3GPP TSG-T (Terminals) Meeting #15
Jeju, Korea, 6 – 8 March 2002

Tdoc TP-020063

Source: T3

Title: Change Request on secure messaging (TS 03.48 / 23.048)

Document for: Approval

This document contains several change requests as follows:

T3 Doc	Spec	CR	Rel	Cat	Subject
T3-020111	23.048	017	5	B	Define link between Open Platform Security Domain and 23.048 secure messaging
T3-020112	23.048	018	4	F	Clarifications on Access Domain Parameter
T3-020113	23.048	019	5	F	Clarifications on Access Domain Parameter

3GPP T3 Meeting #22
Marbella, Spain, 22 - 25 Jan 2002

Tdoc T3-020111
Revised T3-020082

CR-Form-v3

CHANGE REQUEST

⌘ **23.048** **CR** **017** ⌘ rev **-** ⌘ Current version: **5.2.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Define link between Open Platform Security Domain and 23.048 secure messaging
Source:	⌘	T3
Work item code:	⌘	USAT1-SM
Date:	⌘	25/01/02
Category:	⌘	**B**
Release:	⌘	REL-5

Use one of the following categories:
F *(essential 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)

Reason for change:	⌘	Relation between 23.048 security layer and Open Platform security architecture is not fully standardized.
Summary of change:	⌘	Add an Annex B for Open Platform that specifies: - The association between counter and key set version within the security domain - Use of KIc and KID fields by a security domain.
Consequences if not approved:	⌘	

Clauses affected:	⌘	§ 3.1, § 5.1.2, § 5.1.3, § 5.1.4, Annex B
Other specs Affected:	⌘	[ ] Other core specifications [ ] Test specifications [ ] 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/3G_Specs/CRs.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://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 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.

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Application Layer: layer above the Transport Layer on which the Application Messages are exchanged between the Sending and Receiving Applications

Application Message: package of commands or data sent from the Sending Application to the Receiving Application, or vice versa, independently of the transport mechanism

NOTE 1: An Application Message is transformed with respect to a chosen Transport Layer and chosen level of security into one or more secured packets.

Card Manager: An application in charge of application management as defined in the Open Platform Card Specification [14].

Command Header: Security Header of a Command Packet. It includes all fields except the Secured Data

Command Packet: Secured Packet transmitted by the Sending Entity to the Receiving Entity, containing a secured Application Message

Counter: mechanism or data field used for keeping track of a message sequence

NOTE 2: This could be realised as a sequence oriented or time stamp derived value, maintaining a level of synchronisation between the Sending Entity and the Receiving Entity.

Cryptographic Checksum: string of bits derived from some secret information, (e.g. a secret key), part or all of the Application Message, and possible further information (e.g. part of the Security Header)

NOTE 3: The secret key is known to the Sending Entity and to the Receiving Entity. The Cryptographic Checksum is often referred to as Message Authentication Code.

DES: standard cryptographic algorithm specified as DEA in ISO 8731-1 [9]

Digital Signature: string of bits derived from some secret information, (e.g. a secret key), the complete Application Message, and possible further information (e.g. part of the Security Header)

NOTE 4: The secret information is known only to the Sending Entity. Although the authenticity of the Digital Signature can be proved by the Receiving Entity, the Receiving Entity is not able to reproduce the Digital Signature without knowledge of the secret information owned by the Sending Entity.

Message Identifier: two-octet field used to identify the source and type of the message

Page Parameter: single octet field used to represent the CBS page number in the sequence and the total number of pages in the SMS-CB message

Receiving Application: the entity to which the Application Message is destined

Receiving Entity: the entity where the Secured Packet is received (e.g. SMS-SC, UICC, USSD entry point, or dedicated (U)SIM Toolkit Server) and where the security mechanisms are utilised

NOTE 5: The Receiving Entity processes the Secured Packets.

Redundancy Check: string of bits derived from the Application Message and possible further information for the purpose of detecting accidental changes to the message, without the use of any secret information

Response Header: security Header of a Response Packet

Response Packet: secured Packet transmitted by the Receiving Entity to the Sending Entity, containing a secured response and possibly application data

Secured Data: field contains the Secured Application Message and possibly padding octets

Secured Packet: information flow on top of which the level of required security has been applied

NOTE 6: An Application Message is transformed with respect to a chosen Transport Layer and chosen level of security into one or more Secured Packets.

