



- (51) International Patent Classification:
H04L 29/08 (2006.01) *H04L 29/06* (2006.01)
- (21) International Application Number:
PCT/EP2015/058347
- (22) International Filing Date:
17 April 2015 (17.04.2015)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
14165160.4 17 April 2014 (17.04.2014) EP
- (71) Applicant: **COMPTEL OYJ** [FI/FI]; Salmisaarenaukio 1, FI-00180 Helsinki (FI).
- (72) Inventors: **ENQVIST, Juhana**; Myötätuulenmäki 8 A 22, FI-02330 Espoo (FI). **BERG, Jyrki**; Haarsillantie 4, FI-08700 Lohja (FI).
- (74) Agent: **BOCO IP OY AB**; Itämerenkatu 5, 00180 Helsinki (FI).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM,

AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: METHOD AND SYSTEM FOR USER AUTHENTICATION

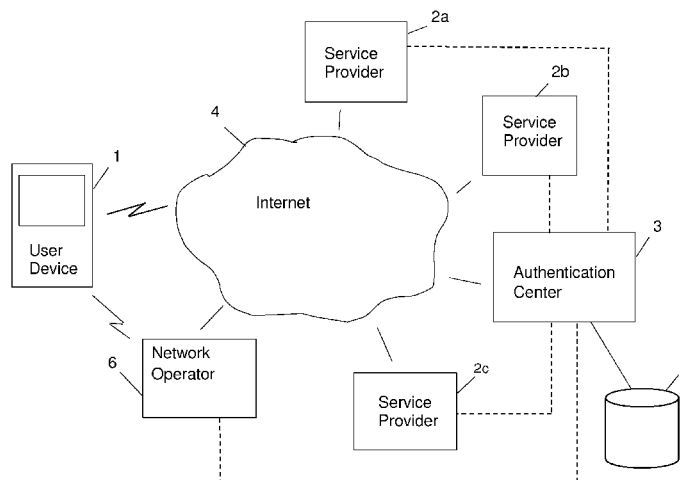
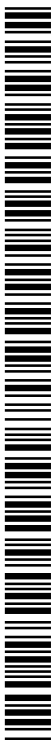


FIG. 1

(57) Abstract: The method of the invention for user authentication in a telecommunication network comprises an authentication server with an authentication service and comprises an initial identity check of a upon a user request. The method is mainly characterized by the following steps as performed by the authentication server, in which steps the authentication server receives a request with user behavior data for further authentication of a user, stores the user behavior data, matches the initial identity with previous information of the user by using an algorithm, performs further checking of the identity of the user if the initial identity of the user and the previous information of the user did not match in a predetermined manner, and reports the result of the further authentication as a reply to the request. The system of the invention has means for performing the steps of the method of the invention. The invention is also concerned with a computer program product that performs the steps of the method of the invention when run in a computer readable media.



METHOD AND SYSTEM FOR USER AUTHENTICATION

TECHNICAL FIELD

The invention is concerned with a method and system for user authentication in a telecommunication network comprising an authentication server with an authentication service. The method involves initial identity check of the user upon a user requesting the user service.

BACKGROUND

Because the Internet is easily accessible to anyone, the use of it involves different kinds of risks. Without any security actions the persons dealt with are not known and personal information might be spread out and made use of.

Examples of internet risks are identity thieves that use information they find online to drain bank account or ruin credit ratings. Generally, information on people in e.g. popular social networking sites might be misused or used in an undesired way for a user even resulting in monetary losses for people.

Authentication and actions for data privacy are therefore used as methods to increase security. The ability to control the information one reveals about oneself over the Internet, and who can access that information, has become a growing concern. Another concern is web sites which collect, store, and possibly share personally identifiable information about users.

Information privacy, or data privacy (or data protection), is the relationship between collection and dissemination of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. Legislation with respect to protection of people's privacy is becoming stricter around the world and along with the risks with e.g. the use of internet, people are getting more and more interested in the protection of their own privacy.

Privacy concerns exist wherever personally identifiable information is collected and stored – in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for data and other privacy issues.

Also authorization (or authorisation), which is the function of specifying access rights to resources, is related to information security and computer security in general and to access control in particular. More formally, "to authorize" is to define access policy. During operation, the system uses the access control rules to decide whether access requests from (authenticated) consumers shall be approved (granted) or disapproved (rejected).

10 Authentication is used as a defense against unauthorized access to a service provided by a service provider or to a communication network. Information is exchanged to verify the identity of a user. The information can be encrypted at both ends. Authentication over a network is an especially important part for enabling security when remote clients are allowed to access network servers.

15 Authentication over a data network, especially a public data network like the Internet, is difficult because the communication between the client and server is susceptible to many different types of attacks.

A basic authentication scheme is for a server to request a password from the client. A password is a secret word or string of characters that is used for user authentication. The client types in the password and sends it to the server. This technique is vulnerable to eavesdroppers who may learn secret information by intercepting communication between the client and the server. Captured information can also be used by a hacker in what is called a "replay attack" to illegally log on to a system.

Another type of attack is a spoofing attack, in which an adversary impersonates the server, so that the client believes that it is communicating with the legitimate server, but instead it is actually communicating with the adversary. Further, in any password based authentication protocol, there exists the possibility that passwords will be weak and even easily guessed such that they are susceptible to dictionary attacks. A dictionary

attack is a brute force attack on a password that is performed by testing a large number of likely passwords.

One solution to avoid attacks with replaying captured reusable passwords is to use one-time passwords (OTP). A one-time password can e.g be one password in a set of passwords, so constructed that it is extremely difficult to calculate the next password in the set or a one-time password system granting the visitor access for a limited time, e.g. one day.

Generally, authentication can be accomplished by verifying one or more of a password or PIN (something that a user knows, i.e. a knowledge factor), biometric information (something that a user is, such as a fingerprint, voiceprint or iris, i.e. an inherence factor), and some identification token, such as a smart-card or mobile phone (something that a user has, i.e. a possession factor). Multi-factor authentication, or two-factor authentication, is an approach to authentication which requires the presentation of two or more of the above mentioned three authentication factors. After presentation, each factor must be validated by the other party for authentication to occur.

As presented above, knowledge factors are the most common form of authentication as a basic authentication scheme.

Biometric authentication is usually unacceptably slow and comparatively expensive when a large number of users are involved. In addition, it is vulnerable to a replay attack. Voice biometrics, however, significantly reduce the risk of a successful replay attack but there is great user resistance to biometric authentication. Users resist having their personal physical characteristics captured and recorded for authentication purposes.

For many biometric identifiers, the actual biometric information is rendered into string or mathematic information. Comparison is therefore made between two data strings, and if there is sufficient commonality a pass is achieved. As it is a matter of choice of how much data to match, and to what degree of accuracy, all biometric devices, therefore, do not provide unambiguous guarantees of identity, but rather probabilities, and all may

provide false positive and negative outputs. A bio-identifier can also be faked. For example, fingerprints can be captured on sticky tape and false gelatin copies made, or simple photos of eye retinas can be presented.

Two-factor authentication is commonly found in electronic computer authentication and seeks to decrease the probability that the requester is presenting false evidence of its identity. However, in reality, there are more variables to consider when establishing the relative assurance of truthfulness in an identity assertion than simply how many "factors" are used.

Other factors under debate are time and location. For example, two users (even perfect twins with cloned knowledge and tokens) cannot be in the same place at the same time.

Existing authentication methodologies involve the explained three types of basic "factors". Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods.

A new category of Two-Factor Authentication, TFA, tools transforms the PC user's mobile phone into a token device using SMS messaging, an interactive telephone call, or via downloadable application to a smartphone. Since the user now communicates over two channels, the mobile phone becomes a two-factor, two-channel authentication mechanism.

According to proponents, Multi-Factor Authentication, MFA, could drastically reduce the incidence of online identity theft, and other online fraud, because the victim's password would no longer be enough to give a thief permanent access to their information. However, many MFA approaches remain vulnerable to man-in-the-browser and man-in-the-middle attacks.

