Title: METHOD, APPARATUS, SYSTEM AND COMPUTER PROGRAM FOR KEY PARAMETER PROVISIONING

Abstract: A method includes receiving, for a specific user equipment, an inquiry for key generation-related information, and user equipment processing instruction information, generating first key information on the received user equipment processing instruction information, encrypting at least core-network related dynamic identity information based on the generated key information, and sending the key generation-related information comprising at least the encrypted core-network related dynamic identity information and the received user equipment processing instruction information. Also described is a method that includes receiving key generation-related information that has at least encrypted core-network related dynamic identity information and user equipment processing instruction information, generating first key information on the received user equipment processing instruction information, decrypting the received encrypted core-network related dynamic identity information based on the generated first key information, and deriving second key information based on the decrypted core-network related dynamic identity information.
METHOD, APPARATUS, SYSTEM AND COMPUTER PROGRAM FOR KEY PARAMETER PROVISIONING

FIELD OF THE INVENTION

The exemplary embodiments of this invention relate generally to authentication and security techniques, and more specifically to key parameter provisioning employing any NAF (Network Application Function) and UE (User equipment) using a GBA (Generic Bootstrapping Architecture) service. In particular, MBMS (multimedia broadcast / multicast service). Mobile TV (television) and Device Management are example services in which the key parameter provisioning according to the exemplary embodiments of this invention may be deployed.

BACKGROUND

3GPP (3rd Generation Partnership Project) MBMS Systems offering Mobile TV service are now requested by mobile operators. An MBMS may use, for security purposes, 3GPP Generic Bootstrapping Architecture (GBA) or broadcasting schemes in general, encompassing IP (Internet Protocol) TV and applications such as settop boxes, which may use also derivations of GBA, for example, extended with details to support core or other specific networks.

The 3GPP Generic Authentication Architecture (GAA) is based on mobile algorithms AKA (Authentication and Key Agreement Protocol) for 3GPP and CHAP (Challenge-Handshake Authentication Protocol), and CAVE (Cellular Authentication and Voice Encryption) for 3GPP2. GBA is also adapted for specific needs e.g. for cable network operators and considers their security protocol preferences. The usage of GBA for OMA (Open Mobile Alliance) Broadcast Content Protection and Multimedia Broadcast Multicast Service caused that a new 3GPP GBA specification was created (TS (Technical Specification) 33.223 GBA Push). GBA is a network and a device based security feature.
In the 3GPP TS 33.220 (e.g. BSF (Bootstrapping Server Function), GBA), section 4.4.1 1, the following definitions are given:

"When referring to GBA keys, the following keys are intended: Ks and NAF specific keys derived from the Ks.

When referring to NAF specific keys, the following keys are intended: Ks_ext/int_NAF (in GBAJJ (GBA with UICC (Universal Integrated Circuit Card) -based enhancements) context) (..), and any keys derived from these keys.

The notation Ks_(ext/int)_NAF refers to Ks_ext/int_NAF in GBAJJ context (..).

The notation Ks_(ext)_NAF refers to Ks_ext_NAF in GBAJJ context (..)."

According to 3GPP TS 33.223, sections 3.1 and 4.3.9, the term GBA-PUSH-INFO may contain data relevant for key derivation in GBA Push such as AUTN(*), RAND, NAFJD, B-TID. GBA-PUSH-INFO that may be sent, for example, via the Upa-reference point from the NAF to the UE. Furthermore, the B-TID (Bootstrapping Transaction Identifier) may be contained, for example, in the push message in order to correct possible reverse order cases of GBA-PUSH-INFO and push message protected by a security association generated from GBA-PUSH-INFO (in case that the GBA-PUSH-INFO and push message are sent separately). That is, B-TID may be usable, for example, as a key identifier in protocols used in the reference point Upa and Ua (to be described herein below).

Within 3GPP TS 33.223 it is currently assumed that the Bootstrapping Transaction Identifier (B-TID), which identifies the cryptographic key, is used for Ua-message identification (see, e.g., 3GPP Meeting Document of SA3#47 S3-070456) and is additionally transferred in Upa-messages. 3GPP TS 33.223 does not include any user identification in Upa. Furthermore, it can be assumed that a UE identity is transferred together with the Upa message, which is the message to deliver at least the GBA-PUSH-INFO.
SUMMARY OF THE EXEMPLARY EMBODIMENTS OF THIS INVENTION

In a first aspect the exemplary embodiments of this invention provide a method that includes: receiving user equipment processing instruction information and an inquiry for key generation-related information; generating first key information on the received user equipment processing instruction information; encrypting at least core-network related dynamic identity information; and replying to the inquiry with the key generation-related information comprising at least the encrypted core network related dynamic identity information and received user equipment processing instruction information.

In another aspect the exemplary embodiments of this invention provide a memory medium configured to store program instructions. The execution of the program instructions results in performing operations that comprise: receiving user equipment processing instruction information and an inquiry for key generation-related information; generating first key information on the received user equipment processing instruction information; encrypting at least core-network related dynamic identity information; and replying to the inquiry with the key generation-related information comprising at least the encrypted core network related dynamic identity information and received user equipment processing instruction information.

In another aspect the exemplary embodiments of this invention provide an apparatus that includes: a receiver configured to receive user equipment processing instruction information and a request for key generation-related information; a generator configured to generate first key information on the received user equipment processing instruction information; an encryptor configured to encrypt at least core-network related dynamic identity information; and a sender configured to respond to the request with the key generation-related information comprising at least the encrypted core network related dynamic identity information and received user equipment processing instruction information.

In a further aspect the exemplary embodiments of this invention provide an apparatus that includes: means for receiving user equipment processing instruction information and an
inquiry for key generation-related information; means for generating first key information on the received user equipment processing instruction information; means for encrypting at least core-network related dynamic identity information; and means for replying to the inquiry with the key generation-related information comprising at least the encrypted core network related dynamic identity information and received user equipment processing instruction information.

In a still further aspect the exemplary embodiments of this invention provide a method that includes: receiving user equipment processing instruction information and key generation-related information comprising at least encrypted core-network related dynamic identity information; generating first key information on the received user equipment processing instruction information; decrypting the received encrypted core-network related dynamic identity information; and deriving second key information based on the decrypted core-network related dynamic identity information.

In another aspect the exemplary embodiments of this invention provide a memory medium configured to store program instructions. The execution of the program instructions results in performing operations that comprise: receiving user equipment processing instruction information and key generation-related information comprising at least encrypted core-network related dynamic identity information; generating first key information on the received user equipment processing instruction information; decrypting the received encrypted core-network related dynamic identity information; and deriving second key information based on the decrypted core-network related dynamic identity information.

In a further aspect the exemplary embodiments of this invention provide an apparatus that includes: a receiver configured to receive user equipment processing instruction information and key generation-related information comprising at least encrypted core-network related dynamic identity information; a generator configured to generate first key information on the received user equipment processing instruction information; and a decryptor configured to decrypt the received encrypted core-network related dynamic identity information for use in deriving second key information based on the
decrypted core-network related dynamic identity information.

In a further aspect the exemplary embodiments of this invention provide an apparatus that comprises: means for receiving user equipment processing instruction information and key generation-related information comprising at least encrypted core-network related dynamic identity information; means for generating first key information on the received user equipment processing instruction information; means for decrypting the received encrypted core-network related dynamic identity information; and means for deriving second key information based on the decrypted core-network related dynamic identity information.

In a still further aspect the exemplary embodiments of this invention provide a method that includes: receiving user equipment processing instruction information and an inquiry for a generic bootstrapping architecture push information (GPI); generating first key information \(K_s_{(ext/int)_BSF}\) on the received user equipment processing instruction information; encrypting at least a network application function domain name server (NAF DNS) name, where an \(E_{GPI}\) portion of the GPI comprises the encrypted NAF DNS name; and replying to the inquiry with the \(E_{GPI}\) and received user equipment processing instruction information.

