3GPP TSG SA #6 **Tdoc TSG SA SP-99591**
Nice, FRANCE
15th - 17th December 1999

Source: TSG SA WG3

Subject: LS to SA
Agenda item: 5.3

This document Liaison Statements agreed by SA WG3 #9 to be presented to SA#6. In addition, an LS in SP-99503 had been sent (in a copy) to SA by SA WG3 #8.

Tdoc S3-99	Topic
537	LS to TSG-CN, CN-2, cc: SA, on A mechanism for reporting authentication failures from VLR/SGSN to HLR
551	LS to TIA TR-45 Plenary, cc: TIA TR-45.2, TIA TR-45 AHAG, 3GPP TSG SA, on 3GPP AKA proposal as presented in TIA TR-45.2./99.11.08.09
553	LS to TSG-SA and TSG-CN on MAP security
554	LS to SA, SA2, CN and CN OSA ad-hoc: Statement on security issues in VHE/OSA (answer to S2-99E05)

TSG-SA WG3 (Security) meeting #9
Helsinki, 6-9 December, 1999

TSGS-WG3#9(99)537

Source: TSG-SA3

To: TSG-CN, CN-2

Copy: TSG-SA

Title: A mechanism for reporting authentication failures from VLR/SGSN to HLR

S3 wants to inform N2 that a new mechanism for reporting authentication failure from VLR/SGSN to HLR is being specified in TS 33.102.

The mechanism itself is quite simple and only consists of an *authentication failure report* from VLR or SGSN to HLR. HLR will then acknowledge the *authentication failure report*.

The *authentication failure report* will need to contain the user identity (IMSI) and a failure cause code information element. The only two codes identified so far is:

- wrong network signature
- wrong user response

S3 recognises that this request comes very late for R99 and we apologise if this causes unnecessary problems for N2, but we only very recently became aware that UMTS entirely lacks a mechanism for reporting authentication failures from the serving network back to the home environment.

Since authentication failures may be an indication of an active attack against the networks, it is important that the home environment is informed about authentication failures. S3 therefore considers it very important that this mechanism is included in R99.

Please find attached the recent S3 agreed CR 33.102-040.

TSG S3-99551

To: TIA TR-45 Plenary
Copy: TIA TR-45.2, TIA TR-45 AHAG, 3GPP TSG SA
From: 3GPP TSG SA WG3 (Security)

Subject: 3GPP AKA proposal as presented in TIA TR-45.2./99.11.08.09

SA WG3 thanks TR-45 for the liaison statement on the adoption by TR-45 of the 3GPP AKA proposal, pending a further three month evaluation period.

We look forward to offering any aid that we can on development of the proposal to meet all TR-45 requirements, and if there are any issues or clarification on which you feel we can help, then please let us know.

We would like to extend a welcome for a one day joint session (of interest to TR-45.2 and AHAG) during our meeting in Stockholm, Sweden hosted by Ericsson, and suggest the dates of 12th or 13th of April 2000. The objective will be to discuss and if necessary amend the various 3GPP(1) standards to meet the TR-45 requirements and to discuss other matters of mutual interest.

Notes:

- Details of the joint meeting will be sent out closer to the date. It may be desirable for AHAG to co-locate a parallel meeting with SA WG3.
- All our standards and documents are available on the 3GPP server at http://www.3gpp.org, access is open to all.
- SA WG3 contact point: Timothy Wright (timothy.wright@vf.vodafone.co.uk)

Tdoc S3-99553

TSG-SA WG3 (Security) meeting #9
Helsinki, 7-9 December, 1999

From: SA WG3 (Security)

To: CN, SA

Title: LS to TSG-SA and TSG-CN on MAP security

With reference to a recent liaison statement from N2 on MAP security (S3-99435=N2-99G32), S3 would like to express their disappointment that N2 cannot do the work on 3G TS 29.002 before the December 1999 TSG plenary meetings. S3 consider MAP security to be a very important feature for R99 and would request that TSG-SA allow for the MAP security work for R99 to be completed by the March 2000 TSG plenary meetings.

