3GPP TSG SA 3 Meeting #15
Washington, 12-14 September 2000

Document S3-000545
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 0xx Current Version: 3.5.0

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

For submission to: SA#9	for approval	☒	strategic	□	*(for SMG use only)*
list expected approval meeting # here ↑	for information	□	non-strategic	□	

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: Vodafone

Date: 4 September 2000

Subject: Removal of duplicate text on USIM toolkit secure messaging and addition of a reference to 02.48 and 03.48 instead.

Work item: Security

Category: *(only one category Shall be marked With an X)*

F	Correction	□	
A	Corresponds to a correction in an earlier release	□	
B	Addition of feature	□	
C	Functional modification of feature	□	
D	Editorial modification	☒	

Release:

Phase 2	□
Release 96	□
Release 97	□
Release 98	□
Release 99	☒
Release 00	□

Reason for change: To avoid duplication of USIM toolkit secure messaging specifications it is necessary to delete some text in 33.102 and include a reference to 02.48 and 03.48 instead. The new formulation follows the style of the other sections on USIM-based security features in 33.102.

Clauses affected: 2.2, 5.4.1, 8.1

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: This CR should be forwarded to T3 for information.

help.doc

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

** Add new reference to section 2.2 **

2.2 Informative references

[x] 3G TS 31.111, USIM Application Toolkit

** Next modified section **

5.4 Application security

5.4.1 Secure messaging between the USIM and the network

USIM Application Toolkit, as specified in 3G TS 31.111 [x],~~It is expected that 3GMS will~~ provides the capability for operators or third party providers to create applications which are resident on the USIM (similar to SIM Application Toolkit in GSM). There exists a need to secure messages which are transferred over the ~~3GMS~~ network to applications on the USIM, with the level of security chosen by the network operator or the application provider.

Security features for USIM Application Toolkit are implemented by means of the mechanisms described in GSM 03.48 [19]. These mechanisms address the security requirements identified in GSM 02.48 [16].

~~The following security features are provided with respect to protecting messages transferred to applications on the USIM over the 3GMS network:~~

- ~~**Entity authentication of applications:** the property that two applications are able to corroborate each other's identity.~~
- ~~**Data origin authentication of application data:** the property that the receiving application is able to verify the claimed data origin of the application data received;~~
- ~~**Data integrity of application data:** the property that the receiving application is able to verify that application data has not been modified since it was sent by the sending application;~~
- ~~**Replay detection of application data:** the property that an application is able to detect that the application data that it receives is replayed;~~
- ~~**Sequence integrity of application data:** the property that an application is able to detect that the application data that it receives is received in sequence;~~
- ~~**Proof of receipt:** the property that the sending application can proof that the receiving application has received the application data sent.~~
- ~~**Confidentiality of application data:** the property that application data is not disclosed to unauthorised parties.~~

~~NOTE: It is assumed that these security features will be based on GSM SIM Application Toolkit security features. Further work is required to identify what enhancements need to be made to SIM Application Toolkit security. Possible areas of enhancement may include: key management support, enhancement of security mechanisms/features, increased flexibility in algorithm choice and security parameter size. A joint 3GPP TSG-SA 'Security'/3GPP TSG-T 'USIM' working group may be required to progress this issue.~~

8 Application security mechanisms

8.1 ~~Secure messaging between the USIM and the network~~Void

~~This clause will specify the structure of the secured messsages in a general format so that they can be used over a variety of transport channels between an entity in a 3GMS network and an entity in the USIM. The sending/receiving entity in the 3GMS network and in the USIM are responsible for applying the security mechanisms to application messages as defined to provide the security features identified in 5.4.1.~~

~~Note: A joint 3GPP TSG-SA 'Security'/3GPP TSG-T 'USIM' working group may be required to progress this issue.~~

8.2 Void