3GPP TSG SA WG3 #11 (Security)
Mainz, Germany, 22-24.02.2000

S3-000150

Agenda Item: (tbd)

Source: Nokia

Title: Initial status report of specifications which implement ciphering and integrity protection

Document for: Discussion

3GPP specifications which are relevant for ciphering and integrity protection are listed. The status of the specifications from the point of view of these two security features are briefly commented.
A similar study has been done for authentication and key agreement in S3-000097. Because AKA procedure is needed to obtain the keys for ciphering and integrity protection many specifications listed in that document are also relevant in our context. In the present document we concentrate on the issues not mentioned in S3-000097.

There are three principal areas of interest for the review:
- the access network
- the terminal equipment
- the UICC/USIM

The access network part is the most critical one. The layers that implement the security functions are MAC and RLC for ciphering and RRC for integrity protection. These layers are implemented in the RNC and in the UE.

For the UICC/USIM the most important specification is 31.102 .

Specification	Sections	Comments
23.110	5	Access nw services and functions: integrity missing; questions about ciphering
24.007	6.7.2,9.1.2,9.4.1,10.1	Mobile layer 3 – General aspects
24.065	5.1,5.2	SNDCP
25.301	**8**	**Radio Interface Protocol Architecture: integrity mainly missing, ciphering on common/shared channels? Use of HFN not totally clear**
25.321	**4.2,8.2,8.3**	**MAC protocol**
25.322	**5,6,8,9**	**RLC protocol: RLC SN handling with HFN missing**
25.331	**8.1,8.2,10.1,10.2**	**RRC protocol: integrity optional? Separate HFN for integrity? Several signaling bearers -> bearer ID has to affect MAC-I (bearer id inside existing input parameters or inside the message itself?)**
25.401	**3,7.2.2**	**General UTRAN**
31.102	**4.2,5.2**	**Characteristics of the USIM Application: Ciphering and integrity quite OK**
34.108		UE conformance testing: ciphering and integrity mentioned briefly
34.123		UE conformance spec: very little about security

As in S3-000097 **bold** indicates that the specifications should be reviewed. The review as proposed is not complete, but it should cover the essential specifications.