3GPP TSG SA WG3 Security — S3#26 **S3-020704**
19 - 22 November 2002
Oxford, UK

Title:	**LS on Requirement to allow access to IMS by means of SIM**
Response to:	**LS on Requirement to allow access to IMS by means of SIM (S1-022109)**
Release:	**Rel-5 and Rel-6**
Source:	**SA 3**
To:	**TSG SA, SA 1, CN 1, CN 4, SA 2, T 3**
Cc:	**-**

Contact Person:
Name: Stefan Schröder
Tel. Number: +49 882 936 3312
E-mail Address: stefan.schroeder@t-mobile.de

Attachments: **S3-020703: CR to TS 33.203 V.5.3.0**

1. Overall Description:

SA 3 thanks SA 1 for their LS on IMS access.

SA 3 considered the SA 1 requirement and concluded that it can be addressed by conversion functions in the UE and in the HSS as described in the attached CR. An alternative solution with the conversion done in the S-CSCF instead of the HSS was also considered but abandoned due to its potential impact on the Cx interface.

SA 3 would like to emphasize that allowing IMS access to subscribers still using a SIM does only provide a 2G level security to those subscribers: the home network will not be authenticated and the session keys are limited to maximum 64 bit effective strength. Therefore, SIM-based access to IMS should only be considered for a transition period and not as a long-term solution.

This new requirement may have an impact on T 3 specifications for Release 5 terminals.

Further changes are needed in CN specifications which might have an impact on addressing the requirement within the Rel-5 timeframe.

SA 3 did not find any technical problem in transporting the GSM AKA over Digest-AKA (RFC 3310) because all parameters are populated. This use of Digest-AKA goes beyond the originally intended purpose.

2. Actions:

CN 1 and T 3 are kindly asked to consider the impact of this change on their Release 5 specifications.

CN 4 is kindly asked to confirm that this change has no impact on Cx interface.

3. Date of Next SA 3 Meetings:

SA3 #27	25 - 28 February 2003	Sophia Antipolis, Fr
SA3 #28	06 - 09 May 2003	Berlin, De

3GPP TSG SA WG3 Security — S3#26 **S3-020703**
19- 22 November 2002, Oxford, UK

CR-Form-v7

CHANGE REQUEST

⌘ **33.203** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **5.3.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Allowing IMS access with SIM cards
Source:	⌘	T-Mobile
Work item code:	⌘	IMS-ASEC
Date:	⌘	19/11/2002
Category:	⌘	**B**
Release:	⌘	Rel-5

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:	⌘	A new requirement from SA1, to allow IMS access using a SIM.
Summary of change:	⌘	Conversion functions within UE and HSS are introduced to map SIM AKA to IMS AKA.
Consequences if not approved:	⌘	SA1 requirements will not be addressed.

Clauses affected:	⌘	3.1, 4., 5.1.1, 6.1, 6.1.1, 8., 8.1

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications		24.229, 23.228
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

******* first change *******

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Authenticated (re-) registration: A registration i.e. a SIP register is sent towards the Home Network which will trigger a authentication of the IMS subscriber i.e. a challenge is generated and sent to the UE.

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

ISIM – IM Subscriber Identity Module: For the purposes of this document the ISIM is a term that indicates the collection of IMS security data and functions on a UICC or SIM. The ISIM may be a distinct application on the UICC.

******* next change *******

4 Overview of the security architecture

In the PS domain, the service is not provided until a security association is established between the mobile equipment and the network. IMS is essentially an overlay to the PS-Domain and has a low dependency of the PS-domain. Consequently a separate security association is required between the multimedia client and the IMS before access is granted to multimedia services. The IMS Security Architecture is shown in the following figure.

IMS authentication keys and functions at the user side shall be stored on a UICC or SIM. It shall be possible for the IMS authentication keys and functions to be logically independent to the keys and functions used for PS domain authentication. However, this does not preclude common authentication keys and functions from being used for IMS and PS domain authentication according to the guidelines given in section 8.

For the purposes of this document the ISIM is a term that indicates the collection of IMS security data and functions on a UICC or SIM. Further information on the ISIM is given in section 8.

