3GPP TSG-SA WG2 meeting #28 **Tdoc S2-023677**
Bangkok, Thailand, 11th – 15th November 2002

Title:	**Requirement to Allow Access to IMS by means of SIM in 3G UEs**
Response to:	**LS (S1-022109 (S2- S2-023416)) on " Requirement to allow access to IMS by means of SIM" from SA1**
Source:	SA2
To:	SA, CN
Cc:	SA3, CN1, SA1, T3

Contact Person:
Oscar Lopez-Torres **T-Mobile International**
Phone Number: +49 228 936 3340
E-mail Address: oscar.lopez-torres@t-mobile.de

Attachments: Discussion paper presented at SA2#28: Tdoc S2-023330.

---

1. Overall Description:

SA2 thank SA1 for the information contained in the above mentioned liaison. During the SA2 meeting held in Bangkok, 11 - 15 November 2002, the requirement from SA1 on "Allowing IMS Access Using SIM in 3G UEs" was discussed and resulted in the following:

SA2 has discussed the issues surrounding the support of IMS access using SIM in 3G UEes and has not identified any architectural reasons preventing this support. Some concern was raised in the meeting with respect to the IMS time scales, but it was felt that SA3 and CN1 should comment on this, as the issues are directly addressed to SA3 authentication work and IMS stage-3 specifications.

SA2 thank in advance SA3, CN1, and T3 for their help on the topic, and foreseeing the next meetings for SA3 and SA are coming in one and two weeks respectively, request prompt actions as follows:

2. Actions:

To SA3 group.

ACTION:

- Verify urgently the authentication/security technical impact of the requirement, and use the information of the possible scenarios included in the attachment as initial considerations from an architectural point of view and its feasibility within the Rel. 5 time frame

To CN1, CN groups.

ACTION:

- Verify urgently the technical impact of the requirement and its feasibility within the Rel 5 time frame

To SA1 group.

ACTION:

- Evaluate the results from SA3 and CN1 as soon as they are available.

3. Date of Next TSG-SA2 Meeting:

SA29#18	20-24 January 2003, San Francisco, USA

3GPP TSG-SA WG2 meeting #28 **Tdoc S2-023330**
Bangkok, Thailand, 11 – 15 November 2002

Title: **IMS Access via SIM in 3G UEs**

Source: **T-Mobile International**

Agenda item: **8.2**

Document for: **DISCUSSION AND DECISION**

Contact Person:
Name: Oscar Lopez-Torres
Phone Number: +49 228 936 3340
E-mail Address: **oscar.lopez-torres@t-mobile.de**

---

1. Introduction:

3GPP decided to provide new authentication procedures for 3G systems. However, considering that early deployment of IMS systems might be necessary, and that a graceful phasing down of SIM cards to USIM cards for IMS subscribers is needed, the question on budget savings for operators comes to mind. In other words, it seems more realistic now that, at the launch of initial IMS services, the amount of operators' SIM card replacement cannot be considered small, since the migration towards new USIMs will not happen overnight. Operators should be given flexibility in planning SIM card replacement instead of being urged by potential incoming SIM incompatible new IMS services. While at the same time avoiding complains from IMS users' experience, on the lines of: "why do some calls and GPRS work but not the 'shiny' new IMS services! - I was told that my new UMTS phone will work with my old SIM card.".

As specified today, access to IMS is performed using AKA Authentication, this implies that access to IMS will be denied to subscribers using a SIM rather than a USIM. Similarly, to the access to UTRAN using a SIM card, the choice on whether to allow it or disallow it is left to the operator.

Due to the high cost of deployment of the UTRAN, it is likely that the additional expenses to replace the SIM cards will be performed in different phases; i.e., during the transition period, some operators will not be willing to deny access to IMS to subscribers still owning a SIM card. Savings in deployment of USIM cards will also allow operators to comprehensively deploy a better UTRAN coverage.
It is an operator decision to balance out the savings against the reduced security offered by the SIM. However, it can be envisioned that enhancements to EAP-SIM could be a means to increase such security, as in Section 3.

