3GPP TSG SA WG3 Security — S3#34 **S3-040508**
6 – 9 July 2004
Acapulco, Mexico

Source: **Siemens**
Title: Use of USIM and ISIM in GBA
Work Item: 7.9.2 GBA
Document for: Discussion and decision

Abstract

It may happen that several USIM and/or ISIM applications are present on the UICC. In this case, the specification text in TS 33.220 v610 is ambiguous, when referring to the run of http digest aka over Ub, and the private user identity IMPI and its use in key derivation. This discussion paper and the attached CR propose a solution to remove the ambiguity.

1. Problem statement

Which UICC application to use in GBA?

The 3G specifications for Rel6 allow that several USIM and/or ISIM applications are present on a UICC. All of these UICC applications are capable of running AKA, and, in principle, they may have different long-term keys K. Then, for a run of the Ub protocol, there need to be rules for the ME, which of the USIM or ISIM applications to involve in the run of http digest aka over the Ub reference point. This contribution and the companion CR suggest such rules.

A first suggestion is that the ME selects one of the active UICC applications, if there is one, and does not first try to activate an inactive one. One reason for this suggestion is that, in the general case, activation of a UICC application requires human user intervention (PIN code entry), which may be undesirable from a user interface point of view. A second reason is that the number of UICC applications, which can be simultaneously active, is limited. If several UICC applications are active then further decision rules are needed, see attached CR.

As the GBA is a generic tool which may be used to provide keys to all kinds of NAFs / application servers and is not limited to IMS, a mapping of NAF to UICC application is not suitable as a selection rule for the ME. Please note here that the Ub protocol can be run before the ME decides to run a particular application, and the keys resulting from the run of the Ub protocol can be used for any type of NAF. Please note also that e.g. a presence list server, which may be seen as an IMS application, shall be accessible without the user having to register with the IMS first, i.e. without the ISIM having to be active.

Which IMPI to use for key derivation in GBA?

The key derivation in the GBA takes the IMPI as an input, see the following quotations from TS 33.220 v610:

Section 4.5.2:“Ks_NAF is computed as Ks_NAF = KDF (Ks, key derivation parameters), where KDF is a suitable key derivation function, and the key derivation parameters consist of the user's IMPI, the NAF_Id and RAND. The NAF_Id consists of the full DNS name of the NAF. KDF shall be implemented in the ME.”

and

Section 5.3.2: “ Ks_ext_NAF is computed as Ks_ext_NAF = h2 (Ks_ext, h2-key derivation parameters), and Ks_int_NAF is computed in the UICC as Ks_int_NAF = h2 (Ks_int, h2-key derivation parameters), where h2 is a suitable key derivation function, and the h2-key derivation parameters include the user's IMPI, the NAF_Id and RAND. The NAF_Id consists of the full DNS name of the NAF.”

Which IMPI to use depends on the selected UICC application.

2. Proposed solution

See attached CR.

3GPP TSG SA WG3 Security — SA3#34 **S3-040xxx**
6 – 9 July 2004 **Acapulco, Mexico**

CR-Form-v7

CHANGE REQUEST

⌘ **33.220** **CR** ⌘ **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:	⌘	Use of USIM and ISIM in GBA
Source:	⌘	Siemens
Work item code:	⌘	SSC-GBA
Date:	⌘	29/06/2004
Category:	⌘	**F**
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:	⌘	There is ambiguity in the specification regarding the use of USIM and ISIM applications on the UICC in the procedures of the Generic Bootstrapping Architecture.
Summary of change:	⌘	Rules are given, in which order active UICC applications shall be selected for the procedures of the Generic Bootstrapping Architecture.
Consequences if not approved:	⌘	Ambiguous specification.

Clauses affected:	⌘	2, 4

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications		TS 24.109, TS 31.102, TS 31.103
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	-

BEGIN OF 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"

END OF CHANGE

BEGIN OF 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.

END OF CHANGE

BEGIN OF 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]. The interface to the ISIM is as specified in TS 31.103 [10].

END OF CHANGE

BEGIN OF 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;
- 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 authentication over Ub in the following order of preference:
  - select the default USIM, if it is active;
  - if not, select any other active USIM, if there is one;

-if not, select any other active ISIM, if there is one;

-if not, activate the default USIM before initiating the protocol run over Ub;

- 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: 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;

- the BSF shall be able to send a Transaction Identifier to the UE.

END OF CHANGE