(19) IPOS INTELLECTUAL PROPERTY OFFICE OF SINGAPORE

(11) Publication number: **SG 176839 A1**
(43) Publication date: **28.02.2012**
(51) Int. Cl: **H04W 12/06, H04L 29/06, H04W 8/06;**

(12) Patent Application

(21) Application number: **2011092475**
(22) Date of filing: **09.06.2010**
(30) Priority: **DE 10 2009 026 953.3 16.06.2009**

(71) Applicant: **BUNDESDRUCKEREI GMBH ORANIENSTRAßE 91 10958 BERLIN DE**
(72) Inventor: **KÜTER, JOACHIM AM KRÖGEL 3 10179 BERLIN DE**
LOER, THOMAS WILMSSTRAßE 21 B 10961 BERLIN DE
LANGEN, KIRSTEN ROSENTHALERSTRAßE 40 10178 BERLIN DE

(54) **Title:**
METHOD FOR REGISTERING A MOBILE RADIO IN A MOBILE RADIO NETWORK

(57) **Abstract:**
Method for registering a mobile radio in a mobile radio network Abstract The invention relates to a method for registering a mobile radio (100) in a mobile radio network (116) using at least one attribute stored in an ID token (106), wherein the ID token is associated with a user (102), having the following steps: - the user is authenticated to the ID token, a first computer system (136) is authenticated to the ID token, successful authentication of the user and of the first computer system to the ID token is followed by the first computer system effecting read access to the at least one attribute stored in the ID token via the mobile radio network, the at least one attribute is used for the registration. (Figure 1)

Method for registering a mobile radio in a mobile radio network

Abstract

The invention relates to a method for registering a mobile radio (100) in a mobile radio network (116) using at least one attribute stored in an ID token (106), wherein the ID token is associated with a user (102), having the following steps:

- the user is authenticated to the ID token,
- a first computer system (136) is authenticated to the ID token,
- successful authentication of the user and of the first computer system to the ID token is followed by the first computer system effecting read access to the at least one attribute stored in the ID token via the mobile radio network,
- the at least one attribute is used for the registration.

(Figure 1)

Method for registering a mobile radio in a mobile radio network

Description

The invention relates to a method for registering a mobile radio in a mobile radio network, to a computer program product, to an ID token and to a mobile radio system.

On the basis of the GSM standard, a mobile radio is registered in a GSM mobile radio network using the international mobile subscriber identity (IMSI). The IMSI is stored in the subscriber identity module (SIM). The IMSI identifies the home location register (HLR) in which the registration needs to be effected. The registration based on the UMTS standard and other mobile radio standards is also effected in a similar manner.

US 2007/0294431 A1 discloses a method for managing the digital identities which requires user registration.

In addition, token-based authentication methods are known from US 2001/0045451 A1 and US 6 257 486 B1, for example.

Further token-based authentication methods are disclosed in the patent applications DE 10 2008 000 067.1-31, DE 10 2008 040 416.0-31 and DE 10 2008 042 262.2-31 from the same patent applicant, these being unpublished at the time of filing.

The invention is based on the object of providing an improved method for registering a mobile radio in a mobile radio network, a computer program, an ID token and a mobile radio system.

The objects on which the invention is based are each achieved by means of the features of the independent patent claims. Embodiments of the invention are specified in the dependent patent claims.

According to embodiments of the invention, a mobile radio is registered in a mobile radio network using at least one attribute stored in an ID token, wherein the ID token is associated with a user, with the following steps:
the user is authenticated to the ID token, a first computer system is authenticated to the ID token, successful authentication of the user and of the first computer system to the ID token is followed by the first computer system effecting read access to the at least one attribute stored in the ID token via the mobile radio network, the at least one attribute is used for the registration.

Embodiments of the invention are particularly advantageous because the registration of the mobile radio does not require a SIM card but rather requires an ID token associated with the user, said ID token possibly being an identity document, particularly an electronic identity card, belonging to the user, for example. If the user has such an ID token, there is thus no additional requirement for a SIM card in order to register the mobile radio of the user in the mobile radio network. There is therefore also no longer the technical, logistical and financial complexity for producing, personalizing and distributing the SIM cards to the users. A further particular advantage is that a recently added user, i.e. a "subscriber", can immediately register his mobile radio in the mobile radio network without having to wait for a SIM card to be supplied.

Embodiments of the invention allow one or more of the attributes stored in an ID token to be read by the

first computer system, the connection between the ID token and the first computer system being able to be set up via the mobile radio network, particularly the Internet. The at least one attribute may be a statement regarding the identity of the user associated with the ID token, particularly regarding the "digital identity" of said user. By way of example, the first computer system reads the attributes family name, first name, address, in order to forward these attributes to a second computer system, for example a mobile radio network component of the mobile radio network, particularly a central database or a home location register (HLR).

According to one embodiment of the invention, the attribute stored in the ID token is an identifier. The identifier may be in a form such that it explicitly identifies the user and additionally a home location register relevant to this user in the mobile radio network. In particular, the identifier may be in the form of a globally unique identifier (GUID); by way of example, the identifier may be an IMSI.

In this context, a "home location register" is understood to mean any network component of a mobile radio network which is used for registering mobile radios in the mobile radio network.

In this context, the process of "registering" a mobile radio in a mobile radio network is understood to mean any process in which the identity of a user of the mobile radio is communicated to the mobile radio network, so that the user is registered using his mobile radio as an active subscriber who can make or receive voice calls, for example, can send or receive messages and/or can use other services provided via the mobile radio network, such as downloading data via the mobile radio network.

The ID token may be a portable electronic appliance, e.g. in the form of what is known as a USB stick, or may be a document, particularly a value document or security document.

According to the invention, a "document" is understood to mean paper-based and/or plastic-based documents, such as identity documents, particularly passports, identity cards, visas and driver's licenses, vehicle registration certificates, vehicle registration documents, corporate identity cards, health cards or other ID documents, and also chip cards, means of payment, particularly banker's cards and credit cards or other credentials which incorporate a data memory for storing the at least one attribute.

Embodiments of the invention are thus particularly advantageous because the at least one attribute is read from a particularly trustworthy document, for example an official document. The invention thus allows a particularly high level of trustworthiness for the conveyance of the attributes associated with a digital identity, accompanied by optimum data protection with extremely convenient handling.

According to one embodiment of the invention, the first computer system has at least one certificate which is used to authenticate the first computer system to the ID token. The certificate contains a statement indicating those attributes for which the first computer system has read authorization. The ID token uses this certificate to check whether the first computer system has the requisite read authorization for the read access to the attribute before such read access can be performed by the first computer system.

According to one embodiment of the invention, the first computer system sends the at least one attribute read from the ID token directly to a second computer system.

By way of example, the second computer system may be a mobile radio network component of the mobile radio network, which component effects the registration.

According to one embodiment of the invention, the attributes read from the ID token are transmitted from the first computer system first of all to the mobile radio of the user.

According to one embodiment of the invention, the attributes read from the ID token are signed by the first computer system and are then transmitted to the mobile radio. The user of the mobile radio is thus able to read the attributes, but without being able to alter them. Only after clearance by the user are the attributes forwarded from the mobile radio to the second computer system.

According to one embodiment of the invention, the user is able to augment the attributes with further data, for example with attributes which are required for providing a service which the user requires and which needs to be provided via the mobile radio network, prior to their being forwarded.

According to one embodiment of the invention, the mobile radio is a mobile telephone, particularly a smart phone, a personal digital assistant having a mobile radio interface, a portable computer having a mobile radio interface or another portable electronic appliance, such as a digital camera, having a mobile radio interface.

