

Service-based authentication to a network.

Field of the invention

The invention relates to a service-based authentication to a network and, in particular, though not exclusively, to a method and a system for a service-based authentication of a terminal to a network.

Background of the invention

The new generation mobile devices, such as smart phones, provide more and more enhanced computational functionalities via open network connections. Such mobile devices are e.g. capable of receiving e-mail, share software with one another through short-range connections, downloading and executing software from the Internet, making automated calls and act under remote control. Hence, similar to a personal computer, mobile devices and in particular the software components involved in the setting up of a connection between the mobile device to the network, are vulnerable to attacks of malicious code (malware). Typically malware attempts to make misuse of mobile device or to simply disrupt legitimate use of a mobile device.

One type of malware is capable of enabling the remotely connection to a mobile device of a victim and subsequently enabling the request of and use authentication information from the (U)SIM of the victim which is used by the attacker to obtain access to the network. Hence, the attacker can achieve network access as if the connection was set up by the victim. Such attack, usually referred to as a man-in-the-middle attack, thus allows to set up calls on the expenses of the victim thereby causing substantial damage.

One problem relates to the fact that the network should be informed about such attack. Current mobile networks like GSM and UTSN networks do not provide the (U)SIM with information which allows the (U)SIM to check the origin

(source) of an authentication request. Hence, measures against such man-in-the-middle attack are difficult to implement.

Further - if the device is infected with malware - information generated by the mobile device which may allow the network to examine the source of a request received by a mobile device should be reported to the network in a simple and secure way which is not detectable or at least very difficult to detect by malware and which allows easy implementation in current networks without the requirement of substantial modifications to the network infrastructure and/or communications standard.

Commented [f1]: Dit gedeelte lijkt uit de octrooiaanvraag 'SIM reports' te komen. Is hier niet passend.

Summary of the invention

It is an object of the invention to reduce or eliminate at least one of the drawbacks known in the prior art and to provide in a first aspect of the invention a method for service-based authentication of a terminal to a network wherein the terminal comprises a number of communications interfaces, each communications interface allowing the terminal to set-up a predetermined communication channel with the network. The method comprises the steps of: sending a service request for access to a network service; receiving in response to the service request an authentication request from the network; identifying the communication channel through which the authentication request was received; and, sending an authentication response RES to the network, wherein the authentication response depends on the identified communication channel. Using information regarding the communication channel through which the authentication response was received by the terminal, allows the terminal to make the response specific for the service requested. The use of such service specific response RES can be used to prevent malware to make misuse of the authentication information which is sent between a terminal and the network.

In an embodiment the method comprises the steps of: determining a service code associated with the identified communication channel; calculating the response RES on the

basis of the information in the authentication request and the service code, thereby including into the response in a
~~(encrypting cryptographically?)~~ secure way information
 regarding the identity of the communication channel through
 5 which the authentication request was received ~~into the~~
~~response. The information embodied in the service code, i.e. the information regarding the communication channel through~~
~~which the authentication response was received, is encrypted~~
~~in the response.~~ Such ~~(cryptographically?)~~ secure ~~encrypted~~
 10 information is not or at least very difficult to ~~modify~~ detect
 by malware.

In another embodiment, the terminal comprises an identity module, preferably a removable identity module, and a radio module comprising a number of communications interfaces
 15 and configured to identify the communications channel through which the authentication request was received. The method further comprises the step of: the radio module sending an service code SC to the identity module, wherein the service code identifies the communications channel through which the authentication request was received. Preferably, the radio
 20 module comprises one or more trusted ~~module-channels~~ allowing the service code to be sent to the identity module, e.g. a (U)SIM, in a secure way.

In one embodiment, the hardware of the terminal is
 25 configured in such a way that all incoming authentication requests for a network service will be routed via the radio card, so that the identity module receives for each incoming authentication request a service code. Such hardware architecture ensures that all incoming authentication requests
 30 are identified with respect to the communication channel the request was received by the terminal.

