International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

J.366.9

(11/2006)

SERIES J: CABLE NETWORKS AND TRANSMISSION OF TELEVISION, SOUND PROGRAMME AND OTHER MULTIMEDIA SIGNALS

IPCablecom

IPCablecom2 IP Multimedia Subsystem (IMS): Generic authentication architecture specification

ITU-T Recommendation J.366.9

ITU-T Recommendation J.366.9

IPCablecom2 IP Multimedia Subsystem (IMS): Generic authentication architecture specification

Summary

This Recommendation describes the security features and a mechanism to bootstrap authentication and key agreement for application security.

Source

ITU-T Recommendation J.366.9 was approved on 29 November 2006 by ITU-T Study Group 9 (2005-2008) under the ITU-T Recommendation A.8 procedure.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

ITU-T Recommendation J.366.9

IPCablecom2 IP Multimedia Subsystem (IMS): Generic authentication architecture specification

1 Scope

1.1 Relationship between IPCablecom 2.0 and 3GPP IMS

The Third Generation Partnership Project (3GPP) has developed the specification in a form optimized for the wireless environment. This Recommendation references the ETSI version of the 3GPP specification and specifies only the modifications necessary to optimize it for the cable environment. Additions are shown in blue underline and deletions in ~~red strikethrough.~~

It is an important objective of this work that interoperability between IPCablecom 2.0 and 3GPP IMS is provided. IPCablecom 2.0 is based upon 3GPP IMS, but includes additional functionality necessary to meet the requirements of cable operators. Recognizing developing converged solutions for wireless, wireline, and cable, it is expected that further development of IPCablecom 2.0 will continue to monitor and contribute to IMS developments in 3GPP, with the aim of alignment of 3GPP IMS and IPCablecom 2.0.

The modifications to ETSI TS 133.220 V6.7.0 (2005-12), *Generic Authentication Architecture (GAA); Generic bootstrapping architecture* are listed below.

1.2 Scope of the present Recommendation

The present document describes the security features and a mechanism to bootstrap authentication and key agreement for application security from the 3GPP AKA mechanism and from HTTP Digest over TLS. Candidate applications to use this bootstrapping mechanism include but are not restricted to subscriber certificate distribution TS 33.221 [5]. Subscriber certificates support services whose provision mobile operator assists, as well as services that mobile operator provides.

The scope of this specification includes a generic AKA bootstrapping function, an HTTP Digest over TLS function, an architecture overview and the detailed procedures on how to bootstrap the credential.

Clause 4 of this specification describes a mechanism, called GBA_ME, to bootstrap authentication and key agreement, which does not require any changes to the UICC. Clause 5 of this specification describes a mechanism, called GBA_U, to bootstrap authentication and key agreement, which does require changes to the UICC, but provides enhanced security by storing certain derived keys on the UICC. Clause 6 of this specification describes the HTTP Digest over TLS mechanism.

2 References

<<Add the following references>>

[27] IETF RFC 4279 (2005): "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)". ~~IETF Internet-Draft: "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", December 2005, URL: http://www.ietf.org/internet-drafts/draft-ietf-tls-psk-09.txt.~~

[30] IETF RFC 2782 (2000): "A DNS RR for specifying the location of services (DNS SRV)."

[31] IETF RFC 1750 (1994): "Randomness Recommendations for Security".

3 Definitions, abbreviations symbols and conventions

3.1 Definitions

<<Add the following definition>>

HTTP Digest over TLS-based GBA: This is a GBA that uses HTTP Digest over TLS.

3.2 Abbreviations

<< Add the following abbreviation>>

GBA_H GBA with HTTP Digest over TLS enhancements

3.3 Symbols

<<No Change>>

3.4 Conventions

<<No Change>>

4 Generic Bootstrapping Architecture

<<No Change>>

4.1 Reference model

<<No Change>>

4.2 Network elements

4.2.1 Bootstrapping server function (BSF)

A generic Bootstrapping Server Function (BSF) and the UE shall mutually authenticate using the AKA protocol or the HTTP Digest over TLS mechanisms, and agree on session keys that are afterwards applied between UE and a Network Application Function (NAF). The BSF shall restrict the applicability of the key material to a specific NAF by using the key derivation procedure as specified in Annex B. The key derivation procedure may be used with multiple NAFs during the lifetime of the key material. The lifetime of the key material is set according to the local policy of the BSF. The generation of key material is specified in clause 4.5.2.

