Technical Specification Group Services and System Aspects ***TSGS#5(99)478***

Meeting #5, Kyongju, Korea, 11-13 October 1999

TSG SA WG3 **S3-99273**

Meeting #5bis, Bonn, 25 August, 1999

Source: **Secretary TSG SA WG3 (Ansgar Bergmann)**

Title: **Report of TSG SA WG3 Meeting #5bis**

Status: **Approved**

Table of contents

1 General

Bart Vinck, Rapporteur of 33.102, welcomed the delegates and thanked DETECON and T-Mobil for hosting the meeting. As the S3 Chairman and both Vice Chairmen were unable to attend the meeting, Bart Vinck accepted to chair the meeting.

Scope of the meeting: The meeting had been convened with the restricted scope to agree CRs to 33.102. At the joint T3/S3/S2 meeting the day before, there had been a long discussion on the requirements for GSM/UMTS roaming and handover concerning security functions. It was agreed that preparation of CRs to 33.102 for this aspect would also be in the scope of S3#5bis, whence also the preparation of such CRs would be in the scope; therefore, and due to the urgency, it was found justified, that S3#5bis could write a LS to S2 (meeting in the same week) fixing the basic functions, requirements, facts and assumptions.

2 Assignment of Input Documents / Agenda

The agenda in S3-99264 was approved:

1. Assignment of Input Documents / Agenda S3-99264
2. Editorial changes to TS 33.102 S3-99261
3. CR on Cipher key selection S3-99262, S3-99268
4. Interoperation between UMTS and GSM S3-99271, S3-99263, S3-99267, S3-99269
5. Data integrity protection
6. Encryption
7. Enhanced user identity confidentiality S3-99270
8. Remaining issues from the joint meeting with T3 and SA2
9. Any other business

For the assignment of documents to agenda items, see annex A.

2 Editorial changes to TS 33.102

Some major restructuring of 33.102 and also the addition of description seems necessary, see S3-99261. Main points:

- to describe common aspects (key setting, capability negotiations, lifetime control) of the cipher and integrity mechanisms once instead of twice in a separate section on all issues related to secure connection set-up;
- to add a separate section on interoperation and handover issues;
- to describe network-wide encryption in a separate section.

The document outlines a new structure for section 6.

Discussion in S3#5bis: It was recommended to separate:

- an editorial change request where material is re-ordered but in principle not changed;
- other CRs to add descriptions;
- other CRs to change existing descriptions.

There will probably be several CRs on the same piece of text. Such problems can be sorted out after SA approval between the rapporteurs and S3 secretary. However it would be ideal if a draft version is already produced before approval in order to provide some consistency checking.

3 CR on Cipher key selection

Input documents were S3-99262 and S3-99268.

Background: cipher and integrity keys can be set in the packet domain (PD) and in the circuit switched domain (CD). For signalling (of both domains), however, it had been agreed that only one single cipher key should be applied. Several ways had been discussed to realise this.

RAN had expressed preference not to use a "one key" solution where the same key would be applied for CD user plain, PD user plane and for the signalling plane.

As a consequence, some rule or communication has to be defined which key to apply for signalling, if both the packet and circuit key are in use.

S3-99262 proposes to allow the Core Network nodes to give an order to the RNC which would pass it to the mobile. In a typical application, a packet session might be running for a longer time, and the packet switch would change the cipher key with some frequency (say every 20 minutes); then there might be CS connections during the packet session, however the circuit switch would only order usage of its key for signalling when it changes the circuit key; as a consequence, each switch would normally get its wanted level of key freshness or a better one, and too frequent on-line changes of the signalling key in ciphered mode would be avoided.

S3-99268 proposes to set the signalling key together with each cipher setting. For example, when from idle mode a packet session is established and ciphering is activated, the P-key would be applied for signalling. When later a C-connection is established in parallel and C-ciphering is activated, the key for signalling would be changed from P-key to C-key. If in the example, the C-connection terminates, the C-key would continue to be used for signalling until either for the packet domain or for the circuit oriented domain a new cipher procedure is invoked. Discussion in S3#5bis:

- This concept has the advantage to be simpler.
- The question was raised whether order of messaging between circuit oriented signalling and packet oriented signalling is guaranteed: if not, it could happen that the RNC receives two cipher mode complete messages in the wrong order, so that mobile and RNC would apply different keys for signalling. It was concluded that problems of this nature are quite familiar to RAN, and that they would report back if such a problem existed.
- The S3-99268 solution has the drawback that the key for a ciphered signalling connection may change unnecessarily often, and that in phases where a good performance of signalling is important. But the meeting concluded, that the 5 seconds allowed time for changing the key give sufficient time to perform the necessary procedures, so that the actual change would be delayed to a time with less signalling.