In yet another embodiment, the authentication request comprises authentication information, preferably a random challenge RAND, and the method further comprises the steps of:
 35 modifying the authentication information ~~on~~ the basis of the identified communications channel; generating, preferably using an authentication and key agreement (AKA) of a telecommunication telecommunications standard, an

authentication response RES on the basis of the modified authentication information. In a further embodiment the authentication request comprises authentication information, preferably a random challenge RAND, and the method further
 5 comprises the steps of: generating, preferably on the basis of an authentication and key agreement (AKA) of a telecommunication telecommunications standard, an authentication response RES; modifying the authentication parameter RES on the basis the identified communications
 10 channel. Hence, the invention is easy to implement in 2G or 3G type communications systems. It can be used without changing the existing AKA and only requires a few adaptations to the terminal ((U)SIM and radio card) and the network (AuC/HLR).

In one embodiment the method comprises the steps of:

15 sending an authentication data request via predetermined communications channel to the network; generating an expected service code XSC on the basis of the type of communications channel the authentication data request was sent to the network; determining on the basis of expected service code XSC
 20 an expected response XRES; comparing the expected response XRES with the authentication response RES of the terminal; and, determining the terminal to be in an un-trusted state if RES is not equal to XRES. The invention thus allows the network to check whether the service request send to the
 25 network and the authentication request received by the terminal are transmitted over the same communication channel. If this is not the case, then this is an indication for the network that the service request cannot be trusted. In that case, the network may take further action in order to examine
 30 whether the terminal is infected with malware. The invention thus provides an effective method to prevent a malware attack, especially a man-in-the-middle attack.

In one embodiment the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a wireless
 35 LAN interface, a digital enhanced cordless (DECT) radio interface or a data bus interface. The invention assigns a service code to these different interfaces thereby allowing the terminal to modify the response of the terminal and to

send ~~protected~~ encrypted information in the modified response to the network.

In another aspect the invention relates to a radio module for establishing a wireless communication channel between a terminal and a network. The radio module comprises: an RF interface comprising a RF amplifier connected to one or more antenna's for establishing a communication channel with a network; means for generating a service code (SC) for identifying the wireless connection and for sending the service code to the terminal; and, means for sending a signal received via the communication channel to the terminal.

In one embodiment the radio module further comprises: a signal convertor for converting a radio signal received via the wireless connection into a digital signal; means for inserting the service code into the digital signal; means for sending the digital signal to the terminal, preferably to an identity module in the terminal.

In a further aspect the invention relates to an identity module, preferably a smartcard, configured to receive signals from a radio module, preferably from a radio module as described above, wherein the identity module comprises: means for calculating a response RES - preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA - upon receipt of an authentication request, the authentication request preferably comprising a random challenge RAND; means for receiving a service code from the radio module; means for modifying the response RES on the basis of a predetermined mathematical function using the service code as an input parameter.

In yet a further aspect the invention relates to a terminal, preferably a mobile device, for accessing network services, the terminal comprising a radio module and an identity module as described above.

In another aspect the invention relates to a network node for service based authentication to a network, wherein the network node comprises: means for receiving an ~~service authentication data~~ request from a terminal; means for generating an expected service code XSC ~~based on the basis~~ the type of communication channel the ~~authentication data~~ service

request was sent to the network; means for generating an expected response XRES, preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA; and, means for modifying the expected response XRES on the basis of a predetermined mathematical function using the expected service code XSC as an input parameter.

In one embodiment the network node comprises: means for receiving a response RES from a terminal; means for comparing the response RES with the modified expected response XRES'.

The invention further relates to a system for service based authentication to a network, comprising: a terminal configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal; a network node configured to generate in response to the receipt of an authentication data ~~response RES' request~~ a modified expected response XRES' and configured to compare RES' with XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

The invention also relates to a computer program product comprising software code portions configured for, when run in the memory of a mobile device, executing the method steps as described above.

The invention will be further illustrated with reference to the attached drawings, which schematically will show embodiments according to the invention. It will be understood that the invention is not in any way restricted to these specific embodiments.

Brief description of the drawings

Fig. 1 depicts a schematic representation of a system according to one embodiment of the invention.

Fig. 2 illustrates a schematic flow diagram of the GSM authentication procedure and the UMTS authentication procedure.

Fig. 3 depicts a flow diagram according to one embodiment of the invention.