The BSF shall be able to acquire the GBA user security settings (GUSS) from the HSS.

The BSF shall be able to keep a list, which assigns NAFs to NAF Groups. This list is used to select if any and which application-specific USS within GUSS is valid for a certain NAF.

NOTE 1 – The operator does the assignment of NAFs to NAF Groups. NAF Group definitions in HSS and all connected BSFs belonging to the same operator's network shall be equal (cf., clause 4.2.3). As these network elements belong to the same operator's network, standardization of the NAF Group definitions themselves is not necessary in 3GPP.

NOTE 2 – The NAF grouping may be e.g., "home" and "visited". It allows the BSF to send USSs for the same application with e.g., different authorization flags to different NAFs, e.g., in home network and visited networks. The NAF e.g., in visited network indicates only the requested application, but it is unaware of the grouping in home network of the subscriber.

4.2.2 Network application function (NAF)

<<No Change>>

4.2.2a Diameter proxy (D-Proxy)

<<No Change>>

4.2.3 HSS

<<No Change>>

4.2.4 UE

The required functionalities from the UE that supports a UICC are:

– the support of HTTP Digest AKA protocol;

– the capability to use both a USIM and an ISIM in bootstrapping;

– the capability to select either a USIM or an ISIM to be used in bootstrapping, when both of them are present;

– the capability for a Ua application on the ME to indicate to the GBA Function on the ME the type or the name of UICC application to use in bootstrapping (see clause 4.4.8);

– the capability to derive new key material to be used with the protocol over Ua interface from CK and IK;

– support of NAF-specific application protocol (For an example see TS 33.221 [5]).

The required functionalities from the UE that does not support a UICC are:

– the support of HTTP Digest over TLS;

– support of NAF-specific application protocol defined in TS 33.222 [25]).

A UE that supports a UICC may support the HTTP Digest over TLS functionality.

A GBA-aware ME with a UICC shall support both GBA_U, as specified in clause 5.2.1 and GBA_ME procedures, as specified in clause 4.5.

4.2.5 SLF

<<No Change>>

4.3 Bootstrapping architecture and reference points

4.3.1 Reference point Ub

The reference point Ub is between the UE and the BSF. Reference point Ub provides mutual authentication between the UE and the BSF. It allows the UE to bootstrap the session keys based on 3GPP AKA infrastructure or by using HTTP Digest over TLS mechanism.

The HTTP Digest AKA protocol, which is specified in RFC 3310 [4], is used on the reference point Ub. It is based on the 3GPP AKA TS 33.102 [2] protocol. The interface to the USIM is as specified in TS 31.102 [1] and to the ISIM is as specified in TS 31.103 [10].

The HTTP Digest protocol, which is specified in RFC 2617 [3], in conjunction with TLS is also used on the reference point Ub.

4.3.2 Reference point Ua

The reference point Ua carries the application protocol, which is secured using the keys material agreed between UE and BSF as a result of the run of HTTP Digest AKA or HTTP Digest over TLS over reference point Ub. For instance, in the case of support for subscriber certificates TS 33.221 [5], it is a protocol, which allows the user to request certificates from the NAF. In this case the NAF would be the PKI portal.

4.3.3 Reference point Zh

<<No Change>>

4.3.4 Reference point Zn

The reference point Zn is used by the NAF to fetch the key material agreed during a previous HTTP Digest AKA protocol or HTTP Digest over TLS run over the reference point Ub from the UE to the BSF. It is also used to fetch application-specific user security settings from the BSF, if requested by the NAF.

4.3.5 Reference point Dz

<<No Change>>

4.4 Requirements and principles for bootstrapping

<<No Change>>

4.4.1 Access Independence

<<No Change>>

4.4.2 Authentication methods

Authentication between the UE and the BSF shall not be possible without a valid ~~cellular~~ subscription. Authentication shall be based on the 3GPP AKA protocol or HTTP Digest over TLS.

