3GPP TSG-T (Terminals) Meeting #14
Kyoto, Japan, 12 - 14 December 2001

Tdoc TP-010268

Agenda Item: 5.2.3

Source: T2

Title: "MExE" Change Requests

Document for: Approval

Spec	CR	Rev	Rel	Subject	Cat	Vers-Curr	Vers-New	T2 Tdoc	Workitem
23.057	098		Rel-4	Changing figure number 6A to 7	F	4.3.1	4.4.0	T2-010946	MEXE-ENHANC
23.057	099		Rel-4	Spell check and clarifications	F	4.3.1	4.4.0	T2-010957	MEXE-ENHANC
23.057	100		Rel-4	Addition reference to 23.227	F	4.3.1	4.4.0	T2-010959	MEXE-ENHANC
23.057	101		Rel-4	Certificate chain level inconsistency	F	4.3.1	4.4.0	T2-011131	MEXE-ENHANC
23.057	102		Rel-4	Signature algorithm specification	F	4.3.1	4.4.0	T2-011132	MEXE-ENHANC
23.057	103		Rel-4	Marking MRPK/ARPK Invalid through Secure Mechanism	F	4.3.1	4.4.0	T2-011133	MEXE-ENHANC
23.057	104		Rel-4	Context of MCC+MNC Missing	F	4.3.1	4.4.0	T2-011135	MEXE-ENHANC
23.057	105		Rel-4	Removing References to Sun Microsystems	F	4.3.1	4.4.0	T2-011136	MEXE-ENHANC
23.057	106		Rel-4	Correction of PKCS #15 reference and editorial changes	F	4.3.1	4.4.0	T2-011245	MEXE-ENHANC

3GPP TSG-T2 #15
Cancun, Mexico
26-30 November 2001

T2-010946

CR-Form-v5

CHANGE REQUEST

⌘ **23.057** **CR** **098** ⌘ **rev** **-** ⌘ Current version: **4.3.1** ⌘

*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:	⌘	Changing figure number 6A to 7
Source:	⌘	T2
Work item code:	⌘	MEXE-ENHANC
Date:	⌘	18 November
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:	⌘	Changing figure number 6A to 7
Summary of change:	⌘	Changed the figure number 6A to 7
Consequences if not approved:	⌘	Not an easyfollowing figure numberscheme in the specification.

Clauses affected:	⌘	8.4.4
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://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.

8.4.4 Certificate Chain Verification

This clause presents the procedure of validation of any downloaded MExE executable. It checks for the presence of the signature used to sign the application as well as the presence and integrity of all the certificates needed to successfully verify the signature. As a result, the application under scrutiny is deemed trusted or untrusted, i.e. will be allowed execution in one of the secure domains or in untrusted area, or otherwise the application will not be allowed to be executed and will be deleted. In any outcome of the verification, the user is notified about the result. The user also may wish to see certificate details if the application is allowed to be executed on the MExE device.

The MExE device shall follow "certificate verification" procedure as described below. The procedure shall contain at least the following logical phases (not necessarily in the order stated below):

Signature and Certificate Verification Supported: Checks whether signature and certificate verification procedure is supported on the MExE ME.

Executable with Signature and End Entity Certificate (note): Checks whether the executable contains a signature together with the corresponding end entity certificate.

Valid Application Signature (note): This phase comprises the following checks:

- Check if the signature and the end entity certificate formats are supported by the device. If this check fails, the application is classified as untrusted.
- Check if the signature algorithm is supported/known by the device. If this check fails, the application is classified as untrusted.
- Check if the signature can be cryptographically verified by using the accompanying end entity certificate . If this check fails, the application is not allowed execution and is deleted.

Complete set of Intermediate Certificates Available (note): Checks if all the necessary intermediate certificates (certificates between the RPK and the end entity certificate) are available.

Valid RPK on (U)SIM/ME: Checks if a valid RPK (not expired) exists on the (U)SIM or on the ME that could verify a certificate chain originating from the end entity certificate accompanying the application.

NOTE: These steps could include validation (e.g. expiration, revocation, etc.) checking by means of e.g. OCSP, SCVP, CRL-Consultation, and etc. The use of certificate revocation checking is recommended but is not mandated or defined in this specification.

Certificate Chain Cryptographically Verified: Checks if all the certificates from the end entity certificate to the RPK can be verified cryptographically. Certificate verification shall be performed according to the functional requirements given in clause "Basic Path Validation" of RFC 2459 [43] excluding revocation checking.

Secure Domains Supported: Checks whether MExE ME supports secure domains.

Only if all the above checks are successful, the downloaded application is deemed trusted and is allowed to be executed in the designated trusted domain (operator, manufacturer, trusted third party). Otherwise, the application is either untrusted (execution in the untrusted area only is allowed) or deleted (execution is not allowed at all) as per the figure 7~~6A~~ "Certificate Chain Verification Diagram"and as explained above. The executable shall only be designated into one of the trusted domains, and it shall be possible to verify the certificate chain unambiguosly to one and only one root public key.

The MExE ME shall allow for a "user notification" procedure as described below.

It shall be possible to display certificate details to the user if requested, however, since the terminal might not have a display or might not be meant for a human user the methods presented in "user notification" section are not discussed any further in this specification. Figure 7~~6A~~ "Certificate Chain Verification Diagram"shows an example of the certificate chain verification procedure.

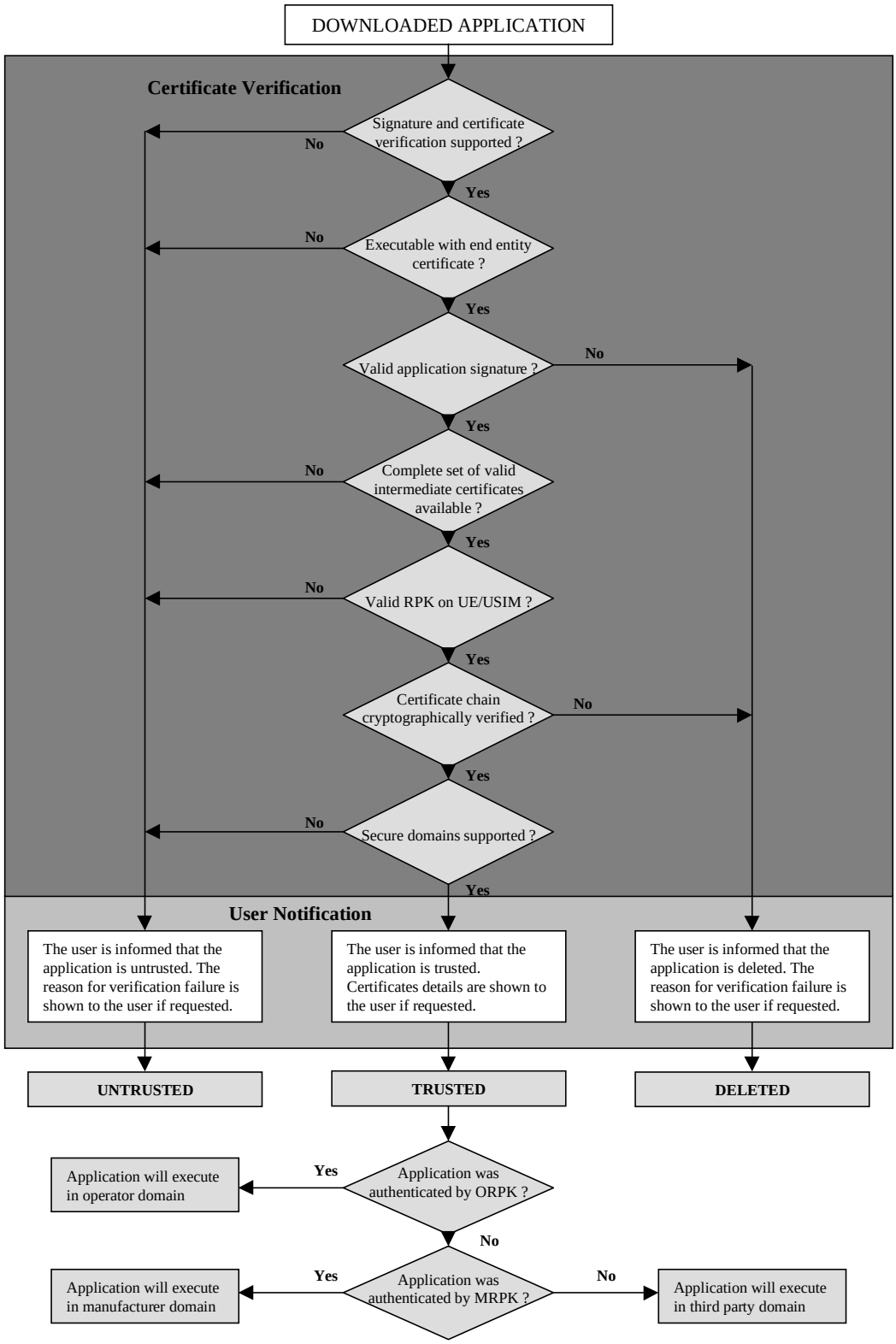


Figure 7~~6~~A: Certificate Chain Verification Diagram

3GPP TSG-T2 #15
Cancun, Mexico
26-30 November 2001

T2-010957

CR-Form-v5

CHANGE REQUEST

⌘ **23.057** **CR** **099** ⌘ **rev** **-** ⌘ Current version: **4.3.1** ⌘

*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:	⌘	Spell check and clarifications
Source:	⌘	T2
Work item code:	⌘	MEXE-ENHANC
Date:	⌘	18 November 2001
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:	⌘	Correct the spelling in the specification.
Summary of change:	⌘	Spelled the word correct and reworded where necessary.
Consequences if not approved:	⌘	Risk of misinterpretation

Clauses affected:	⌘	Chapter 3, 4, 5, 6, 8 and annexes
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://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.

3 Definitions and abbreviations

3.1 Definitions

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

administrator: administrator of the MExE device is the entity that~~which~~ has the control of the third party trusted domain, and all resources associated with the domain

...

MExE certificate: used in the realisation ~~of MExE~~of MExE security domains

...

MExE device: UE (User Equipment~~) which~~) that supports MExE functionality in the ME (Mobile Equipment)

...

MIDP application: MIDP application, or "MIDlet~~,~~", is one that uses only the APIs defined by the MIDP and CLDC specifications.

4 Generic MExE aspects

Support of at least one MExE classmark is mandatory. A MExE device may also include optional support for applications from any other MExE classmark (refer to clause 4.4).

This clause defines the common aspects of all MExE compliant devices, independent of MExE technology.

Considering the wide and diverse range of current and future technology and devices that (will) use wireless communication and provide services based thereon a one-size-fits-all approach is unrealistic. Instead the present document categorises devices by giving them different MExE classmarks. In this specification the following MExE classmarks are defined:

- MExE classmark 1 - based on WAP (Wireless Application Protocol) [6] - requires limited input and output facilities (e.g. as simple as a 3 lines by 15 characters display and a numeric keypad) on the client side, and is designed to provide quick and cheap information access even over narrow and slow data connections.
- MExE classmark 2 - based on PersonalJava [3] - provides and utilises a run-time system requiring more processing, storage, display and network resources, but supports more powerful applications and more flexible MMIs.
- MExE classmark 3 – based on J2ME CLDC and MIDP environment [34] and [35] – supports Java applications running on ~~resource constrained~~resource-constrained devices.

…

4.4 Multiple classmark support

Support of multiple MExE classmarks on a MExE device is optional.

A given MExE Classmark identifies support by a MExE device for a defined level of MExE functionality as defined by that classmark. Support of MExE classmarks by a MExE device shall enable flexible support of MExE functionality. A MExE device may support any multiple ~~combination~~combinations of MExE classmarks.

The support of any other functionality by a MExE device is also possible, and is out of scope of this specification.

NOTE: Some implementation issues may arise from the multiple support of classmarks on a device, e.g.:

1) In conforming to all of the requirements, how are mandatory requirements in one classmark compatible with optional requirements for another?

2) With Kk Java and pJava on one device, MIDP can be on top of a JavaVM. Which of the classmarks will it be then? In conforming with both Classmark 2 and 3 requirements, are 2 VMs required in one device?

...

4.11 ~~Journalling~~Journaling of network events

Support of the ~~journalling~~journaling of network events is mandatory.

To support the user in monitoring (potentially chargeable) network events initiated by services in the MExE environment, the MExE device shall maintain a record of network events initiated by MExE executables on the MExE device.

Network events for the purposes of ~~journalling~~journaling, are defined as events which result in the origination of connections by a service in the MExE environment of the MExE device. Examples of such events (any (potentially chargeable) network event initiated by services in the MExE environment) are:

- Sending an SMS message;
- Sending an USSD message;
- Initiating a circuit switched connection;
- Initiating a packet switched connection;
- Sending data over a packet switched connection.

The length, format and longevity of the journal is undefined and subject to manufacturers' discretion.

The journal shall be managed by the MExE device, and not be accessible by MExE executables.

4.12 User notification

Support of user notification is optional.

It is recommended that the MExE device should clearly display an indicator whenever network activity is in progress.

Ideally, this would be an icon on the phone's screen which is displayed whenever the MExE device is sending/receiving SMS, USSD, data call, voice call, or packets.

However, there are certain cases when this indicator need not be displayed, especially if it is obvious by some other means that the MExE device is performing network actions.

4.13 Quality of service

Support of Quality of Service is optional.

Quality of Service (QoS) [28] is seen by the end user as a measure of the amount of network resources given to an application by the underlying network. The network may employ a number of QoS mechanisms, but the end user / MExE executable is not involved in these. The end user / MExE executable requires an interface into the network QoS through a visible set of standard parameters.

A QoS aware MExE executable may request a QoS from the network at the beginning of a QoS session. Changes in the level of QoS provided shall be notified to the end user / MExE executable. An end user may request a change in the QoS through the MExE device MMI. A MExE executable may have several QoS streams open simultaneously.

When the MExE execution environment supports QoS, the MExE executable shall be able to dynamically request a change in the level of QoS at connection setup request or subsequently during the connection. The end user / MExE

executable may receive a rejection to a QoS modification request, upon which the end user / MExE executable must be notified.

The end user's service level QoS subscription parameters are stored in the network, they identify the maximum permissible QoS that a user may negotiate with the network. Several QoS subscriptions may be possible for one user. MExE is neither aware nor able to determine or modify the end user's service level QoS subscriptions.

Clause 9 Quality of Service defines the necessary functions for a MExE device to ~~accomodate~~accommodate QoS management and provisioning. QoS management may be available directly to the MExE executables themselves, or to the MExE environment.

...

5.2 WAP components~~Optionality~~

Mandatory and optional components of WAP are specified in the WAP specifications. Services and applications shall be able to determine the presence of optional parts of the functionality.

6.1.2 High level functions

6.1.2.1 Optional~~ity~~ Java packages

The use of Java encourages development of modular interfaces and minimal required functionality. Additional functionality is provided by optional APIs specified in terms of the Java language. ~~In general, optionality is specified in terms of Java packages. P~~Java packages are containers for the highest level of functionality in the Java language. In some cases, optional~~ity~~ Java packages are~~is~~ specified in terms of Java classes and interfaces. Classes and interfaces are elements contained inside packages.

The following table 4 "Optional~~ity~~ Java packages of the Wireless Profile of the JavaPhone APIs" specifies the Sun Microsystems defined optional~~ity~~ Java packages of the Wireless Profile of the JavaPhone APIs. Within some of the packages, certain classes and methods may be individually specified as optional by the JavaPhone API specification.