This paper proposes to use similar mechanisms to access IMS by using a SIM card. Thus, the parameters necessary to access IMS shall be derived from the IMSI according to the rules defined in 23.003 and 23.228; i.e., IMPU, IMPI, and network domain name. The operator shall be able to allow or disallow access to the IMS via a SIM.

On the security side, the opinion of SA3 is required to correctly assess other methods based on GSM SIM algorithms and its applicability to IMS authentication to enable access via legacy SIMs.

2. Involved Nodes:

The following section (ref. TS 33.203 ver. 5.3.0.) present excerpts of the IMS authentication procedure and, at the same time the node-path. From this flow, the next Section builds up three scenarios to discuss architectural impacts for consideration.

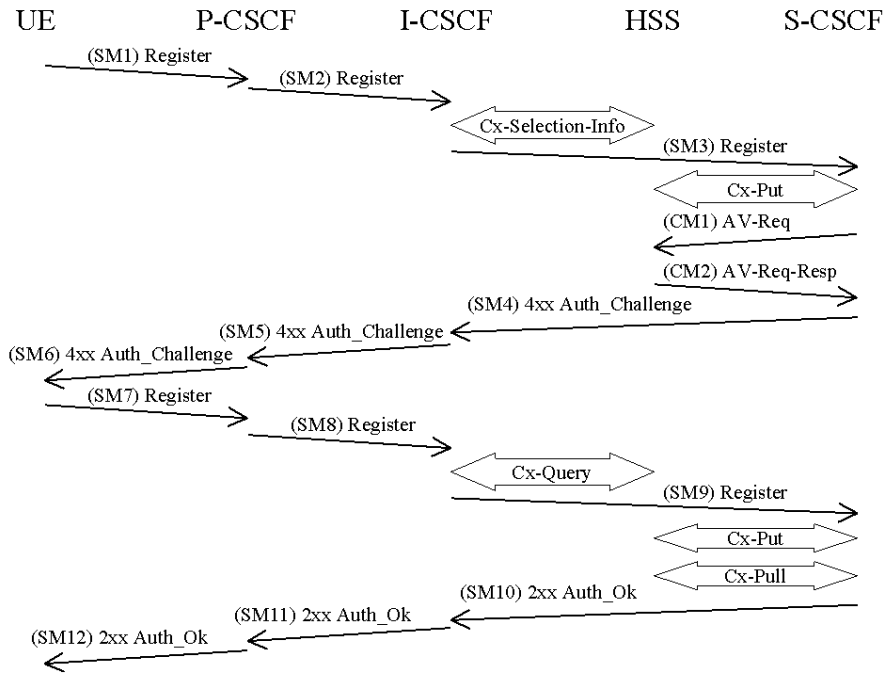

Figure 1. IMS Authentication and Key Agreement for an unregistered IM subscriber (Ref. 33.203, ver. 5.3.0)

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, 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.

SMn stands for SIP Message n and CMm stands for Cx message m which has a relation to the authentication process:

SM1:
REGISTER(IMPI, IMPU)

Upon receiving the SIP REGISTER the S-CSCF CSCF shall use an Authentication Vector (AV) for authenticating and agreeing a key with the user. If the S-CSCF has no valid AV then the S-CSCF shall send a request for AV(s) to the HSS in CM1 together with the number m of AVs wanted where m is at least one.

CM1:
Cx-AV-Req(IMPI, m)

Upon receipt of a request from the S-CSCF, the HSS sends an ordered array of *n* authentication vectors to the S-CSCF using CM2. The authentication vectors are ordered based on sequence number. Each authentication vector consists of the following components: a random number RAND, an expected response XRES, a cipher key CK, an integrity key IK and an authentication token AUTN. Each authentication vector is good for one authentication and key agreement between the S-CSCF and the IMS user.