Fig. 4 illustrates how a fraudulent authentication procedure can be prevented by using the invention.

Detailed description

Fig. 1 illustrates a schematic representation of a communications system **100** according to one embodiment of the invention. The system comprises a terminal **102** connected to a communications network **104**. In one embodiment the network may be a 2G-type (e.g. GSM) mobile network comprising a base transceiver station (BTS) **106** serving as an access node. The BSC is connected via a base station controller (BSC) **108** to a mobile switching center (MSC) **110** of e.g. a visiting network (VN). The MSC is linked to a visited location register (VLR) **112**, which is a database that stores user related data and performs security functions. The MSC is further linked to an authentication centre (AuC) **114** and a home location register (HLR) **116** which is located in the home network (HN) where the user of the terminal **102** has a subscription with the network operator. The HLR **116** stores user related data, e.g. subscription related data, and co-operates with the MSC/VLR **110** to keep track of the location of the terminal. The HLR is connected to an authentication centre (AuC) **114**. The authentication centre (AuC) comprises (amongst others) algorithms for the calculation of authentication parameters used in the authentication procedure. For each subscriber the AuC stores a secret authentication key K which is also stored in an associated identity module, e.g. a (U)SIM card or the like, located in the terminal.

Alternatively, the network in Fig. 1 may also depict a 3G-type (e.g. UMTS) mobile network comprising 3G network elements. In that case, the network may comprise a radio base station (Node-B) **106** connected via a Radio Network

Commented [f2]: Ik heb deze passage wat gewijzigd omdat de MSC/VLR niet gekoppeld is aan het AuC, maar aan het HLR. Het AuC is weer gekoppeld aan het HLR, of is er een onderdeel van. Ik heb ook de figuur gewijzigd.

Controller (RNC) **108** to a Serving GPRS Support Node (SGSN) **110**. The SGSN is further connected to a VLR **112** and an AuC/HLR **114,116** in a similar way as in the 2G-type network as described above.

In a further embodiment the communications network **104** may comprise IMS-based network elements in the form of a set of Call/Session Control Functions (CSCF) such as a Proxy-CSCF (P-CSCF), an Interrogating-CSCF (I-CSCF), a Serving-CSCF (S-CSCF) and a Home Subscriber Server (HSS). In yet further embodiments the communications network may comprise 3GPP LTE or 3GPP SAE network elements.

The terminal **102** may be a personal computer or a mobile device such as a smart phone, a personal digital assistant (PDA), a laptop or any other mobile communications device capable of providing services over one or more networks. The terminal comprises a radio module **118**, an operating system (OS) **126** and an identity module **120**.

The radio module **118** acts as connection point to wired and wireless network services and comprises for that purpose a number of service interfaces. For example, for wireless services, it includes an RF interface comprising an RF receiver connect to one more antenna^s. **Fig. 1** depicts an exemplary implementation wherein the radio card provides radio contact with the base station **106**. The RF interface of the radio module is capable of receiving and/or transmitting RF signals in accordance with various wireless technologies (e.g. TDMA for GSM services, W-CDMA for UMTS services, IEEE 802.11 used for WiFi services, Bluetooth, DECT, etc.).

Similarly, for wired services, the radio module may comprise e.g. an Ethernet interface which allows the radio module to be connected to the network using a wired Ethernet communication channel. An access and configuration (AC) manager manages the set-up of a communication channel to an access node of a network or - in case of a short-range connection such as Bluetooth - to another terminal. The AC manager provides the RF interface or the Ethernet interface in the radio card with the correct parameters for operation under

a specific RF technology and/or protocol associated with the networks services requested by the terminal.

Commented [f3]: Nee, dit zijn vrijwel altijd allemaal verschillende modules.

The Operating System (OS) **126** of the terminal comprises a kernel which manages the resources of the mobile device e.g. the Central Processing Unit (CPU), memory for storing program instructions and data and Input/Output (I/O) devices such as the radio module. Further, the OS comprises Application Programming Interfaces (APIs) through which application programs **128** may access services offered by the OS. The OS may e.g. comprise a radio network API for setting up a radio connection with a mobile network.

