3GPP TSG-T (Terminals) Meeting #13
Beijing, China, 19 - 21 September, 2001

Tdoc TP-010192

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	086	1	Rel-4	Status of applications when valid RPK not available	F	4.2.0	4.3.0	T2-010691	MEXE-ENHANC
23.057	092	1	Rel-4	Clarification of root public keys	F	4.2.0	4.3.0	T2-010681	MEXE-ENHANC
23.057	093		Rel-4	Update to the states in the diagram D4	F	4.2.0	4.3.0	T2-010855	MEXE-ENHANC
23.057	094		Rel-4	Clarifying Description of CCM Format	F	4.2.0	4.3.0	T2-010672	MEXE-ENHANC
23.057	095		Rel-4	Trust Hierarchy and Administrator RPK	F	4.2.0	4.3.0	T2-010683	MEXE-ENHANC
23.057	096		Rel-4	Implementations with Non-persistent Caching of RPKs	F	4.2.0	4.3.0	T2-010684	MEXE-ENHANC
23.057	097		Rel-4	A specified certificate format for MExE	F	4.2.0	4.3.0	T2-010689	MEXE-ENHANC

3GPP TSG-T2 #14
Edinburgh, Scotland
3-7 September 2001

T2-010691

CR-Form-v3

CHANGE REQUEST

⌘ **23.057** **CR** **086** ⌘ rev **1** ⌘ Current version: **4.2.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Status of applications when valid RPK not available
Source:	⌘	T2
Work item code:	⌘	MEXE-ENHANC
Date:	⌘	4-September-2001
Category:	⌘	**F**
Release:	⌘	REL-4

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

Use one of the following releases:

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

Reason for change:	⌘	The TS is currently unclear on how to handle MExE executables when their valid root public key is not present.
Summary of change:	⌘	The text in subclause 8.5.1.2 currently only applies to operator applications, however it is generically applicable to all secure MExE executables. The relevant text is therefore moved to a new subclause, and together with other text, identifies the following procedures when the root public key is not available:- • how to handle launching of new secure MExE executables • how to handle currently executing secure MExE executables
Consequences if not approved:	⌘	The current requirements for the support of applications when an RPK is invalidated requires clarification to avoid differing implementations by manufacturers.

Clauses affected:	⌘	Sub-clause 8.5
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	This was approved in T2-MExE-010081.

How to create CRs using this form:

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

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

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

8.5 Root Public keys

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

8.5.1 Operator root public key

The ME shall support secure storage for at least one certificate containing an operator root public key. The ME shall support the use and management of a certificate containing an operator root public key stored on the MExE-(U)SIM and in the ME. The ME shall behave according to section 8.5.1.1 “ME actions on SIM insertion and/or power up”. 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 certificate contains a root public key generated either by the operator, or by a CA trusted by the operator. The ME shall get the operator root public key from the secure area every time it needs to verify a signature, rather than cache the root public key for use in subsequent verifications.

If the MExE device does not contain a valid operator root public key, then the certificate chain to MExE executable previously executing in the Operator Domain will be invalid, and the MExE executables will be excluded from the operator domain.

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

Optionally, the operator may install a corresponding disaster-recovery root public key stored in the MExE device, enabling the operator to use a secure mechanism (involving the disaster-recovery key) to replace the certificate containing the standard operator root public key. It shall not be possible to use the disaster recovery operator root public key to replace the standard operator root public key unless both public keys are from the same operator.

There shall be no more than one valid operator root public key on the MExE device (excluding the disaster recovery root public key) at any one time.

An application signed by an operator shall not be able to execute in the Operator Domain unless the root public key of that operator is installed in the MExE device (either ME or MExE-(U)SIM) and is marked as trusted.

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

This subclause 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 subclause 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.

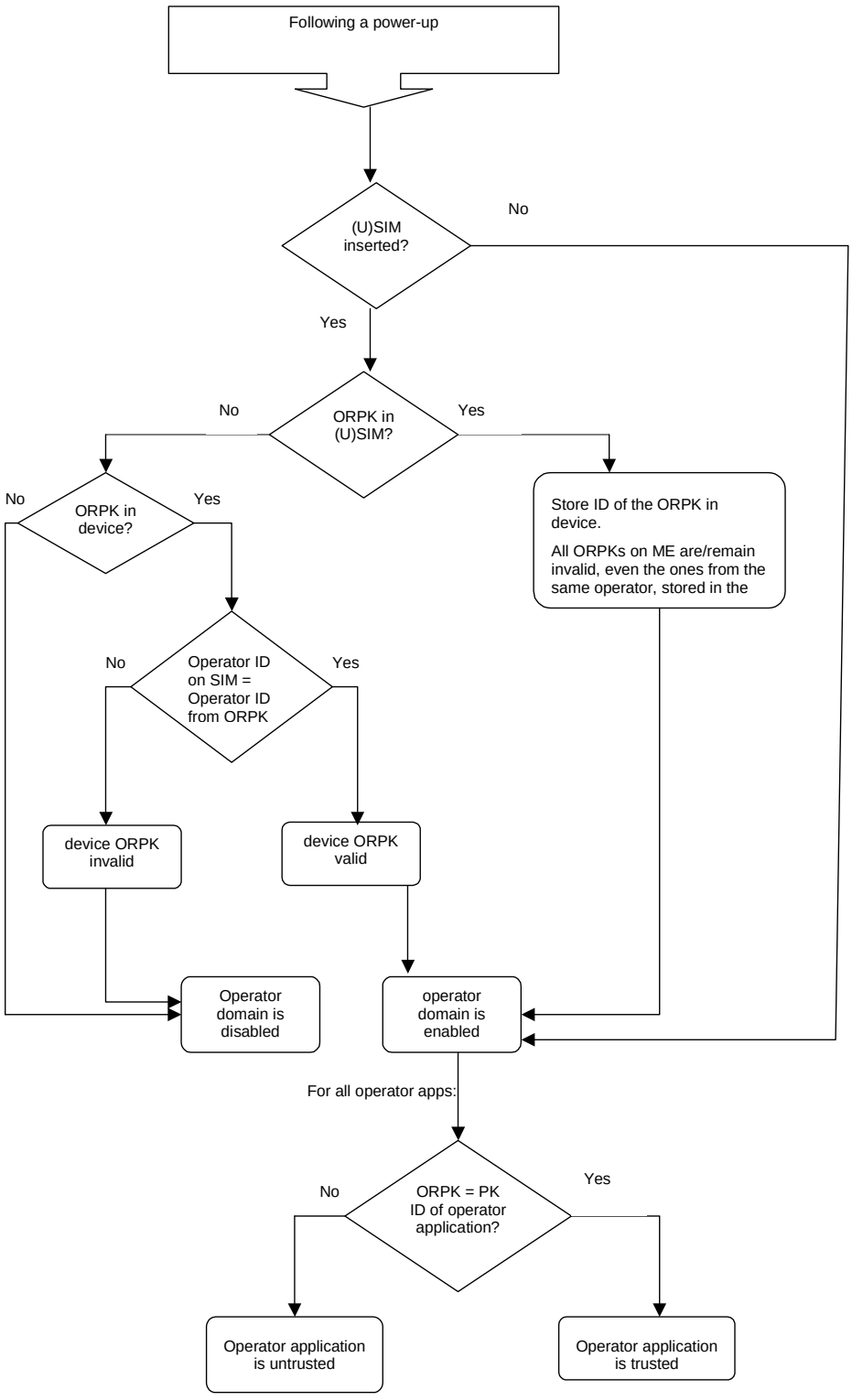


Figure 7: MExE device behaviour on power up

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.

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.

~~8.5.1.2 MExE device actions when a valid (U)SIM application is no longer present~~

~~This subclause concerns the status of authenticated applications (i.e. having a certificate chain to a root public key of a secure domain) on identification by the MExE ME that a valid SIM card, or USIM application on the UICC, is no longer present. This could occur, for example, through removal of (U)SIM card, expiry/compromise of the root public key etc.).~~

~~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.~~

~~If the valid (U)SIM application is no longer present in the MExE device (without another valid (U)SIM application being detected), operator applications shall continue to execute in the operator domain.~~

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.