In a still further aspect the exemplary embodiments of this invention provide a method that includes: receiving a message comprising a generic bootstrapping architecture push information (GPI) pushed by a network application function (NAF) and user equipment processing instruction information, where an \(E_{GPI}\) portion of the GPI comprises an encrypted network application function domain name server (NAF DNS) name; generating first key information \(K_s_{(ext/int)_BSF}\) on the received user equipment processing instruction information; decrypting the received encrypted NAF DNS name; and deriving second key information \(K_s_{(ext/int)_NAF}\) based on the decrypted NAF DNS name.
BRIEF DESCRIPTION OF THE DRAWINGS

Exemplary embodiments of this invention are described below with reference to the accompanying drawings, in which:

Fig. 1 shows respective methods for key parameter provisioning according to the exemplary embodiments of the present invention; and

Fig. 2 shows respective apparatuses (e.g., a user equipment and NAF/BSF) for key parameter provisioning according to the exemplary embodiments of this invention.

DETAILED DESCRIPTION OF THE EXEMPLARY EMBODIMENTS

It is to be noted that for this description, abbreviations GPI (GBA Push Information), Ks_(ext/int)_BSF, Ks_(ext)_NAF, NAF DNS name etc. are examples for the key-generation-related information, first key information, second key information, core-network related dynamic identity information and unique user identity information that is stored in a database for further security purposes like authentication or application security) etc., respectively, without restricting the latter terms to the special technical or implementation details imposed to these abbreviations or to the baseline credential used for the service specific key derivation (i.e. Ks_(ext/int)_NAF).

The exemplary embodiments of the present invention are described with reference to Figs. 1 and 2.

First, however, it is noted that a main feature of GBA Push, and difference to GBA as outlined by 3GPP TS 33.220, may be considered to encompass the fact that 3GPP TS 33.223 may bootstrap keys for use within broadcast networks, i.e., unidirectional use such as network-initiated establishment of a security association between at least one network node and a UE or terminal, as an example. However, the use of GBA Push in a broadcast network needs special considerations with regard to the key derivation techniques that are used in 3GPP TS 33.220. One of these aspects may be the NAF Name that is used in the
cryptographic key derivation. It cannot be assumed that all broadcast networks use DNS (Domain Name Server) based names for the so-called Head-ends in a case where they would function as a NAF sending GBA Push messages. The use of GBA Push in the unidirectional mode does not rule out that there might be a potential back-channel that the UE may use, e.g., if the key delivery was unsuccessful.

For example, when performing broadcasting over an IP (Internet Protocol) network such as DVB-H (Digital Video Broadcasting-Handheld), no DNS names are used. Furthermore, it can be assumed that a user has no means to perform an uplink reverse DNS query to resolve the DNS name related to the source IP address. Also EPGs (electronic program guides) used in DVB-H do not contain mapping information of an IP address towards DNS names.

Hence, explicit DNS name transmission (along with the Ua security protocol identifier when it cannot be derived by some other means) might be considered as a solution to this problem, and may maintain some compatibility of the GBA push solution with UE-initiated GBA concepts.

However, transferring the NAF Identifier (in short NAF-ID, NAF DNS name and Ua protocol ID) may pose a privacy problem, if both the user identity and the NAF ID are visible in the clear when transmitted over the broadcast network. This type of operation may enable tracking of the user behavior and therefore may be objectionable.

In consideration of the foregoing, the exemplary embodiments of this invention provide enhanced key parameter provisioning.

For example, a first method can include:

- receiving, for a specific user equipment, an inquiry for key generation-related information, and user equipment processing instruction information;
- generating first key information on the received user equipment processing instruction information;
- encrypting at least core-network related dynamic identity information based on the generated key information; and
sending the key generation-related information comprising at least the encrypted core-network related dynamic identity information and the received user equipment processing instruction information.

The method can further include obtaining an authentication vector comprising at least one of a random number and cryptographic key material; and deriving generic key information for subsequent use in the generating of the key information. The method may further include obtaining a user identity token from a user database; and deriving generic key information for subsequent use in the generating of the key first information. The received user equipment processing instruction information may further comprise a mobile application identifier, and the method can further comprise generating second key information based on the received user equipment processing instruction information.

Further in accordance with the exemplary embodiments of this invention a second method comprises:

receiving key generation-related information comprising at least encrypted core-network related dynamic identity information and user equipment processing instruction information;

generating first key information on the received user equipment processing instruction information;

decrypting the received encrypted core-network related dynamic identity information based on the generated first key information; and

deriving second key information based on the decrypted core-network related dynamic identity information.

This method can further include, when receiving, receiving a first key generation identifier and, when generating, generating the first key information also on the received key generation identifier. A first key generation identifier may be preconfigured, and, when generating, the first key information may be generated also on the preconfigured key generation identifier. When receiving, a Ua message is received, and the method further comprises processing the received message based on the derived second key information, and the Ua message is secured and is packed with the key generation-related
Further in accordance with the foregoing methods, core-network related dynamic identity information comprises at least one of a network application function domain name server name and a Ua interface protocol identifier. The key generation-related information may comprise at least one of the following: a unique user identifier; at least one of a random number and a signed result; cryptographic key material; an encrypted portion of generic bootstrapping architecture push information; an integrity-protected portion of the generic bootstrapping architecture push information; derived first and second keys; a key lifetime; and at least one generic bootstrapping architecture user setting. The user equipment processing instruction information comprises at least one non-encrypted information element indicating mobility selection.

Further in accordance with the exemplary embodiments there can be a step of creating generic key information based on the authentication token, and the method can further include authenticating the integrity-protected portion of the generic bootstrapping architecture push information based on the first key information.

The foregoing methods may be performed as a result of the execution of computer program instructions that are stored in a computer-readable memory medium of any suitable type.

These exemplary embodiments further include a first apparatus that includes a receiver configured to receive an inquiry, for a specific user equipment, for key generation-related information, and user equipment processing instruction information; a generator configured to generate first key information on the user equipment processing instruction information received by the receiver; an encryptor configured to encrypt at least core-network related dynamic identity information based on the key information generated by the generator; and a sender configured to send the key generation-related information comprising at least the core-network related dynamic identity information encrypted by the encryptor and the user equipment processing instruction information received by the receiver.
The apparatus can further include an obtainer configured to obtain an authentication vector comprising one random number and cryptographic key material; and a deriver configured to derive generic key information for subsequent use in the generator configured to generate the key information.

The apparatus may further comprise an obtainer configured to obtain an user identity token from a user database; and a deriver configured to derive generic key information for subsequent use in the generator configured to generate the first key information.

The user equipment processing instruction information received by the receiver can further comprise a mobile application identifier, and where the generator is further configured to generate second key information on the user equipment processing instruction information received by the receiver.

These exemplary embodiments further include a second apparatus that includes a receiver configured to receive key generation-related information comprising at least encrypted core-network related dynamic identity information and user equipment processing instruction information; a generator configured to generate first key information on the user equipment processing instruction information received by the receiver; a decryptor configured to decrypt the encrypted core-network related dynamic identity information received by the receiver based on the first key information generated by the generator; and a deriver configured to derive second key information based on the core-network related dynamic identity information decrypted by the decryptor.

Further in accordance with this aspect the receiver is further configured to receive a first key generation identifier and the generator is further configured to generate the first key information also on the key generation identifier received by the receiver. A first key generation identifier is preconfigured, and the generator is further configured to generate the first key information also on the preconfigured key generation identifier.

The receiver is further configured to receive a Ua message, and the apparatus additionally
comprises a processor configured to process the message received by the receiver based on the derived second key information.

The apparatus can comprise one of a universal integrated circuit card and a secure memory, and an interface configured to provide at least a portion of the key generation-related information to the universal integrated circuit card or the secure memory.

