3GPP TSG SA WG3 #14 **S3-000482**

01-04 August, 2000

Kjeller, Norway

Source:	**SA WG3**
To:	**CN WG4**
CC:	**TIA TR-45 AHAG**
Title:	**Evaluation of the impact on positive authentication reporting on network performance**
Document for:	**Evaluation**
Agenda Item:	**tbd**

Introduction

At the SA3 #14 meeting in Stockholm there was a joint meeting between SA3 and TIA TR-45 AHAG on harmonization of 3GPP and 3GPP2 security standards. In particular, the two groups discussed how to make 3GPP AKA the common international Authentication and Key Agreement standard for 3G.

During the joint meeting a few features were identified that TIA TR-45 AHAG would want SA3 to include in the UMTS security architecture. One of these features is the possibility of having a positive acknowledge of the use of the Authentication Vectors at the request of the home network.

At the SA3#14 meeting SA3 then sent an LS to CN4 requesting advice on this issue (S3-000308). At the joint CN/SA3 meeting in June 2000, CN4 informally asked for more time to complete the evaluation analysis. At the same time the question was asked whether the positive authentication reporting mechanism could be limited to only apply to 3GPP – 3GPP2 communications. The answer appears to be "yes".

At SA3#14 this question was discussed and it became clear that there is no internal 3GPP requirement for a positive authentication reporting mechanism.

SA3 has also had some informal advice from AHAG members on this subject and it has become clear that positive authentication reporting is most likely to be requested for the first successful authentication carried out when the 3GPP2 subscriber roams onto a 3GPP network, but other circumstances exist at the HLR's option.

Given this, SA3 assumes that this feature would not impose a large network load, but we will want CN4's advice to confirm or reject this assumption.

SA3 therefore kindly requests CN4 for advice on what impact such mechanism might have on network performance and if CN4 foresees any problems in implementing such mechanism within 3GPP networks. We also confirm that this LS supersede the previous LS contained in S3-000308.

Authentication Status Reporting

The UMTS Security Architecture already contains the feature “Authentication Failure Report” which provides a mechanism for the VLR/SGSN to report authentication failures back to the HLR.

However, this is not sufficient for TIA TR-45 AHAG since they also have a requirement that the VLR/SGSN should be able to report successful authentications. So to facilitate roaming between 3GPP and 3GPP2 systems it may become a requirement that a 3GPP SN should be able to report successful authentications to 3GPP2 systems.

Taking this as a starting point, what seems to be required is that the current 3GPP Authentication Failure Report mechanism be extended to also be able to report successful authentication.

The shaded section below is a rewritten version of chapter 6.3.6 from TS 33.102 (v3.4.0) that should provide CN4 with a rough idea of what the generic authentication reporting mechanism might look like.

6.3.6 Reporting authentication ~~failures~~ results from the SGSN/VLR to the HLR

The purpose of this procedure is to provide a mechanism for reporting authentication ~~failures~~ results from the serving environment back to the home environment.

The procedure is shown in Figure 13.

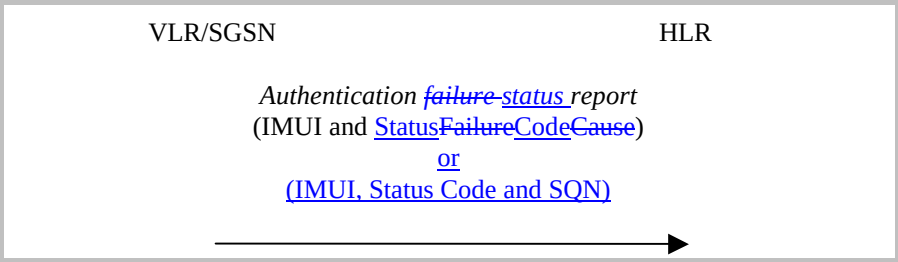

Figure 13: Reporting authentication ~~failure~~ results from VLR/SGSN to HLR

The procedure is invoked by the serving network VLR/SGSN when the authentication procedure fails or if the HLR requires authentication status reporting. The *authentication ~~failure~~ status report* shall contain the subscriber identity and a ~~failure cause~~status code. The possible failure causes are either that the network signature was wrong or that the user response was wrong.

When reporting successfull authentication the report shall contain the the sequence number SQN such that the HE can uniquely determine which AV was used. A successful report is likely to be sent on an initial registration and only when explicitly requested by the HLR.

The HE may decide to cancel the location of the user after receiving an *authentication ~~failure~~ status report* indicating that the authentication failed.

At this point in time SA3 has not decided whether or not we will recommend this change to the existing mechanism.

One concern that has been voiced is that reporting successful authentication may be expensive to operate in terms of network performance.

We appreciate that it may be difficult to estimate the network performance impact of the mechanism since it probably will be difficult to forecast the number of subscribers roaming from 3GPP2 systems onto 3GPP systems.

Nevertheless, SA3 would be grateful for some advice from CN4 on the proposed mechanism and we would in particular be grateful to receive comments on how to specify such mechanism to avoid unnecessary network loading.

SA3 therefore kindly requests CN4 for advice on what impact such a mechanism might have on network performance and if CN4 foresees any problems in implementing such mechanism within 3GPP networks.