There shall be no more than one valid manufacturer root public key on the ME (excluding the disaster recovery root public key).

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 subclause 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 subclause 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 subclause 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 section 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. Only one administrator root public key shall be valid on the MExE device at any one time.

The MExE device shall support the administrator designation mechanism explained in subclause 8.8 "Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device" and the secure downloading of CCMs explained in subclause 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 subclause 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 subclause 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.

See subclause 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 subclause 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).

8.5.5.1 Launching of MExE executables when their valid RPK is not available

It shall not be possible to launch a MExE executable to run in a security domain unless the root public key of that security domain is available and valid.

8.5.5.2 Currently executing secure MExE executables when their valid RPK is no longer available

On detection that the valid root public key of a secure domain is no longer present, the MExE device shall permit MExE executables currently executing in the secure domain controlled by that root public key to continue executing. Furthermore, if the same RPK is available again, the executable is allowed to keep on executing. However, if a different RPK is validated, the currently running MExE executables (under the old RPK) in that secure domain shall be terminated.

3GPP TSG T2
Edinburgh, Scotland
3 - 7 September 2001

T2-010681

CR-Form-v3

CHANGE REQUEST

⌘ **23.057** **CR** **092** ⌘ rev **1** ⌘ Current version: **4.2.0** ⌘

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

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

Title:	⌘	Clarification of root public keys
Source:	⌘	T2
Work item code:	⌘	MEXE-ENHANC
Date:	⌘	25/07/2001
Category:	⌘	**F**
Release:	⌘	REL-4

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

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	The TS is insufficiently clear on how root public keys may be replaced, and their relationship to other root public keys of the same type.
Summary of change:	⌘	It is clarified:- • specifically which entity is permitted up replace a root public key • which mechanism may be used to replace a root public key • in the event of keys of the same root public key type on the (U)SIM and the ME, that the valid root public key on the (U)SIM shall always have precedence over any root public key of the same type on the ME • in the event of keys of the same root public key type on the (U)SIM and the ME, any root public key(s) on the ME shall be marked invalid whilst a valid root public key of the same type is present on the (U)SIM.
Consequences if not approved:	⌘	Lack of clarification may lead to insecure implementations

Clauses affected:	⌘	
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	TSG-T had approved a previous version of this CR as CR92 at TSG-T#13, however as it was based on an old version of 23.057, it proved difficult for it to be incorporated. This CR is based on the current version of 23.057

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at:
http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

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

8.5 Root Public keys

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

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

8.5.1 Operator root public key

The ME shall support secure storage for at least one certificate containing an operator root public key. The ME shall support the use and management of a certificate containing an operator root public key stored on the MExE-(U)SIM and in the ME. The ME shall behave according to section 8.5.1.1 “ME actions on SIM insertion and/or power up”. 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 certificate contains a root public key generated either by the operator, or by a CA trusted by the operator. The ME shall get the operator root public key from the secure area every time it needs to verify a signature, rather than cache the root public key for use in subsequent verifications.

If the MExE device does not contain a valid operator root public key, then the certificate chain to MExE executable previously executing in the Operator Domain will be invalid, and the MExE executables will be excluded from the operator domain.

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

Optionally, the operator may install a corresponding disaster-recovery root public key stored in the MExE device, enabling the operator to use a secure mechanism (involving the disaster-recovery key) to replace the certificate containing the standard operator root public key. It shall not be possible to use the disaster recovery operator root public key to replace the ~~standard~~ operator root public key unless both public keys are from the same operator.

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

An application signed by an operator shall not be able to execute in the Operator Domain unless the root public key of that operator is installed in the MExE device (either ME or MExE-(U)SIM) and is marked as trusted.

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

This subclause 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 subclause 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.

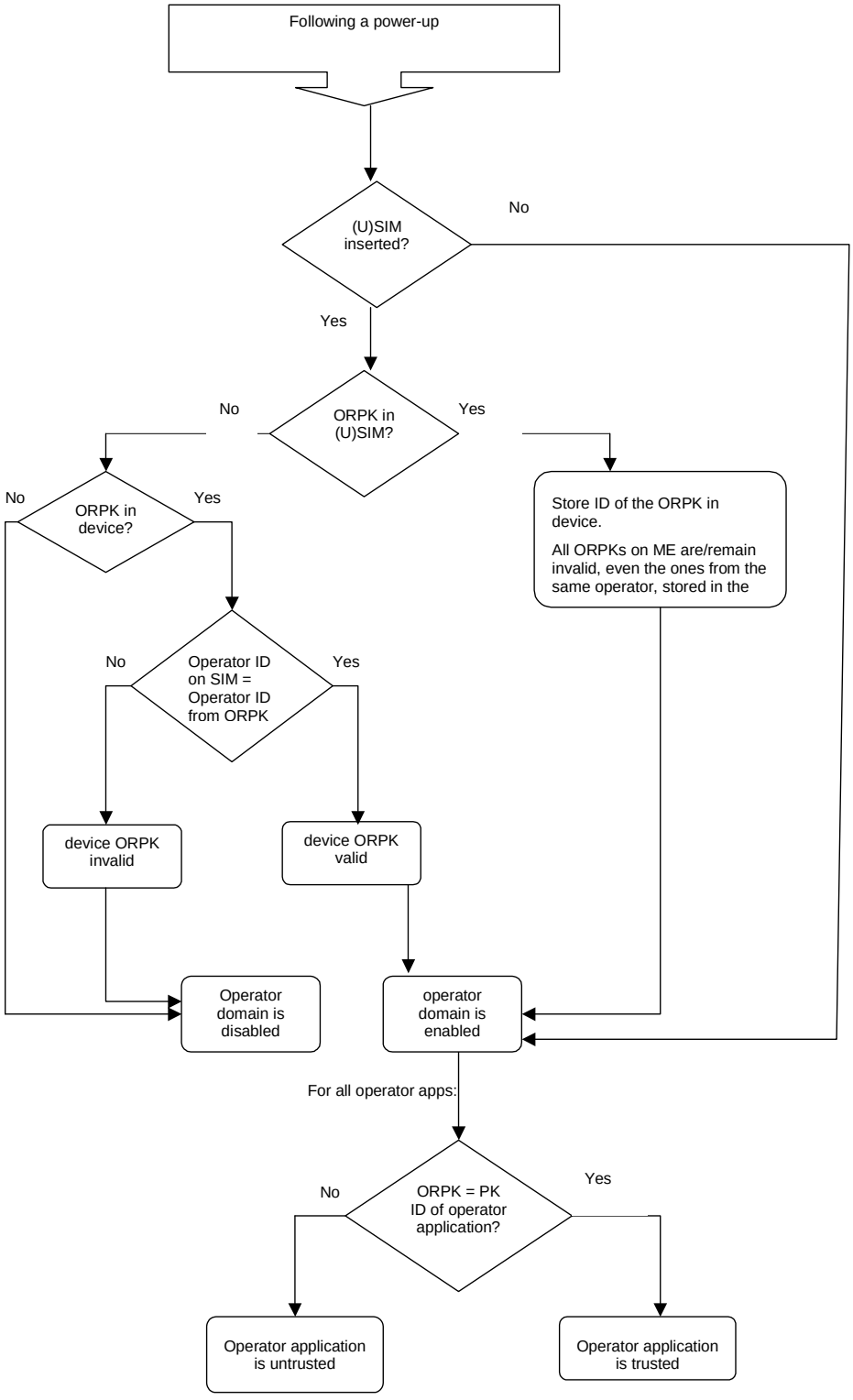


Figure 7: MExE device behaviour on power up

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.

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.

8.5.1.2 MExE device actions when a valid (U)SIM application is no longer present

This subclause concerns the status of authenticated applications (i.e. having a certificate chain to a root public key of a secure domain) on identification by the MExE ME that a valid SIM card, or USIM application on the UICC, is no longer present. This could occur, for example, through removal of (U)SIM card, expiry/compromise of the root public key etc.).

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.