According to one embodiment of the invention, the identifiers, such as the IMSIs of the users, are stored in a database. The at least one attribute which is read from the ID token is used to access the database in order to read the identifier associated with the user from the database. The identifier also identifies the

home location register which is relevant to the user. The mobile radio of the user is then registered in this home location register which is relevant to the user. The user is then able to use his mobile radio to make or receive any calls via the mobile radio network or to use the mobile radio network for other purposes, such as for downloading data or other online services, such as using the Internet.

According to one embodiment of the invention, the database also stores the telephone number associated with the user. The at least one attribute is thus used to read not only the identifier but also the telephone number associated with the user from the database. This telephone number is then transmitted to the home location register, identified by the identifier, which is relevant to the user, where it is stored at least for the period of time for which the mobile radio is registered in the mobile radio network. Alternatively, the telephone number can be stored permanently in the home location register which is relevant to the user.

A particular advantage in this context is that the telephone number does not need to be prescribed by the operator of the mobile radio network, but rather the user can determine his telephone number himself provided that the desired telephone number has not already been allocated. The telephone number desired by the user is input into the database and/or the relevant HLR and is stored, as a result of which it is then stipulated for further action. The telephone number can be registered in the database and/or the relevant HLR by the user, for example using an Internet platform provided by the operator of the mobile radio network.

According to one embodiment of the invention, a first identifier is stored in the mobile radio of the user. Database access is used to read a second identifier from the database, the key used for the database access

being the at least one attribute read from the ID token of the user. The first and second identifiers are then compared with one another on the network. If the two identifiers match, the mobile radio is registered in the home location register identified by the first and second identifiers which is relevant to the user.

According to one embodiment of the invention, the at least one attribute which is stored in the ID token is an identifier which explicitly identifies the user, and also the home location register which is relevant to the user in the mobile radio network. By way of example, the identifier is in the form of an IMSI. The first computer system transfers the identifier read from the ID token to the relevant home location register, which is identified by the identifier, so that the mobile radio of the relevant user can be registered by this home location register.

According to one embodiment of the invention, the communication between the mobile radio and the ID token is effected contactlessly, particularly using an RFID or near field communication (NFC) standard. Preferably, the range of the communication method used for the data interchange between the mobile radio and the ID token is in the region of fewer than 50 cm, particularly in the region of no more than 30 cm. The data interchange between the mobile radio and the ID token using radio signals, particularly on the basis of an RFID or NFC standard, has particular handling advantages for the user.

By way of example, the user carries the ID token in a pocket, particularly a wallet. In order to register his mobile radio, the user does not need to remove the ID token from the pocket, since this is not necessary for communication by means of radio signals. On account of the short range of the communication method used for the data interchange, there is the simultaneous

assurance that the communication is not effected between the mobile radio of the user and the ID token of another user who is close by.

In a further aspect, the invention relates to a computer program product having instructions which can be executed by a computer system for the purpose of performing a method according to the invention. The computer program product may be of modular design, so that particular modules are executed by the first computer system and other modules are executed by the second computer system.

In a further aspect, the invention relates to an ID token, such as an identity document, particularly an electronic identity card, having a protected memory area for storing at least one attribute, means for authenticating a user associated with the ID token to the ID token, means for authenticating a first computer system to the ID token, means for setting up a protected connection to the first computer system via a mobile radio, wherein the first computer system is able to read the at least one attribute via the protected connection, wherein a necessary prerequisite for the reading of the at least one attribute from the ID token by the first computer system is the successful authentication of the user and of the first computer system to the ID token, and wherein the at least one attribute is able to identify a home location register in a mobile radio network.

In a further aspect, the invention relates to a mobile radio system for registering a mobile radio in a mobile radio network using at least one attribute stored in an ID token, wherein the ID token is associated with a user, having means for authenticating a first computer system to the ID token, means for performing read access for the first computer system to the at least one attribute stored in the ID token via the mobile

radio network, wherein the read access can be performed after the user and the first computer system have authenticated themselves to the ID token, and means for using the at least one attribute for the registration.

According to one embodiment of the invention, the ID token has means for end-to-end encryption. This allows the connection between the ID token and the first computer system to be set up via the mobile radio of the user, since the user cannot make any changes to the data transmitted via the connection on account of the end-to-end encryption.

Embodiments of the invention are explained in more detail below with reference to the drawings, in which:

Figure 1 shows a block diagram of an embodiment of an ID token according to the invention and a mobile radio system according to the invention,

Figure 2 shows a flowchart for an embodiment of a method according to the invention,

Figure 3 shows a UML diagram for an embodiment of a method according to the invention,

Figure 4 shows a block diagram for a further embodiment of an ID token according to the invention and a mobile radio system according to the invention,

Figure 5 shows a block diagram for a further embodiment of an ID token according to the invention and a mobile radio system according to the invention,

Figure 6 shows a block diagram for a further embodiment of an ID token according to the

invention and a mobile radio system according to the invention.

Elements of the embodiments below which correspond to one another are denoted by the same reference symbols.

Figure 1 shows a mobile radio 100 belonging to a user 102. The mobile radio 100 may be a portable computer, such as a laptop or palmtop computer, a personal digital assistant, a mobile telecommunication appliance, particularly a mobile telephone, a smart phone, or the like. The mobile radio 100 has an interface 104 for communicating with an ID token 106, which has a corresponding interface 108. The interface 104 may be a radio interface, particularly an RFID or NFC interface.

In particular, the ID token 106 may be a document, particularly a value document or security document, such as a machine-readable travel document (MRTD), such as an electronic passport or an electronic identity card, or a means of payment, such as a credit card.

The mobile radio 100 has at least one processor 110 for executing program instructions 112 and also a mobile radio network interface 114 for communicating via a mobile radio network 116. The mobile radio network may be a GSM, UMTS, CDMA 2000 network or a mobile radio network based on another mobile radio standard, such as 3GPP Long Term Evolution or 4G.

The ID token 106 has an electronic memory 118 having protected memory areas 120, 122 and 124. The protected memory area 120 is used for storing a reference value which is required for authenticating the user 102 to the ID token 106. By way of example, this reference value is an identifier, particularly what is known as a personal identification number (PIN), or is reference data for a biometric feature of the user 102 which can

be used for authenticating the user to the ID token 106.

The protected area 122 is used for storing a private key, and the protected memory area 124 is used for storing attributes, for example from the user 102, such as his name, place of residence, date of birth, sex, and/or attributes which relate to the ID token itself, such as the institution which produced or issued the ID token, the validity period of the ID token, a passport number or a credit card number.

Alternatively or in addition, the memory area 124 may store an identifier which explicitly identifies the user 102 with whom the ID token 106 is associated. The identifier may also identify a network component 150 of the mobile radio network 116. This network component 150 prompts or performs the registration of the mobile radio 100 in the mobile radio network 116. In particular, the identifier may be in the form of an IMSI. In particular, the identifier may be in the form of a multi-digit number, with predetermined digits in this multi-digit number forming an HLR number which identifies the HLR which is relevant to the user 102.

The electronic memory 118 may also have a memory area 126 for storing a certificate. The certificate contains a public key which is associated with the private key stored in the protected memory area 122. The certificate may have been produced on the basis of a public key infrastructure (PKI) standard, for example on the X.509 standard.

The certificate does not necessarily need to be stored in the electronic memory 118 of the ID token 106. Alternatively or in addition, the certificate may also be stored in a public directory server.

The ID token 106 has a processor 128. The processor 128 is used for executing program instructions 130, 132 and 134. The program instructions 130 are used for user authentication, i.e. for authenticating the user 102 to the ID token.

In the case of an embodiment with a PIN, the user 102 inputs his PIN, for the purpose of authenticating himself, into the ID token 106, for example via the mobile radio 100. As a result of execution of the program instructions 130, the protected memory area 120 is then accessed in order to compare the input PIN with the reference value stored therein for the PIN. If the input PIN matches the reference value for the PIN, the user 102 is deemed authenticated.

