把从多个预定的掩码中选出的某个掩码应用于伪随机字串，并由此提供一个附加级别的安全性。

可以预见，本发明并不局限于信用卡或借记卡交易，它提供了一种在很多情况下进行识别的安全方法和系统。举例来说，可以通过提供一台中心计算机来控制对建筑物或交通工具的访问，该计算机拥有授权进入建筑物或交通工具的所有人员的资料，并且可以为每个授权进入建筑物或交通工具的人配备一张条卡，该条卡带有一个唯一识别码或磁编码格式的代码。在建筑物或交通工具的入口处可以提供连接到读卡器和电子键盘的电子锁，该读卡器和键盘能与中心计算机通信。当授权用户希望进入建筑物或交通工具时，他或她通过读卡器刷卡，该读卡器然后将唯一识别号或编码发送到中心计算机。中心计算机把唯一识别号或编码与个人的个人资料（其中包括预定掩码）关联起来，然后中心计算机把伪随机字串发送到键盘，以便在其上所具有的显示器中显示。然后个人

必须把他或她的掩码应用于伪随机字串，并将由此产生的易失性识别码输入键盘，之后，键盘将易失性识别码发送到中心计算机，以便如前所述，与计算机中产生的易失性识别码相比较。如果这两个易失性识别码匹配，那么中心服务器发出一个信号解开电子锁。这种系统所提供的一个显著的优点在于，它比通过键入预定编码来操作的现有电子锁更为先进，因为在个人每次进入建筑物或是交通工具的时候，他或她都必须输入一个不同的易失性识别码。这意味着潜在的窃贼或其他人无法通过观察被授权的个人键入入口代码并随后输入相同的入口代码来进入建筑物或交通工具。

此外，没有必要为每个被允许进入建筑物或交通工具的人员提供一张条卡。取而代之的是，每个人都配备一个唯一并且可存储的永久识别号或识别码，在需要进入建筑物或是交通工具的时候，该永久识别号或识别码可以通过电子键盘输入。然后，唯一永久识别号或识别码在中心计算机中与恰当的掩码相关联，并且一个伪随机字串被发送到电子键盘，以便如前文所述显示在电子键盘的显示器上。

可以预见，在以上实施例中，电子键盘和可选的读卡器形成了至少一个电子通信设备以及特定电子通信设备。对附加的安全性来说，虽然包含了额外的不便之处，但是准许进入建筑物或交通工具的个人可以拥有作为特定电子通信设备的移动电话，伪随机字串被发送到移动电话而不是被发送到电子键盘的显示器上。

对于本发明的方法和系统来说，其可选的应用包括任何在电子通信环境中需要个人安全识别的情况。例如，该系统和方法可用于保护远程登录计算机，并且用于保护普通电信（例如企业对企业的电子商务交易、空中交通管制通信等等），该系统和方法还可以被应用于交通工具的固定器和/或报警器上，由此交通工具的授权用户必需将一个掩码应用于伪随机字串，以便解除固定器或报警器。

本发明的另一个用途是充当一个安全的检票系统。旅行车票、音乐会入场券、电影票和戏票、体育比赛门票等等的供应商可以发行“虚拟”门票，该门票是以一个永久用户识别码和一个从主机传送到特定电子通信设备的伪随机字串作为形式。一旦到达集合地点或是应检票员的要求，

拥有该“虚拟”门票的个人需要将其掩码应用于伪随机字串并将由此生成的虚拟识别码连同永久用户识别码一起提供给检票员。检票员可以配备一个电子通信设备，借助于此设备，该信息被回送到主机进行验证，如果个人被认定是一个许可的持票人，那么主机向电子通信设备发送一个确认信号。

本发明还可被用于承运包裹的车站或是邮件库房，例如邮局、目录商店或是仓库等等，人们前往那些地方领取包裹、邮件或其它物品，在移交包裹、邮件或其他物品之前，绝对有必要对个人进行识别。领取物品的个人会被分配一个伪随机字串，在收取的时候，他将被要求提供一个易失性识别码，该识别码是通过将其掩码应用于伪随机字串而产生的。

根据本发明的第三个方面，它提供了一种身份验证安全交易处理系统，该系统包括：

i）一台计算机主机，它用于存储与用户关联的用户码，为交易提供一个伪随机安全字串，其中所述主机通过将所述用户码应用于所述伪随机安全字串来确定一个一次性交易码；

ii）至少一个电子设备，该设备通过接收并显示所述伪随机安全字串来与管理所述交易的所述主机进行电子通信，并且接收一个用户交易输入码，其中所述用户交易输入码是通过将所述用户码应用于显示在所述至少一个电子设备上的所述伪随机安全字串来确定的，所述用户交易输入码被发送到所述主机；其中：

iii）所述计算机主机证实所述用户输入码与所述一次性交易码的匹配。

用户通过将他或她的用户码应用于显示在电子设备上的伪随机安全字串来确定交易输入码。用户把交易输入码输入到显示出伪随机安全字串的电子设备中或是与计算机主机通信的设备中。所输入的用户交易码被发送到主机，以便用一次性交易码来验证。伪随机安全字串可被显示出来，并且用户输入的交易码可以被输入到具有包括以下设备在内的任何组合形式的设备中，这些设备包括销售点资金电子过户（EFT/POS）设备、与用户关联的无线设备、经由互联网与主机相连的计算机或是任何能够与计算机主机进行电子通信的设备。此外，计算机主机可以传送

一次性交易码，以便显示在电子设备上，通过与计算机主机以及用户计算机或设备相连的商家计算机或网站，系统可被用于完成与商家的交易。该系统可以用于向数据库或账户信息提供安全的或规定的访问。

根据本发明的第四个方面，它提供了一种用于验证身份以便实施安全交易的方法，该方法包括以下步骤：

i）存储涉及与计算机主机关联的用户 PIN 的信息；

ii）由所述计算机主机产生一个伪随机安全字串；

iii）通过将所述用户 PIN 应用于所述伪随机安全字串来确定一个交易码；

iv）将所述伪随机安全字串传送到至少一个电子设备；

v）在所述至少一个电子设备上显示所述伪随机安全字串，以便所述用户通过将所述用户码应用于所述伪随机安全字串来确定一个用户交易输入码；

vi）在所述至少一个电子设备上输入所述用户交易输入码；

vii）将所述用户交易输入码从所述至少一个电子设备发送到所述计算机主机；以及

viii）所述计算机主机确定所述交易码是否与所述用户交易输入码匹配。

电子设备显示出伪随机安全字串，从而使用户可以通过将其用户码应用于伪随机安全字串来确定一个用户交易输入码。该用户在一个与主机进行电子通信的相同或不同电子设备上输入交易输入码。用户输入的交易码被传送到计算机主机，以用于验证计算机主机确定的交易码与用户输入的交易输入码相互匹配。根据本发明这个方面所述的方法完善了这个交易，当主机确定的交易码与用户输入的交易输入码相匹配时，该方法允许对数据库或账户信息进行访问。

根据本发明的第五个方面，它提供了一种安全的用户码输入界面系统，该系统包括：

i）一个安全用户代码输入界面，用于在电子设备上输入用户码，其中所述电子设备具有一个显示器；其中所述安全用户代码输入界面包含至少一个发光显示，用于由所述用户输入所述用户代码中的至少一位数

字；其中所述发光显示照明或加亮所述发光显示中的至少一位显示数字，并且，当符合所述用户码中至少一位数字的所述至少一位显示数字在所述发光显示上被照明或加亮的时候，所述用户将在应答的时间上使用输入设备做出一个应答，以输入所述用户代码中至少一位数字；并且其中

ii）一个随机的连续时间被添加到所述应答时间中，用以延长所述至少一个发光显示。

所述用户码输入界面保存并运行于一个具有显示器的电子设备上。在该显示器上可以看到上述安全的用户码输入界面，其中包含至少一个发光显示，用以使用户在界面的每个循环中输入一位用户码。该界面的发光显示照明或加亮界面上的至少一个显示数字，当被照明或加亮的数字与用户代码中将被输入的那个数字相匹配时，用户点击辅助键盘或鼠标上的任意按键或是接触触摸显示屏上的任意区域。当用户敲击按键时，一个随机的连续时间将被添加，这样，发光显示将保持激活，由此与输入的数字相关的信息就无法被确定。该安全用户界面为用户代码中的每一个数字都包含一个循环。

根据本发明的第六个方面，它提供了一种身份验证安全交易系统，该系统包括：

i）一台计算机主机，用于保存一个与用户关联的用户代码；

ii）一个电子设备，它与所述计算机主机进行电子通信，其中所述电子设备具有一个显示器和一个用户输入设备；以及

iii）一个安全用户代码输入界面，它在所述至少一个电子设备的所述显示器上可视，用于输入所述用户代码，其中所述安全用户代码输入界面包含至少一个具有发光显示的循环，用于输入所述用户码；其中，当符合所述用户代码中的所述至少一个用户码数字的显示数字在所述发光显示中被照明或是被加亮的时候，所述用户在应答时间使用所述用户输入设备做出一个响应，以输入所述用户代码中的至少一个用户码数字；

iv)其中所述至少一位用户代码数字的所述各位数字是在所述至少一个循环的各个循环中被输入的，并且一个随机的连续时间被添加到所述应答时间，用以延长所述至少一个循环的各个循环；以及

v）其中，输入的所述用户代码被发送到所述计算机主机，以便利用

保存的所述用户代码进行验证。

所述计算机主机中保存有涉及用户的信息，其中包括账户和用户代码信息。所述至少一个电子设备与计算机主机进行电子通信，并且显示用于输入用户代码的安全用户输入界面。所述至少一个电子设备具有至少一个显示器和一个用户输入设备。安全用户代码输入界面包含至少一个循环以用于用户代码的各位数字，并且包含一个用于输入用户代码的发光显示。当符合用户代码中恰当数字的显示数字被在所述界面的发光显示中照明或是加亮的时候，用户在应答时间使用一个用户输入设备来做出一个应答，以输入用户代码中的各位数字。当每个数字记录在一个循环中被输入之后，一个随机的连续时间被添加到用户响应时间中，以便延长发光显示的各个循环，这样，任何人都无法通过查看用户界面来确定哪个数字被选。

在输入完全部用户代码之后，输入的用户代码被发送到计算机主机，以便用计算机主机保存的用户码来加以验证。用户可以通过敲击键盘或鼠标上的按键来输入应答，也可以通过接触触摸显示屏上任意区域来做出应答。

为了更好的理解本发明并显示本发明是如何实现的，现在将以举例的方式并参考附图对本发明进行说明，在以下的附图中：

图 1 是本发明一个优选实施例的示意图；

图 2 是双信道模式的一个优选实施例的示意图；

图 3 是当用户与本发明所述系统进行交互时将会采取的步骤的流程图；

图 4 是本发明所述单信道模式的一个优选实施例的示意图；

图 5 是本发明所述单信道模式的一个附加实施例的示意图；

图 6 是本发明所述单信道模式的一个附加实施例的示意图；

图 7 是本发明所述单信道模式的一个附加实施例的示意图；

图 8 是一个结合本发明各个方面和特征的附加实施例的示意图；

图 9 是一个本发明所述安全数据访问系统的示意图；

图 10 是一个用于检索银行账户信息的安全系统的示意图；

图 11 是一个伪随机字串的图示；

图 12 是用户临时性或交易性修改和集中处理的示意图；

图 13a 是本发明所述用户界面的一个图形表示；

图 13b 是本发明所述用户界面的一个图形表示；

图 13c 是本发明所述用户界面的一个图形表示；

图 13d 是本发明所述用户界面的一个图形表示；

图 13e 是本发明所述用户界面的一个图形表示；

图 13f 是本发明所述用户界面的一个图形表示；

图 13g 是本发明所述用户界面的一个图形表示；

图 13h 是本发明所述用户界面的一个图形表示；

图 14 是本发明所述 PIN 安全界面的启动屏幕的图形表示；

图 15a 是 PIN 安全用户界面的第一循环的图形表示；

图 15b 是 PIN 安全用户界面的第二循环的图形表示；

图 15c 是 PIN 安全用户界面的第三循环的图形表示；

图 15d 是 PIN 安全用户界面的第四循环的图形表示；

图 15e 是用符号或字符取代数字后的 PIN 安全用户界面的图形表示；

图 16 的示意图示出了应用于以互联网为媒介的数据库访问系统之中的本发明的特征；

图 17 的示意图包含有应用于以互联网为媒介的多数据库访问之中的本发明的特征；

图 18 是一个描述经由互联网通信的本发明的各种特征和组成的示意图；

图 19 是一个描述经由互联网通信的本发明的各种特征和组成的示意图；

图 20 是一个描述经由互联网通信的本发明的各种特征和组成的示意图；

图 21 是根据本发明一个附加实施例所述的访问和数据通道的示意图；

图 22 示出了一个结合有本发明各个方面的通用服务器网关模式的示意图；

图 23 示出了一个根据本发明所述的通用集成平台的示意图。

图 1 显示了一台由信用卡或借记卡的发卡方操作的主机 1，一个拥有移动电话 3 的用户 2，以及一个 EFTPOS 终端 4。用户 2 配备一张卡（未示出），其上印有一个唯一的 16 位账号，该账号被磁性编码在卡上。在主机 1 中，这个 16 位账号被与涉及该用户的账户资料、用户在信用卡/借记卡方初始登记时选择或被分配的一个 4 位掩码、以及移动电话 3 的一个唯一的电话号码相关联起来。选择 16 位账号是为了兼容现有的信用卡/借记卡协议，选择 4 位掩码是为了兼容现有的 PIN 协议。当用户 2 希望从操作 EFTPOS 终端 4 的零售商（未示出）处购买物品时，他或她会出示卡，然后该卡被 EFTPOS 终端 4 扫描。关于一次购买的资料也被零售商输入 EFTPOS 终端 4，这些信息与账号一起通过一个调制解调器链路 5 被发送到计算机主机 1。然后，计算机主机 1 将该账号与包含移动电话 3 的电话号码的用户 2 的资料相关联，并且产生一个 13 位的伪随机字串，该伪随机字串通过 SMS 或语音邮件协议 6 的方式被发送给移动电话 3。伪随机字串的前三位并不是随机的，它们被保留以便向用户指示：接收到的 SMS 消息来自计算机主机。例如，这前三位可以是“T1：”或“T2：”等等，用于表示计算机主机 1 希望用户 2 将第一或第二掩码应用于该伪随机字串。伪随机字串中接下来的 10 位为任意 4 位掩码提供了足够的冗余度，以便如上文所述方式对其产生作用。通过为伪随机字串选择一个 13 位的字串长度，就可以保证与现有移动电话显示和 EAN13（欧洲商品编号）条形码协议的兼容性。

当移动电话 3 接收到伪随机字串后，那么如上文所述，用户必须将掩码应用于该字串，以便产生一个易失性识别码，然后，该识别码被传递（8）到零售商那里，并且被输入 EFTPOS 终端 4，以便传送到计算机主机 1。另外，该易失性识别码也可以通过移动电话 3 的方式被用户 2 返回给计算机主机 1。

当计算机主机 1 接收到易失性识别码时，它把该识别码与计算机主机 1 中通过将掩码应用于伪随机字段而产生的易失性识别码相比较，如果发现这两个掩码相同，那么计算机主机 1 向 EFTPOS 终端 4 发出一个

信号以授权购买，并且还将必要的资金过户到零售商。作为可选项，在授权资金过户之前，计算机主机 1 还可以用 SMS 或语音邮件的格式 6 来向移动电话 3 发送一条消息，该消息中最好包含交易资料，并且计算机主机 1 要求用户 2 返回一个信号 7，以便最终确认交易。此举可以为数额非常大的交易提供内心的平静（peace-of-mind），并且可以在用户卡正被盗用的情况下向用户 2 发出警告。

本发明既能以双通道模式实施，也可能以单通道模式实施，这些模式将结合图 2－10 而得到公开和说明。

双通道协议适于所有拥有 G2 移动电话的用户。交易类型可以包括：（1）销售点资金电子过户（EFT/POS）以及（2）电话定购。EFT/POS 是这样一种交易，其中用户在商家那里以正常方式购买物品，当使用读卡器刷取信用卡/借记卡时，商家将被提示索取顾客的交易确认码（TAC）或掩码。用户回忆起他或她的四位 PIN 代码，该代码用于从销售点给出的伪随机字串中确定 TAC。如果用户想要在短时间或是在移动电话接收质量较差的地方进行多次购买，那么用户可以预先选择将同一 TAC 用于单独的一天。电话定购交易基本上采用与上文相同的方法，只不过商家在被提示索取 TAC 之前会以通常方式人工地输入卡片的资料。

双通道模式的其它特征在于：顾客能够选择其它的用户友好方法来从伪随机安全字串中识别出 TAC，例如谜语界面或语音识别系统。谜语界面在制造过程中只包含对电话或寻呼机中 SIM 卡的较少修改，但是它可使用户避免自己去计算 TAC。用户可以键入他们的 PIN 并点击他们选择的一个附加键，电话或寻呼机会自动算出作为结果的 TAC，而用户甚至不用看到安全字串。这种计算完全是在内部发生的，由此确保只有 TAC 被显示出来，而 PIN 不会保留在移动电话或寻呼机中。语音识别界面可以在由语音激活的电话中实施，并且基于来源于已核准语音的简单命令“TAC！”，该界面能够计算出合适的 TAC。

当顾客申请一张被允许使用的卡片时，他也可以选择下文中将要详细讨论的一个几何图形，安全字串始终在该几何图形中被传递。顾客只需要登记屏幕上显示的他或她选择的几何图形，然后直观选择他或她的 PIN 图形，就可以确定出相应的 TAC 结果。这个显示可以通过 WAP 移

动电话、G3移动电话、互联网站点的显示提示或是销售点上的辅助专用终端而被连接。

本发明的协议可以被"栓接"在一个现有数据库服务器上，并且至少可以在未经修改的EFT/POS硬件上运行，这些硬件如：（1）AMEX；（2）分离拨号的EPOS；以及（3）VESA SVS3。此外，双通道协议可用于提高Mondex系统的安全性(这些系统在POS端已经使用了4位PIN数字)。

双请求模式可以使用标准的G2移动电话、G3以及WAP设备来接收安全字串。如果这些设备包含一个经过修改的SIM卡界面以用于这个安全字串，那么该设备还可以包含一个GUI或是谜语界面，以便简化对TAC的推导过程。