If the valid (U)SIM application is no longer present in the MExE device (without another valid (U)SIM application being detected), operator applications shall continue to execute in the operator domain.

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 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~~(excluding the disaster recovery root public key)~~.

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 subclause 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 subclause 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 subclause 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 section 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 ~~Only~~ one valid administrator root public key ~~shall be valid~~ 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 subclause 8.8 "Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device" and the secure downloading of CCMs explained in subclause 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 subclause 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 subclause 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.

See subclause 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 MExE
Edinburgh, Scotland
3 - 7 September 2001

T2-010855

CR-Form-v3

CHANGE REQUEST

⌘ **23.057** **CR** **093** ⌘ rev **-** ⌘ Current version: **4.2.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Update to the states in diagram D4
Source:	⌘	T2
Work item code:	⌘	Security
Date:	⌘	18-July-2001
Category:	⌘	**F**
Release:	⌘	REL-4

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

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	There is no such state called “domainless” in the specification and it is inconsistent with section 8.4.3 “Certificate Chain Verification”. Also the text does not reflect that the executable shall be deleted as specified in section 8.4.3 and therefore needs to be updated.
Summary of change:	⌘	The term Domainless is replaced with the term “Deleted” and text is added to explicitly state that the executable is deleted.
Consequences if not approved:	⌘	Inconsistent specification

Clauses affected:	⌘	Appendix D “MExE Executable Life Cycle”
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

How to create CRs using this form:

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

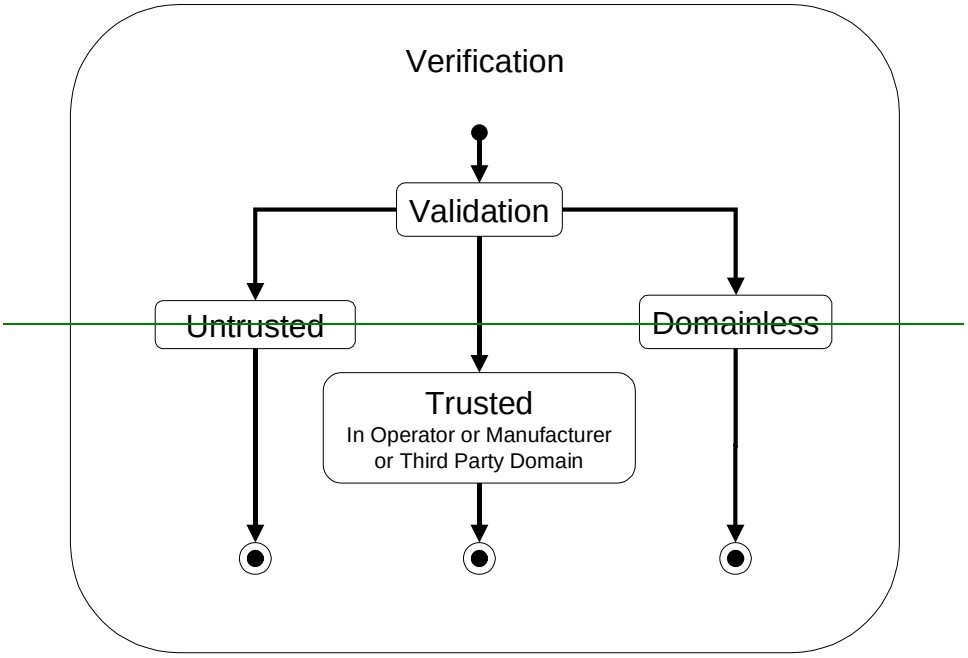
1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

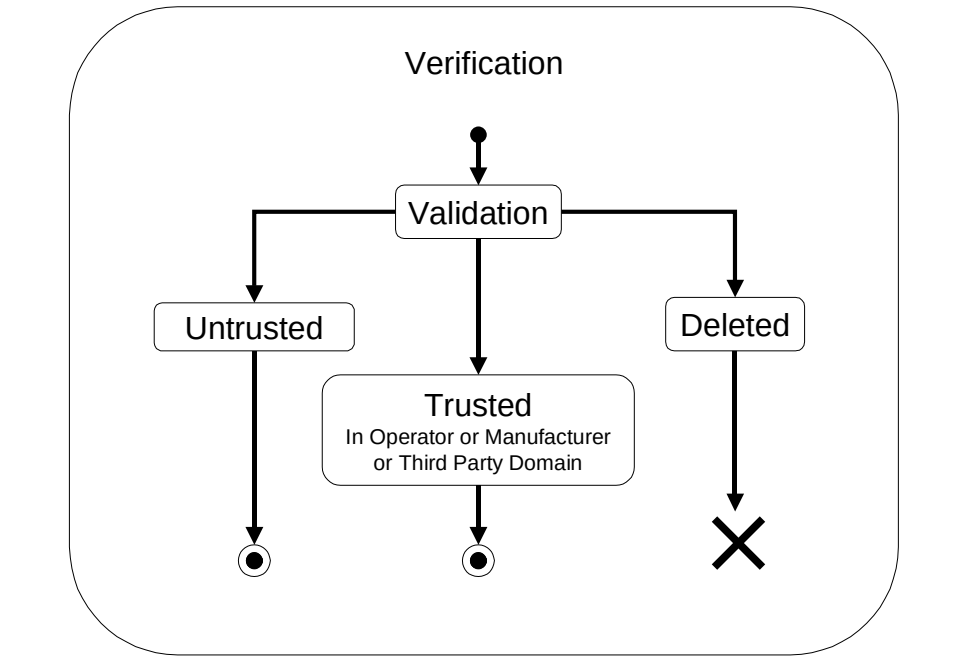
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

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

D.4 Verification

The integrity and certification validation (8.6 "Certificate management") is done in the Verification state. The result of validation determines the change of state.





State	Description
Validation	This is the initial state. The integrity and certification validation (8.6 "Certificate management") is done.
Untrusted	The executable is untrusted (8.1 "Generic security")
Trusted in Operator Domain	The executable is verified to belong to the Operator Domain (8.1 "Generic security").
Trusted in Manufacturer Domain	The executable is verified to belong to the Manufacturer Domain (8.1 "Generic security").
Trusted in Third Party Domain	The executable is verified to belong to the Third Party Domain (8.1 "Generic security").
~~Domainless~~Deleted	The executable is not permitted in any Domain and ~~may not run at all.~~it is deleted.

3GPP TSG-T2 #14
Edinburgh, Scotland
3-7 September 2001

T2-010672

CR-Form-v3

CHANGE REQUEST

⌘ **23.057** **CR** **094** ⌘ rev **-** ⌘ Current version: **4.2.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Clarifying Description of CCM Format
Source:	⌘	T2
Work item code:	⌘	MEXE-ENHANC
Date:	⌘	27-August-2001
Category:	⌘	**F**
Release:	⌘	REL-4

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

Use one of the following releases:

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

Reason for change:	⌘	The figure titled “Format of a CCM” is separated from the leading discussion with detailed formats on the fields within the CCM, and there are several inconsistencies between the figure labels and descriptive text.
Summary of change:	⌘	The figure and descriptive text for “Format of a CCM” is moved from a placement after sub-clause 8.7.3 to a placement before sub-clause 8.7.1. Figure labels or descriptive text is modified in order to have more consistent information
Consequences if not approved:	⌘	The placement and wording of the “Format of a CCM” is currently difficult to understand and may result in inconsistent implementations. For consistent implementations, the field names in the figure descriptions are changed to match the field names in the figure graphics.

Clauses affected:	⌘	Sub-clause 8.7
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

How to create CRs using this form:
Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

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

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

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

8.7 Certificate configuration message (CCM)

If the 3 MExE security domains defined in subclause 8.1 "Generic security" are not supported, then the certificate configuration message described in this subclause is optional.

The MExE device shall use the CCM to determine the third party certificates (and only the Third Party certificates) that are trusted for use on the MExE device. The CCM shall only be used to enable or disable third party certificates and can not be used to delete certificates. The CCM may be periodically fetched or downloaded to a MExE device by the Administrator to dynamically configure the third party list using the mechanisms defined in subclause 8.7.4 "Authorised CCM download mechanisms".

