3GPP TSG SA WG3 Security — S3#29 **S3-030412**

15 – 18 July 2003

San Francisco, USA

Source: **Siemens**

Title: **HSS/HLR-related security architecture issues and implications for presence, MBMS and support for subscriber certificates**

Document for: **Discussion and decision**

Agenda Item: **7.9 Subscriber Certificates, 7.18 Presence, 7.20 MBMS**

Abstract

The 3G authentication and key agreement protocol was designed in Release 99 with only two domains in mind, the circuit and the packet domain. Since then, more uses of the protocol within 3GPP have been identified for various applications. The security solutions for these applications were largely developed independently, without a view of the resulting overall architecture. This may lead to a proliferation of similar, but different methods. This contribution addresses potential problems arising from this situation. It focuses on the HSS and the HLR which arguably are the most valuable assets of an operator. The contribution proposes certain architectural design rules for security solutions currently being developed or future security solutions in 3GPP. The implications of these rules on the security for presence, MBMS, and the support for subscriber certificates are briefly addressed.

---

1. Introduction

Over the past years, a number of uses of the 3G authentication and key agreement protocol within 3GPP have been identified for various applications.

Release 99: the 3G AKA protocol is used for the circuit and the packet domain. The interface between the nodes consuming authentication vectors, i.e. VLR and SGSN, and the HLR is MAP-based.

Release 5: the http digest aka protocol is used for authenticating IMS users. The interface between the nodes consuming authentication vectors, i.e. the S-CSCFs, and the HSS is the Cx-interface.

Release 6: several new uses of the 3G AKA protocol are being proposed. The following is a, hopefully, complete list of proposals currently under discussion.

- the EAP-AKA protocol has been proposed for authenticating a 3G user requesting to communicate over a WLAN. The interface between the nodes consuming authentication vectors is the Wx-interface between the 3GPP AAA server and a Release 6 HSS, and the D' interface between the 3GPP AAA server and a pre-Release 6 HSS/HLR;

- the http digest aka protocol has been proposed for authenticating a 3G user to a Bootstrapping Server Function (BSF), e.g. in the context of the provision of subscriber certificates. The interface to the HSS is "Cx-like", requirements for this interface have been proposed, but no specification is available yet;

- a variant of the http digest aka protocol (http digest akav2) has been proposed for authenticating a 3G user communicating over the Ut (formerly: Mt) reference point, e.g. in the context of presence services. The node consuming authentication vectors may be an authentication proxy or an application server, the interface to the HSS may be "Cx-like", requirements for this interface are not yet available;

- MBMS security needs to be bootstrapped. It is likely that the UE and the BM-SC will authenticate using a variant of the http digest aka protocol, the interface between BM-SC and HSS is currently not known.

More proposed uses may be upcoming. In particular, the following feature may have to be considered:

- For 3G users requesting access to 3G services over a WLAN (so-called scenario 3) a UE-initiated secure tunnel, terminating either in the home or a visited PLMN, has been proposed. No consideration has been given up to now to the key management to set up such a secure tunnel, but the re-use of 3G AKA may play a role here as well.

All the interfaces to the HSS allow network nodes to retrieve authentication vectors from the HSS.

Terminology: the notion of "authentication domain" is used here to denote a subsystem of a 3G network which uses authentication vectors. Examples are the CS and the PS domain, from where the terminology is derived. In addition all the uses of the 3G AKA protocol listed in this section refer to different authentication domains. This terminology may be useful when discussing synchronisation issues, see section 2.

2. HSS/HLR-related security architecture issues

The issues below are believed to be standardisation-relevant, and not only a matter of deployment and operation, as they affect architectural design decisions. The order is not necessarily one of priority.

1. **Complexity of the HSS/HLR:** an HSS is designed to serve a very large number of users in a very efficient way. Its complexity should be kept reasonably low. Different types of interfaces with similar functionality would unnecessarily add to the complexity of the HSS. It is therefore suggested to reduce the number of different types of interfaces to the HSS as much as possible.

2. **Performance of the Authentication Centre in HSS/HLR:** an authentication centre attached to an HSS or HLR may serve several millions of users. Its performance is therefore crucial. Hence, the number of authentication vectors requested from the authentication centre should be kept low, and sudden bursts in authentication vector requests should be avoided. Mechanisms which make economical use of authentication vectors should be preferred. In addition to the considerations on the authentication centre, it should be kept in mind that the handling of requests for authentication vectors also consumes non-negligible resources in the HSS or HLR, and in the transmission network between the requesting node and the HSS or HLR.

