3GPP TSG SA WG3 Security — S3#11 **S3-000213**

22-24 February, 2000

Mainz, Germany

From:	**TSG SA WG3**
To:	**TSG CN WG1**
Copy:	**TSG RAN WG2, TSG T WG3**
Title:	**LS on UE triggered authentication and key agreement during connections**

3G TS 33.102 v3.3.1 section 6.4.3 specifies a mechanism to allow the UE to force the authentication and key agreement procedure to be run at the start of an RRC connection if the value of the hyperframe number at the end of the previous RRC connection exceeds a maximum value. This mechanism is used to control the lifetime of the cipher and integrity keys, CK and IK. The value of the hyperframe number at the end of the previous RRC connection and its maximum permitted value are both stored on the USIM. It is intended to correct a potential weakness in this mechanism so that the authentication and key agreement procedure can be triggered by the UE during a connection if the maximum permitted hyperframe counter value is reached. It is felt that due to timescales, it may not be feasible to introduce this feature in R99. If this is the case then it should be introduced in R00.

UE triggered authentication and key agreement during a connection may be useful if long connections are expected. One of the objectives of 3G security is to minimise the amount of trust that needs to be placed in the serving network. UE triggered authentication based on a maximum permitted hyperframe number set in the USIM can help to minimise the trust that the home environment needs to place in the serving network to implement an appropriate re-authentication policy for long connections. This feature is likely to be of most value in the PS domain where long connections are more likely.

In order to implement this feature, it is required that the UE is able to indicate to the core network during a connection that the authentication and key agreement procedure should be run. N1 are asked to ensure that this functionality is implemented in their specifications.

Attached: S3-000194 (CR on key setting) and S3-000193 (CR on key lifetime).

Contact person: Peter Howard
Email: peter.howard@vf.vodafone.co.uk
Tel: +44 1635 676206

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

***Document* S3-000193**
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**	**076**	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 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: SA WG3 **Date:** 2000-02-22

Subject: Cipher key and integrity key lifetime

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: It is required to correct a potential weakness in the key lifetime control mechanism so that the authentication and key agreement procedure can be triggered by the UE during a connection if the maximum permitted hyperframe counter value is reached.

Clauses affected: 6.4.3

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.

6.4.3 Cipher key and integrity key lifetime

Authentication and key agreement which generates cipher/integrity keys is not mandatory at call set-up, and there is therefore the possibility of unlimited and malicious re-use of compromised keys. A mechanism is needed to ensure that a particular cipher/integrity key set is not used for an unlimited period of time, to avoid attacks using compromised keys. The USIM shall therefore contain a mechanism to limit the amount of data that is protected by an access link key set.

Each time an RRC connection is released the highest value of the hyperframe number (the current value of COUNT) of the bearers that were protected in that RRC connection is stored in the USIM. When the next RRC connection is established that value is read from the USIM and incremented by one.

The USIM shall trigger the generation of a new access link key set (a cipher key and an integrity key) if the counter reaches a maximum value set by the operator and stored in the USIM at the next RRC connection request message sent out or during an RRC connection.

This mechanism will ensure that a cipher/integrity key set cannot be reused ~~more times than~~beyond the limit set by the operator.

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

Document ***S3-000194***
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** **077** 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
list expected approval meeting # here ↑

for approval	☒	strategic	□	*(for SMG use only)*
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: SA WG3 **Date:** 2000-02-22

Subject: Cipher key and integrity key setting

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	☒	**Release:**	Phase 2	□
A	Corresponds to a correction in an earlier release	□		Release 96	□
B	Addition of feature	□		Release 97	□
C	Functional modification of feature	□		Release 98	□
D	Editorial modification	□		Release 99	☒
				Release 00	□

Reason for change: It is required to clarify that after an authentication the new keys are taken into use as part of the security mode control procedure that follows in both the PS and CS domain.

Clauses affected: 6.4.3

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.

6.4.3 Cipher key and integrity key setting

Mutual key setting is the procedure that allows the MS and the RNC to agree on the key IK used to compute message authentication codes using algorithm UIA. Authentication and key setting is triggered by the authentication procedure and described in 6.3. Authentication and key setting may be initiated by the network as often as the network operator wishes. Key setting can occur as soon as the identity of the mobile subscriber (i.e. TMUI or IMUI) is known by the SN/VLR. The key IK is stored in the SN/VLR and transferred to the RNC when it is needed. The key IK is stored in the USIM until it is updated at the next authentication.

If an authentication procedure is performed during ~~a data transfer in the PS mode~~a connection (PS or CS mode), the new cipher key CK and integrity key IK shall be taken in use in both the RNC and the UE as part of the security mode negotiation (see 6.4.5) that follows the authentication procedure.