3GPP TSG SA WG3 Security — S3#22 **S3-020033**

25 - 28 February 2002

Bristol, UK

Title: The use of USIMs and ISIMs for IMS
Source: SA3
To: SA2
Copy: SA1, T3, CN1, T2

Contact Person:
Name: Peter Howard
Tel. Number: +44 1635 676206
E-mail Address: peter.howard@vodafone.com

Attached : TS 33.203 v1.0.0

SA3 have handled the following incoming LSs on the use of USIMs and ISIMs for IMS:

- S2-013599
- T3-020139
- S1-020577
- S1-020579
- S2-020912

Based on these LSs, SA3 have updated the relevant parts of the IMS security specification TS 33.203 which will be presented to SA#15 for approval. Section 8 is devoted to the security functions which are required to be implemented on the UICC. In particular, it is specified how a R99/Rel-4 USIM may be used to provide the IMS security functions.

TS 33.203 does not contain any guidelines on how the relevant IMS identities should be derived when a USIM is used for IMS access. This is believed to be an issue for other WGs. However, SA3 have reviewed the CR on TS 23.228 on deriving IMS identities (S2-020912) and would like to make the following comments:

1. SA3 have reviewed the security implications of deriving the IMPI and Home Domain Name from the IMSI when a USIM is used for IMS access. SA3 did not identify any security problems with this approach, even if the derivation function is reversible. Furthermore, SA3 would like to indicate that a reversible function would allow the HSS to use the IMSI as the basis for indexing the correct record in the AuC without having to maintain a large look-up table.

2. SA3 have also reviewed the security implications of deriving the IMPU from the IMSI when a USIM is used for IMS access. SA3 have assumed that unlike the IMPI, the IMPU may be published. Clearly, if the derivation function is reversible, this will increase the exposure of the IMSI. While the increased exposure of the IMSI is not considered to be a major security problem by SA3, some concerns have been raised about the implications of binding the IMPU to the IMSI. In particular, there was concern that a user receiving malicious calls may not be able to change their contact details (i.e. IMPU) without changing their UICC.

Actions:

- SA2 should consider the above comments on the implications of deriving IMS identities from the IMSI when a USIM is used for IMS access.

- The involved groups should use the IMS security specifications in TS 33.203 to guide their specification work.