Where a mandatory package is identified, it is implicit that any packages called by that mandatory package are also mandatory.

Table 4: Optionality Java packages of the Wireless Profile of the JavaPhone APIs

JavaPhone API	Java package	Optionality/Mandatory
Addressbook	Javax.pim.addressbook	Mandatory
User Profile	Javax.pim.userprofile	Mandatory
Calendar	Javax.pim.calendar	Mandatory
Network	Java.net	Mandatory
Datagram	Javax.net.datagram	Mandatory
Power Monitor	Javax.power.monitor	Mandatory
Power Management	Javax.power.management	Optional
Install	Javax.install	Optional
Communications	Java.comm	Optional
SSL	Javax.net.ssl	Optional
JTAPI Core Package	Javax.telephony	Mandatory
JTAPI Core Capabilities Package	Javax.telephony.capabilities	Mandatory
JTAPI Core Events Package	Javax.telephony.events	Mandatory
JTAPI Call Control Package	Javax.telephony.callcontrol	Optional
JTAPI Call Control Capabilities Package	Javax.telephony.callcontrol.capabilities	Optional
JTAPI Call Control Events Package	Javax.telephony.callcontrol.events	Optional
JTAPI Phone Package	Javax.telephony.phone	Optional
JTAPI Phone Capabilities Package	Javax.telephony.phone.capabilities	Optional
JTAPI Phone Events Package	Javax.telephony.phone.events	Optional
JTAPI Mobile Package	Javax.telephony.mobile	Mandatory
	Java.math	Optional
	Java.rmi	Optional
	Java.rmi.dgc	Optional
	Java.rmi.registry	Optional
	Java.rmi.server	Optional
	Java.security	Optional
	Java.security.interfaces	Optional
	Java.sql	Optional
	Java.io	Optional

6.1.2.2 Required and optional PersonalJava APIs

MExE classmark 2 devices shall support the PersonalJava specification [3]. The PersonalJava APIs provide a standardised and readily implementable execution environment as a means for applications, applets, and content:

- to access and personalise the user interface via the java.awt packages;
- to utilise both Internet and Intranet connections via the java.net package.

…

6.1.2.5.1 Network protocol support

Support for network protocols in MExE classmark 2 devices is specified in the following table 5 "Support for network protocols":.

Table 5: Support for network protocols

Protocol	Optionality/Mandatory
HTTP/1.1 [9]	Mandatory
HTTPS	Mandatory
Gopher	Optional
ftp	Optional
mailto [25]	Mandatory
File	Optional

...

6.2.2.2.1 Networking

While CLDC specifies only a generic Connector used for all types of connections, MIDP extends connectivity support by providing support of the subset of the HTTP protocol. HttpConnection API provides the additional functionality to set request header, parse response headers and perform HTTP specific functions. The API must support RFC 2396 [40] and RFC 2616 [41].

The MIDP does not provide support for dDatagrams. If a Datagram API is to be implemented, the DatagramConnection interface defined in CLDC shall be used.

...

8.2.1 MExE executable permissions for operator, manufacturer and third party security domains

The following table 6 "Security domains and actions" specifies the permissions of operator, manufacturer and third party security domains in the order of restriction.

The actions listed in the security table 6 "Security domains and actions" are generic actions. These actions can only be performed by MExE executables via application programming interfaces (APIs) (which are intrinsically part of the MExE implementation) The security restrictions shall apply to MExE executables whether the API functionality is called directly or indirectly by the MExE executable. Explicit user permission is required for all actions by MExE executables in all domains. Types of user permission are defined in clause 8.3 User permission types.

Untrusted MExE executables are not permitted access to any actions which access the phone functionality (phone functionality includes all the actions in table 6 "Security domains and actions") except for the exceptions identified in clause 8.2.2 "MExE executable permissions for untrusted MExE executables".

Actions available using interfaces giving access to the phone functionality (either in existence at the time of approval of this specification or not) that are not listed in the security table 6 "Security domains and actions" shall be categorised into one of the groups in the security table 6 "Security domains and actions" by comparing its action against the groups in order as they are listed in the table 6 "Security domains and actions". If an action can be categorised into a more restrictive group near the top of the table, then it shall not be again categorised into another, less restrictive, group further down in the table. E.gFor example, if a new action eventually results in forwarding a call, it shall be categorised into Network access. If the action is totally new, it shall be categorised into some of the groups by comparing its functionality to the group description below and by comparing with the list of actions listed in the table within the group.

1. Device core function access includes functions, which are an essential part of the phone functionality .
2. Support of core software download, which allows updating the ME radio, characteristics and properties by changing the core software in the ME (e.g. a new CODEC may be loaded into a ME, a new air interface, etc.)
3. (U)SIM smart card low level access includes functions, which allow communications at the transport service access point (send and receive application protocol data unit).
4. Network security access includes all functionalities which relate to CHV, CHV2, UNBLOCK CHV and UNBLOCK CHV2 (verification, management, reading or modifying), GSM authentication, GSM ciphering.
5. Network property access includes functions, which enable the management of operator-related data parameters and network settings.
6. Network services access includes all functionalities which result in or need interaction via the operator´soperator's network.
7. User private data access includes all functionalities which relate to management, reading or modifying of data that the user has stored in the MExE device including user preferences.

...

8.3 User permission types

Support of user permission types is mandatory.

The term "user permission" is defined to mean that the user can give permission for a specific action in one of the ways defined in table 8 "User Permissions". Support single action permission is mandatory, but support of blanket permission and session permission is optional.

All prompts for user permission as described in table 8 "User ~~Permissions" must~~Permissions" must display a user friendly name identifying the signer of the corresponding MExE executable, if available. The user shall be able to request to see the "subject" field of the certificate of the signer ("subject" here refers to the "subject" fields of WTLS and X.509 certificates and an equivalent field for any other format of certificate). If an application, for which user permission is being sought, is untrusted, the fact that the application is untrusted shall be at least visually indicated to the user, if the MExE device is capable of visual indication, whenever user permission is sought. Other means of indication are additionally permitted. If the MExE device is not capable of visual indication, or is not designed for use by a human user, other means of indication shall be used.

The user shall be prompted for user permission relating to all action groups listed in the table 6 "Security domains and actions" that are required by the MExE executable. If a prompt for permission relates to more than one action, e.g. networking and user data, then it shall list the individual action group permissions which will be granted, though the action group permissions can all be granted with a single user action. This condition applies to any prompts relating to user permissions in table8 "User Permissions".

…

8.4.4 Certificate Chain Verification

This clause presents the procedure of validation of any downloaded MExE executable. It checks for the presence of the signature used to sign the application as well as the presence and integrity of all the certificates needed to successfully verify the signature. As a result, the application under scrutiny is deemed trusted or untrusted, i.e. will be allowed execution in one of the secure domains or in untrusted area, or otherwise the application will not be allowed to be executed and will be deleted. In any outcome of the verification, the user is notified about the result. The user also may wish to see certificate details if the application is allowed to be executed on the MExE device.

The MExE device shall follow "certificate verification" procedure as described below. The procedure shall contain at least the following logical phases (not necessarily in the order stated below):

Signature and Certificate Verification Supported: Checks whether signature and certificate verification procedure is supported on the MExE ME.

Executable with Signature and End Entity Certificate (note): Checks whether the executable contains a signature together with the corresponding end entity certificate.

Valid Application Signature (note): This phase comprises the following checks:

- Check if the signature and the end entity certificate formats are supported by the device. If this check fails, the application is classified as untrusted.
- Check if the signature algorithm is supported/known by the device. If this check fails, the application is classified as untrusted.
- Check if the signature can be cryptographically verified by using the accompanying end entity certificate . If this check fails, the application is not allowed execution and is deleted.

Complete set of Intermediate Certificates Available (note): Checks if all the necessary intermediate certificates (certificates between the RPK and the end entity certificate) are available.

Valid RPK on (U)SIM/ME: Checks if a valid RPK (not expired) exists on the (U)SIM or on the ME that could verify a certificate chain originating from the end entity certificate accompanying the application.

NOTE: These steps could include validation (e.g. expiration, revocation, etc.) checking by means of e.g. OCSP, SCVP, CRL-Consultation, and etc. The use of certificate revocation checking is recommended but is not mandated or defined in this specification.

Certificate Chain Cryptographically Verified: Checks if all the certificates from the end entity certificate to the RPK can be verified cryptographically. Certificate verification shall be performed according to the functional requirements given in clause "Basic Path Validation" of RFC 2459 [43] excluding revocation checking.

Secure Domains Supported: Checks whether MExE ME supports secure domains.

Only if all the above checks are successful, the downloaded application is deemed trusted and is allowed to be executed in the designated trusted domain (operator, manufacturer, trusted third party). Otherwise, the application is either untrusted (execution in the untrusted area only is allowed) or deleted (execution is not allowed at all) as per the figure 6A and as explained above. The executable shall only be designated into one of the trusted domains, and it shall be possible to verify the certificate chain ~~unambiguoslyunambiguously~~ to one and only one root public key.

The MExE ME shall allow for a "user notification" procedure as described below.

...

8.5.1.1 Caching of root public keys

The ME shall behave as if it reads the operator root public key from the secure area every time the ME needs the key to verify a signature. Examples of the secure area include an area on a (U)SIM or a secure, persistent area on the ME.

If the ME uses a mechanism for caching public keys, it shall do so in a way that maintains the integrity of the secure area and is consistent with the keys stored in the secure area. With the exception of improved performance, the operation of the device using cached public keys must be indistinguishable from that of a device that reads the key from the secure area every time it uses the key for verification.

No cached version of a key may ~~may~~ exist beyond the expiration or termination of the key in the secure area. For example, if the ME caches a root public key held on the (U)SIM, the ME shall purge the cache when the (U)SIM application is stopped (or the SIM card is withdrawn).

...

8.6.1.1 X.509 version 3

The MExE certificate format as specified in section 8.4.1.1 shall support the X.509 version 3 access-Restriction extension.

X509 version 3 provides a mechanism to define extensions. An Object identifier (OID) is defined for each private extension as defined in X509 [26]. The extension is defined to be within the ETSI Object Identifier (OID) name space.

This extension shall apply irrespective of the presence or otherwise of any other X.509 key usage or extended key usage field.

Normal use of the "critical" flag for extensions apply. That is, if this extension is marked as critical in the certificate used to verify the signature on the application or in any certificate in the chain used to verify the signature and this extension cannot be processed in the MExE ~~devicethen~~device then the certificate shall be considered invalid.

The syntax of the extension is defined in annex C “Access restriction certificate extension”.

...

8.11 MExE executable integrity

If the 3 MExE security domains defined in clause 8.1 "Generic security" are not supported, then the pre-verification of MExE executables at launch time described in this clause is optional.

A potential threat is that MExE executables may be securely authenticated at the time of download, but tampered with or corrupted prior to being launched. Further a certificate may be compromised or expired. Authentication of a MExE executable at the time of download does not ensure that the MExE executable has not been modified when it is subsequently launched. Furthermore, authentication of a MExE executable at the time of launch does not ensure that the MExE executable is not modified during execution. Similarly, verification of the certificate at the time of download may not ensure that the certificate is valid at time of application launch, and verification of the certificate at the time of launch does not ensure that the certificate remains valid during execution.

Therefore, the MExE device shall ensure application integrity immediately prior to application execution.

Application integrity is defined as the state in which:-

- application code has not been modified since authentication; and
- the certificate containing the root public key is checked and known to be valid.

The mechanism by which the device preserves integrity is an implementation detail, dependant on the application storage mechanism and access. Examples of mechanisms that contribute to such application integrity could include :

- Storage of applications in a ~~non-compromisable~~ memory area that cannot be compromised on the device;
- Preventing launch of the application when the MExE device becomes aware that the certificate is invalidated;
- Full signature verification prior to each application invocation (see clause 8.11.1);
- Optimised pre-launch signature verification (see clause 8.11.2);
- Periodic full signature verification by separate process during application execution.

The list of examples is not exhaustive and any other mechanisms ensuring application integrity may be equally considered.

…

Annex E (informative): MExE conformance requirements

The table of Conformance Requirements define the minimum set of features that a conformant MExE device must implement.

Legend:-

M - Mandatory feature/requirement

O - Optional feature

N/A - Feature is not applicable: the MExE specification does not prevent this feature from being implemented~~ing a feature;~~, however, support of this~~e~~ feature is not required for a MExE device to be regarded as being compliant with a specific MExE Classmark device.~~, and t~~Therefore the specification does not indicate whether the feature is optional~~ity~~ or mandatory ~~of the feature is not indicated in the specification~~.

M/O – Support as such is required. Mandatory and Optional features are gathered into a table

ID	Requirement	Reference	CM1	CM2	CM3
4-1	Support of at least one MExE classmark on a MExE device	4	M	M	M
4-2	Support of multiple combinations of MExE classmarks	4.4	O	O	O
4-3	Support of WAP	4.2.5	M	O	O
4-4	If Classmark 1 services are supported by non-Classmark 1 devices, Classmark 1 services shall execute in the same manner as they execute in a MExE Classmark 1 device	4.4.1	N/A	M	M
4-5	Support of PersonalJava	4.2, 6.1	O	M	O
4-6	If Classmark 2 services are supported by non-Classmark 2 devices, Classmark 2 services shall execute in the same manner as they execute in a MExE Classmark 2 device.	4.4.2	M	N/A	M

ID	Requirement	Reference	CM1	CM2	CM3
4-7	Support of CLDC and MIDP	4.3, 6.2	O	O	M
4-8	If Classmark 3 services are supported by non-Classmark 3 devices, Classmark 3 services shall execute in the same manner as they execute in a MExE Classmark 3 device.	4.4.3	M	M	N/A
4-9	Support of capability negotiation process	4.6	M	M	M
4-10	Support for interaction between the MExE device and the MSE by the use of HTTP/1.1or HTTP/1.1 derived protocol (e.g. WSP)	4.6	M	M	M
4-11	Support of the properties in the UAProf schema for capability negotiation	4.6.1	M/O	M/O	M/O
4-12	Support of content negotiation	4.6	O	O	O
4-13	Support of user profiles	4.7	O	O	O
4-14	Support of more than one user profile (if user profiles supported)	4.7.1	O	O	O
4-15	Ability to retain the user profile in the network (if user profiles supported)	4.7.1	O	O	O
4-16	User permission for retaining the user profile in the network (if user profiles supported)	4.7.1	M	M	M
4-17	Support of direct and indirect referencing mechanisms in retrieval of MExE preferences (if user profiles supported)	4.7.3	O	O	O
4-18	Support of the properties in the UAProf schema for user preference information (if user profiles supported)	4.7.3	M	M	M
4-19	Support of user interface personalisation	4.8	O	O	O
4-20	Support of direct and indirect referencing mechanisms in retrieval of user interface personalisation preferences	4.8.1	O	O	O
4-21	Ability to support VHE	4.7.4	O	O	O
4-22	Storage of the VHE characteristics as a part of the user profile (if VHE and user profile is supported)	4.7.4	M	M	M
4-23	Capability to discover new services	4.9.1	M	M	M
4-24	Support for a browser for service discovery	4.9.1	O	O	O
4-25	Ability to control service installation and configuration	4.9.3	N/A	M	M
4-26	Ability to determine which services are transferred to, resident, configured or executing on the MExE device (provide the name and, if available, version number)	4.9.4	M	M	M
4-27	Service termination capability	4.9.5	M	M	M
4-28	Capability to delete a service	4.9.6	M	M	M
4-29	User's ability to terminate or suspend any active connection associated with any MExE executable	4.10	M	M	M
4-30	User's ability to obtain information on all connections associated with any MExE executable on the MExE device	4.10	M	M	M
4-31	Support of ~~journalling~~journaling of network events by MExE executables	4.11	M	M	M
4-32	Management of the journal by the MExE device, with no access to it by MExE executables	4.11	M	M	M
4-33	Indicate whenever network activity is in progress	4.12	O	O	O
4-34	Support of QoS management by MExE	4.13, 9	O	O	O
4-35	Support of core software download functionality	4.14	O	O	O
4-36	Core software download (if supported) only under control of the MExE device manufacturer	4.14	M	M	M
5-1	Call control using WTA scripts	5.3	M	O	O
6-1	Support of the Wireless Profile of the JavaPhone API specification (Optional~~ity~~ Java packages of Wireless Profile of the JavaPhone APIs as presented in ~~t~~Table 4 "Optional~~ity~~ Java packages of the Wireless Profile of the JavaPhone APIs")	6.1.2.1, 6.1.2.3	O	M/O	O
6-2	Support of the JAR file manifest entries as per JavaPhone specification	6.1.2.3.1	O	M	O
6-3	The use of icons to launch applications	6.1.2.3.1	O	O	O
6-4	If icons are used as elements to launch the application, then the icon file within the JAR file named by the Main-Icon attribute shall be displayed	6.1.2.3.1	O	M	O
6-5	Implementation of "BatteryCritical", "BatteryNormal" event generation	6.1.2.3.2	O	M	O
6-6	Support for the following formats in Datagram recipient addressing: raw text-only GSM SMS message, UDP datagram via IP, and WAP datagram via GSM SMS message(s)	6.1.2.3.3	O	M	O
6-7	Support any other Java APIs which comply with the MExE security requirements in Table 6 "Security domains and actions"	6.1.2.4	O	O	O