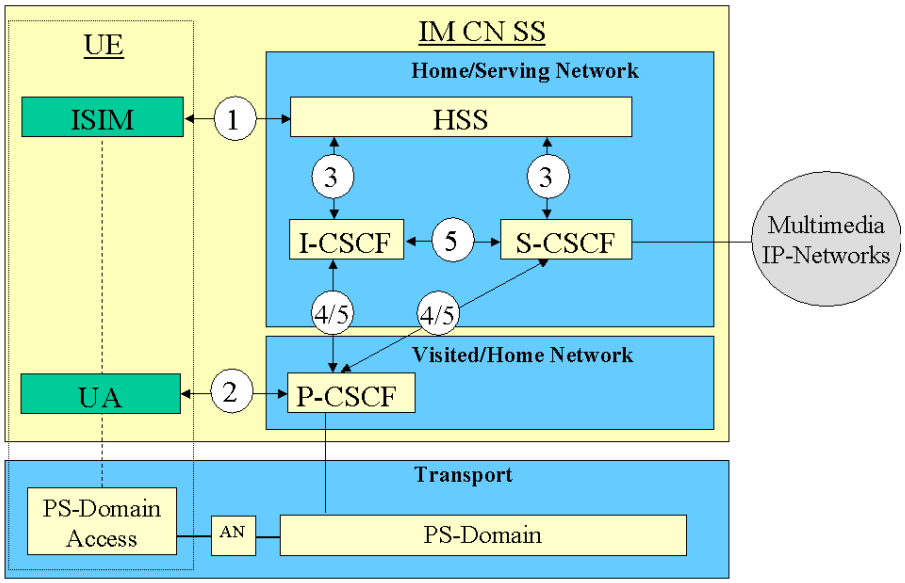

Figure 1: The IMS security architecture

There are five different security associations and different needs for security protection for IMS and they are numbered 1,2, 3, 4 and 5 in figure 1 where:

1. Provides mutual authentication unless the ISIM is implemented with~~as~~ a SIM. The HSS delegates the performance of subscriber authentication to the S-CSCF. However the HSS is responsible for generating keys and challenges. The long-term key in the ISIM and the HSS is associated with the IMPI. The subscriber will have one (network internal) user private identity (IMPI) and at least one external user public identity (IMPU).

2. Provides a secure link and a security association between the UE and a P-CSCF for protection of the Gm reference point. Data origin authentication is provided i.e. the corroboration that the source of data received is as claimed. For the definition of the Gm reference point cf. TS23.002 [9].

3. Provides security within the network domain internally for the Cx-interface. This security association is covered by TS 33.210 [5]. For the definition of the Cx-interface cf. TS23.002 [9].

4. Provides security between different networks for SIP capable nodes. This security association is covered by TS 33.210 [5]. This security association is only applicable when the P-CSCF resides in the VN and if the P-CSCF resides in the HN then bullet point number five below applies, cf. also Figure 2 and Figure 3.

5. Provides security within the network internally between SIP capable nodes. This security association is covered by TS 33.210 [5]. Note that this security association also applies when the P-CSCF resides in the HN.

There exist other interfaces and reference points in IMS, which have not been addressed above. Those interfaces and reference points reside within the IMS, either within the same security domain or between different security domains. The protection of all such interfaces and reference points apart from the Gm reference point are protected as specified in TS 33.210 [5].

Mutual authentication is required between the UE and the HN, unless the ISIM is implemented with~~as~~ a SIM.

The mechanisms specified in this technical specification are independent of the mechanisms defined for the CS- and PS-domain.

******* next change *******

5.1.1 Authentication of the subscriber and the network

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

An IM-subscriber will have its subscriber profile located in the HSS in the Home Network. The subscriber profile will contain information on the subscriber that may not be revealed to an external partner, cf. [3]. At registration an S-CSCF is assigned to the subscriber by the I-CSCF. The subscriber profile will be downloaded to the S-CSCF over the Cx-reference point from the HSS (Cx-Pull). When a subscriber requests access to the IP Multimedia Core Network Subsystem this S-CSCF will check, by matching the request with the subscriber profile, if the subscriber is allowed to continue with the request or not i.e. Home Control (Authorization of IM-services).

All SIP-signaling will take place over the PS-domain in the user plane i.e. IP Multimedia Core Network Subsystem is essentially an overlay to the PS-domain. Hence the Visited Network will have control of all the subscribers in the PS-domain i.e. Visited Control (Authorization of bearer resources) since the Visited Network provides the subscriber with a transport service and its associated QoS.

For IM-services a new security association is required between the mobile and the IMS before access is granted to IM-services.

The mechanism for mutual authentication in UMTS is called UMTS AKA. It is a challenge response protocol and the AuC in the Home Stratum derives the challenge. A Quintet containing the challenge is sent from the Home Stratum to the Serving Network. The Quintet contains the expected response XRES and also a message authentication code MAC. The Serving Network compares the response from the UE with the XRES and if they match the UE has been authenticated. The UE calculates an expected MAC, XMAC, and compares this with the received MAC and if they match the UE has authenticated the Serving Network.

The AKA-protocol is a secure protocol developed for UMTS and the same concept/principles will be reused for the IP Multimedia Core Network Subsystem, where it is called IMS AKA.

