













































































41

said recording unit storing magnetic data on information for use in processing which is carried out by said management device.

14. The portable electronic device according to claim 10, wherein upon receipt of a predetermined signal via said transceiving interface, said portable electronic device transmits public key information of said authorized user, which public key information is registered in said portable electronic device, from said transceiving interface to said processing device.

15. The portable electronic device according to claim 10, further comprising a lock function section which is operable to prohibit input of biometric feature information to said portable electronic device, if the evaluation is made a predetermined number of times successively, as a result of the comparison by said feature data verifying section, that said to-be-verified biometric feature data never matches said pre-stored valid biometric feature data in terms of said predetermined matching condition.

16. The portable electronic device according to claim 10, further comprising a management log recording section storing a management log of said PIN, said management log accumulating the dates and times when said PIN has been transmitted, or descriptions of transactions performed, or both of these.

17. A portable electronic device with a user verification function utilizing biometric information, which device is for use in a user verification system that includes the portable electronic device, adapted to be carried by a user, with a function as a debit card; a data processing device for directly accessing such portable electronic device, temporarily installed therein, so as to function as a debit card terminal for the portable electronic device; a management device installed in a bank to serve as a host computer that manages the user's bank account from which payment for a purchase made with the portable electronic device, as the debit card, is withdrawn, said managing device accessing said portable electronic device via said data processing device and verifying said user utilizing a person identification unit number (PIN), said portable electronic device comprising:

- a biometric feature data register section having pre-stored valid biometric feature data of an authorized user of said portable electronic device;
- a transceiving interface for transmitting/receiving data to/from said data processing device;
- a biometric feature data verifying section for comparing to-be-verified biometric feature data, which is received from said data processing device via said transceiving interface, with said pre-stored valid biometric feature data; and
- a PIN register section having a pre-stored PIN of said authorized user of said portable electronic device, said biometric feature data verifying section comparing said to-be-verified biometric feature data, which has been received via said transceiving interface, with said pre-stored valid biometric feature data, and as the result of the comparison, if said to-be-verified biometric feature data matches said pre-stored valid biometric feature data in terms of a predetermined matching condition, said PIN being transmitted from said transceiving interface to said management device via said data processing device,
- a clock function section for calculating the current time; and
- a time stamp verifying section for comparing a time stamp, if any, attached to the original to-be-verified

42

biometric feature data, with said current time, which has been calculated by said clock function section, said time stamp indicating the date and time when said to-be-verified biometric feature data has been extracted,

if it is found, as the comparison result by said biometric feature data verifying section, that said to-be-verified biometric feature data matches said pre-stored valid biometric feature data in terms of a predetermined matching condition, and also if it is found, as the comparison result by said time stamp verifying section, that a difference between said time stamp and said current time falls within a predetermined range, said user being identified as said authorized user of said portable electronic device to transmit the PIN to the management device.

18. The portable electronic device according to claim 17, wherein if said user is identified as said authorized user of said portable electronic device, as the comparison result by said biometric feature data verifying section and said time stamp verifying section, an encryption section encodes both said PIN and the date and time of the comparison performed, which date and time is obtained by said clock function section, and the encoded PIN and the encoded date and time of the comparison are then sent out from said transceiving interface to said management device.

19. A user verification system, comprising:

- a portable electronic device, adapted to be carried by a user, with a function as a debit card;
- a data processing device for directly accessing such portable electronic device, temporarily installed therein, so as to function as a debit card terminal for the portable electronic device; and
- a management device installed in a bank to serve as a host computer that manages the user's bank account from which payment for a purchase made with the portable electronic device, as the debit card, is withdrawn, said managing device accessing said portable electronic device via said data processing device and verifying said user utilizing a personal identification number (PIN),

said data processing device including:

- a biometric information measuring unit for measuring biometric information of said user;
- a biometric feature data extracting section for extracting to-be-verified biometric feature data from said biometric information, which has been measured by biometric information measuring unit;
- a first encryption section for encoding said to-be-verified biometric feature data with a public key; and
- a first transceiving interface for transmitting/receiving data to/from said portable electronic device,

said portable electronic device including:

