3GPP TSG-CN Meeting #23 **Tdoc NP-040099**

Phoenix, Arizona, USA 10 – 12 March 2004

CR-Form-v7

CHANGE REQUEST

⌘ **24.008** **CR** **846** ⌘ **rev** **3** ⌘ Current version: **5.10.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	Handling of key sets
Source:	⌘	Ericsson, Siemens
Work item code:	⌘	TEI5
Date:	⌘	19/02/2004
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	At present, it is ambiguously specified what key set shall be used for ciphering (and/or integrity protection) after inter-system change for the case, that ciphering (and/or integrity protection) was started in the original system, but there was a UMTS or GSM AKA procedure performed prior to the inter-system change and this key set has not been taken into use yet. The sections 4.3.2.7a and 4.7.7.7 indicate that the keys shall be loaded from the SIM or USIM when a "valid SECURITY MODE COMMAND or CIPHERING MODE COMMAND" message is received. This statement does not cover all scenarios. For instance, when the MS has an ongoing connection (ciphered) and **after** activation of ciphering, but **prior** inter-system change a new UMTS or GSM AKA procedure takes place (so, the new agreed key set has not been taken into use yet). So, the fact that "inter-system change" is not specifically mentioned by TS 24.008 in sections 4.3.2.7a and 4.7.7.7 makes the specificaiton unclear in the scenario described previously. Additionally, TS 44.018 explicitly states that during handover to GSM the key shall not be changed, so in case of two key sets, the old one is still valid until othewise indicated by CIPHERING MODE COMMAND.
Summary of change:	⌘	It is clarified that the MS in CS domain shall continue using the old key set used until otherwise indicated by the SECURITY MODE COMMAND or CIPHERING MODE COMMAND messages in UMTS and GSM respectively. Then, the new key set (the one residing in the SIM or USIM), if received during an ongoing, already ciphering and/or integrity protected RR connection, is taken into account.

		Finally, in UMTS, the MS for PS domain has to take into account the new key set, if received during an ongoing, already ciphering and/or integrity protected RR connection, immediately after an inter-system change to GSM.
Consequences if not approved:	⌘	The handover (including inter-system change) scenarios after 'late AKA' procedure always fail. This leads to undesirable effects, because ciphering and/or integrity protection will fail; in the CS domain, the call will be dropped and in the PS domain, data based services will not be possible. The specification remains unclear in the scenario described in the reason for change of this change request, which may also lead to different implementations in terminals and networks. Misalignment among different specifications remains.

Clauses affected:	⌘	4.3.2.7, 4.3.2.7a, 4.3.2.8, 4.7.7.7, 4.7.7.8, 4.7.7.9.				
		Y	**N**			
Other specs affected:	⌘		**X**	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

FIRST CHANGE

4.3.2.7 Handling of keys at intersystem change from UMTS to GSM

At inter-system change from UMTS to GSM, ciphering may be started (see 3GPP TS 44.018 [86]) without any new authentication procedure. Deduction of the appropriate security key for ciphering in GSM, depends on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GSM ciphering key according to table 4.3.2.7.1.

Table 4.3.2.7.1/3GPP TS 24.008: Inter-system change from UMTS to GSM

Security context established in MS and network in UMTS	At inter-system change to GSM:
GSM security context	An ME shall apply the stored GSM cipher key that was received from the GSM security context residing in the SIM/USIM.
UMTS security context	An ME shall apply the stored GSM cipher key that was derived by the USIM from the UMTS cipher key and the UMTS integrity key.

NOTE: A USIM with UMTS security context, passes the UMTS cipher key, the UMTS integrity key and the derived GSM cipher key to the ME independent on the current radio access being UMTS or GSM.

4.3.2.7a Use of established security contexts

In GSM, in the case of an established GSM security context, the GSM ciphering key shall be loaded from the SIM/USIM and taken into use by the ME when any valid CIPHERING MODE COMMAND is received during an RR connection (the definition of a valid CIPHERING MODE COMMAND message is given in 3GPP TS 44.018 [84] subclause 3.4.7.2).