Related to the foregoing apparatus the core-network related dynamic identity information comprises at least one of a network application function domain name server name and a Ua interface protocol identifier, and the key generation-related information comprises at least one of: a unique user identifier; one of at least one random number and a signed result; cryptographic key material; an encrypted portion of generic bootstrapping architecture push information; an integrity-protected portion of the generic bootstrapping architecture push information; derived first and second keys; a key lifetime; and at least one generic bootstrapping architecture user setting (GUSS). The user equipment processing instruction information comprises at least one non-encrypted information element indicating mobility selection.

The second apparatus can further comprise a creator configured to create generic key information based on the authentication token, and an authenticator configured to authenticate the integrity-protected portion of the generic bootstrapping architecture push information based on the first key information.

The first apparatus may be constituted by one of a bootstrapping server function and a network application function, while the second apparatus may be constituted by one of a user equipment, a mobile equipment and a universal integrated circuit card.

Further in accordance with these exemplary embodiments another apparatus includes means for receiving an inquiry, for a specific user equipment, for key generation-related information, and user equipment processing instruction information; means for generating first key information on the user equipment processing instruction information
received by the means for receiving; means for encrypting at least core-network related
dynamic identity information based on the key information generated by the means for
generating; and means for sending the key generation-related information comprising at
least the core-network related dynamic identity information encrypted by the means for
encrypting and the user equipment processing instruction information received by the
means for receiving.

Further in accordance with these exemplary embodiments a further apparatus includes
means for receiving key generation-related information comprising at least encrypted
core-network related dynamic identity information and user equipment processing
instruction information; means for generating first key information on the user equipment
processing instruction information received by the means for receiving; means for
decrypting the encrypted core-network related dynamic identity information received by
the means for receiving based on the first key information generated by the means for
generating; and means for deriving second key information based on the core-network
related dynamic identity information decrypted by the means for decrypting.

The use of these exemplary embodiments provides a number of advantages. For example,
there is no need to communicate the source IP-address from the IP-layer to a GBA client,
and thus there is no need to have inter-layer communication.

Further by example, the use of these exemplary embodiments provides an insensitivity to
changes in the IP address of the NAF, and is thus applicable to, for example, networks
with bad connectivity, where the IP address may change frequently.

Further by example, the use of these exemplary embodiments provides an invariance to
the location of the NAF. For example, proximity servers and firewalls do not pose an
additional problem if, for example, the NAF resides behind a firewall or a Network
Address Translation Traversal Server is used.

Further by example, the use of these exemplary embodiments provides a mitigation of
DoS (Denial of Service) attacks (since core IP addresses easily fall victim to such DoS
attacks).

Further by example, the use of these exemplary embodiments removes a requirement for both Ua-endpoints to implement an additional key derivation mechanism, and to select between them depending on the use case.

Further by example, the use of these exemplary embodiments removes a requirement, for example, to make change to a smart card in a terminal (such as UICC).

Fig. 1 shows respective methods for key parameter provisioning according to the exemplary embodiments of the invention. Signaling between elements is indicated in the horizontal direction, while time aspects between signaling are reflected in the vertical arrangement of the signaling sequence, as well as in the sequence numbers.

As shown in Fig. 1, a communication system 100 may comprise an access network 104 and user equipment UE 102. The access network 104 in turn may comprise a network application function NAF 101, a bootstrapping server function BSF 103 and an optional base station BS 104 for providing an access technology for the UE 102, as described herein below. It is to be noted that the NAF 101 and the BSF 103 may be separate functionalities communicating via the Zpn interface point, for example, in the access network 104. Alternatively, the NAF 101 and the BSF 103 may also be functionalities comprised, for example, in a single server (indicated by a dashed box around the symbols of the NAF 101 and the BSF 103). As a further alternative, the BSF 103 may be configured to act as a NAF 101. If the BSF 103 and the NAF 101 are co-located then the Zpn reference point may be eliminated. Without being restricted thereto, the following description only addresses the latter alternative for descriptive simplicity, and the reference sign "NAF/BSF 101" is used for describing the BSF 103 acting as the NAF 101.

In addition, the NAF 101 and the UE 102 may be configured to communicate, for example, an application protocol via the Ua reference point and, for example, an AKA protocol via the Upa reference point. The BS 104 may be situated in the signal path between the NAF 101 and the UE 102 for providing compliance with the access
technology of interest.

As shown in Fig. 1, according to a first method, in step S1-1, the NAF 101 (or NAF/BSF 101) may perform receiving an inquiry, for a specific user equipment, for key generation-related information (e.g. a GBA-PUSH-INFO GPI), and user equipment processing (security) instruction information (e.g., an indication of Upa usage).

In step S1-2, the NAF 101 may perform a step of generating first key information (e.g., Ks_(ext/int)_BSF) on the received user equipment processing instruction information (e.g., indication of Upa usage). As an optional input to this first key derivation procedure there are several different possibilities. For example, the BSF 103 name (and assigned specific Ua-protocol identity), or any other generally known (not privacy compromising) information (or pre-configured information) may be used as long as it is compliant with the NAF-ID format (and thus does not require changes to, for example, smart cards issued under 3GPP Release 6 or 3GPP Release 7 or, if used in a similar manner such as 2G GBA TR 33.920, then to subscriber identity module SIM cards). The key derivation may be performed in the BSF 103.

In step S1-3, the NAF 101 may perform encrypting at least core-network related dynamic identity information (e.g., encrypting the NAF DNS name, resulting in an encrypted portion of the GPI referenced as "E_GPI" hereinafter). The E_GPI may also comprise, for example, non-encrypted information. For example, information pertaining to selecting the endpoint of the bootstrapping ME or UICC (Upa-usage) or, for example, pertaining to the type of bootstrapping of the endpoint (e.g., permanent or short-lived keys) based on the generated key information (for example, Ks_(ext/int)_BSF).

In step S1-4, the NAF 101 may perform sending to the UE 102 the key generation-related information (e.g., pushing GPI) comprising at least the encrypted core network related dynamic identity information (e.g. encrypted NAF DNS name) and the received user equipment processing instruction information.

The UE 102, according to a second method, in step S2-1, may perform receiving the key
generation-related information (e.g., GPI pushed by the NAF/BSF 101) comprising at least the encrypted core-network related dynamic identity information (e.g. the E_GPI comprising the encrypted NAF DNS name) and the user equipment processing instruction information (e.g., indication of Upa usage).

5 In step S2-2, the UE 102 may perform generating first key information (e.g., Ks_(ext)_BSF remaining on a UICC within the UE 102) on the received user equipment processing instruction information (e.g., on the indication of Upa usage). As optional input to this first key derivation, there may be different possibilities. For example, the BSF name (and assigned specific Ua-protocol identity) or any other generally known (not privacy compromising) information, or preconfigured information, may be used so long as it complies with the NAF-ID format (and thus does not require changes to, for example, smart cards issued under 3GPP Release 6 or 3GPP Release 7, or used in a similar manner such as 2G GBA TR 33.920). It should be noted that the BSF name is used as a non-limiting example.

In step S2-3, the UE 102 may perform decrypting the received encrypted core-network related dynamic identity information (e.g., decrypting E_GPI, resulting in the DNS name of the NAF/BSF 101) based on the generated first key information (e.g. Ks_(ext)_BSF).

In step S2-4, the UE 102 may perform deriving second key information (e.g., Ks_(ext)_NAF) based on the decrypted core-network related dynamic identity information (e.g., DNS name of the NAF/BSF 101).

25 According to further embodiments and refinements of the above first method, in step S1-1-1, the NAF/BSF 101 may further perform obtaining an AV (authentication vector) that contains, for example, the master key data (also referred to as cryptographic key material hereinafter) used for further application specific credentials, comprising at least one random number (RAND), an authentication token (AUTN), an expected response (XRES), a cipher key (CK) and an integrity key (IK), and deriving generic key information (e.g. Ks) for subsequent use in the generating of the key information (e.g., Ks_(ext/int)_BSF) may be performed. Alternatively, a user identity token may be
obtained during the above-described obtaining. In addition, the received user equipment processing instruction information may further comprise a mobile application identifier (e.g., Ua-appli-id), such that in step SI-2-1 the NAF/BSF 101 may perform generating second key information (e.g. Ks_(ext/int)_NAF) based on the received user equipment processing instruction information.