4.4.3 Roaming

<<No Change>>

4.4.4 Requirements on reference point Ub

The requirements for reference point Ub are:

– the BSF shall be able to identify the UE;

– the BSF and the UE shall be able to authenticate each other based on AKA;

– the BSF and the UE shall be able to authenticate each other based on HTTP Digest over TLS;

– the BSF shall be able to send a bootstrapping transaction identifier to the UE;

– the UE and the BSF shall establish shared keys;

– the BSF shall be able to indicate to the UE the lifetime of the key material. The key lifetime sent by the BSF over Ub shall indicate the expiry time of the key.

NOTE – This does not preclude a UE to refresh the key before the expiry time according to the UE's local policy.

4.4.5 Requirements on reference point Zh

The requirements for reference point Zh are:

– mutual authentication, confidentiality and integrity shall be provided;

NOTE 1 – This requirement may be fulfilled by physical or proprietary security measures if BSF and HSS are located within the same operator's network.

– the BSF shall be able to send bootstrapping information request concerning a subscriber;

– the HSS shall be able to send one 3GPP AKA vector at a time to the BSF;

– the HSS shall be able to send HTTP Digest credentials to the BSF;

– the HSS shall be able to send the complete set of subscriber's GBA user security settings needed for security purposes to the BSF;

NOTE 2 – If subscriber's GUSS is updated in HSS, this is not propagated to the BSF. The GUSS in the BSF is updated when the BSF next time fetches the authentication vectors and GUSS from the HSS over Zh reference point as part of the bootstrapping procedure.

– no state information concerning bootstrapping shall be required in the HSS;

– all procedures over reference point Zh shall be initiated by the BSF;

– the number of different interfaces to HSS should be minimized.

4.4.6 Requirements on reference point Zn

<<No Change>>

4.4.7 Requirements on Bootstrapping Transaction Identifier

<<No Change>>

4.4.8 Requirements on selection of UICC application and related keys

The requirements in this clause apply when a UICC is present in the UE.

When several applications are present on the UICC, which are capable of running AKA, then the ME shall choose one of these UICC applications for performing the GBA procedures specified in this document in the following order of preference:

<<There are no additional changes to this clause>>

4.4.9 Requirements on reference point Ua

<<No Change>>

4.4.10 Requirements on reference point Dz

<<No Change>>

4.5 Procedures

<<No Change>>

4.5.1 Initiation of bootstrapping

<<No Change>>

4.5.2 Bootstrapping procedures

The requirements in this clause apply when a UE is performing AKA.

When a UE wants to interact with a NAF, and it knows that the bootstrapping procedure is needed, it shall first perform a bootstrapping authentication (see Figure 4.3). Otherwise, the UE shall perform a bootstrapping authentication only when it has received bootstrapping initiation required message or a bootstrapping negotiation indication from the NAF, or when the lifetime of the key in UE has expired (cf., clause 4.5.3).

<<There are no additional changes to this clause>>

4.5.3 Procedures using bootstrapped Security Association

<<No Change>>

4.5.4 Procedure related to service discovery

BSF discovery may occur in one of several ways:

– ~~The~~When using the HTTP Digest AKA method, the UE may ~~shall~~ discover the address of the BSF the from the identity information related to the UICC application that is used

during bootstrapping procedure, i.e., IMSI for USIM, or IMPI for ISIM. The address of the BSF is derived as specified in 3GPP TS 23.003 [11].

– A UE may discover the BSF through the use of DNS SRV as defined in RFC 2782 [30]. The UE shall have knowledge of the DNS SRV service name and the protocol for the BSF it is trying to locate. The procedures of RFC 2782 shall be followed to determine the address of the BSF.

– A UE may be configured with the address of the BSF.

5 UICC-based enhancements to Generic Bootstrapping Architecture (GBA_U)

<<No Change>>

6 HTTP Digest Over TLS enhancements to Generic Bootstrapping Architecture (GBA_H)

The following clauses describe procedures for UEs performing GBA_H, which is based on HTTP Digest over TLS.