The Certificate Configuration Message shall be as shown in Figure ~~8~~9 "Format of a CCM". This message is essentially a simplified version of a certificate revocation list to satisfy a particular use case. More complex usage requires a full certificate revocation list.

The MExE device may additionally support other means of enabling/disabling root certificates.

Bit 7 6 5 4 3 2 1 0	Octet
Version	0
Certificate Advice	1
Issue Timestamp . .	2 – 8
Expiry Timestamp . .	9 –15
SignerInfo	16
Listlength	17 –18
Fingerprint 1 Hashtype	19
Hashvalue (Variable length k according to hash type) . .	20
Fingerprint 2 Hashtype	k+20
Hashvalue (Variable length m according to hash type) . .	
Fingerprint 3 Hashtype	(k+20)+m+1
Hashvalue (Variable length) . .	
Fingerprint n Hashtype	etc.
Hashvalue (Variable length) . .	
CCM Signature Hashtype	Listlength+19
CCM signature (Variable length according to CCM signature type)	

Figure 8: Format of a CCM

Version = The CCM format version is 0. All other values are reserved for future use.

Certificate Advice = enumerated { enable all present and future Third Party certificates (0), disable all present and future Third Party certificates (1), enable present list only (2),enable CCM list (3), disable CCM list (4) }. All other values are reserved for future use.

Issue and Expiry Timestamps = Fields used to identify the issue and expiry date of the CCM. The issue timestamp indicates a time before the current time of day (GMT) when a CCM message must be considered invalid. The expiry timestamp (GMT) identifies the time when a CCM is to be deemed no longer valid. The receiver shall use these parameters to detect a replay attack. A MExE device maintains information on the last valid CCM message received. A replay attack is an attacker replaying a previous valid CCM message to a MExE device in order to change the security settings. This is particularly dangerous for CCM messages used to enable certificates. Administrators should try and set the expiration time to be no longer than the next expected system update time of CCM information. CCM messages used to enable-all (rather than disable-all) certificates should be very short lived as the danger of these being used in a replay attack should be considered serious.

The encoding of time (GMT) shall be coded as an OCTET SEQUENCE of seven octets in length as follows:

Octet 0	1	2	3	4	5	Octet 6
Year		Month	Day	Hour	Minute	Second

Element	Size (bits)	Range
Year	16	$(0 – 65535)_{10}$
Month	8	$(1 – 12)_{10}$
Day	8	$(1 - 31)_{10}$
Hour	8	$(0- 23)_{10}$
Minute	8	$(0 – 59)_{10}$
Second (see note)	8	$(0 – 60)_{10}$
NOTE: The second field range includes the value 60 in order to accommodate leap seconds.		

For example, 1st January, 2001 00:00:30 would be encoded as: 07 d1 01 01 00 00 1E.

SignerInfo = one octet indicating the type of signer information for this CCM. The only currently defined value is device-admin = 0. In this case, no further signer information follows as it is implicit. All other values are reserved for future use.

Listlength = The total length of the fingerprint list not including the final CCM signature. Shall be zero when certificateAdvice = enable-all, disable-all or enable present list.

Hashtype = enumerated { signature (0), MD5 (1), SHA-1 (2) } All other values are reserved for future use.

The length of the Hashvalue field, number of octets output by the selected hash type, is 16 for MD5 [23] or 20 for SHA-1 [24].

The list entries shall contain certificate *fingerprints* in the form of hashes of the encoded signed certificates. The full hash output for the specified algorithm shall be used to generate the fingerprint. A list generator shall check to insure that no two list entries match when creating a list. For an X509v3 [26] or X9.68 (currently being drafted) certificate the fingerprint hash shall be computed over the ASN.1 encoded signed certificate object, first octet to last octet. For WTLS certificates the hash shall be computed over the signed WTLS certificate in network transmission format, first octet to last octet.

The signature type and length shall be indicated by the administrator certificate, which shall be present on the MExE device. If no administrator certificate is on the MExE device or if the signature is not verified, the message shall be rejected.

Upon receipt of a valid certificate configuration message the MExE device shall go through the third party certificate list, computing fingerprints if they are not stored with the certificate and enabling or disabling each certificate according to the following conditions:

- certificateAdvice is enable-all all Third Party certificates shall be enabled;
- certificateAdvice is disable-all all Third Party certificates shall be disabled;

- certificateAdvice is enable present list only	enable all Third Party certificates currently on MExE device, do not enable any future certificates (this option allows the list to be frozen at time of manufacture) until Administrator changes;
- certificateAdvice is enable-list	if its fingerprint occurs in the CCM, it shall be enabled, otherwise it shall be disabled;
- certificateAdvice is disable-list	if its fingerprint occurs in the CCM, it shall be disabled, otherwise it shall be enabled.

For future releases, the setting of fine grained permissions for each certificate is expected to be supported.

An implementation shall keep track of the domain that authorised a given application. If a CCM message is received while MExE applications are currently running, the implementation shall check to ensure any applications no longer in the Third Party domain have their permissions re-configured appropriately and actions that are no longer permissible are terminated.

8.7.1 CCM numbering convention

Bits are grouped into octets. The bits of an octet are shown horizontally and are numbered from 0 to 7. Multiple octets are shown vertically and are numbered from 0 to n.

8.7.2 CCM order of transmission

Frames are transferred in units of octets, in ascending numerical octet order (i.e., octet 0, 1, …, n-1, n). The order of bit transmission is specific to the underlying protocols used to transport the CCM.

8.7.3 CCM field mapping convention

When a field is contained within a single octet, the lowest bit number of the field represents the lowest-order value. When a field spans more than one octet, the order of bit values within each octet progressively decreases as the octet number increases. In that part of the field contained in a given octet the lowest bit number represents the lowest-order value.

For example, a 16 bit number can be represented as shown in Figure 98 "Field mapping convention".