In addition, in both the first and second methods the core-network related dynamic identity information may comprise a network application function domain name server (NAF DNS) name and/or a Ua interface protocol identifier. Furthermore, the key generation-related information (e.g., GPI) may comprise a unique user identifier, such as IMPI (internet protocol multimedia subsystem private user identity), IMPU (internet protocol multimedia subsystem public user identity) or other user identifier, at least one random number (RAND) or a signed result (SRES), cryptographic key material, the above mentioned encrypted portion of generic bootstrapping architecture push information (E_GPI), an integrity-protected portion of the generic bootstrapping architecture push information (called I_GPI hereinafter), derived first and second keys (Ks_(int/ext)_NAF), a key lifetime and/or at least one generic bootstrapping architecture user setting (GUSS). Moreover, the user equipment processing instruction information may comprise at least one non-encrypted information element (e.g. a bit) indicating Upa usage.

In addition, according to further embodiments and refinements of the above second method, in step S2-1-1 the UE 102 may further perform creating generic key information (Ks) based on the random number and the authentication token. Furthermore, in step S2-2-1, the UE 102 may perform authenticating the integrity-protected portion of the generic bootstrapping architecture push information (I_GPI) based on the first key information. Alternatively, in the receiving (step SI-1), a first key generation identifier may be received and, in the generating step, the first key information may be generated also on the received key generation identifier. Alternatively, the first key generation identifier may be preconfigured and, in the generating (step S1-2), the first key information may be generated also on the preconfigured key generation identifier. As an additional alternative, e.g. the UE 102 may further perform receiving of a Ua message,
and, in step S2-5, the UE 102 may further perform processing the received message (e.g., Ua message) based on the derived second key information (e.g. Ks_(ext)_NAF).

Fig. 2 shows respective apparatuses (e.g., NAF/BSF 101 and user equipment UE 102) for key parameter provisioning according to exemplar embodiments of this invention. As an example, the UE 102 may be a terminal with IP capability having access to the access network 104, wherein the UE 102 may further contain a given form of security module, such as a smart card, a separate chip, or a secure software module.

As shown in Fig. 2, the NAF 101 (or the BSF 103 acting as the NAF 101) may comprise a central processing unit CPU 1011, a memory 1012, a sender (Tx) 1013, a receiver (Rx) 1014, a generator 1015, an encryptor 1016, an optional deriver 1017 and at least one optional additional CPU 1011. It is to be noted that hereinafter, for description brevity, each reference to the CPU 1011 of the NAF/BSF may also refer to at least one of the at least one optional additional CPU 1011.

As indicated with the dashed extension of the functional block of the CPU 1011, the generator 1015, the encryptor 1016 and the optional deriver 1017 may be implemented, for example, as software running on the CPU 1011 or as separate entities. It is to be noted that the functionalities of the sender 1013 and the receiver 1014 may be separate entities as shown in Fig. 2, or may alternatively be performed by an integral transceiver (not shown).

The CPU 1011 may be configured to process various data inputs and to control the functions of the memory 1012, the sender 1013, the receiver 1014, the generator 1015, the encryptor 1016, the optional deriver 1017 and the at least one additional optional CPU 1011. The memory 1012 may serve for storing program instruction code (more generally code means) for carrying out the respective method according to the exemplary embodiments of this invention when run on the CPU 1011.

As described in conjunction with the respective method according to the embodiments of the invention, the receiver 1013 of the NAF/BSF 101 may be configured to receive an
inquiry for key generation-related information (e.g., GPI), and user equipment processing instruction information (e.g., indication of Upa usage).

It is to be noted that this inquiry may originate from another network element (not shown) in the access network 104.

The generator 1015 of the NAF/BSF 101 may be configured to generate first key information A1 (e.g. \text{Ks}_{(\text{ext/int})_{BSF}}) on the user equipment processing instruction information received by the receiver 1013.

The encryptor 1016 of the NAF/BSF 101 may then be configured to encrypt at least core-network related dynamic identity information (Dyn. ID info, e.g. encrypting the DNS name of the NAF/BSF 101, resulting in \text{E}_\text{GPI}) based on the key information A1 generated by the generator 1015.

The sender 1014 of the NAF/BSF 101 may be configured to send the key generation-related information (e.g. GPI) comprising at least the core-network related dynamic identity information (Encrypted dyn. ID info) encrypted by the encryptor 1015 and the user equipment processing instruction information (e.g. indicator for Upa usage) received by the receiver 1013.

As is also shown in Fig. 2, the UE 102 may comprise a CPU 1021, a memory 1022, a sender (Tx) 1023, a receiver (Rx) 1024, a generator 1025, a decryptor 1026, a deriver 1027, an optional creator 1028, an optional authenticator 1029 and an optional interface (I/F) 10210.

As indicated with the dashed extension of functional block of the CPU 1021, the generator 1025, the decryptor 1026, the deriver 1027, the optional creator 1028, the optional authenticator 1029 and the optional interface 10210 may be implemented as software running on the CPU 1021, or as separate entities. It is to be noted that the functionalities of the sender 1023 and the receiver 1024 may be separate entities as shown in Fig. 2, or may alternatively be performed by an integral transceiver (not shown).
The CPU 1021 may be configured to process various data inputs and to control the functions of the memory 1022, the sender 1023, the receiver 1024, the generator 1025, the decryptor 1026, the deriver 1027, the optional creator 1028, the optional authenticator 1029 and the optional interface 10210. The memory 1022 may serve for storing code means for carrying out e.g. the respective method according to the invention, when run on the CPU 1021.

As described in conjunction with the respective method according to the exemplary embodiments of the invention, the receiver 1023 of the UE 102 may be configured to receive, for a specific user equipment, key generation-related information (e.g. GPI) comprising at least encrypted core-network related dynamic identity information (e.g. E_GPI, encrypted NAF/BSF DNS name) and user equipment processing instruction information (e.g. indication of Upa usage). As an option, the receiver 1023 of the UE 102 may further be configured to receive a Ua message.

It is to be noted that this optional message (msg) may originate from the NAF/BSF 101. In this case the subsequent operations of generation, decryption, derivation and processing may result in a successful overall handling of the message (msg). Alternatively, the message (msg) may originate from another NAF/BSF 101 in the communication system 100. In this case the subsequent operations of generation, decryption, derivation and/or processing may fail partially or as a whole, thus resulting in an unsuccessful overall handling of the optional message (msg).

The generator 1025 of the UE 102 may be configured to generate first key information A2 (e.g., Ks_(ext)_BSF) on the user equipment processing instruction information (e.g. indication of Upa usage) received by the receiver 1023.

The decryptor 1026 of the UE 102 may be configured to then decrypt the encrypted core-network related dynamic identity information (e.g. decrypting E_GPI, resulting in NAF DNS name) received by the receiver 1023 based on the first key information A2 generated by the generator 1025.
The deriver 1027 of the UE 102 may be configured to derive second key information B2 (e.g. Ks_(ext)_NAF) based on the core-network related dynamic identity information (e.g. NAF DNS name) decrypted by the decryptor 1026.