6.1 Bootstrapping procedure

The bootstrapping procedure starts by establishing a TLS tunnel between the client and the BSF. After establishing the TLS tunnel, the Ub interface shall use the HTTP Digest mechanism to establish the credentials (i.e., derive a session key(s)) between the UE and the BSF.

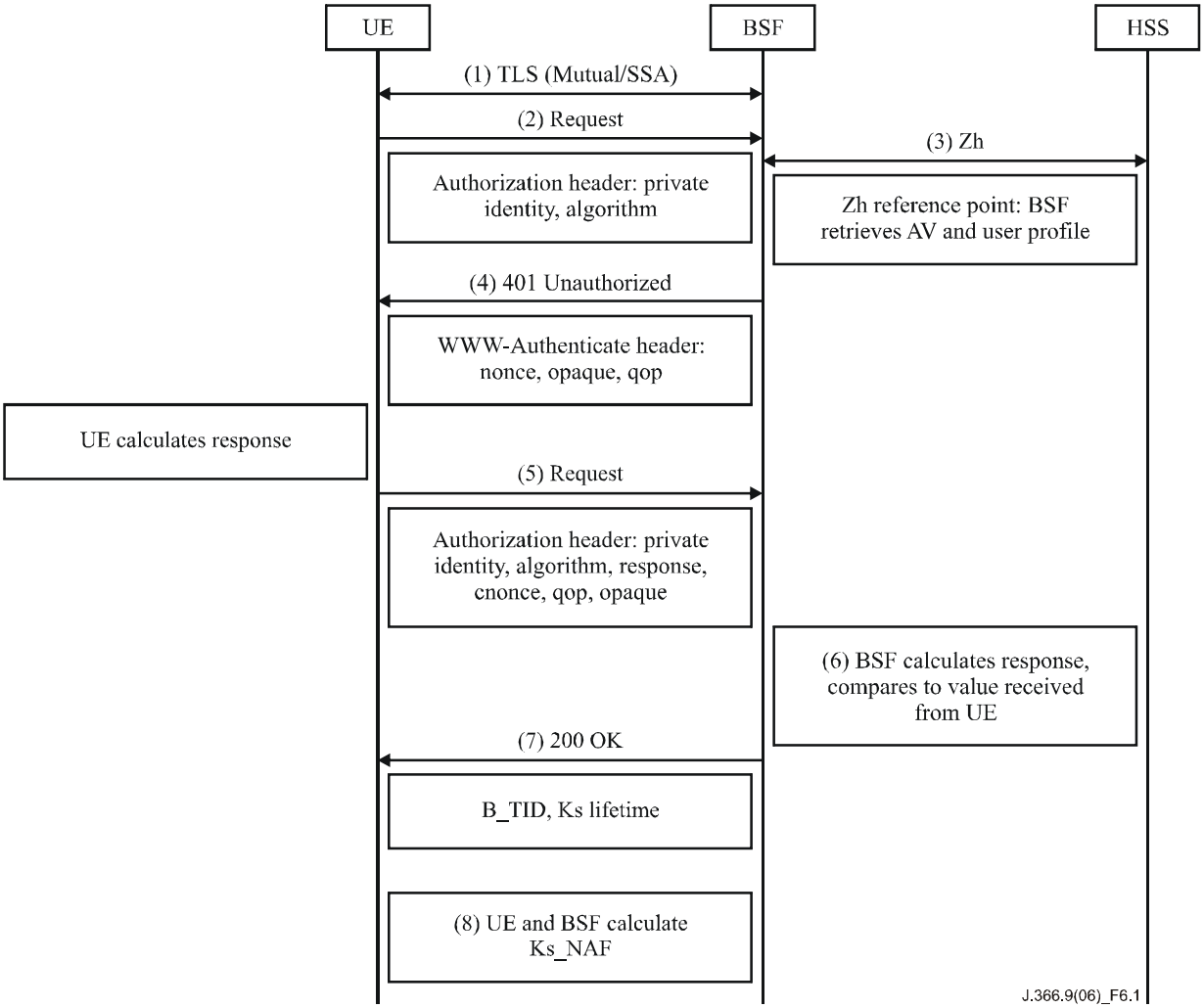

Figure 6.1 – HTTP digest over TLS bootstrapping procedure

The new bootstrapping exchange on the Ub interface is illustrated in Figure 6.1 and described below.

