3GPP TSG SA WG3 Security — S3#32 **S3-040174**
09 - 13 February 2004
Edinburgh, Scotland, UK

3GPP TSG-T3 Meeting #30 **Tdoc T3-040125**
Sophia Antipolis, France, 9-13 February 2004.

Title: Response LS on Status of VGCS work in SA3
Response to: LS on status of VGCS work in SA3 (S3-030803, T3-040013)

Source: 3GPP TSG T WG3
To: 3GPP TSG SA WG3
Cc: ETSI EP RT, GERAN2, ETSI SCP

Contact Person:
Name: François Ennesser
Tel. Number: +33-1-4600-4526
E-mail Address: **FEnnesser@axalto.com**

---

1. Overall Description:

T3 thanks SA3 for their LS in T3-040013 (S3-030803) regarding the status of VGCS work in SA3. SA3 is welcome to confirm to T3 whether the VGCS work is due for Release 6, as this will impact the timeframe in which the CR have to be drafted.

T3 confirms to SA3 that the required UICC functionalities, i.e. storage of long-term Group Keys and short-term key derivation using a random number can indeed be implemented on the USIM for Release 6, as long as the requirements are clarified on time.

In order to propose CRs to T3 specifications at its next meeting in Berlin, T3 would appreciate further information from SA3 on the following points:

1/ Is there an SA3 specification that will provide an external description of the algorithm to run in the UICC for derivation of the short-term VGCS key that we could refer to, or is there an assigned name that T3 could use in its specification to refer to this algorithm?

2/ Can SA3 confirm the length of the keys (current understanding is 128 bits) and of the random number (32 bits?) to be used in the VGCS context?

3/ The T3 specification today provides storage for up to 50 VGCS groups that the user may be subscribed to. Can SA3 indicate whether there is any intended relationship between the VGCS Group key identifiers and the VGCS groups that a user is subscribed to? I.e. is it 15 keys for each of the up to 50 groups?

4/ Can SA3 confirm that the Group keys should preferably be updatable by OTA, while the UICC does not need to provide storage for the derived short-term keys?

T3 will inform SA3 on the proposed CRs to its specification as soon as the requirements from SA3 will permit the drafting of such a CR.

2. Actions:

To 3GPP SA WG3:

T3 kindly ask SA3 to provide answers to the above questions and welcome further cooperation on these matters.

3. Date of Next TSG-T WG3 Meetings:

TSG-T3 Meeting #31	27th – 30th April 2004	Berlin, Germany.
TSG-T3 Meeting #32	10th – 13th August 2004	New York, USA.