3GPP TSG SA WG3 Security — S3#10 **S3-000073**

19-21 January, 2000

Antwerpen, Belgium

Source: **Vodafone**

Title: **Report on TR45.2, 10-14 January, 2000, Panama City, Florida**

Document for: **Information**

Agenda Item:

Executive Summary

- Though left as an open issue for e-mail discussion it seems there are some significant companies with TR45 that will not accept an AKA that does not have implicit registration (first authentication using global challenge). A decision on whether to provide this or not will be made at the February (14-18) TR45.2 in San Diego.
- GTE are not satisfied with the home control given by the AKA at present. Therefore will need to provide an authentication success/failure message from the SN to the HN that gives the HN the option of continuing with the call even if the authentication fails.

Authentication Focus group

The main issues were whether an implicit registration (first authentication in an SN using broadcast challenge) solution for AKA was required or not, and the issue of home control of the authentication process ("non shared SSD").

Implicit registration

This is an issue as 2G ANSI-41 systems do not have dedicated signalling channels so authentication must take place on a full traffic channel, which can cause capacity problems, apparently.

Qualcomm and VF argued that it was not necessary, as there are ways of reducing the effects of having to assign a traffic channel for authentication. 3GPP2 systems do have dedicated traffic channels and for 2G the granting of the traffic channel can wait until the vector has got to the SN. The issue was held over until the next meeting.

Non shared SSD

This is mainly the concern of GTE. ANSI-41 allow the HN to control the authentication entirely, even to the extent of granting a call even if the authentication in the SN fails. The authentication failure report that S3 have proposed goes some way, but GTE seem to want more. This issue also is held over until San Diego.

GTE would like to see authentication success indicated to the HN. This would allow transmission of the ESN to the HN (see below).

This would also mean that the HN could delay cancellation of the previous registration of the user until the SN had confirmed that authentication was successful. This would stop the theoretical temporary denial of service attack whereby a "clone" (just with IMSI) requests service and so cause the de-registration of the legitimate subscriber somewhere else. We have put measures to stop this at an RRC layer (integrity on location update, routing area update), do we want to provide such protection at the MM layer?

Local authentication
TR45.2.2/2000.01.13.3, VF, method of local authentication with the 3GPP AKA. This paper discussed four ways of providing local authentication:

1. Use of ciphering
2. Use of integrity
3. IK as SSD-A and CK for ciphering for duration of AV use
4. IK as SSD-A and CK as SSD-B

I argued for option 3 (integrity cannot be provided in either 2G or 3G ANSI-41 systems) over option 4, as option 4 could mean that the same AV is used for a long time, which presents a risk as CK and IK were not intended to be medium-long term keys and are not protected as such (transmitted to the terminal, given to the SN, transmitted across open HN-SN links). The decision on this will happen at San Diego.

Dynamic ESN re-binding
The final implementation of the AKA for ANSI-41 will have to supply the ESN to the HN - there are still large numbers of non-authenticating phones in America. ESN is therefore still a consideration, and TR45 have not made a clean break with ESN as they go into 3G.

Next meeting

At the San Diego TR45.2 (February 14-18) meeting, authentication focus group will meet on Tuesday morning at 9 and along with the AHAG at 1pm. Cheryl will ask Chris Carroll if AHAG can meet for administration at 8 and then cease until Wednesday morning.

Tim Wright will be attending this. Those S3 companies that participate in TR45 are also asked to consider attending – detailed knowledge of the AKA is sparse in the TR45.