图2示出了应用于销售点环境中的本发明的协议。图2显示了涉及这个交易的主要部件及步骤，并且显示了两个不同的选择。第一种选择是使用一个分离拨号的销售点资金电子过户机（EFT/POS），其中交易资料直接通过授权服务器207发送。第二种选择使用了商业受让方（acquirer）的网络。

在直接拨号的方案中，用户201从位于设备202的授权服务器207接收一个安全字串210。在用户准备购买物品之前，该安全字串210存在于诸如移动电话的设备202上。当用户201准备进行购买时，在步骤220，他或她会把自己持有的被允许使用的信用卡204交给商家205，以便进行销售点资金电子过户（EFT/POS）。卡204照例在商家205的EFT/POS终端被刷取。用户201检查驻留在设备202上的安全字串210，并确定出该次交易的TAC。四位数字的TAC 230被用户201提供给商家205。用户201可以口头告知TAC，也可将其输入POS终端，还可以在移动设备202上输入代码。信用卡204、TAC 230以及交易金额随后将通过直接拨号网络240被发送到授权服务器207。授权服务器207与发卡方209一起证实账户中具有足够资金，并且TAC与用户的PIN代码以及所给出的安全字串210相关联。如果账号、交易金额以及TAC都通过验证，那么授权服务器207将允许交易继续进行。

在称为商业受让方网络方案的第二种方案中，相同的初始步骤被应用。用户201接收一个安全字串210，这个安全字串驻留在例如移动电话

的设备 202 上，当用户 201 准备从商家 205 那里购买一件物品时，在步骤 220 中，他或她把已经登记的信用卡或借记卡 204 交给商家 205。卡 204 在 EFT/POS 终端被刷取，并且用户 201 再次通过移动电话或设备 202 上留有的安全字串 210 来确定他或她的四位 TAC 230。在这个方案中，包含卡 200 账号以及购买金额的交易信息经由路径 250 被发送到系统（scheme）252。标准的信用卡交易资料和预先授权的 PIN 则被发送到发卡方的计算机主机服务器 209。系统 252 将卡 204 的信息和预先授权的 PIN 经由通信路径 256 发送到发卡方的计算机主机 209 上。同时，系统 252 与授权服务器 207 通信并且验证预先授权的 PIN 与用户 PIN 相关。发卡方 209 继续对交易进行处理，一旦通过验证，则允许交易继续进行。

除了上述双通道方案之外，本发明还允许采用单通道模式，利用这种模式，用户能够将本发明用于这样的交易，例如，通过互联网网站进行在线购物。在安全字串被接收并且 TAC 在相同设备上被传送的情况下，单通道模式和协议经由计算机、WAP 设备、智能卡、专有系统或是 G3 移动电话而被执行。这个协议并不需要辅助通道来实施安全交易。

单通道协议借助用户下载到其计算机、WAP 设备或 G3 移动电话上的一个 applet （一种 java 程序）而得到实现。安全字串和 TAC 只能由一个许可的服务器接收，并且经由一条 SSL 链路传送。由于商家（无论是否具有资格）只拥有用户的“用户姓名和卡的 ID”而没有相关的 TAC，因此本发明能够抵抗在其中用户并不知道与自己做生意的站点是不具有资格的“幽灵（ghost）”网站。

单通道解决方案指示用户的 ISP（Web 浏览器）只把用户姓名发送到商家，而把相关 TAC 传送到许可的服务器/数据库，从而解决了在互联网上发送相关 TAC 和安全字串时所遇到的问题。

图 3 显示了在用户注册并使用单通道模式的处理中将会采取的各个步骤。该过程始于步骤 300，在步骤 310 中，用户通过一个单通道设备接通本发明的服务器主机，该单通道设备可以是个人计算机、连接到互联网络的手持设备、蜂窝电话或无线电话、或是任何可以经由单一通信通道支持网络浏览器的设备。一旦与本发明的服务器或计算机主机接通，那么包含界面 applet 的登录网页将被发送到用户设备。在步骤 320 中，

用户被要求通过适当的输入方法来输入其用户ID以及预先授权的信用卡或借记卡代码。该用户界面可以包括屏幕上的下拉菜单或是其他各种用户友好的应用程序，用以增强用户ID和信用卡或借记卡代码的输入处理。用户ID被发送到服务器进行验证。如果服务器核实用户身份，那么服务器将使用低处理开销协议（LPO协议）而把一个安全字串发送到客户网页，同时发送一个提示来启动Applet。该Applet根据LPO协议提取和重装TAC代码，并且启动PIN安全界面。

在步骤330中，能够使用户安全输入一个PIN或TAC的PIN安全界面被启动。LPO协议提取是使用一个自动系统识别数字（SID）和产生系统输出数字（SOD）来执行的。如在下文将要详细描述的那样，TAC代码被从安全字串中提取出并根据LPO协议重装，然后该TAC代码被发送到服务器主机进行验证。在步骤340中，Applet被终止并被破坏，所有数值都被清零，并且驻留在设备上的安全字串被清除。用户会看到一个对设备正在等待一个服务器响应进行识别的界面。在步骤350中，根据用户ID和TAC码的响应，登录到服务器受到确认或拒绝。如果通过验证，那么一个其后跟随着被请求的服务访问或交易的确认信息将被发送到客户浏览器。在步骤360中，会话或交易完成，这使得用户能够关闭会话或进程，或者，也可以使用一定长度的空闲时间来触发会话自动关闭。在步骤370中，采用单通道模式的用户信息被终止。

图4示出了本发明所述单通道模式的一个优选实施例的主要组件。用户401访问本发明的服务器407，该服务器407提供下载到用户设备403上的applet 470。用户401经由路径421下载470，该程序被保存在设备403上以作为用户applet 422。网络商家405将通过路径450访问授权服务器407，并经由路径451下载applet 470，该程序470被保存在商家站点405上以作为商家的applet 452。使用设备403的用户401经由路径430访问商家网站405，并且选择他或她希望购买的物品，这种选择是通过将物品放入购物篮406并选取适合的信用卡或借记卡407来实现的。商家站点405然后对购物篮406中的物品和涉及卡407的信息加以累计，并且使用商家的applet 452而把该信息沿路径431发送到授权服务器407。

授权服务器407启动验证处理，并且使用通信路径432通过商家applet

452将适当的信息回送给驻留于用户设备403中的用户applet 422。用户401被要求输入TAC。一旦用户输入了TAC，那么TAC将沿着路径433经由商家被送回授权服务器407以使响应生效。此外，在步骤434中，授权服务器407确认账户中具有足够资金，并且在步骤435中，授权服务器407确定出与卡407、TAC以及账户资金可用性有关的信息通过验证。授权服务器407沿路径436把一个“接受”通知发送到商家网站405，后者则将该通知通过路径437转发到用户设备403。

图5－7还涉及使用不同方面和安全协议的单通道模式。在图5中，用户501访问一个商家互联网站点505并且选择所要购买的各种物品。在结账的时候，商家网站505经由路径510向用户501要求付费。个人计算机或设备503包含一个与网站505通信的applet 522，并且还包含恰当的软件或applet 522，以便沿路径520将需要进行一次授权交易的信息告知授权服务器507。商家域名、交易金额、用户ID以及交易验证码（TAC）从用户设备503沿路径530被传送到授权服务器507。个人计算机或用户设备503上已经有用于使用户确定其TAC码的安全字串。

授权服务器507经由路径540而与商家互联网站点505进行通信，用以对卡和交易金额的信息加以确认。授权服务器507还将交易ID经由路径541并通过用户个人计算机503转发给用户501。交易ID从用户个人计算机503沿路径542转发到商家的互联网站点。授权服务器507验证出购买金额、卡片信息以及TAC是合适的，并且将卡和金额的资料沿着路径550发送到商家的互联网站点505。交易资料从商家互联网站点505通过路径560发送到发卡方509，最终发卡方509把支付费经由路径570发送到商家的互联网站点505。

图6显示的单通道模式与图5显示的单通道模式相似，只不过图6中包含了一个无线设备604，它用于从用户个人计算机603中消除安全字串。在图 6 显示的模式中，安全字串被省略，只有用于交易的四位TAC 620被从授权服务器607传送到用户的无线设备604。

图 7 是一个与图5、图6所示的单通道模式相类似的单通道模式，但其不同之处在于：一个十三位的安全字串被发送到无线设备704，而不是在上文中结合图6所描述的那样，将四位TAC从授权服务器707发送到无

线设备704。在图7所公开的模式中，当用户701从商家的互联网站点705选定将要购买的物品时，付费请求沿路径710并经由用户个人计算机703发送给用户。然后，applet 722提示用户输入TAC码，该TAC码是由用户通过从授权服务器发送到无线设备704的安全字串而确定的。applet 722沿着路径730把商家域名、交易金额、用户ID以及TAC转发给授权服务器707。授权服务器707沿着路径740证实交易，并将用户账号和金额沿着路径750转发给商家的互联网站点705。交易资料从商家的互联网站点705沿着路径760发送到发卡方709，然后，支付费从发卡方709沿着路径770转发给商家的互联网站点705。

如图2－7所示，在各种使用单通道或双通道模式的在线商务方案中，可能会存在因商家库存中没有某件物品而不能立即完成整个交易的情况。在这些情况下，商家通常在发货之后才会结束交易。然而，用户可能已经输入了他或她的TAC，并且系统想要向用户发送一个新的伪随机安全字串。

本发明通过让服务器接收付费请求和有效的TAC来克服这个障碍。商家服务器通常会在额定的一分钟时限之内将定购请求发送到授权服务器。然而，如果商家已经接收了一个涉及无现货商品的购货单，那么这个定购请求将被延迟。直到接收到商品并且商品即将发送给顾客的时候，延迟的定购请求才被发送到授权服务器。一旦接收到用户TAC和交易资料并且在一分钟期限内没有收到此次定购的商家传输，那么授权服务器将默认执行一个延期支付程序。

该延期支付程序在授权服务器保留有效TAC，并且作为一个说明用户已经定购商品的证据。然后，一个新的安全字串将被发给用户，以便在下次交易中使用。授权服务器程序将立即向用户发送一个电子邮件，用以说明他或她从商家那里所要求的商品的资料。每个星期或是在某个其他预定的时间间隔内，授权服务器将向用户提醒其定购请求。用户由此得知任何未决交易，这些交易最终将通过其账户而被清除。

当商品抵达商家仓库并且即将发货的时候，商家资料被发送到授权服务器，并且交易完成。如果这个时候用户资金不足以支付交易金额，那么交易将被拒绝，这与标准的信用卡交易一样。

图 8 描述了使用本发明特征的一个附加模式，其中用户具有一个预先授权的或是借记的账户804。用户看到一个真实的设备805，例如一个自动售货机，并且通过路径810选择物品，由此触发真实的设备805以要求支付费用。该付费请求将通过预先授权的流动账户804而被发送，这个处理是在步骤840中使用一个刷卡设备806刷取预先授权的账户804（例如信用卡或借记卡）来完成的。此外，小额付费请求还把将要请求一个TAC的消息通知给刷卡设备806。用户可以具有诸如无线电话这样的个人设备803，该设备包含一个TAC或是安全字串，由此用户可以确定TAC并将TAC 830输入刷卡设备806。用户还可以将TAC 830输入无线设备803，后者会将TAC 830无线发送到刷卡设备806或授权服务器807。交易资料从刷卡设备806沿着路径850发送到授权服务器807。授权服务器807包含涉及流动账户的信息，并且，如果通过验证，那么它将会沿着路径860通知小额付费计算机主机808以授权支付费用。然后，小额付费主机808沿着路径870把支付数额过户到上述真实的设备805。

图9描绘了一种数据控制模式，利用这个模式，本发明的部件可用于将一个安全层和预先授权添加到数据库中，以便对访问数据库加以控制。在图9中，用户901通过他或她的计算机或笔记本计算机903来访问数据库909。该访问是从授权服务器907沿着路径910请求的。一个安全字串经由路径920被从授权服务器907发送到计算机903，由此使用户确定出他或她的TAC。用户输入TAC，该TAC沿着路径930传送到授权服务器907。如果用户提供的TAC与已被用户901验证的适当PIN向匹配，则授权服务器907将允许沿着路径940来访问数据库909。

另外，该系统可以只简单地发送TAC，而不发送安全字串。然后，访问数据通过授权服务器907并经由路径950被传送到用户计算机903。此外，安全字串可以通过另外一条路径921（例如通过使用一个无线设备904）而被发送到用户901。

图10描述了一种远程银行存款余额查询模式，通过这种模式，用户可以检查账户的余额。在图10所给出的模式中，通过使用蜂窝电话、寻呼机或无线设备1004，用户1001可以要求查询银行1008中的账户余额。该用户通过路径1010被提供一个安全字串或TAC，该安全字串或TAC驻

留在无线设备1004中。用户确定他或她的TAC代码，并且向银行出纳员提交其TAC代码，或是将其输入至无线设备1004。TAC代码被发送到授权服务器1007，并由该服务器验证出TAC代码适于安全字串并且对应于用户PIN。然后，授权服务器1007沿着路径1020与银行1008通信以检索账户信息，由此为用户提供被请求的信息。

本发明的两个重要方面（即低处理开销协议和安全字串操作）在结合图2－10所描述的双通道和单通道模式中得到了应用。某些无线设备，例如web设备，它们由于自身的低处理开销，因而无法运行高级别的加密程序。本发明引入了一种低处理开销协议，该协议能使这类设备运行高度安全的交易，也可以在不使用大容量存储内核（footprint）的情况下进行下载。低处理开销协议的一个额外好处在于：在处理信息时，现有的交易数据提供服务器要快于传统的加密系统。通过同时使用多个安全字串,低处理开销协议避开了TAC与安全字串之间相互关联的可能性。在多个安全字串中，实际上只有一个字串是相关的，剩余字串只是用于隐藏该相关字串。安全字串包含相同的数字，但是它们以不同的随机顺序排列。用户applet接收多个安全字串，并且利用一个系统识别数字（SID）来识别哪一个字串相关。识别数字的系统知道哪一个安全字串是真实的并且立即清除不相关的字串，而只对正确和相关的字串加以处理。举例来说，如果识别数字的值为4，那么本发明将把第四个安全字串识别为相关的安全字串。

在交易过程中，如结合图11和12将要描述的那样，用户输入他或她的PIN，并且TAC是在无线设备、个人计算机以及EFT/POS的applet中内部算出的，或者如图11所示，一个十三位的安全字串1100被从授权服务器发送到用于识别一个行随机数字的用户设备，在这个实例中为十三（13）。安全字串1100可以始于两个字母识别前缀1101，该前缀标识出是哪一个服务器发出了安全字串1100。举例来说，在图11中，如果用户的PIN是2468并且用户将PIN代码应用于安全字串1100中的数字位置。那么用户将查看第二点、第四点、第六点和第八点上的数字，以便为该次交易确定其交易验证码或TAC。在这个例子中，数值为2468的用户PIN将产生一个数值为7693的TAC。因此，用户将会输入7693作为TAC，用以

通知授权服务器继续验证处理。

关于在被传送的保密安全字串中使TAC受到保护的方式的进一步描述将结合图12加以说明。如图12所示，用户或顾客1201具有一个已知的PIN 1202（即1234）。保存在用户设备上并从服务器1207下载的信息是十三位伪随机字串1203。在个例子中，数值为“1234”的顾客PIN在与伪字串1203相关联的时候将会指示一个数值为“6891”的TAC代码1204。当用户被要求验证TAC 1204或是将其输入以授权服务器1207证实顾客1201实际上是已被授权和注册的用户时，TAC1204可被操作并以无数种方式反转，以便在沿着通信路径到达服务器1207的传送过程中保护该代码。一种用于为顾客PIN 1202和TAC代码1204提供安全层的方法是：将TAC代码合并入多个字串中的一个十三位字串，就像先前所述的那样。

为了识别适当的字串，运行在顾客设备上的applet将通过一个系统识别数字1205来识别相关的字串。SID 1205被用于识别哪一个安全字串是相关的。该SID 1205可以用无数种方式确定，其中包括：使用用户PIN1202的某些数字或数字组合、由用户设定SID 1205以及由系统服务器设定SID 1205。在图12所示实例中，系统将SID的值设定为3。因此，九个字串中的第三个字串就是相关字串。十三（13）个数字中的九个（9）字串经由一个数据连接（例如数据流1230）被发送到用户或顾客1201的设备。该设备上的applet知道SID 1205的值并且提取出相关的字串1203。

顾客检查驻留在其设备上的相关字串1203，并且确定他或她的TAC 1204。然后，TAC 1204被编结到一个输出的相关字串中，该字串被分成八（8）个非相关字串组。输出数据流1240包含九个十三位数字的输出字串。相关输出字串的位置通过一个系统输出数字（SOD）1209而被识别，它也可以用无数种方式来确定，例如，使用或添加一定数量的用户PIN 1202或是由用户或系统服务器来选择SOD 1209。

在这个例子中，系统将系统输出数字（SOD）1209的值设置在2上。因此，TAC 1204将被合并入字串1240的数据流内九个字串中的第二个字串。TAC代码1204也可以被倒置和操作、被增加一个自动数字（即每个数字都增加1），或是采用其中PIN代码可以在传送之前得到修改的其他任何方式。在图12所示的例子中，TAC代码1204被翻转，以用于确定相

关输出字串中TAC数字的位置。例如，由于在这个实例中，TAC 1204的值为“6891”，其翻转值“1986”将规定位于第一点的是TAC码的第一位数字，位于第九点的是TAC的第二位数字，依此类推，直到TAC被并入相关的安全字串为止。

含有九个十三位字串的输出安全字串的数据流1240被发送到服务器1207，该服务器具有一个执行验证的applet。服务器1207还具有一个applet，该程序知道SOD 1209的值，并且可以识别出用于对用户PIN进行验证的相关的输出安全字串。因此，服务器1207上的applet知道用户的PIN 1202为“1234”，并且可以基于所建立的协议确定出SOD 1209的值为2，进而确定出相关字串为第二个字串。服务器1207根据用户保存的PIN来分析第二个字串，并且等待响应，以便验证该响应与来自初始字串1230的TAC 1204代码相匹配。

当接收到九个载体字串后，服务器1207知道相关的TAC载体字串的输出数字位置，并且立即清除不相关的字串，同时对正确选出的TAC载体字串进行处理。然后，服务器1207上的验证过程对正确的TAC与所给出的安全字串和用户PIN号进行比较。如果所有三个都相关，则完成授权，并且一个新的安全字串被发送到用户的applet。