Alternatively, a biometric feature of the user 102 is captured. By way of example, to this end the ID token 106 has a fingerprint sensor or a fingerprint sensor is connected to the mobile radio 100 or integrated therein. In this embodiment, the biometric data captured from the user 102 are compared with the biometric reference data stored in the protected memory area 120 by virtue of execution of the program instructions 130. If there is a sufficient match between the biometric data captured from the user 102 and the biometric reference data, the user 102 is deemed authenticated.

The program instructions 134 are used for executing those steps of a cryptographical protocol for authenticating an ID provider computer system 136 to the ID token 106 which relate to the ID token 106. The cryptographical protocol may be a challenge response protocol based on a symmetric key or an asymmetric key pair.

By way of example the cryptographical protocol implements an extended access control method, as is

specified for machine-readable travel documents (MRTD) by the international aviation authority (ICAO). By successfully executing the cryptographical protocol, the ID provider computer system 136 authenticates itself to the ID token and thereby verifies its read authorization to read the attributes stored in the protected memory area 124. The authentication may also be reciprocal, i.e. the ID token 106 then also needs to authenticate itself to the ID provider computer system 136 on the basis of the same or a different cryptographical protocol.

The program instructions 132 are used for the end-to-end encryption of data transmitted between the ID token 106 and the ID provider computer system 136, but at least of the attributes read by the ID provider computer system 136 from the protected memory area 124. For the end-to-end encryption, it is possible to use a symmetric key which is agreed between the ID token 106 and the ID provider computer system 136 when the cryptographic protocol is executed, for example.

As an alternative to the embodiment shown in Figure 1, the mobile radio 100 can use its interface 104 to communicate with the interface 108 not directly but rather via a reader for the ID token 106, which reader is connected to the interface 104. This reader, such as what is known as a class 2 chip card terminal, can also be used to input the pin.

The ID provider computer system 136 has a mobile radio network interface 138 for communicating via the mobile radio network 116 or with a network component of the mobile radio network 116, particularly via what is known as the backbone or the core network of the mobile radio network 116. The ID provider computer system 136 also has a memory 140 which stores a private key 142 from the ID provider computer system 136 and also the relevant certificate 144. By way of example, this

certificate may also be a certificate based on a PKI standard, such as X.509.

The ID provider computer system 136 also has at least one processor 145 for executing program instructions 146 and 148. Execution of the program instructions 146 executes the steps of the cryptographical protocol which relate to the ID provider computer system 136. Overall, the cryptographical protocol is thus executed by virtue of execution of the program instructions 134 by the processor 128 in the ID token 106 and by virtue of execution of the program instructions 146 by the processor 145 in the ID provider computer system 136.

The program instructions 148 are used for implementing the end-to-end encryption on the ID provider computer system 136, for example on the basis of the symmetric key which has been agreed between the ID token 106 and the ID provider computer system 136 when the cryptographical protocol was executed. In principle, it is possible to use any method inherently known in advance for agreeing the symmetric key for the end-to-end encryption, such as Diffie Hellman key exchange.

The ID provider computer system 136 is preferably located in a specially protected environment, particularly in what is known as a trust center, as a result of which the ID provider computer system 136, in combination with the need for the user 102 to be authenticated to the ID token 106, forms the trust anchor for the authenticity of the attributes read from the ID token 106.

According to a further embodiment of the invention, the ID provider computer system 136 may also form an integral part of the network component 150.

The network component 150 may be in the form of a home location register or the network component 150 may be designed to interact with the home location register of the mobile radio network 116 in order to perform or prompt the registration of mobile radios.

The network component 150 has a mobile radio network interface 152 for connection to the mobile radio network 116 or to another network component of the mobile radio network 116, particularly via what is known as the backbone or the core network of the mobile radio network 116. Particularly the communication between the network component 150 and the ID provider computer system 136 can be effected via the backbone or the core network of the mobile radio network 116.

In addition, the network component 150 has at least one processor 154 for executing program instructions 156. Execution of the program instructions 156 registers the mobile radio, for example, in the mobile radio network 116 using the at least one attribute, or the registration is initiated thereby.

The process for registering the mobile radio 100 in the mobile radio network 116 is as follows:

1. The user 102 is authenticated to the ID token 106.

   The user 102 authenticates itself to the ID token 106. In the case of an implementation with a PIN, the user 102 does this by inputting his PIN, for example using the mobile radio 100 or a chip card terminal connected thereto or integrated therein. By executing the program instructions 130, the ID token 106 then checks the correctness of the input PIN. If the input PIN matches the reference value stored in the protected memory area 120 for the PIN, the user 102 is deemed authenticated. A similar process can be used when a biometric

feature of the user 102 is used to authentic him, as described above.

2. The ID provider computer system 136 is authenticated to the ID token 106.

To this end, a connection is set up between the ID token 106 and the ID provider computer system 136 via the mobile radio 100 and the mobile radio network 116. By way of example, the ID provider computer system 136 transmits its certificate 144 to the ID token 106 via this connection. The program instructions 134 then generate what is known as a challenge, i.e. a random number, for example. This random number is encrypted with the public key from the ID provider computer system 136, which is contained in the certificate 144. The resulting cipher is sent from the ID token 106 to the ID provider computer system 136 via the connection. The ID provider computer system 136 decrypts the cipher using its private key 142 and thus obtains a random number. The random number is returned to the ID token 106 by the ID provider computer system 136 via the connection. By executing the program instructions 134, the ID token checks whether the random number received from the ID provider computer system 136 matches the originally generated random number, i.e. the challenge. If this is the case, the ID provider computer system 136 is deemed authenticated to the ID token 106. The random number can be used as a symmetric key for the end-to-end encryption.

3. The at least one attribute is read

When the user 102 has successfully authenticated himself to the ID token 106, and when the ID provider computer system 136 has successfully authenticated itself to the ID token 106, the ID

provider computer system 136 is provided with read authorization to read a, a plurality of or all the attribute(s) stored in the protected memory area 124. On the basis of an appropriate read command which the ID provider computer system 136 sends to the ID token 106 via the connection, the requested attributes are read from the protected memory area 124 and are encrypted by virtue of execution of the program instructions 132. The encrypted attributes are transmitted to the ID provider computer system 136 via the connection and are decrypted by the ID provider computer system by virtue of execution of the program instructions 148. As a result, the ID provider computer system 136 obtains knowledge of the attributes which have been read from the ID token 106.

These attributes are signed by the ID provider computer system using its certificate 144 and are transmitted to the network component 150 via the mobile radio 100 or directly. This informs the network component 150 about the attributes which have been read from the ID token 106, as a result of which the network component 150 can use these attributes to register the mobile radio 100 in the mobile radio network 116 or can prompt the registration using the attributes.

The need for the user 102 to be authenticated to the ID token 106 and for the ID provider computer system 136 to be authenticated to the ID token 106 provides the necessary trust anchor, as a result of which the network component 150 can be certain that the attributes of the user 102 which are communicated to it by the ID provider computer system 136 are correct and not corrupted.

Depending on the embodiment, the order of the authentication may be different. By way of example,

provision may be made for the user 102 to have to authenticate itself to the ID token 106 first, followed by the ID provider computer system 136. Alternatively, it is fundamentally possible for the ID provider computer system 136 to have to authenticate itself to the ID token 106 first, followed by the user 102 only then.

In the first case, the ID token 106 is designed such that it is enabled only by input of a correct pin or a correct biometric feature by the user 102, for example. Only this enabling allows the program instructions 132 and 134 to be started and hence the ID provider computer system 136 to be authenticated.