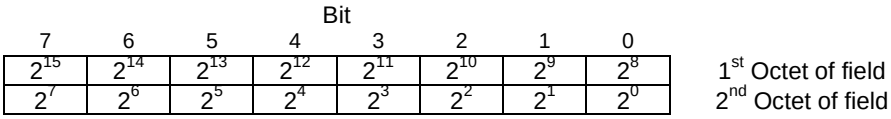


Figure 98: Field mapping convention

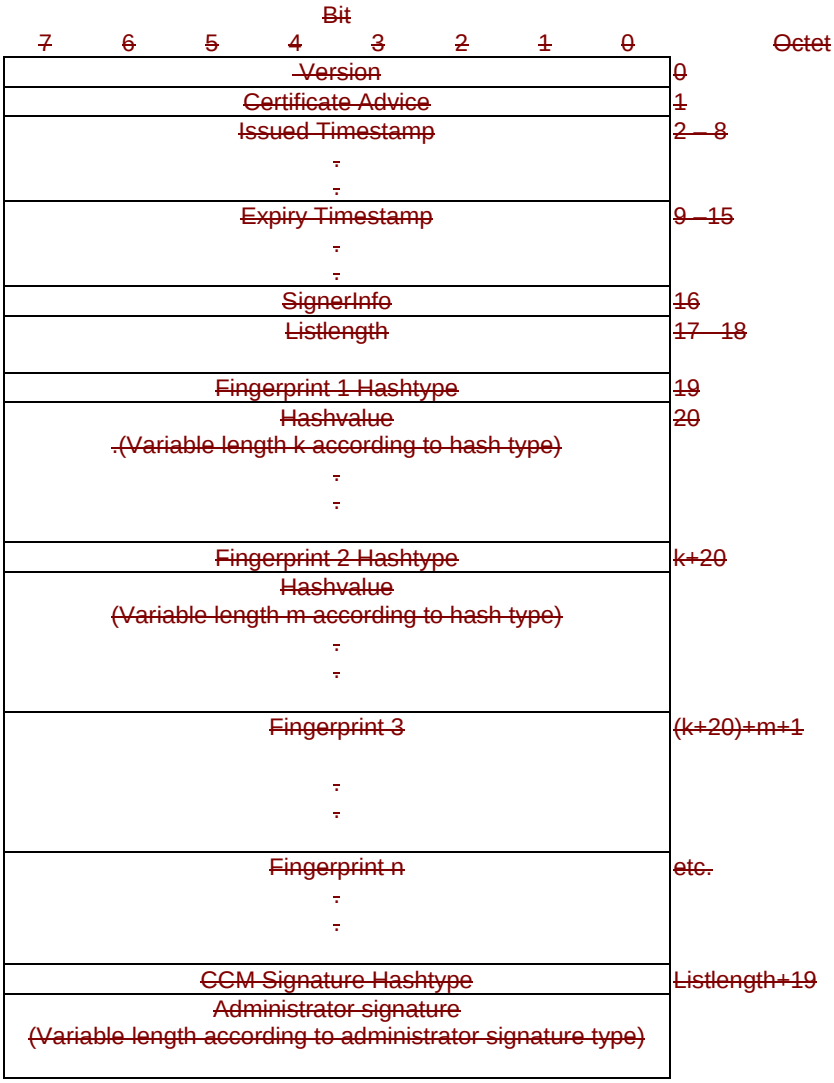


Figure 9: Format of a CCM

version = The CCM format version is 0. All other values are reserved for future use.

certificateAdvice = enumerated { enable all present and future Third Party certificates (0), disable all present and future Third Party certificates (1), enable present list only (2),enable CCM list (3), disable CCM list (4) }. All other values are reserved for future use.

Issue and Expiry Timestamps = Fields used to identify the issue and expiry date of the CCM. The issue timestamp indicates a time before the current time of day (GMT) when a CCM message must be considered invalid. The expiry timestamp (GMT) identifies the time when a CCM is to be deemed no longer valid. The receiver shall use these parameters to detect a replay attack. A MExE device maintains information on the last valid CCM message received. A replay attack is an attacker replaying a previous valid CCM message to a MExE device in order to change the security settings. This is particularly dangerous for CCM messages used to enable certificates. Administrators should try and set the expiration time to be no longer than the next expected system update time of CCM information. CCM messages used to enable all (rather than disable all) certificates should be very short lived as the danger of these being used in a replay attack should be considered serious.

The encoding of time (GMT) shall be coded as an OCTET SEQUENCE of seven octets in length as follows:

Octet 0	1	2	3	4	5	Octet 6
Year		Month	Day	Hour	Minute	Second

Element	**Size (bits)**	**Range**
Year	16	$(0 \ldots 65535)_{10}$
Month	8	$(1 \ldots 12)_{10}$
Day	8	$(1 \ldots 31)_{10}$
Hour	8	$(0 \ldots 23)_{10}$
Minute	8	$(0 \ldots 59)_{10}$
Second (see note)	8	$(0 \ldots 60)_{10}$
NOTE: The second field range includes the value 60 in order to accommodate leap seconds.		

For example, 1st January, 2001 00:00:30 would be encoded as: 07 d1 01 01 00 00 1E.

SignerInfo = one octet indicating the type of signer information for this CCM. The only currently defined value is device_admin = 0. In this case, no further signer information follows as it is implicit. All other values are reserved for future use.

listLength = The total length of the fingerprint list not including the final CCM signature. Shall be zero when certificateAdvice = enable-all, disable-all or enable present list.

hashType = enumerated { signature (0), MD5 (1), SHA-1 (2) } All other values are reserved for future use.

hashLength = The number of octets output by the selected hash type (16 for MD5 [23] and 20 for SHA-1 [24]).

The list entries shall contain certificate *fingerprints* in the form of hashes of the encoded signed certificates. The full hash output for the specified algorithm shall be used to generate the fingerprint. A list generator shall check to insure that no two list entries match when creating a list. For an X509v3 [26] or X9.68 (currently being drafted) certificate the fingerprint hash shall be computed over the ASN.1 encoded signed certificate object, first octet to last octet. For WTLS certificates the hash shall be computed over the signed WTLS certificate in network transmission format, first octet to last octet.

The signature type and length shall be indicated by the administrator certificate, which shall be present on the MExE device. If no administrator certificate is on the MExE device or the signature does not verify the message shall be rejected.

Upon receipt of a valid certificate configuration message the MExE device shall go through the third party certificate list, computing fingerprints if they are not stored with the certificate, enabling or disabling each certificate according to the following conditions:

- certificateAdvice is enable-all – all Third Party certificates shall be enabled;
- certificateAdvice is disable-all – all Third Party certificates shall be disabled;
- certificateAdvice is enable present list only – enable all Third Party certificates currently on MExE device, do not enable any future certificates (this option allow the list to be frozen at time of manufacture) until Administrator changes;
- certificateAdvice is enable-list – if its fingerprint occurs in the CCM, it shall be enabled, otherwise it shall be disabled;
- certificateAdvice is disable-list if its fingerprint occurs in the CCM, it shall be disabled, otherwise it shall be enabled.

For future releases, the setting of fine grained permissions for each certificate is expected to be supported.

~~An implementation shall keep track of the domain that authorised a given application. If a CCM message is received while MExE applications are currently running the implementation shall check to ensure any applications no longer in the Third Party domain have their permissions re-configured appropriately and actions that are no longer permissible are terminated.~~

8.7.4 Authorised CCM download mechanisms

The download of third party certificate lists by a remote administrator shall be performed by using a secure mechanism as defined below. The download mechanisms shall use HTTP over IP and/or the WAP Protocol. The URL from which the CCM is downloaded shall be in the administrator certificate if the CCM was not downloaded with the Administrator certificate. The format for storing the URL information with the certificate shall be as shown in Figure 10 "CCM Message URL storage format":

UrlType	**CharacterSet**	**UrlLength**	**URL**

Figure 10: CCM Message URL storage format

UrlType= one byte, enumerated {WAP (0), HTTP (1)}. All other values are reserved for future use.

CharacterSet = one byte, Internet Assigned Numbers Authority assigned character set.

UrlLength = one byte unsigned integer, length of the URL in octets.

URL = a field where t~~T~~he format for storing the URL information in the certificate shall be defined as part of the enhanced administrator mechanism.

When the administrator is changed, then the CCM shall also be changed. If there is URL information with the certificate as described in Figure 10 "CCM Message URL storage format", then the new CCM shall be obtained using the URL. If the Administrator certificate was downloaded in a JAR file, the CCM shall be obtained from the same JAR file.

3GPP TSG-T2 #14
Edinburgh, Scotland
3-7 September 2001

T2-010683

CR-Form-v3

CHANGE REQUEST

⌘ **23.057** **CR** **095** ⌘ rev **-** ⌘ Current version: **4.2.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Trust Hierarchy and Administrator RPK
Source:	⌘	T2
Work item code:	⌘	MEXE-ENHANC
Date:	⌘	29-August-2001
Category:	⌘	**F**
Release:	⌘	REL-4

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

Use one of the following releases:

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

Reason for change:	⌘	The presentation of the administrator root public key is disjoint. Part of the information is placed in sub-clauses 8.5.4, 8.6, 8.7, and 8.8. There is no leading information, so the presentation is awkwardly started in sub-clause 8.5.4. The placement in sub-clause 8.5.4 is confusing, since there are 3 domains with a root public key and then there is a fourth root public key that does not fit with the Trust Hierarchy described in sub-clause 8.4.1.
Summary of change:	⌘	Generalized, descriptive information is placed after sub-clause 8.4.1 with references to details in sub-clauses 8.5.4, 8.6, 8.7, and 8.8.
Consequences if not approved:	⌘	If the concepts for the administrator root public key is not adequately introduced, developers, designers, and implementers will implement inconsistent systems.

Clauses affected:	⌘	Sub-clause 8.4
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://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

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

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.

