3GPP TSG-T (Terminals) Meeting #8
Düsseldorf, Germany, 21 - 23 June, 2000

Tdoc TP-000110

CHANGE REQUEST No : 040

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

Technical Specification 3G TS 31.102 Version: Release 99

Submitted to TSG	T #08	for approval	X	without presentation ("non-strategic")	
list SMG plenary meeting no. here ↑		for information		with presentation ("strategic")	

PT SMG CR cover form is available from: http://docbox.etsi.org/tech-org/smg/Document/smg/tools/CR_form/crf28_1.zip

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

Work item: MEXE

Source: T3 **Date:** 22/06/00

Subject: Support of root public keys (certificates) in the SIM for use by MExE terminals.

Category:
(one category and one release only 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	X		Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X

Reason for change: Support of operator public keys (certificates) in the USIM for use by MExE terminals.

Clauses affected:

References: Addition of MExE stage 2, 23.057

Abbreviations: Addition of MeXE definition

Section 4.2.8: addition of entry for “MExE ” in SIM service table.

Section 4.3: Addition of MExE Directory Identifier

Section 4.4.1.4: New section giving EFs below DF_{MExE}.

Section 5.5: New section on MExE related procedures.

Other specs affected:

Other releases of same spec	□	→ List of CRs:	
Other core specifications	□	→ List of CRs:	
MS test specifications / TBRs	□	→ List of CRs:	
BSS test specifications	□	→ List of CRs:	
O&M specifications	□	→ List of CRs:	

Other comments:

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] 3G TS 21.111: "USIM and IC Card Requirements".

....

[27] 3G TS 22.022: "Personalisation of GSM Mobile Equipment (ME); Mobile functionality specification".

[28] 3G TS 23.057 Terminals;Mobile Station Application Execution Environment (MExE);Functional description; Stage 2

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3rd Generation Partnership Project
AC	Access Condition
ACL	APN Control List
ADF	Application Dedicated File
AID	Application IDentifier
AK	Anonymity key
ALW	ALWays
AMF	Authentication Management Field
AoC	Advice of Charge
APN	Access Point Name
AuC	Authentication Centre
AUTN	Authentication token
BDN	Barred Dialling Number
CCP	Capability Configuration Parameter
CK	Cipher key
CLI	Calling Line Identifier
CNL	Co-operative Network List
CS	Circuit switched
DCK	Depersonalisation Control Keys
DF	Dedicated File
DO	Data Object
EF	Elementary File
EMUI	Encrypted Mobile User Identity
EUIC	Enhanced User Identity Confidentiality
FCP	File Control Parameters
FFS	For Further Study
GK	User group key
GMSI	Group Identity
GSM	Global System for Mobile communications
HE	Home Environment
ICC	Integrated Circuit Card
ICI	Incoming Call Information
ICT	Incoming Call Timer
ID	IDentifier
IK	Integrity key
IMSI	International Mobile Subscriber Identity
K	USIM Individual key
K_C	Cryptographic key used by the cipher A5
KSI	Key Set Identifier
LI	Language Indication
LSB	Least Significant Bit
MAC	Message authentication code
MAC-A	MAC used for authentication and key agreement
MAC-I	MAC used for data integrity of signalling messages
MCC	Mobile Country Code
MExE	Mobile Execution Environment
MF	Master File
MMI	Man Machine Interface
MNC	Mobile Network Code
MODE	Indication packet switched / circuit switched mode
MSB	Most Significant Bit
NEV	NEVer

4.2.8 EF$_{UST}$ (USIM Service Table)

This EF indicates which services are available. If a service is not indicated as available in the USIM, the ME shall not select this service.

Identifier: '6F38'	Structure: transparent	Mandatory
SFI: Mandatory		
File size: X bytes, X >= 2	Update activity: low	
Access Conditions: READ PIN UPDATE ADM DEACTIVATE ADM ACTIVATE ADM		

Bytes	Description	M/O	Length
1	Services n°1 to n°8	M	1 byte
2	Services n°9 to n°16	O	1 byte
3	Services n°17 to n°24	O	1 byte
4	Services n°25 to n°32	O	1 byte
etc.			
X	Services n°(8X-7) to n°(8X)	O	1 byte