Security Domain: An application in charge of security management as defined in the Open Platform Card Specification [14]

Security Header: that part of the Secured Packet which consists of all security information (e.g. counter, key identification, indication of security level, checksum or Digital Signature)

Sender Identification: this is the simple verification of the identity of the Sending Entity by the Receiving Entity comparing the sender identity with an apriori stored identity of the sender at the Receiving Entity.

Sending Application: entity generating an Application Message to be sent

Sending Entity: this is the entity from which the Secured Packet originates (e.g. SMS-SC, UICC, USSD entry point, or dedicated (U)SIM Toolkit Server) and where the security mechanisms are invoked

NOTE 7: The Sending Entity generates the Secured Packets to be sent.

Serial Number: two octet field which identifies a particular message.

NOTE 8: It is linked to the Message Identifier and is altered every time the message is changed.

Short Message: information that may be conveyed by means of the SMS Service as defined in 3G TS 23.040 [3].

Status Code: this is an indication that a message has been received (correctly or incorrectly, indicating reason for failure).

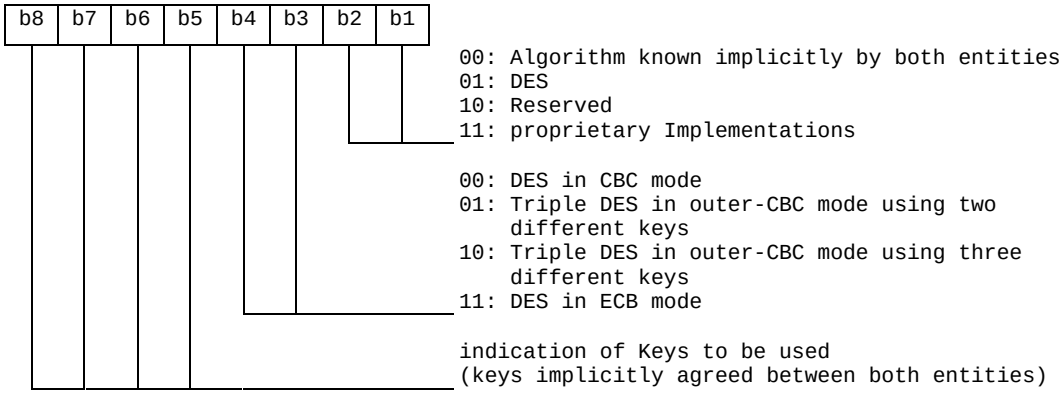
Transport Layer: this is the layer responsible for transporting Secured Packets through the 3G and GSM network.

NOTE 9: The transport layer implements one or more transport mechanisms, (e.g. SMS or USSD).

Unsecured Acknowledgement: this is a Status Code included in a response message

5.1.2 Coding of the KIc

The KIc is coded as below.



DES is the algorithm specified as DEA in ISO 8731-1 [9]. DES in CBC mode is described in ISO/IEC 10116 [10]. Triple DES in outer-CBC mode is described in section 15.2 of [20]. DES in ECB mode is described in ISO/IEC 10116 [10].

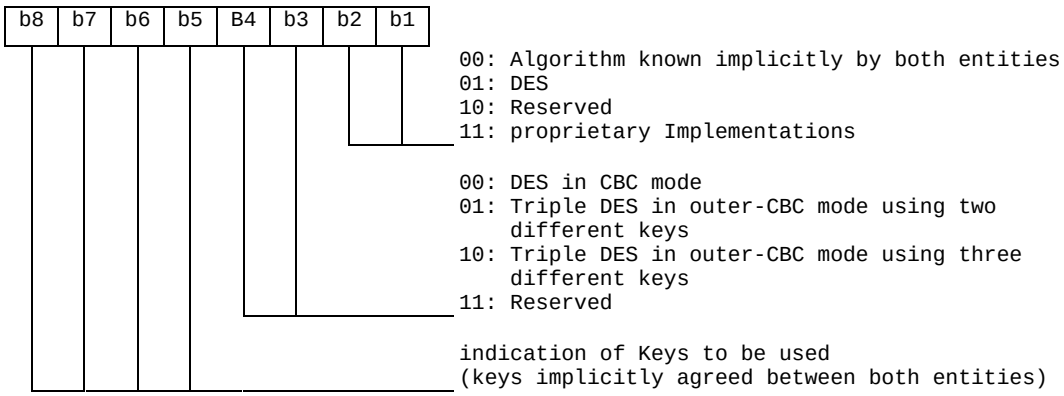
The initial chaining value for CBC modes shall be zero. For the CBC modes the counter (CNTR) shall be used.