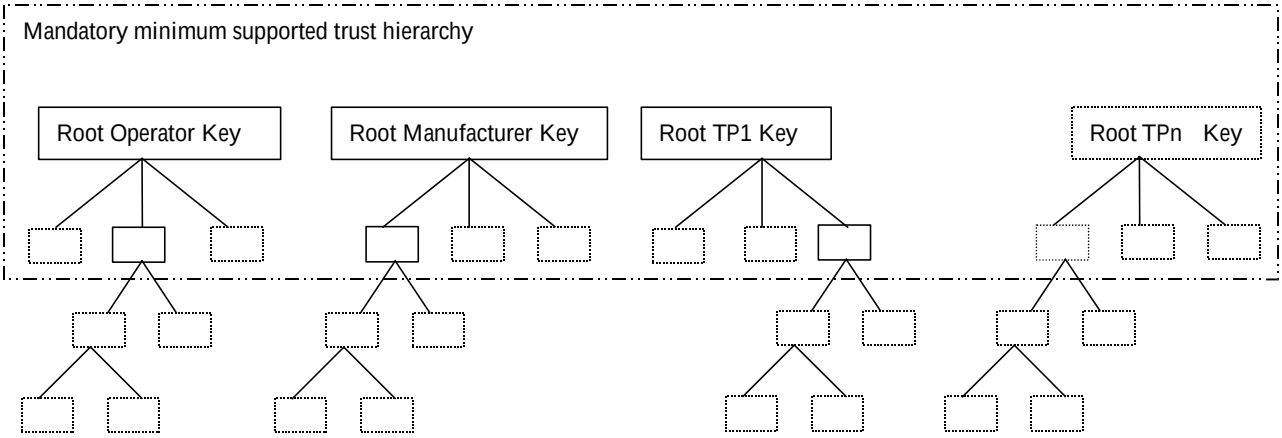


Figure 6: Trust hierarchy

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 subclause 8.5.4 “Administrator root public key”.

This certificate is managed separately from the hierarchy of Figure 6 “Trust Hierarchy” discussed in subclause 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 subclause 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 subclause 8.7 “Certificate configuration message (CCM)”.

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

8.4.~~2~~3 Example certification process

The following processes might be followed in order to securely download a Third Party application to a MExE device.

Root public keys for a number of Certification Authorities (CAs) are installed in the MExE device, along with the MExE device browser, at manufacture. These root public keys can be used to verify certificates for Third Party MExE executables.

1. A third party software developer generates a private and public key pair (or obtains such a pair from a CA).
2. The third party software developer obtains a certificate for the public key from a CA. The certificate contains the developer public key, signed with the private key of the CA.
3. The 3rd party software developer adds all the certificates required in the key chain in the JAR.
4. The MExE device downloads a MExE executable of the third party software developer.
5. The MExE device verifies the certificate using the root public key, contained in the browser, of the relevant CA, and extracts the third party software developer public key and may store it in the certificate store for future use.
6. The MExE device verifies that the MExE executable was signed using the private key corresponding to the third party software developer public key and installs or rejects the MExE executable accordingly.

All downloaded applications shall follow the procedure described in section 8.4.3 "Certificate Chain Verification" in order to verify the application signature and the certificate chain. If the 3 security domains are not supported, the procedure described in the next section is optional.

8.4.~~3~~4 Certificate Chain Verification

3GPP TSG-T2 #14
Edinburgh, Scotland
3-7 September 2001

T2-010684

CR-Form-v3

CHANGE REQUEST

⌘ **23.057** **CR** **096** ⌘ rev **-** ⌘ Current version: **4.2.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	Implementations with Non-persistent Caching of RPKs
Source:	⌘	T2
Work item code:	⌘	MEXE-ENHANC
Date:	⌘	29-August-2001
Category:	⌘	**F**
Release:	⌘	REL-4

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

Use one of the following releases:

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

Reason for change:	⌘	The description for not storing an operator/administrator root public key from the MExE-(U)SIM on the ME is prohibitive of implementations that can still follow the requirements written in TS 22.057.
Summary of change:	⌘	The phrasing in sub-clauses 8.5.1 and 8.5.4 are modified to avoid prohibiting viable implementations that still meet the essential requirements.
Consequences if not approved:	⌘	Prohibiting viable implementations is unnecessary and confusing. These undue constraints lead to the possibilities of inconsistent behaviours in implementations, unless the requirements and functional behaviours are clarified.

Clauses affected:	⌘	Sub-clauses 8.5.1 and 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://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

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

8.5.1 Operator root public key

The ME shall support secure storage for at least one certificate containing an operator root public key. The ME shall support the use and management of a certificate containing an operator root public key stored on the MExE-(U)SIM and in the ME. The ME shall behave according to section 8.5.1.~~2~~1 "ME actions on SIM insertion and/or power up". 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 certificate contains a root public key generated either by the operator, or by a CA trusted by the operator. ~~The ME shall get the operator root public key from the secure area every time it needs to verify a signature, rather than cache the root public key for use in subsequent verifications.~~

If the MExE device does not contain a valid operator root public key, then the certificate chain to MExE executable previously executing in the Operator Domain will be invalid, and the MExE executables will be excluded from the operator domain.

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

Optionally, the operator may install a corresponding disaster-recovery root public key stored in the MExE device, enabling the operator to use a secure mechanism (involving the disaster-recovery key) to replace the certificate containing the standard operator root public key. It shall not be possible to use the disaster recovery operator root public key to replace the standard operator root public key unless both public keys are from the same operator.

There shall be no more than one valid operator root public key on the MExE device (excluding the disaster recovery root public key) at any one time.

An application signed by an operator shall not be able to execute in the Operator Domain unless the root public key of that operator is installed in the MExE device (either ME or MExE-(U)SIM) and is marked as trusted.

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).

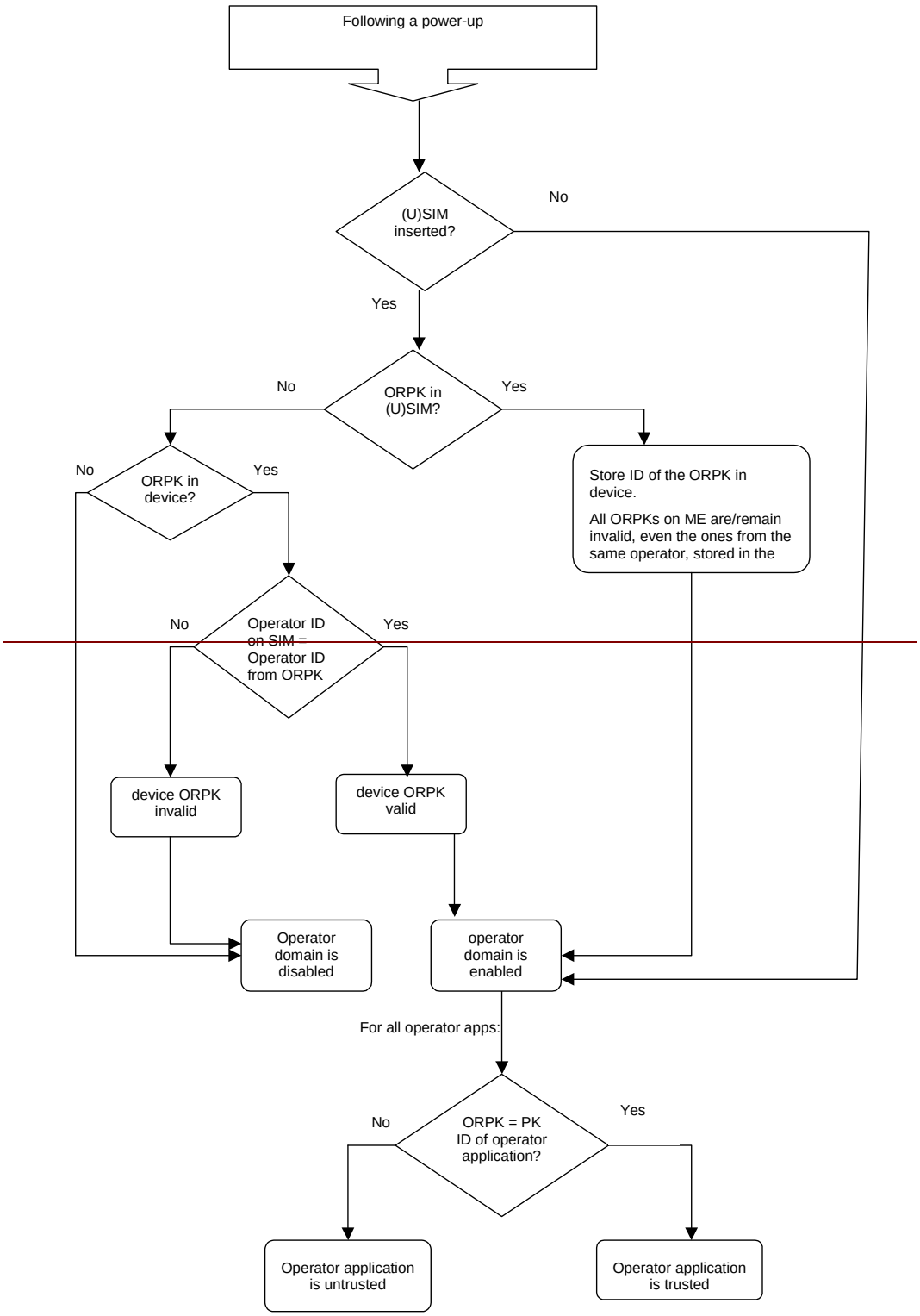
8.5.1.~~2~~1 MExE device actions on detection of valid (U)SIM application and/or power up