Another drawback of two-factor authentication that are keeping many approaches from becoming widespread is that some consumers have difficulty keeping track of a hardware token or a USB plug. Furthermore, many consumers do not have the technical skills needed to install a client-side software certificate.

As a result, adding a second factor to the authentication process typically leads to significant increase in costs for implementation and maintenance. Most hardware token-based systems are proprietary and charge an annual fee per user. Deployment of hardware tokens is logistically challenging since hardware tokens may get damaged or lost and issuance of tokens in large industries such as banking or even within large enterprises needs to be managed.

In addition to capital expenses (CAPEX), two-factor authentication often carries significant additional operational expense (OPEX). Software certificates and software toolbar approaches have been reported to have the highest support costs.

10 As a result of challenges with cost integration and user acceptance, true two-factor authentication is not yet widespread, although it can be found in certain sectors requiring additional security (e.g. banking, military).

Furthermore, two-factor authentication is not standardized. There are various incompatible implementations of it. Therefore, interoperability is a further issue. There exist many processes and facets to consider in choosing, developing, testing, implementing and maintaining an end-to-end secure identity management system, inclusive of all relevant authentication mechanisms and their technologies.

Pre-authentication methods use call information to verify the calling number and dialed number, respectively, before answering a call. Using callback for added security takes place so that after authentication is complete, the call is hang up and a call back is made, ensuring that the connection is made only with a trusted number.

New hacker techniques are developed and new security vulnerabilities in networks are found every day. Computer-based attacks are likely to continue. For governments, businesses and ordinary individuals, the threat of hacking has created a need for secure information systems and networks which has never been greater.

The above described problems indicate that there is a continuous need to develop new methods and aspects for ensuring secrecy in order to be one step before advanced hackers.

5 The aforementioned two- and multifactor authentication methods are effective in many situations but in certain situations additional layers of security are desired, especially such methods which allow extra costs and complicated signaling to be simultaneously avoided.

The following references are mentioned as prior art.

10 US patent application 2007/0056022 discloses a two-factor authentication method that employs user's Internet Protocol (IP) address associated with a service and/or authentication request and user details of the request with an Internet Service Provider (ISP) account. If there is an indication that the IP address was issued by an ISP to a user matching the user details, the user is authenticated.

15 US patent application 2013/0055368 discloses a multi-factor authentication method using a designated link in a notification to an intended recipient of the message. The designated link includes a unique identifier associated with the message. Upon receiving a request to access the message, the method authenticates the request. The authentication includes verifying whether the request corresponds to the designated link provided in the notification. If the request passes authentication, the method
20 communicates the message.

US patent 8,286,227 presents an enhanced multifactor authentication method by using a first and a second authentication factor for successful verification of the identity.

25 US patent 7,908,645 presents a method for authenticating access requests from user devices, which are identified with fingerprint information and their associated risks of fraud are determined from past experience or with similar devices and from third party information. The determination applies a set of predetermined evaluation rules for authenticating access requests at the server. The evaluation rules provide a score

reflecting the likelihood that a current request is a security problem. Decision tables are used for a hierarchically arranged security evaluation. The tables return a score of "0" in case all evaluated data items are present and "10" if no data item is present, the score of "10" indicating a high likelihood of fraud for the request. In case some data items are present and match but some data items are absent and do not match, the tables invokes further checks. The rules can be based on historical behavior of a particular user by giving a mismatch if the user suddenly changes habits and this might indicate malicious intent. The rules can also restrict logins based on input from 3rd party database or black-listed IP addresses.

10 Instead of rule-based behavioural analysis, machine-learning algorithms can be used for determining the behaviour. The algorithms automatically learn the behavioural patterns of each individual user, and any anomalies in behaviour can be scored. The algorithms can automatically adjust the expected behaviour according to the changes in user behaviour, and use further authentication steps, like two-factor authentication, to
15 strengthen the learning performance. The algorithms can also predict unforeseen behavioural attribute combinations as part of normal behaviour unlike standard rule-based calculations, and also detect minute changes in the patterns as abnormal behaviour.

The above method, however, requires certain pre-defined information for the algorithm
20 to work properly.

The object of the method is a flexible two-factor or multi-factor authentication method that works in all situations.

SUMMARY OF THE INVENTION

25 The method and system of the invention has the characteristics of the main claims.

The method of the invention for user authentication in a telecommunication network comprises an authentication server with an authentication service and comprises an initial identity check of a upon a user request. The method is mainly characterized by the following steps as performed by the authentication server, in which steps the authentication server receives a request with user behavior data for further authentication of a user, stores the user behavior data, matches the initial identity with previous information of the user by using an algorithm, performs further checking of the identity of the user if the initial identity of the user and the previous information of the user did not match in a predetermined manner, and reports the result of the further authentication as a reply to the request.

The system of the invention has means for performing the steps of the method of the invention.

The invention is also concerned with a computer program product that performs the steps of the method of the invention when run in a computer readable media.

The preferable embodiments have the characteristics of the sub claims.

Different score values can be defined to represent different authentication levels and a threshold score value selected for the user to represent an authentication level to pass in the matching, whereby the matching is performed by calculating a score value for the identity match. The score value is calculated on the basis of the number of parameters matching previous behavior in relation to the number of parameters matching or mismatching previous behavior. Deviations of one or more individual parameters can be taken into consideration in the calculation of the score value. The threshold score value represents an authentication level on the basis of how the service connected to is used. The threshold score value can be set by the service provider, a network operator providing the network connections for the user or the user himself.

The previous information being based on previous behavior patterns of a user received and collected from one or more service providers in connection with the user's use of services provided by these one or more service providers.

5 The request for further authentication can be a continuous feed comprising information of the behaviour of the user requesting the service to be sent during the whole further authentication session. The user can request updating of the score value on the basis of updated user behavior information from the continuous feed. The score value for the user can be updated during one session of further authentication on the basis of updated user behavior information from the continuous feed.

10 The parameters are preferably dynamically selected for the matching on the basis of availability.

The authenticating can be combined with authorization of the user to the service requested by specifying different access rights to different resources and services in the form of different authentication levels to pass defined by different threshold score
15 values.

The result of the further authentication can be sent as a reply to the request. The reply is to be meant as an answer or a response to the sender of the request optionally by using a reply function for the sending. In the preferable embodiments, the telecommunication network further comprises one or more service providers, whereby
20 the request for further authentication is received by a service provider and the result of the matching is sent to the same service provider.

The authentication server is connected to a database with user profiles for each user and structured information of the use of services of users with relating data of the user and his way of using services, the information including data from use of services
25 provided by different service providers.

In the database, the structured information comprises data categorized by means of parameters and sub-parameters in manageable objects. A parameter describes different aspects of the service used, such as user device used, user device location,

online times, type of visited sites, shopping habits, type and characteristics of products purchased, and/or amount of money used. Each user profile comprises one or more authentication levels to pass consisting of a threshold score value to reach for a given service.

- 5 The algorithm for calculating the score value is based on the number of matching parameters or sub-parameters versus mismatching parameters or sub-parameters or a percentage of matching parameters or sub-parameters.

With the invention, more precise user identification can be made without other costly identification methods. With this approach, the usage of such other identification
10 methods can significantly be diminished to a lot smaller number. The invention can also be designed to provide different security criteria for different services. For example participating in a forum discussion needs less security certainty compared to e.g. banking services.

In further embodiments of the invention, more secure authentication can be made, for
15 example for users performing online shopping. For example when connecting a user to an online shopping site, a certain authentication level usually needs to be fulfilled. But if the shopping basket of user grows over a certain limit, the security level for the user can be increased in order to launch additional verifications before the purchase can be finalized.

20 In still further embodiments of the invention, the invention further collects information of shopping habits, objects of interests, parameters of objects purchased (like price, colour, technical data, favorite manufacturers and vendors. The invention enables following consumer behavior from more than one vendor since it allows combining information collected from several vendors.