- a biometric feature data register section having pre-stored valid biometric feature data of an authorized user of said portable electronic device;
- a second transceiving interface for transmitting/receiving data to/from said data processing device;
- a biometric feature data verifying section for comparing to-be-verified biometric feature data, which is received from said data processing device via said second transceiving interface, with said pre-stored valid biometric feature data;
- a secret key register section having a pre-stored valid secret key corresponding to said public key; and
- a decryption section for decoding encoded data, which has been encoded with said public key, with said valid secret key,

43

the encoded to-be-verified biometric feature data, which has been encoded by said first encryption section, being transmitted from said first transceiving interface to said portable electronic device,  
 said decryption section decoding said encoded data, 5  
 which has been received via said second transceiving interface, into the original to-be-verified biometric feature data, and  
 said biometric feature data verifying section comparing the original to-be-verified biometric feature data with 10  
 said pre-stored valid biometric feature data.

20. The user verification system according to claim 19, wherein upon receipt of a predetermined signal via said second transceiving interface, said portable electronic device transmits public key information of said authorized user, which public key information is registered in said 15  
 portable electronic device, from said second transceiving interface to said data processing device.

21. The user verification system according to claim 19, further comprising a lock function section which is operable to prohibit input of biometric feature information to said portable electronic device, if the evaluation is made a predetermined number of times successively, as a result of the comparison by said feature data verifying section of said portable electronic device, that said to-be-verified biometric feature data never matches said pre-stored valid biometric feature data in terms of said predetermined matching condition.

22. A user verification system, comprising:  
 a portable electronic device, adapted to be carried by a 30  
 user, with a function as a debit card;  
 a data processing device for directly accessing such portable electronic device, temporarily installed therein, so as to function as a debit card terminal for the portable electronic device; and 35  
 a management device installed in a bank to serve as a host computer that manages the user's bank account from which payment for a purchase made with the portable electronic device, as the debit card, is withdrawn, said managing device accessing said portable electronic device via said data processing device and verifying 40  
 said user utilizing a personal identification number (PIN).

said data processing device including:  
 a biometric information measuring unit for measuring 45  
 biometric information of said user;  
 a biometric feature data extracting section for extracting to-be-verified biometric feature data from said biometric information, which has been measured by biometric information measuring unit;  
 a first encryption section for encoding said to-be-verified biometric feature data with a public key; and  
 a first transceiving interface for transmitting/receiving data to/from said portable electronic device, 50

said portable electronic device including: 55  
 a biometric feature data register section having pre-stored valid biometric feature data of an authorized user of said portable electronic device;  
 a second transceiving interface for transmitting/receiving data to/from said data processing device; 60  
 a biometric feature data verifying section for comparing to-be-verified biometric feature data, which is received from said data processing device via said second transceiving interface, with said pre-stored valid biometric feature data;  
 a secret key register section having a pre-stored valid secret key corresponding to said public key; and 65

44

a decryption section for decoding encoded data, which has been encoded with said public key, with said valid secret key,  
 the encoded to-be-verified biometric feature data, which has been encoded by said first encryption section, being transmitted from said first transceiving interface to said portable electronic device,

said decryption section decoding said encoded data, which has been received via said second transceiving interface, into the original to-be-verified biometric feature data, and

said biometric feature data verifying section comparing the original to-be-verified biometric feature data with said pre-stored valid biometric feature data,

wherein said data processing device further includes a time stamp generating section for generating a time stamp as the date and time when said biometric feature data extracting section has extracted said to-be-verified biometric feature data,

wherein, said time stamp is encoded, together with said to-be-verified biometric feature data, by said first encryption section, and the encoded time stamp is then sent out from said first transceiving interface to said portable electronic device,

wherein said portable electronic device further includes: a clock function section for calculating the current time; and

a time stamp verifying section for comparing the original time stamp, which has been restored by said decryption section, with said current time, which has been calculated by said clock function section, and

wherein, if it is found, as the comparison result by said biometric feature data verifying section, that said to-be-verified biometric feature data matches said pre-stored valid biometric feature data in terms of a predetermined matching condition, and also if it is found, as the comparison result by said time stamp verifying section, that a difference between said time stamp and said current time falls within a predetermined range, said user is identified as said authorized user of said portable electronic device.

