3GPP TSG SA WG3 Security — S3#29 **S3-030460**

15 – 18 July 2003

San Francisco, USA

Source: **Ericsson / Nokia / Nortel Networks / Siemens / T-Mobile / Vodafone**

Title: **HSS/HLR-related security architecture guidelines**

Document for: **Discussion and decision**

Agenda Item: **7.9 Subscriber Certificates, 7.10 3G-WLAN interworking, 7.18 Presence, 7.20 MBMS**

Abstract

This document proposes guidelines, which are to be documented in the meeting minutes.

1. HSS-related design guidelines for a security architecture

It is recommended that these guidelines are taken into account for all features currently being specified for 3GPP Release 6, and features in future releases. It is certainly not possible nor desirable to make any changes to earlier Releases. It is also clear that often a trade-off has to be made between these guidelines and other criteria, e.g. regarding service provision or the impact on other entities. However, it should be noted that the HSS is arguably one of the most valuable assets of an operator.

1. The number of different types of interfaces to the HSS should be minimised in order to keep the complexity of the HSS low. This applies in particular to interfaces over which authentication vectors are retrieved from the HSS as they are highly security-critical.

2. For reasons of HSS and AuC-performance, the overall number of authentication vectors requested from the authentication centre as well as the number of requests should be kept low. Mechanisms, which make economical use of authentication vectors, should be preferred. In particular, mechanisms, which avoid bursts in authentication vector requests, should be preferred.

3. The number of nodes with access to authentication vectors should be limited in order to reduce the possibility of illegitimate access to authentication vectors.

4. The number of authentication domains (e.g. CS and the PS domain, the IMS, 3G-WLAN interworking, presence and MBMS) as well as the number of nodes within a domain for which authentication vectors for one user are stored (e.g. 3GPP AAA servers) should be kept small. This is to avoid frequent re-synchronisation. Re-synchronisation problems do not occur if unused AVs are forwarded to other nodes where they are needed, as is the case e.g. with VLRs in the same PLMN.

5. Mechanisms should be designed in such a way that the effect of a compromise of authentication information in one authentication domain on other domains is minimised.

6. Authentication information should be securely stored in nodes and securely transported between nodes.

Terminology: The notion of “authentication domain” is used here to denote a subsystem of a 3G network, which uses authentication vectors.

Conclusions and Proposal

HSS-related design guidelines for security architecture were presented here. It is proposed that these guidelines are taken into account for all features currently being specified for 3GPP Release 6, and features in future releases. It is certainly not possible nor desirable to make any changes to earlier Releases. It is proposed that SA3 approves these guidelines and, if approved, they are recorded in the meeting minutes.