尽管在这个例子中，所述数字被限制为九行十三个数字加上每行三个（3）系统数字（总计144个数字）。但是它并不意味着是对可被使用的行或数字的限制。对许多160个字符的设备来说，九行十三个数字总计144个数字是有意低于总的全球分组标准。因此，将数字长度保持在160以下将会使处理开销最小，以便顾及WAP应用和无线设备的低处理能力。此外，这个低处理开销将产生非常快的验证时间。验证过程还采用了一个过滤步骤，其后跟随的是一个单维阵列处理过程，而该过程并不是一个需要更多处理时间的密集型算术计算体系。

除了各种单和双通道模式、低处理开销协议以及使用多个安全字串的安全层以外，本发明还可以在用户界面内部提供一个安全层。图13a－13h示出了各种用户界面的例子，这些界面都可以提供给用户以用于输入用户TAC。在图13a－13h所提供的例子中，用户把他或她的个人PIN记忆成一个图案，而不是一个数字序列。举例来说，如果用户选择使用形状

1301并且出示图13e中的显示，那么他们只须记住他们创建了一个PIN，该PIN在图13c公开的形状1301的内部创建了一个小方块1303。当该显示被随机数填充时，则用户可以应用他或她所选择的设计（也就是小方块1303）。在这个实例中，来自方块1303的用户PIN将是“2389”。因此，知道PIN为“2389”并且察看了随机显示1302内部随机产生的数字，用户将会了解，数字“7538”对应于他或她的PIN数字位置。因此，用于完成交易或是输入数据库的用户TAC将是“7538”。图13a-h中所公开的用户界面仅仅是示范性的，各种显示、以及颜色和图形符号也可以被合并到用户界面中。因此，用户能够创建他或她的PIN的图形表示，而不需要记住四位PIN数字。

本发明另一个用于处理系统的用户界面的特征涉及到一个PIN安全阻碍界面的使用。任何带有键盘或是触摸界面（它可被连接到一个网络上或是能够下载数据或机器码）的设备都会需要含有一个口令或按键输入安全系统以实现完整性。一种构成该系统的方法是使用一个特洛伊木马（Trojan）程序。该程序是一个小程序，它收集键盘信息以便以后使用。还有其它程序也可以收集口令或键输入信息，然而在登录输入最后一位数字的时候，该程序会伪造一个登录失败的提示，并且在不为实际用户知晓的情况下，该程序将通过猜测最后一位数字（称为一个“嗅觉”程序）来尝试继续登录。这些技术都需要来自设备键盘或辅助键盘以及其他输入设备的实际数据。尽管数据可以通过加密或其他方式递送，并被安全的重传到设备处理单元进行的实际处理中，也可以从该处理中被重新发送，但是，如果安全系统需要输入有意义的用户数据以访问和操作安全系统，那么该数据可能被截取和转运，从而极大地降低了系统安全性。

虽然键盘或少量其他输入数据可以被重定向，或是在很少或没有用户指示或者系统性能影响的情况下被保存，但是对于具有高吞吐量输出和特定于设备的输出的图形显示来说，这种情况则不再适用。虽然有可能进行屏幕抓取或屏幕捕捉，但是由于系统资源集中，因此这很有可能会被用户发现，尤其是在处理能力相对较低的设备上。由此可以通过一个界面来提供良好的对抗性，该界面把信息提供给一个安全系统，这些信息只对那些在处在自身时间界面参数范围内的系统有意义，并且在那

些系统中，所获取的任何键盘信息都不具有外部意义。与之相似，任何可能的屏幕抓取或屏幕捕捉信息都不会危及系统的登录安全性。

当前，在计算机、PDA、2.5G或3G移动设备上输入用户名、口令或PIN代码是存在缺陷的，这是因为：（1）旁观者可能看到用户将他或她的PIN代码输入设备（称作“肩窥”）；（2）键盘有可能包含一个特洛伊木马程序，该程序记录输入的用户名、口令或PIN代码（特洛伊木马程序在未曾告知用户的情况下被下载到计算机，并且该程序可以无限期的驻留在那里）；（3）PKI验证可以证实该交易是在一台经过验证的计算机上实施的，但是它们不能有效验证计算机背后的用户；以及（4）运行微软视窗系统的计算机存在一个问题，因为视窗系统会记忆用户名、口令或者PIN代码，这将会产生一种情况，即，设备将用户的I/D保存在计算机内部。

“雷达”阻碍或本发明的PIN安全用户界面实现了一种良好的用户I/D，因为在每次交易过程中，用户都必须在场。PIN安全用户界面可以防止特洛伊木马程序，因为任何按键都可被用于输入PIN或TAC，而所述PIN或TAC则可使任何被特洛伊截获的按键信息都没有用处，就像屏幕上显示的信息一样。

此外，该用户界面是防肩窥的，因为观察屏幕或是观察按键输入并不能收集到什么信息，这使得肩窥成了一种毫无意义的行为。另外，当系统使用双通道和单通道（applet）协议时，它能够防止PIN被截取。本发明所述的协议是唯一的，因为它在每次交易时都会发送一个易失性TAC。即使截取/解密这个信息的尝试获得成功，也不会导致用户的真实PIN受到危及。

本发明的另一个特征在于，它是一个多平台系统。由于PIN安全用户界面具有低存储内核以及简单的通用用户界面，因此它可以工作在多种计算机和应用上。作为一个整体，协议和系统并不特定于某种设备，而是可以运行在诸如公用计算机的任何设备上。系统并不需要运行在一个程序历史纪录已知的可信计算机系统上。在不需要为计算机进行数字认证的情况下，用户可以在全世界任何一台计算机上进行交易。

另外，该用户界面很容易使用，因为用户无须了解协议、TAC以及

安全字串。PIN安全用户仅需将他或她的不变PIN经由PIN安全用户界面输入即可。另外，PIN安全用户界面是“搅乱”的证据，因为该界面并不将用户PIN或TAC（伪PIN）显示在屏幕上，因此也就不会受到来源于VDU的电磁辐射的影响，而这方面的内容是经由搅乱技术进行监测的一个主题。通过使用本发明的PIN安全用户界面所得到的强有力的保护允许将安全的单个PIN应用在多种具有不同安全体系的账户上，这可以通过使用一个中心PIN授权服务器来实现。即使安全字串存在于设备上也不会产生问题，因为本发明并不需要数字认证，因此，如果计算机落入不合适的人的手中，计算机存储器中也不会存在可能危及用户I/D的信息。

PIN安全用户界面包含一种将PIN代码输入计算机、ATM、PDA、2.5G或3G移动设备的独特方法。图14和15a－15e是这种PIN安全用户界面屏幕的典型实例。当用户希望进行在线交易时，PIN安全applet将激活，该程序提供如图14所示的“开始”用户界面。点击用户计算机屏幕上的任意按键，激活TAC或PIN的输入界面屏幕。该界面可以使用键盘、鼠标或触摸显示屏来激活。

如图15a－15e所示，PIN安全界面现在将开始依次显示（本实例中采用顺时针方向的方式）12个数字（从1开始，结束于12）。在这个显示循环中，当用户希望登记的数字被照亮时，用户只要按下其键盘、鼠标上的任意按键或是点击触摸显示屏上任意一点，就可以登记他或她的PIN或TAC。该PIN安全显示将会循环4次，每次用于4个PIN代码中的一位数字。

在第十二个位置上存在一个停留时间，以使用户准确地响应下一个循环的启动。当用于第一个PIN代码的第一个循环结束时，该显示将重新开始另一个循环。该循环也可通过改变照明颜色而被识别。这个处理过程被重复4次，直到所有4个数字都被输入，以便组成用户的4位PIN。

举例来说，如图15a－15d所示，如果用户的PIN是“2468”，那么在第一个循环，参见图15a，当第二个数字被照亮时，键盘应被按下。在第二个循环，当第四个数字被照亮（参见图15b）时，键盘应被按下，在第三个循环，当第六个数字被照亮时（参见图15c），键盘应被按下，在第四个循环，当第八个数字被照亮（参见图15d）时，键盘应被按下。在任一时刻，屏幕上只能看到一个显示，由此防止旁观者判定哪一个PIN正被输

入。另外，背景颜色以及所显示数字的变化可以是伪随机的。

当用户点击键盘以注册其第一位PIN TAC数字之后，一个随机的连续周期（run on period）时间将被激活。该连续处理能够防止旁观者对被注册的数字进行仔细查看。举例来说，如结合图15a所示的那样，当用户想要注册第一个数字（例如数字2）时，在数字2或第二个数字被照亮时，他们将会按下键盘上的任意按键，然而，该显示将继续照亮循环中2以后的代码或数字。在加速照亮所有数字直到结束循环之前，系统也可以只照亮被选数字之后的一部分数字，例如被选代码之后的0到4位数字。旁观者只能看到该循环在数字2、3、4、5或6被照亮之后加速，但是无法判定已经注册的是哪一个数字。在这个连续周期之后，系统可以提高循环速度以便结束循环，这样用户无须捱到整个循环时间结束，这有助于快速输入PIN。所述连续周期通常要短于从点击按键到用户开始怀疑是否已经给出一个明确选择所经过的时间。对人类的短期视觉记忆来说，这个时间最多是三秒钟。

连续周期和提高的循环速度可应用于所有4个周期和显示。处于数字照亮与循环中的变化之间的停顿时间是伪随机的，由此可以防止特洛伊木马程序通过将显示与键盘和用户计算机的时钟速度相关联来确定正被输入的数字。

如图15e所示，PIN安全用户界面还可以使用字符、字母或符号来代替显示器上的数字，这使得用户代码或PIN可以是符号或构成单词的字母的任意组合。此外，如上所述并且结合图9，本发明可被应用于利用双通道或单通道模式或协议以及PIN安全界面来实现的数据的远程访问。

通过配备一台授权服务器计算机，就可以使现有的数据库具有根据本发明所述的PIN安全界面，该计算机能够记录用户的PIN代码，提供并保存安全字串，并且能还对接收到的TAC进行关联，从而对用户的身份加以验证。

此外，PIN安全或雷达（Radar）界面可以在计算机自身处理器的内部、局域网结构的内部以及互联网上工作。在计算机自身处理器内部操作的PIN安全界面可以作为一个防黑客的屏幕保护程序，这意味着当用户首次启动他或她的计算机时，他或她将被给出这个界面。因此用户必须

输入PIN，如果用户决定短时间离开计算机，对罪犯来说，这时有机会使用他或她的计算机，那么用户可以按下一个功能键，该功能键将会激活PIN安全界面。当用户返回到他或她的计算机时，他或她只要点击鼠标或是任意按键并且通过该PIN安全界面输入PIN即可。

此外，如果一个用户未能在4个扫描循环中的任何一个循环内输入其PIN数字，那么本发明将允许在任意扫描中输入PIN数字（假如它们处于正确的顺序）。这意味着不需要按下“复位”按键，除非用户有意犯错误。

使用本发明所述安全特性、措施、协议、界面以及外层的其它模式将结合图16-23而得到讨论。

如图16所示，授权服务器1607直接连接到一个客户的主机网关服务器1609。该主机网关服务器1609是数据库1611与互联网1613之间的连接装置，它被放置于围绕在主机数据库1611四周的防火墙1615的外部（这样可以确保任何黑客活动都无法在数据库1611内部发生）。远程数据访问结构也可以连同用户1601和用户设备1604一起来使用PIN安全界面1623。系统还可以使用一个备份服务器或数据库1630。

授权服务器1607可以被配置成充当双通道或单通道系统。其结构使得主机网关服务器1609能够经由本发明或是现有访问程序来访问数据库1611。这意味着在安装完成之后，可以在不影响原始配置的情况下进行允许访问测试。

图17显示了如何利用一个PIN代码从一个用户1701访问多个客户机1740、1750。此举是通过安装一个中心PIN授权服务器1707来实现的，该服务器把接收到的TAC与从任意被激活的客户机1740、1750给出的安全字串结合在一起。

PIN安全界面可以通过各种方式得到应用，包括双通道和单通道：瘦（thin）客户机和多个单通道Applet实施例。在图18所示的双通道应用中，用户的TAC通过PIN安全界面1823而被输入，并且通过互联网1813被直接发送给授权服务器1807。在双通道应用中，没有安全字串被发送给用户计算机1822，取而代之的是，安全字串经由SMS被发送到移动设备1804。

如图18所示，安全字串被从授权计算机1807发送到用户移动设备1804。用户通过PIN安全界面1823输入TAC，授权服务器1807通过互联网

1813接收TAC。

在单通道瘦客户机的应用中，如图19所示，PIN安全界面的applet 1923驻留在授权服务器1907上。用户1901从任意计算机1922远程访问这个applet 1923，并且不需要通过预先下载的任何程序形成而对计算机1922进行“设置”。如图19所示，用户经由互联网1913访问授权服务器1907和applet 1923。用户1901输入他或她的PIN，该PIN在源头或授权服务器1907处被相关。

在单通道Applet应用中，如图20所示，PIN安全界面的applet 2023驻留在用户计算机2022上。该applet 2023只需下载一次，并且会在注册过程中被自动发送到用户计算机2022。PIN安全界面被特别设计成具有极小的存储器内核，此举使下载和使用过程都很快。

如图20所示，用户经由互联网2013访问授权服务器2007。用户2001输入他或她的PIN，applet 2023将该PIN转换成一个TAC（该转换通过利用驻留于applet 2023中的易失性安全字串而被自动完成），然后，该TAC经由互联网2013被发出，以便在授权服务器2007那里进行关联。

图21显示了一个典型的数据访问应用，其中授权服务器2107已被安装在一个访问数据库2111的网关服务器2109上。图21假设用户2101已经在系统中进行了注册，并且其计算机上装有PIN安全界面的applet 2123。要从数据库2111中访问信息，授权服务器2107将一个新的安全字串经由互联网2113或无线链路2151发送到用户计算机或G2移动电话。该安全字串2151驻留在设备2104上，直到用户2101希望访问数据库2111为止。

用户2101将他或她的易失性TAC发送至授权服务器2107用以确认他/她的身份。在双通道方案中，用户从G2移动设备2104获取他或她的TAC，这个获取可以经由可视提取（将其PIN用作一个序列发生器）、智能PIN或是SIMM来完成，其中用户2101将他或她的PIN输入设备2104，并且相关的TAC数字被显示在设备2104的屏幕上。然后，TAC被输入用户计算机（未示出）。在单通道方案中，用户只将他或她的PIN输入PIN安全界面2123。之后，该PIN在applet 2123内部被转换成一个TAC，并且经由路径2120被发送给授权服务器2107。

只有当用户的身份通过将接收到的TAC与用户PIN相关联而被肯定

地证实并且先前发出的安全字串是通过网关服务器2109并经由路径2130初始化的数据请求2130时，被请求的数据才可以经由路径2140被传递到用户计算机。

如果安全字串的递送和TAC的提取是在一个第二设备（例如通过双通道协议）上实施的，则不需要PIN安全界面。用户可以使用G2移动电话来接收一个安全字串，并且提取独立于数据存取计算机的TAC。这意味着TAC可以被输入数据存取计算机，而不需要经过PIN安全界面，因为对于肩窥、特洛伊木马程序、搅乱技术以及在线用户身份窃取来说，TAC是具有内在安全性的。

图22显示了一个结合本发明所述各个方面的通用服务器/网关模式。该通用安全服务器模式还可以引入UPS（不间断电源）、二重冗余、磁盘镜像、Linux的WEB服务器2245以及内部防火墙2215、PIN安全applet 2223、用户数据库2207以及一个内部维护的任何报告功能2211。

图23示出了通用集成平台，其中显示了防火墙2315内部的授权服务器2307。该授权服务器2307被连接到一个网络服务器2317和一个主机数据库2311。主机数据库2311也可以位于自身防火墙2316的内部。

另外，授权过程通过一个响应而不是一个识别账户及其参数来对用户加以识别，其中该参数能够防止由在线欺诈性保证的滥用所产生的所谓的“友好欺诈”（Friendly Fraud）。一个附加的好处在于，对于数据库文件存取来说，还存在着一个审计追踪过程。

本文中所述的计算机指得是任意的个人计算机、ATM、PDA、G2.5移动设备、G3移动设备，或是任何具有CPU的设备。本文中所述的交易指得是任何财务交易、远程数据存取程序，或是任何用户与系统之间的接口交易。各种用户界面和显示上的数字只是示范性的，并且字符、字母、颜色等可以被独立使用，也可以被结合在一起使用，但它们仍然包含在本发明的意图范围内。

虽然在这里已经通过实例而对本发明的优选实施例和各种备选实施例进行了详细描述和公开，但是对本领域技术人员来说，很明显，在不脱离本发明范围的情况下，可以对本发明进行各种形式和细节上的改动。本发明的范围仅由以下权利要求限定。

