3GPP TSG SA WG3 Security — S3#20 **S3-010502**

16 - 19 October, 2001

Sydney, Australia

Source: **Siemens**

Title: **Proposed response on LS S3z0100109 from SA2 on the usage of public user identifiers and the assignment of S-CSCFs**

Document for: **Discussion and Decision**

Agenda Item: **5.3**

Abstract

This document contains a proposed response to an LS from S2. 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-SA SA2**

Cc: **TSG-CN WG1, TSG-CN WG4**

Title: **Response to LS from SA2 (S2-012456= S3z0100109) on the usage of public user identifiers and the assignment of S-CSCFs**

Contact person: **Guenther Horn**

Guenther.horn@mchp.siemens.de

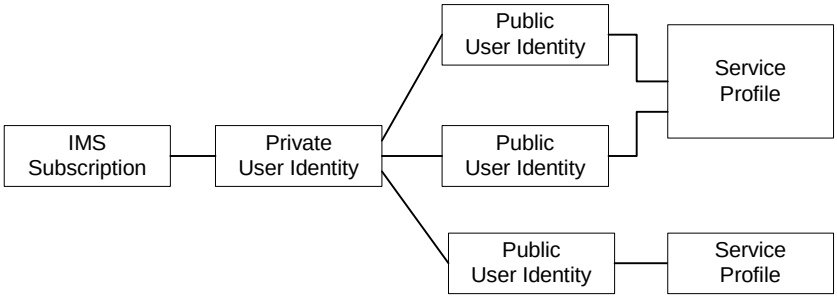
Phone: +49 89 636 41494

---

1. Overall Description:

This LS contains the response from SA3 to S2-012456 = S3z0100109, an LS received from SA3 in SA3#19bis (14th September, 2001).

In S2-012456 SA2 presents the scenario for the relation of public and private user identities and associated service profiles that should be supported by the IMS in Release 5.



Based on this scenario SA2 further describes the principles for the selection of S-CSCFs. One of these principles is that different service profiles may be assigned to different S-CSCFs, even when the service profile belongs to the same private user identity.

In principle the security architecture for IMS can be designed in such a way that the use of different S-CSCFs for one Private ID can be supported.

SA3 would however like to point out that this would significantly increase the complexity of security procedures compared to a scenario in which all public user identities belonging to a particular private user identity would be registered at the same S-CSCF at a given time:

- The P-CSCF at which the user is roaming may have to hold and manage a security association for each S-CSCF on which the user is registered. This implies that the same multiple of security associations would have to be held and managed at the P-CSCF simultaneously, as registrations are active on different S-CSCFs simultaneously. This includes in particular the storage of an appropriate multiple of keys for integrity and optional confidentiality protection (each key has a length of 128 bits).
- Furthermore, for each new SA, an IMS authentication and key agreement procedure has to be run which adds considerably to the required signalling and the load on the HSS.
- The same increase in complexity would also have to be managed on the terminal side.
- In particular, the ISIM (=IMS USIM) would have to handle several sets of keys in parallel. This functionality is currently not supported (assuming that the ISIM is modelled after the USIM).
- When only one S-CSCF is assigned to one private ID at a time it would be possible to have only one IMS authentication and key agreement procedure (when the first registration occurs) and one security association at a time, cf. also the report of S3#19 which states in this context: " It was noted that network initiated re-authentication would greatly reduce the complexity and that one SA would then be sufficient, providing flexibility to operators to define their own authentication policies." Please note that S3 have accepted a requirement for network initiated re-authentication in the meantime and that CN1 has agreed to provide a solution for network initiated re-authentication.

2. Actions:

For the complexity reasons given above, SA3 kindly requests SA2 to reconsider their approach and inform S3 whether S2 could accept for Release 5 that all public user identities belonging to the same private user identity are always registered at the same S-CSCF at any one time. This would be very much appreciated by S3. This suggestion seems to be in line with general efforts to reduce the complexity of Release 5 specifications.