~~If the indication of the key to be used refers to an Open Platform key set version number the algorithm to be used with the key shall be the algorithm associated with the key (as described in the Open Platform specification [14]).~~

For Open Platform security architecture compliant cards see Annex B.

5.1.3 Coding of the KID

The KID is coded as below.



DES is the algorithm specified as DEA in ISO 8731-1 [9]. DES in CBC mode is described in ISO/IEC 10116 [10]. Triple DES in outer-CBC mode is described in section 15.2 of [20].

The initial chaining value for CBC modes shall be zero. For the CBC modes the counter (CNTR) shall be used. If padding is required, the padding octets shall be coded hexadecimal '00'.

~~If the indication of the key to be used refers to an Open Platform key set version number the algorithm to be used with the key shall be the algorithm associated with the key (as described in the Open Platform specification [14]).~~

For Open Platform security architecture compliant cards see Annex B.

5.1.4 Counter Management

If in the first SPI byte b4b5=00 (No counter available) the counter field shall be ignored by the RE and the RE shall not update the counter.

If b5 of the first SPI byte is equal to 1 then the following rules shall apply to counter management, with the goal of preventing replay and synchronisation attacks:

- The SE sets the counter value. It shall only be incremented.
- The RE shall update the counter to its next value upon receipt of a Command Packet after the corresponding security checks (i.e. RC/CC/DS and CNTR verification) have been passed successfully.

  The next counter value is the one received in the incoming message.
- When the counter value reaches its maximum value the counter is blocked.

If there is more than one SE, care has to be taken to ensure that the counter values remain synchronised between the SE's to what the RE is expecting, irrespective of the transport mechanism employed.

The level of security is indicated via the proprietary interface between the Sending/Receiving Application and Sending/Receiving Entity. Application designers should be aware that if the Sending Application requests "No RC/CC/DS" or "Redundancy Check" and "No Counter Available" from the SE, no security is applied to the Application Message and therefore increased threat of malicious attack.

For Open Platform security architecture compliant cards see Annex B.

Annex B (normative): Relation between security layer and Open Platform security architecture

This annex only applies to cards implementing the security architecture defined in the Open Platform Card Specification [14].

The security of Application Messages (i.e. RC/CC/DS, ciphering/deciphering, counter management) shall be managed by the Security Domain of the Application.

B.1 Key set version - counter association within a Security Domain

A separate and different counter shall be associated to each key set version as described in the following table:

	Key Set Version 0	**Key Set Version 1**	**….**	**Key Set Version n (maximum 'F')**
	Reserved	Counter 1		Counter n
Key Index 1	Reserved	KIc 1		KIc n
Key Index 2	Reserved	KID 1		KID n
Key Index 3	Reserved	KIK 1		KIK n

B.2 Security keys KIc, KID

The indication of the key to be used in the KIc and KID fields shall refer to an Open Platform key set version number.

The algorithm to be used with the key shall be the algorithm associated with the key (as described in the Open Platform Card specification [14]).

The key set version number indicated in the KIc and KID fields shall be identical when different from 0. If the key set version numbers are different (and both different from 0) then the message shall be rejected with the “Unidentified security error” Response Status Code.

3GPP T3 Meeting #22
Marbella, Spain, 22 - 25 Jan 2002

Tdoc T3-020112
Revised T3-010681

3GPP T3 (USIM) Meeting #21
Kyoto, Japan, 5 - 7 November 2001

Tdoc T3-010681

CR-Form-v4

CHANGE REQUEST

⌘ **23.048** **CR** **018** ⌘ ev **-** ⌘ Current version: **4.2.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarifications on Access Domain Parameter
Source:	⌘	T3
Work item code:	⌘	USAT1-SM
Date:	⌘	25/01/02
Category:	⌘	**F**
Release:	⌘	REL-4

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)

Reason for change:	⌘	Avoid the applet performing operations on files which are protected by NEVER. Clarify the file access conditions defined in the Access Domain Parameter: the note which has been suppressed can lead to misinterpretations.
Summary of change:	⌘	Clarifications on the Full Access and on access conditions to the GSM File system in the Access Domain Parameter of the install(install)
Consequences if not approved:	⌘	It will be possible to do operations on files even if there are protected by NEVER

Clauses affected:	⌘	§ A.1.4.2.3.1		
Other specs affected:	⌘	[X] Other core specifications	⌘	23.048 Rel-5
		[ ] Test specifications		
		[ ] 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/3G_Specs/CRs.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.