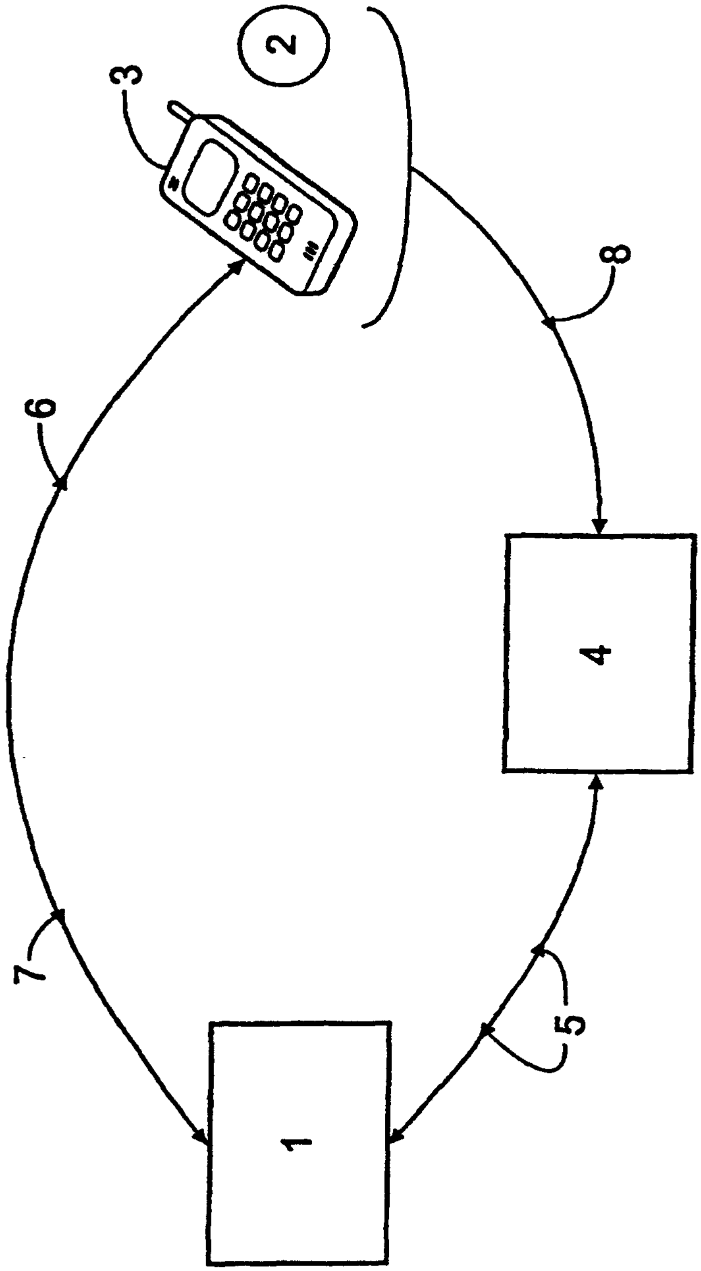


图1

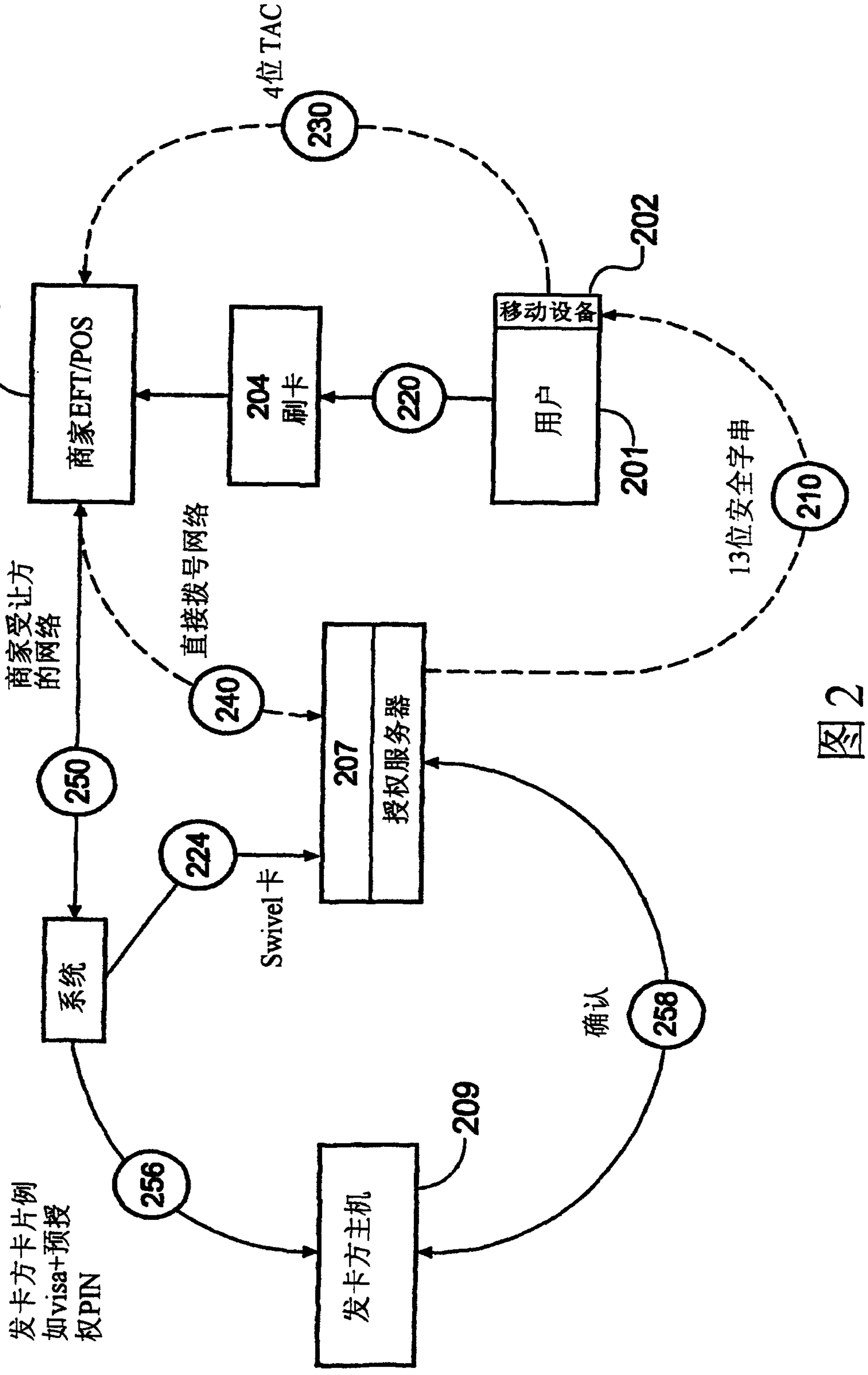

4位 TAC
230
202
移动设备
用户
201
205
商家EFT/POS
204
刷卡
220
13位安全字串
210
直接拨号网络
240
207
授权服务器
商家受让方的网络
250
224
Swivel卡
系统
确认
258
209
发卡方主机
256
发卡方卡片例如visa+预授权PIN

图2

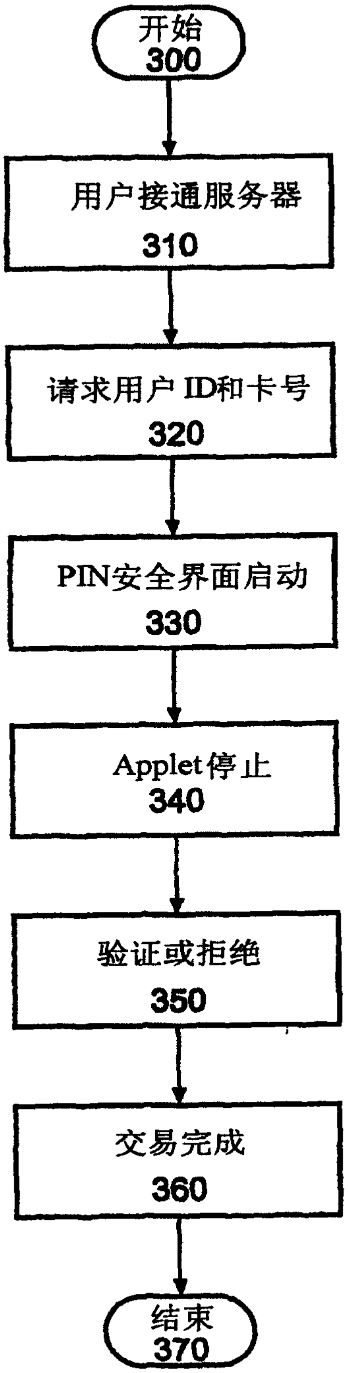

开始
300
用户接通服务器
310
请求用户ID和卡号
320
PIN安全界面启动
330
Applet停止
340
验证或拒绝
350
交易完成
360
结束
370

图3

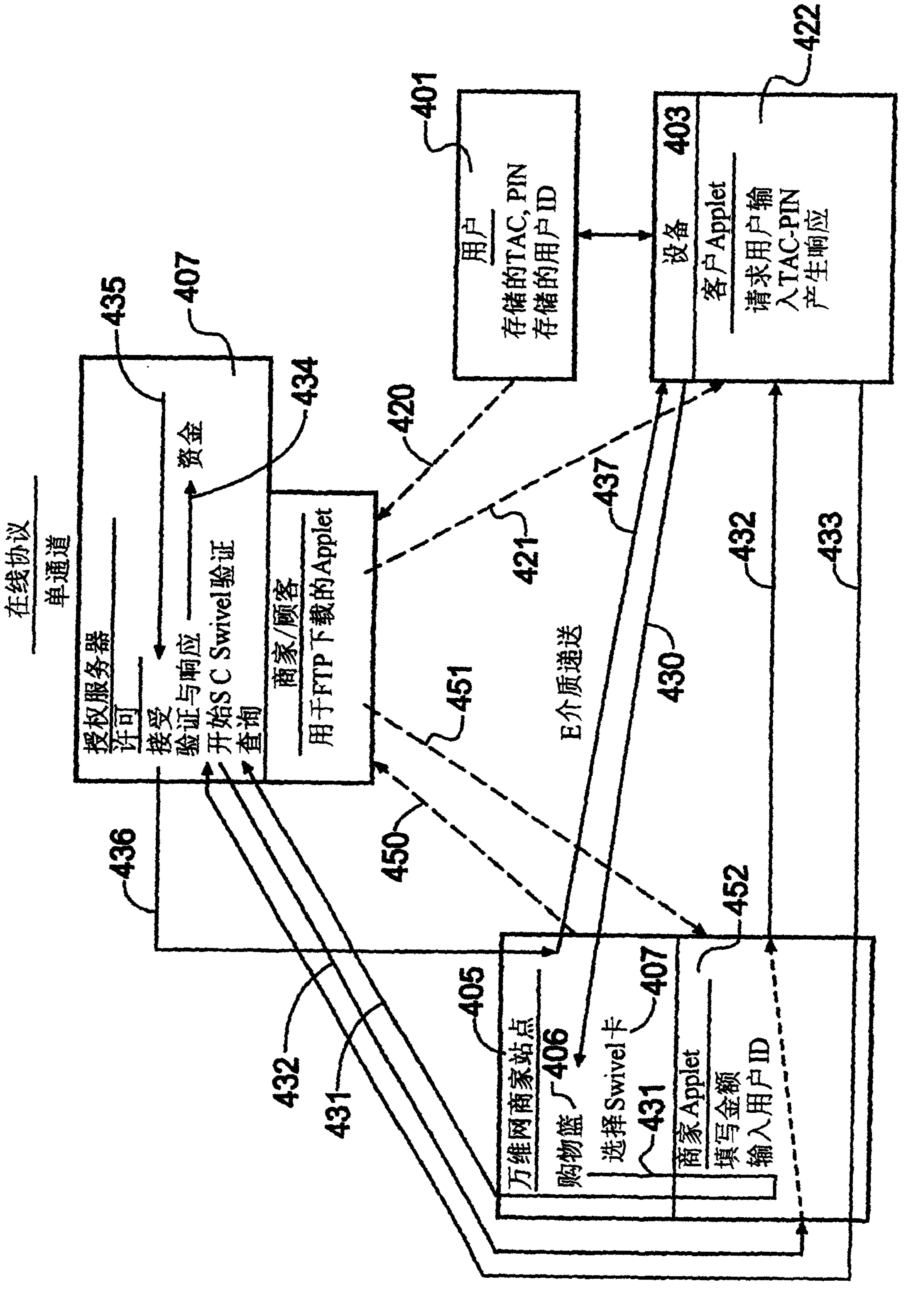

在线协议
单通道
授权服务器
许可
接受
验证与响应
开始S C Swivel验证
查询
资金
435
407
434
商家/顾客
用于FTP下载的Applet
420
401
用户
存储的TAC, PIN
存储的用户ID
403
设备
客户Applet
请求用户输入TAC-PIN
产生响应
422
421
437
432
433
451
E介质递送
430
436
450
452
405
万维网商家站点
406
购物篮
选择Swivel卡
407
431
商家Applet
填写金额
输入用户ID
432
431

图4

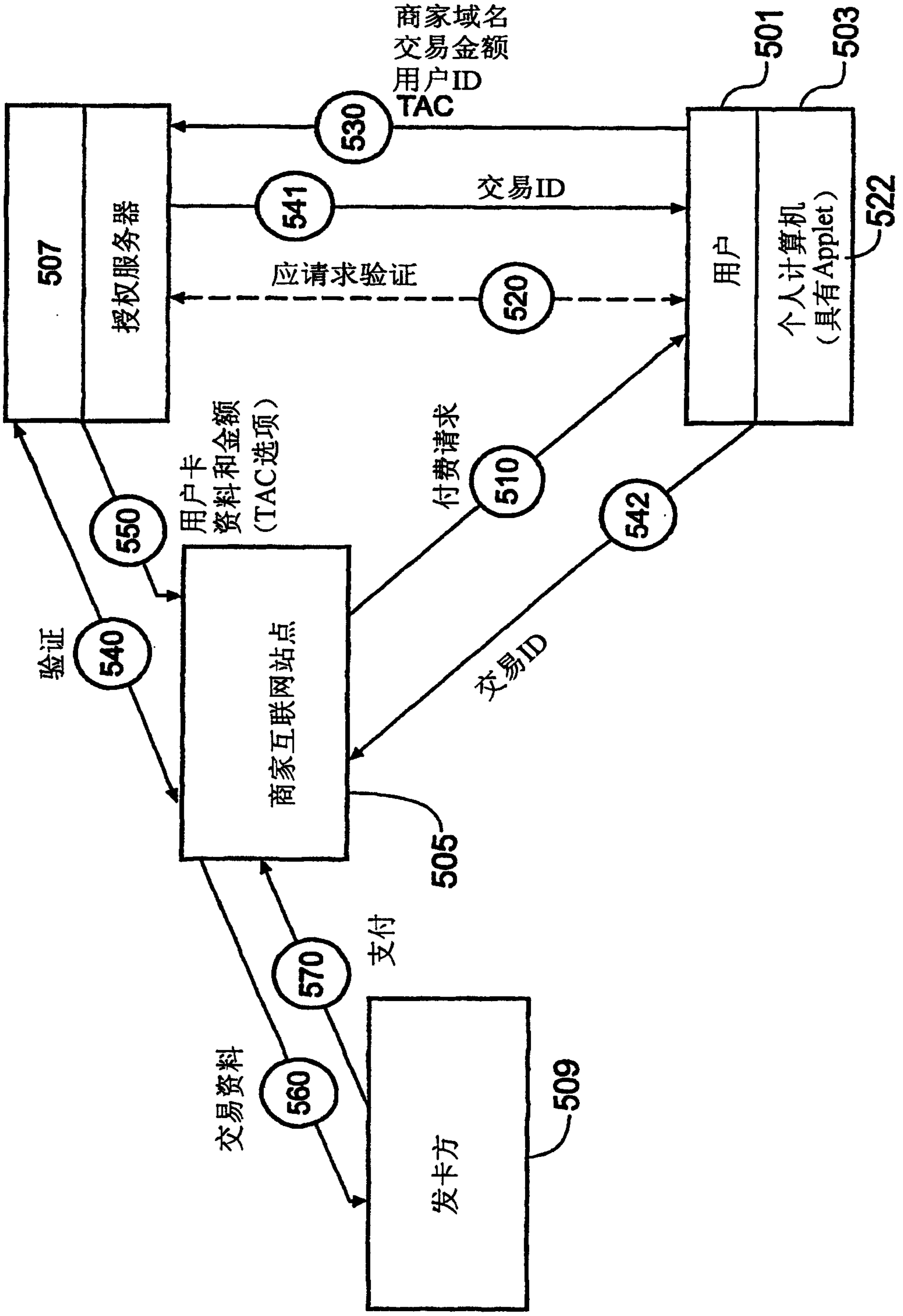

507
授权服务器
501
503
用户
个人计算机
（具有Applet）
522
530
商家域名
交易金额
用户ID
TAC
541
交易ID
520
应请求验证
510
付费请求
542
交易ID
550
用户卡
资料和金额
（TAC选项）
540
验证
商家互联网站点
505
570
支付
560
交易资料
发卡方
509

图5

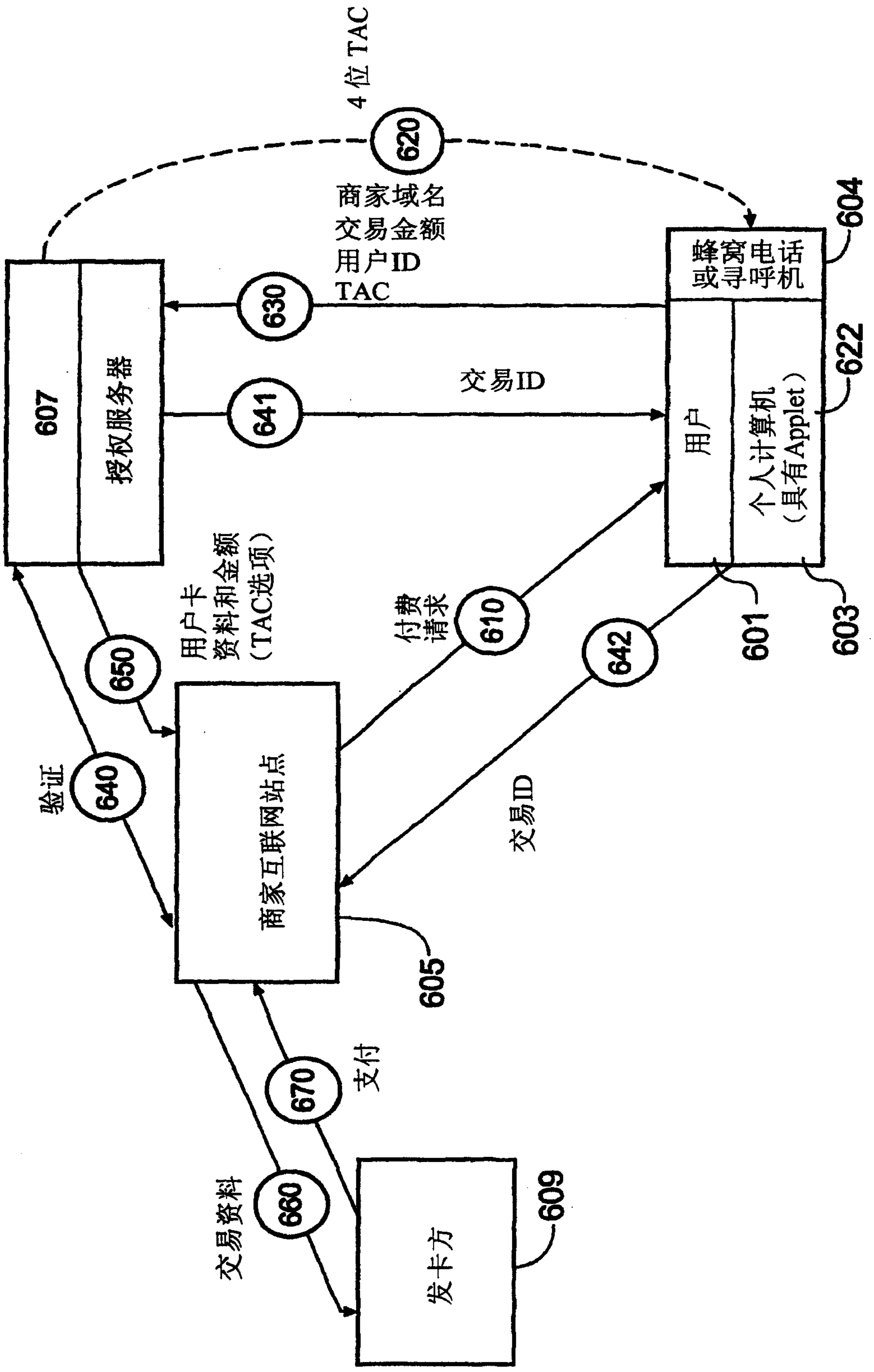

4位 TAC
620
商家域名
交易金额
用户ID
TAC
蜂窝电话
或寻呼机
604
607
授权服务器
630
641
交易ID
用户
个人计算机
（具有Applet）
622
601
603
用户卡
资料和金额
（TAC选项）
650
付费
请求
610
642
交易ID
验证
640
商家互联网站点
605
670
支付
660
交易资料
发卡方
609

