3GPP TSG SA WG3 Security — S3#20 **S3-010454**

16 - 19 October, 2001

Sydney, Australia

3GPP TSG-T WG2#14
Edinburgh, Scotland
3 - 7 September 2001

T2-010692

Title:	PKCS#15 support for MExE in the USIM
Source:	TSG-T WG2
To:	TSG-T WG3
CC:	TSG-T WG1, SA WG3
Contact Person:	**Name:** Pubudu Chandrasiri **Company:** Vodafone **E-mail Address:** Pubudu.chandrasiri@vodafone.com **Tel. Number:** +44 (0) 1635 682986

TSG-T WG2 would like to bring to T3's attention that the current MExE specification (3GPP TS 23.057) specifies in Annex A a PKCS#15 file structure and an object format when storing and referencing MExE certificates in the USIM. However it has been noted that MExE file and object format as specified in current USIM specifications is not actually based on PKCS#15.

TSG-T WG2 has considered a CR to TS 31.102 to correct this but could not reach complete consensus. However, as the close of release 5 is approaching, and as any CR T2 approve on this issue must be examined carefully by T3, T2 would like T3 to consider the attached draft CR (*T2-010693*) and give T2 any feedback that T3 can. T2 hope to present an agreed CR at the next T3 meeting based on T3 comments and further discussion within TSG-T WG2.

TSG-T WG2 considers full use of PKCS#15 for storing root certificates on the USIM as advantageous both for efficiency reasons (MEs) that support the WIM can re-use this capability for storage and retrieval of certificates for WAP and because PKCS#15 is a useful and elegant way to store and retrieve security related information such as certificates.

Please note that the reference to the Wireless Identity Module (WIM) in the draft CR does not imply WIM support in the USIM, we are only using the WIM specification as a useful reference for PKCS#15. There is a precedent for storing data as PKCS#15 objects on the (U)SIM without requiring support of the WIM and that precedent is the WAP Smartcard Provisioning specification (WAP-186-PROVSC-20010710-a).

TSG-T WG2 therefore requests T3 to consider the enclosed draft CR to TS 31.102 and give feedback on it to TSG-T WG2. TSG-T WG2 looks forward to continuing fruitful cooperation with T3.

3GPP TSG-T WG2#14
Edinburgh, Scotland
3 - 7 September 2001

T2 – 010693

CR-Form-v4

CHANGE REQUEST

⌘	**TS 31.102**	**CR**	**CRNum**	⌘	ev	**-**	⌘	Current version:	**V4.0.0** ⌘

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 ☒ ME/UE ☒ Radio Access Network □ Core Network □

Title: ⌘	MExE root certificate storage on the USIM		
Source: ⌘	Vodafone & Ericsson		
Work item code: ⌘	MExE-ENHANC	***Date:*** ⌘	10 August 2001
Category: ⌘	**C**	***Release:*** ⌘	Release 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: ⌘	TS 23.057, MExE, require a generic format for storing certificates and related information based PKCS#15. The current text related to MExE in TS 31.10 fails to meet that requirement by defining a new storage format.
Summary of change: ⌘	Instead of specifying a MExE format for storing certificates on the USIM the more generic PKCS#15 scheme is introduced. The introduction is done by referring to the DF(PKCS#15) and EF CDF defined for WAP Provisioning Smart Card.
Consequences if not approved: ⌘	Interoprability problems between MExE terminals and USIM

Clauses affected: ⌘	2 and 4.4.4	
Other specs affected: ⌘	□ Other core specifications ⌘ □ Test specifications □ O&M Specifications	
Other comments: ⌘		

[34] 3GPP TS 05.05: "Radio Transmission and Reception"

[35] ISO/IEC 8825(1990): "Specification of Basic Encoding Rules for Abstract Syntax Notation One" Second Edition.

[36] 3GPP TS 23.097: "Multiple Subscriber Profile (MSP)"

[37] WAP Provisioning Smart Card specification, WAP-186-PROVSC-20010710-a, www.wapforum.org/what/technical.htm

[38] PKCS#15: “Cryptographic Token Information Standard”, version 1.1, RSA Laboratories June 2000

4.4.4 Contents of files at the MExE level

This subclause specifies the EFs in the dedicated file DF$_{MExE}$. It only applies if the USIM supports MExE (see TS 23.057 [30]).

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

MExE root certificates shall be stored in EF CDF located under DF(PKCS#15) as defined by [37]. The operator root certificate shall be stored in a trusted certificates CDF. Operator and Administrator root certificates are identified by the values XX and YY respectively in the PKCS#15[38] object ZZ~~YY~~. ~~All other~~ CA certificates without these values in PKCS#15 object ZZ in the EF CDF shall be considered ~~handled~~ as third party root certificates.

4.4.4.1 EF$_{MExE-ST}$ (MExE Service table)

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

<table>
<tr><td colspan="2">Identifier: '4F40'</td><td colspan="2">Structure: transparent</td><td>Optional</td></tr>
<tr><td colspan="3">File size: X bytes, X □ 1</td><td colspan="2">Update activity: low</td></tr>
<tr><td colspan="5">Access Conditions:
READ PIN
UPDATE ADM
DEACTIVATE ADM
ACTIVATE ADM</td></tr>
<tr><td>Bytes</td><td colspan="2">Description</td><td>M/O</td><td>Length</td></tr>
<tr><td>1</td><td colspan="2">Services n°1 to n°8</td><td>M</td><td>1 byte</td></tr>
<tr><td>2</td><td colspan="2">Services n°9 to n°16</td><td>O</td><td>1 byte</td></tr>
<tr><td>etc.</td><td colspan="2"></td><td></td><td></td></tr>
<tr><td>X</td><td colspan="2">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.