In GSM, in the case of an established UMTS security context, the GSM ciphering key shall be loaded from the USIM and taken into use by the MS when a valid CIPHERING MODE COMMAND is received during an RR connection (the definition of a valid CIPHERING MODE COMMAND message is given in 3GPP TS 44.018 [84] subclause 3.4.7.2). The network shall derive a GSM ciphering key from the UMTS ciphering key and the UMTS integrity key by using the conversion function named "c3" defined in 3GPP TS 33.102 [5a].

In UMTS, in the case of an established GSM security context, the ME shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102 [5a]. The GSM ciphering key shall be loaded from the SIM/USIM and the derived UMTS ciphering key and UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating CS domain is received during an RR connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331 [23c]). The network shall derive a UMTS ciphering key and a UMTS integrity key from the GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102 [5a].

In UMTS, in the case of an established UMTS security context, the UMTS ciphering key and UMTS integrity key shall be loaded from the USIM and taken into use by the MS when a valid SECURITY MODE COMMAND indicating CS domain is received during a RR connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331 [23c]).

~~NOTE:~~ In UMTS and GSM, if during an ongoing, already ciphering and/or integrity protected RR connection, the network ~~might~~ initiates a new Authentication procedure and~~in order to~~ establishes a new GSM/UMTS security context~~.~~ ~~T~~the new keys are taken into use in the MS when a new valid SECURITY MODE COMMAND indicating CS domain in UMTS, or a new valid CIPHERING MODE COMMAND in GSM, is received during the RR connection. In case of handover to UMTS or GSM the MS and the network shall continue to use the old keys until a new valid SECURITY MODE COMMAND indicating CS domain in UMTS, or a new valid CIPHERING MODE COMMAND in GSM, is received during the RR connection.

4.3.2.8 Handling of keys at intersystem change from GSM to UMTS

At inter-system change from GSM to UMTS, ciphering and integrity may be started (see 3GPP TS 25.331 [23c]) without any new authentication procedure. Deduction of the appropriate security keys for ciphering and integrity check in UMTS, depend on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the UMTS cipher key and the UMTS integrity key according to table 4.3.2.8.1.

Table 4.3.2.8.1/3GPP TS 24.008: Inter-system change from GSM to UMTS

Security context established in MS and network in GSM	At inter-system change to UMTS:
GSM security context	An ME shall derive the UMTS cipher key and the UMTS integrity key from the stored GSM cipher key that was provided by the SIM/USIM. The conversion functions named "c4" and "c5" in 3GPP TS 33.102 [5a] are used for this purpose.
UMTS security context	An ME shall apply the stored UMTS ciphering key and the stored UMTS integrity key that were received from the UMTS security context residing in the USIM.

NOTE A USIM with UMTS security context, passes the UMTS cipher key, the UMTS integrity key and the derived GSM cipher key to the ME independent on the current radio access being UMTS or GSM.

SECOND CHANGE

4.7.7.7 Use of established security contexts

In GSM, in the case of an established GSM security context, the GPRS GSM ciphering key shall be taken into use by the MS before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted.

In GSM, in the case of an established UMTS security context, the GPRS GSM ciphering key shall be taken into use by the MS before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted. The network shall derive a GPRS GSM ciphering key from the GPRS UMTS ciphering key and the GPRS UMTS integrity key, by using the conversion function named "c3" defined in 3GPP TS 33.102 [5a].

In GSM, if during an ongoing, already ciphering protected RR connection, the network initiates a new Authentication and ciphering procedure, the new GPRS GSM ciphering key shall be taken into use by the MS before the AUTHENTICATION AND CIPHERING RESPONSE message is transmitted. In case of inter-system change to UMTS after receipt of the AUTHENTICATION AND CIPHERING REQUEST message, the MS and the network shall take the new keys into use immediately after the inter-system change.

