3GPP TSG SA WG3 Security — SA3#34 **S3-040648**
6-9 July, 2004
Acapulco, Mexico

Source: Nokia, Siemens, Gemplus, Motorola

Title: USIM and ISIM selection in GAA

Agenda item: GBA

Document for: Discussion/Approval

1 Introduction

Contributions S3-040591, S3-040592, and S3-040593 from Nokia, Alcatel, Gemplus, and Motorola, and contribution S3-040508 from Siemens discuss the possible ways to select the UICC application, i.e., USIM or ISIM, to be used in bootstrapping. The concept was developed further in offline discussions during the SA3#34 meeting, and this contribution presents the result of these discussions.

2 Discussion

2.1 Identified issues/problems

The following issues/problems have been identified in the parallel usage of USIM and ISIM in GAA:

(a) Some applications may have a preference to use the ISIM while other applications may want to use USIM. *There is a need to let applications on the ME state their preference, e.g., the application on the ME talking to the presence list server over the Ut reference point may always want to use an ISIM, whereas the MBMS application on the ME wants to use the USIM.*

(b) If the UE has more than one ISIM or USIM application, e.g., the subscriber as a private person and the subscriber as a company employer, which ISIM or USIM should be used in GBA, i.e., in which role the subscriber wants to access the NAF. *The ME needs to able to select the correct application on the UICC that is applicable to the particular situation.*

(c) The UICC can only have a limited number of applications active (one for Release 99 UICCs and four for UICCs from later releases), i.e., the activation of an application on the UICC may not be possible. Furthermore, the activation of a UICC application may require human user involvement (PIN entry). *An activation of an inactive application on the UICC should be avoided.*

(d) The user profile information / user security settings in the HSS may be different or may be the same for different private identities (ISIMs or USIMs respectively), depending on the role to which they relate. It should be ensured that different identities and UICC applications used in the Ub protocol point to the same user security settings, if they relate to the same role.

2.2 Proposed selection process

Both the USIM and the ISIM can be used to authenticate the UE and the network and derive the key Ks in the protocol over the Ub reference point. If there is more than one UICC application of type either ISIM or USIM, then different keys Ks may result depending on the selected application. Consequently, for each derivation of a key Ks_NAF from a Ks, there needs to be a rule to decide, from which UICC application the key Ks shall be derived.

The selection process proceeds in the following steps:

1. The UE determines which UICC application is to be involved:

a. the application on the ME that needs Ks_NAF may indicate to the GBA application the type of the UICC application: no preference, USIM, or ISIM. If the application on the ME indicated that the UICC application type should be:

   - the USIM on the UICC; step b below is skipped and in step d only the USIM applications are considered.

   - the ISIM on the UICC; step c below is skipped and in step d only the ISIM applications are considered.

   If the application on the ME did not indicate a preference, the selection process is executed as described below,

b. the ME shall select among the active ISIMs; if there is more than one active ISIM, the UE may show an ISIM selection dialog to the end user (the list contains the "Labels" from the application list of the UICC), from which the end user selects the ISIM; if no dialogue is shown the ME shall select any one of the active ISIMs.

c. the ME shall select among the active USIMs; if there is more than one active USIM, the UE may show a USIM selection dialog to the end user (the list contains the "Labels" from the application list of the UICC), from which the end user selects the USIM; if no dialogue is shown the ME shall select any one of the active USIMs.

d. if there are no UICC applications active:

   - if there is only one UICC application, the UE activates it, if possible, and selects it;

   - if there is more than one UICC application, the UE may show a UICC application selection dialog to the end user (the list contains the "Labels" from the application list of the UICC), from which the end user selects the UICC application to be activated; if no dialogue is shown the ME shall activate the default USIM, if possible, and select it.

2. If there already is a key Ks derived from the selected UICC application, the UE takes this key to derive Ks_NAF.

3. If there is no such key Ks, the UE first runs the Ub protocol involving the selected UICC application and then goes to step 2.

3 Proposal

- Add the selection method described in section 2.2 to TS 33.220.

- Add requirements to TS 33.220 that it shall be possible to map multiple private identities to the subscriber's user profile / user security settings.

- Possibly send an LS to SA1 and T2 asking what their view on the user involvement during UICC application selection.

Annex A: Dialog example

A dialog window example is described below:

The title of the dialog: "Authentication request".