The identity module **120**, which is typically removable, may be a UICC (Universal Integrated Circuit Card) for use in mobile devices suitable for 2G-type network services (GSM) or 3G-type network services, (UMTS). To that end, the UICC may comprise a Subscriber Identity Module (SIM) comprising SIM applications and/or a UMTS Subscriber Identity Module (USIM) comprising USIM applications. It is to be understood that the identity module is not limited to SIM and/or USIM applications. In further embodiments, the identity module may be an IP Multimedia Sub-system SIM (ISIM) for authenticating and accessing IMS-based services according to a predetermined IMS-based AKA as e.g. described in ETSI technical specification TS 33.203 or an extensible authentication protocol (EAP) based SIM for authentication and accessing a network according to a predetermined EAP-based AKA as described for instance in RFC4187.

The identity module may comprise a processor, one or more memory components e.g. ROM, RAM and/or EEPROM and I/O circuitry. For authentication purposes the UICC comprises a secret service-subscriber authentication key K and one or more algorithms for calculating a response comprising one or more authentication parameters upon the reception of a random challenge.

Fig. 2(a) illustrates a schematic flow diagram of the standard GSM authentication procedure which may be used by the SIM module in the identity module. In the GSM standard the MSC initiates, in response to a service request of a network

service originating from the terminal, a request for authentication data to the AuC/HLR (step **202**). A random number generator at the AuC/HLR generates a random value RAND that is input to the GSM A3/A8 algorithms which generate an expected response XRES and a cipher key K_c . The triplet {RAND, XRES, K_c } is returned to the MSC (step **204**) that subsequently forwards the RAND value to the SIM card of the terminal (step **206**). Corresponding calculations are performed by the terminal, typically by the integrity module, which returns a calculated response RES back to the MSC (step **208**). By comparison of the RES with the XRES the MSC can authenticate the terminal to the network.

In the standard UMTS authentication procedure similar steps as the GSM procedure are performed. However, in order to improve the security additional parameters and a set of eight functions f_0 - f_5 , f_1^* , f_2^* are used. **Fig. 2(b)** illustrates a schematic flow diagram of the UMTS authentication procedure, which may be used by a USIM module in the identity module. In response to a request for authentication data from the SGSN/VLR (step **210**), the AuC/HRL generates a random number RAND (using function f_0) and a fresh sequence number SQN. The AuC/HRL provides the secret authentication key K (which is both stored in the AuC and the USIM but never directly exchanged) and an operator specific Authentication Management Field AMF. These four parameters are fed into the five symmetric encryption functions f_1 - f_5 , resulting in five new parameters: the Message Authentication Code (MAC), the Expected Response (XRES), the Ciphering Key (CK), the Integrity Key (IK) and the Anonymity Key (AK). The sequence number SQN is separately encrypted into SQN^1 .

The AuC/HLR returns these parameters in an authentication vector (AV) {AUTN, RAND, XRES, CK, IK} to the SGSN/VLR (step **212**) wherein the Authentication token AUTN is a triplet { SQN^1 , AMF, MAC}. Thereafter, the SGSN/VLR forwards an Authentication and Ciphering request comprising RAND and AUTN to the mobile device (step **214**). Using RAND and AUTN the USIM calculates - amongst others - a response RES, which is sent

back to the SGSN (step 216) and compared with the XRES as received from the AuC/HLR.

The keys for ciphering and integrity checking have a limited lifetime to prevent attempts to break the cipher or integrity protection by brute force long duration monitoring attacks. Upon expiry, a new set of ciphering and integrity keys are generated with a re-authentication between the terminal and the network. This re-authentication process is regularly repeated.

The GSM AKA is described in detail in ETSI standards GSM 02.09 and GSM 03.20 and the UMTS AKA described in detail in ETSI technical specification TS 33.102, which are hereby incorporated by reference.

Now turning back to Fig. 1, the AC manager in the radio module 118 is configured to generate a service code (SC) identifying the specific service interface for setting up a wired or a wireless communication channel. To that end, the AC manager may use a look-up table comprising the different types of service interfaces supported by the mobile terminal and the associated service codes. The AC manager may be implemented in the form of a processor and one or more memory modules comprising e.g. the configuration data of the look-up table.