In UMTS, in the case of an established GSM security context, the ME shall derive a GPRS UMTS ciphering key and a GPRS UMTS integrity key from the GPRS GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102 [5a]. The derived GPRS UMTS ciphering key and GPRS UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating PS domain is received during an RR connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331 [23c]). The network shall derive a GPRS UMTS ciphering key and a GPRS UMTS integrity key from the GPRS GSM ciphering key by using the conversion functions named "c4" and "c5" defined in 3GPP TS 33.102 [5a].

In UMTS, in the case of an established UMTS security context, the GPRS UMTS ciphering key and the GPRS UMTS integrity key shall be taken into use by the MS when a valid SECURITY MODE COMMAND indicating PS domain is received during an PS signalling connection (the definition of a valid SECURITY MODE COMMAND message is given in 3GPP TS 25.331[23c]).

NOTE: In UMTS, if during an ongoing, already ciphering/integrity protected PS signalling connection, the network might initiates a new Authentication and ciphering procedure and in order to establishes a new GSM/UMTS security context,. tThe new GPRS UMTS ciphering key and GPRS UMTS integrity key are taken into use by the MS, when a new valid SECURITY MODE COMMAND indicating PS domain is received during the PS signalling connection. In case of inter-system change to GSM, the MS and the network shall take the new keys into use immediately after the inter-system change.

4.7.7.8 Handling of keys at intersystem change from UMTS to GSM

At an inter-system change from UMTS to GSM, ciphering may be started (see 3GPP TS 44.064 [78a]) without any new authentication and ciphering procedure. Deduction of the appropriate security key for ciphering in GSM, depends on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GPRS GSM ciphering key according to table 4.7.7.8.1.

Before any initial GMM message is sent in the new cell in GSM, the GMM layer in the MS shall notify the LLC layer if ciphering shall be used or not. If yes, the GPRS GSM ciphering key and the applicable ciphering algorithm according to the stored *Ciphering Algorithm IE* in the MS shall also be indicated to the LLC layer (see 3GPP TS 44.064 [78a]).

Table 4.7.7.8.1/3GPP TS 24.008: Inter-system change from UMTS to GSM

Security context established in MS and network in UMTS	At inter-system change to GSM:
GSM security context	An ME shall apply the latest GPRS GSM cipher key that was received from the GSM security context residing in the SIM/USIM.
UMTS security context	An ME shall apply the GPRS GSM cipher key that was derived by the USIM from the GPRS UMTS cipher key and the GPRS UMTS integrity key during the latest successful authentication procedure.

NOTE A USIM with UMTS security context, passes the GPRS UMTS ciphering key, the GPRS UMTS integrity key and the derived GPRS GSM ciphering key to the ME independent on the current radio access being

4.7.7.9 Handling of keys at intersystem change from GSM to UMTS

At an inter-system change from GSM to UMTS, ciphering and integrity may be started (see 3GPP TS 25.331) without any new authentication and ciphering procedure. Deduction of the appropriate security keys for ciphering and integrity check in UMTS, depend on the current GSM/UMTS security context stored in the MS and the network.

The ME shall handle the GPRS UMTS cipher key and the GPRS UMTS integrity key according to table 4.7.7.9.1.

Table 4.7.7.9.1/3GPP TS 24.008: Inter-system change from GSM to UMTS

Security context established in MS and network in GSM	At inter-system change to UMTS:
GSM security context	An ME shall derive the GPRS UMTS cipher key and the GPRS UMTS integrity key from the GPRS GSM cipher key that was provided by the SIM/USIM during the latest successful authentication procedure. The conversion functions named "c4" and "c5" in 3GPP TS 33.102 [5a] are used for this purpose.
UMTS security context	An ME shall apply the latest GPRS UMTS ciphering key and the GPRS UMTS integrity key that were received from the UMTS security context residing in the USIM.

NOTE: A USIM with UMTS security context, passes the GPRS UMTS ciphering key, the GPRS UMTS integrity key and the derived GPRS GSM ciphering key to the ME independent on the current radio access being UMTS or GSM.