Explanation: "A service requires you to authenticate, please select your identity:"

List of identities: *A selectable list of applications on the UICC. The text visible for each application is extracted from the "Label" field of the application list on the UICC.*

Buttons: "Select" and "Cancel".

3GPP TSG-SA WG3 Meeting S3#34
Acapulco, Mexico, July 6-9, 2004

Tdoc ⌘S3-040xxx

CR-Form-v7

CHANGE REQUEST

⌘ **33.141** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.0.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: | UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☐

Title:	⌘	ISIM used in GBA
Source:	⌘	Nokia, Siemens, Gemplus, Motorola
Work item code:	⌘	Presence security
Date:	⌘	08/07/2004
Category:	⌘	**C**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	The UE should use an ISIM in bootstrapping when it accesses the Presence list server, since the presence account is based on an ISIM.
Summary of change:	⌘	The ISIM is used in bootstrapping when the UE accesses the Presence list server.
Consequences if not approved:	⌘	The ISIM is not used in bootstrapping when the UE accesses the Presence list server.

Clauses affected:	⌘	5.1.1

		Y	N		
Other specs affected:	⌘		X	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments:	⌘	

5.1.1 Authentication of the subscriber and the network

A subscriber shall be authenticated before accessing user data in a server. The subscriber shall only be able to manipulate data that is associated with that particular subscriber.

Editors note: Relationship between Transaction Identifier and subscriber identity is ffs. In the case of Presence Ut interface, there are several potential identities that are related to the Transaction Identifier, i.e. IMPI and IMPUs. The subscriber may have several Presence accounts related to same IMPI. Transaction Identifier does not carry enough information on which IMPU the end-user is trying to use.

Authentication between the subscriber and the network shall be performed as specified in clause 6.1.

Subscriber authentication can be made by the operator using proprietary or non-3G standardized methods. In case 3GPP authentication mechanisms are used as specified in TS33.220 [11], the authentication of the subscriber shall be based on the ~~USIM~~ISIM. The authentication of the subscriber and the network shall be based on Generic Authentication Architecture as defined in 3GPP TR 33.919 [15]. Generic Authentication Architecture enables the use of different authentication methods to be used for the authentication of the subscriber by using:

- subscriber certificates (e.g., TLS, cf. [6,8,9]), or
- shared secrets (e.g., TLS with HTTP Digest, cf. [17]).

The server certificate to be used for application server authentication shall be based on WAPCert [12].

~~Editors Note: If 3GPP decides that ISIM-only UICCs are allowed then it needs to be studied further if also the ISIM may be used in the Generic Authentication Architecture~~

A UE may contact the Presence Server/AP for further instructions on authentication procedures.

The consumption of Authentication Vectors should be minimized. The architecture shall ensure that SQN synchronization failures are minimized.

3GPP TSG-SA WG3 Meeting S3#34
Acapulco, Mexico, July 6-9, 2004

Tdoc ⌘S3-040xxx

CR-Form-v7

CHANGE REQUEST

⌘ **33.220** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **6.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Details of USIM/ISIM usage in GAA
Source:	⌘	Nokia, Siemens, Gemplus, Motorola
Work item code:	⌘	GBA and SSC
Date:	⌘	08/07/2004
Category:	⌘	**C**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	For a service that utilizes the GBA, e.g., Presence, it should be possible to access the server with an ISIM, since the presence account based on an ISIM may be different than that in the USIM which are received from a BSF, e.g., an IMPI value, and IMPUs added to enable new services.
Summary of change:	⌘	ISIM support in GAA is added.Default selection logic is added to make the selection on the UE whether to use an ISIM or a USIM in GBA.
Consequences if not approved:	⌘	Service may have conflicts when handling the UE's identities.

Clauses affected:	⌘	2, 4, 4.2.3, 4.2.4, 4.3.1, 4.4.4, 4.4.8 (new), 4.5.3, 5.3.3, Annex D (new)

Other specs affected:	Y	N		
⌘		X	Other core specifications	⌘
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

===== BEGIN CHANGE =====

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 31.102: "3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM application".

[2] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture".

[3] Franks J., et al,: "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[4] A. Niemi, et al,: "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", RFC 3310, September 2002.

[5] 3GPP TS 33.221: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Support for Subscriber Certificates".