ID	Requirement	Reference	CM1	CM2	CM3
6-8	Support for network protocols as per table 5 "Support for network protocols"	6.1.2.5.1	O	M/O	O
6-9	Support of MIDlet discovery and management via a browser using MIME type text/vnd.sun.j2me.app-descriptor	6.2.3	O	O	O
6-10	Indication of MIDlets and MIDlet suites to the user (with a tag or icon and tag)	6.2.3	O	O	O
7-1	Support of charging regimes of MExE services (charging mechanisms are outside the scope of MExE specification).	7.1	O	O	O
8-1	Support of the untrusted area	8.1	M	M	M
8-2	Support of all three security domains together (i.e. operator, manufacturer and third party), or no security domains at all	8.1	M	M	M
8-3	Security restrictions shall apply to MExE executables when API functionality is directly or indirectly called by MExE executables	8.2	M	M	M
8-4	Support for permissions of operator, manufacturer and third party security domains in the order of restriction (as defined in table 6 of MExE specification).	8.2.1	M	M	M
8-5	Access by MExE untrusted executables limited to the functionality specified in the table 7 of MExE specification	8.2.2	M	M	M
8-6	Separation of the user interface input and output streams between different MExE executables (except for the MIDlets in the same MIDlet suite)	8.2.3	M	M	M
8-7	Support of single action permission with a prompt for the user	8.3	M	M	M
8-8	Support of session permission and blanket permission with a prompt for the user	8.3	O	O	O
8-9	Indication to the user whenever user permission is sought by an untrusted MExE executable	8.3	M	M	M
8-10	Ability of the user to request to be informed of the "subject" field of the certificate of the signer (if secure domains supported)	8.3	M	M	M
8-11	Support for public key based solution of content authentication (if secure domains supported)	8.4	M	M	M
8-12	Support of certificate chains (if secure domains supported)	8.4	M	M	M
8-13	Support at least one level of certificate under operator, manufacturer or Third Party root public keys (if secure domains supported)	8.4	M	M	M
8-14	Secure installation of root public keys in the MExE device (if secure domains supported)	8.4.1	M	M	M
8-15	Prohibition to share public keys between domains (if secure domains supported)	8.4.1	M	M	M
8-16	Support the use and management of an operator root public key on the (U)SIM (if secure domains supported)	8.5.1	M	M	M
8-17	Prohibition of the user to add or delete any type of operator public keys (if secure domains supported)	8.5.1	M	M	M
8-18	Support of operator and manufacturer disaster recovery root public keys (if secure domains supported)	8.5.	O	O	O
8-19	Support of the use and management of the operator root public key (if secure domains supported)	8.5.1.	M	M	M
8-20	Support of the use and management of the manufacturer root public key (if secure domains supported)	8.5.2	M	M	M
8-21	Support of the use and management of the third party root public keys (if secure domains supported)	8.5.3	M	M	M
8-22	Support of the use and management of the administrator root public key (if secure domains supported)	8.5.4	M	M	M
8-23	Support of the administrator designation mechanism (if secure domains supported)	8.5.4	M	M	M
8-24	Support of the certificate configuration management (if secure domains supported)	8.6	M	M	M
8-25	Use of the CCM by MExE device to determine the third party certificates that are trusted for the use on the MExE device (if secure domains supported)	8.7	M	M	M
8-26	Additional support of other means to enable/disable root certificates (if secure domains supported)	8.7	O	O	O
8-27	Support of authorised CCM download mechanisms (if secure domains supported)	8.7.	M	M	M
8-28	When the administrator is changed, then the CCM shall also be changed. (if secure domains supported)	8.7.	M	M	M
8-29	Support of provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device (if secure	8.8	M	M	M

ID	Requirement	Reference	CM1	CM2	CM3
	domains supported)				
8-30	Support of the cases: the user is the owner, the user is at remote location, the owner of the MExE-(U)SIM wants to be a temporary administrator (if secure domains supported)	8.8	M	M	M
8-31	Support for determining the administrator of the MExE device (if secure domains supported)	8.8.1	M	M	M
8-32	Either sandbox or fine grain Java security shall be supported	8.9.1	N/A	M	N/A
8-33	Support for trusted applets (if secure domains supported)	8.9.1	N/A	O	O
8-34	Verification of the certification of the application or applet (if secure domains supported)	8.9.1.2	M	M	M
8-35	Java loading native libraries that are intrinsically part of the MExE device implementation, and MExE native libraries	8.9.1.3	O	O	O
8-36	No loading of other native libraries	8.9.1.3	N/A	M	N/A
8-37	Support of the JAR file format devices for securely packaging objects that are to be downloaded and installed on the MExE device	8.10	N/A	M	M
8-38	Support for other proprietary means of downloading and installing objects	8.10	O	O	O
8-39	Support of MExE native library signed package installation	8.10.1	N/A	O	O
8-40	Support for the case when a certificate containing an Administrator root public key is thus contained in a signed package, the signed package (JAR) shall contain two files: the Administrator root public key and the CCM (if secure domains supported).	8.10.2	N/A	M	M
8-41	Support of installation of other signed data (e.g. proprietary binaries or Java classes such as native DSP code, provisioned functionality upgrades and patches) (if secure domains supported).	8.10.3	O	O	O
8-42	Support for administrator root certificate mechanism (if secure domains supported).	8.10.4	M	M	M
8-43	Support of alternative methods to download an administrator root certificate (if secure domains supported).	8.10.4	O	O	O
8-44	Support of optimised signature verification of applications (if secure domains supported).	8.11	O	O	O
9-1	Support of QoS API by MExE device	9	O	O	O
9-2	Support of a basic QoS operations	9.1	O	O	O
9-3	Support of MExE QoS API by MExE QoS Manager	9.2	O	O	O
9-4	Provision of the MExE QoS Manager functions	9.2	O	O	O
9-5	Ability to manage QoS through the MExE device's MMI	9.2	O	O	O
9-6	QoS control by MExE QoS Manager, if it is not provided in the network control	9.3	O	O	O
9-7	Provision of a standard set of parameters by a QoS API to MExE executable	9.4	O	O	O
9-8	Ability of MExE QoS Manager to deal independently with each of the several simultaneous QoS streams	9.6	O	O	O

Annex F (informative): Change history

TSG	T-Tdoc	T2-Tdoc	CR	Rev	Rel	Subject	Cat	Version-Current	Version-New
T#7	TP-000024	T2-000047	001		R99	Corrections to WAP chapters	F	3.0.0	3.1.0
T#7	TP-000024	T2-000049	002		R99	QoS	F	3.0.0	3.1.0
						Editorial change by MCC		3.1.0	3.1.1
T#8	TP-000073	T2-000307	003		R99	Addition of phonebook entry and addition/modification of user data update for untrusted applications	F	3.1.1	3.2.0
T#8	TP-000073	T2-000298	004		R99	Editorial clarifications	F	3.1.1	3.2.0
T#8	TP-000073	T2-000304	005		R99	ME actions on SIM insertion and/or power up	F	3.1.1	3.2.0
T#8	TP-000073	T2-000295	006		R99	Client/Server 'negotiation'	F	3.1.1	3.2.0
T#8	TP-000073	T2-000296	007		R99	Third Party Root Public Key	F	3.1.1	3.2.0
T#8	TP-000073	T2-000291	008		R99	Third Party root public keys management	F	3.1.1	3.2.0
T#8	TP-000073	T2-000300	009		R99	User permission types (visual indication)	F	3.1.1	3.2.0
T#9	TP-000143	T2-000401	010		R99	Storage of user private data in the user profile in the network	F	3.2.0	3.3.0
T#9	TP-000143	T2-000504	011		R99	UAProf tags	F	3.2.0	3.3.0
T#9	TP-000143	T2-000523	012		R99	WAP UAProf URL correction	F	3.2.0	3.3.0
T#10	TP-000193	T2-000631	013		Rel4	Support of blanket user permission	C	3.3.0	4.0.0
T#10	TP-000193	T2-000632	014		Rel4	Update of WAP version MExE release 4 refers to	C	3.3.0	4.0.0
T#10	TP-000193	T2-000633	015		Rel4	Application version number	C	3.3.0	4.0.0
T#10	TP-000193	T2-000634	016		Rel4	Capability negotiation for browsing	C	3.3.0	4.0.0
T#10	TP-000193	T2-000637	017		Rel4	Addition of the definitions of MExE API and MExE server	C	3.3.0	4.0.0
T#10	TP-000193	T2-000639	018		Rel4	Generic MExE Classmark 1 aspects	D	3.3.0	4.0.0
T#10	TP-000193	T2-000640	019		Rel4	Core software download support	C	3.3.0	4.0.0
T#10	TP-000193	T2-000641	020		Rel4	Application connection information	C	3.3.0	4.0.0
T#10	TP-000193	T2-000642	021		Rel4	Support of ~~journalling~~journaling	C	3.3.0	4.0.0
T#10	TP-000193	T2-000643	022		Rel4	Support of the user profile	C	3.3.0	4.0.0
T#10	TP-000193	T2-000644	023		Rel4	Capability Negotiation	F	3.3.0	4.0.0
T#10	TP-000193	T2-000796	024		Rel4	Datagram recipient addressing	C	3.3.0	4.0.0
T#10	TP-000193	T2-000646	025		Rel4	QoS support in MExE devices	C	3.3.0	4.0.0
T#10	TP-000193	T2-000647	026		Rel4	Core software download	B	3.3.0	4.0.0
T#10	TP-000193	T2-000648	027		Rel4	RDF and XML References	C	3.3.0	4.0.0
T#10	TP-000193	T2-000649	028		Rel4	Support of VHE	C	3.3.0	4.0.0
T#10	TP-000193	T2-000794	029		Rel4	High level architecture	C	3.3.0	4.0.0
T#10	TP-000193	T2-000666	030		Rel4	Personal Java Reference	C	3.3.0	4.0.0
T#10	TP-000193	T2-000740	031		Rel4	Deletion of unnecessary text	C	3.3.0	4.0.0
T#10	TP-000193	T2-000744	032		Rel4	User Profile CC/PP tags	C	3.3.0	4.0.0
T#10	TP-000193	T2-000745	033		Rel4	Service management	C	3.3.0	4.0.0
T#10	TP-000193	T2-000746	034		Rel4	Classmark 3 non-security and conformance	B	3.3.0	4.0.0
T#10	TP-000193	T2-000747	035		Rel4	Classmark 3 security and conformance	B	3.3.0	4.0.0
T#10	TP-000193	T2-000748	036		Rel4	Update of HTTP RFC Reference	C	3.3.0	4.0.0
T#10	TP-000193	T2-000752	037		Rel4	Table of UAProf tags	C	3.3.0	4.0.0
T#10	TP-000193	T2-000753	038		Rel4	Added Annex about MExE Executable Life Cycle	C	3.3.0	4.0.0
T#10	TP-000193	T2-000754	039		Rel4	Update to security section for Rel4	C	3.3.0	4.0.0
T#10	TP-000193	T2-000755	040		Rel4	Conformance Table	B	3.3.0	4.0.0