25 Information of specific user profile behavior can be collected from multiple sources (such as service providers, the network operator and other sources) for calculating a score value to pass in the matching step, which score value is calculated based on parameters describing the user's ways of using services.

Previous information about e.g. the used device location for service usage, shopping habits, online times, devices used, type of sites used for services and/or type of products purchased can be taken into account when calculating the score value. Also sub-parameters for those products can be collected for calculating the score value. One such sub-parameter can, for example consist of typical characteristics of certain products purchased by a certain user. A user might for instance usually buy his electrical devices in black. If he then suddenly buys a pink device, the behavior will create an anomaly in the user profile and might launch additional security checks. Another sub-parameter can e.g. consist of the exact site address used for a given type of service.

Behaviour information to be collected for the user profile can include for example usual locations for use of the user devices (e.g. home, office, often visited places), the type and brand of devices used (mobile phone, computer, tablet,...) , location and/or time information (separately or combined), normal online times, normal home PC use times, surfing habits, time of day, purchase trends of purchased products (books, devices, clothes,...) parameters for a typical purchase (price range, colours, quality, manufacturers, product categories (detective stories, love stories, etc)...), purchase habits (buying just a few things at a time vs buying multiple items, the information of how often a service is used, how the services are used, spending habits/(one time visit, typical time and day of usage), where the service usually is used. Further information might relate to the time spent with the service/location/device, social behavior.

As consumer behavior can be followed over longer time periods, the normal behavior of a consumer can be noted. A user might e.g. be impulsive, visit a web page several times before a purchase decision, compare prices and/or behave differently with different types of products.

All this information can be used to detect unusual behavior and to estimate demographics (age, gender, education level, etc), interests and wrongful use of the device/services.

Also the provider of the Internet connection (the network operator) can be involved by giving information to the authentication service of the invention. One parameter to be checked optionally is the user's IP address from which the service provider received the request for service usage. The provider of the internet connection is aware of the user's real IP address and if these two do not match there is probably a man-in-the middle attack and the service can be denied. The network operator can also tell the actual user behavior, which information contributes in analyzing whether the behaviour is normal or whether there is a reason to suspect misuse.

This invention makes it possible for service providers to adjust the security requirements for their services, but it also creates the same possibility for the network operator and even the user. With multiple security requirements, the system needs to fulfill them all in the most secure solution before it can grant access. For example with extremely security sensitive information, the user might define his/her security requirements a lot higher than the service provider does and in that way demand a stronger authentication level for all of his/her actions.

In addition to be able to adjust his security or authentication level, the user can also determine his data privacy with this invention. The user can e.g. determine his settings to define the data that is allowed to be collected and analysed by the service providers. For example location and behavior information can be sensitive information for some people which they do not want to share with anyone. In such a case and for those users there might be additional authentication steps in the method of the invention.

Single sign-on (SSO) is a session/user authentication process that permits a user to enter a user ID and password in order to access multiple applications. It is a method used for access control of multiple related, but independent software systems. The process authenticates the users for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session so that a user only has to log in once to gain access to all systems without being prompted to log in again at each of them.

In the invention, Single sign-on (SSO) can also be used as a portal to different Internet locations so that when the user logs in to the authentication service of the invention, the logging information can be used to log in to the web page of the service providers. This takes place so that along with the logging to the service, the service providers receives
5 the information of the user's identity since the user data is connected to the service provider's system. In this stage, the continuous follow-up of the user behaviour performed influences on the score level of the identification. At the log-in, the user gets a certain score value, which is forwarded to the service provider. As information is collected from each action of the user, the reliability of the identity can be more reliably
10 evaluated the more actions there have been. Thus, it has to be noted that not only signings are followed, but also every user action after it is followed.

The authentication method of the invention can also be connected to authorization by specifying different access rights to different resources and services. For example, if a user just requests to read the information of his purchase history or have his saldo
15 information, or even make some cheap purchases, a lower score or fewer additional authentication steps can be required than for purchasing products over a certain price limit or number. In other words, a part of the services might be accessed with lower security requirements. Next time, however, the score might have changed for this user, since more information has been collected from the user's service use. The score might
20 either become lower or higher. If a score value has become low enough, additional authentication might be required for the access of a service even for normal user behaviour. If, in contrary, the score value has become high enough, the user can be granted more rights within the service without additional authentication.

This method can also be used to screen possible spam e-mails, or other misuse or
25 misdirection with electrical communication. Also network operators can use this kind of a system to spot possible misuse of mobile devices, like stolen or lost phones from radically changed user behavior. In these cases, the mobile operator could actually instruct the device holder to visit a store with the device or shut down the connection.

This method can also be used for verifying a user that uses public computers and for
30 collecting information of e.g. the areas, where the users use computers, the information

they provide, where they browse, and what they do in the network. These features can be used to check the profile in order to create additional guarantee for that the user to be authenticated is the correct person to use a certain account.

5 Therefore, our invention performs dynamic user identity analysis on the basis of different parameters available since there are no rigid rules for how the score value is calculated. The invention can use new information when it appears without the need to change the algorithm used in the method of the invention.

10 The invention can also take missing information into account as a parameter in the authentication. If information that normally is available is suddenly missing it might indicate misuse. Or vice versa, if a user normally does not want to share certain information it is suspect if the information suddenly is available.

15 The user might have certain standard privacy settings, which prohibits the sharing of certain information. If such information suddenly is present, there is a possible fraud going on. Different service providers might, however, have different ways of acting and the analysis can therefore consider also what limitations are possible with different service providers.

20 The service providers can from case to case decide themselves how strictly the score value is used but the user himself/herself can influence the process of authentication. The user can also link different services together by telling what service he/she uses and with what identification and thus make the linking easier. The user can set different authentication levels for different services or use only one general level or both.

25 The invention is preferably implemented as an independent server service in order to help service providers to authenticate their users. In this way, information from multiple sources can be used without the service providers giving any information of the users to each other, providing information only to the service, and for the sole reason to help each other authenticate users. The service providers using the service give similar information to the service and each of them gain of a bigger database compared to if they used only own information. The service providers do not share information directly with each other since the service only sends out the score value but no user data itself.

In the following, the invention is described more in detail to illustrate the invention by means of an embodiment of the invention by referring to figures. The detailed description is not meant to restrict the invention to the details of the examples described.

5

FIGURES

Figure 1 is a view of a network, wherein the invention can be implemented.

10 Figure 2 is a sequence diagram of an example embodiment of the method of the invention.

Figure 3 is an example of a database structure useful in an embodiment of the invention

15 Figure 4 is an example of a flow scheme, which presents the part of the invention calculating a score value.

Figure 5 is an other example of a flow scheme, which presents the part of the invention calculating a score value.

20 DETAILED DESCRIPTION

Figure 1 is an example view of a telecommunication network, wherein the invention can be implemented. The telecommunication network comprises a user device 1, service providers 2a, 2b, 2c providing services for users and an authentication server 3 with an authentication service and a network operator 6. The authentication server 3 provides
25 the authentication service to the service providers 2a, 2b, 2c. All these entities mentioned are connected to the Internet 4 by means of a wired or wireless connection. The authentication service can, however, also be implemented to work through a telephone network, such as the Global System for Mobile Communications (GSM).

With service provider (SP) is here meant a company that provides application services to users and companies through the Internet referring to a third party or outsourced supplier. The network operator 6 can be a mobile network operator or MNO, also known as a wireless service provider, being a provider of wireless communications services that owns or controls all the elements necessary to sell and deliver services to an end user including e.g. radio spectrum allocation, and wireless network infrastructures. It can also be an Internet provider. The dotted line drawn between the authentication server 3 and the network operator 6 shows that the network operator 6 communicates with the authentication server 3, e.g. when performing additional authentication by checking an IP address of a user. The network operator can also be any other type of communications service provider (landline or satellite for example). In some occasions, the network operator can also be seen as a service provider in this invention.