23. The user verification system according to claim 22, wherein said portable electronic device further includes: a user information register section having pre-stored user information about said authorized user of said portable electronic device; and

a second encryption section for encoding data, which is to be transmitted from said second transceiving interface to said data processing device, with said valid secret key, and

wherein as a result of comparison by said biometric feature data verifying section and said time stamp verifying section, if said user is identified as said authorized user of said portable electronic device, said second encryption section encodes at least one of the following items: said user information; the level of correlation between said to-be-verified biometric feature data and said pre-stored valid biometric feature data, which correlation level is obtained at the comparison; and the date and time of said comparison performed, which is provided by said clock function section, and the encoded item is sent out from said second transceiving interface to said data processing device as a verification result.

24. The user verification system according to claim 23, wherein said data processing section further includes a message digest creating section for creating a message

45

digest as a value obtained by inputting data to be transferred to said portable electronic device to a predetermined one-way function,

wherein said message digest and said to-be-verified biometric feature data are both encoded by said first encryption section, and are then sent out from said first transceiving interface to said portable electronic device,

wherein if said user is identified as said authorized user of said portable electronic device, as the comparison result by said biometric feature data verifying section and said time stamp verifying section, said second encryption section encodes the message digest which has been restored by said decryption section, and the encoded message digest is sent out from said second transceiving interface to said data processing device, as a verification result.

25. The user verification system according to claim 23, wherein said portable electronic device further includes a verification log recording section storing said verification result as a verification log for a predetermined time period.

26. A portable electronic device for use in a user verification system that includes the portable electronic device, adapted to be carried by a user, with a function as a debit card; a data processing device for directly accessing such portable electronic device, temporarily installed therein, so as to function as a debit card terminal for the portable electronic device; and a management device installed in a bank to serve as a host computer that manages the user's bank account from which payment for a purchase made with the portable electronic device, as the debit card, is withdrawn, said managing device accessing said portable electronic device via said data processing device and verifying said user utilizing a personal identification number (PIN),

said portable electronic device, comprising:

a biometric feature data register section having pre-stored valid biometric feature data of an authorized user of said portable electronic device;

a transceiving interface for transmitting/receiving data to/from said data processing device;

a biometric feature data verifying section for comparing to-be-verified biometric feature data, which is received from said data processing device via said transceiving interface, with said pre-stored valid biometric feature data;

a secret key register section having a pre-stored valid secret key corresponding to a public key; and

a decryption section for decoding encoded data, which has been encoded with said public key, with said valid secret key,

said decryption section decoding said encoded data, which has been received from said data processing device via said transceiving interface, into the original to-be-verified biometric feature data, and

said biometric feature data verifying section comparing the original to-be-verified biometric feature data with said pre-stored valid biometric feature data.

27. The portable electronic device according to claim 26, wherein upon receipt of a predetermined signal via said transceiving interface, said portable electronic device transmits public key information of said authorized user, which public key information is registered in said portable electronic device, from said transceiving interface to said data processing device.

46

28. The portable electronic device according to claim 26, further comprising a lock function section which is operable to prohibit input of biometric feature information to said portable electronic device, if the evaluation is made a predetermined number of times successively, as the result of the comparison by said feature data verifying section, that said to-be-verified biometric feature data never matches said pre-stored valid biometric feature data in terms of said predetermined matching condition.