图6

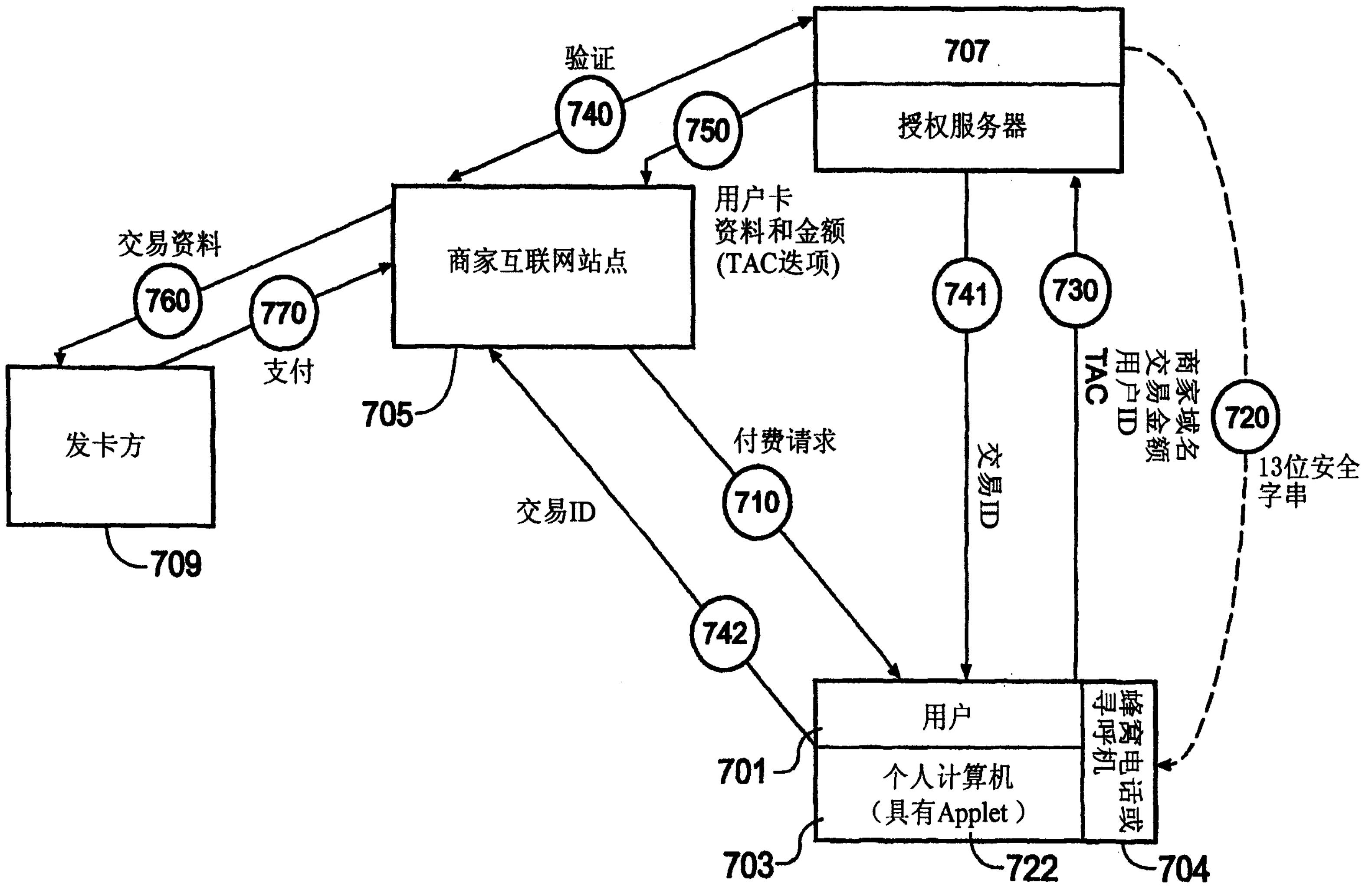

707
授权服务器
验证
740
750
用户卡
资料和金额
(TAC选项)
交易资料
760
770
支付
商家互联网站点
705
发卡方
709
741
交易ID
730
商家域名
交易金额
用户ID
TAC
720
13位安全
字串
付费请求
710
交易ID
742
用户
个人计算机
（具有Applet）
蜂窝电话或
寻呼机
701
703
722
704

图 7

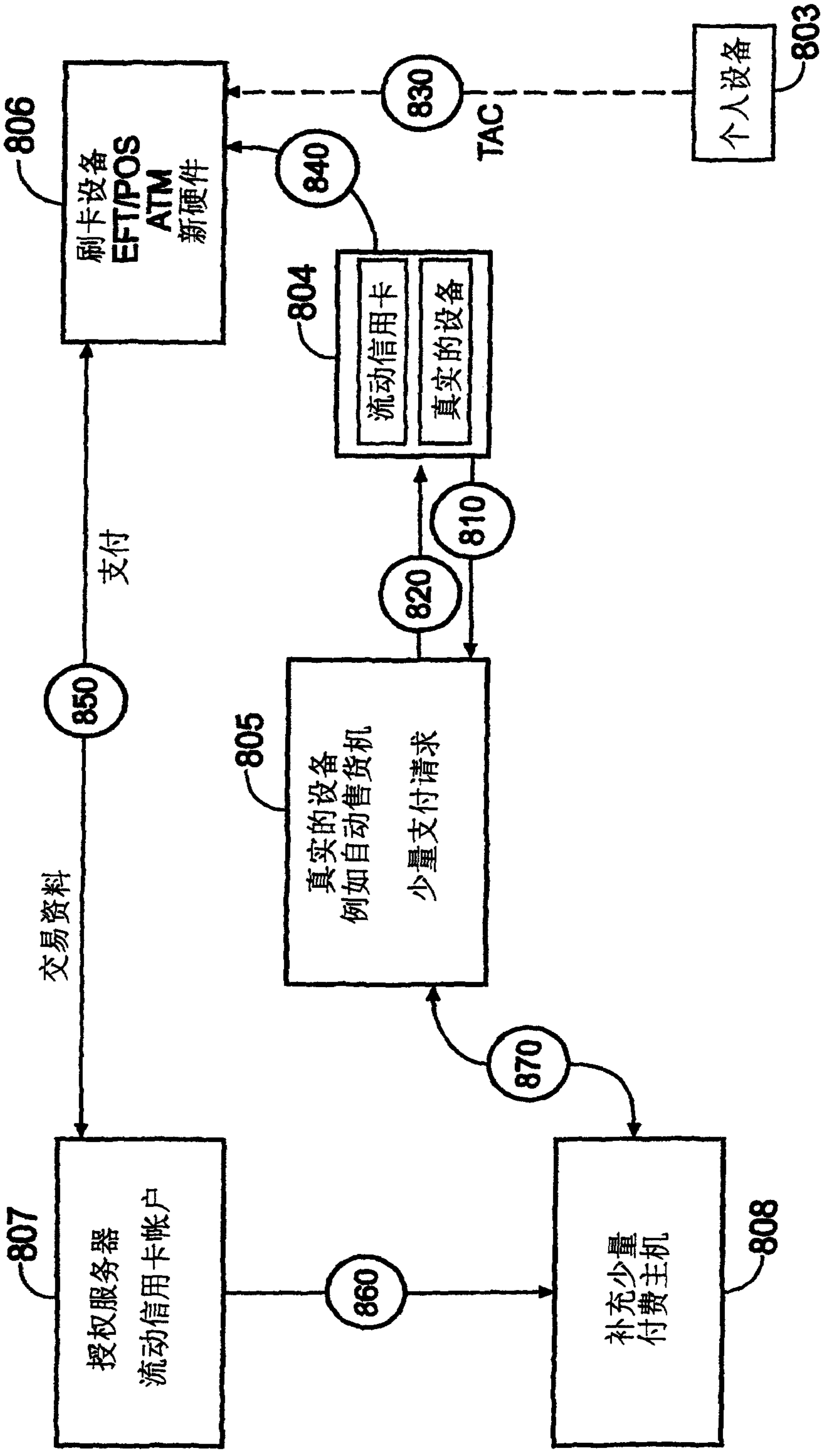
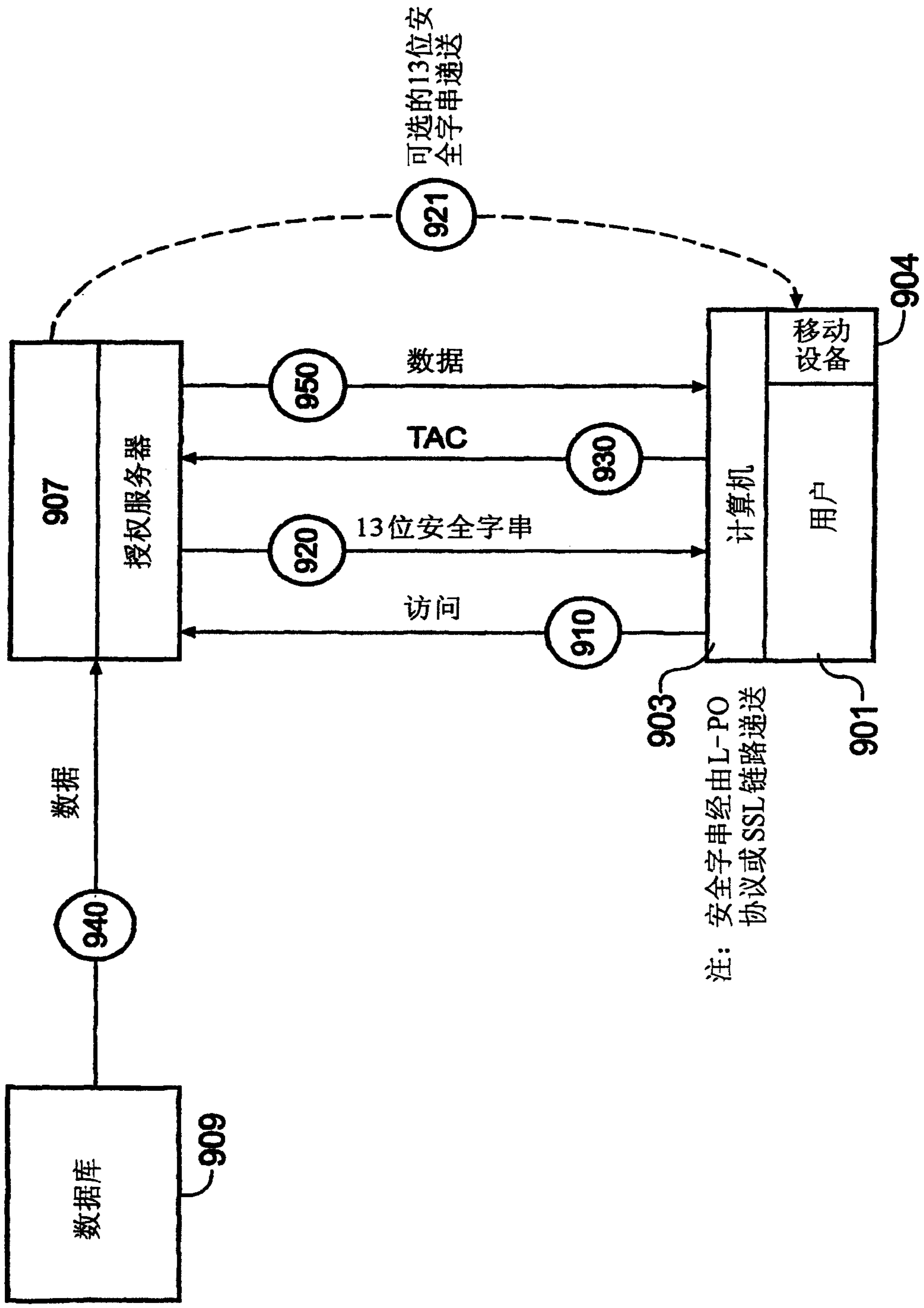

806
刷卡设备
EFT/POS
ATM
新硬件
830
TAC
803
个人设备
840
804
流动信用卡
真实的设备
810
820
850
支付
交易资料
805
真实的设备
例如自动售货机
少量支付请求
870
807
授权服务器
流动信用卡帐户
860
808
补充少量
付费主机

图 8



注：安全字串经由L-PO协议或SSL链路递送

图 9

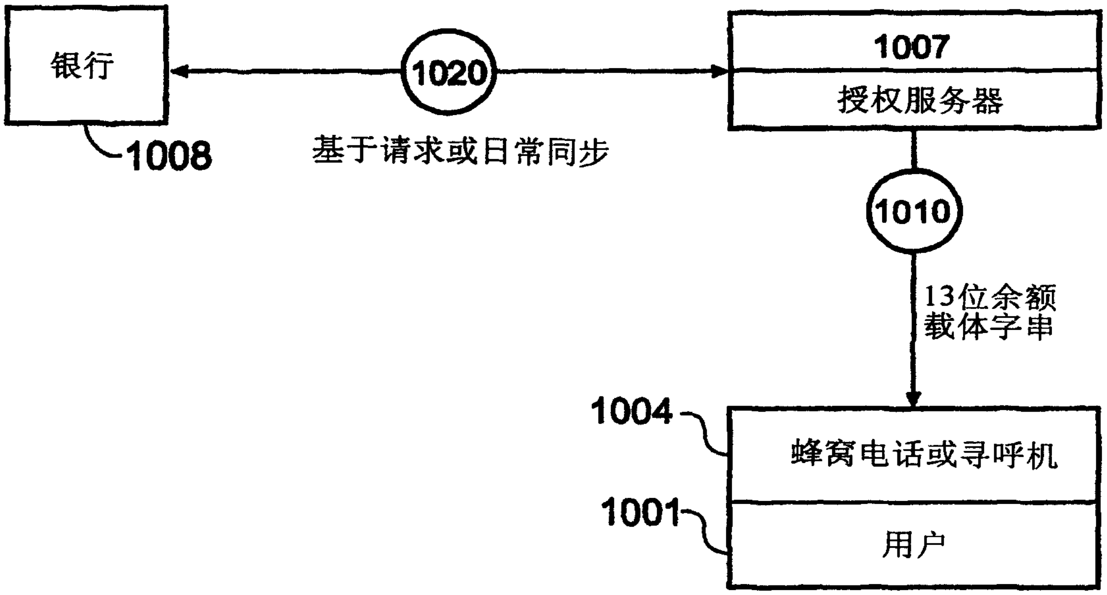

银行
1008
1020
基于请求或日常同步
1007
授权服务器
1010
13位余额
载体字串
1004
蜂窝电话或寻呼机
1001
用户

图 10

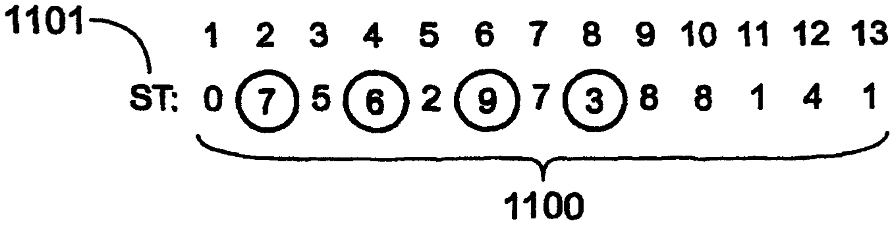
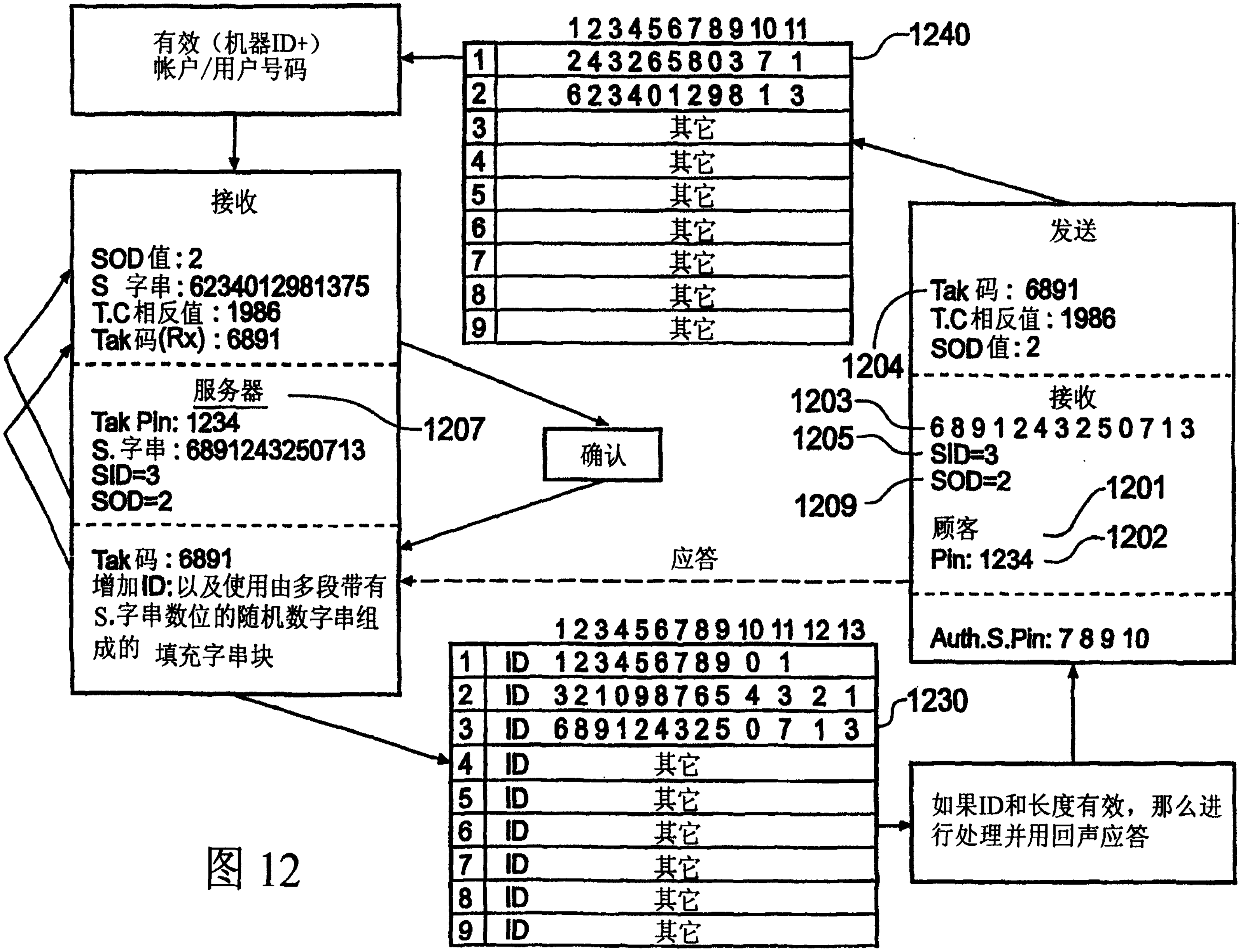