In the second case, the program instructions 132 and 134 can actually be started even when the user 102 has not yet authenticated itself to the ID token 106. In this case, by way of example, the program instructions 134 are designed such that the ID provider computer system 136 can perform read access to the protected memory area 124 for the purpose of reading of one or more of the attributes only when the program instructions 130 have signaled the successful authentication of the user 102 too.

For the purpose of registering the mobile radio 100, the mobile radio 100 can use its network interface 114 to send a signal 101 to the mobile radio network 116, for example. It is even possible to send this signal 101 when the mobile radio 100 is not registered in the mobile radio network 116.

The signal 101 is processed by the network component 150 of the mobile radio network 116 by virtue of the network component 150 directing a request 103 to the ID provider computer system 136. On the basis of this request 103, the ID provider computer system 136 reads at least one attribute value from the ID token 106

after the user 102 and the ID provider computer system 136 have been authenticated. The ID provider computer system 136 then responds to the request 103 with a message 105 which contains the at least one attribute value and the signature thereof. This message is received by the network component 150 or another network component of the mobile radio network 116 and is used to register the mobile radio 100 of the user 102.

The communication between the ID token 106 and the ID provider computer system 136 can also be effected before the mobile radio 100 is actually registered via the mobile radio network 116. By way of example, this is done by virtue of a temporary identifier being allocated to the mobile radio 100 on the basis of the reception of the signal 101 by the mobile radio network 116, said temporary identifier being used for the communication with the mobile radio 100 via the mobile radio network 116 for as long as the mobile radio 100 is not yet registered.

Figure 2 shows an embodiment of a method according to the invention.

The process for registering the mobile radio 100 of the user 102 using his ID token 106 is as follows, for example: in step 200, the user authenticates himself to the ID token. This can be done by virtue of the user using a keypad on the mobile radio to input his PIN, which is transmitted from the mobile radio via the interface thereof to the interface of the ID token. If the authentication of the user to the ID token was successful, a connection is set up between the ID token and the ID provider computer system in step 202.

This is preferably a secure connection, for example on the basis of what is known as a secure messaging method.

In step 204, the ID provider computer system is at least authenticated to the ID token via the connection which was set up in step 202. In addition, there may also be provision for the ID token to be authenticated to the ID provider computer system.

When the user and the ID provider computer system have been successfully authenticated to the ID token, the ID provider computer system receives from the ID token the access authorization to read at least one of the attributes. In step 206, the ID provider computer system sends one or more read commands for reading the required attributes from the ID token. The attributes are then transmitted by means of end-to-end encryption via the secure connection to the ID provider computer system and are decrypted therein.

The attribute values which have been read are signed by the ID provider computer system in step 208. In step 210, the ID provider computer system sends the signed attribute values to a network component. The attribute value(s) can be transmitted via the mobile radio network. Alternatively, the ID provider computer system is part of the network component, which means that no transmission is necessary.

The signed attribute values reach the network component either directly or via the mobile radio. In the latter case, the user may have the opportunity to take note of the signed attribute values and/or to augment them with further data. Provision may be made for the signed attribute values to be forwarded, possibly with the added data, from the mobile radio to the network component only following clearance by the user. This provides the greatest possible transparency for the user in terms of the attributes sent from the ID provider computer system to the network component.

In step 212, the mobile radio is then registered in the mobile radio network by the network component using the attribute values read from the ID token.

Figure 3 shows a further embodiment of a method according to the invention.

To register his mobile radio 100 in the mobile radio network 116, the user 102 first of all authenticates himself to the ID token 106. When the user 102 has been successfully authenticated to the ID token 106, the mobile radio 100 sends a signal to the network component 150 of the mobile radio network via the mobile radio network 116 in order to signal to the mobile radio network that the mobile radio 100 needs to be registered in the mobile radio network.

The network component 150 then sends a request to the ID provider computer system 136. This request can be sent by the mobile radio network 116. The request can also be communicated directly from the network component 150 to the ID provider computer system 136, particularly if the ID provider computer system 136 is an integral part of the network component 150.

On the basis of the request received from the network component 150, the ID provider computer system 136 authenticates itself to the ID token 106 and directs a read request to read one or more of the attributes to the ID token 106.

Assuming prior successful authentication of the user 102 and of the ID provider computer system 136, the ID token 106 responds to the read request with the desired attributes. The ID provider computer system 136 signs the attributes and sends the signed attributes to the mobile radio 100. Following clearance by the user 102 on the mobile radio 100, the signed attributes are then transmitted to the network component 150. The network

component 150 then prompts the registration of the mobile radio 100.

Figure 4 shows an embodiment of a mobile radio system according to the invention with a database 158. The database 158 contains at least one database table 160 which stores an explicit identifier and a telephone number for each registered user of the mobile radio network 116. To read the identifier and the telephone number of the user 102, knowledge of at least one attribute value is required, said attribute value needing to be read from the ID token 106 of the user 102 by the ID provider computer system 136.

The database 158 has at least one processor 162 for executing program instructions 164. Execution of the program instructions 164 allows access to the database table 160 in order to use the attribute value read from the ID token 106 of the user 102 to read the identifier and the telephone number of the user 102.

The identifier explicitly identifies not only the user 102 but also a home location register which is relevant to the user 102. In the embodiment under consideration here, the mobile radio network 116 has a number I of home location registers HLR1, HLR2, ..., HLRi, ..., HLRI.

The identifiers stored for each of the registered users of the mobile radio network 116 in the database table 160 may be in the form of IMSIs, for example.

To register the mobile radio 100, the process in the case of the embodiment under consideration here is such that at least one attribute value is read from the ID token 106 by the ID provider computer system 136 after the user 102 and the ID provider computer system 136 have authenticated themselves to the ID token 106, for example as described above with reference to Figures 1,

2 and 3. The ID provider computer system 136 then sends the message 105 with the attribute value to the database 158. By executing the program instructions 164, database access is then performed using the attribute value in order to read the identifier associated with the user 102 and the telephone number of the user 102 from the database table 160 using the attribute value as a key. The database 158 then sends a message 107 in order to communicate this identifier and the telephone number of the user 102 to the mobile radio network 116. The message 107 is received by the home location register identified by the identifier, and said home location register then registers the mobile radio 100.

Figure 5 shows an alternative embodiment in which the identifier is stored in a memory 166 in the mobile radio 100. By way of example, this identifier can be input into the mobile radio 100 by the user 102 manually, so that it is stored in the memory 166. Alternatively, the identifier can be automatically written to the memory 166 in the mobile radio 100 using an over the air (OTA) technique.

As an addition to the embodiment shown in Figure 4, the mobile radio 100 performs the registration by sending the identifier stored in its memory 166 to the database 158 via the mobile radio network 116.

The database table 160 in the embodiment under consideration here stores only the identifiers but not the telephone numbers. By contrast, the telephone numbers of the registered users are stored in local databases of the individual home location registers. Figure 5 shows the database 168 of the home location register 1 by way of example, said database storing the telephone numbers of those registered users to whom the home location register 1 is relevant. These telephone

numbers can be accessed using the identifiers of the relevant users.

In the embodiment under consideration here, the processor 162 in the database 158 is additionally used to execute program instructions 170. By executing the program instructions 170, a check is performed to determine whether the identifier received from the mobile radio 100 is identical to the identifier read from the database table 160. Only if this is the case does the database 158 send the message 107, otherwise the registration is rejected.

The process for registering the mobile radio 100 in this case is thus as follows:

The mobile radio 100 sends the signal 101 to the mobile radio network 116, the signal 101 in this embodiment bearing the identifier stored in the memory 166. The ID provider computer system 136 reads the at least one attribute value from the ID token 106 when the user 102 and the ID provider computer system 136 have authenticated themselves to the ID token 106, as explained above with reference to Figures 1 to 4. The ID provider computer system 136 then sends the message 105 with the attribute value to the database 158.