A.1.4.2.3.1 Access Domain Parameter

This parameter indicates the mechanism used to control the applet instance access to the GSM file System.

Value	Name	Support	ADD length
'00'	Full access to the File System	Mandatory	0
'01'	APDU access mechanism (see A.1.4.2.3.2)	Optional	2
'02'	3GPP access mechanism (see A.1.4.2.3.3)	Optional	[To be defined]
'03' to '7F'	RFU	RFU	RFU
'80' to 'FE'	Proprietary mechanism	-	-
'FF'	No access to the File System	Mandatory	0

The access rights granted to an applet and defined in the access domain parameter shall be independent from the access rights granted at the (U)SIM/ME interface.

If an applet with Access Domain Parameter 'FF' (i.e. No Access to the File System) tries to access a file the framework shall throw an exception.

If an applet has Access Domain Parameter '00' (i.e. Full Access to the File System), all actions can be performed on a file except the ones with NEVER access condition.

~~NOTE: The file access conditions specified in 3GPP TS 51.011 [5] are relevant for the SIM/ME interface only. The file access conditions specified in the access domain parameter are used internally by the card operating system.~~

If the Access Domain Parameter requested is not supported, the card shall return the Status Word '6A80', incorrect parameters in data field, to the Install(Install) command.

3GPP T3 Meeting #22
Marbella, Spain, 22 - 25 Jan 2002

Tdoc T3-020113
Revised T3-010681

3GPP T3 (USIM) Meeting #21
Kyoto, Japan, 5 - 7 November 2001

Tdoc T3-010681

CR-Form-v4

CHANGE REQUEST

⌘ **23.048** **CR** **019** ⌘ ev **-** ⌘ Current version: **5.2.0** ⌘

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

Proposed change affects: ⌘ (U)SIM [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Clarifications on Access Domain Parameter
Source:	⌘	T3
Work item code:	⌘	USAT1-SM
Date:	⌘	25/01/02
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)

Reason for change:	⌘	Avoid the applet performing operations on files which are protected by NEVER. Clarify the file access conditions defined in the Access Domain Parameter: the note which has been suppressed can lead to misinterpretations.
Summary of change:	⌘	Clarifications on the Full Access and on access conditions to the GSM File system in the Access Domain Parameter of the install(install)
Consequences if not approved:	⌘	It will be possible to do operations on files even if there are protected by NEVER

Clauses affected:	⌘	§ A.1.4.2.3.1		
Other specs affected:	⌘	[X] Other core specifications	⌘	23.048 Rel-4
		[ ] Test specifications		
		[ ] 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/3G_Specs/CRs.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.

A.1.4.2.3.1 Access Domain Parameter

This parameter indicates the mechanism used to control the applet instance access to the GSM file System.

Value	Name	Support	ADD length
'00'	Full access to the File System	Mandatory	0
'01'	APDU access mechanism (see A.1.4.2.3.2)	Optional	2
'02'	3GPP access mechanism (see A.1.4.2.3.3)	Optional	[To be defined]
'03' to '7F'	RFU	RFU	RFU
'80' to 'FE'	Proprietary mechanism	-	-
'FF'	No access to the File System	Mandatory	0

The access rights granted to an applet and defined in the access domain parameter shall be independent from the access rights granted at the (U)SIM/ME interface.

If an applet with Access Domain Parameter 'FF' (i.e. No Access to the File System) tries to access a file the framework shall throw an exception.

If an applet has Access Domain Parameter '00' (i.e. Full Access to the File System), all actions can be performed on a file except the ones with NEVER access condition.

~~NOTE: The file access conditions specified in 3GPP TS 51.011 [5] are relevant for the SIM/ME interface only. The file access conditions specified in the access domain parameter are used internally by the card operating system.~~

If the Access Domain Parameter requested is not supported, the card shall return the Status Word '6A80', incorrect parameters in data field, to the Install(Install) command.