4.4.4.2 ~~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 in the USIM. Each record of this EF contains one certificate descriptor.~~

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

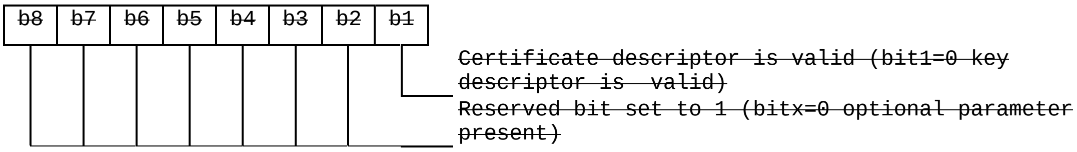
~~Identifier: '4F41'~~	~~Structure: linear fixed~~		~~Optional~~
~~Record length : X + 10 bytes~~		~~Update activity: low~~	
~~Access Conditions:~~ ~~READ PIN~~ ~~UPDATE ADM~~ ~~DEACTIVATE ADM~~ ~~ACTIVATE ADM~~			
~~Bytes~~	~~Description~~	~~M/O~~	~~Length~~
~~1~~	~~Parameters indicator~~	~~M~~	~~1 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 (X)~~	~~M~~	~~1 byte~~
~~11 to 10+X~~	~~Key identifier~~	~~M~~	~~X bytes~~

- ~~Parameter indicator~~

  ~~Contents:~~

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

  ~~Coding: bit string~~

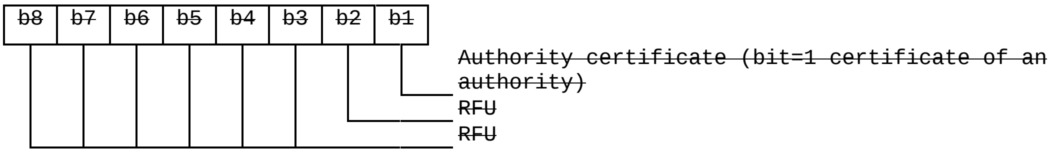

~~b8~~
~~b7~~
~~b6~~
~~b5~~
~~b4~~
~~b3~~
~~b2~~
~~b1~~
~~Certificate descriptor is valid (bit1=0 key descriptor is valid)~~
~~Reserved bit set to 1 (bitx=0 optional parameter present)~~

- ~~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 4.4.4.5), 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 contain 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 [30].~~

~~Coding:~~

~~octet string~~

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

~~4.4.4.3 EF$_{\text{ARPK}}$ (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 in the USIM. Each record of this EF contents one certificate descriptor.~~

~~This file shall contain only one record.~~

~~Identifier: ’4F42’~~	~~Structure: linear fixed~~		~~Optional~~
~~Record length: X + 10 bytes~~		~~Update activity: low~~	
~~Access Conditions:~~ ~~READ PIN~~ ~~UPDATE ADM~~ ~~DEACTIVATE ADM~~ ~~ACTIVATE 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 (X)~~	~~M~~	~~1 byte~~
~~11 to 10+X~~	~~Key identifier~~	~~M~~	~~X bytes~~

~~For contents and coding of all data items see the respective data items of the EF$_{\text{ORPK}}$ (sub-clause 4.4.4.2).~~

~~4.4.4.4 EF$_{\text{TPRPK}}$ (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 USIM issuer wishes to verify applications and certificates in the MExE Third Party domain using root public key(s) held in the USIM. This EF can contain one or more root public keys. Each record of this EF contains one certificate descriptor.~~

~~For example, an operator may provide several Third Party Root Public Keys.~~

~~Identifier:’4F43’~~	~~Structure: linear fixed~~		~~Optional~~
~~Record length : X + Y + 11 bytes~~		~~Update activity: low~~	
~~Access Conditions:~~ ~~READ PIN~~ ~~UPDATE ADM~~ ~~DEACTIVATE ADM~~ ~~ACTIVATE 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 (X)~~	~~M~~	~~1 byte~~
~~11 to 10+X~~	~~Key identifier~~	~~M~~	~~X bytes~~
~~11+X to 11+Y~~	~~Certificate identifier length (Y)~~	~~M~~	~~1 byte~~
~~12+X to 11+X+Y~~	~~Certificate identifier~~	~~M~~	~~Y bytes~~

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

- ~~Certificate identifier~~
  ~~Contents:~~
  ~~This field identifies the issuer and provides an easy way to find a certificate. For more information about the value and usage see TS 23.057 [30].~~
  ~~Coding:~~
  ~~Octet string~~

~~For contents and coding of all other data items see the respective data items of the EF$_{ORPK}$ (sub-clause 4.4.4.2).~~

~~4.4.4.5 EF$_{TKCDF}$ (Trusted Key/Certificates Data Files)~~

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

~~Identifier: ’4FXX’~~	~~Structure: transparent~~		~~Optional~~
~~File size: Y bytes~~		~~Update activity: low~~	
~~Access Conditions:~~ ~~READ PIN~~ ~~UPDATE ADM~~ ~~DEACTIVATE ADM~~ ~~ACTIVATE ADM~~			
~~Bytes~~	~~Description~~	~~M/O~~	~~Length~~
~~1 to Y~~	~~Key/Certificate Data~~	~~M~~	~~Y bytes~~

~~Contents and coding:~~

~~Key/certificate data are accessed using the key/certificates descriptors provided by EF$_{TPRPK}$ (see sub-clause 4.4.4.4).~~

~~The identifier ’4FXX’ shall be different from one key/certificate data file to another. For the range of ’XX’, see TS 31.101 [11]. The length Y may be different from one key/certificate data file to another.~~