3GPP TSG SA WG3 Security — S3#26 **S3-020609**
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:	⌘	13/11/2002
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 S-CSCF are introduced to map SIM AKA to IMS AKA.
Consequences if not approved:	⌘	Requirements will not be addressed and IMS market penetration will be delayed due to smaller subscriber base.

Clauses affected:	⌘	5.1.1, 6.1, 8.

Other specs affected:	⌘	Y	N		⌘	
		X		Other core specifications		24.229
		X		Test specifications		Is there an IMS Implementation Test?
			X	O&M Specifications		

Other comments:	⌘	

******* first 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 card, GSM AKA will be mapped onto UMTS AKA. However, GSM AKA does not provide Serving Network authentication as UMTS AKA does.

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. 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 (or USIM) 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 below.

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 or USIM based authentication

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 SIM based authentication

If the UE is equipped with a SIM only, the authentication data and key material is generated from the GSM triplets by conversion functions. This conversion takes place in the UE and S-CSCF. The conversion is transparent to all other NEs.

<... insert agreed conversions here ...>

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 *******

6.1.2.2 Network authentication failure

In this section the case when the authentication of the network is not successful is specified. When the check of the MAC in the UE fails the network can not be authenticated and hence registration fails. The flow is identical as for the successful registration in 6.1.1 up to SM6. Network authentication failures can not happen in SIM-based authentication because there is no MAC check in the UE. If a faulty UE sends an authentication failure message nevertheless, the network shall follow the procedure for the ISIM/USIM case below.

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

6.1.3 Synchronization failure

In this section the case of an authenticated registration with synchronization failure is described. After re-synchronization, authentication may be successfully completed, but it may also happen that in subsequent attempts other failure conditions (i.e. user authentication failure, network authentication failure) occur. In below only the case of synchronization failure with subsequent successful authentication is shown. The other cases can be derived by combination with the flows for the other failure conditions. Synchronization failures can not happen in SIM-based authentication because there is no synchronization check in the UE. If a faulty UE sends a synchronization failure message nevertheless, the network shall follow the procedure for the ISIM/USIM case below.

******* 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. 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 application on a GSM ICC.

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

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.