This subclause 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 subclause 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.


Following a power-up
(U)SIM inserted?
No
Yes
ORPK in (U)SIM?
No
Yes
ORPK in device?
No
Yes
Store ID of the ORPK in device.
All ORPKs on ME are/remain invalid, even the ones from the same operator, stored in the
Operator ID on SIM = Operator ID from ORPK
No
Yes
device ORPK invalid
device ORPK valid
Operator domain is disabled
operator domain is enabled
For all operator apps:
ORPK = PK ID of operator application?
No
Yes
Operator application is untrusted
Operator application is trusted

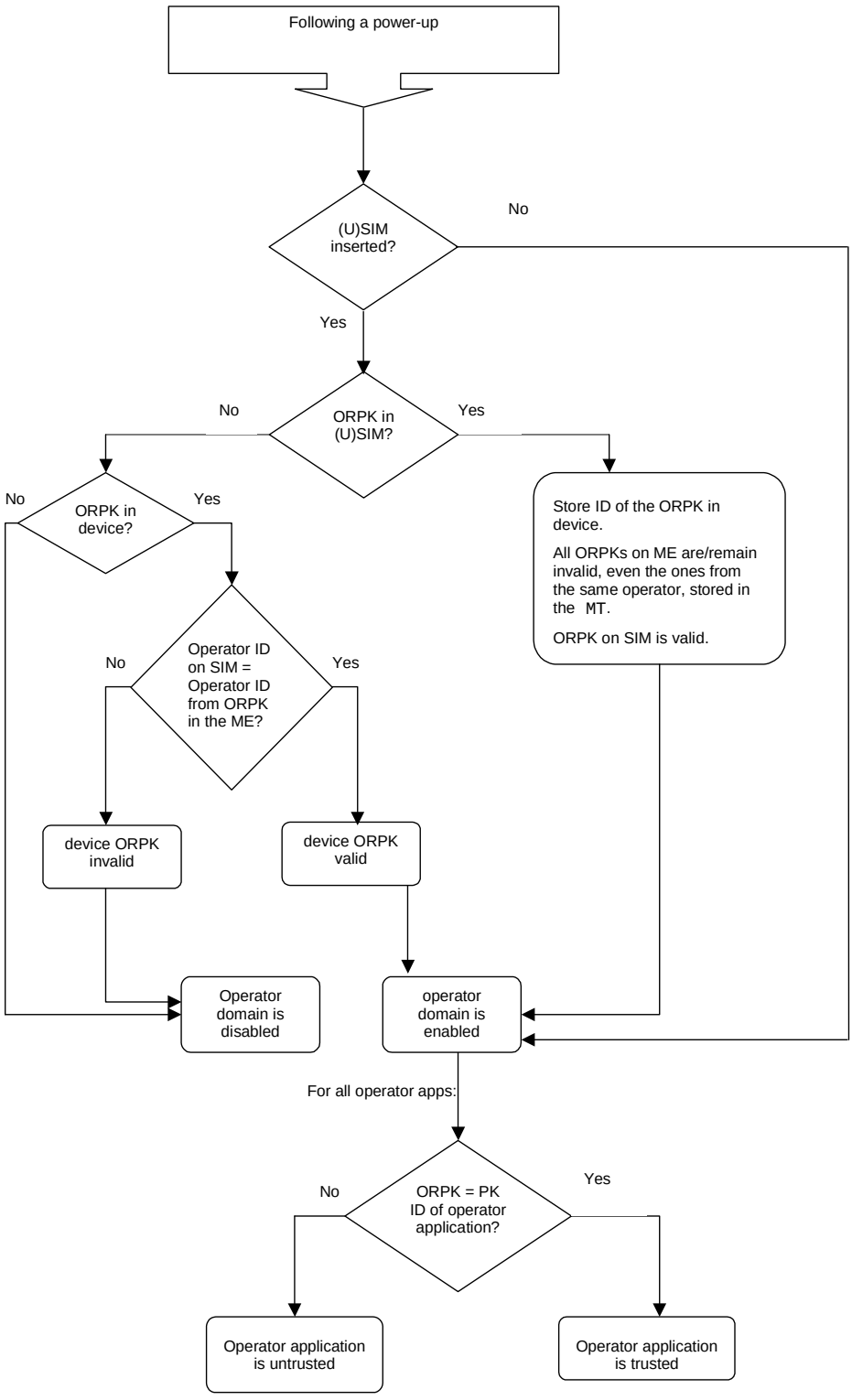


Figure 7: MExE device behaviour on power up

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 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.

8.5.1.32 MExE device actions when a valid (U)SIM application is no longer present

This subclause concerns the status of authenticated applications (i.e. having a certificate chain to a root public key of a secure domain) on identification by the MExE ME that a valid SIM card, or USIM application on the UICC, is no longer present. This could occur, for example, through removal of (U)SIM card, expiry/compromise of the root public key etc.).

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.

If the valid (U)SIM application is no longer present in the MExE device (without another valid (U)SIM application being detected), operator applications shall continue to execute in the operator domain.

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 section 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. Only one administrator root public key shall be valid on the MExE device at any one time.

The MExE device shall support the administrator designation mechanism explained in subclause 8.8 "Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device" and the secure downloading of CCMs explained in subclause 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 subclause 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 subclause 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 subclause 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
Edinburgh, Scotland
3 - 7 September 2001

T2-010689

CR-Form-v3

CHANGE REQUEST

⌘ **23.057 CR 097** ⌘ rev **-** ⌘ Current version: **4.2.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☒ Radio Access Network ☐ Core Network ☐

Title:	⌘	A specified certificate format for MExE
Source:	⌘	T2
Work item code:	⌘	MExE-EHANC
Date:	⌘	04-September-2001
Category:	⌘	**F**
Release:	⌘	REL-4

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

Use one of the following releases:

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

Reason for change:	⌘	The current MExE specification does not contain a specified certificate format that could be used to authenticate downloaded signed content. This will also align MExE with work done in WAP.
Summary of change:	⌘	WAP certificate profile is mandated as the specified MExE certificate format for signed content.
Consequences if not approved:	⌘	The MExE specification will not have a specified certificate format for downloaded signed content.

Clauses affected:	⌘	2, 8.4.1.1, 8.6.1.1
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://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

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

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

[39] 3G TS 31.102: "Universal Mobile Telecommunications System (UMTS); Characteristics of the USIM applications".

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

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

[42] Description of the "JAR Manifest" file encoding, Sun Microsystems. URL: http://java.sun.com/j2se/1.3/docs/guide/jar/jar.html

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

[44] 3GPP TS 21.905: 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications.