[6] T. Dierks, et al,: "The TLS Protocol Version 1.0", RFC 2246, January 1999.

[7] OMA: "Provisioning Content Version 1.1", Version 13-Aug-2003. Open Mobile Alliance.

[8] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 6)".

[9] IETF RFC 3546 (2003): "Transport Layer Security (TLS) Extensions".

[10] 3GPP TS 31.103: “3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the IP Multimedia Services Identity Module (ISIM) application”.

[11] 3GPP TS 23.003: “3rd Generation Partnership Project; Technical Specification Group Core Network; Numbering, addressing and identification”.

===== BEGIN NEXT CHANGE =====

4 Generic Bootstrapping Architecture

The 3GPP authentication infrastructure, including the 3GPP Authentication Centre (AuC), the USIM or the ISIM, and the 3GPP AKA protocol run between them, is a very valuable asset of 3GPP operators. It has been recognised that this infrastructure could be leveraged to enable application functions in the network and on the user side to establish shared keys. Therefore, 3GPP can provide the "bootstrapping of application security" to authenticate the subscriber by defining a Generic Bootstrapping Architecture (GBA) based on AKA protocol.

===== BEGIN NEXT CHANGE =====

4.2.3 HSS

HSS shall store new parameters in the subscriber profile related to the use of the bootstrapping function. Possibly also parameters related to the usage of some NAFs are stored in the HSS. In the case where the subscriber has multiple subscriptions, i.e., multiple ISIM or USIM applications on the UICC, the HSS shall contain one or more subscriber profiles that are mappable to one or more private identities, i.e., IMPIs and IMSIs.

Editor's note: Needed new subscriber profile parameters are FFS.

4.2.4 UE

The required functionalities from the UE 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 an application on the ME using the shared secret to indicate the type of UICC application to use in bootstrapping (i.e., ISIM or USIM);
- 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]).

===== BEGIN NEXT CHANGE =====

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.

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].

===== BEGIN NEXT 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 shall be able to send a Transaction Identifier to the UE;
- the UE and the BSF shall establish shared keys.

===== BEGIN NEXT CHANGE =====

4.4.8 Requirements on selection of UICC application and related keys

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

1. The UE determines which UICC application is to be involved:

a. the application on the ME that needs Ks_NAF may indicate to the GBA application the type of the UICC application: no preference, USIM, or ISIM. If the application on the ME indicated that the UICC application type should be:

- the USIM on the UICC; step b below is skipped and in step d only USIM applications are considered.

- the ISIM on the UICC; step c below is skipped and in step d only ISIM applications are considered.

If the application on the ME did not indicate a preference, the selection process is executed as described below,

b. the ME shall select among the active ISIMs; if there is more than one active ISIM, the UE may show an ISIM selection dialog to the end user (the list contains the "Labels" from the application list of the UICC), from which the end user selects the ISIM; if no dialogue is shown the ME shall select any one of the active ISIMs.

c. the ME shall select among the active USIMs; if there is more than one active USIM, the UE may show a USIM selection dialog to the end user (the list contains the "Labels" from the application list of the UICC), from which the end user selects the USIM; if no dialogue is shown the ME shall select any one of the active USIMs.

d. if there are no UICC applications active:

- if there is only one UICC application, the UE activates it, if possible, and selects it;

- if there is more than one UICC application, the UE may show a UICC application selection dialog to the end user (the list contains the "Labels" from the application list of the UICC), from which the end user selects the UICC application to be activated; if no dialogue is shown the ME shall activate the default USIM, if possible, and select it.

2. If there already is a key Ks derived from the selected UICC application, the UE takes this key to derive Ks_NAF.

3. If there is no such key Ks, the UE first runs the Ub protocol involving the selected UICC application and then goes to step 2.

If a USIM is selected, the IMPI obtained from the IMSI stored on the USIM as specified in 3GPP TS 23.003 section 13.3 [11], is used in the protocol run over Ub.

NOTE 1: Strictly speaking, an IMPI, and the derivation of an IMPI from an IMSI as in 3GPP TS 23.003 section 13 [11] are only defined in the context of the IMS. For the purposes of this specification, however, an identifier obtained from an IMSI as specified in 3GPP TS 23.003 section 13.3 [11] is also called an IMPI, even if the user has no IMS subscription.

If an ISIM is selected, the IMPI stored on the ISIM is used in the protocol run over Ub.

