

Source: BT
Subject: S-CSCF issues and security in IM CN SS
Purpose: Discussion

Agenda item:

The contribution from Ericsson on Authentication and Protection mechanisms for IM CN SS (S3z00010) has been reviewed, SA2 is developing 23.228 IM Stage 2. Based upon these documents the following comments need discussion:

1. S3z00010 states “It is the policy of the HN that decides if the S-CSCF shall be located in either HN or VN.” 23.228 outlines the support of S_CSCF in the HN or SCSCF in the VN. It is important that the resulting S3 specifications provide equal support to S-CSCF when supported in the HN or the VN. Specifically the diagrams and text within S3 reports and specifications should clearly show the support of SCSCF in both HN and VN. In particular the current diagram in S3z00010 (and any subsequent incorporation into S3 documentation) should be revised to show the SCSCF in the HN, and also to show the SCSCF in the VN (two figures may be useful).
2. TS 23.228 outlines that the Cx interface (between S-CSCF and HSS) pass the subscriber profile 9amongst other aspects). The relationship of this information transfer and the transfer of security parameters e.g. CK, IK etc from the HSS to the S_CSCF needs to be determined. The transfer from the HSS to the S_CSCF needs to be standardised to take into account the possibility to support S_CSCF in both HN and VN.
3. It is understood that the P-CSCF will hold some security information (e.g. CK/IK). The mechanisms needed to transfer these security parameters from the HSS to the P-CSCF needs to be made clear in relation to the current architecture and interfaces. The relationship of this requirement and the information transfer between the HSS and S-CSCF also needs to be determined.
4. The S3 specifications need to clarify the requirements and operator configurable options for preventing internal IP addresses and internal network topology from becoming visible to other network operators or UE,s For example, 3G TS 23.228 V1.0.0 (2000-09) contains the following (with some unapproved additions from discussion documents shown in *italics*). These aspects need to be discussed and any suitable conclusion on the requirements recorded within the S3 specifications.
 - **Network configuration hiding:** It is a requirement that it shall be possible to hide the network topology from other operators. It shall be possible to restrict the following information from being passed outside of an operator’s network: exact number of S-CSCFs, capabilities of S-CSCFs, or capacity of the network. Hiding requirements of P-CSCFs are for further study (Note that UE needs to have the address of P-CSCF).**Editor's Note: The material in this paragraph needs to be further clarified.** *It shall also be possible to hide internal network topology from UEs within the operator’s network including: addresses of S-CSCFs, and IP addresses of other UEs. The only information known by the UE should be the address of its corresponding P-CSCF (and any entity used as first hop for the bearer channels within the network).*
 - **Restrict access from external networks.** The signaling solution shall allow the operator to restrict access from external networks (application level).
 - **Access to HSS.** A network operator can control access to the HSS.
 - **The UE’s address shall be protected and if necessary hidden from any entity other than its corresponding P-CSCF in the local network (whether it can also be known by the S-CSCF is FFS).**