According to further embodiments of the above NAF/BSF 101, e.g., the CPU 1011 in conjunction with the memory 1012 (constituting what may be considered as an obtainer) of the NAF/BSF 101 may further be configured to obtain an AV (authentication vector) that contains the master key data (also referred to as cryptographic key material) used for further application specific credentials, comprising at least one of at least one random number (RAND), an authentication token (AUTN), an expected response (XRES), a cipher key (CK) and an integrity key (IK). The optional deriver 1017 may be configured to derive generic key information (e.g., Ks, indicated by the dashed key symbol) for subsequent use in the generator 1015 configured to generate the key information A1 (e.g., Ks_(ext/int)_BSF). Alternatively, the obtainer may be configured to obtain a user identity token. In addition, the received user equipment processing instruction information may further comprise a mobile application identifier (e.g. Ua-appli-id), such that the generator 1015 may further be configured to generate second key information B1 (e.g., Ks_(ext/int)_NAF) based on the received user equipment processing instruction information. As an alternative, the generic key information (Ks) might also be based on 2G Authentication vector (2G authentication vectors (AV = RAND, SRES (Signed Response), Ke (Cipher Key))).

In addition, in both the NAF/BSF 101 and the UE 102 according to the present invention, the core-network related dynamic identity information (dyn. ID info) may comprise a network application function domain name server (e.g., NAF DNS) name and/or a Ua interface protocol identifier. Furthermore, the key generation-related information (e.g., GPI) may comprise a unique user identifier, such as IMPI, IMPU or other user identifier, at least one random number (RAND) or a signed result (SRES), cryptographic key material, the above mentioned encrypted portion of generic bootstrapping architecture push information (E_GPI), an integrity-protected portion of the generic bootstrapping architecture push information (I_GPI), derived first and second keys, a key lifetime and/or at least one generic bootstrapping architecture user setting (GUSS). The user
equipment processing instruction information may comprise at least one non-encrypted information element (e.g., a bit) indicating e.g. Upa usage.

In addition, according to further embodiments and refinements of the UE 102, the optional creator 1028 of the UE 102 may be configured to create generic key information (Ks, as indicated with the dashed key symbol) based on the random number (RAND) and the authentication token (AUTN). Furthermore, the optional authenticator 1029 of the UE 102 may be configured to authenticate the integrity-protected portion of the generic bootstrapping architecture push information (I_GPI) based on the first key information Al'. The first key information Al' may be key information corresponding to the key information A1 generated by the generator 1015 of the NAF/BSF 101. Alternatively, the receiver 1023 may be configured to receive a first key generation identifier and the generator 1025 may be configured to generate the first key information also on the key generation identifier received by the receiver 1023. Alternatively, the first key generation identifier may be preconfigured, and the generator 1025 may further be configured to generate the first key information also on the preconfigured key generation identifier. As an additional alternative, e.g., the CPU 1021 of the UE 102 may farther be configured to process the above-described optional message (e.g. Ua message) received by the receiver 1023 based on the second key information B2 (e.g. Ks_(exf)_NAF) derived by the deriver 1027.

In addition, the UE 102 may alternatively be constituted by a mobile equipment or a universal integrated circuit card. Moreover, the optional creator 1028 may also be constituted by a universal integrated circuit card being chipset-insertable into the UE 102 (indicated by the functional block of the optional creator 1028 extending to the functional block of the UE 102).

The UE 102 may further comprise the universal integrated circuit card (1028) or a secure memory (not shown), and the optional interface (10210) which may be configured to provide at least a portion of the key generation-related information (e.g., GPI or portion of the GPI) to the universal integrated circuit card or the secure memory.
The UE 102 may also be implemented as a chip or module.

The exemplary embodiments of this invention also provide a system comprising at least one of the NAF/BSF 101 and the UE 102 according to the present invention.

5

The exemplary embodiments of this invention may be summarized according to the following, without being restricted to the technical and implementation details given.

For the NAF-key derivation at the UE 102, the NAF ID needs to be available before the keys Ks_ext/int_NAF can be derived from Ks. Therefore, the latter keys are not useful for confidentially protecting the NAF ID. A possible solution to provide confidentiality protection of the NAF ID transfer is to use an additional key. An additional (intermediate) key derivation can be used for this purpose. As input to this key derivation, there are different possibilities. The BSF name (and assigned specific Ua-protocol identity) or any other generally known (not privacy compromising) information can be used as long as it complies with the NAF-ID format (and thus does not require additions to the previously issued UICC). This implies that this NAF ID compliant information be preconfigured in the UE (smartcard or ME for both GBA_ME and GBA_U) or be transferred/broadcasted before bootstrapping, as two examples. As this key derivation is to be performed in the BSF, a BSF name may be utilized. Otherwise, a name is added to the Zpn-request message. In addition, the keys that are derived at the BSF using the NAF-ID = BSF name are not transferred to the requesting NAF. This provides the property that the NAF will be unable to modify (for integrity protection of GPI) and read the protected parts of the GPI. In this case, the BSF acts as a trusted server, encrypting the NAF ID that needs to be transferred towards the UE. The NAF has no means to modify this data. A UE that has the possibility to resolve the NAF ID from an IP address is able to check and match this data. At the same time, the encrypted value serves as an authorization token (similar but not equal to an authenticated B-TID approach where this form of B-TID served as a means to check the involvement of the UE) that can be verified by the UE in order to prove that the sending NAF is authorized to push information to the UE. If the bootstrapping lifetime is in clear-text included in GPI and integrity protected by Ks_(ext)_BSF, then it allows to reject bootstrapping by a UE when a NAF would store
for too long the GPI in the network (by validating the lifetime before bootstrapping). A NAF sending falsified GPI with invalid RAND AUTN cannot be prevented, but the bootstrapping attempt will fail. A NAF sending a falsified GPI with a valid (but unused) RAND AUTN cannot be prevented, and this can result in a successful bootstrapping if that NAF is not allowed as a Push NAF than it also will be unable to integrity protect GPI and hence being detected by the UE (that NAF would use Zn-interface to request NAF keys as specified for 3GPP specification TS 33.220).

For correct key derivation, the DNS name and other key derivation data may need to be communicated to the user safely and be integrated into the key derivation procedure on the terminal and on the networks side. This mechanism may ensure both integrity protection of the transferred DNS name and ensure confidentiality protection (privacy). The security of a DNS name may be of importance to prevent a potential so-called phishing attack. The confidentiality protection may be important to avoid a situation that a user may be linked to a certain content via the NAF host name. The mechanism also has the property that the Broadcasting server (the NAF, which may be in a visited network) will be unable to modify the bootstrapping related data that are to be transmitted to the UE. This would allow that roaming users in other countries would be able to receive "unfiltered" information as usual.

The solutions according to the exemplary embodiments of this invention provide a mechanism to protect certain data in a network initiated GBA bootstrapping from tampering and observation. Especially when there is no underlying bearer network security (such as in broadcast mode networks), these embodiments are needed and important.

Other embodiments of this invention can also be provided.

For the purpose of the present invention as described herein above, it should be noted that an access technology may be any technology by means of which a user equipment can access an access network. Any present or future technology, such as WLAN (Wireless Local Access Network), Cable networks, WiMAX (Worldwide Interoperability for
Microwave Access), BlueTooth, Infrared, and the like may be used. It should be further noted that an access network may be any device, unit or means by which a mobile station entity or other user equipment may connect to and/or utilize services offered by the access network. Such services include, among others, data and/or (audio-) visual communication, data download, and so forth.

Generally, the exemplary embodiments of this invention also applicable in those network/terminal environments that rely on a data packet based transmission scheme according to which data are transmitted in data packets and which are, for example, based on the Internet Protocol IP. These exemplary embodiments are, however, not limited thereto, and any other present or future IP or mobile IP (MIP) version, or, more generally, a protocol following similar principles as (M)IPv4/6, is also applicable. A user equipment entity may be any device, unit or means by which a system user may experience services from an access network.

It is pointed out that those method steps likely to be implemented as software code portions, and being run using a processor, are software code independent and can be specified using any known or future developed programming language, so long as the overall functionality defined by the method steps is preserved.

Generally, any method step is suitable to be implemented as software or by hardware without changing the nature of the exemplary embodiments of this invention in terms of the functionality implemented.