3. **Illegitimate access to authentication vectors**: the possession of AVs makes it possible to mount false base station attacks on 3GPP networks. Any interface over which AVs can be retrieved from the HSS, and any node where AVs are handled, are therefore very security-sensitive. An attacker may try to **physically attack** such a node. But the more such nodes exist the more difficult it may be to physically protect them. An attacker may also try to **remotely hack** such a node by exploiting security holes in the functionality present on the node. There more different types of nodes with access to AVs there are, there more likely it is that a security hole in a function implemented on the node exists. Security would therefore be enhanced if the number of nodes, and the number of different types of nodes with access to AVs would be limited.

4. **Synchronisation problems:** the USIM may trigger a re-synchronisation procedure if the sequence number is not in the correct range. This can occur under certain conditions in regular operations, when a user switches back and forth between two nodes which both store authentication vectors related to the user. Sequence number management schemes have been introduced in Annex C of TS 33.102 to limit this effect. In particular, the array mechanism was introduced to enable the use of the 3G AKA protocol independently in each authentication domain, i.e. the use of the protocol in one domain does not affect the other. The separation occurs through the use of different values of the parameter IND in different domains. IND is a part of the sequence number. IND has five bits (according to the optional interoperability guidelines of Annex C.4 of TS 33.102), so a maximum of 32 domains can be distinguished. However, depending on the policy of requesting authentication vectors (number of authentication vectors in a batch), storing them in a requesting node and forwarding them between nodes, it may be advisable to assign several IND-values to a single domain in order to achieve the desired effect of reducing re-synchronisation. The latter will apply to the CS and the PS domain, whereas a single IND value for a domain may suffice e.g. if a single 3GPP AAA server is used for 3G-WLAN interworking.
   The generation of AVs specific to several authentication domains could be seen as being in conflict with a high performance of an authentication centre, as it may make it difficult to pre-compute and store AVs and, in such a way, buffer bursts of AV requests and reduce authentication delay. But to a certain extent, this could be alleviated by restricting pre-computation of AVs to domains with the largest number of AV requests and/or the most stringent delay requirements.
   The consideration in this clause suggests economical use of the space of IND-values. In particular, it means that the number of authentication domains as well as the number of nodes within a domain for which authentication vectors for one user are stored should be kept small.

5. **Man-in-the middle attacks in tunnelled authentication:** this issue is not particular in any way to the 3G AKA protocol. It may occur whenever a client authentication protocol is run through a server-authenticated tunnel and the client's credentials may be used in different contexts, e.g. inside and outside a tunnel. This issue was discussed in SA3 in the context of the possible use of PEAP and similar schemes for 3G-WLAN interworking, as well as in the context of the use of http digest aka for security of the Ut (formerly: Mt) interface. One way to make sure that these attacks are not possible is to ensure that the same client credentials are used in only one context. This could be achieved in a uniform way by ensuring that client credentials (authentication responses) are derived from keys which are different for each application context (authentication domain), i.e. by ensuring the cryptographic separation of authentication domains.

3. HSS-related design guidelines for a security architecture

This section summarises the conclusions drawn in section 2. 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 also clear that often a trade-off has to be made between these guidelines and other, e.g. service-related, criteria.

1. The number of different types of interfaces to the HSS should be limited in order to keep the complexity of the HSS low. If at all possible, there should be only one interface to retrieve authentication vectors from the HSS in addition to the legacy MAP-interface.

2. For reasons of HSS and AuC-performance, the 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.

3. The number of nodes, and the number of different types 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 as well as the number of nodes within a domain for which authentication vectors for one user are stored and not forwarded should be kept small. This is to avoid frequent re-synchronisation.

6. Mechanisms which ensure in a uniform way that the same client credentials are not used in different contexts should be preferred in order to prevent man-in-the-middle attacks in tunnelled authentication. Cryptographic separation of authentication domains is to be achieved.

4. Implications for presence security

Three proposals have been presented so far for security at the Ut (formerly: Mt) reference point. A companion contribution by Siemens evaluates these proposals also with respect to the guidelines suggested here.

5. Implications for the architecture to support subscriber certificates

The current version of the TS on subscriber certificates foresees a new run of protocol A, and hence the consumption of an authentication vector, for each request of a NAF to a BSF to obtain a key. This is not well in line with guideline 2 in section 3. A solution where keys are derived in the BSF for various NAFs from one CK, IK would reduce the required number of AVs. Such a solution is described in a companion contribution by Siemens. It also achieves cryptographic separation of authentication domains.

6. Implications for MBMS security

A companion contribution by Siemens evaluates alternative security solutions for MBMS also with respect to the guidelines suggested here.

Conclusions and Proposal

HSS-related design guidelines for a 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. In order for the guidelines not to get lost, it

is proposed to record them in a way that they can be referenced later, e.g. in an informative Annex to TS 33.102, Release 6.