3GPP TSG SA WG3 Security — S3#20 **S3-010503**

16 - 19 October, 2001

Sydney, Australia

Source:	**Siemens**
Title:	**Proposed response to LS S3z0100105 from CN4 on signalling for user authentication**
Document for:	**Discussion and Decision**
Agenda Item:	**5.3**

Abstract

This document contains a proposed response to an LS from CN4. The LS from S2 stated that " different service profiles may be assigned to different S-CSCFs even when these service profiles have the same Private ID". It is argued in this document that, while it would be feasible for S3 to define the security procedures for this case, it would introduce considerable complexity. Therefore, S2 is asked to reconsider their approach and, if ever possible, base Release 5 of IMS on the assumption that only one S-CSCF is assigned to one Private ID at any one time. This seems in line with the approach that the complexity of Release 5 specifications should be minimised.

Source:	**TSG-SA WG3**
To:	**TSG-CN WG4**
Cc:	**TSG-SA WG2, TSG-SA CN1**
Title:	**Response to LS from CN4 (N4-010969) on signalling for user authentication**
Contact person:	**Guenther Horn** Guenther.horn@mchp.siemens.de Phone: +49 89 636 41494

1. Answers to questions raised by CN4:

This LS contains the response from SA3 to N4-010969= S3z0100105, an LS received from CN4 in SA3#19bis (14th September, 2001):

- Second bullet of N4-010969:

It is stated that concerns arose in CN4 because of the sentence in the liaison from SA3 (S3-010387) (= N4-010943) ".... that SA3 sees no need for Authentication Failure Reporting or Positive Authentication reporting back to the HSS". SA3 believes that there should be no reason for concern do not apply here. The following section is meant to clarify this:

Clarification:

The newly introduced flag in S3-010355 is needed: The reason for introducing this flag was the handling of mobile terminated calls while initial registration is still in progress and not successfully completed.

This flag shall be stored in the HSS together with the S-CSCF name. The aim of the flag is to indicate whether a particular public identity of the user is unregistered or registered at a particular S-CSCF or if the initial registration at a particular S-CSCF is pending. The HSS receives the information about this state (together with the S-CSCF name and the user identity) from the S-CSCF with which (re-) registration of the user is carried out only when a *Cx-Put* message is sent from the S-CSCF to the HSS. (This is at least the case when the state of the flag changes.)

In case of an initial registration this is necessary in message 8 of S3-010355, where the flag is set to “initial registration pending”. But also in the Cx-Put message after successful / unsuccessful authentication, where the flag is reset to “registered” or “unregistered”, respectively, resolving the “initial registration pending” state.

This is different for re-registration (cf. S3-010355, section3). Here, the flag will never be in the status “initial registration pending” as the user is already registered. Therefore, at the beginning of a re-registration (cf. S3-010355, figure 5) the state of the flag in the HSS is always “registered”. Therefore message 6 and 7 are optional, as the S-CSCF may detect that this is a re-registration.

Whether the content of the flag has to be changed in the HSS in course of the re-registration procedure, depends on the policy of the home provider in the S-CSCF for the handling of an unsuccessful re-registration.

First case: User is de-registered after unsuccessful re-registration.
In this case the flag would be set to “unregistered” and an appropriate message would be sent from the S-CSCF to the HSS.

Second case: User remains registered until the lifetime of the previous successful registration expires. Then even in the case of an authentication failure, the flag in the HSS remains in the state “registered” and therefore no information has to be sent to the HSS.

- Third bullet of N4-010969:

It is asked for a clarification how the validation of public identities described in S3-010402 (= N4-010945) should be carried out.

It is proposed to validate the public identities in the HSS (i.e. alternative 2 of S3-010402 shall be used).

Clarification:

The underlying problem to be solved is that there is no security relation between the public user identity IMPU and the private user identity IMPI. Therefore it has to be checked if the IMPI and IMPU sent in a register message belong to the same user. The IMPI and all associated IMPUs for a certain user are stored in the HSS together with the appropriate service profiles.

In course of a (re-)registration there are several requests from the I-CSCF and the S-CSCF to the HSS, e.g. Cx-Query, Cx-Put, Cx-Pull, Cx-AuthDataReq (Cf. S3-010355). All these messages contain the subscriber identity (i.e. IMPI and IMPU received by the CSCF in the register message). In order to create the appropriate response messages the HSS has to find the appropriate IMPI in its storage and subsequently the requested IMPU has to be found. Therefore the check, if IMPI and IMPU belong to the same user has to be carried out by the HSS anyhow. If IMPI or IMPU do not belong to the same user the response messages has to indicate the failure by an appropriate failure code.

2. Actions:

none