To enable IMS access for subscribers still using a SIM, GSM AKA will be mapped onto IMS AKA. However, GSM AKA does not provide Home Network authentication as UMTS AKA does. No MAC and XMAC calculations are performed if the ISIM is implemented with~~as~~ a SIM.

The Home Network authenticates the subscriber at anytime via the registration or re-registration procedures.

******* next change *******

6.1 Authentication and key agreement

The scheme for authentication and key agreement in the IMS is called IMS AKA. The IMS AKA achieves mutual authentication between the ISIM and the HN, cf. Figure 1, unless the ISIM is implemented with~~as~~ a SIM. The identity used for authenticating a subscriber is the private identity, IMPI, which has the form of a NAI, cf. [3]. The HSS and the ISIM share a long-term key associated with the IMPI.

The HN shall choose the IMS AKA scheme for authenticating an IM subscriber accessing through UMTS. The security parameters e.g. keys generated by the IMS AKA scheme are transported by SIP.

The generation of the authentication vector AV that includes RAND, XRES, CK, IK and AUTN shall be done in the same way as specified in [1]. The ISIM (unless implemented ~~as~~with a SIM) and the HSS keep track of counters SQN_{ISIM} and SQN_{HSS} respectively. The requirements on the handling of the counters and mechanisms for sequence number management are specified in [1]. The AMF field can be used in the same way as in [1].

If the UE is equipped with a SIM only, the AV is generated from the GSM triplets by conversion functions as defined in section 6.1.1.2.

Furthermore a security association is established between the UE and the P-CSCF. The subscriber may have several IMPUs associated with one IMPI. These may belong to the same or different service profiles. Only one SA shall be active between the UE and the P-CSCF. This single SA shall be updated when a new successful authentication of the subscriber has occurred, cf. section 7.4.

It is the policy of the HN that decides if an authentication shall take place for the registration of different IMPUs e.g. belonging to same or different service profiles. Regarding the definition of service profiles cf. [3].

6.1.1 Authentication of an IM-subscriber

6.1.1.1 ISIM implemented as a distinct ISIM application or with a USIM

Before a user can get access to the IM services at least one IMPU needs to be registered and the IMPI authenticated in the IMS at application level. In order to get registered the UE sends a SIP REGISTER message towards the SIP registrar server i.e. the S-CSCF, cf. Figure 1, which will perform the authentication of the user. The message flows are the same regardless of whether the user has an IMPU already registered or not.

******* next change *******

6.1.1.2 ISIM implemented ~~as~~with a SIM

If the ISIM is implemented ~~as~~with a SIM, the authentication data and key material is generated from the GSM triplet by conversion functions identical to those defined in [1]. This conversion takes place in the UE and the HSS. The conversion is transparent to all other NEs. The parameters needed in IMS AKA are derived as follows:

CK = Kc || Kc;

IK = Kc_1 xor Kc_2 || Kc || Kc_1 xor Kc_2; whereby Kc_i are both 32 bits long and Kc = Kc_1 || Kc_2.

AUTN = 0

RES_{IMS} = $SRES_{GSM}$

$XRES_{IMS}$ = $SRES_{GSM}$

$RAND_{IMS}$ = $RAND_{GSM}$

The IMS AKA procedure for SIM based authentication is nearly identical to the one shown in section 6.1.1.1. The only difference is: after receiving SM6, the UE does not check AUTN.

******* next change *******

8 ISIM

For the purposes of this document the ISIM is a term that indicates the collection of IMS security data and functions on a UICC or SIM. The following implementation options are permitted:

- Use of a distinct ISIM application on a UICC which does not share security functions with the USIM;
- Use of a distinct ISIM application on a UICC which does share security functions with the USIM;
- Use of a R99/Rel-4 USIM application on a UICC.
- Use of a SIM

NOTE: For later releases other implementations of ISIM are foreseen to be permitted.

If there is a R99/Rel-4 USIM and a SIM application on a UICC, the USIM shall be used for IMS authentication.

There shall only be one ISIM for each IMPI. The IMS subscriber shall not be able to modify or enter the IMPI. The IMS subscriber shall not be able to modify or enter the Home Domain Name.

8.1 Requirements on the ISIM application

This section identifies requirements on the ISIM application to support IMS access security. It does not identify any data or functions that may be required on the ISIM application for non-security purposes.

The ISIM shall include:

- The IMPI;
- At least one IMPU;
- Home Network Domain Name;
- Support for sequence number checking in the context of the IMS Domain, unless the ISIM is implemented ~~as~~with a SIM;
- The same framework for algorithms as specified for the USIM applies for the ISIM;
- An authentication Key.

The ISIM shall deliver the CK to the UE although it is not required that SIP signaling is confidentiality protected.

At UE power off the existing SAs in the MT shall be deleted. The session keys and related information in the SA shall never be stored on the ISIM.