[45] WAP Binary XML Content Format Specification (WBXML), http://www.wapforum.org/what/technical.htm

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

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document the following definitions apply:

administrator: The administrator of the MExE device is the entity which has the control of the third party trusted domain, and all resources associated with the domain. The administrator of the MExE device could be the user, the operator, the manufacturer, the service provider, or a third party as designated by the owner of the MExE device.

best effort QoS (Quality of Service): The best effort QoS refers to the lowest of all QoS traffic classes. If the guaranteed QoS cannot be delivered, the bearer network delivers the QoS which can also be called best effort QoS [28].

certificate: An entity that contains the issuer's public key, identification of the issuer, identification of the signer, and possibly other relevant information. Also, a certificate contains a signed hash of the contents. The signer can be a 3rd. party other than the issuer.

delivered QoS: Actual QoS parameter values with which the content was delivered over the lifetime of a QoS session [28].

End Entity: user of PKI certificates and/or end user system that is the subject of a certificate.

fine grain: Refers to the capabilities of the Java security system to allow applications, sections of code or Java classes to be assigned permissions to perform a specific set of privileged operations. The smallest programming element that can be given permission attributes is a Java class [19].

key pair: Key pairs are matching private and public keys. If a block of data is encrypted using the private key, the public key from the pair can be used to decrypt it. The private key is never divulged to any other party, but the public key is available, e.g. in a certificate.

Operator: The term operator as used in this specification refers to the term Home Environment, defined as "Home Environment: The home environment is responsible for enabling a user to obtain UMTS services in a consistent manner regardless of the user's location or terminal used (within the limitations of the serving network and current terminal)" in [44].

8.4 Certification and authorisation architecture

If the 3 MExE security domains defined in subclause 8.1 "Generic security" are not supported, then the certificate and authorisation architecture described in this subclause is optional.

In order to enforce the MExE security framework a MExE device is required to operate an authentication mechanism for verifying downloaded MExE executables. A successful authentication will result in the MExE executable being trusted; and able to be executed in a security domain (as determined by the root public key of its certification tree).

As the MExE device may want to authenticate content from many sources, a public key based solution is mandatory. Before trusting MExE executables, the MExE device will therefore check that the MExE executable was signed with a private key, for which the MExE device has the corresponding public key. The corresponding public key held in the MExE device must either be a root public key (securely installed in the MExE device, e.g. at manufacture) or a signed public key provided in a certificate. The MExE device must be able to verify certificates, i.e. have the public key (as a root key or in a certificate) corresponding to the private key used to sign the certificate. Support of certificate chains is therefore mandatory.

The requirements on authorisation and certification are given in subclause 8.4.1 "Certification requirements". An example authorisation and certification process is described in subclause 8.4.2 "Example certification process".

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” [XZ] together with additional requirements defined in the MExE specification, see section 8.6.1.1 “X509 version 3”.

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

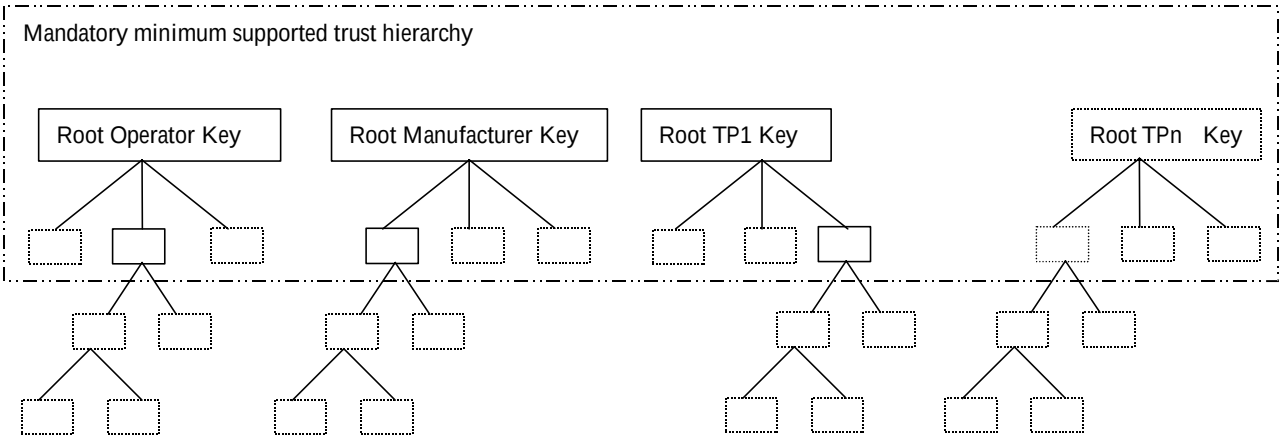


Figure 6: Trust hierarchy

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 Example certification process

The following processes might be followed in order to securely download a Third Party application to a MExE device.

Root public keys for a number of Certification Authorities (CAs) are installed in the MExE device, along with the MExE device browser, at manufacture. These root public keys can be used to verify certificates for Third Party MExE executables.

1. A third party software developer generates a private and public key pair (or obtains such a pair from a CA).
2. The third party software developer obtains a certificate for the public key from a CA. The certificate contains the developer public key, signed with the private key of the CA.
3. The 3rd party software developer adds all the certificates required in the key chain in the JAR.
4. The MExE device downloads a MExE executable of the third party software developer.
5. The MExE device verifies the certificate using the root public key, contained in the browser, of the relevant CA, and extracts the third party software developer public key and may store it in the certificate store for future use.
6. The MExE device verifies that the MExE executable was signed using the private key corresponding to the third party software developer public key and installs or rejects the MExE executable accordingly.

All downloaded applications shall follow the procedure described in section 8.4.3 "Certificate Chain Verification" in order to verify the application signature and the certificate chain. If the 3 security domains are not supported, the procedure described in the next section is optional.

8.6 Certificate management

If the 3 MExE security domains defined in subclause 8.1 "Generic security" are not supported, then the certificate management described in this subclause is optional. The manufacturer may load initial third party certificates on the ME. Downloaded certificates shall be verified by an existing trusted certificate and placed in the domain defined by the root public key at the top of the verification chain for the downloaded certificate.

The administrator root certificate shall be provided on the (U)SIM if support for certificate storage on the (U)SIM exists (e.g. MExE-(U)SIM) or in the MExE device. For (U)SIMs not having certificate storage the administrator root may be downloaded using the root download procedure described in subclause 8.10.4 "Administrator root certificate download mechanism".

The actions that may be performed for a given certificate are:

- addition,
- deletion,
- mark un-trusted (un-trusted certificates cannot be used to verify applications or other certificates. This process may be preferred to certificate deletion as there is a chance that the certificate may become trusted again in the near future),
- mark trusted (marking as trusted is the process of allowing an untrusted certificate to come into use again),
- modify fine grain access permissions (proposed as a future enhancement).

The ability to perform these actions depend on the certificate type being modified as well as the access level of the entity performing the operation.

Users may add a third party certificate as long as it is certified by an existing trusted certificate. Using a provisioned functionality, users may delete Third Party certificates.

The Administrator may mark trusted/untrusted Third-Party certificates using Certificate Configuration Messages (see subclause 8.7 “Certificate configuration message (CCM)”.

Users cannot add or delete any Operator or Manufacturer certificate containing a root public key.

8.6.1 Certificate extension for removal of network access

MExE defines the certificate extension (attribute) " access-Restriction". If the access-Restriction extension is present in a certificate used to verify the signature on a trusted application or in any certificate in the certificate chain used to verify that signature, then the application shall not be permitted the capabilities listed under "network service access" in the security table, (Table 6 "Security domains and actions"). This restriction applies irrespective of any user permission for network service access that may or may not be requested by the application and/or given by the user.

The extension prevents the trusted applications of developers who do not need network service access from writing applications that can perform network service access.

The support of this extension in the operator domain is mandatory. The support of this extension in the manufacturer and third party domains is optional.

The extension is defined for X.509v3 only. Support for WTLS, X9.68 certificate formats is for further study.

8.6.1.1 X.509 version 3

~~If MExE devices support X.509v3 format in operator, manufacturer or third party domains, it~~ The MExE certificate format as specified in section 8.4.1.1~~2~~ shall support the X.509 version 3 access-Restriction extension.

X509 v3 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”.