1101
1 2 3 4 5 6 7 8 9 10 11 12 13
ST: 0 7 5 6 2 9 7 3 8 8 1 4 1
1100

图 11



	1 2 3 4 5 6 7 8 9 10 11
1	2 4 3 2 6 5 8 0 3 7 1
2	6 2 3 4 0 1 2 9 8 1 3
3	其它
4	其它
5	其它
6	其它
7	其它
8	其它
9	其它

		1 2 3 4 5 6 7 8 9 10 11 12 13
1	ID	1 2 3 4 5 6 7 8 9 0 1
2	ID	3 2 1 0 9 8 7 6 5 4 3 2 1
3	ID	6 8 9 1 2 4 3 2 5 0 7 1 3
4	ID	其它
5	ID	其它
6	ID	其它
7	ID	其它
8	ID	其它
9	ID	其它

图 12

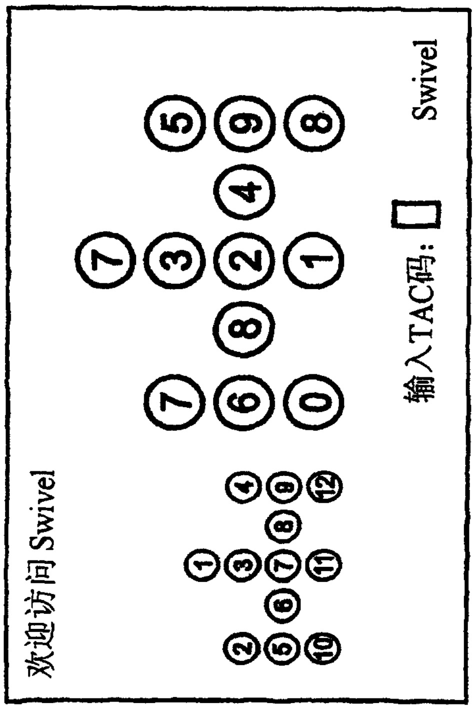


图13a

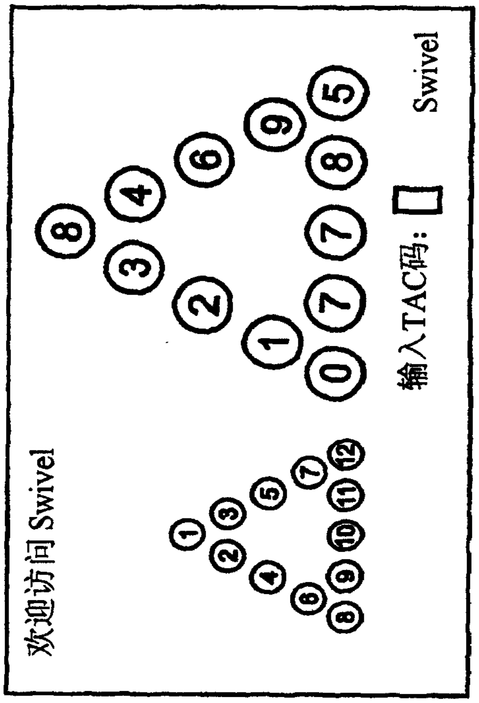


图13b

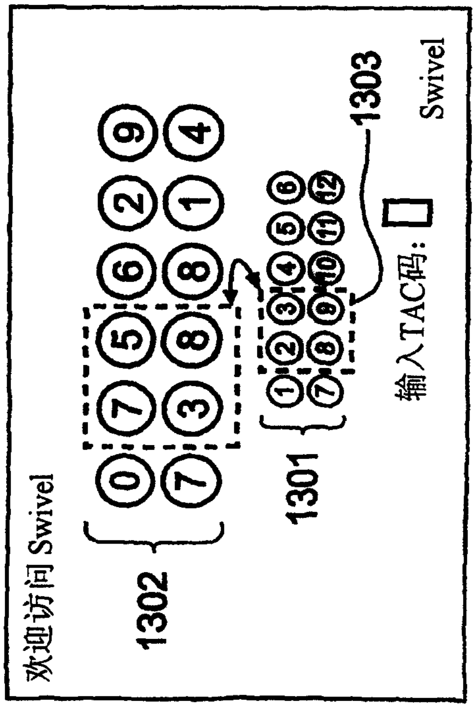


图13c

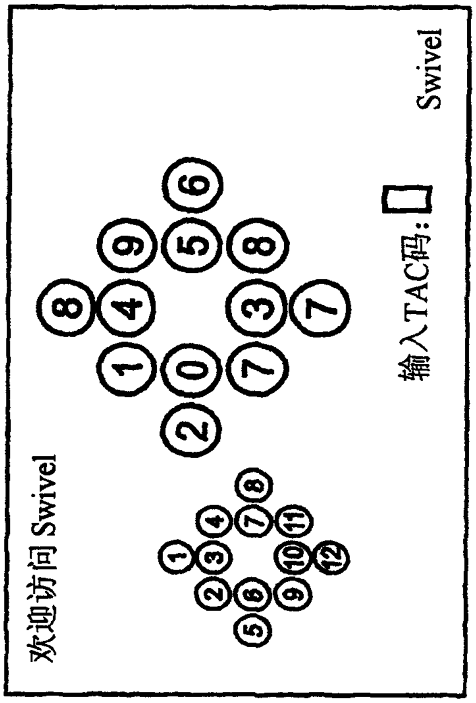


图13d

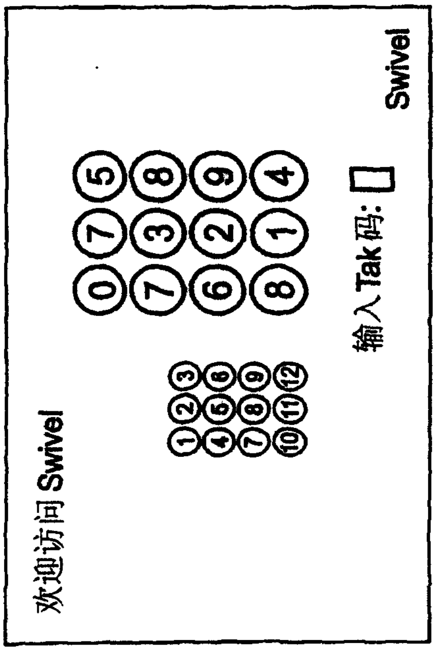


图 13e

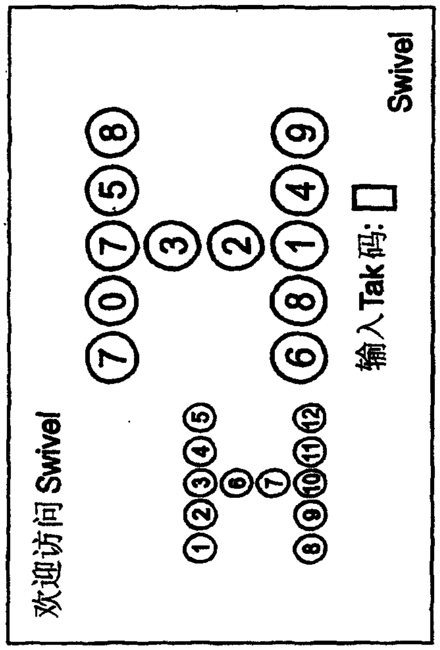


图 13f

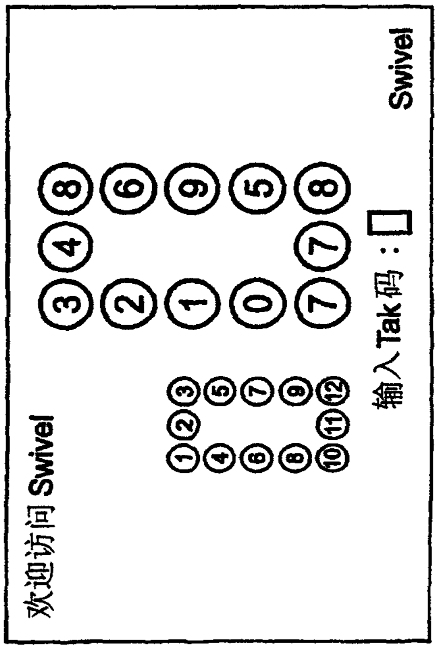


图 13g

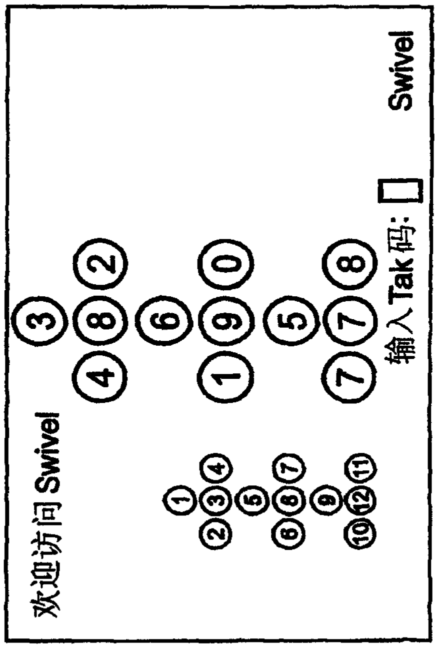


图 13h

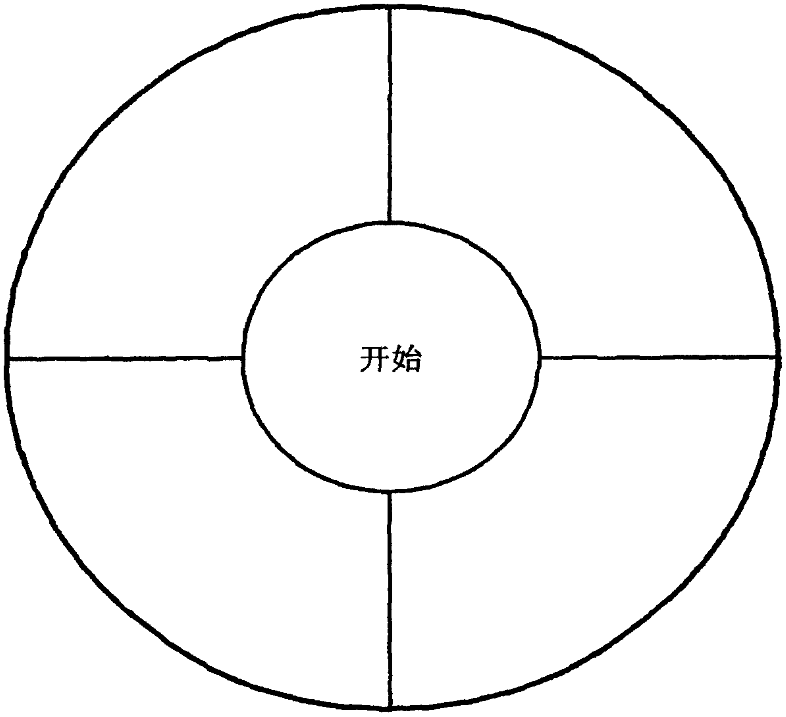


图14

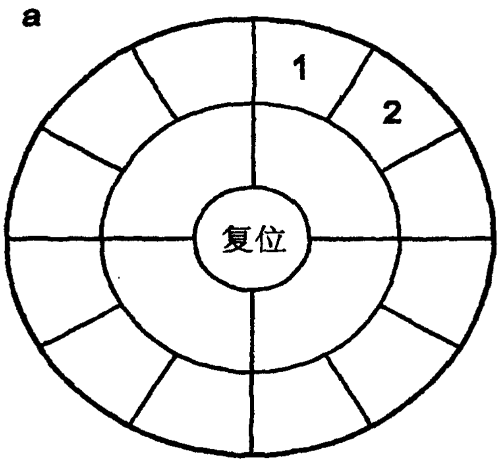


图15a

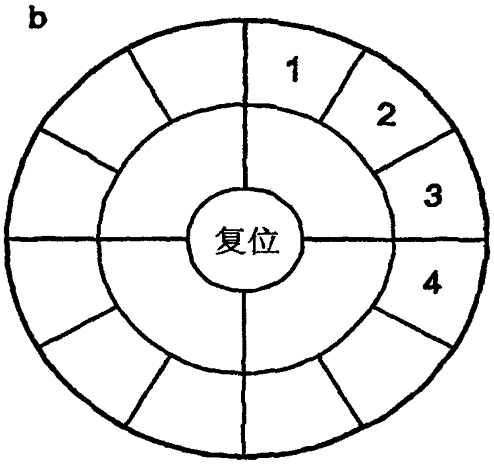


图15 b

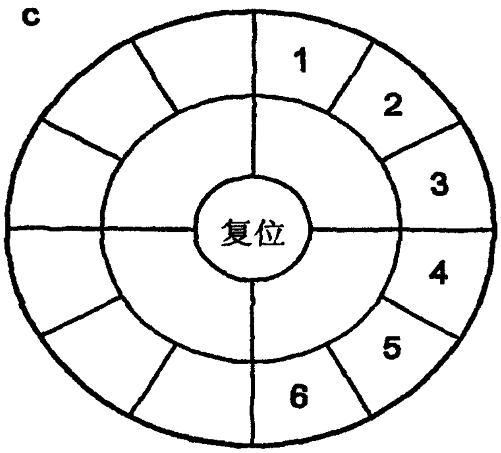


图15c

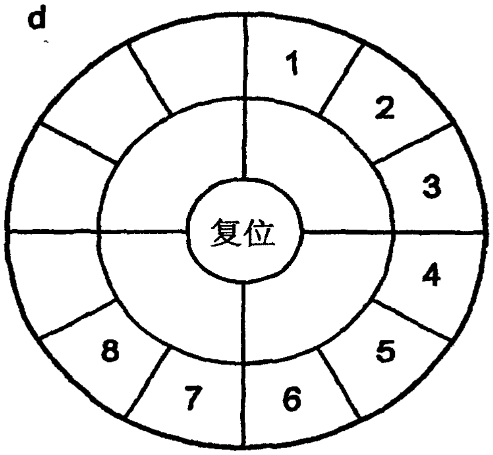


图15 d

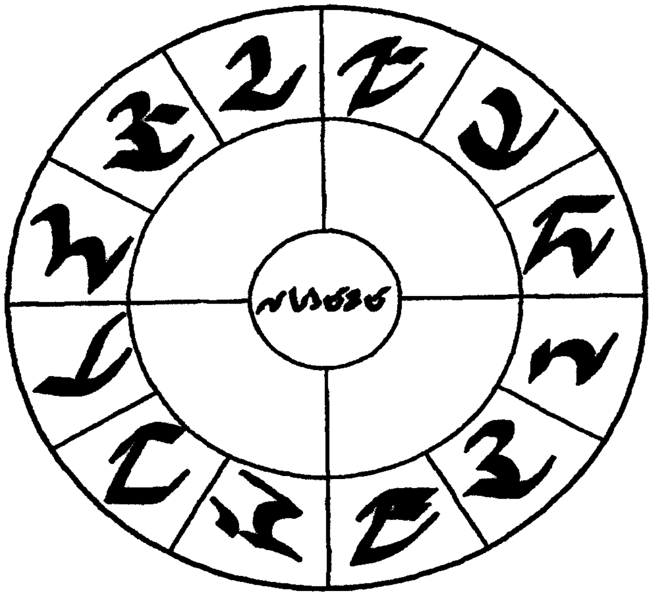


图15e

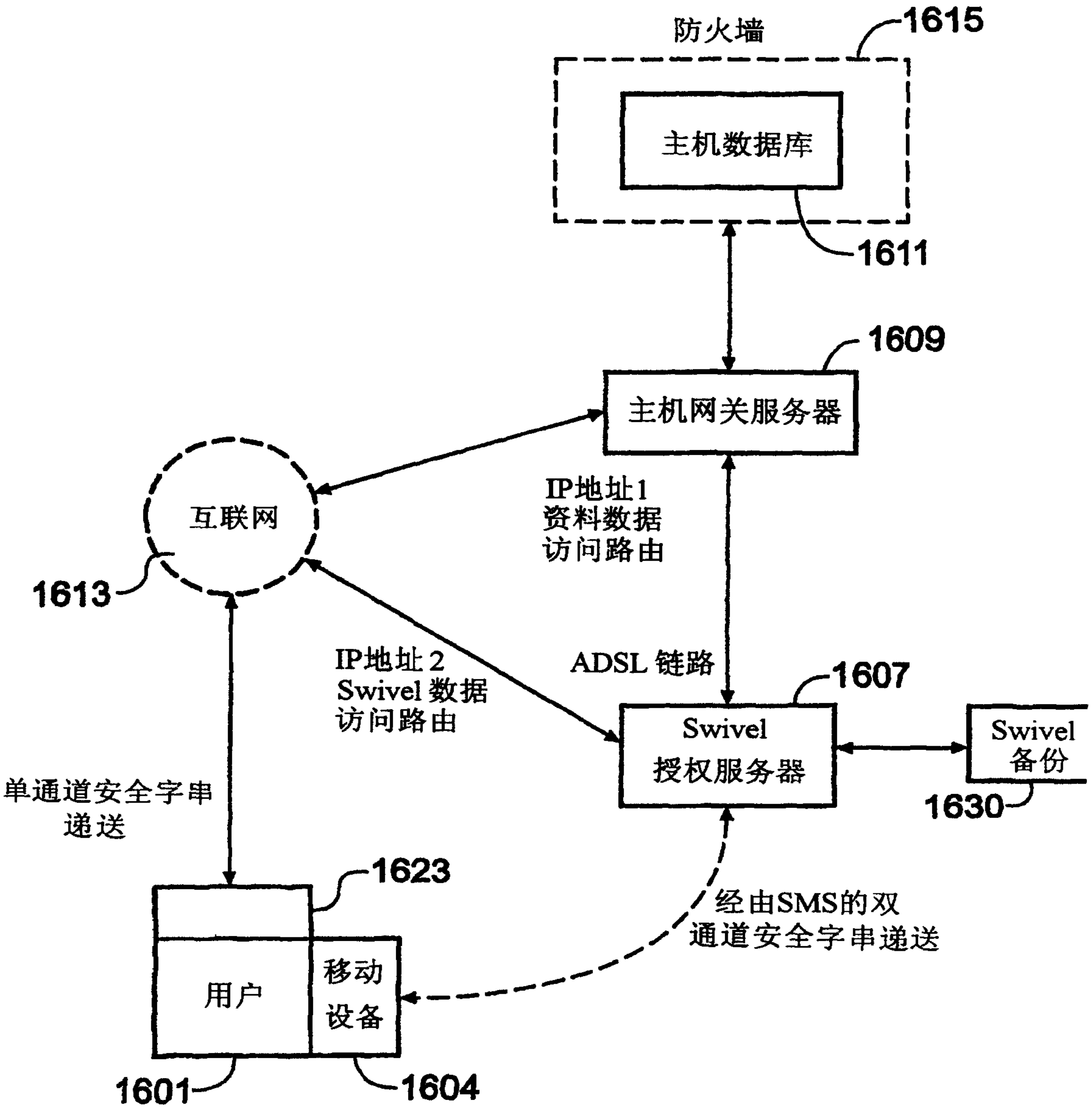

防火墙
1615
主机数据库
1611
1609
主机网关服务器
互联网
1613
IP地址1
资料数据
访问路由
ADSL 链路
IP地址2
Swivel 数据
访问路由
1607
Swivel
授权服务器
Swivel
备份
1630
单通道安全字串
递送
1623
经由SMS的双
通道安全字串递送
用户
移动
设备
1601
1604