TSG	T-Tdoc	T2-Tdoc	CR	Rev	Rel	Subject	Cat	Version-Current	Version-New
T#11	TP-010027	T2-010044	042		Rel4	TS11.11 reference updates	D	4.0.0	4.1.0
T#11	TP-010027	T2-010050	043		Rel4	Abbreviations	D	4.0.0	4.1.0
T#11	TP-010027	T2-010051	044		Rel4	CCPP web site in reference	D	4.0.0	4.1.0
T#11	TP-010027	T2-010053	045		Rel4	Capability and Content editorials	D	4.0.0	4.1.0
T#11	TP-010027	T2-010056	046		Rel4	High level architecture editorial	D	4.0.0	4.1.0
T#11	TP-010027	T2-010057	047		Rel4	Java application signature verification editorials	D	4.0.0	4.1.0
T#11	TP-010027	T2-010059	048		Rel4	QoS editorials	D	4.0.0	4.1.0
T#11	TP-010027	T2-010060	049		Rel4	RFC references correction	D	4.0.0	4.1.0
T#11	TP-010027	T2-010061	050		Rel4	Root public keys correction	D	4.0.0	4.1.0
T#11	TP-010027	T2-010062	051		Rel4	Support of user profile editorials	D	4.0.0	4.1.0
T#11	TP-010027	T2-010063	052		Rel4	Transfer of capability negotiation editorials	D	4.0.0	4.1.0
T#11	TP-010027	T2-010065	053		Rel4	User control of application connection editorials	D	4.0.0	4.1.0
T#11	TP-010027	T2-010066	054		Rel4	User profile editorials	D	4.0.0	4.1.0
T#11	TP-010027	T2-010067	055		Rel4	X.509 version 3 editorials	D	4.0.0	4.1.0
T#11	TP-010027	T2-010075	056		Rel4	WAP reference correction	D	4.0.0	4.1.0
T#11	TP-010027	T2-010076	057		Rel4	WAP compliance	C	4.0.0	4.1.0
T#11	TP-010027	T2-010083	058		Rel4	Conformance requirements table update	D	4.0.0	4.1.0
T#11	TP-010027	T2-010084	059		Rel4	Correction to the definition of MIDP application	D	4.0.0	4.1.0
T#11	TP-010027	T2-010088	060		Rel4	Abbreviations	D	4.0.0	4.1.0
T#11	TP-010027	T2-010172	061		Rel4	Trust hierarchy figure correction	D	4.0.0	4.1.0
T#11	TP-010027	T2-010176	062		Rel4	Definition of the Untrusted Area	D	4.0.0	4.1.0
T#11	TP-010027	T2-010203	063		Rel4	Generic security editorials	D	4.0.0	4.1.0
T#11	TP-010027	T2-010204	064		Rel4	CCM update with new administrator signed package	F	4.0.0	4.1.0
T#11	TP-010027	T2-010206	065		Rel4	Executable pre-launch signature verification	F	4.0.0	4.1.0
T#11	TP-010027	T2-010231	066	1	Rel4	Clarification of ORPK and ARPK support on MExE MT	F	4.0.0	4.1.0
T#11	TP-010027	T2-010209	067		Rel4	Untrusted executable permission to access the network	D	4.0.0	4.1.0
T#11	TP-010027	T2-010210	068		Rel4	Capability negotiation updates	C	4.0.0	4.1.0
T#11	TP-010027	T2-010211	069		Rel4	Correction to capability negotiation methods	C	4.0.0	4.1.0
T#11	TP-010027	T2-010212	070		Rel4	WAP WTA	C	4.0.0	4.1.0
T#11	TP-010027	T2-010213	071		Rel4	Update of Some of the 3GPP Document References	D	4.0.0	4.1.0
T#11	TP-010027	T2-010214	072		Rel4	Annex A corrections	D	4.0.0	4.1.0
T#11	TP-010027	T2-010215	073		Rel4	Miscellaneous editorial corrections	D	4.0.0	4.1.0
T#11	TP-010027	T2-010216	074		Rel4	Definition of an Operator	D	4.0.0	4.1.0
T#11	TP-010027	T2-010217	075		Rel4	Mobile Execution Environment	F	4.0.0	4.1.0
T#11	TP-010027	T2-010218	076		Rel4	Capability negotiation editorials	D	4.0.0	4.1.0
T#11	TP-010027	T2-010225	077		Rel4	Sharing of Transmissions between untrusted executables	D	4.0.0	4.1.0
T#11	TP-010027	T2-010226	078		Rel4	Core software download	D	4.0.0	4.1.0
T#12	TP-010126	T2-010381	079		Rel4	Manufacturer RPK	F	4.1.0	4.2.0
T#12	TP-010126	T2-010382	080		Rel4	Correction of SIM insert/remove terminology	F	4.1.0	4.2.0
T#12	TP-010126	T2-010384	081		Rel4	Administrator mechanism	F	4.1.0	4.2.0
T#12	TP-010126	T2-010386	082		Rel4	Clarification of note 10 in table 6	F	4.1.0	4.2.0
T#12	TP-010126	T2-010390	083		Rel4	MExE Device Administrator	F	4.1.0	4.2.0
T#12	TP-010126	T2-010395	084		Rel4	Quality of Service Support	F	4.1.0	4.2.0

TSG	T-Tdoc	T2-Tdoc	CR	Rev	Rel	Subject	Cat	Version-Current	Version-New
T#12	TP-010126	T2-010397	085		Rel4	Administrator Determination Mechanism	F	4.1.0	4.2.0
T#12	TP-010126	T2-010406	087		Rel4	Executable integrity	F	4.1.0	4.2.0
T#12	TP-010126	T2-010554	088		Rel4	Clarifications on call control and signed packages	F	4.1.0	4.2.0
T#12	TP-010126	T2-010555	089		Rel4	More Abbreviations	F	4.1.0	4.2.0
T#12	TP-010126	T2-010556	090		Rel4	CC/PP Working Group Web Page	F	4.1.0	4.2.0
T#12	TP-010126	T2-010557	091		Rel4	Using WBXML when transporting CC/PP over WSP	F	4.1.0	4.2.0
T#12	TP-010126	T2-010408	093		Rel4	Certificate Chain Verification Diagram	F	4.1.0	4.2.0
T#13	TP-010192	T2-010691	086	1	Rel4	Status of applications when valid RPK not available	F	4.2.0	4.3.0
T#13	TP-010192	T2-010681	092	1	Rel4	Clarification of root public keys	F	4.2.0	4.3.0
T#13	TP-010192	T2-010855	093		Rel4	Update to the states in diagram D4	F	4.2.0	4.3.0
T#13	TP-010192	T2-010672	094		Rel4	Clarifying Description of CCM Format	F	4.2.0	4.3.0
T#13	TP-010192	T2-010683	095		Rel4	Trust Hierarchy and Administrator RPK	F	4.2.0	4.3.0
T#13	TP-010192	T2-010684	096		Rel4	Implementations with Non-persistent Caching of RPKs	F	4.2.0	4.3.0
T#13	TP-010192	T2-010689	097		Rel4	A specified certificate format for MExE	F	4.2.0	4.3.0
T#13						Editorial modification		4.3.0	4.3.1

3GPP TSG-T2 #14
Cancún, Mexico
26-30 November 2001

T2-010959

CR-Form-v4

CHANGE REQUEST

⌘ **23.057** **CR** **100** ⌘ ev **-** ⌘ Current version: **4.3.1** ⌘

*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:	⌘	Addition reference to 23.227
Source:	⌘	T2
Work item code:	⌘	MEXE-ENHANC
Date:	⌘	27 Nov 2001
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:	⌘	In order to cover all the requirements on Aplication and User Interactions, a reference is needed to the TS 23.227.
Summary of change:	⌘	Reference added
Consequences if not approved:	⌘	All the requirements on Application and User Interactions stated in 23.227 will not be covered.

Clauses affected:	⌘	2, 4.9, 4.10
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://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.

2 References

- 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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[2] 3GPP TS 22.057: "Mobile Execution Environment (MExE); Stage 1".

[3] Personal Java 1.1.1 or higher, Sun Microsystems

[4] JavaPhone API version 1.0, http://java.sun.com/products/javaphone/.

[5] JTAPI 1.2, Sun Microsystems http://www.java.sun.com.

[6] Wireless Application Protocol (WAP) June 2000 Conformance Release http://www.wapforum.org.

[7] vCard – The Electronic Business Card Exchange Format – Version 2.1, The Internet Mail Consortium (IMC), September 1996, http://www.imc.org/pdi/vcard-21.doc.

[8] vCalendar – The Electronic Calendaring and Scheduling Exchange Format – Version 1.0, The Internet Mail Consortium (IMC), September 1996, http://www.imc.org/pdi/

[9] Hypertext Transfer Protocol – HTTP/1.1, IETF document RFC2616, http://www.w3.org/Protocols/rfc2616/rfc2616

[10] Java Mail API version 1.0.2, http://www.java.sun.com

[11] 3GPP TR 22.170: "Universal Mobile Telecommunications System (UMTS); Service aspects; Provision of Services in UMTS - The Virtual Home Environment".

[12] 3GPP TS 22.121: "The Virtual Home Environment; Stage 1".

[13] ISO 639: "Code for the representation of names of languages".

[14] 3GPP TS 22.101: "Service Aspects; Service Principles".

[15] CC/PP Exchange Protocol based on HTTP Extension Framework; W3C

[16] Composite Capability/Preference Profiles (CC/PP):A user side framework for content negotiation;

[17] UAProf Specification http://www.wapforum.org/what/technical.htm

[18] JDK 1.1 security

[19] Java 2 security

[20] Java security tutorial http://java.sun.com/docs/books/tutorial/security1.2/overview/index.html

[21] OCF 1.1.: "Smartcard API specified by OpenCard Consortium http://www.opencard.org

[22] RFC 1738: "Uniform Resource Locators (URL)" http://www.w3.org/pub/WWW/Addressing/rfc1738.txt.

[23] The MD5 Message Digest Algorithm", Rivest, R., RFC 1321, April 1992. URL:

[24] ISO/IEC 10118-3 (1996): "Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions".

[25] IETF RFC 2368: "The mailto URL scheme".

[26] ITU-T Recommendation X.509: "Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks".

[27] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) interface".

[28] 3GPP TS 23.107: "QoS Concept and Architecture".

[29] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General Aspects".

[30] 3GPP TS 24.008: "Mobile radio interface layer 3 specification, Core Network Protocols; Stage 3".

[31] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2".

[32] PKCS #15 "Cryptographic Token Information Standard" version 1.0, RSA Laboratories, April 1999
URL: ftp://ftp.rsa.com/pub/pkcs/pkcs-15/pkcs15v1.doc

[33] RFC 2510 (1999): "Internet X.509 Public Key Infrastructure Certificate Management Protocols".

[34] Connected Limited Device configuration, J2ME version 1.0,
http://java.sun.com/aboutJava/communityprocess/final/jsr030/index.html

[35] Mobile Information Device Profile, J2ME version 1.0,
http://java.sun.com/aboutJava/communityprocess/final/jsr037/index.html

[36] eXtensible Markup Language (XML) 1.0, W3C Recommendation.
URL:

[37] Resource Definition Framework (RDF) Model and Syntax, W3C Recommendation.
URL:

[38] UML Partners: Unified Modelling Language. URL: http://www.omg.org.

[39] 3GPP TS 31.102: "Characteristics of the USIM applications".

[40] RFC 2396 (1998): "Uniform Resource Identifiers (URI): Generic Syntax". T. Berners-Lee, R. Fielding, L. Masinter.

[41] RFC 2616 (1999): "Hypertext Transfer Protocol -- HTTP/1.1". R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee.

[42] Description of the "JAR Manifest" file encoding, Sun Microsystems. URL:

[43] RFC 2459 (1999): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile".
R. Housley, W. Ford, W. Polk, D. Solo.

[44] 3GPP TR 21.905: Vocabulary for 3GPP Specifications.

[45] WAP Binary XML Content Format Specification (WBXML),

[46] RFC 1766: "Tags for the Identification of Languages".

[47] WAP Certificate and CRL Profiles, WAP-211-WAPCert
http://www.wapforum.org/what/technical.html

[48] 3GPP TS 23.227 “3rd Generation Partnership Project; Technical Specification Group Terminals; Applications and User interaction in the UE-Principles and specific requirements”.

4.9 Provisioning and management of services

fSupport of management of services as detailed in this clause is mandatory.

The MExE device shall be capable of supporting services in a standard (WAP or Java) execution environment independently of the MExE device manufacturer. Service provisioning provides a standardised method for a MExE device to discover and install services. It includes download and installation of the service's client application. Once discovered and delivered, services are managed by the user, under the principles stated in 3GPP TS 23.227 [48]. Management of services provides the user with the capability to:

- control the transfer of services;
- install and configure services;
- control the execution of services;
- terminate or suspend executing services;
- delete services;

on his MExE device.

4.10 User control of application connections

Support of the user control of application connections is mandatory. and shall follow the principles and requirements stated in 3GPP TS 23.227 [48]

This clause addresses the generic aspects of connection control supported by both WAP and Java classmark MExE devices.

In order to allow the user to maintain control over connections on his MExE device and the ability to initiate connections, the user shall be able to terminate or suspend any active connection associated with an application in the MExE environment of the MExE device. The user shall be able to obtain information about all connections associated with applications on the MExE device (e.g. requesting information, being informed by the MExE device etc.). Behaviour of the application following termination or suspension of its connection is undefined.

The specific support of connection control by WAP classmark MExE devices is identified in subsequent clause 5.3 Call control, the security aspects of connection control are identified in clause 8 "Security", and the user control of connection authorisation is identified in clause 4.7 "User profile".

3GPP TSG-T2 #15
Cancun, Mexico
26-30 November 2001

T2-011131

CR-Form-v5

CHANGE REQUEST

⌘ **23.057** **CR** **101** ⌘ **rev** **-** ⌘ Current version: **4.3.1** ⌘

*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:	⌘	Certificate chain level inconsistency
Source:	⌘	T2
Work item code:	⌘	MEXE-ENHANC
Date:	⌘	16 November 2001
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:	⌘	As the MExE group mandated X509 certificates profiled in the "WAP Certificate and CRL Profile", there are now conflicting information, regarding certificate chain depths. The reference to the WAP specification mandates three layers, while the MExE specification itself mandates only two layers.
Summary of change:	⌘	The change makes clear, that it is the mandated requirements stated in the MExE specification, which are to be followed.
Consequences if not approved:	⌘	Contradicting requirements in the MExE spec and the referred WAP spec ("WAP Certificate and CRL Profile"), making it impossible for the implementer to know the minimum requirements.

Clauses affected:	⌘	8.4.1.1
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://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.

8.4.1 Certification requirements

A MExE device cannot verify certified MExE executables of a particular domain unless it has a root public key for that particular domain.

Root public keys shall be securely installed in the MExE device, say, at the time of manufacture.

It is recommended that a "disaster recovery" root public key be securely installed on the MExE device, to be used to install new root public keys when all other root public keys on the MExE device are invalid.

Third Party Domain root public keys will typically be installed along with and integrated into the MExE device browser, as is done for PC-based browsers.

A MExE executable can only be verified if the MExE device contains a valid root or certified public keys corresponding to the private key used to sign the MExE executable.

A MExE device shall support at least one level of certificate under operator, manufacturer or Third Party root public keys. The MExE device shall support at least one level of certificate chain analysis in a signed content package, as shown in figure 6 "Trust hierarchy".

A certificate (other than one containing a root public key) shall only be considered valid if the signature on the certificate is verified by a valid public key (root or contained in a certificate) already present on the MExE device and if the certificate being verified has not expired.

Public keys shall not be shared between domains.

8.4.1.1 MExE terminal requirements for certificate processing

A MExE device shall support the processing of X509 certificates profiled in the “WAP Certificate and CRL Profile” [47] together with additional requirements defined in the MExE specification, see section 8.6.1.1 “X509 version 3”. The certificate chain depth is still mandated to be one level only, as mentioned in clause 8.4.1 “Certificate requirements” and indicated in figure 6 "Trust hierarchy".

MExE devices may also support the processing of other certificate formats.

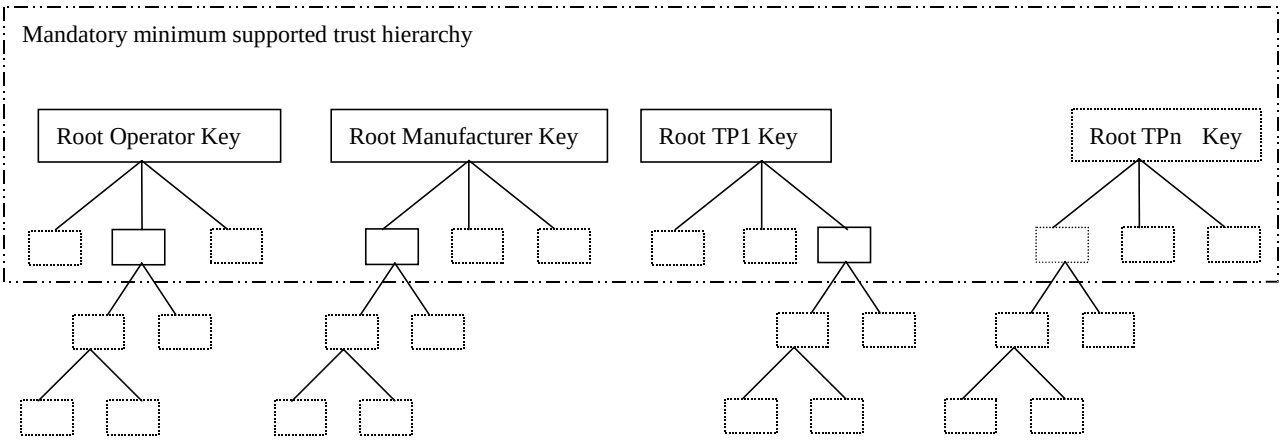


Figure 6: Trust hierarchy

The boxes below the root keys represent individual public key certificates. The solid boxes represent the minimum MExE, and the dotted boxes represent possible further support for public key certificates (either at the first or subsequent levels).