Whenever an ISIM or a USIM is activated or deactivated, the rules in this subsection for selecting the UICC application are re-applied and, consequently, the selected UICC application may change.

Whenever a UICC application is de-selected the shared key Ks established from it in the protocol over the Ub reference point (according to sections 4.5.2 and 5.3.2) shall be deleted.

NOTE 2: At any one time, there is at most one UICC application selected for performing the GBA procedures.

NOTE 3: The applications on the ME can continue using the NAF specific keys derived also after the shared key Ks itself has been deleted until the key lifetime expires.

===== BEGIN NEXT CHANGE =====

4.5.3 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.

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 for the selected UICC application is available in the UE, the UE derives the key Ks_NAF from Ks, as specified in clause 4.5.2;

  - if no key Ks for the selected UICC application 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 for the selected UICC application 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, it shall send a suitable bootstrapping renegotiation request to the UE and terminates the protocol used over reference point Ua, see figure 4.5. 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 4.5.2, 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 2 of section 4.5.2). For each protocol used over Ua it shall be specified if only cases (1) and (2) of NOTE 2 of section 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 security association for subsequent removal.

- the UE supplies the Transaction Identifier 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.

- when the UE is powered down, or when the UICC is removed, any keys Ks and Ks_NAF shall be deleted from storage;

- 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;

NAF starts communication over reference point Zn with BSF

- The NAF requests key material corresponding to the Transaction Identifier 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);

- 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 verify that NAF is authorized to use that hostname;

- 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 4.5.2, and supplies to NAF the requested key Ks_NAF, as well as the lifetime of that key. If the key identified by the Transaction Identifier 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 5: The NAF shall 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.

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.

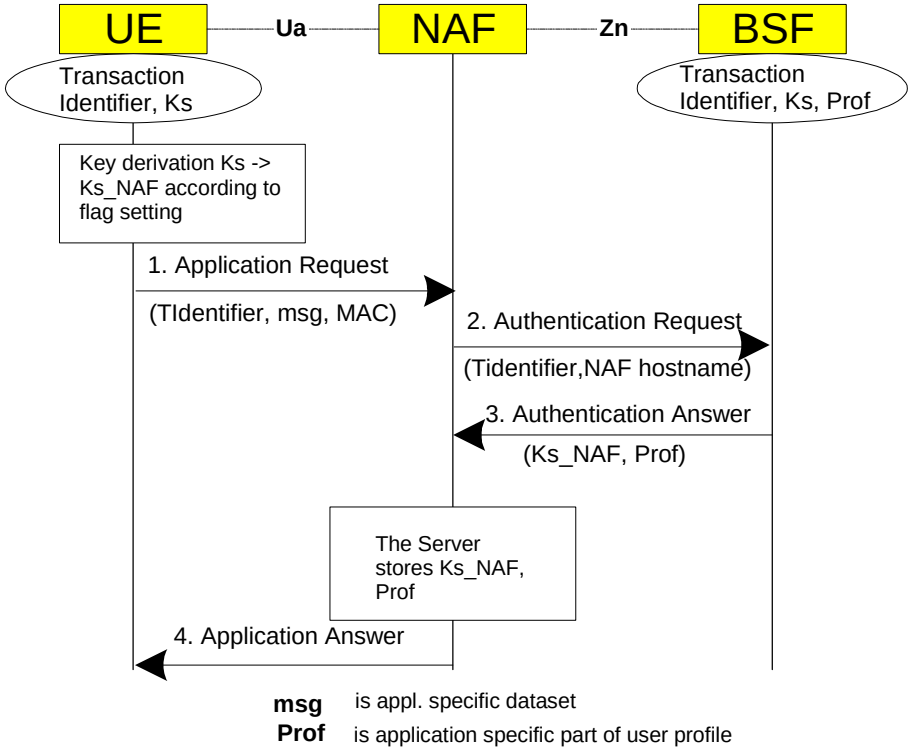

Figure 4.4: The bootstrapping usage procedure

===== BEGIN NEXT CHANGE =====

5.3.3 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 5.3.1.

Once the UE and the NAF have established that they want to use GBA then every time the UE wants to interact with a NAF the following steps are executed as depicted in figure 5.3.