1) The UE shall start the bootstrapping procedure by initiating a TLS session with the BSF. The UE and BSF shall negotiate server side authenticated TLS. The UE shall authenticate the BSF by the certificate presented by the BSF. The BSF does not require authentication from the UE at this point.

2) After negotiation of TLS, the UE shall send an HTTP Request message to the BSF containing the private identity in an Authorization header. The UE indicates the algorithm it supports in the algorithm parameter of the Authorization header.

3) The BSF shall send a MAR command to the HSS to retrieve an authentication vector for that user. The HSS shall respond with the appropriate authentication vector for that user and algorithm in a MAA message. The authentication vector contents are enhanced as in SIP Digest to allow the BSF to calculate a challenge to the UE as described in RFC 2617 [3].

NOTE 1 – In a multiple HSS environment, the BSF may have to obtain the address of the HSS where the subscription of the user is stored by querying the SLF, prior to step 3.

4) The BSF shall respond to the UE request with a 401 Unauthorized message containing a www-authenticate header to force the UE to authenticate itself. The www-authenticate header includes a 32-octet ASCII hexadecimal encoded nonce, created following the

guidelines described in RFC 1750 [31]. The algorithm parameter informs the UE of the algorithm it should use to calculate its response.

5) Upon receiving the challenge, the UE shall use the data received in the www-authenticate header to create a second HTTP Request with the challenge response in an Authorization header. The challenge response is calculated per RFC 2617 [3]. A cnonce shall be included and calculated in the same manner as the nonce. The UE shall select a qop value from the list of qop values sent by the BSF and compute the response accordingly. The message shall be sent to the BSF over the TLS session.

6) The BSF shall check the validity of the challenge response sent by the UE by calculating the response on its own and comparing the values. The BSF calculates the response per RFC 2617 [3]. It uses the HA1 value supplied by the HSS over the Zh reference point.

7) If the challenge response sent by the UE is identical to the response calculated by the BSF, the BSF shall send a 200 OK message including the B-TID to the UE to indicate successful authentication. In addition, in a 200 OK message, the BSF shall supply the lifetime of the key Ks. The B-TID value shall be generated in the format of NAI by taking the base64 encoded [12] nonce value from step 4, and the BSF server name, i.e., base64encode(nonce)@BSF_servers_domain_name.

NOTE 2 – Before base64 encoding the nonce from step 4, the nonce shall first be converted from a hexadecimal ASCII encoded value to a binary encoded value.

8) Both the UE and the BSF shall use the Ks to derive the key material Ks_NAF during the procedures as specified in clause 6.2. Ks_NAF shall be used for securing the reference point Ua.

Ks_NAF is computed as Ks_NAF=KDF(Ks, "gba-h", RAND, IMPI, NAF_Id) where KDF is the key derivation function described in Annex B. The binary encoded nonce is substituted for the AKA-based RAND variable when calculating Ks_NAF. Ks is the master secret from the existing TLS session.

The UE and the BSF shall store the key Ks with the associated B-TID for further use, until the lifetime of Ks has expired, or until the key Ks is updated.

6.2 Procedures using bootstrapped Security Association

Before communication between the UE and the NAF can start, the UE and the NAF first have to agree whether to use shared keys obtained by means of the GBA. If the UE does not know whether to use GBA with this NAF, it uses the Initiation of Bootstrapping procedure described in clause 4.5.1.