Method steps and/or devices, units or means likely to be implemented as hardware components at a mobile station or network element or module thereof are hardware independent, and can be implemented using any known or future developed hardware technology, or any hybrids of these, such as MOS (Metal Oxide Semiconductor), CMOS (Complementary MOS), BiMOS (Bipolar MOS), BiCMOS (Bipolar CMOS), ECL (Emitter Coupled Logic), TTL (Transistor-Transistor Logic), etc., using for example ASIC (Application Specific IC (Integrated Circuit)) components, FPGA (Field-programmable Gate Arrays) components, CPLD (Complex Programmable Logic
Device) components or DSP (Digital Signal Processor) components.

In addition, any method steps and/or devices, units or means likely to be implemented as software components may, for example, be based on MBMS (Multimedia Broadcast Multicast Service); in particular, MBMS security-compliant software modules may be used. Although secured MBMS is used as an example for a secured service herein for descriptive purposes, any security architecture capable of, for example, authentication, authorization, keying and/or traffic protection may be applied.

Devices, units or means (e.g., user equipment, BSF, and NAF) can be implemented as individual devices, units or means, but this does not exclude that they are implemented in a distributed fashion throughout the system, as long as the functionality of the device, unit or means is preserved.

Further, the various names used for the described parameters, functions, message types, interfaces and the like (e.g., BSF, GPI, Ks_(ext/int)_BSF, etc.) are not intended to be limiting or convey any other specific. All these parameters, functions, message types, interfaces and the like may be identified by any suitable names.

It should be noted that the terms "connected," "coupled," or any variant thereof, mean any connection or coupling, either direct or indirect, between two or more elements, and may encompass the presence of one or more intermediate elements between two elements that are "connected" or "coupled" together. The coupling or connection between the elements can be physical, logical, or a combination thereof. As employed herein, two elements may be considered to be "connected" or "coupled" together by the use of one or more wires, cables and/or printed electrical connections, as well as by the use of electromagnetic energy, such as electromagnetic energy having wavelengths in the radio frequency region, the microwave region and the optical (both visible and invisible) region, as several nonlimiting and non-exhaustive examples.

Furthermore, some of the features of the various non-limiting and exemplary embodiments of this invention may be used to advantage without the corresponding use
of other features. As such, the foregoing description should be considered as merely illustrative of the principles, teachings and exemplary embodiments of this invention, and not in limitation thereof.
CLAIMS

What is claimed is:

1. A method, comprising:

receiving user equipment processing instruction information and an inquiry for key generation-related information;

generating first key information on the received user equipment processing instruction information;

encrypting at least core-network related dynamic identity information; and

replying to the inquiry with the key generation-related information comprising at least the encrypted core network related dynamic identity information and received user equipment processing instruction information.

2. The method of claim 1, where the inquiry for key-generation related information comprises a GBA-PUSH-INFO generic bootstrapping architecture push information (GPI).

3. The method of claim 1, where the user equipment processing instruction information comprises an indication of Upa usage.

4. The method of claim 1, where generating the first key information considers a bootstrapping server function (BSF) name and assigned specific Ua-protocol identity.

5. The method of claim 1, where the first key information comprises Ks_(ext/int)_BSF, where the core-network related dynamic identity information comprises a network application function domain name server (NAF DNS) name, where encrypting encrypts the NAF DNS name based on the generated Ks_(ext/int)_BSF, resulting in an encrypted
portion (E_GPI) of a generic bootstrapping architecture push information (GPI).

6. The method of claim 5, where the E_GPI also comprises non-encrypted information.

7. The method of claim 6, where the non-encrypted information comprises Upa-usage.

8. The method of claim 6, where the non-encrypted information comprises universal integrated circuit card (UICC) selection information.

9. The method of claim 1, where generating comprises obtaining an authentication vector (AV).

10. The method of claim 9, where the AV comprises cryptographic key material comprising at least one of a random number (RAND), an authentication token (AUTN), an expected response (XRES), a cipher key (CK) and an integrity key (IK) for use in generating the first key information.

11. The method of claim 1, where the received user equipment processing instruction information comprises a mobile application identifier (UA-appli-Id).

12. The method of claim 1, where the core-network related dynamic identity information comprises at least one of a network application function domain name server (NAFDNS) name and a UA interface protocol identifier.

13. The method of claim 1, where the key generation-related information comprises a unique user identifier.

14. The method of claim 1, where the key generation-related information comprises an internet protocol multimedia subsystem private user identity (IMPI) or an internet protocol multimedia subsystem public user identity (IMPU).

15. The method of claim 1, where the key generation-related information comprises at
least one of a random number and a signed result; cryptographic key material; an encrypted portion of generic bootstrapping architecture push information; an integrity-protected portion of the generic bootstrapping architecture push information; derived first and second keys; a key lifetime; and at least one generic bootstrapping architecture user setting.

16. The method of claim 1, where the user equipment processing instruction information comprises at least one non-encrypted information element indicating mobility selection.

17. A memory medium configured to store program instructions, the execution of which results in performing operations that comprise:

receiving user equipment processing instruction information and an inquiry for key generation-related information;

generating first key information on the received user equipment processing instruction information;

encrypting at least core-network related dynamic identity information; and

replying to the inquiry with the key generation-related information comprising at least the encrypted core network related dynamic identity information and received user equipment processing instruction information.

18. The memory medium of claim 17, where the inquiry for key-generation related information comprises a GBA-PUSH-INFO generic bootstrapping architecture push information (GPI).

19. The memory medium of claim 17, where the user equipment processing instruction information comprises an indication of Upa usage.

20. The memory medium of claim 17, where generating the first key information
considers a bootstrapping server function (BSF) name and assigned specific Ua-protocol identity.

21. The memory medium of claim 17, where the first key information comprises $K_s_{(ex/int)}_{BSF}$, where the core-network related dynamic identity information comprises a network application function domain name server (NAF DNS) name, where encrypting encrypts the NAF DNS name based on the generated $K_s_{(ex/int)}_{BSF}$, resulting in an encrypted portion (E_GPI) of a generic bootstrapping architecture push information (GPI).

22. The memory medium of claim 21, where the E_GPI also comprises non-encrypted information.

23. The memory medium of claim 22, where the non-encrypted information comprises Upa-usage.

24. The memory medium of claim 22, where the non-encrypted information comprises universal integrated circuit card (UICC) selection information.

25. The memory medium of claim 17, where generating comprises obtaining an authentication vector (AV).

26. The memory medium of claim 25, where the AV comprises cryptographic key material comprising at least one of a random number (RAND), an authentication token (AUTN), an expected response (XRES), a cipher key (CK) and an integrity key (IK) for use in generating the first key information.

27. The memory medium of claim 17, where the received user equipment processing instruction information comprises a mobile application identifier Ua-appli-id.

28. The memory medium of claim 17, where the core-network related dynamic identity information comprises at least one of a network application function domain name server
(NAF DNS) name and a Ua interface protocol identifier.

29. The memory medium of claim 17, where the key generation-related information comprises a unique user identifier.

30. The memory medium of claim 17, where the key generation-related information comprises an internet protocol multimedia subsystem private user identity (IMPI) or an internet protocol multimedia subsystem public user identity (IMPU).

31. The memory medium of claim 17, where the key generation-related information comprises at least one of a random number and a signed result; cryptographic key material; an encrypted portion of generic bootstrapping architecture push information; an integrity-protected portion of the generic bootstrapping architecture push information; derived first and second keys; a key lifetime; and at least one generic bootstrapping architecture user setting.

32. The memory medium of claim 17, where the user equipment processing instruction information comprises at least one non-encrypted information element indicating mobility selection.

33. The memory medium of claim 17, embodied in a bootstrapping server function (BSF).

34. The memory medium of claim 17, embodied in an integrated circuit chip or module.

35. An apparatus, comprising:

a receiver configured to receive user equipment processing instruction information and a request for key generation-related information;

a generator configured to generate first key information on the received user equipment processing instruction information;
an encryptor configured to encrypt at least core-network related dynamic identity information; and

a sender configured to respond to the request with the key generation-related information comprising at least the encrypted core network related dynamic identity information and received user equipment processing instruction information.