图16

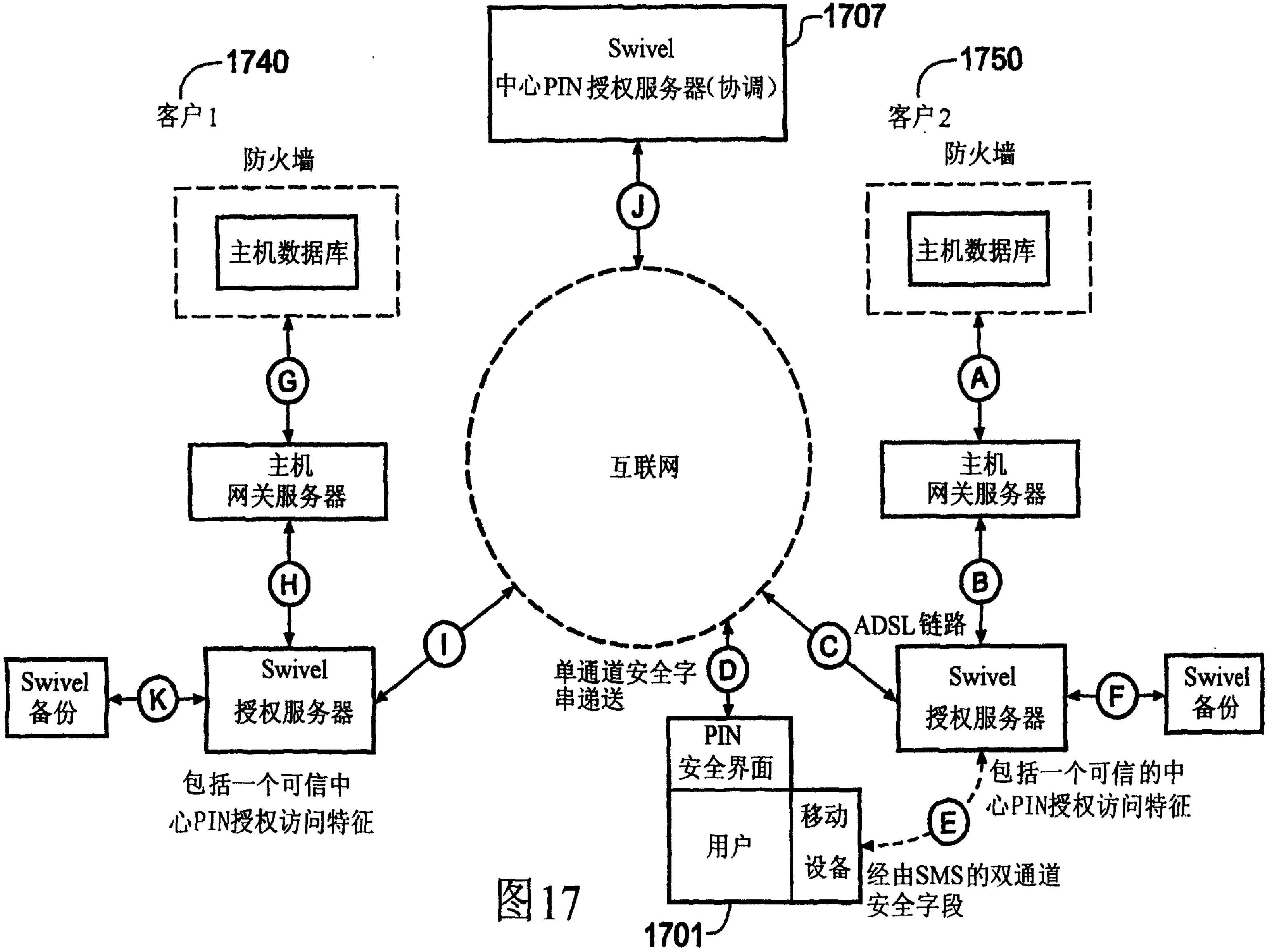

1740
客户1
防火墙
主机数据库
G
主机
网关服务器
H
Swivel
授权服务器
K
Swivel
备份
包括一个可信中
心PIN授权访问特征
I
1707
Swivel
中心PIN授权服务器(协调)
J
互联网
单通道安全字
串递送
D
PIN
安全界面
用户
移动
设备
1701
1750
客户2
防火墙
主机数据库
A
主机
网关服务器
B
ADSL链路
C
Swivel
授权服务器
F
Swivel
备份
包括一个可信的中
心PIN授权访问特征
E
经由SMS的双通道
安全字段

图17

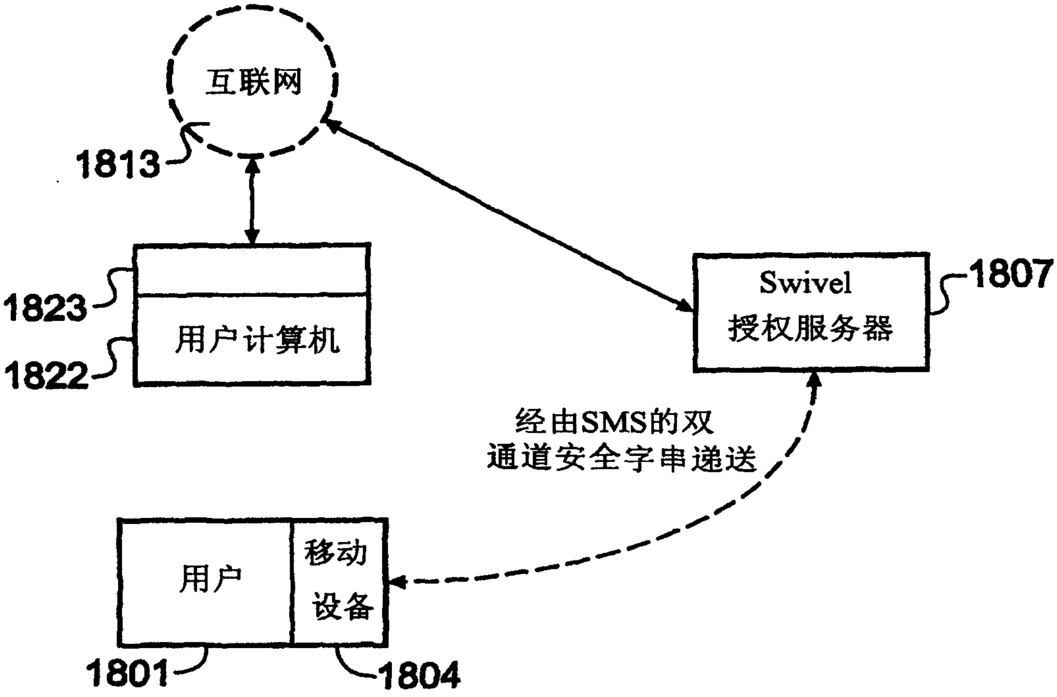

互联网
1813
1823
1822
用户计算机
Swivel
授权服务器
1807
经由SMS的双
通道安全字串递送
用户
移动
设备
1801
1804

图18

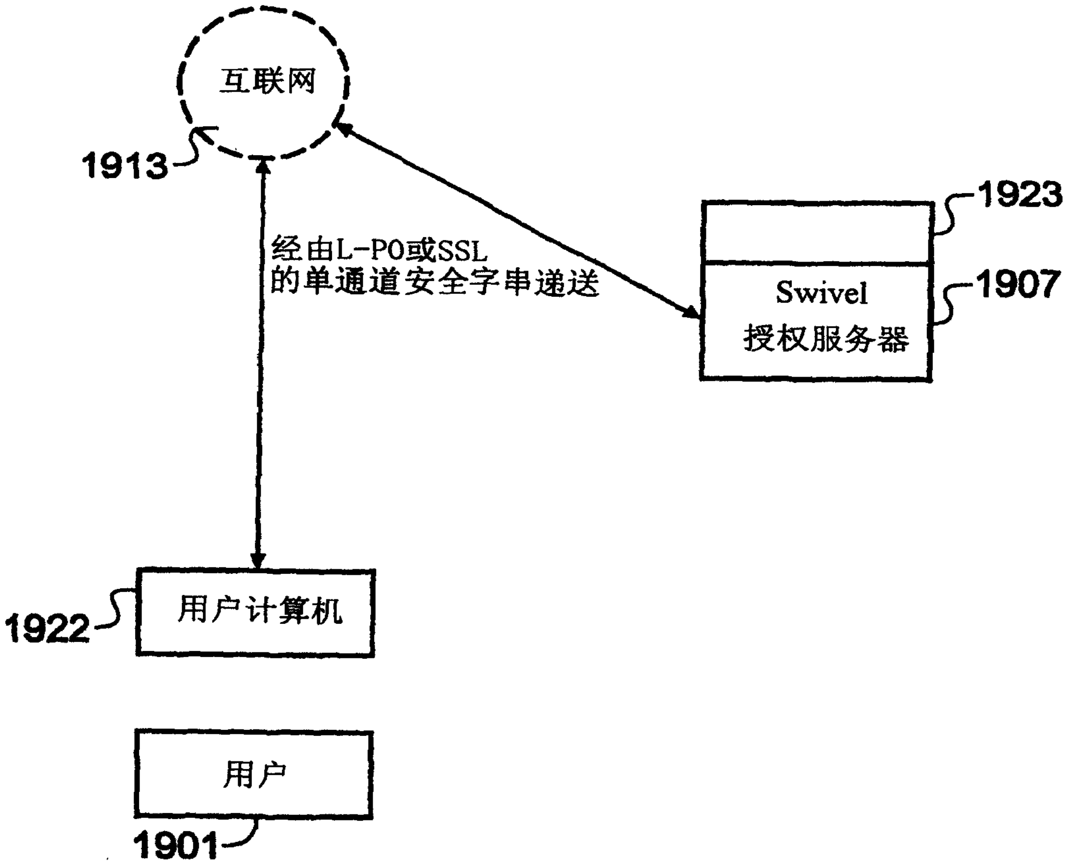

互联网
1913
经由L-PO或SSL
的单通道安全字串递送
1923
Swivel
授权服务器
1907
用户计算机
1922
用户
1901

图19

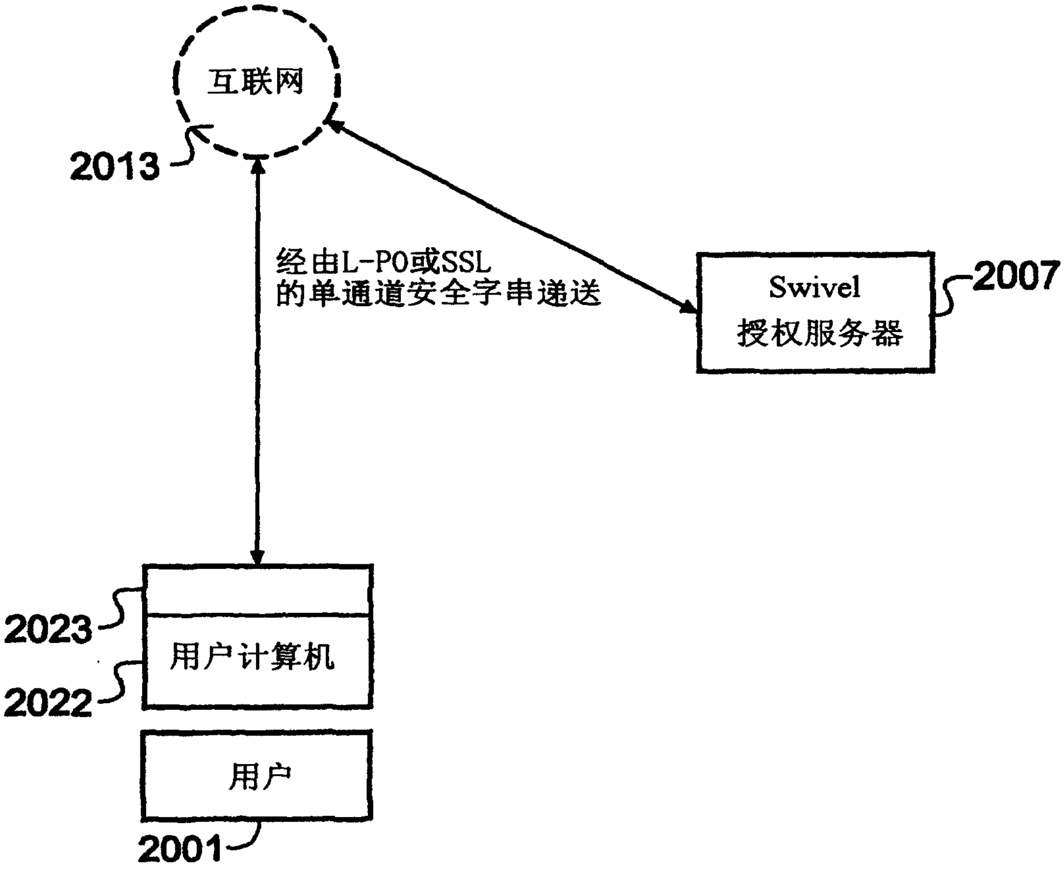

互联网
2013
经由L-PO或SSL
的单通道安全字串递送
Swivel
授权服务器
2007
2023
用户计算机
2022
用户
2001

图20

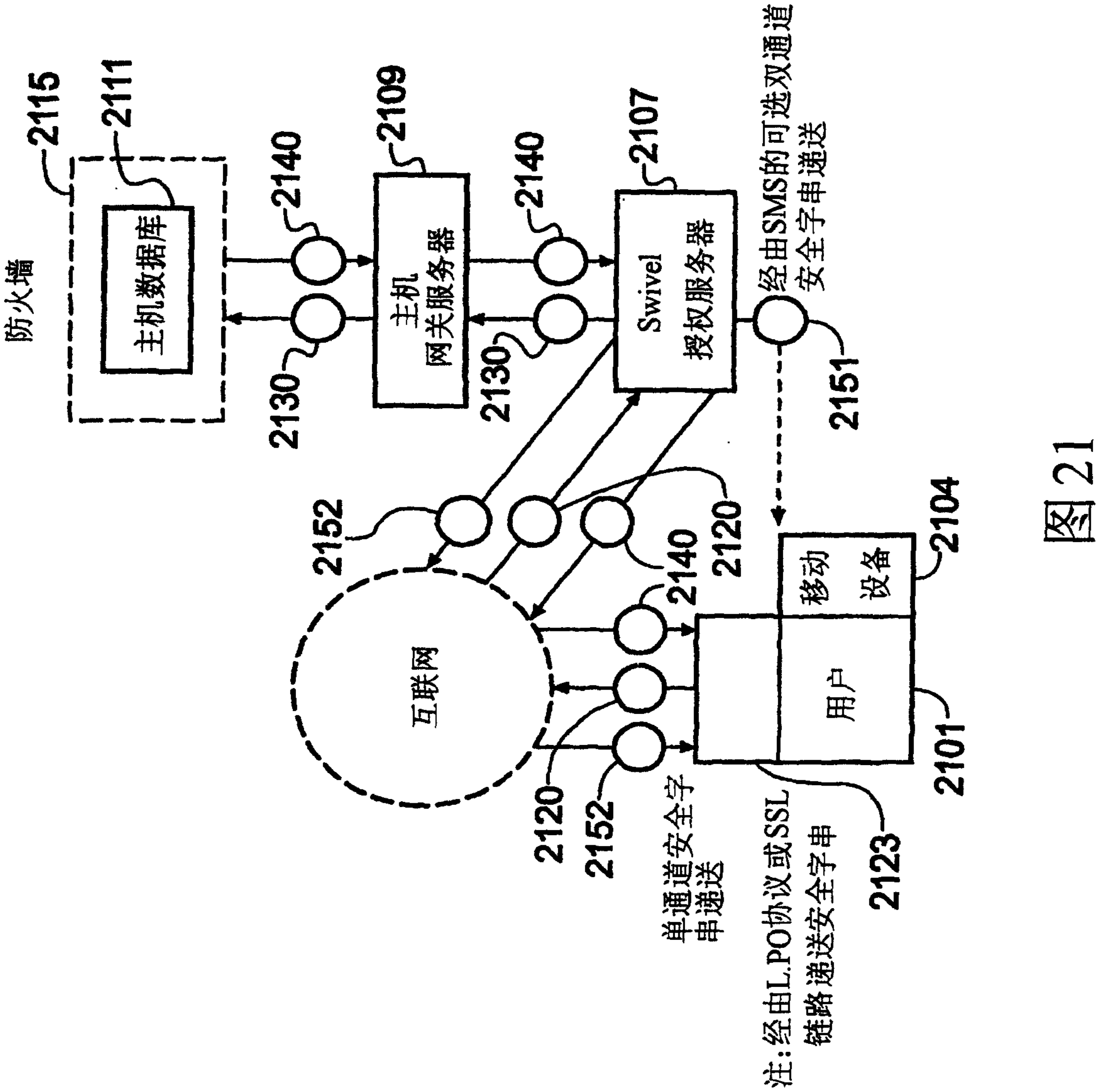

防火墙
2115
2111
主机数据库
2140
2130
2109
主机
网关服务器
2140
2130
2107
Swivel
授权服务器
经由SMS的可选双通道安全字串递送
2151
2152
2120
2140
2120
互联网
2140
移动设备
2104
用户
2101
2120
2152
单通道安全字串递送
2123
注:经由L.PO协议或SSL链路递送安全字串

