Technical Specification Group Services and System Aspects *TSGS#12(01)0349*
Meeting #12, Stockholm, Sweden, 18-21 June 2001

3GPP TSG SA WG3 Security — S3#18 **S3-010289**

21 - 24 May, 2001

Phoenix, USA

Source: **TSG-SA WG3**

To: **S1, T2, T3**
Cc: **SA, T, EP-SCP**

Title: **Security and UE functionality split**

Contact: Michael Walker, Vodafone Group, SA3 Chair
Email: mike.walker@vodafone.co.uk

S3 would like to thank S1 and T3 for the liaison statements in S1-010575, S1-010166 and T3-010250 regarding possibilities for splitting UE functionality, and the potential impact of such splits on 3G security.

To set the scene for an in-depth analysis of the security implications of different functional splits it is of value to recall that the 3G security architecture was derived from that of GSM. The architecture was therefore designed to consist of two layers:

- the network layer where subscriber, or more accurately USIM, and network authentication are performed and where cipher and integrity keys are generated;
- the UTRAN layer where user traffic and signalling data are encrypted and integrity protected for transfer across the UMTS radio access network.

Moreover, the USIM is designed to be a security device where secure authentication and key generation processes can be executed without the secret subscriber key being revealed. The USIM is the only secure processor in the UE.

The implications of the design of the 3G security architecture on the UE are as follows:

1. The USIM is the only device with the UE environment that is authenticated, and by implication the IMSI is the only identity that is authenticated. Authentication of the USIM can in no way be taken to imply, either explicitly or implicitly, authentication of any other component part of the UE or any identity associated with it.
2. Only the user traffic and signalling data is afforded encryption and integrity protection and then only when transmitted over the radio access network. Communications within the UE are not provided with any cryptographic protection – so if intercepted they may be read, and may be changed without the change being detectable. In particular:
   - Keys used to encrypt and integrity protect UTRAN traffic and signalling are transferred in clear, that is to say without any cryptographic protection, within the UE from the USIM to the cipher and integrity functions within the UE. The vulnerability of these keys to interception is thus a function solely of the physical characteristics of the interface between the USIM and that component of the UE where encryption and integrity processing are performed, no protection is provided by the 3G security functions.
   - User traffic and signalling data is not provided with cryptographic protection within the UE, only on the UTRAN. The vulnerability of such data to interception or manipulation is thus a function of the

physical characteristics of the interfaces within the UE over which it flows and the components of the UE in which it is processed, no protection is provided by the 3G security functions.

3. The only device within the UE that is required for 3G security to provide an environment in which data can be processed or stored whilst remaining protected against eavesdropping or manipulation is the USIM. No other devices or components within the UE are required to possess this capability.

These three design implications can be used to analyse the security implications of different splits in the UE functionality for Release 1999 systems. Similar considerations will apply to later Releases, in particular, to IMS security features.

S3 would be pleased to undertake such an analysis. To make this an effective and efficient process, and to remove the need for a potentially lengthy exchange of liaison statements, S3 suggest that we host a one day joint meeting of S3, S1, T3 and T2 delegates to conduct the analysis. S3 is meeting from the3-6th July 2001in London, and would be pleased to make the 3rd available for the joint meeting.

The LS from T2 (T2-010426) is noted, however, for logistical reasons it is unlikely that any S3 members would be present at the proposed meeting, and it is also noted that the EP-SCP are meeting during the same week in Finland and thus it is very unlikely that any T3 members will attend the meeting.