36. The apparatus of claim 35, where the request for key-generation related information comprises a GBA-PUSH-INFO generic bootstrapping architecture push information (GPI).

37. The apparatus of claim 35, where the user equipment processing instruction information comprises an indication of Upa usage.

38. The apparatus of claim 35, where said generator when generating the first key information considers a bootstrapping server function (BSF) name and assigned specific Ua-protocol identity.

39. The apparatus of claim 35, where the first key information comprises $K_{s_{(ext/int)}}$ BSF, where the core-network related dynamic identity information comprises a network application function domain name server (NAF DNS) name, where encrypting encrypts the NAF DNS name based on the generated $K_{s_{(ext/int)}}$ BSF, resulting in an encrypted portion ($E_{GPI}$) of a generic bootstrapping architecture push information (GPI).

40. The apparatus of claim 39, where the $E_{GPI}$ also comprises non-encrypted information.

41. The apparatus of claim 39, where the non-encrypted information comprises Upa-usage.
42. The apparatus of claim 39, where the non-encrypted information comprises universal integrated circuit card (UICC) selection information.

43. The apparatus of claim 35, where said generator is further configured to obtain an authentication vector (AV).

44. The apparatus of claim 43, where the AV comprises cryptographic key material comprising at least one of a random number (RAND), an authentication token (AUTN), an expected response (XRES), a cipher key (CK) and an integrity key (IK) for use in generating the first key information.

45. The apparatus of claim 35, where the received user equipment processing instruction information comprises a mobile application identifier Ua-appli-id.

46. The apparatus of claim 35, where the core-network related dynamic identity information comprises at least one of a network application function domain name server (NAF DNS) name and a Ua interface protocol identifier.

47. The apparatus of claim 35, where the key generation-related information comprises a unique user identifier.

48. The apparatus of claim 35, where the key generation-related information comprises an internet protocol multimedia subsystem private user identity (IMPI) or an internet protocol multimedia subsystem public user identity (IMPU).

49. The apparatus of claim 35, where the key generation-related information comprises at least one of a random number and a signed result; cryptographic key material; an encrypted portion of generic bootstrapping architecture push information; an integrity-protected portion of the generic bootstrapping architecture push information; derived first and second keys; a key lifetime; and at least one generic bootstrapping architecture user setting.
50. The apparatus of claim 35, where the user equipment processing instruction information comprises at least one non-encrypted information element indicating mobility selection.

51. The apparatus of claim 35, embodied in a bootstrapping server function (BSF).

52. The apparatus of claim 35, embodied in an integrated circuit chip or module.

53. An apparatus, comprising:

means for receiving user equipment processing instruction information and an inquiry for key generation-related information;

means for generating first key information on the received user equipment processing instruction information;

means for encrypting at least core-network related dynamic identity information; and

means for replying to the inquiry with the key generation-related information comprising at least the encrypted core network related dynamic identity information and received user equipment processing instruction information.

54. The apparatus of claim 53, where the inquiry for key-generation related information comprises a GBA-PUSH-INFO generic bootstrapping architecture push information (GPI), where the user equipment processing instruction information comprises an indication of Upa usage.

55. The apparatus of claim 53, where the first key information comprises $K_s_{(ext/int)}_{BSF}$, where the core-network related dynamic identity information comprises a network application function domain name server (NAF DNS) name, where said encrypting means encrypts the NAF DNS name based on the generated $K_s_{(ext/int)}_{BSF}$, resulting in an encrypted portion (E_GPI) of a generic bootstrapping
architecture push information (GPI), where the E_GPI also comprises non-encrypted information.

56. The apparatus of claim 53, where the core-network related dynamic identity information comprises at least one of a network application function domain name server (NAF DNS) name and a Ua interface protocol identifier.

57. The apparatus of claim 53, embodied in an access network coupled with the user equipment through a base station.

58. The apparatus of claim 53, embodied in a bootstrapping server function (BSF).

59. The apparatus of claim 53, embodied in an integrated circuit chip or module.

60. A method, comprising:
receiving user equipment processing instruction information and key generation-related information comprising at least encrypted core-network related dynamic identity information;

   generating first key information on the received user equipment processing instruction information;

   decrypting the received encrypted core-network related dynamic identity information; and

   deriving second key information based on the decrypted core-network related dynamic identity information.

61. The method of claim 60, where the received key-generation related information comprises a generic bootstrapping architecture push information (GPI) pushed by a network application function (NAF).

62. The method of claim 60, where the encrypted core-network related dynamic identity
information includes an encrypted portion (E_GPI) of a generic bootstrapping architecture push information (GPI), said E_GPI comprising an encrypted network application function domain name server (NAF DNS) name, and where the user equipment processing instruction information comprises an indication of Upa usage.

63. The method of claim 60, where generating the first key information employs Ks_(ext)_BSF remaining on a universal integrated circuit card (UICC) within the user equipment.

64. The method of claim 60, where generating the first key information considers a bootstrapping server function (BSF) name and assigned specific Ua-protocol identity.

65. The method of claim 60, where decrypting the received encrypted core-network related dynamic identity information decrypts an encrypted generic bootstrapping architecture push information (GPI) based on the generated first key information, resulting in a DNS name of a network application function (NAF).

66. The method of claim 60, where deriving second key information derives Ks_(ext)_NAF.

67. The method of claim 60, where the core-network related dynamic identity information comprises at least one of a network application function domain name server (NAF DNS) name and a Ua interface protocol identifier.

68. The method of claim 60, where the key generation-related information comprises a unique user identifier.

69. The method of claim 60, where the key generation-related information comprises an internet protocol multimedia subsystem private user identity (IMPI) or an internet protocol multimedia subsystem public user identity (IMPU).

70. The method of claim 60, where the key generation-related information comprises at
least one of a random number and a signed result; cryptographic key material; an encrypted portion of generic bootstrapping architecture push information; an integrity-protected portion of the generic bootstrapping architecture push information; derived first and second keys; a key lifetime; and at least one generic bootstrapping architecture user setting.

71. The method of claim 60, where the user equipment processing instruction information comprises at least one non-encrypted information element indicating mobility selection.

72. A memory medium configured to store program instructions, the execution of which results in performing operations that comprise:

receiving user equipment processing instruction information and key generation-related information comprising at least encrypted core-network related dynamic identity information;

generating first key information on the received user equipment processing instruction information;

decrypting the received encrypted core-network related dynamic identity information; and

deriving second key information based on the decrypted core-network related dynamic identity information.

73. The memory medium of claim 72, where the received key-generation related information comprises a generic bootstrapping architecture push information (GPI) pushed by a network application function (NAF).

74. The memory medium of claim 72, where the encrypted core-network related dynamic identity information includes an encrypted portion (E_GPI) of a generic bootstrapping architecture push information (GPI), said E_GPI comprising an encrypted network application function domain name server (NAF DNS) name, and where the user
equipment processing instruction information comprises an indication of Upa usage.

75. The memory medium of claim 72, where generating the first key information employs Ks_(ext)_BSF remaining on a universal integrated circuit card (UICC) within the user equipment.

76. The memory medium of claim 72, where generating the first key information considers a bootstrapping server function (BSF) name and assigned specific Ua-protocol identity.

77. The memory medium of claim 72, where decrypting the received encrypted core-network related dynamic identity information decrypts an encrypted generic bootstrapping architecture push information (GPI) based on the generated first key information, resulting in a DNS name of a network application function (NAF).

78. The memory medium of claim 72, where deriving second key information derives Ks_(ext)_NAF.

79. The memory medium of claim 72, where the core-network related dynamic identity information comprises at least one of a network application function domain name server (NAF DNS) name and a Ua interface protocol identifier.

