3GPP TSG SA3#11 **3GPP S3-000152**
Mainz Germany
22-24 February 2000

Source: T-Mobil/T-Nova

From: TSG SA WG3
To: TSG SA WG5
CC: TSG CN WG2

Proposed LS on Functions of Key Distribution and Key Administration for MAP security

Second generation core network security has long been identified as a problem area which must be tackled in 3G. The threats include eavesdropping and modification of customer information, denial of service and fraud. The range of possible "false network" attacks is alarming. For these reasons, a mechanism for securing sensitive MAP messages has been specified by SA WG3.

3G TS 33.102 defines three layers for the handling of MAP security, Key Administration (Layer I), Key Distribution (Layer II) and Message Encryption and Integrity Protection (Layer III). The procedures for the protection of MAP signalling (Layer III) are the responsibility of TSG CN WG2. TSG CN WG2 and TSG SA WG3 were asked by the TSG SA #6 to work on a solution for MAP security in Release 99 (SP-99622).

However it was recognised that the procedures for Key Administration and Key Distribution have impact on the System Architecture as well as on the Telecom Management of the 3G system. 3G TS 33.102 introduces the concept of the Key Administration Centre (KAC). Each Network Operator shall have its own KAC, which serves two purposes:

1. Firstly, it exchanges keys with the KACs of other network operators in a secure manner (Key Administration Layer). The mechanism for doing this is specified in 33.102. Further details, such as the choice of transport mechanism to be used, could be agreed on in the course of roaming agreement establishment between two network operators
2. Secondly, the KAC also initiates the distribution of keys to the network elements of its own domain (Key Distribution Layer). The mechanism for doing this is in principle the same as in the Key Administration Layer. Because of the number of network elements under control of a given KAC and the fact that they may be multi-vendor, a standardised interface between the KAC and the network elements is needed.

Therefore, TSG SA WG5 is asked to clarify the issues concerning the management architecture for network domain security mechanisms, including identifying suitable protocols to be used for the intra-PLMN transfer of security keys and to investigate a possible inclusion of these protocols, e.g. into 3G TS 32.101, for Release 99.

Attached: 3G TS 33.102, version3.3.1. ftp://ftp.3gpp.org/Specs/December_99/33-series/33102-331.zip

Contact Person:
Roland Schmitz
e-mail: schmitz@tzd.telekom.de
Tel: +49 6151 83 2033
Fax: +49 6151 83 4464