Dotted lines are drawn between the authentication server 3 and the service providers 2a, 2b, 2c to show that the service providers 2a, 2b, 2c communicate with the authentication server 3 and provides information to the authentication server 3 even if the communication takes place over the Internet. Of privacy reasons, the service providers 2a, 2b, 2c do not share user information and the authentication server 3 does not send user information to the service providers. In reality, there are usually much more user devices and service providers in the system of the invention but only one user device 1 and only three service providers 2a, 2b, 2c are indicated for illustrative purposes.

The authentication server 3 systematically collect information of different users into a database 5, in the register of which each user is connected to formatted information parameters describing the use of services of this particular user.

Figure 2 is a sequence diagram of an example embodiment of the method of the invention.

It is assumed that several service providers, (2a, 2b and 2c in Figure 1, cooperate in sharing information with the authentication server and use its authentication service.

These service providers provide services for users with user devices that can communicate over a public network, like the Internet, with the service providers.

- 5 For illustrative purposes, only one user device is discussed in Figure 2. In the example of Figure 2, it is assumed that the user uses the services of all these three service providers by using his/her user device.

The communication between the user device and service provider 2a back is referred to as signal 1 in Figure 2. The service provider 2a might use the same authentication
10 service for an initial identity check. Before starting use of the authentication service of authentication server 3, the service provider probably uses other authentication services for authenticating its users. To be able to fully make use of the completed authentication check provided by authentication server 3, the authentication server should have
15 information of previous user behavior. The service provider might have submitted this information to the authentication in advance or might submit it separately anytime. If the service provider already is a user of the authentication service of the authentication server 3, information of user behavior is advantageously submitted to the authentication server in connection with each authentication of the user after or upon the use of the
20 service provided by the service provider or in connection with the use of the authentication service.

Thus, in Figure 2, the service provider 2a informs the authentication server with signal 2 upon each service use of the user and gives data about how the user used the service including e.g. information of the device used by the user, the location of the device used
25 for the service, the duration of the on-line time, the visited site, the purchased product or service, and the price of the product or service.

The corresponding communication between the user device and service provider 2b is referred to as signals 3 and 4 in Figure 2 and that between the service provider 2c and the authentication server is referred to as signals 5 and 6 in Figure 2.

In step 7, the authentication server stores the user information received in signals 2, 4 and 6 (or information that is separately sent) in a categorized and formatted way into a database. In the database, each user has a user profile with relating data of the user and his way of using services. An example of a way in which the parameters of the user information might be stored and categorized is shown as an example in Figure 3.

The authentication server also stores one or more threshold values for this user to be used as authentication levels to pass. The threshold value can be defined e.g. by the user or the service provider. There might be different threshold values for different services and different products. The threshold value might depend on e.g. the price of the product, a limit for one-time purchases, type of service, the number of products to be purchased or any desired value on a certain parameter or sub-parameter. In the database, the services are categorized by means of parameters and sub-parameters in manageable objects for example in a way described in Figure 3.

Next, it is assumed that the user now request a service from service provider 2a in signal 8.

For authentication of the user, the service provider first performs an initial identity check of the user. This might take place by using the same authentication server 3 or in some other way. Therefore, this step is just indicated as step 9 in the Figure.

In signal 10, the service provider 2a requests the authentication server to perform a further authentication check. In this signal, information of the service requested by the user is informed as well. The information comprises detailed data in the form of parameters for e.g. the device used, its location, the visited site, the purchased product or service, and the price of the product or service. The authentication server categorizes and stores this new data in the database as in step 7 (not shown).

An additional authentication check is performed by the authentication server 3 by matching the initial identity with a user profile. In the matching, available parameters and sub-parameters are matched against each other and depending on how many parameters and sub-parameters matched (and/or mismatched), a score value for

example between 1 and 10 is calculated, 1 meaning e.g. the lowest degree of match and 10 the highest. This score value defines the degree of matching, i.e. the correspondence between current (newly received) parameters and previous parameters of the user.

5 Different algorithms can be constructed for the matching. An algorithm might e.g. simply be based on the number of matching parameters or sub-parameters versus mismatching parameters or sub-parameters or a percentage of matching parameters or sub-parameters. More weight can be given for parameters or sub-parameters considered important in the calculation of the score. Furthermore, parameters or sub-
10 parameters that are considered important might be defined on user basis, for example because some users e.g. show more variation in their behavior. A detailed example of a matching base is explained in connection with Figure 3, wherein it is explained that the data received is categorized by a hierarchic list of parameters and sub-parameters.

An authentication level was earlier (in this example in step 7) defined and stored in the
15 form of a threshold score value to pass. This threshold score value can be different for different services and different users. The threshold score value can also be defined by the user or the service provider or them both.

For example, if a score value of 8 is required but the calculation in the matching step ended up to a score value of only 7, the system might require further identity check or it
20 might just deny the service for the user directly, if e.g. the score value is far from the accepted authentication level. Thus, there might be conditions for the score value to be close enough to the score value if the authentication level (describing degree of security) so that the system would allow further checks or alternatively, failed checks lead to some number of further checks.

25 In the example of Figure 2, it is assumed that the score value calculated in step 11 did not pass the authentication level and therefore a further identity check is performed in signals 12 and 13. This is performed in Figure 2 by checking the Internet Protocol, IP, address of the user device from the Internet provider (being the network operator).

Optionally, for example a Short Message Service (SMS) check from the MNO (being the network operator for wireless services) can be made after the IP check if the IP check failed (not shown) or a check by Interactive Voice Response, and/or IVR, verification. The SMS check or IVR can also be an alternative to the IP check. Further alternatives or additional checks (not shown in Figure 2) include the location check, asking security questions or other additional checking methods.

In Figure 2, even this check failed, which was stated upon matching the requesting user's IP address with that of the user identity in step 14. Therefore, the service was denied from the user in step 14.

10 Naturally, the system can be configured to allow further identity checks in different ways.

Figure 3 is an example of a database structure useful in an embodiment of the invention.

15 In the database, the use of the services are categorized by means of parameters and sub-parameters in manageable objects for example in a way described in Figure 3.

One parameter might consist of a description of different aspects of using a series by successive numbers being a form of manageable objects. These might consist of e.g. 1) the device used for the service, 2) the device location for the use of the service, 3) the on-line time, 4) the time of the day, 5) the amount of money to be used/been used, 6) a 20 1st category of visited site, 7) a 1st category of purchased product/service, 8) a 2nd category of visited site, and 9) a 2nd category of purchased product/service.

The sub-parameters for these objects describing e.g. values for the parameters or more detailed information are described by sub-objects like e.g. those used by user I, i.e. 1.1) iPhone, 2.1.) home address, 3.1.) 1h, 4.1.) 6 p.m., 5.1.) 50Eur, 6.1.) Music store, 7.1.) 25 CDs, 8.1.) news subscription, and 9.1.) Book, or by user II 1.2) Samsung Galaxy 2.2.) work address, 3.2.) 0,5h, 4.2.) 1 p.m., 5.2.) 80 Eur, 6.2.) Game playing site, 7.2.) Tickets, 8.2.) Ticket store, and 9.2.) Electronics for music, or by user III II 1.3) HTC

model X 2.3.) on the road, 3.3.) 15 min, 4.3.) 10 a.m., 5.3.) 200 Eur, 6.3.) Music site, 7.3.) Sport items, 8.3.) Social media site, and 9.3.) Sport socks. Optionally, these sub-parameters can be further described by different characteristics for type of music, colour of products, etc. by the means of manageable objects in the form of 1.1.1, 1.1.2 and so
5 on.

Figure 4 is a first example of an overall flow scheme of the part of the invention from the view of the authentication server for calculating a score value and using the score value for authentication purposes.

In step 1 of figure 4, the authentication server receives a request from a service provider
10 to perform a further authentication check on an initial identity of a user. This request comprises information of the service and the parameters and sub-parameters of the service requested by the user.