80. The memory medium of claim 72, where the key generation-related information comprises a unique user identifier.

81. The memory medium of claim 72, where the key generation-related information comprises an internet protocol multimedia subsystem private user identity (IMPI) or an internet protocol multimedia subsystem public user identity (IMPU).

82. The memory medium of claim 72, where the key generation-related information comprises at least one of a random number and a signed result; cryptographic key material; an encrypted portion of generic bootstrapping architecture push information; an
integrity-protected portion of the generic bootstrapping architecture push information; derived first and second keys; a key lifetime; and at least one generic bootstrapping architecture user setting.

83. The memory medium of claim 72, where the user equipment processing instruction information comprises at least one non-encrypted information element indicating mobility selection.

84. An apparatus, comprising:

a receiver configured to receive user equipment processing instruction information and key generation-related information comprising at least encrypted core-network related dynamic identity information;

a generator configured to generate first key information on the received user equipment processing instruction information; and

a decryptor configured to decrypt the received encrypted core-network related dynamic identity information for use in deriving second key information based on the decrypted core-network related dynamic identity information.

85. The apparatus claim 84, where the received key-generation related information comprises a generic bootstrapping architecture push information (GPI) pushed by a network application function (NAF).

86. The apparatus claim 84, where the encrypted core-network related dynamic identity information includes an encrypted portion (E_GPI) of a generic bootstrapping architecture push information (GPI), said E_GPI comprising an encrypted network application function domain name server (NAF DNS) name, and where the user equipment processing instruction information comprises an indication of Upa usage.

87. The apparatus claim 84, where said generator generates the first key information at
least partially in accordance with $K_{s\,(ext)}\_BSF$ remaining on a universal integrated circuit card (UICC) within a user equipment.

88. The apparatus claim 84, where said generator generates the first key information at least partially in accordance with a bootstrapping server function (BSF) name and assigned specific Ua-protocol identity.

89. The apparatus claim 84, where said decryptor decrypts an encrypted generic bootstrapping architecture push information (GPI) based on the generated first key information, resulting in a DNS name of a network application function (NAF).

90. The apparatus claim 84, where derived second key information comprises $K_{s\,(ext)}\_NAF$.

91. The apparatus claim 84, where the core-network related dynamic identity information comprises at least one of a network application function domain name server (NAF DNS) name and a Ua interface protocol identifier.

92. The apparatus claim 84, where the key generation-related information comprises a unique user identifier.

93. The apparatus claim 84, where the key generation-related information comprises at least one of a random number and a signed result; cryptographic key material; an encrypted portion of generic bootstrapping architecture push information; an integrity-protected portion of the generic bootstrapping architecture push information; derived first and second keys; a key lifetime; and at least one generic bootstrapping architecture user setting.

94. The apparatus claim 84, where the user equipment processing instruction information comprises at least one non-encrypted information element indicating mobility selection.

95. The apparatus of claim 84, embodied in an integrated circuit chip or module.
96. An apparatus, comprising:

means for receiving user equipment processing instruction information and key generation-related information comprising at least encrypted core-network related dynamic identity information;

means for generating first key information on the received user equipment processing instruction information;

means for decrypting the received encrypted core-network related dynamic identity information; and

means for deriving second key information based on the decrypted core-network related dynamic identity information.

97. The apparatus of claim 96, where the received key-generation related information comprises a generic bootstrapping architecture push information (GPI) pushed by a network application function (NAF).

98. The apparatus of claim 96, where the encrypted core-network related dynamic identity information includes an encrypted portion (E_GPI) of a generic bootstrapping architecture push information (GPI), said E_GPI comprising an encrypted network application function domain name server (NAF DNS) name, and where the user equipment processing instruction information comprises an indication of Upa usage.

99. The apparatus of claim 96, where said decrypting means decrypts an encrypted generic bootstrapping architecture push information (GPI), resulting in a DNS name of a network application function (NAF), and where said second key information comprises Ks_(ext)_NAF.

100. The apparatus of claim 96, where the core-network related dynamic identity
information comprises at least one of a network application function domain name server (NAF DNS) name and a Ua interface protocol identifier, and where the key generation-related information comprises a unique user identifier.

101. The apparatus of claim 96, embodied in an integrated circuit chip or module.

102. The apparatus of claim 96, where the means for decrypting is further for decrypting the received encrypted core-network related dynamic identity information based on the generated first key information.

103. A method, comprising:
receiving user equipment processing instruction information and an inquiry for a generic bootstrapping architecture push information (GPI);

  generating first key information (Ks_(ext/int)_BSF) on the received user equipment processing instruction information;

  encrypting at least a network application function domain name server (NAF DNS) name, where an E_GPI portion of the GPI comprises the encrypted NAF DNS name; and

  replying to the inquiry with the E_GPI and received user equipment processing instruction information.

104. A method, comprising:
receiving a message comprising a generic bootstrapping architecture push information (GPI) pushed by a network application function (NAF) and user equipment processing instruction information, where an E_GPI portion of the GPI comprises an encrypted network application function domain name server (NAF DNS) name;

  generating first key information (Ks_(ext/int)_BSF) on the received user equipment processing instruction information;
decrypting the received encrypted NAF DNS name; and

deriving second key information (Ks_(ext/int)_NAF) based on the decrypted NAF DNS name.
Fig. 1

Access network 104

UE 102

BoS 104

BSF

NAF

Zpn

S1-1: Receiving
Inquiry (key-gen. rel. info, e.g. GPI and Upa usage = UICC / ME)

(S1-1-1: Obtaining AV, e.g. RAND || AUTN || XRES || CK || IC deriving KS)

S1-2: Generating 1st key information, e.g.
KS_(ext/int)_BSF (with BSF acting as NAF and Ua-appl_id = 'GBA_push')

(S1-2-1: Generating 2nd key information, e.g.
KS_(ext/int)_NAF (with Ua-appl_id as received e.g. via Zpn)

S1-3: Encrypting core-nw rel. dyn. ID info with key information, e.g.
At least NAF DNS name with KS_(ext/int)_BSF dependent on Upa-usage →
E_GPI equals the encrypted part of GBA_PUSH_INFO and includes e.g. non-
encrypted information e.g. on selecting the endpoint of the bootstrapping i.e.
ME or UICC (Upa-usage) or e.g. on the type of bootstrapping of the endpoint
(e.g. permanent or short-lived keys)

S1-4: Sending key-gen. rel. info (encrypted core-nw rel. dyn. ID info +
UE proc. Inst. info), e.g.
BSF replies to the NAF Zpn request by sending GPI = IMPI || RAND || AUTN
|| E_GPI || l_GPI and KS_(ext/int)_NAF; Key Lifetime, GUSS* to the NAF;
GPI may be integrity-protected e.g. by using KS_(ext/int)_BSF → l_GPI

S2-1: Receiving key-gen. rel. info (encrypted core-nw rel. dyn. ID info + UE proc. Inst. Info
+ optional Ua message), e.g. Rec. GPI (Upa usage = e.g. ME) and Ua mess.

(S2-1-1: Creating generic key information e.g. based on RAND and AUTN, e.g.
ME sends RAND, AUTN to UICC to create KS)

S2-2: Generating 1st key information on UE-specific proc. Inst. Info, e.g. ME initiates
KS_(ext/int)_BSF derivation (with BSF acting as NAF and Ua-appl_id = 'GBA-Push')

(S2-2-1: Authenticating integrity-protected based on 1st key information, e.g.
ME verifies l_GPI using KS_(ext/int)_BSF)

S2-3: Decrypting encr. core-nw rel. dyn. ID info based on 1st key info, e.g.
ME decrypts (at least) NAF DNS name with KS_(ext/int)_BSF

S2-4: Deriving 2nd key info based on decr. core-nw rel, e.g.
ME initiates KS_(ext/int)_NAF derivation using NAF name (and Ua-appl-id)

(S2-5: Processing message based on 2nd key info, e.g.
ME processes e.g. Ua messages using KS_(ext/int)_NAF)