Preferably, the radio module is implemented in the form of one or more trusted hardware components. The hardware of the terminal is preferably configured in such a way that all incoming authentication requests for a network service will be routed via the radio card, so that the identity module receives for each incoming authentication request a service code and receives it in a secure way. Such hardware architecture ensures that all incoming authentication requests are identified with respect to the communication channel the request was received by the terminal.

If the terminal receives a signal via RF interface, the radio module translates the signal into a digital signal in accordance with the technical specifications of the wireless air interface selected by the AC manager. Thereafter, the AC manager selects the correct service code, inserts this code into the digital signal and sends it to the identity

Commented [f4]: Kunnen we dit nog generieker maken? Voor mij hoeft het niet de radio module te zijn die de Service Code genereert, als het maar een trusted module is, die bovendien veilig met de (U)SIM kan communiceren. Deze trusted module zou voor elk interface waarmee de challenge binnenkomt VEILIG de SC moeten kunnen toevoegen. Zie mijn nieuwe Figuur 6.

module for further processing (e.g. authentication and/or computation of the decryption key). Hence, the digital signal sent to the identity module comprises information via which service interface (and hence via which communications channel) the signal was received. Further variants for sending the service code to the identity module-integrity may include, e.g. sending the service code to the identity module in a separate signal.

Similarly, if the terminal receives a signal via the wired interface, the AC manager will select the service code for e.g. an Ethernet interface and inserts this code into the signal. This way, all wired and wireless incoming signals are routed via radio card to the other hardware components of the terminal such as the identity module.

The identity module such as a (U)SIM uses the service code during the authentication procedure as explained in relation to **Fig. 2**. If the (U)SIM receives an authentication request from the network via a particular interface, the (U)SIM may modify the calculated response RES on the basis of the service code.

In one embodiment the (U)SIM may modify the authentication information in the authentication request, e.g. a random challenge RAND, on the basis of the service code IC and subsequently calculate a response RES on the basis of an authentication and key agreement (AKA) of a telecommunications standard. For example, in the case of a GSM service the SIM may perform the steps: $RAND' = f(RAND, SC)$ and $RES' = A3(RAND', K_c)$, wherein f is a ~~secret~~, predetermined mathematical algorithm inserting/encrypting the information embodied in the service code into the response. The algorithm f is also known by the AuC/HLR in the network. In another variant, the SIM first calculates the response RES on the basis of the RAND and then modifies RES on the basis of S+C: $RES = A3(RAND, K_c)$ and $RES' = f(RES, SC)$. In the case of an UMTS service, the f1-f5 algorithms of the UMTS AKA are used instead of the A3 algorithm of the GSM AKA.

~~The~~ The mathematical algorithm f ~~must~~ be a so-called one-way function~~simple binary operation~~, e.g. a secure hash~~XOR~~

operation with the S~~+~~C. It allows the (U)SIM to inform the network about the communication channel (e.g. GSM, UMTS, Bluetooth, WiFi, etc.) the authentication request was received from~~by~~ the network in a way which is not, -detectable or at least very difficult, to modify~~detect~~ by malware. In order for the network to extract the channel information, the network, preferably the AuC/HLR, comprises - in addition to the functionality for determining the expected response according to a predetermined AKA - a service identification unit (SIU). A more detailed explanation of the SIU will be given in relation to **Fig. 3**.

Fig. 3 depicts a process flow between a UMTS network and a terminal comprising a USIM and a radio card (RC) as described in relation with **Fig. 1**. The process is started by a terminal application requesting a UMTS service from the network (step **302**). The request triggers the AC manager to configure the RF interface of the radio card to set-up up a wireless UMTS communication channel between the terminal and an access node of the requested UMTS network. Thereafter, an authentication data request is transmitted via the wireless communication channel and the SGSN/VLR to the AuC/HLR of the network. In response, the AuC/HLR generates a UMTS authentication vector AV and determines through which service interface (UMTS, GSM, WiFi, Bluetooth, etc.) contact was established with the terminal [Q: is this a standard procedure in UMTS; can we say something more about it? A: NO, it is not a standard interface. Hence a solution in which the AuC/HLR does not need to determine the service interface is better.]. The identified service interface information is forwarded to the SIU, which determines on the basis of the information on the identified service interface an expected service code XSC (step **304**). The SIU may determine XSC by retrieving the service code associated with the identified service interface (in this case a UMTS service) from a look-up table - substantially identical to the one used in the terminal - which is stored in a secure memory of the AuC/HLR. Depending on the specific scheme implemented in the USIM, the SUI which comprises the mathematical function f used by the USIM in the