-Services

Contents:	Service n°1 :	Local Phone Book
	Service n°2 :	Fixed Dialling Numbers (FDN)
	Service n°3 :	Extension 2
	Service n°4 :	Service Dialling Numbers (SDN)
	Service n°5 :	Extension3
	Service n°6 :	Barred Dialling Numbers (BDN)
	Service n°7 :	Extension4
	Service n°8 :	Outgoing Call Information (OCI and OCT)
	Service n°9 :	Incoming Call Information (ICI and ICT)
	Service n°10:	Short Message Storage (SMS)
	Service n°11:	Short Message Status Reports (SMSR)
	Service n°12:	Short Message Service Parameters (SMSP)
	Service n°13:	Advice of Charge (AoC)
	Service n°14:	Capability Configuration Parameters (CCP)
	Service n°15:	Cell Broadcast Message Identifier
	Service n°16:	Cell Broadcast Message Identifier Ranges
	Service n°17:	Group Identifier Level 1
	Service n°18:	Group Identifier Level 2
	Service n°19:	Service Provider Name
	Service n°20:	PLMN selector
	Service n°21:	MSISDN
	Service n°22:	Image (IMG)
	Service n°23:	Not used (reserved for SoLSA)
	Service n°24:	Enhanced Multi-Level Precedence and Pre-emption Service
	Service n°25:	Automatic Answer for Emlpp
	Service n°26:	EUIC (Enhanced User Identity Confidentiality)
	Service n°27:	GSM Access
	Service n°28:	Data download via SMS-PP
	Service n°29:	Data download via SMS-CB
	Service n°30:	Call Control by USIM
	Service n°31:	MO-SMS Control by USIM
	Service n°32:	RUN AT COMMAND command
	Service n°33:	Packet Switched Domain
	Service n°34:	Enabled Services Table
	Service n°35:	APN Control List (ACL)
	Service n°36:	Depersonalisation Control Keys
	Service n°37:	Co-operative Network List
	Service n°38:	GSM security context
	Service no. nn	MExE

4.3 DFs at the USIM ADF (Application DF) Level

DFs may be present as child directories of USIM ADF. The following DFs are defined:

- DF$_{\text{PHONEBOOK}}$ '5F3A'.
- DF$_{\text{MExE}}$ '5F3B'

(DF for application specific phonebook. This DF has the same structure as the DF$_{\text{PHONEBOOK}}$ under DF$_{\text{TELECOM}}$).

'5F70' is reserved for DF$_{\text{SoLSA}}$ and is expected to be defined in the release 2000 ver of the present document.

4.4 Contents of DFs at the USIM ADF (Application DF) level

4.4.1 Contents of files at the DF SoLSA level

This subclause is expected to be defined in the release 2000 version of the present document.

4.4.1.1 EF$_{\text{SAI}}$ (SoLSA Access Indicator)

This subclause is expected to be defined in the release 2000 version of the present document.

4.4.1.2 EF$_{\text{SLL}}$ (SoLSA LSA List)

This subclause is expected to be defined in the release 2000 version of the present document.

4.4.1.3 LSA Descriptor files

This subclause is expected to be defined in the release 2000 version of the present document.

4.4.1.4 Contents of files at the MExE level

This subclause specifies the EFs in the dedicated file DF$_{\text{MExE}}$. It only applies if support of MExE by the USIM is supported (see TS 23.057 [28]).

The EFs in the Dedicated File DF$_{\text{MExE}}$ contain execution environment related information.

4.4.1.4.1 EF$_{\text{MExE\_ST}}$ (MExE Service table)

This EF indicates which MExE services are allocated, and whether, if allocated, the service is activated. If a service is not allocated or not activated in the USIM, the ME shall not select this service.

<table>
<tr><td colspan="2">Identifier: '????'</td><td>Structure: transparent</td><td>Optional</td></tr>
<tr><td colspan="2">File size: X bytes, X ≥ 1</td><td colspan="2">Update activity: low</td></tr>
<tr><td colspan="4">Access Conditions:
READ PIN
UPDATE ADM
INVALIDATE ADM
REHABILITATE ADM</td></tr>
<tr><td>Bytes</td><td>Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1</td><td>Services n°1 to n°8</td><td>M</td><td>1 byte</td></tr>
<tr><td>2</td><td>Services n°9 to n°16</td><td>O</td><td>1 byte</td></tr>
<tr><td>etc.</td><td></td><td></td><td></td></tr>
<tr><td>X</td><td>Services (8X-7) to (8X)</td><td>O</td><td>1 byte</td></tr>
</table>

-Services
Contents:

Service n°1 :	Operator root public key
Service n°2 :	Administrator root public key
Service n°3 :	Third party root public key
Service n°4 :	RFU

Coding:

the coding rules of the USIM Service Table apply to this table.

4.4.1.4.2 EF$_{ORPK}$ (Operator root public key)

This EF contains the descriptor(s) of certificates containing the operator root public key. This EF shall only be allocated if the operator wishes to verify applications and certificates in the MExE operator domain using a root public key held on the SIM. Each record of this EF contains one certificate descriptor.

For example, Operator may provide a second key for recover disaster procedure in order to limit OTA data to load.