3GPP TSG-T2 #15
Cancun, Mexico
26-30 November 2001

T2-011132

CR-Form-v5

CHANGE REQUEST

⌘ **23.057** **CR** **102** ⌘ **rev** **-** ⌘ Current version: **4.3.1** ⌘

*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:	⌘	Signature algorithm specification
Source:	⌘	T2
Work item code:	⌘	MEXE-ENHANC
Date:	⌘	16 November 2001
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:	⌘	The MExE group has mandated X509 certificates profiled in the "WAP Certificate and CRL Profile". The WAP specification does not mandate a signature algorithm, but leaves it open to choose between two algorithms.
Summary of change:	⌘	The signature algorithm SHA1WithRSA (which is one of the two mentioned in the WAP spec.) is mandated for MExE devices.
Consequences if not approved:	⌘	Applications signed with one algorithm, would not be able to run on MExE devices, that does not support that algorithm, but the other algorithm instead. Application writers would have no chance of knowing, which algorithm would make their application survive in the market and reach most MExE devices.

Clauses affected:	⌘	8.4.1.1
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://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.

2 References

- 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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[2] 3GPP TS 22.057: "Mobile Execution Environment (MExE); Stage 1".

…

[46] RFC 1766: "Tags for the Identification of Languages".

[47] WAP Certificate and CRL Profiles, WAP-211-WAPCert http://www.wapforum.org/what/technical.html

[XX] PKCS#1 “RSA Cryptographic Standard” " version 2.0, RSA Laboratories, October 1998

URL: http://www.rsalabs.com/pkcs/pkcs-1/index.html

8.4.1.1 MExE terminal requirements for certificate processing

A MExE device shall support the processing of X509 certificates profiled in the “WAP Certificate and CRL Profile” [47] together with additional requirements defined in the MExE specification, see section 8.6.1.1 “X509 version 3”.

A MExE device shall support the SHA1WithRSA signature algorithm. The object identifier value can be found in [XX]. A MExE device may also support other signature algorithms.

MExE devices may also support the processing of other certificate formats.

3GPP TSG-T2 #15
Cancun, Mexico
26-30 November 2001

T2-011133

CR-Form-v4

CHANGE REQUEST

⌘ **23.057** **CR** **103** ⌘ rev **-** ⌘ Current version: **4.3.1** ⌘

*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 **X** Radio Access Network ☐ Core Network ☐

Title:	⌘	Marking MRPK/ARPK Invalid through Secure Mechanism
Source:	⌘	T2
Work item code:	⌘	MEXE-ENHANC
Date:	⌘	28-November-2001
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:	⌘	In one sentence, the manufacturer can use a secure mechanism to mark a new MRPK/ARPK as valid, only when all other MRPKs/ARPKs are marked as invalid. There is no explicit definition for having an MRPK/ARPK marked as invalid. Therefore, it appears to be impossible for marking a new MRPK/ARPK when there is another MRPK/ARPK on the device that is marked valid at a previous point.
Summary of change:	⌘	Since there does not appear to be a specified method for marking MRPKs/ARPKs as invalid, this Change Request makes an explicit notation that the secure mechanism can mark a MRPK/ARPK as valid or invalid.
Consequences if not approved:	⌘	Since the current statements do not have explicit means for marking MRPKs/ARPKs invalid, implementations of the specification may yield a system that results in a deadlock with upgrading MRPKs/ARPKs.

Clauses affected:	⌘	8.5.2, 8.5.4
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://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.

8.5.2 Manufacturer root public key

The ME shall support secure storage for a certificate containing a manufacturer root public key. The certificate contains a root public key generated by the manufacturer of the MExE device, or by a CA trusted by the manufacturer of the MExE device.

If the ME does not contain a valid manufacturer root public key, then the certificate chain to MExE executable previously executing in the Manufacturer Domain will be invalid, and the MExE executables will be excluded from the manufacturer domain and marked as untrusted.

The user shall not be able to add or delete any type of manufacturer public key (root or contained in a certificate).

The Manufacturer shall put a root public key and optionally its corresponding disaster-recovery key in the ME at the time of manufacture, and use a proprietary secure mechanism (e.g. using the disaster-recovery key) to replace the certificate containing the manufacturer root public key. It shall not be possible to use the disaster recovery manufacturer root public key to replace the standard manufacturer root public key unless both public keys are from the same manufacturer.

An application signed by a manufacturer shall not be able to run in the Manufacturer Domain unless the root public key of that manufacturer is installed in the ME and is marked as trusted.

The manufacturer, and only the manufacturer, may use a secure mechanism to mark as valid/invalid a ~~new~~ certificate containing the manufacturer root public key on the ME. It shall only be possible to use this mechanism to mark a certificate containing a new manufacturer root public key on the ME as valid, when all manufacturer root public keys are marked as invalid.

There shall be no more than one valid manufacturer root public key on the ME at any one time. Any other manufacturer root public key(s) on the ME device shall be marked invalid when a different manufacturer root public key is marked as valid on the ME.

8.5.4 Administrator root public key

To help with the control of Third-Party certificates, the ME shall support secure storage for a certificate containing an administrator root public key. The ME shall support the use and management of a certificate containing an Administrator root public key stored on the MExE-(U)SIM and in the ME. The ME shall behave according to clause 8.8.1 “Determining the administrator of the MExE MS”. For support of public key management on the SIM and the USIM refer to GSM 11.11 [27] and 3GPP TS 31.102 [39] respectively.

A secure mechanism may be used to mark as valid/invalid a ~~new~~ certificate containing the administrator root public key on the MExE device. It shall only be possible to use this mechanism to mark a certificate containing a new administrator root public key on the ME as valid, when all administrator root public keys are marked as invalid.

There shall be no more than one valid administrator root public key on the MExE device at any one time. A valid administrator root public key on the (U)SIM shall always have precedence over any administrator root public key on the ME. Any administrator root public key(s) on the ME shall be marked invalid when a valid administrator root public key is present on the (U)SIM.

The MExE device shall support the administrator designation mechanism explained in clause 8.8 "Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device" and the secure downloading of CCMs explained in clause 8.7.4 “Authorised CCM download mechanisms”.

The user shall not be able to delete an administrator root public key or certificate.

The system shall support a mechanism (as part of a provisioned functionality and/or inherently part of the MExE implementation) allowing the owner of the MExE device to manage the administrator root public key (including the download of a new administrator root public key) as defined in clause 8.8.1.1 "Administrator of the MExE device is the user". This mechanism shall be secure so that only the owner can use this functionality.

The administrator root public key can be downloaded to the MExE device as described in clause 8.10.4 "Administrator root certificate download mechanism".

If the Administrator root public key is stored in the (U)SIM, the ME shall only read the Administrator root public key from the MExE-(U)SIM when required and shall not store the Administrator root public key from the MExE-(U)SIM on the ME in a manner inconsistent with that detailed in subclause 8.5.1.1.

See clause 8.6 "Certificate management" for the management of Administrator root public keys.

The same root public key may be used for both the Administrator role and the operator or manufacturer domain. This facility does not imply any increased right of the manufacturer or operator to take the Administrator role.

If the same root public key is used for the operator domain and Administrator role and this root public key is stored on the MExE-(U)SIM (see [27] and [39]), there shall be separate entries relating to each use of the root public key in the operator and administrator trusted certificate directory files. These entries in the operator and Administrator trusted certificate directory files may point to the same root public key in the certificate data file.

If the root public key to be shared is not stored on the (U)SIM, then procedures relating to this are out of the scope of this specification.

3GPP TSG-T2 #15
Cancun, Mexico
26-30 November 2001

T2-011135

CR-Form-v4

CHANGE REQUEST

⌘ **23.057** **CR** **104** ⌘ rev **-** ⌘ Current version: **4.3.1** ⌘

*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 **X** Radio Access Network ☐ Core Network ☐

Title:	⌘	Context of MCC+MNC Missing
Source:	⌘	T2
Work item code:	⌘	MEXE-ENHANC
Date:	⌘	28-November-2001
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:	⌘	The current specification makes a reference to the MCC+MNC being 6 digits for DCS1900, but 5 digits elsewhere. The discussion on the MCC+MNC does not appear anywhere in the diagram of the section with this statement, and there is no other discussion of the MCC+MNC in the specification. Section 8.5.1.2 also states that this issue is outside the scope of the specification. There is also a vague statement of "The identity of the root public key has to be defined", but there are no relevant details on defining the ID. This information is confusing and needs to be clarified. This is an important note on defining the Operator ID on the (U)SIM and root public key.
Summary of change:	⌘	The discussion following Figure 7 is revised to clarify the point that definitions of the Operator ID on the (U)SIM and the ORPK of the ME are left for implementation agreements.
Consequences if not approved:	⌘	Without these clarifications, implementers will miss the critical point of establishing implementation agreements that are essential for operational capabilities of the Operator Domain.

Clauses affected:	⌘	8.5.1.2
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://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.

8.5.1.2 MExE device actions on detection of valid (U)SIM application and/or power up

This clause defines the sequence of actions on identification by the MExE ME that a valid SIM card, or USIM application on the UICC, has been detected (e.g. through insertion of (U)SIM card, power up of MExE device etc.). More specifically, these actions relate to the enabling or disabling of the operator domain and the status of the operator applications on the ME.

The requirements in this clause ensure that the operator domain on the ME belongs to the same operator as the operator that issued the valid (U)SIM application (if detected) in the MExE device and, if there is an operator root public key (ORPK) on the MExE-(U)SIM, that trusted operator applications on the MExE device were verified using that ORPK.

The ME shall support the use and management of an Operator root public key (ORPK) on the MExE-(U)SIM.

On power up the MExE device shall behave as dictated by figure 7 "Terminal behaviour on power up" below.

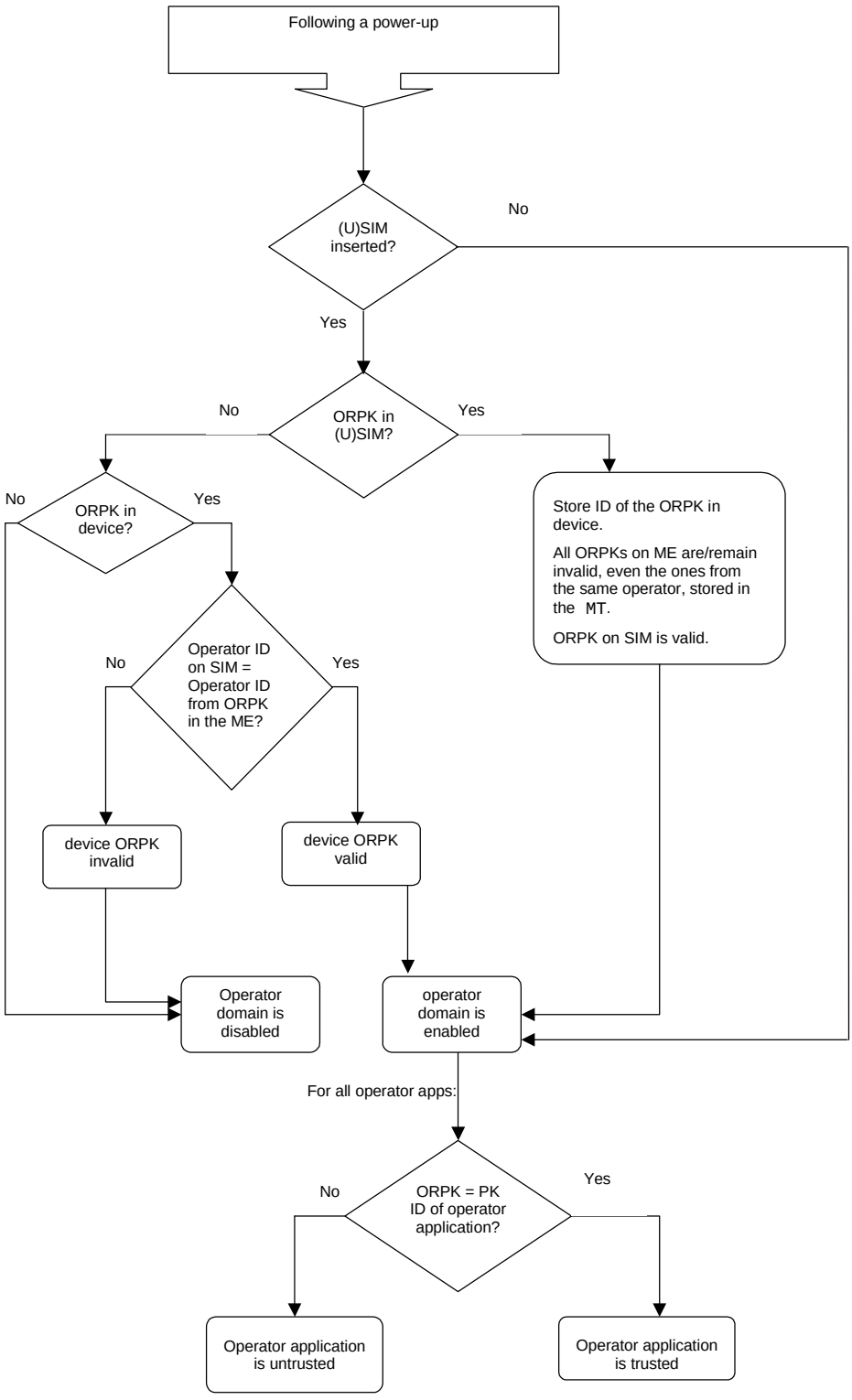


Figure 7: MExE device behaviour on power up

Note that the procedure in Figure 7 checks for a match between the Operator ID on the (U)SIM and the Operator ID from the ORPK in the ME. Currently, one mechanism for defining the Operator ID on the (U)SIM is through use of the MCC+MNC. As an additional note, on DCS1900, the MCC+MNC is 6 digits, but elsewhere it is 5 digits. The MExE device needs to know how many digits to use., ~~H~~however, this is outside the scope of this specification. ~~The identity of the root public key has to be defined.~~The implementations of MExE devices need to establish agreements on using the

MCC+MNC as the Operator ID on the (U)SIM. Likewise, the implementations of MExE devices need to establish agreements on ~~what defines~~how to define the Operator ID ~~from the~~belonging to the ORPK.

The ME shall only read the ORPK from the MExE-(U)SIM when required and shall not store a ORPK from the MExE-(U)SIM on the ME in a manner inconsistent with that detailed in subclause 8.5.1.1. .

When an operator root public key stored on the ME is marked as invalid, all operator applications verified using that root public key or by certificates verified by a chain that terminates with that root public key, shall cease operation as soon as possible and shall be marked as untrusted.

Removal of the (U)SIM shall not cause the status (i.e. valid or invalid) of any operator root public key on the MExE device to change.

3GPP TSG-T2 #15
Cancun, Mexico
26-30 November 2001

T2-011136

CR-Form-v5

CHANGE REQUEST

⌘ **23.057** **CR** **105** ⌘ **rev** **-** ⌘ Current version: **4.3.1** ⌘

*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:	⌘	Removing References to Sun Microsystems
Source:	⌘	T2
Work item code:	⌘	MEXE-ENHANC
Date:	⌘	11/29/01
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:	⌘	This CR requests edits to remove the requirements for Sun approval for classmark compliance.
Summary of change:	⌘	Section 6.1.1, 6.1.2, 6.2.1 edits removes the requirement to obtain approval from Sun for classmark compliance.
Consequences if not approved:	⌘	Independent implementations of classmarks 2 and 3 are not allowed without first approval from Sun Microsystems.
Clauses affected:	⌘	2, 6.1.1, 6.1.2, 6.2.1
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://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.