By executing the program instructions 164, the database 158 reads the identifier of the user 102 from the database table 160 using the attribute value. In addition, by executing the program instructions 170, the database 158 checks whether the identifier received from the mobile radio 100 matches the identifier read from the database table 160. Only if this is the case does the database 158 send the message 107, as a result of which the registration can take place in the relevant home location register, such as the home location register 1. The relevant home location register uses the identifier as a key to access its

local database 168 in order to ascertain the telephone number of the user 102. The registration is then performed in the mobile radio network for the telephone number ascertained in this manner.

Figure 6 shows a further embodiment of a mobile radio system according to the invention. In this embodiment, the identifier, that is to say the IMSI, for example, of the user 102 is stored as an attribute value in the protected memory area 124 of the ID token 106.

To register the mobile radio 100, the process is then such that the ID provider computer system 136 reads the identifier from the ID token 106 when the user 102 and the ID provider computer system 136 have authenticated themselves to the ID token 106, in a similar manner to the embodiments described above from Figures 1 to 5. The ID provider computer system 136 then sends the message 105 with the identifier, said message being received by the home location register identified by the identifier in the mobile radio network 116, such as the HLR1. The relevant home location register effects database access to its local database 168 in order to use the identifier contained in the message 105 to ascertain the telephone number of the user 102, said telephone number then being used to register the mobile radio 100.

List of Reference Symbols

100	Mobile radio
101	Signal
102	User
103	Request
104	Interface
105	Message
106	ID token
107	Message
108	Interface
110	Processor
112	Program instructions
114	Mobile radio network interface
116	Mobile radio network
118	Electronic memory
120	Protected memory area
122	Protected memory area
124	Protected memory area
126	Memory area
128	Processor
130	Program instructions
132	Program instructions
134	Program instructions
136	ID provider computer system
138	Mobile radio network interface
140	Memory
142	Private key
144	Certificate
145	Processor
146	Program instructions
148	Program instructions
149	Program instructions
150	Network component
152	Mobile radio network interface
154	Processor
156	Program instructions
158	Database

160	Database table
162	Processor
164	Program instructions
166	Memory
168	Database
170	Program instructions

Patent Claims

1. A method for registering a mobile radio (100) in a mobile radio network (116) using at least one attribute stored in an ID token (106), wherein the ID token is associated with a user (102), having the following steps:

- the user is authenticated to the ID token,
- a first computer system (136) is authenticated to the ID token,
- successful authentication of the user and of the first computer system to the ID token is followed by the first computer system effecting read access to the at least one attribute stored in the ID token via the mobile radio network,
- the at least one attribute is used for the registration.

2. The method as claimed in claim 1, wherein the first computer system is authenticated to the ID token using a certificate (144) from the first computer system, wherein the certificate contains a statement indicating those attributes stored in the ID token for which the first computer system is authorized for the read access.

3. The method as claimed in claim 2, wherein the ID token checks the read authorization of the first computer system for the read access to at least one of the attributes using the certificate.

4. The method as claimed in one of claims 1, 2 and 3, having the following further steps:

- the at least one attribute read from the ID token is signed by the first computer system,

- the at least one signed attribute is transmitted from the first computer system to a second computer system (150; HLR 1, HLR 2, ... HLR i, ... HLR I), wherein the second computer system is coupled to the mobile radio network in order to perform or initiate the registration.

5. The method as claimed in claim 4, wherein the second computer system is a mobile radio network component of the mobile radio network.

6. The method as claimed in claim 4 or 5, wherein the at least one attribute read from the ID token by the first computer system is sent to the mobile radio, from where it is forwarded to the second computer system following clearance by the user.

7. The method as claimed in claim 6, wherein the user can augment the attributes with further data prior to their being forwarded to the second computer system.

8. The method as claimed in one of the preceding claims, wherein the mobile radio is a mobile telephone, particularly a smartphone, a personal digital assistant having a mobile radio interface, a portable computer having a mobile radio interface or a portable electronic appliance, such as a digital camera, having a mobile radio interface.

9. The method as claimed in one of the preceding claims, wherein database access to a database (158) which stores identifiers is performed, wherein each of the identifiers identifies a home location register, wherein the identifier of a home location register associated with the user (HLR 1, HLR 2, ... HLR i, ... HLR I) is read from the database using the at least one attribute, and

wherein the mobile radio is registered in the home location register identified by the identifier read from the database.

10. The method as claimed in claim 9, wherein the database stores the telephone numbers of the users.

11. The method as claimed in one of the preceding claims, wherein a first identifier is stored in the mobile radio, and wherein the user has an associated second identifier which identifies a home location register, and wherein the at least one attribute is used to check whether the first identifier is the second identifier, and wherein the registration is effected in the home location register identified by the first and second identifiers if the first and second identifiers match.

12. The method as claimed in one of the preceding claims, wherein the at least one attribute is an identifier which identifies a home location register, wherein the mobile radio is registered in the home location register identified by the identifier.

13. A computer program product having instructions which can be executed by a computer system for the purpose of carrying out a method as claimed in one of the preceding claims.

14. An ID token having

- a protected memory area (124) for storing at least one attribute,
- means (120, 130) for authenticating a user (102) associated with the ID token to the ID token,

- means (134) for authenticating a first computer system (136) to the ID token,
- means (132) for setting up a protected connection to the first computer system via a mobile radio, wherein the first computer system is able to read the at least one attribute via the protected connection,

wherein a necessary prerequisite for the reading of the at least one attribute from the ID token by the first computer system is the successful authentication of the user and of the first computer system to the ID token, and wherein the at least one attribute is able to identify a home location register (HLR 1, HLR 2, ... HLR i, ... HLR I) in a mobile radio network.

15. The ID token as claimed in claim 14, having means (132) for the end-to-end encryption of the connection for protected transmission of the at least one of the attributes to the first computer system.

16. The ID token as claimed in claim 14 or 15, wherein it is an electronic appliance, particularly a USB stick, or a document, particularly a value document or security document.

17. A mobile radio system for registering a mobile radio (100) in a mobile radio network (116) using at least one attribute stored in an ID token (106), wherein the ID token is associated with a user (102), having

- means (142, 144, 146) for authenticating a first computer system (136) to the ID token,
- means (138, 148) for performing read access for the first computer system to the at least one attribute stored in the ID token via the mobile

radio network, wherein the read access can be performed after the user and the first computer system have authenticated themselves to the ID token,

- means (150) for using the at least one attribute for the registration.

18. The mobile radio system as claimed in claim 17, wherein the first computer system has means (144) for signing the at least one attribute, and having a network component (150) which is designed to receive the at least one signed attribute from the first computer system.

19. The mobile radio system as claimed in claim 18, wherein the network component has a database (158), wherein the database stores identifiers, wherein each of the identifiers identifies a home location register (HLR 1, HLR 2, ... HLR i, ... HLR I) in the mobile radio network, wherein read access to an identifier associated with the user can be performed using the at least one attribute.