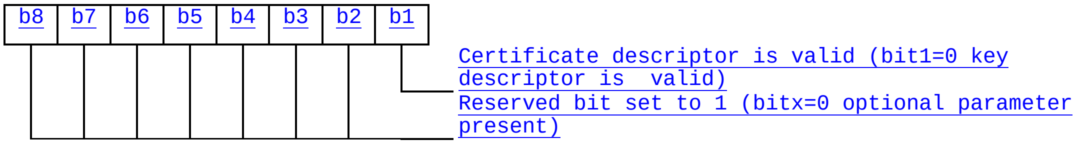
Identifier: '????'	Structure: linear fixed		Optional
Record length : X + 10 bytes		Update activity: low	
Access Conditions: READ PIN UPDATE ADM INVALIDATE ADM REHABILITATE ADM			
Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (k)	M	1 byte
11 to 10+k	Key identifier	M	k bytes

- Parameter indicator

Contents:

The parameter indicator indicates if record is full and which optional parameters are present

Coding: bit string

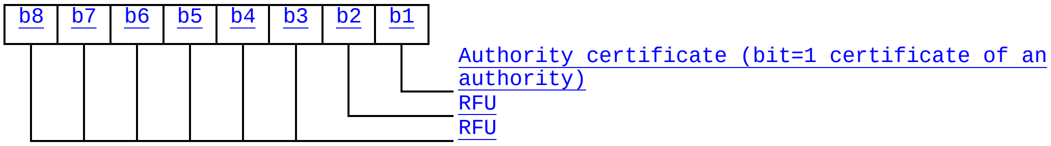

b8
b7
b6
b5
b4
b3
b2
b1
Certificate descriptor is valid (bit1=0 key descriptor is valid)
Reserved bit set to 1 (bitx=0 optional parameter present)

- Flags

Contents:

The authority flag indicates whether the certificate identify an authority (i.e. CA or AA) or not.

Coding: bit string



- Type of certificate

Contents:
This field indicates the type of certificate containing the key.
Coding: binary :
0 : WTLS
1 : X509
2 : X9.68
Other values are reserved for further use

- Key/certificate File Identifier
Contents:
these bytes identify an EF which is the key/certificate data file (see subclause 4.4.1.4.5), holding the actual key/certificate data for this record.
Coding:
byte 4: high byte of Key/certificate File Identifier;
byte 5: low byte of Key/certificate File Identifier.

- Offset into Key/certificate File
Contents:
these bytes specify an offset into the transparent key/certificate data File identified in bytes 4 and 5.
Coding:
byte 6: high byte of offset into Key/certificate Data File;
byte 7: low byte of offset into Key/certificate Data File

- Length of Key/certificate Data
Contents:
these bytes yield the length of the key/certificate data, starting at the offset identified in "Offset into Key/certificate File" field.
Coding:
byte 8: high byte of Key/certificate Data length;
byte 9: low byte of Key/certificate Data length.

- Key identifier length
Contents:
This field gives length of key identifier
Coding:
binary

- Key identifier
Contents:
This field provides a means of identifying certificates that contents a particular public key (chain building) and linking the public key to its corresponding private key. For more information about value and using see TS 23.057 [28].
Coding:
octet string

Note: transparent key/certificate data longer than 256 bytes may be read using successive READ BINARY commands.

4.4.1.4.3 EF_{ARPK} (Administrator root public key)

This EF contains the descriptor(s) of certificates containing the Administrator root public key. This EF shall only be allocated if the SIM issuer wishes to control the Third Party certificates on the terminal using an Administrator root public key held on the SIM. Each record of this EF contents one certificate descriptor.

This file shall contain only one record.

Identifier: '????'	Structure: linear fixed	Optional
Record length: X + 10 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (k)	M	1 byte
11 to 10+k	Key identifier	M	k bytes

For contents and coding of all data items see the respective data items of the EF_{ORPK} (sub-clause 4.4.1.4.2).

4.4.1.4.4 EF_{TPRPK} (Third party root public key)

This EF contains descriptor(s) of certificates containing the Third Party root public key (s). This EF shall only be allocated if the SIM issuer wishes to verify applications and certificates in the MExE Third Party domain using root public key(s) held on the SIM. This EF can contain one or more root public keys. . Each record of this EF contents one certificate descriptor.

For example, an operator may provide several Third Party root public keys.

Identifier: '????'	Structure: linear fixed	Optional
Record length : X + 10 bytes	Update activity: low	

Access Conditions:

READ	PIN
UPDATE	ADM
INVALIDATE	ADM
REHABILITATE	ADM

Bytes	Description	M/O	Length
1	Parameters indicator	M	1 byte
2	Flags	M	1 byte
3	Type of certificate	M	1 byte
4 to 5	Key/certificate file identifier	M	2 bytes
6 to 7	Offset into key/certificate file	M	2 bytes
8 to 9	Length of key/certificate data	M	2 bytes
10	Key identifier length (k)	M	1 byte
11 to 10+k	Key identifier	M	k bytes
11+k to11+k	Certificate identifier length (m)	M	1 byte
12+k to11+k+m	Certificate identifier	M	m bytes

- Certificate identifier length
  Contents:
    This field gives length of certificate identifier
  Coding:
    binary

- Certificate identifier
  Contents:
    This field identify the issuer and provide a easy way to find a certificate. For more information about value and using see TS 23.057 [28].
  Coding:
    Octet string

For contents and coding of all other data items see the respective data items of the EF$_{\text{ORPK}}$ (sub-clause 4.4.1.4.2).