Next, the UE and the NAF have to agree, which type of keys to use, Ks_ext_NAF or Ks_int_NAF, or both. The default is the use of Ks_ext_NAF only. This use is also supported by MEs and NAFs, which are GBA_U unaware. If Ks_int_NAF, or both, are to be used, this use has to be agreed between UE and NAF prior to the execution of the procedure described in the remainder of this clause 5.3.3. How this agreement is reached is application-specific and is not within the scope of this document.

NOTE 1: Such an agreement could e.g. be reached by manual configuration, or by an application-specific protocol step.

Editors' Note: The support of unaware GBA_U MEs, which are GBA_ME aware only is FFS.

In general, UE and NAF will not yet share the key(s) required to protect the Ua reference point. If they do not, the UE proceeds as follows:

- if Ks_ext_NAF is required and a key Ks_ext for the selected UICC application is available in the UE, the UE derives the key Ks_ext_NAF from Ks_ext, as specified in clause 5.3.2;
- if Ks_int_NAF is required and a key Ks_int for the selected UICC application is available in the UICC, the ME requests the UICC to derive the key Ks_int_NAF from Ks_int, as specified in clause 5.3.2;

NOTE 2: If it is not desired by the UE to use the same Ks_ext/int for the selected UICC application to derive more than one Ks_ext/int_NAF then the UE should first agree on new keys Ks_ext and Ks_int with the BSF over the Ub reference point, as specified in clause 5.3.2, and then proceeds to derive Ks_ext_NAF or Ks_int_NAF, or both, as required.

- if Ks_ext and Ks_int for the selected UICC application are not available in the UE, the UE first agrees on new keys Ks_ext and Ks_int with the BSF over the Ub reference point, as specified in clause 5.3.2, and then proceeds to derive Ks_ext_NAF or Ks_int_NAF, or both, as required;

- if the NAF shares a key with the UE, but the NAF requires an update of that key, it shall send a suitable bootstrapping renegotiation request to the UE and terminate the protocol used over Ua reference point. The form of this indication depends on the particular protocol used over Ua reference point. If the UE receives a bootstrapping renegotiation request, it starts a run of the protocol over Ub, as specified in clause 5.3.2, in order to obtain new keys.

NOTE 3: If the shared keys between UE and NAF become invalid, the NAF can set deletion conditions to the corresponding security association for subsequent removal.

NOTE 4: If it is not desired by the NAF to use the same Ks to derive more than one Ks_int/ext_NAF then the NAF should always reply to the first request sent by a UE by sending a key update request to the UE.

UE and NAF can now start the communication over Ua reference point using the keys Ks_ext_NAF or Ks_int_NAF, or both, as required. They proceed as follows:

- The UE supplies the Transaction Identifier to the NAF, as specified in clause 5.3.2, to allow the NAF to retrieve the corresponding keys from the BSF

NOTE 5: To allow for consistent key derivation in BSF and UE, both have to use the same FQDN for derivation (cf. NOTE 2 of clause 4.5.2). For each protocol used over Ua it shall be specified if only cases (1) and (2) of NOTE 2 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 6: The UE may adapt the keys Ks_ext_NAF or Ks_int_NAF to the specific needs of the Ua reference point. This adaptation is outside the scope of this specification.

- when the UE is powered down, or when the UICC is removed, any GBA_U keys shall be deleted from storage in the ME. There is no need to delete keys Ks_int and Ks_int_NAF from storage in the UICC;

NOTE 7: After each run of the protocol over the Ub reference point, new keys Ks_ext and Ks_int, associated with a new transaction identifier, are derived in the UE according to clause 5.3.2, so that it can never happen, that keys Ks_ext and Ks_int with different transaction identifiers simultaneously exist in the UE.

- When new keys Ks_ext and Ks_int are agreed over the Ub reference point and new NAF-specific keys need to be derived for one NAF_Id, then both, Ks_ext_NAF and Ks_int_NAF (if present), shall be updated for this NAF_Id, but further keys Ks_ext_NAF or Ks_int_NAF relating to other NAF_Ids, which may be stored on the UE, shall not be affected;

NOTE 8: This rule ensures that the keys Ks_ext_NAF and Ks_int_NAF are always in synch at the UE and the NAF.

NAF now starts communication over the Zn reference point with the BSF.