6.1.1 High level architecture

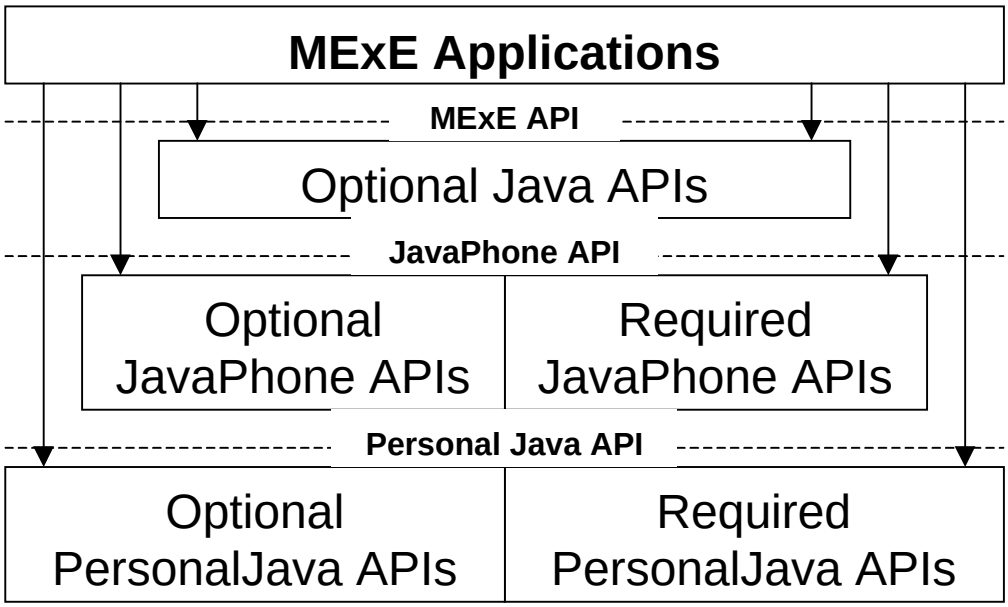


Figure 4: Basic functional architecture of a PersonalJava MExE device

The functional architecture of a Java MExE classmark 2 device is shown in figure 4 "Basic functional architecture of a PersonalJava MExE device". Java applets, applications, and services access functionality via the MExE PersonalJava API. The MExE PersonalJava API is based on a combination of optional Java APIs ~~approved by Sun Microsystems~~ and the Wireless Profile of the JavaPhone API [4] ~~as defined by the JavaPhone Expert Group~~. The JavaPhone API is based on the PersonalJava API [3] ~~defined by Sun Microsystems~~.

6.1.2 High level functions

6.1.2.1 Optionality

The use of Java encourages development of modular interfaces and minimal required functionality. Additional functionality is provided by optional APIs specified in terms of the Java language. In general, optionality is specified in terms of Java packages. Packages are containers for the highest level of functionality in the Java language. In some cases, optionality is specified in terms of Java classes and interfaces. Classes and interfaces are elements contained inside packages.

The following table 4 "Optionality of the Wireless Profile of the JavaPhone APIs" specifies the ~~Sun Microsystems~~ defined optionality of the Wireless Profile of the JavaPhone APIs[4]. Within some of the packages, certain classes and methods may be individually specified as optional by the JavaPhone API specification.

6.2.1 High level architecture

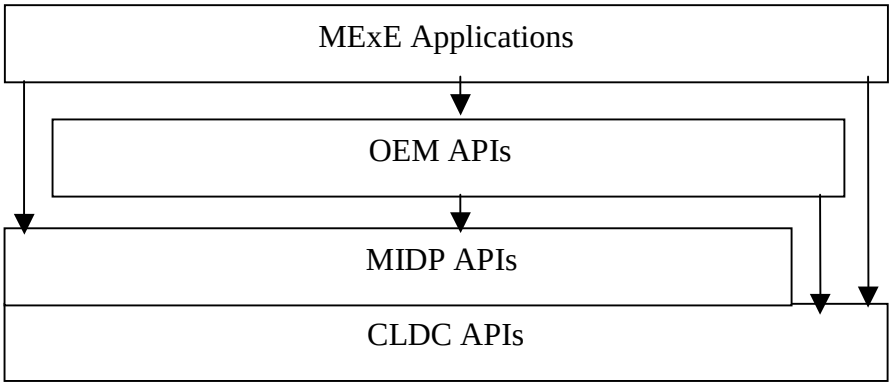


Figure 5: Functional architecture of a Classmark 3 MExE device

The functional architecture of a Classmark 3 MExE device is shown in figure 5 "Functional architecture of a Classmark 3 MExE device". The MExE API is based on the combination of CLDC APIs and MIDP APIs. OEM specific APIs are outside the scope of MExE specification. CLDC and MIDP APIs are defined in J2ME ~~specified by Sun Microsystems~~ [34] and [35].

3GPP TSG-T2 #15
Cancun, Mexico
26-30 November 2001

T2-011245

CR-Form-v5

CHANGE REQUEST

⌘ **23.057** **CR** **106** ⌘ **rev** **-** ⌘ Current version: **4.3.1** ⌘

*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:	⌘	Correction of PKCS #15 reference and editorial changes
Source:	⌘	T2
Work item code:	⌘	MEXE-ENHANC
Date:	⌘	18 November 2001
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:	⌘	To allign the references in 23.057 to look alike and to reference the latest version of PKCS#15
Summary of change:	⌘	Added titles and changed section to clkause and removed “sub” in the word subclause and changed the reference, the URL and the chapters where the reference is mentioned
Consequences if not approved:	⌘	The specification might lead to misinterpretations.

Clauses affected:	⌘	Chapter 2, 4, 8 and annexes
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://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.

2 References

- 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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms".

[2] 3GPP TS 22.057: "Mobile Execution Environment (MExE); Stage 1".

[3] Personal Java 1.1.1 or higher, Sun Microsystems

[4] JavaPhone API version 1.0, http://java.sun.com/products/javaphone/.

[5] JTAPI 1.2, Sun Microsystems http://www.java.sun.com.

[6] Wireless Application Protocol (WAP) June 2000 Conformance Release http://www.wapforum.org.

[7] vCard – The Electronic Business Card Exchange Format – Version 2.1, The Internet Mail Consortium (IMC), September 1996, http://www.imc.org/pdi/vcard-21.doc.

[8] vCalendar – The Electronic Calendaring and Scheduling Exchange Format – Version 1.0, The Internet Mail Consortium (IMC), September 1996, http://www.imc.org/pdi/

[9] Hypertext Transfer Protocol – HTTP/1.1, IETF document RFC2616, http://www.w3.org/Protocols/rfc2616/rfc2616

[10] Java Mail API version 1.0.2, http://www.java.sun.com

[11] 3GPP TR 22.170: "Universal Mobile Telecommunications System (UMTS); Service aspects; Provision of Services in UMTS - The Virtual Home Environment".

[12] 3GPP TS 22.121: "The Virtual Home Environment; Stage 1".

[13] ISO 639: "Code for the representation of names of languages".

[14] 3GPP TS 22.101: "Service Aspects; Service Principles".

[15] CC/PP Exchange Protocol based on HTTP Extension Framework; W3C

[16] Composite Capability/Preference Profiles (CC/PP):A user side framework for content negotiation;

[17] UAProf Specification http://www.wapforum.org/what/technical.htm

[18] JDK 1.1 security

[19] Java 2 security

[20] Java security tutorial http://java.sun.com/docs/books/tutorial/security1.2/overview/index.html

[21] OCF 1.1.: "Smartcard API specified by OpenCard Consortium http://www.opencard.org

[22] RFC 1738: "Uniform Resource Locators (URL)" http://www.w3.org/pub/WWW/Addressing/rfc1738.txt.

[23] The MD5 Message Digest Algorithm", Rivest, R., RFC 1321, April 1992. URL:

[24] ISO/IEC 10118-3 (1996): "Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions".

[25] IETF RFC 2368: "The mailto URL scheme".

[26] ITU-T Recommendation X.509: "Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks".

[27] GSM 11.11: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) interface".

[28] 3GPP TS 23.107: "QoS Concept and Architecture".

[29] 3GPP TS 24.007: "Mobile radio interface signalling layer 3; General Aspects".

[30] 3GPP TS 24.008: "Mobile radio interface layer 3 specification, Core Network Protocols; Stage 3".

[31] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service Description; Stage 2".

[32] PKCS #15 "Cryptographic Token Information Syntax Standard" version 1.1~~0~~, RSA Laboratories, June~~April 1999~~2000.
URL: ftp://ftp.rsa.com/pub/pkcs/pkcs-15/pkcs-15v1_1.doc~~ftp://ftp.rsa.com/pub/pkcs/pkcs-15/pkcs15v1.doc~~

4 Generic MExE aspects

Support of at least one MExE classmark is mandatory. A MExE device may also include optional support for applications from any other MExE classmark (refer to clause 4.4 "Multiple Classmark support").

This clause defines the common aspects of all MExE compliant devices, independent of MExE technology.

...

4.7.1 Location of, access to, and security of, the user profile

As multiple user profiles may be defined, the user is able to set up or receive calls/connections associated with different user profiles simultaneously by securely activating a user profile (with each user profile being associated with at least one unique identifier). Refer to table 6 "Security domains and actions" in the Security clause 8.2 "MExE executable permissions" for further details on user profile activation.

The user's characterisation of the MExE device in the user profile may be modified at any time by the user and the service provider, and changes affected at the earliest possible opportunity.

The security clause shall apply to all user profiles at all times, whether activated or not

The user profile shall be securely managed by the MExE device, and stored in a secure area of the MExE device (either (U)SIM or ME). The service provider may also retain the user profile in the network for service optimisation. User private data in the user profile may also be stored in the network, however only with the user permission.

The support of more than one user profile is not mandatory.

...

4.10 User control of application connections

Support of the user control of application connections is mandatory.

This clause addresses the generic aspects of connection control supported by both WAP and Java classmark MExE devices.

In order to allow the user to maintain control over connections on his MExE device and the ability to initiate connections, the user shall be able to terminate or suspend any active connection associated with an application in the MExE environment of the MExE device. The user shall be able to obtain information about all connections associated with applications on the MExE device (e.g. requesting information, being informed by the MExE device etc.). Behaviour of the application following termination or suspension of its connection is undefined.

The specific support of connection control by WAP classmark MExE devices is identified in subsequent clause 5.3 "Call control", the security aspects of connection control are identified in clause 8 "Security", and the user control of connection authorisation is identified in clause 4.7 "User profile".

...

4.13 Quality of service

Support of Quality of Service is optional.

Quality of Service (QoS) [28] is seen by the end user as a measure of the amount of network resources given to an application by the underlying network. The network may employ a number of QoS mechanisms, but the end user / MExE executable is not involved in these. The end user / MExE executable requires an interface into the network QoS through a visible set of standard parameters.

A QoS aware MExE executable may request a QoS from the network at the beginning of a QoS session. Changes in the level of QoS provided shall be notified to the end user / MExE executable. An end user may request a change in the QoS through the MExE device MMI. A MExE executable may have several QoS streams open simultaneously.

When the MExE execution environment supports QoS, the MExE executable shall be able to dynamically request a change in the level of QoS at connection setup request or subsequently during the connection. The end user / MExE executable may receive a rejection to a QoS modification request, upon which the end user / MExE executable must be notified.

The end user's service level QoS subscription parameters are stored in the network, they identify the maximum permissible QoS that a user may negotiate with the network. Several QoS subscriptions may be possible for one user. MExE is neither aware nor able to determine or modify the end user's service level QoS subscriptions.

Clause 9 "Quality of Service" defines the necessary functions for a MExE device to accomodate QoS management and provisioning. QoS management may be available directly to the MExE executables themselves, or to the MExE environment.

...

8.2.1 MExE executable permissions for operator, manufacturer and third party security domains

The following table 6 "Security domains and actions" specifies the permissions of operator, manufacturer and third party security domains in the order of restriction.

The actions listed in the security table 6 "Security domains and actions" are generic actions. These actions can only be performed by MExE executables via application programming interfaces (APIs) (which are intrinsically part of the MExE implementation) The security restrictions shall apply to MExE executables whether the API functionality is called directly or indirectly by the MExE executable. Explicit user permission is required for all actions by MExE executables in all domains. Types of user permission are defined in clause 8.3 "User permission types".

Untrusted MExE executables are not permitted access to any actions which access the phone functionality (phone functionality includes all the actions in table 6 "Security domains and actions") except for the exceptions identified in clause 8.2.2 "MExE executable permissions for untrusted MExE executables".

Actions available using interfaces giving access to the phone functionality (either in existence at the time of approval of this specification or not) that are not listed in the security table 6 "Security domains and actions" shall be categorised into one of the groups in the security table 6 "Security domains and actions" by comparing its action against the groups in order as they are listed in the table 6 "Security domains and actions". If an action can be categorised into a more restrictive group near the top of the table, then it shall not be again categorised into another, less restrictive, group further down in the table. E.g if a new action eventually results in forwarding a call, it shall be categorised into Network

access. If the action is totally new, it shall be categorised into some of the groups by comparing its functionality to the group description below and by comparing with the list of actions listed in the table within the group.

1. Device core function access includes functions, which are an essential part of the phone functionality .
2. Support of core software download, which allows updating the ME radio, characteristics and properties by changing the core software in the ME (e.g. a new CODEC may be loaded into a ME, a new air interface, etc.)
3. (U)SIM smart card low level access includes functions, which allow communications at the transport service access point (send and receive application protocol data unit).
4. Network security access includes all functionalities which relate to CHV, CHV2, UNBLOCK CHV and UNBLOCK CHV2 (verification, management, reading or modifying), GSM authentication, GSM ciphering.
5. Network property access includes functions, which enable the management of operator-related data parameters and network settings.
6. Network services access includes all functionalities which result in or need interaction via the operator´s network.
7. User private data access includes all functionalities which relate to management, reading or modifying of data that the user has stored in the MExE device including user preferences.
8. MExE security functions access includes all functionalities which, through an API relate to certificate handling in the MExE device; end to end encryption, signed content, hashing, access to public, private, secret keys stored in the MExE device or in a smart card.
9. Application access includes the functionalities which relate to launch provisioned functionality, MExE executables, external executables ((U)SIM tool kit application,…) usage.
10. Lifecycle management includes the functionalities which are needed for installing or removing MExE executables in the MExE device.
11. Terminal data access includes the functions which relate to accessing terminal data, i.e. not user data.
12. Peripheral access includes the functionalities related to peripherals other than user interface peripherals usage through a high level software application interface.
13. Input output user interface access includes the functionalities related to the user interface and user notification means usage.