The information in the request, which is read in step 2, comprises detailed data in the form of parameters and sub-parameters for e.g. the used device, the location of the
15 used device, the visited site, the purchased product or service, and the price of the product or service. Preferably, the authentication server also notes the time of the day for the request.

The parameters and sub-parameters are preprocessed in a proper format so that they could be easily handled. Therefore, the authentication server categorizes the
20 parameters and sub-parameters in the form of manageable objects having a proper format and stores the new data of the objects in the database in step 3.

The further authentication check is performed by the authentication server in step 4 by matching the current objects with previous objects collected for the user in the database.

25 A score value is calculated in step 5, which is based on matching the current objects with corresponding objects in the user profile and identifying lack or correspondence between current objects and existing objects in the user profile, including noting of new

objects. Depending on how many parameters and sub-parameters matched (or mismatched), a given score value is then obtained. The extent of information in the user profile is not only dependent on how many recorded user actions there have been in order to collect as much information as possible but it depends on the user's data
5 privacy settings with respect to what information is allowed to be collected and stored.

In step 6, the obtained core value is compared to a threshold score value, which defines the authentication level to pass for verification.

If the obtained score value to be compared is higher than or equal to the threshold score value, which is stated in step 7, the identity check is passed and it is considered
10 in step 8 whether a random check for additional ID verification should be performed, which is an option in this example embodiment.

If the program of the service decides that a random check, indeed, is to be performed, then an additional ID verification is performed in step 9. This additional ID verification might consist of only one or several layers of additional checks (with different methods),
15 either each of them to be passed or then a check of a further layer is performed only if the foregoing check was failed.

This additional Identity, ID, verification in step 9 is also performed if the authentication level was not passed in step 7.

If the additional ID verification/ additional ID verifications of step 9 is passed in step 10
20 of figure 4, then the service provider is informed in step 11 of the passed check.

Step 11 is also performed if it is stated in step 8 by the program that that no random check need to be performed.

If again the additional ID verification/ additional ID verifications of step 9 are not passed, in step 10 of figure 4, then the service provider is informed in step 12 of the failed check.

After step 11 or step 12, the data of the checking procedure is saved by the authentication server for analytics and for collecting information for following authorisation checks.

Figure 5 is another example of an overall flow scheme of the part of the invention from the view of the authentication server for calculating a score value and using the score value for both authentication and authorization purposes.

In step 1 of Figure 5, the authentication server receives an authentication request from a service provider to perform a further authentication check on an initial identity of a user. This request comprises a feed of information of the service and the parameters of the service requested by the user. In addition, the authentication server receives in this embodiment a feed comprising user behavior information either as a one-time feed for this session or as a continuous feed (during the whole session) with new user behavior information, which the service provider collects during the authentication session for this service request for the continuous feed. Fresh user behavior information might e.g. be possible to collect if the user during the authentication session for this requested service meanwhile uses other services or is searching and/or clicking for information.

The parameters in the feed, which are read and extracted in step 2, comprises detailed data in the form of parameters and sub-parameters for e.g. the used device, the location of the used device, the visited site, the purchased product or service, and the price of the product or service. Preferably, the authentication server also notes the time of the day for the request.

The parameters and sub-parameters are preprocessed in a proper format so that they could be easily handled. For this purpose, the authentication server categorizes the parameters and sub-parameters in the form of manageable objects having a proper format and stores the new data of the objects in the database in step 3.

The further authentication check is performed by the authentication server in step 4 by matching the current objects with previous objects collected for the user in the database.

A score value is calculated in step 5, which is based on matching the current objects with corresponding objects in the user profile and identifying lack or correspondence between current objects and existing objects in the user profile, including noting of new objects. Depending on how many parameters and sub-parameters matched (or mismatched), a given score value is obtained. The extent of information in the user profile is not only dependent on how many recorded user actions there have been in order to collect as much information as possible but also depend on the user's data privacy settings with respect to what information is allowed to be available for the analysis and the matching.

10 In step 6, the obtained core value is compared to a threshold score value, which defines an authentication level to pass for verification.

Different threshold score values to use have been defined in advance as was presented in connection with Figure 2. The threshold score value to be used in a certain situation does not only depend on a certain user since it might depend on the service to be used, and the parameters and sub-parameters of the requested service. Also different threshold score values might be required for different parts of the service and for different authorization levels. A higher authorization level in this context means more extensive rights to use the different parts of the service. Therefore, there can be such rules implemented by the authentication server that the authorization level is raised along with a higher score value reached and lowered or dropped along with a lowered score value.

In some cases, a part of the requested service or services does not require a very high authentication level and are allowed to be used with a lower score value compared to another part, for the use of which higher security is required. In such case, the service provider either requires a higher score value or additional identity check steps, such as an IP address check or SMS messaging.

An example might be a service providing a discussion forum and both cheap and expensive products. The service provider for such a service might require higher

authentication levels (and consequently higher score values) the more money is needed for the use of the actual part of service.

Another example is online games. Playing a game might require a low authentication level, but purchasing something with real money from the in-game store would require a higher authentication level.

If the obtained score value to be compared was higher than or equal to the threshold score value to be reached in step 7, the identity check is passed and the service provider is informed in step 8 of the passed check.

An additional Identity, ID, verification in step 9 might be performed if the authentication level was not passed in step 7. This additional ID verification might consist of only one or then several layers of additional checks (with different methods), either each of them to be passed or then a check of a further layer is performed only if the foregoing check was failed.

If the additional ID verification/ additional ID verifications of step 9 was passed in step 10 of Figure 5, then the service provider is informed in step 8 of the passed check.

If again the additional ID verification/additional ID verifications of step 9 was not passed in step 10 of figure 4, then the service provider is informed in step 11 of the failed check.

As an alternative to immediately proceed to step 11 after a “no” in step 10, the authentication center might try to update the score value by following user behavior information in the continuous feed in step 12 and then proceed to step 2 and repeat the sequence of steps 2 – 8 maybe via steps 9 and 10 or by ending up to step 11.

As an other alternative to immediately proceed to step 11 after a “no” in step 10, the authentication center might try to update the score value if a request from the user for a higher authorization level or a higher score has been received, whereby the authentication server returns to step 1 and performs steps 2 – 7 and maybe 8 or 11

again (maybe via steps 9 and 10) in such a way that in step 6, the current feed information that is compared with previously gained information stored in user profile.

After step 8 or step 11, the data of the checking procedure is saved by the authentication server for analysis and for collecting information for following authentication checks.

It is pointed out that the above embodiments are examples only and are not meant to be restrictive for the implementation of the invention.

An additional feature to be implemented in the invention is that predictive algorithms can e.g. be used to assume user behavior in advance and to predict changes in user behavior and make use of the predictions in the matching step.

CLAIMS

1. Method of user authentication in a telecommunication network comprising an authentication server with an authentication service, the method comprising the step of an initial identity check of a upon a user request, c h a r a c t e r i z e d by the following
- 5 steps as performed by the authentication server:
- a) receiving a request with user behavior data for further authentication of a user,
 - b) storing the user behavior data,
 - c) matching the initial identity with previous information of the user by using an algorithm,
 - 10 d) performing further checking of the identity of the user if the initial identity of the user and the previous information of the user did not match in a predetermined manner, and
 - e) reporting the result of the further authentication as a reply to the request.
- 15 2. Method of claim 1, c h a r a c t e r i z e d by defining different score values to represent different authentication levels and selecting a threshold score value for the user to represent an authentication level to pass in the matching of step c), whereby the matching is performed by calculating a score value for the identity match.
- 20 3. Method of claim 1 or 2, c h a r a c t e r i z e d in that the telecommunication network further comprises one or more service providers, whereby the request for further authentication is received by a service provider and the result of the matching is sent to the same service provider.
- 25 4. Method of any combination of claims 1 - 3, c h a r a c t e r i z e d in that the previous information being based on previous behavior patterns of a user received and collected from one or more service providers in connection with the user's use of services provided by these one or more service providers.
- 30 5. Method of claim any combination of claims 1 - 4, c h a r a c t e r i z e d in that the request for further authentication is a continuous feed comprising information of the

behaviour of the user requesting the service to be sent during the whole further authentication session.