29. A portable electronic device for use in a user verification system that includes the portable electronic device, adapted to be carried by a user, with a function as a debit card; a data processing device for directly accessing such portable electronic device, temporarily installed therein, so as to function as a debit card terminal for the portable electronic device; and a management device installed in a bank to serve as a host computer that manages the user's bank account from which payment for a purchase made with the portable electronic device, as the debit card, is withdrawn, said managing device accessing said portable electronic device via said data processing device and verifying said user utilizing a personal identification number (PIN), said portable electronic device, comprising:

a biometric feature data register section having pre-stored valid biometric feature data of an authorized user of said portable electronic device;

a transceiving interface for transmitting/receiving data to/from said data processing device;

a biometric feature data verifying section for comparing to-be-verified biometric feature data, which is received from said data processing device via said transceiving interface, with said pre-stored valid biometric feature data;

a secret key register section having a pre-stored valid secret key corresponding to a public key;

a decryption section for decoding encoded data, which has been encoded with said public key, with said valid secret key, said decryption section decoding said encoded data, which has been received from said data processing device via said transceiving interface, into the original to-be-verified biometric feature data,

said biometric feature data verifying section comparing the original to-be-verified biometric feature data with said pre-stored valid biometric feature data;

a clock function section for calculating the current time; and

a time stamp verifying section for comparing a time stamp, if any, attached to the original to-be-verified biometric feature data restored by said decryption section, with said current time, which has been calculated by said clock function section, said time stamp indicating the date and time when said to-be-verified biometric feature data has been extracted,

if it is found, as the comparison result by said biometric feature data verifying section, that said to-be-verified biometric feature data matches said pre-stored valid biometric feature data in terms of a predetermined matching condition, and also if it is found, as the comparison result by said time stamp verifying section, that a difference between said time stamp and said current time falls within a predetermined range, said user being identified as said authorized user of said portable electronic device.

30. The portable electronic device according to claim 29, further comprising:

a user information register section having pre-stored user information about said authorized user of said portable electronic device; and

47

an encryption section for encoding data, which is to be transmitted from said transceiving interface to said data processing device, with said valid secret key,

as a result of comparison by said biometric feature data verifying section and said time stamp verifying section, if said user is identified as said authorized user of said portable electronic device, said encryption section encoding at least one of the following items: said user information; the level of correlation between said to-be-verified biometric feature data and said pre-stored valid biometric feature data, which correlation level is obtained at the comparison; and the date and time of said comparison performed, which is provided by said clock function section, and the encoded item being sent out from said transceiving interface to said data processing device as a verification result.

31. The portable electronic device according to claim 30, wherein if said user is identified as said authorized user of

48

said portable electronic device, as the comparison result by said biometric feature data verifying section and said time stamp verifying section, and also if a message digest, which is obtained by inputting data to be transferred to said portable electronic device to a predetermined one-way function, is attached to the original to-be-verified biometric feature data restored by said decryption section, said encoding section encodes said message digest, and the encoded message digest is then sent out from said transceiving interface to said data processing device as a verification result.

32. The portable electronic device according to claim 30, further including a verification log recording section storing said verification results as a verification log for a predetermined time period.

\* \* \* \* \*

UNITED STATES PATENT AND TRADEMARK OFFICE  
**CERTIFICATE OF CORRECTION**

PATENT NO. : 6,957,339 B2  
APPLICATION NO. : 10/163531  
DATED : October 18, 2005  
INVENTOR(S) : Takashi Shinzaki

Page 1 of 1

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title page, Col. 2  
Primary Examiner  
Delete "Avaz" and insert ---Ayaz--.

Col. 43, line 43, after "(PIN)" delete "." and insert --,--, therefor.

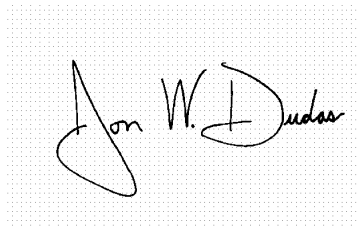
Col. 44, line 30, delete "section." and insert --section--, therefor.

Col. 46, line 20, delete "managina" and insert --managing--, therefor.

Col. 46, line 21, delete "sald" and insert --said--, therefor.

Signed and Sealed this

Twenty-fifth Day of July, 2006

A handwritten signature in black ink on a light gray grid background. The signature reads "Jon W. Dudas" in a cursive style.

JON W. DUDAS  
*Director of the United States Patent and Trademark Office*