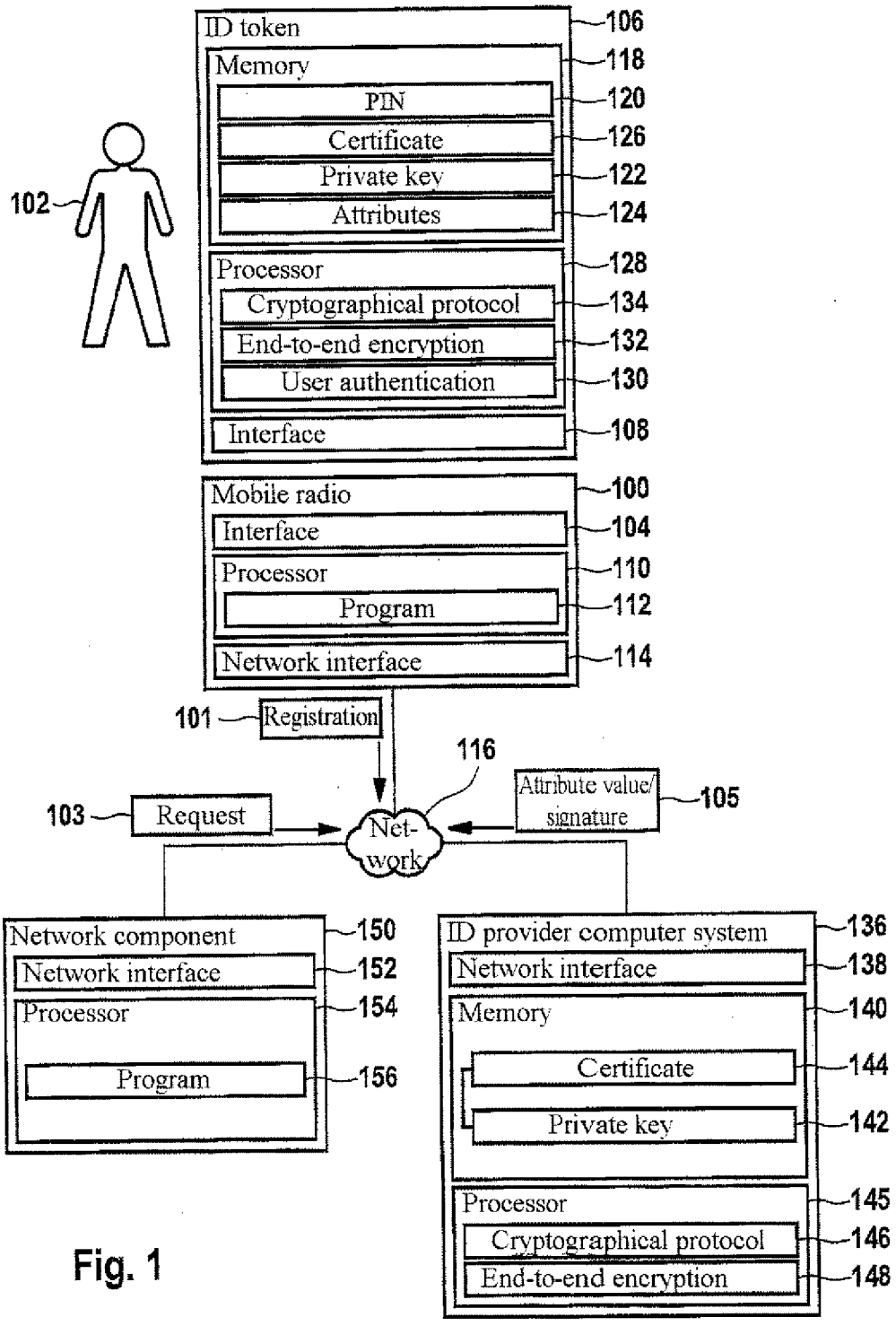
ID token
106
Memory
118
PIN
120
Certificate
126
Private key
122
Attributes
124
Processor
128
Cryptographical protocol
134
End-to-end encryption
132
User authentication
130
Interface
108
102
Mobile radio
100
Interface
104
Processor
110
Program
112
Network interface
114
101
Registration
116
103
Request
Net-work
Attribute value/ signature
105
Network component
150
Network interface
152
Processor
154
Program
156
ID provider computer system
136
Network interface
138
Memory
140
Certificate
144
Private key
142
Processor
145
Cryptographical protocol
146
End-to-end encryption
148

Fig. 1

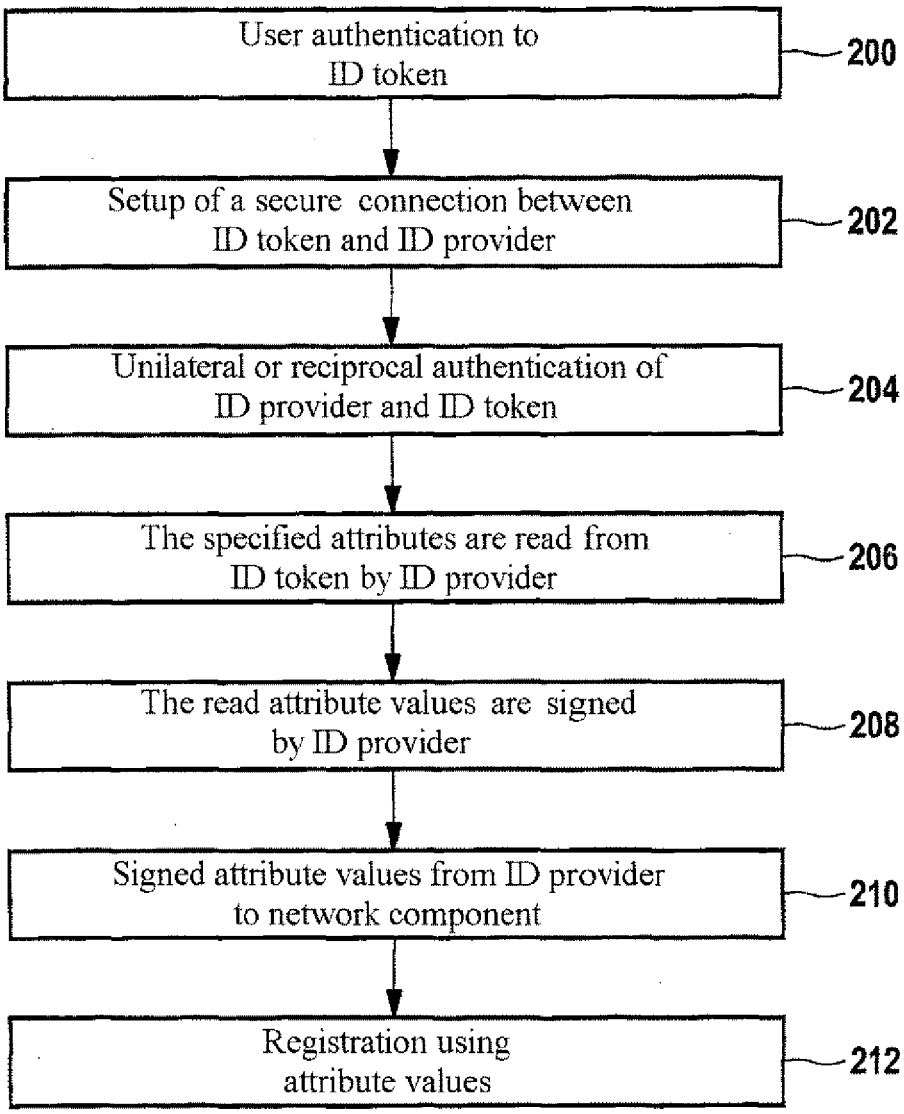
User authentication to ID token
200
Setup of a secure connection between ID token and ID provider
202
Unilateral or reciprocal authentication of ID provider and ID token
204
The specified attributes are read from ID token by ID provider
206
The read attribute values are signed by ID provider
208
Signed attribute values from ID provider to network component
210
Registration using attribute values
212