4.4.1.4.5 EF$_{\text{TKCDF}}$ (Trusted Key/Certificates Data Files)

Residing under DF$_{\text{MExE}}$, there may be several key/certificates data files. These EFs containing key/certificates data shall have the following attributes:

Identifier: '??XX'	Structure: transparent	Optional
Record length: Y bytes	Update activity: low	
Access Conditions: READ PIN UPDATE ADM INVALIDATE ADM REHABILITATE ADM		

Bytes	Description	M/O	Length
1 to Y	Key/Certicates Data	M	Y bytes

Contents and coding:

Key/certificate data are accessed using the key/certificates descriptors provided by EF$_{\text{xrpk}}$ (see sub-clause 4.4.1.4.).

The identifier '??XX' shall be different from one key/certificate data file to the other. For the range of 'XX', see sub-clause 6.6. The length Y may be different from one key/certificate data file to the other.

5.4 USAT related procedures

5.4.1 Data Download via SMS-PP

Requirement: USIM Service n°28 "available".

The procedures and commands for Data Download via SMS-PP are defined in 3G TS 31.111 [12].

5.4.2 Image Request

The terminal sends the identification of the information to be read. The terminal shall analyse the data of EF_{IMG} to identify the files containing the instances of the image. If necessary, then the terminal performs READ BINARY commands on these files to assemble the complete image instance data.

5.4.3 Data Download via SMS-CB

Requirement: USIM Service n°29 "available".

The ME shall perform the reading procedure with EF_{CBMID}, and add the message identifiers to the Cell Broadcast search list. On receiving a cell broadcast message the procedure defined in 3G TS 31.111 [12] applies.

5.4.4 Call Control by USIM

Requirement: USIM Service n°30 "available".

The procedures and commands for Call Control by USIM are defined in 3G TS 31.111 [12]. It is mandatory for the ME to perform the procedures if it has indicated that it supports Call Control by USIM in the TERMINAL PROFILE command.

5.4.5 MO-SMS control by USIM

Requirement: USIM Service n°31 "available".

The procedures and commands for MO-SMS control by USIM are defined in 3G TS 31.111 [12]. It is mandatory for the ME to perform the procedures if it has indicated that it supports MO-SMS control by USIM in the TERMINAL PROFILE command.

5.5 MExE related procedures

MExE is an optional feature. The higher level procedures, and contents and coding of the commands, are given in 3GPP 23.057 [28]. Procedures relating to the transmission of commands and responses across the USIM/ME interface are given in this section. A USIM or ME supporting MExE shall conform to the requirements given in this section.

5.5.1 MExE ST

Requirement: Service n°nn (MExE) "allocated and activated".
Request: The ME performs the reading procedure with EF_{MExE_ST}

5.5.2 Operator root public key

Requirement: Service n°nn (MExE) "allocated and activated" and MExE ST service n°1 (EF_{ORPK})" allocated and activated".
Request: The ME performs the reading procedure with EF_{ORPK} . The ME shall analyse the data of EF_{ORPK} (sub-clause 4.4.1.4.2) to identify the files containing the certificate instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete certificate instance data.

5.5.3 Administrator root public key

Requirement: Service n°nn (MExE) "allocated and activated" and MExE ST service n°2 (EF_{ARPK}) "allocated and activated".
Request: The ME performs the reading procedure with EF_{ARPK}. The ME shall analyse the data of EF_{ARPK} (sub-clause 4.4.1.4.3) to identify the file containing the certificate instance. If necessary, then the ME performs READ BINARY commands on this file to assemble the complete certificate instance data.

5.5.4 Third Party root public key(s)

Requirement: Service n°nn (MExE) "allocated and activated" and MExE ST service n°3 (EF_{TPRPK}) "allocated and activated".
Request: The ME performs the reading procedure with EF_{TPRPK}. The ME shall analyse the data of EF_{TPRPK} (sub-clause 4.4.1.4.4) to identify the files containing the certificate instances. If necessary, then the ME performs READ BINARY commands on these files to assemble the complete certificate instance data.

5.5.5 Trusted Key/Certificates Data Files

Requirement: Service n°nn (MExE) "allocated and activated.
Request: The ME performs the reading procedure with EF_{TKCDF}. The ME shall analyse the data of EF_{TKCDF} and, if necessary, perform READ BINARY commands on these files