3GPP TSG SA WG3 Security — SA3#33 **S3-040383**
10-14 May 2004
Beijing, China

Title:	Reply LS on Potential Security issues relating to use of AT Commands to access UICC
Reply to:	LS (S3-040369=T2-040230) on Potential Security issues relating to use of AT Commands to access UICC
Release:	Release 6
Source:	SA3
To:	T2
Cc:	T3

Contact Person:

Name: Jorge Abellan Sevilla
Tel. Number: +33 1 46005933
E-mail Address: **jsevilla@axalto.com**

Overall Description

SA3 thanks T2 for their liaison on Potential Security issues related to the use of AT Commands to access the UICC.

SA3 has discussed the attached CR and considers that the proposed changes do not add any security threat to the current version of the TS (TS 27.007 v 6.4).

Moreover, the support of logical channels management in the TE-MT interface goes in the direction of enabling a logical separation between the access to the (U)SIM and the access to other UICC applications. This could be applied, for instance, for the access to a WIM from a TE application (external to the MT). Another example is to allow access to a separate ISIM application. From a security perspective these features may be considered beneficial since they enable access by UE applications to the security functions provided in the UICC while enabling extra protection of (U)SIM access in channel 0.

Related to the remote access to the UICC, already specified in TS 27.007, SA3 has not fulfilled a complete analysis at this stage but some points have been raised:

-Restricted SIM access and generic SIM access functionalities are present in 27.007 from Rel-99 and in 07.07 from the very beginning.

-No additional threats have been identified of those already applicable to other AT commands defined in 27.007 (e.g. Select TE character set, Master Reset or any Call control command).

-The existing separation of remote access to the UICC into two categories (Restricted and Generic) provides ways to block certain AT commands coming from untrusted TE's applications.

-Principles and specific requirements included in 3GPP TS 23.227 (Application and user interaction in the UE; Principles and specific requirements) shall be respected by implementations in order to limit the risk of unauthorized access to the functionalities provided by any AT command.

Actions

Actions to T2

Please consider these initial security considerations.

Date of Next 3GPP SA3 Meetings

3GPP SA3#34	6 - 9 July 2004	Acapulco, Mexico
3GPP SA3#35	5 - 8 Oct 2004	Malta