Fig. 2

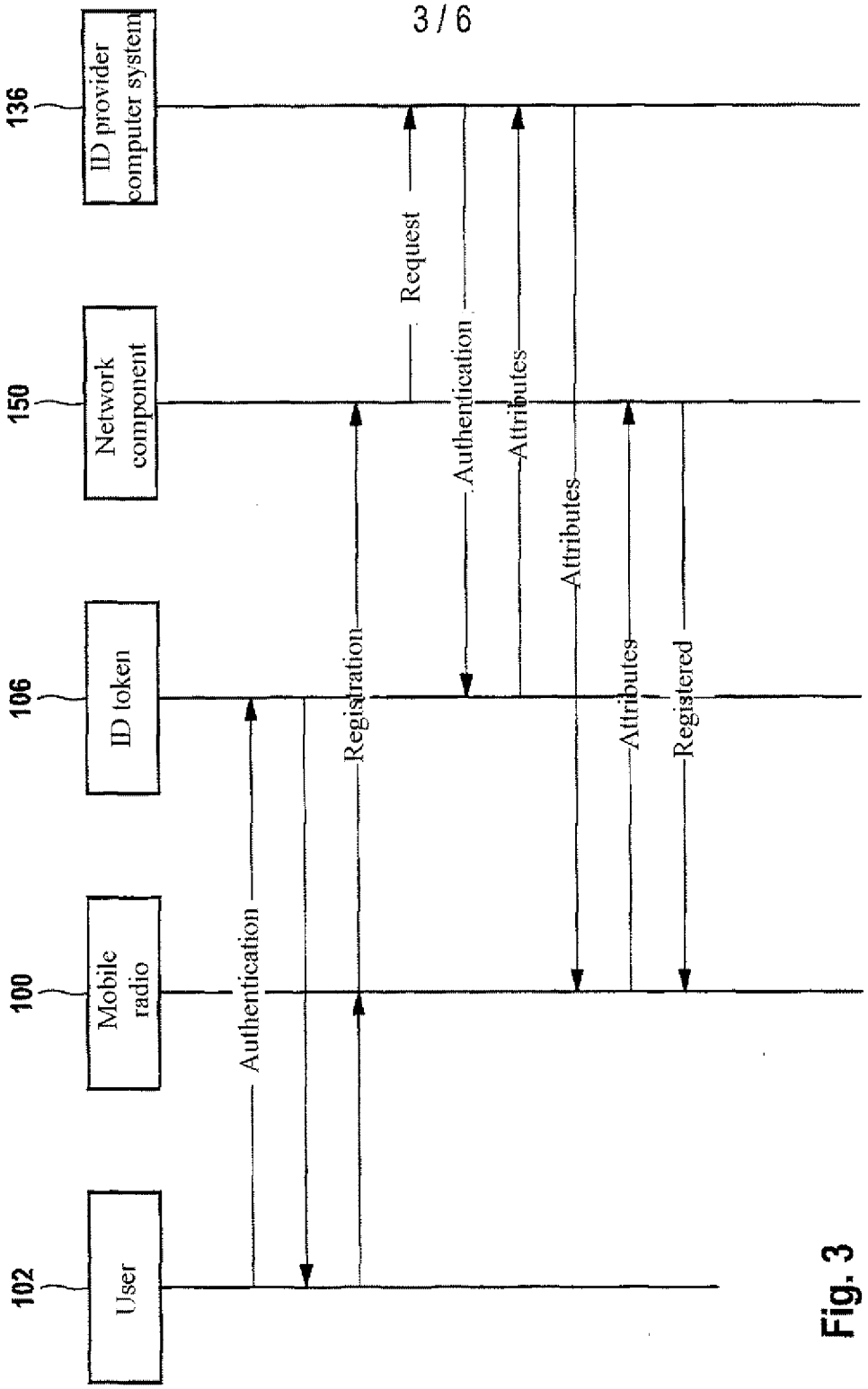
102
User
100
Mobile radio
106
ID token
150
Network component
136
ID provider computer system
Authentication
Registration
Request
Authentication
Attributes
Attributes
Attributes
Registered

Fig. 3

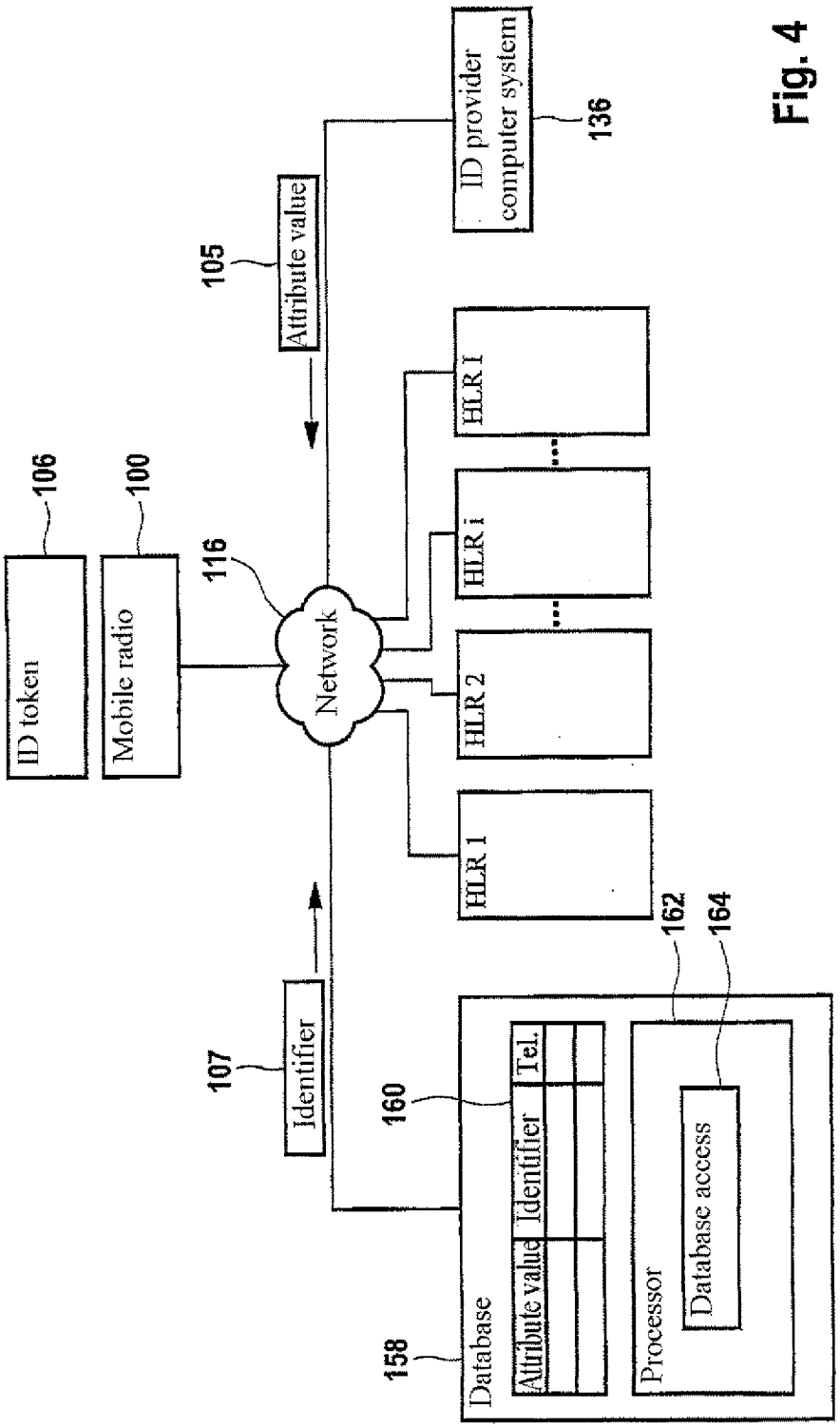
ID token
106
Mobile radio
100
116
Network
105
Attribute value
ID provider computer system
136
HLR 1
HLR 2
HLR i
HLR I
107
Identifier
160
Database
Attribute value
Identifier
Tel.
158
Processor
Database access
162
164