Formatted: Highlight

terminal, may determine $RAND' = f(RAND, XSC)$ and send this value to the AuC/HLR for determining the expected response $XRES'$ on the basis the UMTS AKA using $RAND'$ as one of the input parameters, or alternatively, the AuC/HLR may first determine $XRES$ on the basis the UMTS AKA using $RAND$ as one of the input parameters and then send this value to the SUI for determining the expected response $XRES' = f(XRES, XSC)$.

In the next step (step 306) the AV is sent to the SGSN/VLR, which subsequently sends $RAND$ and $AUTN$ in an Authentication and Ciphering request via the wireless communication channel to the terminal (step 308). When the RC of the terminal receives the radio signal comprising the request via the RF interface, the signal is converted to a digital signal. Next, the AC manager identifies the service code and inserts it into the digital signal (step 310). This signal is forwarded to the USIM (step 312). The USIM responds by calculating RES using $RAND$ and SC as input parameters (step 314). To that end, the USIM may - for example - use a similar scheme as described above in relation with **Fig.1**, using the $f1-f5$ algorithms of the UMTS AKA. This way, the calculated RES will become specific for the service it is meant for.

The response RES is subsequently transmitted back via the radio card to the ~~SGSN/VLR~~AuC/HLR in the network (step 316) for comparison with an expected response $XRES'$ (step 318), which is determined by the network in a similar way as the USIM determines the RES .

~~Depending on the specific scheme implemented in the USIM, the SUI which comprises the secret mathematical function f used by the USIM in the terminal, may determine $RAND' = f(RAND, XSC)$ and send this value to the AuC/HLR for determining the expected response $XRES'$ on the basis the UMTS AKA using $RAND'$ as one of the input parameters, or alternatively, the AuC/HLR may first determine $XRES$ on the basis the UMTS AKA using $RAND$ as one of the input parameters and then send this value to the SUI for determining the expected response $XRES' = f(XRES, XSC)$.~~ Thereafter a comparison between the terminal response RES' and the expected response $XRES'$ is made. If RES' is equal to $XRES'$ then this provides an

indication for the network that the terminal received an authentication request via the communication channel that was expected by the network. In that case access to the network is granted.

If RES' is not equal to XRES' then this provides an indication to the network that the terminal received an authentication request via the communication channel different from the communication channel expected by the network. This may provide the network with an indication that the terminal may be corrupted by malware, in particular malware which allows a man-in-the-middle attack.

Fig. 4 represents a simplified schematic illustrating how the invention may prevent a fraudulent authentication procedure, wherein a first terminal **402** of an attacker remotely connects to an infected second terminal **404** of a victim and subsequently request and use authentication information from the (U)SIM **406** of the victim to obtain access to the network **408**.

The malware in the second terminal **404** allows the terminal of an attacker **402** to make a first communication channel **410**, e.g. a Bluetooth connection, with the infected terminal of the victim. Other types of connections such as a WiFi connection or a wired connection, such as an Ethernet connection, may also be possible. After connecting to the victim, the attacker starts an authentication procedure to the network by sending a ~~servicen authentication data~~ request via a second communication channel **412** to the AuC/HRL. In response, the attacker will receive an authentication request comprising - amongst others - RAND and AUTN. Instead of responding to the request, the attacker forwards the request to the victim using ~~via~~ the Bluetooth connection to the (U)SIM of the victim .

Normally, the (U)SIM cannot distinguish between requests originating from different communication channels (e.g. UMTS, GSM, WiFi, Bluetooth, etc.). In that case, the (U)SIM responds to the request by calculating a correct response RES, which is subsequently send via the Bluetooth connection (i.e. the communication connection where the

request came from) to the network. The attacker may use this RES to authenticate itself successfully to the network. Using this mechanism the attacker is capable of correctly answering each subsequent Authentication and Ciphering Request from the network.