- 5 6. Method of claim 5, c h a r a c t e r i z e d in that user request is a request for updating the score value on the basis of updated user behavior information from the continuous feed.
- 10 7. Method of claim 5 or 6, c h a r a c t e r i z e d by updating the score value for the user during one session of further authentication on the basis of updated user behavior information from the continuous feed.
- 15 8. Method of any combination of claims 1 - 7, c h a r a c t e r i z e d in that the previous information consists of one or more parameters selected from user device used, user device location, online times, type of visited sites, shopping habits, type and characteristics of products purchased, amount of money used.
- 20 9. Method of claim 8, c h a r a c t e r i z e d in that the parameters are dynamically selected for the matching on the basis of availability.
- 25 10. Method of claim 8 or 9, c h a r a c t e r i z e d in that the score value is calculated on the basis of the number of parameters matching previous behavior in relation to the number of parameters matching or mismatching previous behavior.
- 30 11. Method of any combination of claims 8 - 10, c h a r a c t e r i z e d in that deviations of one or more individual parameters are taken into consideration in the calculation of the score value.
12. Method of any combination of claims 2 - 11, c h a r a c t e r i z e d by selecting the threshold score value representing an authentication level on the basis of how the service connected to is used.
13. Method of claim any combination of claims 3 - 12, c h a r a c t e r i z e d in that the threshold score value representing an authentication level is set by the service

provider, a network operator providing the network connections for the user or the user himself.

- 5 14. Method of any combination of claims 1 - 13, c h a r a c t e r i z e d in that the authenticating is combined with authorization of the user to the service requested by specifying different access rights to different resources and services in the form of different authentication levels to pass defined by different threshold score values.
- 10 15. Method of any combination of claims 1 - 14, c h a r a c t e r i z e d in that the further checking is performed by comparing the Internet Protocol, IP, address of the user received from the user's network operator with the Internet Protocol IP address received from the service provider, by means of security questions, Short Message Service, SMS, verification or by Interactive Voice Response, and/or IVR, verification.
- 15 16. Method of any combination of claims 1 - 15, c h a r a c t e r i z e d in that in case the further identity check failed, a security reaction follows consisting in denying connection between the user device and the service provided by the service provider.
- 20 17. System for user authentication in a telecommunication network comprising an authentication server with an authentication service, c h a r a c t e r i z e d by the authentication server having means for
- 25 a) receiving a request with user behavior data for further authentication of a user,
b) storing the user behavior data,
c) matching an initial identity of the user with previous information of the user by using an algorithm
d) performing further checking of the identity of the user if the initial identity of the user and the previous information of the user did not match in a predetermined
30 manner, and
e) reporting the result of the further authentication as a reply to the request.

18. System of claim 17, characterized in that the telecommunication network further comprises one or more service providers, whereby the authentication server having means for receiving the request for further authentication from a service provider and for sending the result of the matching to the same service provider.
- 5
19. System of claim 17 or 18, further characterized in that the authentication server being connected to a database with user profiles for each user and structured information of the use of services of users with relating data of the user and his way of using services, the information including data from use of services
- 10 provided by different service providers.
20. System of claim 19, further characterized in that in the database, the structured information comprises data categorized by means of parameters and sub-parameters in manageable objects.
- 15
21. System of claim 20, further characterized in that a parameter describes different aspects of the service used, such as user device used, user device location, online times, type of visited sites, shopping habits, type and characteristics of products purchased, and/or amount of money used.
- 20
22. System of claim 20 or 21, further characterized in that the algorithm for calculating the score value is based on the number of matching parameters or sub-parameters versus mismatching parameters or sub-parameters or a percentage of matching parameters or sub-parameters.
- 25
23. System of any combination of claims 17 - 22, further characterized in that each user profile comprises one or more authentication levels to pass consisting of a threshold score value to reach for a given service.
- 30
24. Computer program product providing an authentication service and performing the following steps when run in a computer readable media,

- a) receiving a request for further authentication containing user behavior data,
- b) storing the user behavior data,
- c) matching an initial identity of the user read from the request with previous information of the user by using an algorithm,
- 5 d) performing further checking of the identity of the user if the initial identity of the user and the previous information does not match in a predefined manner, and
- e) reporting the result of the further authentication as a reply to the request.

