TSG-SA WG3 (Security) meeting #17 **S3-010068**
GÖTEBORG, 27th February – 2nd March 2001

Agenda Item: TBD
Source: Lucent
Title: Authentication Positive Notification Procedure

Document for: Discussion and Decision

1 Introduction

This contribution proposes changes to the TS 33.102 v3.5.0 that address the needs expressed by ANSI-41 (S3-000566, included for information in Annex 1). Additional clarifications have been presented to S3 in contribution S3-000592 (from TR45.2.2 – Authentication Focus Group) and also included below:

> "TIA Subcommittee TR-45.2 has identified the need for a serving network (SN) to confirm that a successful Authentication and Key Agreement (AKA) has been completed by the SN for a specific subscriber. The SN would report the successful establishment of the new Security Association to the home network (i.e., HLR) when a subscriber first appears in the serving system.
>
> This capability would always provide the HLR with an indication of the success of AKA by the SN. In conjunction with an indication from the SN of an AKA failure, the HLR would always receive a report of the outcome of AKA, even if an event (e.g., MS power-down prior to completion of AKA in a new SN) interrupted normal processing of the intersystem operations required for roaming.
>
> This capability would prevent potential denial of service attacks in environments where a subscriber can roam into both:
>
> a. 3GPP systems using *AK*A
>
> b. Other systems that do not implement authentication
>
> One set of potential attacks is based on the limitations of an Interworking Function (IWF) needed for interworking between GSM-based systems and ANS-41 systems. These limitations are due to specific implementation aspects of the IWF (e.g., the unique identity of the VLR is not provided to the HLR) and to the inherent differences in the intersystem operations of the two types of networks."

The proposed new functionality is targeted for UMTS Release 4 implementations.

2 Successful Authentication Notification

TS 33.102 v3.5.0 (clause 6.3.6) describes a procedure, detailing the requirements for an authentication failure report (AFR), used to inform the Home Environment (HE) about an authentication failure.

This contribution proposes to add to the TS 33.102 v3.5.0 a new clause (or include this functionality in clause 6.3.6), detailing the requirements for an "*Authentication Success Notification*".

The *Successful* A*uthentication Notification* (**SAN**) shall include the subscriber's identity, the serving system's identity, the serving system's capability and the RAND associated with a successfully executed AV.

As requested in S3-000566 (attached), at the HLR's option, the Serving Network (SN) must notify the HLR (HE) when a new Security Association (SA) is created (i.e. new AV is successfully used).

It was further clarified by S3-000592 that this notification is mandatory when a subscriber first appears in the serving system**.**

2.1 Authentication Data Response "Indicator"

An optional SAN indicator (one bit) shall be included in the Authentication Data Response message. This optional parameter (SAN="1") shall be set by the HE to indicate to the Serving Node that an Authentication Success Report is expected after the AV is successfully executed. (or the 1st AV successfully executed, if multiple AVs are included within one Authentication Data Response). The HE has the means to identify when a subscriber 1st registers into a new system, therefore it is expected that the HE will request the SAN at the appropriate time. (e.g., when a subscriber first appears in the serving system).

2.2 Authentication Success Notification Procedure

The SAN shall be implemented as an "one time event", i.e.., shall be generated only once by the serving node, in response to a specific home system request, e.g., an SAN bit in the Authentication Data Response (ADR). If multiple AVs are delivered within one Authentication Data Response message, then the SAN shall be delivered only once, i.e., after the 1st AV is successfully used. This will significantly minimize the potential impact of the new SAN on the overall network performance or traffic bandwidth capacity. An SAN shall be triggered only by a specific directive from the HE.

Note that, by including the RAND in the SAN, the HE can easily identify the AV that has been successfully used to establish the security association, if any potential post-analysis is desired.

2.3 Authentication Success Notification Elements

To be effectively used and analysed by the Home Entity (HE), the SAN shall include the following elements (with the exception of RAND, those elements may be an integral part of the SAN, or be already part of the message used to deliver the SAN e.g., Location Update; the elements shall not be duplicated):

- **User ID.** – This element is needed to identify the user associated with the successful authentication process
- **Serving System Identity.** – This element is needed to identify the serving node physical location.
- **System Capability** – This element can be used to identify the Serving Node as a 3GPP or 3GPP2 system and as well as to indicate to the HE the security capability of a serving node. This parameter is part of the ANSI-41 information flow, and the parameter is needed for interworking between a 3GPP and 3GPP2 system.
- **RAND** – The RAND number can be used to uniquely identify the specific AV that failed authentication, This information can assist in determining which AV has been successfully executed. This parameter is part of the ANSI-41 information flow, and the parameter is needed for interworking between a 3GPP and 3GPP2 system.

3 Conclusions

A new clause 6.3.X in TS 33.102 v3.6.0 shall be included detailing the requirements for an Authentication Success Notification (alternatively, section 6.3.6 can be modified to include both the AFR as well as the SAN). The notification shall be triggered by a specific request from the HE. The notification shall include the following elements:

- User ID (e.g., IMSI).
- Serving Node address.

- Serving System Capability
- RAND

The exact implementation details, i.e., need for a separate message, or integrated the notification within an existing message, are left to the CN4 discretion, ideally the protocol should correspond to an equivalent ANSI-41 protocols as much as possible.

An optional SAN indicator (one bit) shall be included in the Authentication Data Response message.

It should be noted that, based in our current understanding, this notification will not be requested by a 3GPP HE. It is further understood that an ANSI-41 system may request this notification on first network access only. CN4 is strongly encourage to consider the network performance implications associated with this new message, and liaison with ANSI-41 AHAG and TR45.2 subcommittee to ensure that the interworking protocol is optimised and agreed upon.

ANNEX1:

3GPP TSG SA WG3 Security — S3#15 S3-000566

12-14 September, 2000
Washington D.C., USA
TR-45 AHAG/ TR-45.2 Home Control IssuesTR-45.AHAG/2000.09.12.05

Home Control of AKA Issues

1 Revocation of AVs

In response to 3GPP S3's request for clarification regarding Authentication Vector (AV) revocation, the TR-45 AHAG and TR-45.2 request that the HLR (HE) have the capability to:

Revoke all AVs associated with a particular subscriber immediately (Service-affecting).

Revoke the current AV after current services are rendered (Non-service-affecting).

Either command may be accompanied by new AVs.

2 Authentication Success Report

At the HLR's option, the Serving Network (SN) must send an authentication success report to the HLR (HE) when a new Security Association (SA) is created (i.e. new AV is used).
The authentication success report allows the HLR (HE) to monitor the duration of the SA within the SN, which may be helpful to ANSI-41 service providers in preventing/reducing fraud. Also, it may prevent certain denial of service attacks unique to ANSI-41 networks due to the method in which ESN/MSID pairs are validated within ANSI-41 UIMs.

3 3GPP–3GPP2 Reporting

The positive authentication reporting mechanism may be limited to only apply to 3GPP-3GPP2 communications. However, a 3GPP SN must handle a 3GPP2 HLR (HE) request for authentication success reporting.