Table 6: Security domains and actions

	MExE Security Domains		
Actions	**Operator**	**Manufacturer**	**Third Party**
Device core function access Start/stop radio Turn on/off device Write time and/or date Activate a user profile Modify a user profile	No		
Support of Core Software Download e.g. Update ME software	No	Yes	No
(U)SIM smart card low level access[11] Send APDU Slot management (power on/off, reset, port lock…)	No		
[11] – Access to (U)SIM is provided using more high level API as phonebook, application launching			
Network Security access Run algorithm Verify CHV/2 or UNBLOCK CHV/2 Activate/deactivate CHV Modify CHV/2	No		
Network property access Get IMSI Get home network Select network	Yes	No	
Network services access Initiate a voice/data connection [3] Accept a voice/data connection [3] Call forward [4] Multiparty call [4] Call deflection [4] Explicit call transfer [4] Terminate an existing connection Hold an existing connection Resume an existing connection Send point-point message (e.g. SMS, USSD) [4] Query network status Get signal level Get call list QoS management	Yes		Yes [6]
[3] – A network connection may be via any supported bearer service [4] – Multiparty, deflection, and explicit call transfer shall be permitted only to numbers explicitly supplied by the user to the MExE Executable. Modification of call forward numbers stored in the network shall only be permitted to numbers explicitly supplied by the user to the operator. [6] – The Third Party domain's permission to access the networking action depends on the provisioning mechanism as described in ~~sub~~clause 8.8.1 "Determining the administrator of the MExE device"			
User private data access [1] Read Write Get properties Delete Get Location Information Read stored SMS Delete stored SMS Modify user preferences	Yes[2] Yes[2] Yes[2] Yes[2] Yes[2] Yes[2] Yes[2] Yes[7]		
[1] – User private data includes user files, phonebook, etc located on the MExE device. [2] – The user shall be able to specify data access permissions within the capabilities of the MExE device. It is not applied to user preferences [7] – Trusted applications only have permission to modify user preferences, and not to activate or de-activate them. The user shall be able to specify for each domain, the preferences that applications in that domain can access. All other preferences shall not be accessible to that domain. The default shall be that there is no access. Single action user permission is the only type of user permission that shall be possible for changes to User Preferences.			

Actions	MExE Security Domains		
	Operator	**Manufacturer**	**Third Party**
MExE security functions access			
Install a certificate for a given domain	Yes [5]		
Uninstall a certificate for a given domain			
Replace a certificate for a given domain	Yes [5]		
Data encryption API			
Verify a signature API	Yes [5]		
Compute a digital signature API			
Hash a content API	Yes		
Non repudiation API	Yes		
	Yes		
	Yes		
	Yes		
[5] – Only the organisation whose public key is certified (or the organisation that certified the public key) can add, delete or replace a particular certificate.			
Application access			
Get application list	Yes[8]		
Launch an application	Yes[8]		
Get application status	Yes[8]		
Stop, suspend, resume an application	Yes[9]		
[8] – ME provisioned functionality access is limited to manufacturer domain. (U)SIM tool kit application access is limited to operator domain. MExE executable access is limited to MExE executable issued by the same issuer (identify by the certificate) of launched MExE executable [9] – Access is limited to MExE executable which launch the application. But the end user, shall have a way to stop the launched application, MExE environment may stop the launched application or launched application may stop itself.			
Lifecycle management	Yes		
Install a MExE Executable			
Uninstall a MExE executable			
Terminal data access			
Get manufacturer software version	Yes		
Read time and date	Yes		
Peripheral access	Yes		
Sound generation to speaker (e.g. via stream)			
Set speaker volume			
printer access			
Monitor the power state			
Change the power state			
Activate/ access Serial port (RS232, IrDA, Bluetooth, USB …) access			
Activate/access Parallel port			
Activate/access Smart card other than (U)SIM card (Send APDU, Slot management)			
Input output User interface access			
Input device (keyboard, mouse …)	Yes[10]		
Output device (display)	Yes[10]		
Output notification device(smart icon, sound, light, vibrator …)	Yes		
[10] – Access request requires no user permission.			

...

8.4.1.1 MExE terminal requirements for certificate processing

A MExE device shall support the processing of X509 certificates profiled in the "WAP Certificate and CRL Profile" [47] together with additional requirements defined in the MExE specification, see ~~section~~ clause 8.6.1.1 "X509 version 3".

MExE devices may also support the processing of other certificate formats.

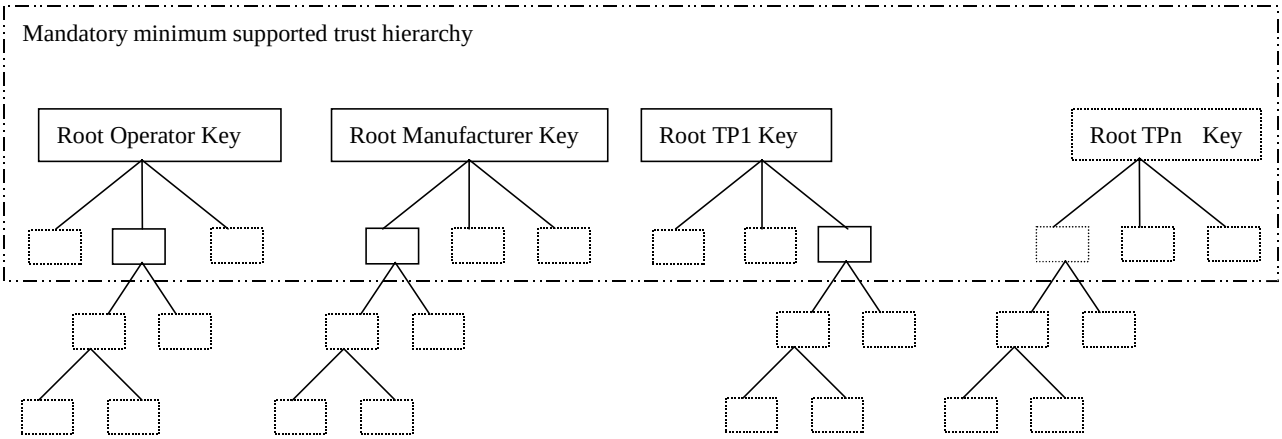


Figure 6: Trust hierarchy

The boxes below the root keys represent individual public key certificates. The solid boxes represent the minimum MExE, and the dotted boxes represent possible further support for public key certificates (either at the first or subsequent levels).

8.4.2 Certification administration requirements

For control of third party certificates, the MExE device supports storage of a certificate containing an administrator root public key as detailed in ~~sub~~clause 8.5.4 “Administrator root public key”.

This certificate is managed separately from the hierarchy of Figure 6 “Trust Hierarchy” discussed in ~~sub~~clause 8.4.1 “Certification requirements”. The administrator root public key in this certificate is primarily used for designating an administrator of the third party certificates. Note, the administrator root public key does not implicitly define a security domain, and is used in complement with the root public keys of the operator, manufacturer, and third party domains.

The relationship of the administrator certificate (and root public key) to the management of third party certificates is detailed in part of ~~sub~~clause 8.6 “Certificate management”.

The relationship of the administrator certificate to the mechanism for determining if a third party certificate is trusted is detailed in part of ~~sub~~clause 8.7 “Certificate configuration message (CCM)”.

Mechanisms for designating an administrator are detailed in ~~sub~~clause 8.8 “Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device”.

...

8.4.4 Certificate Chain Verification

This clause presents the procedure of validation of any downloaded MExE executable. It checks for the presence of the signature used to sign the application as well as the presence and integrity of all the certificates needed to successfully verify the signature. As a result, the application under scrutiny is deemed trusted or untrusted, i.e. will be allowed execution in one of the secure domains or in untrusted area, or otherwise the application will not be allowed to be executed and will be deleted. In any outcome of the verification, the user is notified about the result. The user also may wish to see certificate details if the application is allowed to be executed on the MExE device.

The MExE device shall follow "certificate verification" procedure as described below. The procedure shall contain at least the following logical phases (not necessarily in the order stated below):

Signature and Certificate Verification Supported: Checks whether signature and certificate verification procedure is supported on the MExE ME.

Executable with Signature and End Entity Certificate (note): Checks whether the executable contains a signature together with the corresponding end entity certificate.

Valid Application Signature (note): This phase comprises the following checks:

- Check if the signature and the end entity certificate formats are supported by the device. If this check fails, the application is classified as untrusted.
- Check if the signature algorithm is supported/known by the device. If this check fails, the application is classified as untrusted.
- Check if the signature can be cryptographically verified by using the accompanying end entity certificate . If this check fails, the application is not allowed execution and is deleted.

Complete set of Intermediate Certificates Available (note): Checks if all the necessary intermediate certificates (certificates between the RPK and the end entity certificate) are available.

Valid RPK on (U)SIM/ME: Checks if a valid RPK (not expired) exists on the (U)SIM or on the ME that could verify a certificate chain originating from the end entity certificate accompanying the application.

NOTE: These steps could include validation (e.g. expiration, revocation, etc.) checking by means of e.g. OCSP, SCVP, CRL-Consultation, and etc. The use of certificate revocation checking is recommended but is not mandated or defined in this specification.

Certificate Chain Cryptographically Verified: Checks if all the certificates from the end entity certificate to the RPK can be verified cryptographically. Certificate verification shall be performed according to the functional requirements given in clause 6.1 "Basic Path Validation" of RFC 2459 [43] excluding revocation checking.

Secure Domains Supported: Checks whether MExE ME supports secure domains.

Only if all the above checks are successful, the downloaded application is deemed trusted and is allowed to be executed in the designated trusted domain (operator, manufacturer, trusted third party). Otherwise, the application is either untrusted (execution in the untrusted area only is allowed) or deleted (execution is not allowed at all) as per the figure 6A and as explained above. The executable shall only be designated into one of the trusted domains, and it shall be possible to verify the certificate chain unambiguously to one and only one root public key.

...

8.5 Root Public keys

If the 3 MExE security domains defined in clause 8.1 "Generic security" are not supported, then the root public key management described in this clause is optional.

The definition of the secure mechanism in this ~~sub~~clause to mark as valid a root public key certificate on the ME, is out of the scope of this specification.

...

8.5.1.2 MExE device actions on detection of valid (U)SIM application and/or power up

This clause defines the sequence of actions on identification by the MExE ME that a valid SIM card, or USIM application on the UICC, has been detected (e.g. through insertion of (U)SIM card, power up of MExE device etc.). More specifically, these actions relate to the enabling or disabling of the operator domain and the status of the operator applications on the ME.

The requirements in this clause ensure that the operator domain on the ME belongs to the same operator as the operator that issued the valid (U)SIM application (if detected) in the MExE device and, if there is an operator root public key (ORPK) on the MExE-(U)SIM, that trusted operator applications on the MExE device were verified using that ORPK.

The ME shall support the use and management of an Operator root public key (ORPK) on the MExE-(U)SIM.

On power up the MExE device shall behave as dictated by figure 7 "Terminal behaviour on power up" below.

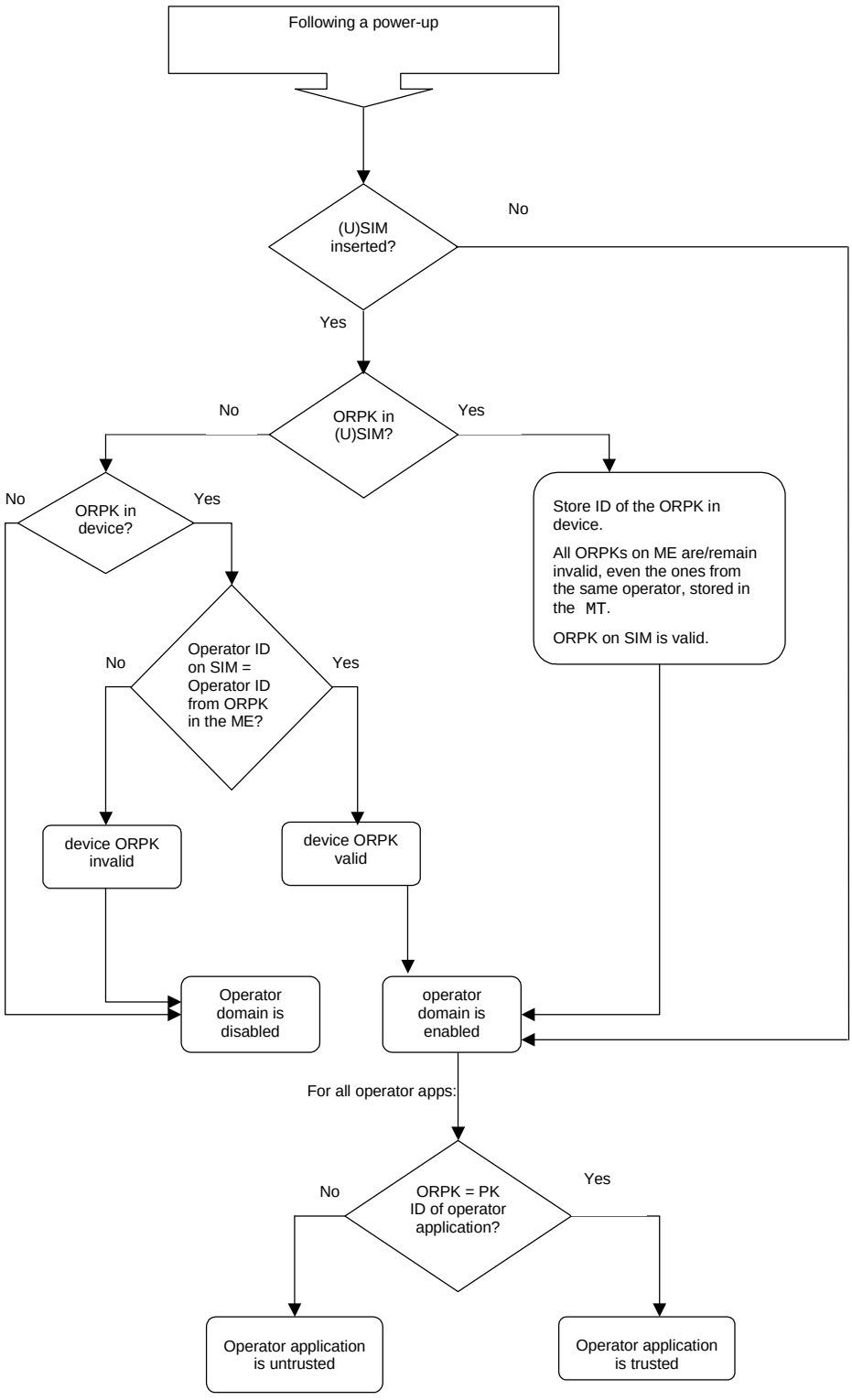


Figure 7: MExE device behaviour on power up

Note that on DCS1900 the MCC+MNC is 6 digits, but elsewhere it is 5 digits. The MExE device needs to know how many digits to use, however this is outside the scope of this specification. The identity of the root public key has to be defined.

The ME shall only read the ORPK from the MExE-(U)SIM when required and shall not store a ORPK from the MExE-(U)SIM on the ME in a manner inconsistent with that detailed in ~~sub~~clause 8.5.1.1~~.~~ "Caching of root public keys".

When an operator root public key stored on the ME is marked as invalid, all operator applications verified using that root public key or by certificates verified by a chain that terminates with that root public key, shall cease operation as soon as possible and shall be marked as untrusted.

Removal of the (U)SIM shall not cause the status (i.e. valid or invalid) of any operator root public key on the MExE device to change.

...

8.5.3 Third party root public key

The ME shall support secure storage for at least one certificate containing a third party root public key. The ME shall support the use and management of certificates containing Third Party root public keys stored on the MExE-(U)SIM and in ME. For support of public key management on the SIM and the USIM refer to GSM 11.11 [27] and 3GPP TS 31.102 [39] respectively. The MExE device may contain root public key (s) generated by CA(s) implicitly trusted by the user. The user will be able to securely install (using a secure transport) or remove Third Party root public keys at any time using a system administrative tool.