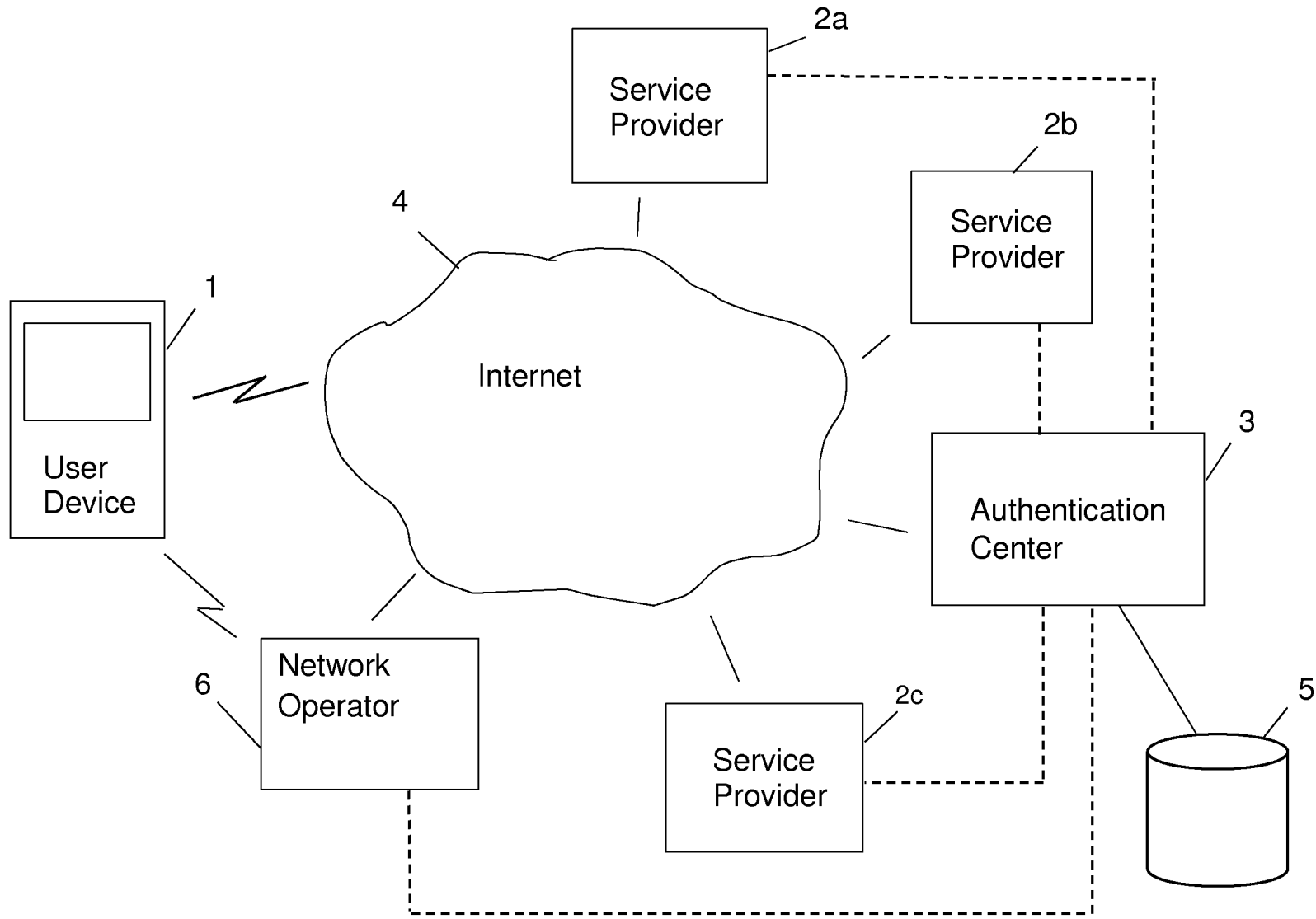


FIG. 1

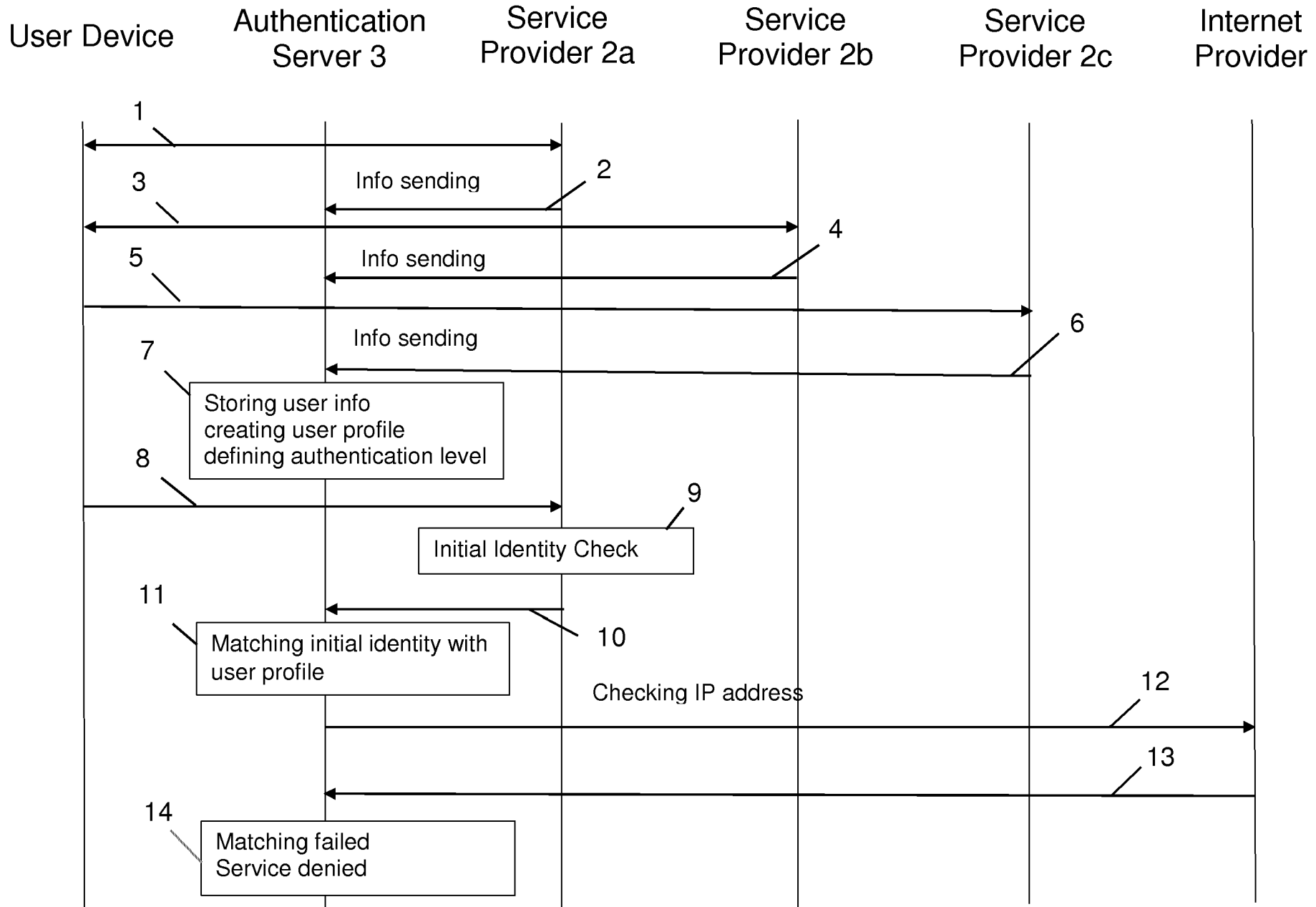


FIG. 2

| Object classification | Parameter | Profile USER1 Name Contact info | Profile USER2 Name Contact info | Profile USER3 Name Contact info |
|-----------------------|-----------------------------------|---------------------------------------|---------------------------------------|--|
| 1 | Device | 1.1. iPhone | 1.2. Samsung Galaxy | 1.3. HTC Model X |
| 2 | Device location for service use | 2.1. Home address | 2.2. Work address | 2.3. On the road (within certain area) |
| 3 | One-time duration | 3.1. 1h | 3.2. 0,5h | 3.3. 15 min |
| 4 | Time of day | 4.1. 6 p.m. | 4.2. 1 p.m. | 4.3. 10 a.m. |
| 5 | amount of money used | 5.1. 50€ | 5.2. 80€ | 5.3. 200€ |
| 6 | 1st category of visited site | 6.1. Music store | 6.2. Game playing site | 6.3. Sport items |
| 7 | 1st category of purchased product | 7.1. CDs | 7.2. Tickets | 7.3. Sport clothes |
| 8 | 2nd category of visited site | 8.1. news subscription | 8.2. Ticket store | 8.3. Social media site |
| 9 | 2nd category of purchased product | 9.1. Book | 9.2. Electronics for music | 9.3. Sport socks |