- The NAF requests from the BSF the keys corresponding to the Transaction Identifier, which was supplied by the UE to the NAF over the Ua reference point. If the NAF is GBA_U aware it indicates this by including a corresponding flag in the request. 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 above on key derivation in this clause).

- With the keys request over the Zn reference point, 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.

- The BSF derives the keys Ks_ext_NAF, and Ks_int_NAF (if additionally required), as specified in clause 5.3.2. If the NAF indicated in its request that it is GBA_U aware, the BSF supplies to NAF both keys, Ks_ext_NAF, and Ks_int_NAF, otherwise the BSF supplies only Ks_ext_NAF. In addition, the BSF supplies the lifetime time of these keys. If the key identified by the Transaction Identifier 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 (See figure 4.5) to the UE.

NOTE: The NAF may adapt the keys Ks_ext_NAF and Ks_int_NAF to the specific needs of the Ua reference point in the same way as the UE did. This adaptation is outside the scope of this specification.

The NAF now continues with the protocol used over the Ua reference point with the UE.

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

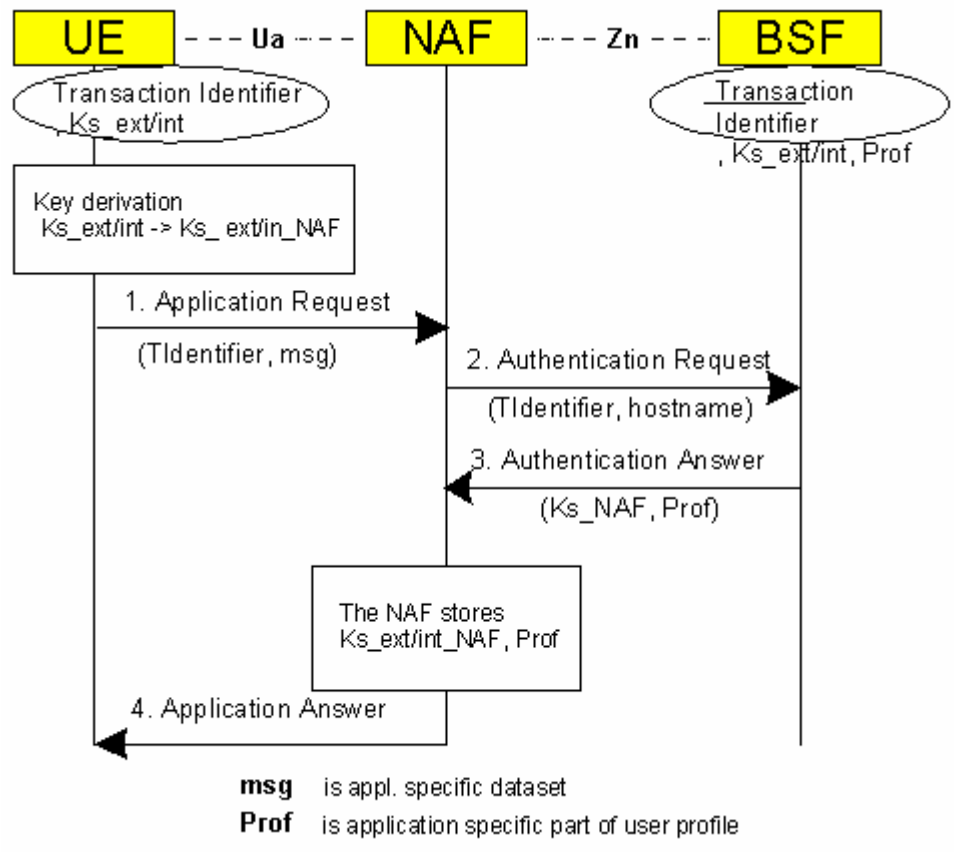

Figure 5.3: The bootstrapping usage procedure with UICC-based enhancements

===== BEGIN NEXT CHANGE =====

Annex D (informative): Dialog example for user selection of UICC application used in GBA

For certain cases, section 4.4.8 specifies user involvement in the selection of the UICC application used for GBA procedures. A dialog window example for such an involvement is described below:

The title of the dialog: "Authentication request".

Explanation: "A service requires you to authenticate, please select your identity:"

List of identities: A selectable list of applications on the UICC. The text visible for each application is extracted from the "Label" field of the application list on the UICC.

Buttons: "Select" and "Cancel".

===== END CHANGE =====