Once the UE and the NAF have established that they want to use GBA, then every time the UE wants to interact with an NAF the following steps are executed as depicted in Figure 4.4:

1) UE starts communication over reference point Ua with the NAF:
   - in general, UE and NAF will not yet share the key(s) required to protect the reference point Ua. If they already do (i.e., if a key Ks_NAF for the corresponding key derivation parameter NAF_Id is already available), the UE and the NAF can start to securely communicate right away. If the UE and the NAF do not yet share a key, the UE proceeds as follows:
     - if a key Ks is available in the UE, the UE derives the key Ks_NAF from Ks, as specified in clause 6.1;
     - if no key Ks is available in the UE, the UE first agrees on a new key Ks with the BSF over the reference point Ub, and then proceeds to derive Ks_NAF;

NOTE 1 – If it is not desired by the UE to use the same Ks to derive more than one Ks_NAF then the UE should agree on a new key Ks with the BSF over the reference point Ub, and then proceed to derive Ks_NAF;

- if the NAF shares a key with the UE, but the NAF requires an update of that key, e.g., because the key's lifetime has expired or will expire soon, or the key cannot meet the NAF local validity condition, it shall send a suitable bootstrapping renegotiation request to the UE, see Figure 4.5. If the key's lifetime has expired the protocol used over reference point Ua shall be terminated. The form of this indication depends on the particular protocol used over reference point Ua. If the UE receives a bootstrapping renegotiation request, it starts a run of the protocol over reference point Ub, as specified in clause 6.1, in order to obtain a new key Ks.

NOTE 2 – To allow for consistent key derivation in BSF and UE, both have to use the same FQDN for derivation (see NOTE 3 of clause 4.5.2). For each protocol used over Ua it shall be specified if only cases (1) and (2) of NOTE 3 of clause 4.5.2 are allowed for the NAF or if the protocol used over Ua shall transfer also the FQDN used for key derivation by UE to NAF.

NOTE 3 – If the shared key between UE and NAF is invalid, the NAF can set deletion conditions to the corresponding TLS session for subsequent removal.

- the UE supplies the B-TID to the NAF, in the form as specified in clause 4.3.2, to allow the NAF to retrieve the corresponding keys from the BSF;

NOTE 4 – The UE may adapt the key material Ks_NAF to the specific needs of the reference point Ua. This adaptation is outside the scope of this specification.

- key management for GBA related keys in the UE (i.e., Ks and Ks_NAF keys):
  - the Key Ks shall be deleted from the UE when the UE is powered down;
  - all other GBA related keys may be deleted from the UE when the UE is powered down. If the UE does not delete the GBA keys at power down then the GBA keys need to be stored in non-volatile memory;
  - when a new Ks is agreed over the reference point Ub and a key Ks_NAF, derived from one NAF_Id, is updated, the other keys Ks_NAF, derived from different values NAF_Id, stored on the UE shall not be affected;

NOTE 5 – According to the procedures defined in clauses 6.1 and 6.2, in the UE there is at most one Ks_NAF key stored per NAF-Id.

2) NAF starts communication over reference point Zn with BSF

- The NAF requests key material corresponding to the B-TID supplied by the UE to the NAF over reference point Ua. If the NAF has several FQDNs, which may be used in conjunction with this specification, then the NAF shall transfer in the request over Zn the same FQDN, which was used over Ua (see NOTE 2 on key derivation in this clause);
- The NAF may also request one or more application-specific USSs for the applications, which the request received over Ua from UE may access;
- With the key material request, the NAF shall supply NAF's public hostname that UE has used to access NAF to BSF, and BSF shall be able to verify that NAF is authorized to use that hostname;

3) The BSF derives the keys required to protect the protocol used over reference point Ua from the key Ks and the key derivation parameters, as specified in clause 6.1, and supplies to NAF the requested key Ks_NAF, as well as the bootstrapping time and the lifetime of that key, and the requested application-specific and potentially NAF group specific USSs if they are available in subscriber's GUSS and if the NAF is authorized to receive the requested USSs. If the key identified by the B-TID supplied by the NAF is not available at

the BSF, the BSF shall indicate this in the reply to the NAF. The NAF then indicates a bootstrapping renegotiation request to the UE.

NOTE 6 – The NAF can further set the local validity condition of the Ks_NAF according to the local policy, for example a limitation of reuse times of a Ks_NAF.

NOTE 7 – The NAF will adapt the key material Ks_NAF to the specific needs of the reference point Ua in the same way as the UE did. This adaptation is outside the scope of this specification.