If however the network and the infected terminal in **Fig.4** are configured as a communications system according to the invention as described in relation with **Fig.1**, the (U)SIM **406** is able to make a distinction between requests originating from different sources. In that case, the network **408** will determine an expected service code XSC on the basis of the request of the attacker. As the attacker requested a UMTS service via second communication channel **412**, it will set the XSC to the service code corresponding to a UMTS service. Similarly, the (U)SIM **406** of the infected terminal will modify the RES using the service code corresponding to a Bluetooth communications channel **410**. This modified RES' is send via the Bluetooth connection to the network, which will then determine that the XRES' calculated by the network on the basis of XSC does not match RES' because the communication channel used to send a request for a UMTS service to the network is different from the communication channel through which the terminal received the authentication request. In that case, the network may take appropriate action.

In one embodiment, the network may calculate the expected response values (XRES'', XRES''', etc.) for each service code available in the look-up table located in the AuC/HLR. If a XRES' value associated with a particular service code matches RES' then the source of the request received by the terminal may be determined.

This information may be used by the network to take appropriate action. It may e.g. provide no or limited access to the network or place the mobile device in a separate isolation or quarantine network in order to provide remediation services to the mobile device of the subscriber. If the response RES' is neither equal to XRES' nor to the other expected responses then the authentication procedure has failed.

It is to be understood that the invention may also be
sued with the IMS AKA (3GPP TS 33.203) in Generic
Bootstrapping (GBA) applications (see 3GPP TS 33.220, 33.222,
33.223) or with the EAP AKA and/or EAP SIM in WLAN

5 interworking applications. It can also be used in generic
access solutions to the mobile network (see 3GPP TS 43.318).

Further, it is to be understood that any feature
described in relation to any one embodiment may be used alone,
or in combination with other features described, and may also
10 be used in combination with one or more features of any other
of the embodiments, or any combination of any other of the
embodiments. Furthermore, equivalents and modifications not
described above may also be employed without departing from
the scope of the invention, which is defined in the
15 accompanying claims.

CLAIMS

1. Method for service-based authentication of a terminal to a network, the terminal comprising a number of communications interfaces, each communications interface allowing the terminal to set-up a predetermined communication channel with the network, the method comprising the steps of:

- sending a service request for access to a network service;
- receiving in response to the service request an authentication request from the network;
- identifying the communication channel through which the authentication request was received; and,
- sending an authentication response RES to the network, wherein the authentication response depends on the identified communication channel.

2. Method according to claim 1, the method further comprising the steps of:

- determining a service code associated with the identified communication channel;
- calculating the response RES on the basis of the information in the authentication request and the service code, thereby (cryptographically?) securely including encrypting information regarding identity of the communication channel through which the authentication request was received into the response.

3. Method according to claims 1 or 2, wherein the terminal comprises an identity module, preferably a removable identity module, and a radio module comprising a number of communications interfaces and configured to identify the communications channel through which the authentication request was received, the method further comprising the step of:

Commented [f5]: Zie de tekst in mijn mail. De highlighted claims passen wel bij de al beschreven uitvoeringsvoorbeelden maar niet bij mijn nieuwe voorkeurs-voorbeeld.

Formatted: Highlight

Formatted: Highlight

- the radio module sending an service code SC to the identity module, the service code identifying the communications channel through which the authentication request was received.

5

4. Method according to any of claims 1 to 3, wherein the authentication request comprises authentication information, preferably a random challenge RAND, the method further comprising the steps of:

Formatted: Highlight

10

- modifying the authentication information on the basis of the identified communications channel;
- generating, preferably using an authentication and key agreement (AKA) of a telecommunication telecommunications standard, an authentication response RES on the basis of the modified authentication information;

15

5. Method according to any of claims 1 to 3, wherein the authentication request comprises authentication information, preferably a random challenge RAND, the method further comprising the steps of:

20

- generating, preferably on the basis of an authentication and key agreement (AKA) of a telecommunication telecommunications standard, an authentication response RES;
- modifying the authentication parameter RES on the basis the identified communications channel;

25

6. Method according to any of claims 2-5, the method further comprising the steps of:

30

- sending an authentication data request via predetermined communications channel to the network;
- generating an expected service code XSC on the basis of the type of communications channel the authentication data request was sent to the network;
- determining on the basis of expected service code XSC an expected response XRES;
- comparing the expected response XRES with the authentication response RES of the terminal; and,

35

- determining the terminal to be in an un-trusted state if RES is not equal to XRES.