S3 have noted that the addition of the security header may result in a requirement to segment some already overloaded MAP messages since a size limit on the MAP payload of approximately 200 bytes (160 bytes for the first two messages of a dialogue) may be imposed by lower layers of the signalling architecture. To help reduce the impact of this, the following principles are proposed by S3:

- Where the length restriction imposed by lower layers of the signalling architecture does not exist, it must be possible to protect all MAP messages.
- Where the length restriction does exist, the following principles should be adopted:
    - All new MAP messages specified in R99 should be protected. It is appreciated that this may involve revisions to existing MAP dialogues for some new messages because the security header extends the MAP payload above the size limit.
    - Remaining MAP messages will be prioritised by S3. It is appreciated that this may involve revisions to existing MAP dialogues for some messages because the security header extends the MAP payload above the size limit. A prioritised list of MAP messages requiring protection will be produced at S3#10 (19-21 January 2000).

It is understood that a new application context would be used to distinguish messages which include the security header from messages which do not include the security header.

S3 have noted a number of other questions on MAP security from the liaison statement. A joint ad hoc meeting of experts from S3 and N2 is proposed to resolve the questions raised by N2, progress the work according to the above principles, and draft the necessary CR to 29.002. It is proposed that the meeting will be held in Darmstadt, Germany on 6th and 7th January 2000, hosted by Deutsche Telekom.

TSG-SA WG3 (Security) meeting #9 ***TSGS-WG3#9(99)554***

Helsinki, 7-9 December, 1999

From: **S3**

To: **SA, SA2, CN and CN OSA ad-hoc**

Title: **Statement on security issues in VHE/OSA**

TSG SA WG2 thanks TSG CN OSA for their Liaison statement SA2-99F07 relating to security requirements in VHE/OSA. In their LS TSG SA WG2 raises the following issue that relates to network and user security, which is considered part of the open issue on authorization and administration of User Profile highlighted in the developing Stage 2 specification (TS 23.127). SA2 states:

> The proposed OSA API provides to an Application, access to a Service Capability Server (SCSs). The authentication and authorization procedures of this API ensure that only verified applications gain access and that that access is only made available to the use of facilities and operations for which they have are authorized.
>
> However in the current definition, there is a further level of security, which is not being addressed. There is, as yet, no mechanism specified for “authentication and authorization user access to the application and user specific data at the application”. Having authorized an application to use a specific method, there is no control over how that method is used or for which particular data set its use would be valid.

S3 would like to point out that the Home Environment provides services to the user in a managed way, possibly by collaborating with HE-VASPs, but this is transparent to the user. The same service could be provided by more than one HE-VASP and HE-VASP can provide more than one service.

Additionally, but not subject to standardisation, the user may access services directly from Value Added Service Providers. The Home Environment does not manage services obtained directly from VASPs. A mechanism may be provided which allows the user to automate access to those services obtained directly from VASPs and personalise those services. However such a mechanism is outside of the scope of this specification. Here a HE-VASP denotes a Home Environment Value Added Service Provider. This is a VASP that has an agreement with the Home Environment to provide services.'

So S3 has the following final comments on the points mentioned:

1. Secure UA to Application End-to-End authorization is an issue between UA and application and as such transaparent for OSA.
2. Secure User Authorization to the Application via secure access to User Profile Data, (to verify that the User has subscription rights to specific applications) VHE/OSA allows applications to be registered and made available to users. Once the user selects an application (made availble through VHE) it can be assumed by the application that the user has the right to subscribe to the application.
3. The transfer of a Secure User Identity (and possibly signature) to the application, to ensure that the Application can secure access to the Appropriate internal data store at the Application/Application Server. The UMTS network will authenticate a user and a secure user identity is available. Since VHE is a mechanism to provide application to user authenticated in the UMTS network, it can be assumed that the user identity used in the UMTS network can be used as a secure user identity for application as well. So it will be a simple matter of transferring this identity to the application.