– The BSF may require that one or more application-specific and potentially NAF group specific USSs shall be present in subscriber's GUSS for the NAF (see clause 4.4.6). If one or more of these required settings are missing from the GUSS, the BSF shall indicate this in the reply to the NAF.

– The BSF may also send the private user identity (IMPI) and requested USSs to NAF according to the BSF's policy;

4) NAF continues with the protocol used over the reference point Ua with the UE.

Once the run of the protocol used over reference point Ua is completed the purpose of bootstrapping is fulfilled as it enabled UE and NAF to use reference point Ua in a secure way.

Annex A

Void

Annex B (normative)

Specification of the key derivation function KDF

<<No Change>>

B.2 Generic key derivation function

<<No Change>>

B.2.1 Input parameter encoding

<<No Change>>

B.3 NAF specific key derivation in GBA, ~~and~~ GBA_U, and GBA_H

In GBA, ~~and~~ GBA_U, and GBA_H, the input parameters for the key derivation function shall be the following:

– FC = 0x01;

– P1 = RAND;

– L1 = length of RAND is 16 octets (i.e., 0x00 0x10);

– P2 = IMPI encoded to an octet string using UTF-8 encoding (see clause B.2.1);

– L2 = length of IMPI is variable (not greater that 65535);

– P3 = NAF_ID with the FQDN part of the NAF_ID encoded to an octet string using UTF-8 encoding (see clause B.2.1); and

– L3 = length of NAF_ID is variable (not greater that 65535).

In the key derivation of Ks_NAF as specified in clause 4 and Ks_ext_NAF as specified in clause 5,

– P0 = "gba-me" (i.e., 0x67 0x62 0x61 0x2d 0x6d 0x65); and

– L0 = length of P0 is 6 octets (i.e., 0x00 0x06).

In the key derivation of Ks_int_NAF as specified in clause 5,

– P0 = "gba-u" (i.e., 0x67 0x62 0x61 0x2d 0x75); and

– L0 = length of P0 is 5 octets (i.e., 0x00 0x05).

The Key to be used in key derivation shall be:

– Ks (i.e., CK || IK concatenated) as specified in clauses 4 and 5,

NOTE 1 – In the specification this function is denoted as:

Ks_NAF = KDF (Ks, "gba-me", RAND, IMPI, NAF_Id);

Ks_ext_NAF = KDF (Ks, "gba-me", RAND, IMPI, NAF_Id); and

Ks_int_NAF = KDF (Ks, "gba-u", RAND, IMPI, NAF_Id).

In GBA_H, the input parameters for the key derivation function shall be the following:

– FC = 0x01;

– P0 = "gba_h" (i.e., 0x67 0x62 0x61 0x2d 0x68);

– L0 = length of P0 is 5 octets (i.e., 0x00 0x06);

– P1 = nonce;

– L1 = length of nonce is 16 octets (i.e., 0x00 0x10);

– P2 = IMPI encoded to an octet string using UTF-8 encoding (see clause B.2.1);

– L2 = length of IMPI is variable (not greater that 65535);

– P3 = NAF_ID with the FQDN part of the NAF_ID encoded to an octet string using UTF-8 encoding (see clause B.2.1); and

– L3 = length of NAF_ID is variable (not greater that 65535).

The Key to be used in key derivation shall be:

– Ks (i.e., CK || IK concatenated) as specified in clauses 4 and 5,

NOTE 2 – In the specification this function is denoted as:

Ks_NAF = KDF (Ks, "gba-h", RAND, IMPI, NAF_Id).

Annex C (informative)

Void

Annex D (informative)

Dialog example for user selection of UICC application used in GBA

<<No Change>>

Annex E (normative)

TLS profile for securing Zn' reference point

<<No Change>>

Annex F (informative)

Handling of TLS certificates

<<No Change>>

Annex G (normative)

GBA_U UICC-ME interface

<<No Change>>

Annex H (normative)

Ua security protocol identifier

<<No Change>>

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	**Cable networks and transmission of television, sound programme and other multimedia signals**
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2007