FIG. 3

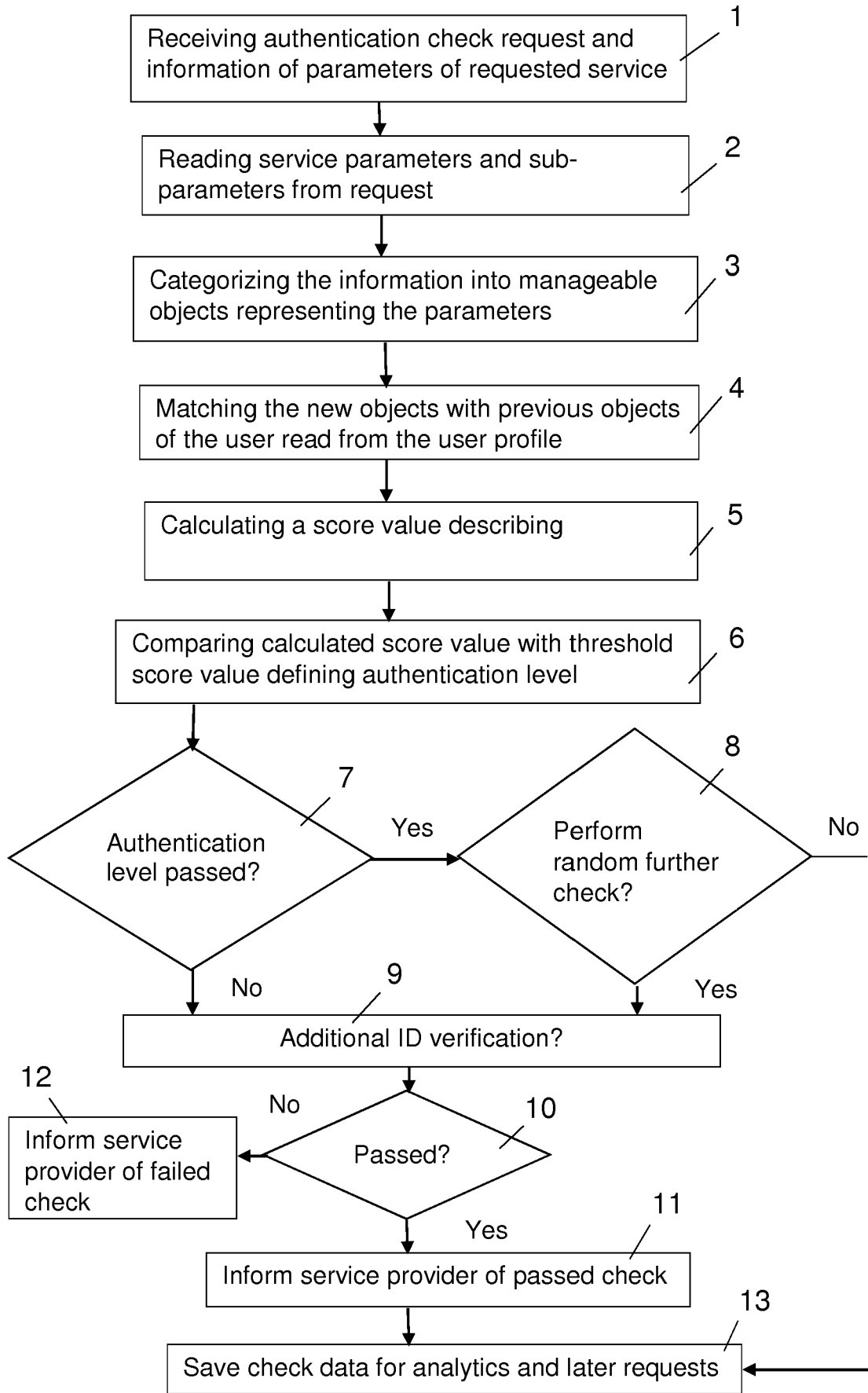


FIG. 4

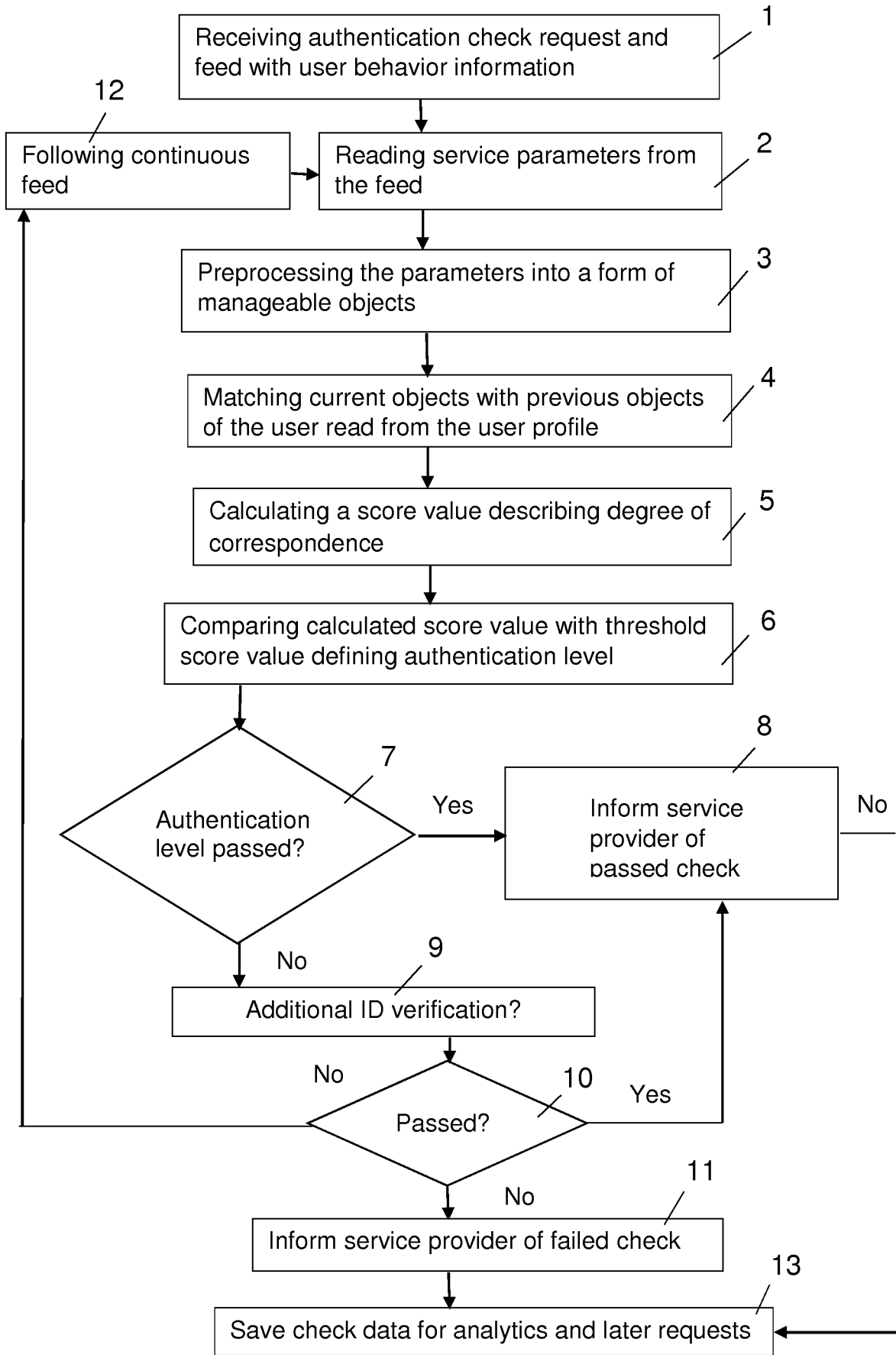


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/058347

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/08 H04L29/06
ADD.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
H04L
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

| C. DOCUMENTS CONSIDERED TO BE RELEVANT | | |
|--|--|-----------------------|
| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
| X | US 2011/016534 A1 (JAKOBSSON BJORN MARKUS [US] ET AL) 20 January 2011 (2011-01-20) figures 1B,3,4 paragraph [0007] - paragraph [0028] paragraph [0057] - paragraph [0067] paragraphs [0075], [0076] ----- | 1-24 |
| X | WO 2011/001026 A1 (ELISA OYJ [FI]; MAANOJA MARKUS [FI]; TIKKANEN KIM [FI]; KURVINEN ESKO) 6 January 2011 (2011-01-06) figures 1,5 page 3, line 12 - line 15 page 7 - page 11 ----- -/-- | 1-24 |

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier application or patent but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

| | |
|--|--|
| Date of the actual completion of the international search 2 July 2015 | Date of mailing of the international search report 09/07/2015 |
| Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016 | Authorized officer Kraska, Nora |

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2015/058347

| C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT | | |
|--|---|-----------------------|
| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
| A | US 2007/236330 A1 (CHO SUNGZOOM [KR] ET AL) 11 October 2007 (2007-10-11) paragraph [0007] - paragraph [0015] paragraph [0028] - paragraph [0030] paragraph [0046] - paragraph [0058] ----- | 1-24 |
| A | US 2013/104203 A1 (DAVIS MARC E [US] ET AL) 25 April 2013 (2013-04-25) paragraph [0012] - paragraph [0019] paragraph [0037] - paragraph [0043] paragraph [0051] - paragraph [0053] paragraph [0067] - paragraph [0093] ----- | 1-24 |

INTERNATIONAL SEARCH REPORT

Information on patent family members

| |
|---|
| International application No PCT/EP2015/058347 |
|---|

| Patent document cited in search report | Publication date | Patent family member(s) | Publication date |
|--|------------------|-------------------------|--|
| US 2011016534 | A1 | 20-01-2011 | NONE |
| | | | |
| WO 2011001026 | A1 | 06-01-2011 | FI 20095731 A 30-12-2010 WO 2011001026 A1 06-01-2011 |
| | | | |
| US 2007236330 | A1 | 11-10-2007 | KR 20070099887 A 10-10-2007 US 2007236330 A1 11-10-2007 |
| | | | |
| US 2013104203 | A1 | 25-04-2013 | NONE |
| | | | |