7. Method according to any of claims 1-6, wherein the terminal comprises a 2G or 3G type radio interface, a Bluetooth radio interface, a wireless LAN interface, a digital enhanced cordless (DECT) radio interface or a data bus interface.

8. Radio module for establishing a wireless communication channel between a terminal and a network, the radio module comprising:

- an RF interface comprising a RF amplifier connected to one or more antenna^s for establishing a communication channel with a network;
- means for generating a service code (SC) for identifying the wireless connection and for sending the service code to the terminal; and,
- means for sending a signal received via the communication channel to the terminal.

Commented [f6]: Kunnen we dit nog generieker maken? Voor mij hoeft het niet de radio module te zijn die de Service Code genereert, als het maar een trusted module is, die bovendien veilig met de (U)SIM kan communiceren. Deze trusted module zou voor elk interface waarmee de challenge binnenkomt VEILIG de SC moeten kunnen toevoegen. Zie mijn nieuwe Figuur 6.

9. Radio module according to claim 8, the radio module further comprising:

- a signal convertor for converting a radio signal received via the wireless connection into a digital signal;
- means for inserting the service code into the digital signal;
- means for sending the digital signal to the terminal, preferably to an identity module in the terminal.

Commented [f7]: Zelfde commentaar als bij Claim 8.

10. An identity module, preferably a smartcard, configured to receive signals from a radio module, preferably from a radio module as claimed in claims 8 or 9, the identity module comprising:

- means for calculating a response RES - preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA - upon receipt of an authentication request, the authentication request preferably comprising a random challenge RAND;

Formatted: Highlight

- means for receiving a service code from the radio module;
- means for modifying the response RES on the basis of a predetermined mathematical function using the service code as an input parameter.

5

11. A terminal, preferably a mobile device, for accessing network services, the terminal comprising a radio module according to claims 8 or 9 and an identity module according to claim 10.

Commented [f8]: Trusted?

10

12. Network node for service based authentication to a network, the network node comprising:

- means for receiving an ~~authentication data~~service request from a terminal;
- means for generating an expected service code XSC on the basis of the type of communication channel the ~~service authentication data~~ request was sent to the network;
- means for generating an expected response XRES, preferably according to a GSM AKA, a 3GPP AKA or an IMS AKA; and,
- means for modifying the expected response XRES on the basis of a predetermined mathematical function using the expected service code XSC as an input parameter.

25

13. Network node according to claim 12, the network node further comprising:

- means for receiving a response RES from a terminal;
- means for comparing the response RES with the modified expected response XRES'.

30

14. A system for service based authentication to a network, comprising:

- a terminal configured to send in response to an authentication request a modified response RES' to the network wherein the modification depends on the type of communication channel the authentication request was received by the terminal;

35

- a network node configured to generate in response to the receipt of an authentication data request a modified expected response XRES' and configured to compare RES' with XRES', wherein the modification of the expected response XRES depends on the type of communication channel the authentication data response was sent to the network.

15. A computer program product comprising software code portions configured for, when run in the memory of a mobile device, executing the method steps according to any of claims 1-5.

ABSTRACT

A method and a system for service-based
5 authentication of a terminal to a network is described,
wherein the terminal comprises a number of communications
interfaces, each communications interface allowing the
terminal to set-up a predetermined communication channel with
the network. The method comprises the steps of: sending a
10 service request for access to a network service; receiving in
response to the service request an authentication request from
the network; identifying the communication channel through
which the authentication request was received; and, sending an
authentication response RES to the network, wherein the
15 authentication response depends on the identified
communication channel.

20 + Fig. 1