图21

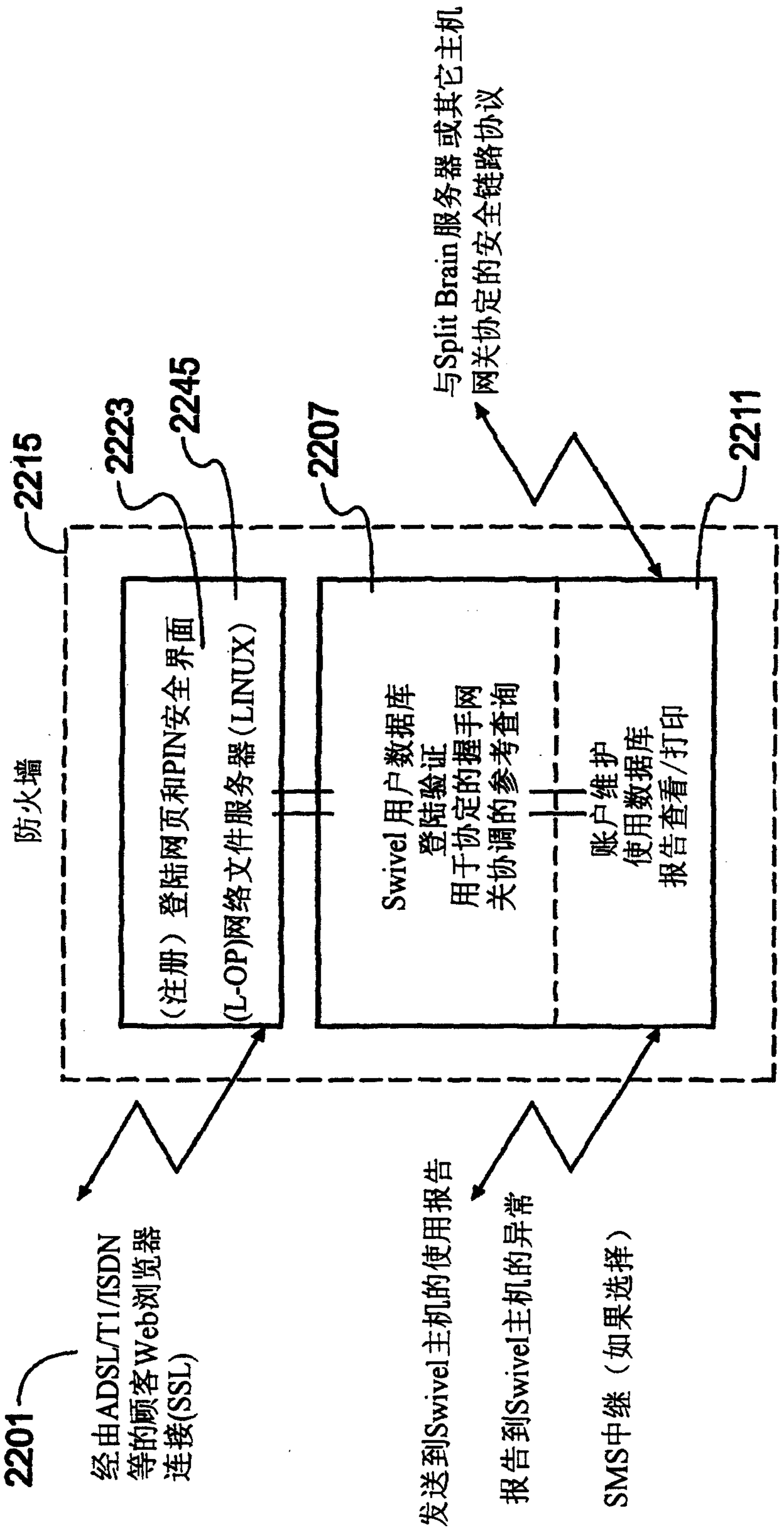

2215
防火墙
2223
2245
（注册）登陆网页和PIN安全界面
(L-OP)网络文件服务器（LINUX）
2207
Swivel 用户数据库
登陆验证
用于协定的握手网
关协调的参考查询
账户维护
使用数据库
报告查看/打印
2211
与Split Brain服务器 或其它主机
网关协定的安全链路协议
2201
经由ADSL/T1/ISDN
等的顾客Web浏览器
连接(SSL)
发送到Swivel主机的使用报告
报告到Swivel主机的异常
SMS中继（如果选择）

图 22

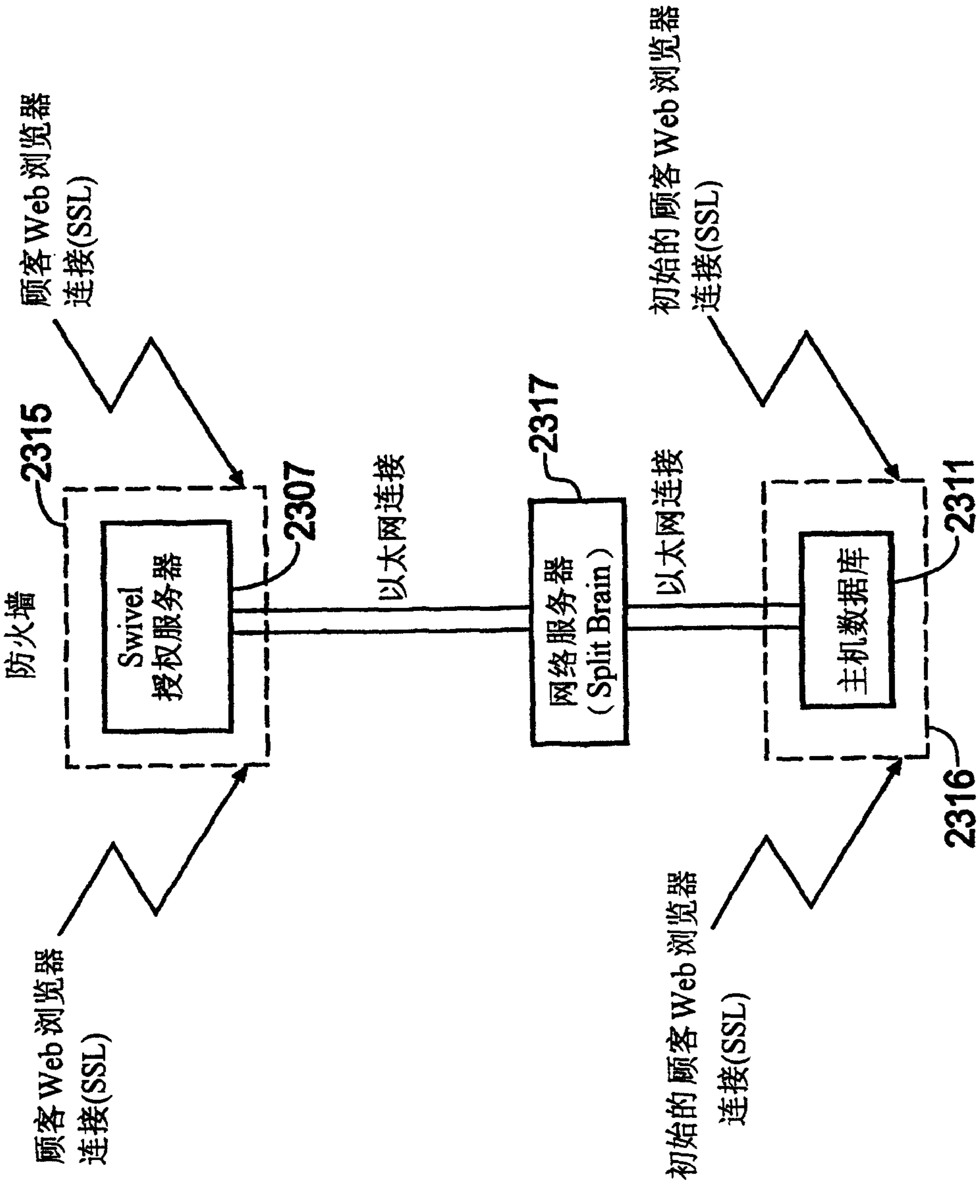

顾客Web浏览器连接(SSL)
防火墙
2315
Swivel授权服务器
2307
顾客Web浏览器连接(SSL)
以太网连接
网络服务器（Split Brain）
2317
以太网连接
初始的顾客Web浏览器连接(SSL)
主机数据库
2311
2316
初始的顾客Web浏览器连接(SSL)

图23

uspto UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
18/197,071	12/06/2023 07:59:45 PM Z ET	104402-5075-US

Title of Invention

METHOD AND SYSTEM FOR PRESENTING REPRESENTATIONS OF PAYMENT ACCEPTING UNIT EVENTS

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	-
CONFIRMATION #	9843	FILED BY	Jackeline De Ranieri
PATENT CENTER #	63518540	AUTHORIZED BY	Douglas Crisman
CUSTOMER #	24341	FILING DATE	05/14/2023
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Paresh K. Patel

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
DA / 500310	E2023B6K02329150	Jackeline De Ranieri
PRE-AUTHORIZED ACCOUNT	PRE-AUTHORIZED CATEGORY	
500310	37 CFR 1.19 (Document supply fees); 37 CFR 1.21 (Miscellaneous fees and charges)	

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2806	SUBMISSION OF AN INFORMATION DISCLOSURE STATEMENT	104.00	1	104.00
			TOTAL AMOUNT:	$104.00

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

24341 7590 04/10/2023
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
OUSSIR, EL MEHDI	
ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 04/10/2023

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/893,514	02/09/2018	Paresh K. Patel	104402-5026-US	4668

TITLE OF INVENTION: REFUND CENTERS FOR PROCESSING AND DISPENSING VENDING MACHINE REFUNDS VIA AN MDB ROUTER

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	07/10/2023

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 40% the amount of undiscounted fees, and micro entity fees are 20% the amount of undiscounted fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications. **Because electronic patent issuance may occur shortly after issue fee payment, any desired continuing application should preferably be filed prior to payment of this issue fee in order not to jeopardize copendency.**

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

24341 7590 04/10/2023

Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/893,514	02/09/2018	Paresh K. Patel	104402-5026-US	4668

TITLE OF INVENTION: REFUND CENTERS FOR PROCESSING AND DISPENSING VENDING MACHINE REFUNDS VIA AN MDB ROUTER

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$480	$0.00	$0.00	$480	07/10/2023

EXAMINER	ART UNIT	CLASS-SUBCLASS
OUSSIR, EL MEHDI	3685	705-050000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

□ Change of correspondence address (or Change of Correspondence Address form PTO/AIA/122 or PTO/SB/122) attached.

□ "Fee Address" indication (or "Fee Address" Indication form PTO/AIA/47 or PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1____________________

2____________________

3____________________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE

(B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : □ Individual □ Corporation or other private group entity □ Government

4a. Fees submitted: □ Issue Fee □ Publication Fee (if required)

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

□ Electronic Payment via Patent Center or EFS-Web □ Enclosed check □ Non-electronic payment by credit card (Attach form PTO-2038)

□ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. __________

5. **Change in Entity Status** (from status indicated above)

□ Applicant certifying micro entity status. See 37 CFR 1.29

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

□ Applicant asserting small entity status. See 37 CFR 1.27

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

□ Applicant changing to regular undiscounted fee status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature ____________________ Date ____________________

Typed or printed name ____________________ Registration No. ____________________

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/893,514	02/09/2018	Paresh K. Patel	104402-5026-US	4668

24341 7590 04/10/2023
Morgan, Lewis & Bockius LLP (PA)
1400 Page Mill Road
Palo Alto, CA 94304-1124

EXAMINER	
OUSSIR, EL MEHDI	
ART UNIT	PAPER NUMBER
3685	

DATE MAILED: 04/10/2023

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	**Application No.** 15/893,514	**Applicant(s)** Patel et al.	
	Examiner EL MEHDI OUSSIR	**Art Unit** 3685	**AIA (FITF) Status** Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.☑ This communication is responsive to 01/30/2023.
□ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2.□ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3.☑ The allowed claim(s) is/are See Continuation Sheet . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4.□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a) □All b) □ Some* c) □ None of the:

1. □ Certified copies of the priority documents have been received.
2. □ Certified copies of the priority documents have been received in Application No. _____ .
3. □ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5.□ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
□ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6.□ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1.☑ Notice of References Cited (PTO-892)
2.☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____.
3.□ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4.□ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. □ Examiner's Amendment/Comment
6. ☑ Examiner's Statement of Reasons for Allowance
7. □ Other _____.

/EL MEHDI OUSSIR/
Primary Examiner, Art Unit 3685

Continuation of 3. The allowed claim(s) is/are: 11,16,18-19 and 21-28

Detailed Action

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

This communication is in response to Applicant's response filed on January 30, 2023 in response to Examiner's Non-Final Office Action filed on September 30, 2022.

The information disclosure statements filed on September 16, 2022 and October 19, 2022 have been considered.

Claims 11, 16, 18-19, and 21-28 are pending. All other claims are cancelled.

Reasons for allowance

Claims 11, 16, 18-19, and 21-28 are allowed.

Applicant's arguments filed on January 30, 2023, pages 6-8, regarding claim rejections under 35 U.S.C. 112 have been fully considered and are persuasive. The claim rejections are withdrawn.

All previous rejections and response to arguments are incorporated entirely herewith.

The claims overcome all objections and rejections.

The claims are novel over prior art because the claims are not obvious in light of the prior art. Although the claims capture different limitations that can be found in various references individually; the limitations as a whole would not be deemed obvious.

Some of the closest art related to the claims include U.S. Patent Application Publication 2015/0235202 to Zabala, U.S. Patent Application Publication 2015/0154579 to Teicher, U.S. Patent 9547859 to Patel et a., and U.S. Patent Application Publication 2016/0086145 to Tsutsui.

Zabala teaches a device in communication with a vending machine to perform cashless payments. A user can utilize a mobile device to establish a connection with the vending machine and purchase a product from the phone and have the vending machine dispense it.

Zabala teaches receiving a request for a cash payment; transmitting the request to an authorizing server distinct from the mobile device; receiving from the authorizing server an authorization message authorizing the cash payment; in response to receiving the authorization message, receiving a user selection of a payment accepting machine distinct from the mobile device; transmitting from the mobile device to the payment accepting machine an electronic command including one or more… payment accepting machine- dependent conditions, wherein a first of the one or more… payment accepting machine-dependent conditions comprises a… button or control at the payment accepting machine must be engaged; Abstract, at least Paragraphs 0004, 0042 and Figures 1, 8, 11, and 16.

Zabala does not explicitly disclose time dependent condition for the transaction; however, a transaction that is completed is understood that it is completed within a predetermined time otherwise the transaction is not processed. Zabala does not specifically disclose that the button must be activated within a predetermined time; however, because Zabala teaches a button is pressed in order to allow for the item to be dispensed, it is understood that said pressing is done within a predetermined time.

U.S. Patent 9,547,859 to Patel el al. is directed to a device with one or more processors, memory, and two or more communication capabilities obtains, from a payment module, an authorization request via a first communication capability (e.g., Bluetooth). The device sends, to a server, the authorization request via a second communication capability distinct from the first communication capability (e.g., cellular or WiFi technology). In response to sending the authorization request, the device obtains, from the server, authorization information via the second communication capability. After obtaining the authorization information, the device detects a trigger condition to perform a transaction with a payment accepting unit associated with the payment module. In response to detecting the trigger condition, the device sends, to the payment module, at least a portion of the authorization information via the first communication capability.

Patel does not teach transmitting from the mobile device to the payment accepting machine an electronic command including one or more time-dependent and payment accepting machine- dependent conditions, wherein a first of the one or more time-dependent and payment accepting machine-dependent conditions comprises a predefined time or time period by which a button or control at the payment accepting machine must be engaged; displaying the one or more time-dependent and payment accepting machine- dependent conditions on a display of the mobile device; at the payment accepting machine: receiving the electronic command and the one or more time-dependent and payment accepting machine-dependent conditions from the mobile device.

U.S. Patent Application Publication 2016/0086145 to Tsutsui teaches a voucher ticket system and method of use employing a bill validator installed into any suitable automated machine, including an Automated Teller Machine (ATM), a gaming machine, etc. The bill validator is integrated with a bill reader, a voucher ticket reader, a reader for acquisition of electronic voucher ticket information from a portable computing device, a printer, and other supporting peripheral devices. The voucher ticket system includes a secured communication link with a host account manager serving a plurality of electronic money accounts. The method includes steps of receiving a value of electronic money or identification information associated with the electronic voucher ticket with account information associated with the electronic money account and sending the received value of the electronic money or the identification information of the voucher ticket to an upper control section of the one of the gaming machine and the ATM for completion of a financial transaction.

Further searches including non-patent literature and foreign references have been carried out. However, the references found and those cited fail to disclose the claim limitations of claim 11 as a whole. The combination of references to teach the claimed limitations would not have been obvious to one of ordinary skill in the art before the effective filing date of the Application.

The references relied upon throughout prosecution, cited, and the newly cited references fail to disclose:

A method, comprising: at a mobile device:

receiving a request for a cash payment; transmitting the request to an authorizing server distinct from the mobile device;