Fig. 4

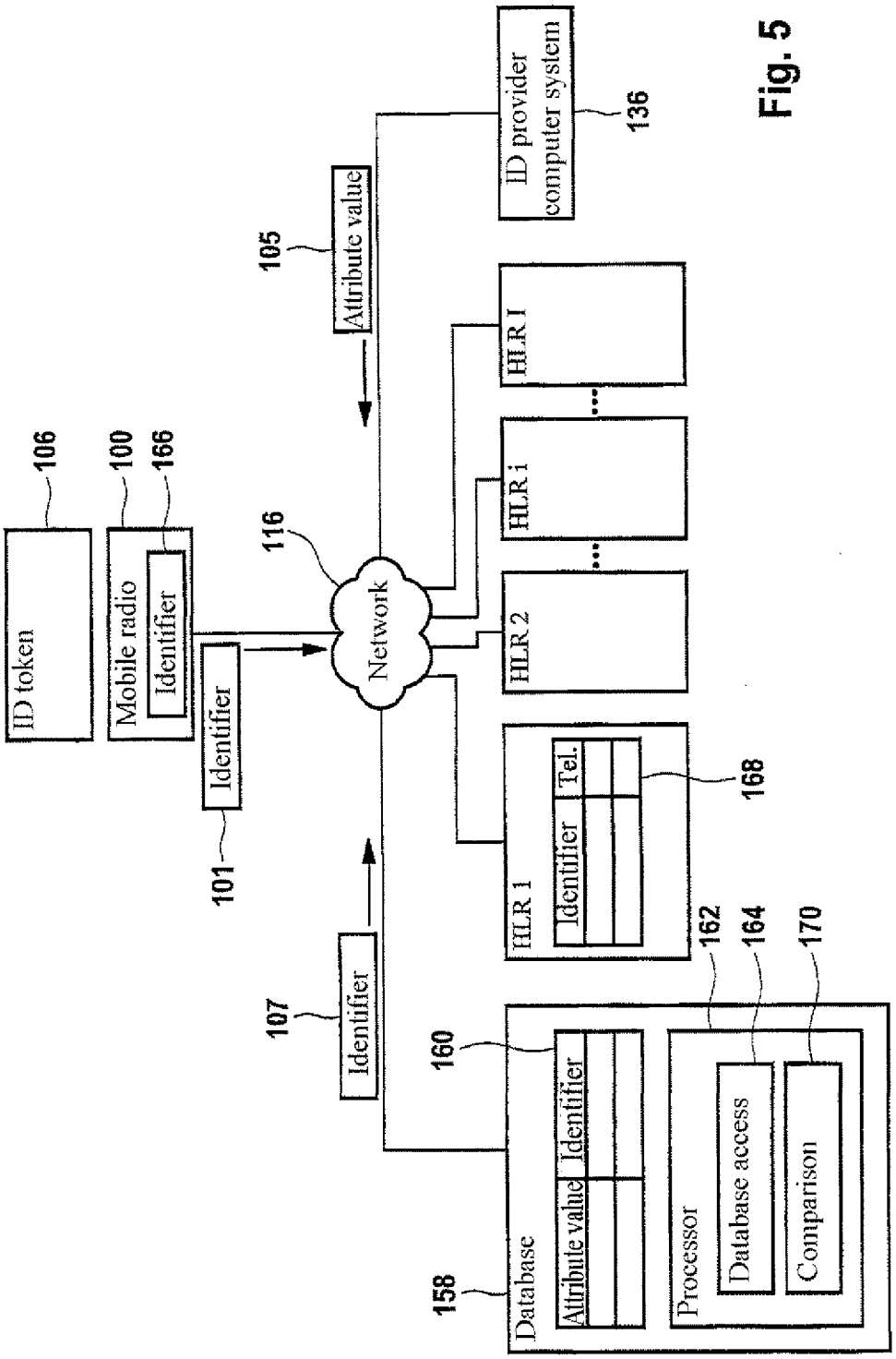
ID token
106
Mobile radio
100
Identifier
166
Identifier
101
116
Network
105
Attribute value
ID provider computer system
136
HLR I
HLR i
HLR 2
HLR 1
Identifier
Tel.
168
162
164
170
107
Identifier
160
Database
Attribute value
Identifier
158
Processor
Database access
Comparison

Fig. 5

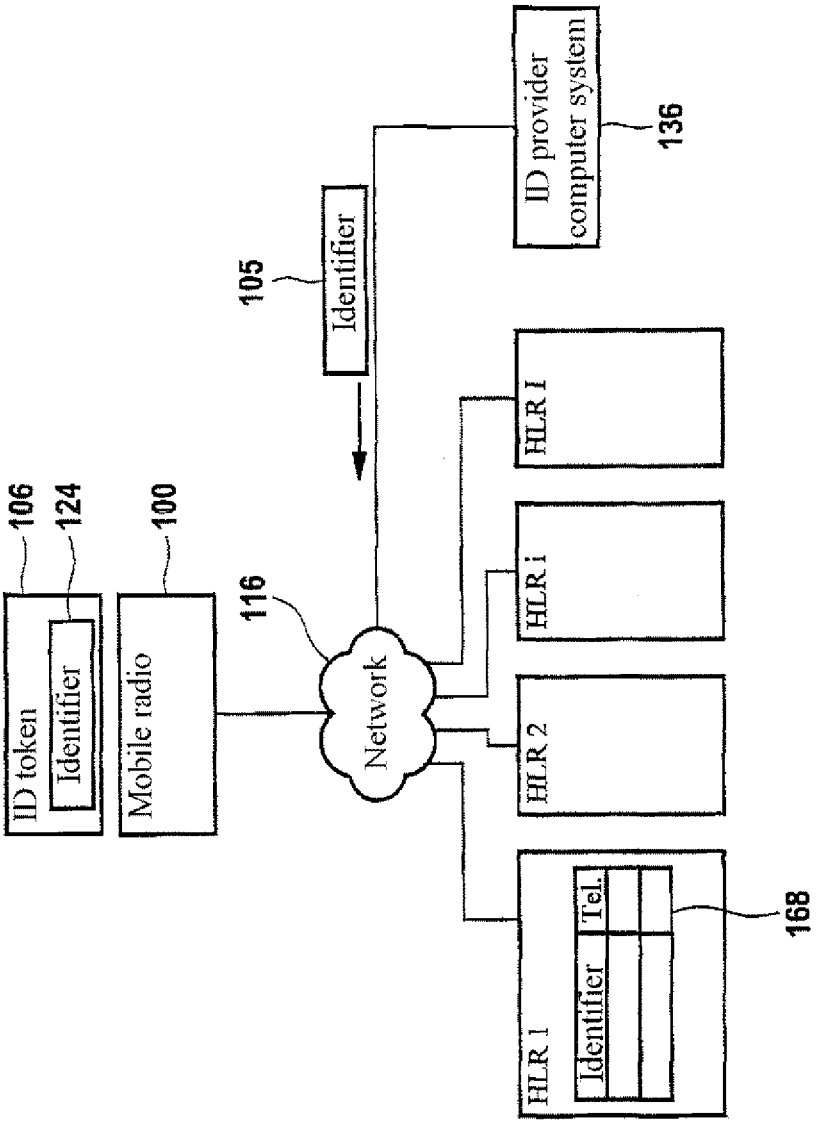
ID token
Identifier
106
124
Mobile radio
100
116
Network
105
Identifier
ID provider computer system
136
HLR I
HLR i
HLR 2
HLR 1
Identifier
Tel.
168

Fig. 6