CM2:
Cx-AV-Req-Resp(IMPI, RAND1||AUTN1||XRES1||CK1||IK1,….,RANDn||AUTNn||XRESn||CKn||IKn)

When the S-CSCF needs to send an authentication challenge to the user, it selects the next authentication vector from the ordered array, i.e. authentication vectors in a particular S-CSCF are used on a first-in / first-out basis.
The S-CSCF sends a SIP 4xx Auth_Challenge i.e. an authentication challenge towards the UE including the challenge RAND, the authentication token AUTN in SM4. It also includes the integrity key IK and the cipher key CK for the P-CSCF. Draft-ietf-sip-digest-aka-01 [17] specifies the fields to populate corresponding parameters of authenticate challenge.

SM4:
4xx Auth_Challenge(IMPI, RAND, AUTN, IK, CK)

When the P-CSCF receives SM5 it shall store the key(s) and remove that information and forward the rest of the message to the UE i.e.

SM6:
4xx Auth_Challenge(IMPI, RAND, AUTN)

Upon receiving the challenge, SM6, the UE takes the AUTN, which includes a MAC and the SQN. The UE calculates the XMAC and checks that XMAC=MAC and that the SQN is in the correct range as in [1]. If both these checks are successful the UE calculates the response, RES, puts it into the Authorization header and sends it back to the registrar in SM7. Draft-ietf-sip-digest-aka-01 [17] specifies the fields to populate corresponding parameters of the response. It should be noted that the UE at this stage also computes the session keys CK and IK.

SM7:
REGISTER(IMPI, RES)

The P-CSCF forwards the RES in SM8 to the I-CSCF, which queries the HSS to find the address of the S-CSCF. In SM9 the I-CSCF forwards the RES to the S-CSCF.
Upon receiving SM9 containing the response, the S-CSCF retrieves the active XRES for that user and uses this to check the response sent by the UE as described in Draft-ietf-sip-digest-aka-01 [17]. If the check is successful then the user has been authenticated and the IMPU is registered in the S-CSCF. If the IMPU was not currently registered, the S-CSCF shall send a Cx-Put to update the registration-flag to *registered*. If the IMPU was currently registered the registration-flag is not altered.

3. SIM access to IMS – Architectural options to be considered:

IMS security requires two 128 bit-keys, whereas GSM AKA only provides one 64 bit key. Three possible alternative approaches to solve this issue are:

1. Apply conversion functions similar to those in TS 33.102 (section 6.8.2.) in the UE and either in the:
   - HSS, or
   - S-CSCF

Advantage: Re-usage of existing protocols is allowed; i.e., the IMS AKA, or Digest-AKA.
Disadvantage: This solution might provide weak security, because the keys do not become stronger by this expansion.

2. Implement EAP-SIM or similar mechanisms in the UE and either in the
   - HSS, or
   - S-CSCF

Advantage: Enhancement of GSM AKA with some network authentication, and provision of stronger Keys. The UE can also authenticate, not only the network as in (1) above.
Disadvantage: This solution requires protocol changes, possibly in all intermediate IMS nodes.

3. Apply conversion functions similar to those in TS 33.102, but enhanced by some ideas of EAP-SIM, in the UE and either in the
   - HSS, or
   - S-CSCF

Advantage: This solution combines the benefits of (1); i.e., re-usage of protocols, and (2); i.e., security

4. Conclusions:

After the above requirements and architectural impacts and options have been presented, some conclusions are drawn and brought to the readers attention.

If the proposal is not accepted, subscribers who still use a SIM card will not be allowed to access IMS.
Operators will incur into high costs to offer IMS services because it will be necessary to provide an USIM to all IMS subscribers, and an early deployment of IMS systems could not be possible.
One should also consider that Rel. 5 UEs need to support SIM cards to be commercially successful.