The Manufacturer, Operator and Administrator may at their discretion, securely install certificates containing Third Party root public key(s) on behalf of the user, e.g. at the time of manufacture by the Manufacturer. See clause 8.6 "Certificate management" for details of Administrator control of Third Party certificate download.

If a Third Party public key is deleted or becomes invalid, then the certificate chain to MExE executables previously executing in the Third Party Domain certified by that public key will become "untrusted".

There may be any number of Third Party root public keys on the MExE device.

The third party domain administrator, i.e. the Administrator (user or other body) shall be able to enable and disable Third Party root public keys by using CCM, see clause 8.7 “Certificate configuration message (CCM)”. The process of adding/removing public keys and enabling/disabling public key are independent.

All third party certificates shall be subject to restrictions imposed by valid certificate configuration messages.

See clause 8.6 "Certificate management" for the management of Third Party root public keys.

8.5.4 Administrator root public key

To help with the control of Third-Party certificates, the ME shall support secure storage for a certificate containing an administrator root public key. The ME shall support the use and management of a certificate containing an Administrator root public key stored on the MExE-(U)SIM and in the ME. The ME shall behave according to clause 8.8.1 “Determining the administrator of the MExE MS”. For support of public key management on the SIM and the USIM refer to GSM 11.11 [27] and 3GPP TS 31.102 [39] respectively.

A secure mechanism may be used to mark as valid a new certificate containing the administrator root public key on the MExE device. It shall only be possible to use this mechanism to mark a certificate containing a new administrator root public key on the ME as valid, when all administrator root public keys are marked as invalid.

There shall be no more than one valid administrator root public key on the MExE device at any one time. A valid administrator root public key on the (U)SIM shall always have precedence over any administrator root public key on the ME. Any administrator root public key(s) on the ME shall be marked invalid when a valid administrator root public key is present on the (U)SIM.

The MExE device shall support the administrator designation mechanism explained in clause 8.8 "Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device" and the secure downloading of CCMs explained in clause 8.7.4 “Authorised CCM download mechanisms”.

The user shall not be able to delete an administrator root public key or certificate.

The system shall support a mechanism (as part of a provisioned functionality and/or inherently part of the MExE implementation) allowing the owner of the MExE device to manage the administrator root public key (including the download of a new administrator root public key) as defined in clause 8.8.1.1 "Administrator of the MExE device is the user". This mechanism shall be secure so that only the owner can use this functionality.

The administrator root public key can be downloaded to the MExE device as described in clause 8.10.4 "Administrator root certificate download mechanism".

If the Administrator root public key is stored in the (U)SIM, the ME shall only read the Administrator root public key from the MExE-(U)SIM when required and shall not store the Administrator root public key from the MExE-(U)SIM on the ME in a manner inconsistent with that detailed in ~~sub~~clause 8.5.1.1 "Caching of root public keys".

See clause 8.6 "Certificate management" for the management of Administrator root public keys.

The same root public key may be used for both the Administrator role and the operator or manufacturer domain. This facility does not imply any increased right of the manufacturer or operator to take the Administrator role.

If the same root public key is used for the operator domain and Administrator role and this root public key is stored on the MExE-(U)SIM (see [27] and [39]), there shall be separate entries relating to each use of the root public key in the operator and administrator trusted certificate directory files. These entries in the operator and Administrator trusted certificate directory files may point to the same root public key in the certificate data file.

If the root public key to be shared is not stored on the (U)SIM, then procedures relating to this are out of the scope of this specification.

8.5.5 Handling of MExE executables when their valid root public key is not available

This ~~sub~~clause considers the effect on MExE executables when the root public key of a secure domain (e.g. operator, manufacturer, third party) is no longer available (e.g. when the UICC is being physically removed, or the root public key is no longer valid).

...

8.6.1.1 X.509 version 3

The MExE certificate format as specified in ~~section~~ clause 8.4.1.1 "MExE terminal requirements for certificate processing" shall support the X.509 version 3 access-Restriction extension.

X509 version 3 provides a mechanism to define extensions. An Object identifier (OID) is defined for each private extension as defined in X509 [26]. The extension is defined to be within the ETSI Object Identifier (OID) name space.

This extension shall apply irrespective of the presence or otherwise of any other X.509 key usage or extended key usage field.

Normal use of the "critical" flag for extensions apply. That is, if this extension is marked as critical in the certificate used to verify the signature on the application or in any certificate in the chain used to verify the signature and this extension cannot be processed in the MExE devicethen the certificate shall be considered invalid.

The syntax of the extension is defined in annex C "Access restriction certificate extension".

...

8.9.1 PersonalJava security

There are two types of Java security [20]: sandbox, and fine grain.

The sandbox model [18] has just one domain; there is no concept of a *partly trusted* domain. The sandbox meaning of "trusted" means it is totally unrestricted to access all system resources.

Using the sandbox system, each MExE security domain shall be implemented as running in a sandbox, configured with different privileges corresponding to those of the domain. If the security domains are not supported then the Java sandbox security model shall be supported and it shall be configured for untrusted MExE executables support only, as defined in clause 8.2 "MExE executable permissions".Using the fine grain Java security system [19], each MExE security domain will be a set of constraints within which a Java fine grain security domain can be configured.

8.9.1.1 Java applet certification in PersonalJava

Support for trusted applets is optional. Although a Java application shall be executed in a trusted domain if its certification can be validated, a Java Applet will not necessarily be executed in a trusted domain even if it does have a valid signature. It will be up to the implementers to decide if "trusted" Applets will be supported. (In certain implementations, all Applets may be always executed as "untrusted".)

8.9.1.2 Java application signature verification in PersonalJava

The verification of the certification of the application or applet shall be performed as described in clauses 8.5 ”Root Public keys” and clause 8.8 “Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE MS”.

...

8.11 MExE executable integrity

If the 3 MExE security domains defined in clause 8.1 "Generic security" are not supported, then the pre-verification of MExE executables at launch time described in this clause is optional.

A potential threat is that MExE executables may be securely authenticated at the time of download, but tampered with or corrupted prior to being launched. Further a certificate may be compromised or expired. Authentication of a MExE executable at the time of download does not ensure that the MExE executable has not been modified when it is subsequently launched. Furthermore, authentication of a MExE executable at the time of launch does not ensure that the MExE executable is not modified during execution. Similarly, verification of the certificate at the time of download may not ensure that the certificate is valid at time of application launch, and verification of the certificate at the time of launch does not ensure that the certificate remains valid during execution.

Therefore, the MExE device shall ensure application integrity immediately prior to application execution.

Application integrity is defined as the state in which:-

- application code has not been modified since authentication; and
- the certificate containing the root public key is checked and known to be valid.

The mechanism by which the device preserves integrity is an implementation detail, dependant on the application storage mechanism and access. Examples of mechanisms that contribute to such application integrity could include :

- Storage of applications in a non-compromisable memory area on the device;
- Preventing launch of the application when the MExE device becomes aware that the certificate is invalidated;
- Full signature verification prior to each application invocation (see clause 8.11.1 “Full signature verification”);
- Optimised pre-launch signature verification (see clause 8.11.2 “Optimised pre-launch signature verification”);
- Periodic full signature verification by separate process during application execution.

The list of examples is not exhaustive and any other mechanisms ensuring application integrity may be equally considered.

A MExE device may furthermore ensure that the application code has not been modified during application execution.

…

Annex A (normative): MExE profile of PKCS#15

A.1 PKCS#15 certificate object attributes presentation

Details from PKCS#15[32] in this ~~clause~~ Annex A.1 "PKCS#15 certificate object attributes presentation" are for information only.

A.1.1 Object common attributes

Label	human readable label to describe the certificate
Flags	indicates whether the object is private (e.g. CHV authentication request), whether the object is read only.
Authentication object identifier	a cross-reference back to the authentication object, which describes the properties of a CHV, used to protect this object.

A.1.2 Certificate common attributes

identifier	the identifier is used for correlation between the public key contained in the certificate and the associated private key.
Authority	indicates whether the certificate is for an authority (i.e. CA or AA) or not.
Request identifier	used to search a certificate : Issuer and serial number SHA-1 hash, or issuer public key SHA-1hash, or public key subject SHA-1 hash.
Thumbprint	used as secure way to verify that no one has tampered with a certificate: hash on to be signed certificate (internet). MExE uses the thumbprint to enable or disable a certificate through the certificate configuration message (CCM).

A.1.3 Certificate attributes

Type of certificate	indicates the type of certificate: WTLS, X509, SPKI, PGP, X9.68.
Value	direct value or indirect file path or URL.

MExE only supports storage of WTLS, X509, X9.68 certificates.

A.1.4 Specific X.509 certificate attributes

For information see PKCS#15 [32].

A.2 MExE profile of PKCS#15

`PKCS15CommonObjectAttributes.label` must be present. The value content is unspecified.

`PKCS15CommonObjectAttributes.Flag` must be present. The value shall be private, not modifiable by MExE device.

PKCS15CommonObjectAttributes.Authentication must be present. The value shall be "CHV1". The certificates files are protected by CHV1, because MExE need also IMSI to manage domains availability.

PKCS15CommonCertificateAttributes.Id must be present. The value content is unspecified.

PKCS15CommonCertificateAttributes.Authority must be present if and only if certificate is a CA certificate. The value is true.

PKCS15CommonCertificateAttributes.RequestId must be at least present if certificate is an operator or third party root certificate. The value shall be the same as the ones used in the issuer/authority key identifier field of the certificates, provided by this issuer (as in RFC2459 document [43]). The aim of this attribute is to give a easy way to search a key issuer of a received certificate without reading all certificates content.

PKCS15CommonCertificateAttributes.Thumbprint must be at least present if certificate is a third party root certificate. The value shall be the same as the ones used in CCM. The aim of this attribute is to give a easy way to search a certificate with reference included in CCM message.

Domain attribute presence and value shall be added as soon as it will be available in PKCS#15 v1.1.

PKCS15(type)CertificateAttributes.value must be present Value is a indirect file path (path, index, offset). Index and offset default value is 0.

Specific X509 attributes are not supported:

PKCS15X509CertificateAttributes.subject must not be present.

PKCS15X509CertificateAttributes.issuer must not be present.

PKCS15X509CertificateAttributes.serialNumber must not be present.

The MExE device shall recognise all optional present fields above. The MExE device shall accept and ignore all unused fields or new field extensions.

A.3 Coding and storage in MExE-(U)SIM

See detail of file hierarchy and file properties in (U)SIM document [27] and [39].

Since the domain attribute is not available in PKCS#15 v1.0, MExE creates one directory file for each trusted domain. If the domain attribute is available in the next PKCS#15 versions, for future new domains, MExE may create a common directory file. See abstract syntax definition and coding detail in PKCS#15 document [32].

The address of the certificate descriptor Elementary File is fixed.

According to PKCS#15 [32] clause 6~~7~~.6 "~~The PKCS15~~Certificates~~ type~~" , the contents of a certificate descriptor Elementary File must be the *value* of the DER encoding of a **SEQUENCE OF PKCS15Certificate** (i.e. excluding the outermost tag and length bytes).

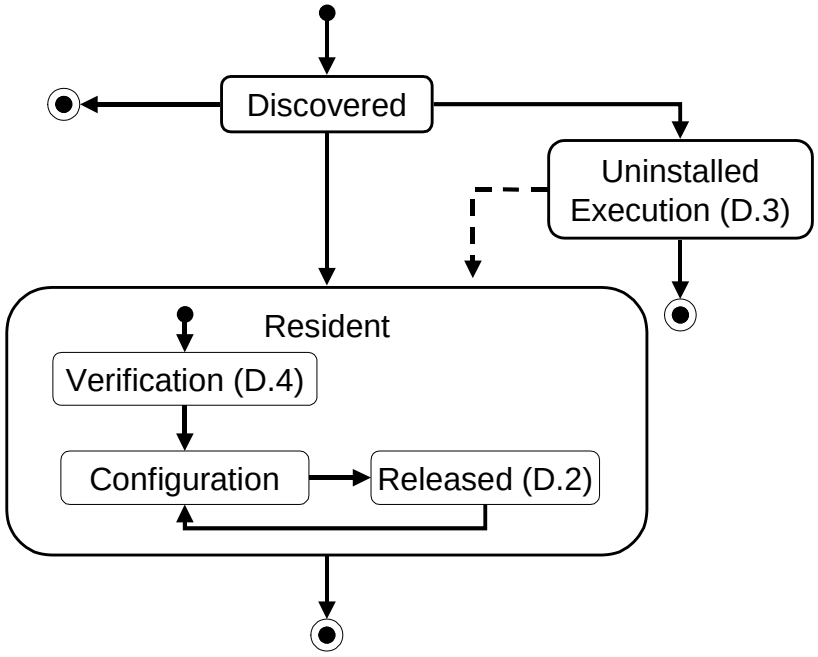
The address of the certificate data Elementary File is unspecified.

According to PKCS#15 [32] clause~~s 7~~6.6~~.1 to 7.6.6~~ "Certificates", the certificate data value is coded according to the related certificate type (e.g. DER for X5.09, base64 for SPKI and PGP, WTLS network format for WTLS, DER or PER for X9.68).

...

D.1 State of a MExE executable

The life cycle of MExE executables (clause 4.9 "Provisioning and management of services") is described using a state machine. In a MExE device a MExE executable can have the following states and transitions between states.



State or Transition (=>)	Description
Initial => Discovered	The MExE executable is discovered (clause 4.9.1 "Service discovery").
Discovered	The MExE executable is discovered and can be installed or executed without installation. (Only executables useable on the MExE device should enter this state.)
Discovered => Resident	The discovered executable is selected to be installed and the executable is transferred (clause 4.9.2 "Service transfer") to the MExE device for installation.
Discovered => Uninstalled Execution	The discovered executable is selected to be executed without installation.
Discovered => final state	The executable is undiscovered.
Resident	The executable is stored in the MExE device. It has been transferred or is pre-loaded.
Verification	This is the initial sub-state of the Resident state. This is a composite state. There is a description of the Verification state in D.4.
Verification => Configuration	The result of the verification indicates that the executable can be installed in one of the Domains.
Configuration	This is a sub-state of the Resident state. The executable can be configured, manually or automatically (clause 4.9.3 "Service installation and configuration").
Configuration => Released	The service is released for execution.
Released	This is a sub-state of the Resident state. The executable is resident, configured and released for execution. This is a composite state and there is a description of it in D.2.
Released => Configuration	The executable is blocked for execution or an executable has changes security domain (The user shall have the possibility to review the configuration before the executable is released for execution with different privileges.).
Resident => final state	The Resident state is left when the service is deleted (clause 4.9.6 "Service deletion"). From the MExE device point of view the executable does not exist any more. (The Integrity and Certification Validation (clause 8.6 "Certificate management") can also force a deletion)
Uninstalled Execution	The executable is executed without installation. This is a composite state. There is a description of the Uninstalled Execution state in D.3.
Uninstalled Execution => final state	The Uninstalled Execution state is left when the executable terminates by itself or when the user terminates the executable (clause 4.9.5 “Service termination”). From the MExE device point of view the executable does not exist any more.
Uninstalled Execution => Resident	This is a possible but unusual transition. A MExE executable that has been used for uninstalled execution is installed without retransferring.