Result of the discussion:

➢ **The CR in S3-99265, elaborated from both contributions, and setting the signalling key with each cipher setting, was agreed.**

4 Interoperation between UMTS and GSM

Input for this agenda item were S3-99271, S3-99263, S3-99267, S3-99269.

The two following tools had already been identified: a conversion function which generates Kc from CK, and a conversion function which generates a CK from Kc.

After intensive and at the same time extensive discussions, the following principles were agreed in S3#5bis:

- It is assumed that all R99 equipment, in particular a R99 GSM only mobile station, can handle the UMTS MM security procedures (authentication); as a consequence, when a USIM in a R99 mobile equipment (even if it is GSM only) roams into a R99 VLR area and when the HLR is R99, both the

CK and the Kc would be derived at authentication - even in the case where the GSM radio access had been used.

- When a R99 switch (packet of circuit)/VLR does not receive Kc from the HLR, it can derive Kc from CK with a standardized procedure, see above.
- If a GSM (pre-R99) authentication has been performed, however later a CK is requested, in can be generated in the mobile equipment and VLR, with a standard function, see above. This CK however has the lower "pre-R99" level of security. (Examples where this would happen, are: a mobile roaming from a GSM pre-R99 VLR area to UMTS; a user with SIM and pre-R99 HLR roaming into a UMTS network.)

On this basis, S3#5bis studied all relevant scenarios. It was verified that all requirements can be fulfilled so that always the highest possible level of security is applied. However for the case of inter-MSC handover from a pre-R99 MSC area to a R99 MSC area, the relay MSC/VLR would have to take over some unusual functions; also it was argued that there might be major difficulties (not related to security) to allow such handovers, and that it might not be worth while to elaborate a solution.

➢ **Result: Tdoc S3-99266.**

5 Data integrity protection

No input received.

6 Encryption

No input received.

7 Enhanced user identity confidentiality

Input: S3-99270.

This document studies the cases where paging with IMSI is foreseen, and proposes a mechanism to avoid it. The basic idea is to use a secret paging identifier, known between the mobile and the HLR, and known to the VLR by some communication flow with mobile or HLR or both.

Comments:

- S3-99270 seems to assume that paging with IMSI is applied regularly when paging with TMSI had no response (in order to cover "synch problems" (SP)). However the SP of TMSI re-allocation appears when the VLR has sent the command, but not received the confirmation: Then the VLR cannot decide whether the command or the confirmation was lost. So, the VLR can clearly identify whether there is a potential SP or not. But even in this case, paging with IMSI can be avoided: Instead, paging with the old and the new TMSI can be used.
- The situations where paging with IMSI occur were collected:
  - VLR restoration;
  - first activation of a USIM "in its life";
  - impossibility to contact the previous VLR.
- In the case of VLR restoration, paging with IMSI may be avoided in most cases as IMSI attach /periodic location update is normally used.
- The encrypted paging identifier would be probably of the same length as the IMSI, whereas the EMUI

would be around twice as long.

- Reduction of traffic load on the paging channels may be important.

A conclusion at the meeting was not reached.

8 Remaining issues from the joint meeting with T3 and SA2

No issue was discussed except the one in section 4.

9 Any other business

None.

10 Closure of the meeting

The meeting was closed.

Annex A: Document list

Tdoc	Title/subject	source	AI
S3-99261	Re-organisation of TS 33.102, clause 6	Siemens Atea	2
S3-99262	Key selection for signalling	Siemens Atea	3
S3-99263	Interoperation between UMTS and GSM	Siemens Atea	4
S3-99264	Draft agenda	Bart Vinck	2
S3-99265	CR to 33.102 on Cipher/integrity key setting	S3	3
S3-99266	LS to S2 on hand-over	S3	
S3-99267	A Possible Handover Mechanism between GSM and UMTS	Ericsson	4
S3-99268	Draft CR to 33.102 on Cipher key setting	Ericsson	3
S3-99269	Inter-system CS and PS handovers	Nokia	4
S3-99270	Enhanced User Identity Confidentiality and IMSI-Paging	Mannesmann	7
S3-99271	An Analysis of Possible Handover Mechanisms between GSM and UMTS	T-Mobil, Deutsche Telekom	4

Annex B: Participants list

Acting Chairman

VINCK Bart	SIEMENS ATEA NV	BE

SECRETARY

BERGMANN Ansgar	ETSI MCC (Detecon)	FR
BLOM Rolf	ERICSSON L.M.	SE
FINKELSTEIN Louis	Motorola	US

HOWARD Peter	VODAFONE Group Plc	GB
NIEMI Valtteri	Nokia Research Center	FI
Roland Schmitz	Deutsche Telekom AG	DE