3GPP TSG SA WG 3 (Security) meeting #11 **S3-000203**
Mainz, 22-24 February, 2000

From: **3GPP TSG SA WG3**
To: **3GPP TSG RAN WG2**

LS concerning the integrity protection mechanism

SA 3 has done a brief review of the specification 25.331 as regards the issues concerning integrity protection mechanism. Attached is the report (S3-000150) from the initial review (including also reviews on other specs). SA 3 wants to inform RAN 2 about some specific issues in the RRC specification:

- integrity protection is mandatory (unlike ciphering which can be turned off).
- SA 3 has the intention of store only one HFN in the USIM as the connection is released. This same HFN can be used as the initialization value for ciphering in all bearers and for integrity protection in all bearers. This implies only one HFN value has to be transmitted from the terminal in the initial connection establishment process.
- To avoid "replay attacks" it is essential that the identity of the signalling bearer affects the message authentication code MAC-I that is appended to the RRC messages.
- Attached is a CR to 33.102 approved by the SA 3 (S3-000168) which clarifies the handling of the case where the integrity check fails.

3GPP TSG SA WG3 #11 (Security) **S3-000150**
Mainz, Germany, 22-24.02.2000

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.

3GPP TSG SA WG3 (Security) meeting #11
Mainz, 22-24 February, 2000

***Document* S3-000168**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102	**CR**	**061r1**	Current Version:	3.3.1

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	TSG SA #7	for approval	☒	strategic	□	*(for SMG*
list expected approval meeting # here ↑		for information	□	non-strategic	□	*use only)*

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: (U)SIM □ ME ☒ UTRAN / Radio ☒ Core Network ☒
(at least one should be marked with an X)

Source: Ericsson **Date:** 2000-02-17

Subject: Unsuccessful integrity check

Work item: Security

Category:	F	Correction	□	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	☒		Release 98	□
with an X)	D	Editorial modification	□		Release 99	☒
					Release 00	□

Reason for change: At detection of an integrity failure, the concerned message shall be discarded. In both the MS and the SRNC there shall be a supervision of failed integrity checks and if the failure situation persists, the connection shall be dropped.

Clauses affected: 6.4.6

Other specs affected:	Other 3G core specifications	□	→ List of CRs:
	Other GSM core specifications	□	→ List of CRs:
	MS test specifications	□	→ List of CRs:
	BSS test specifications	□	→ List of CRs:
	O&M specifications	□	→ List of CRs:

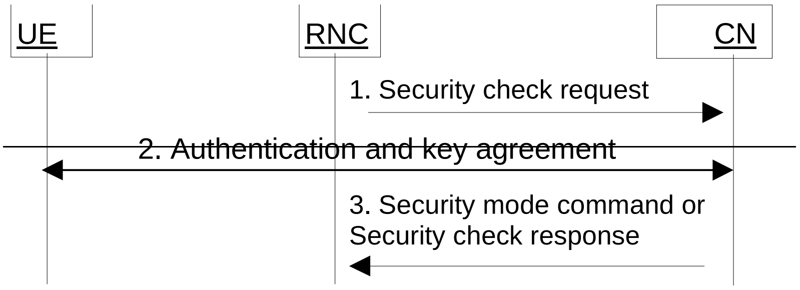
Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

6.4.6 Signalling procedures in the case of an unsuccessful integrity check

The supervision of failed integrity checks shall be performed both in the MS and the SRNC. In case of failed integrity check (i.e. faulty or missing MAC) is detected after that the integrity protection is started the concerned message shall be discarded. This can happen on the RNC side or on the MS side.~~The following procedure is used by the RNC to request the CN to perform an authentication and to provide a new CK and IK in case of unsuccessful integrity check. This can happen on the RNC side or in the UE side. In the latter case the UE sends a SECURITY CONTROL REJECT message to the RNC.~~


UE
RNC
CN
1. Security check request
~~2. Authentication and key agreement~~
3. Security mode command or
Security check response

~~**Figure 15: Procedures at unsuccessful integrity check**~~

~~RNC detects that new security parameters are needed. This may be triggered by (repeated) failure of integrity checks (e.g. COUNT-I went out of synchronisation), or at handover the new RNC does not support an algorithm selected by the old RNC, etc.~~

1. ~~RNC sends a SECURITY CHECK REQUEST message to CN (indicating cause of the request).~~
2. ~~The CN performs the authentication and key agreement procedure.~~
3. ~~If the authentication is successful, the CN sends a Security mode command to RNC. This will restart the ciphering and integrity check with new parameters. If the authentication is not successful, the CN sends a SECURITY CHECK RESPONSE (Cause) to RNC.~~
4. ~~If the failure situation persists, the connection should be dropped.~~