3GPP TSG-T#12
Stockholm, SWEDEN, 13-15 June 2001

Tdoc TP-010126

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	079		rel-4	Manufacturer RPK	F	4.1.0	4.2.0	T2-010381	MEXE-ENHANC
23.057	080		rel-4	Correction of SIM insert/remove terminology	F	4.1.0	4.2.0	T2-010382	MEXE-ENHANC
23.057	081		rel-4	Administrator mechanism	F	4.1.0	4.2.0	T2-010384	MEXE-ENHANC
23.057	082		rel-4	Clarification of note 10 in table 6	F	4.1.0	4.2.0	T2-010386	MEXE-ENHANC
23.057	083		rel-4	MExE Device Administrator	F	4.1.0	4.2.0	T2-010390	MEXE-ENHANC
23.057	084		rel-4	Quality of Service Support	F	4.1.0	4.2.0	T2-010395	MEXE-ENHANC
23.057	085		rel-4	Administrator Determination Mechanism	F	4.1.0	4.2.0	T2-010397	MEXE-ENHANC
23.057	086		rel-4	Status of applications when valid RPK not available	F	4.1.0	4.2.0	T2-010405	MEXE-ENHANC
23.057	087		rel-4	Executable integrity	F	4.1.0	4.2.0	T2-010406	MEXE-ENHANC
23.057	088		rel-4	Clarifications on call control and signed packages	F	4.1.0	4.2.0	T2-010554	MEXE-ENHANC
23.057	089		rel-4	More Abbreviations	F	4.1.0	4.2.0	T2-010555	MEXE-ENHANC
23.057	090		rel-4	CC/PP Working Group Web Page	F	4.1.0	4.2.0	T2-010556	MEXE-ENHANC
23.057	091		rel-4	Using WBXML when transporting CC/PP over WSP	F	4.1.0	4.2.0	T2-010557	MEXE-ENHANC
23.057	092		rel-4	Clarification of root public keys	F	4.1.0	4.2.0	T2-010558	MEXE-ENHANC
23.057	093		rel-4	Certificate Chain Verification Diagram	F	4.1.0	4.2.0	T2-010408	MEXE-SEC

3GPP TSG-T2 #13
Pusan, Korea
14-18 May 2001

T2-010381

3GPP TSG-T2 SWG1
Whistler Canada
March 27 29,2001

T2-MEXE-010025

CR-Form-v3

CHANGE REQUEST

⌘	**23.057**	**CR**	**079**	⌘	rev	**-**	⌘	Current version:	**4.1.0**	⌘

*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:	⌘	Manufacturer RPK		
Source:	⌘	T2		
Work item code:	⌘	MEXE-ENHANC	***Date:*** ⌘	15.05.2001
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:	⌘	If a valid manufacturer RPK is missing, asociated manufacturer applications should be marked as untrusted. Currently such statement is missing.
Summary of change:	⌘	Addition of the statement that manufacturer applications become untrusted if there is no valid MRPK
Consequences if not approved:	⌘	Possibility to execute invalid executables

Clauses affected:	⌘	8.5.2	
Other specs Affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘
Other comments:	⌘		

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).

3GPP TSG-T2 #13
Pusan, Korea
14-18 May 2001

T2-010382

3GPP TSG-T2 MExE
Whistler, Canada
27th-29th March, 2001

T2-MExE-010035

CR-Form-v3

CHANGE REQUEST

⌘	**23.057**	**CR**	**080**	⌘	rev	**-**	⌘	Current version:	**4.1.0**	⌘

*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:	⌘	Correction of SIM insert/remove terminology			
Source:	⌘	T2			
Work item code:	⌘	MEXE-ENHANC	***Date:***	⌘	15/05/2001
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 specification still refers to "SIM insertion" and "SIM removal" which is not consistent with SIM applications on 3G UICCs. Although SIM cards are supported, the support of (U)SIM applications on the UICC is therefore ambiguous.
Summary of change:	⌘	A definition for "valid (U)SIM application" is added to specifically refer to the detection by the MExE ME of a valid SIM on the SIM card, or USIM application on the UICC (e.g. through insertion of (U)SIM card, power up of MExE device etc.). References to SIM insertion and removal are modified to to be in line with the terminology in the definition. This CR is only aligns terminology and consistently uses 3G terminology.
Consequences if not approved:	⌘	The handling of the USIM insertion/removal events is ambiguous and may lead to differing implementations if not properly clarified.

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

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

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

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

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

3 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.

…other definitions removed to reduce size of CR….

signature: "Signing" is the process of encrypting a hash of the data using a private key. If the signature can be decrypted using the public key, then the signature is valid.

signed JAR file: Archives of Java classes or data that contain signatures that also include a way to identify the signer in the manifest [42]. (The Manifest contains a file which has attributes defined in it.)

subscribed QoS: The network will not grant a QoS greater than that subscribed. The QoS profile subscription parameters are held in the HLR. An end user may have several QoS subscriptions. For security and the prevention of damage to the network, the end user cannot directly modify the QoS subscription profile data [31].

user: The user of the MExE device.

valid (U)SIM application: The 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.). Whenever this specification refers to valid (U)SIM, it implies a valid SIM card or USIM application on the UICC.

Further definitions specific to MExE are given in 3GPP TS 22.057 (MExE stage 1) [2].

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 on the 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 [XY] 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.

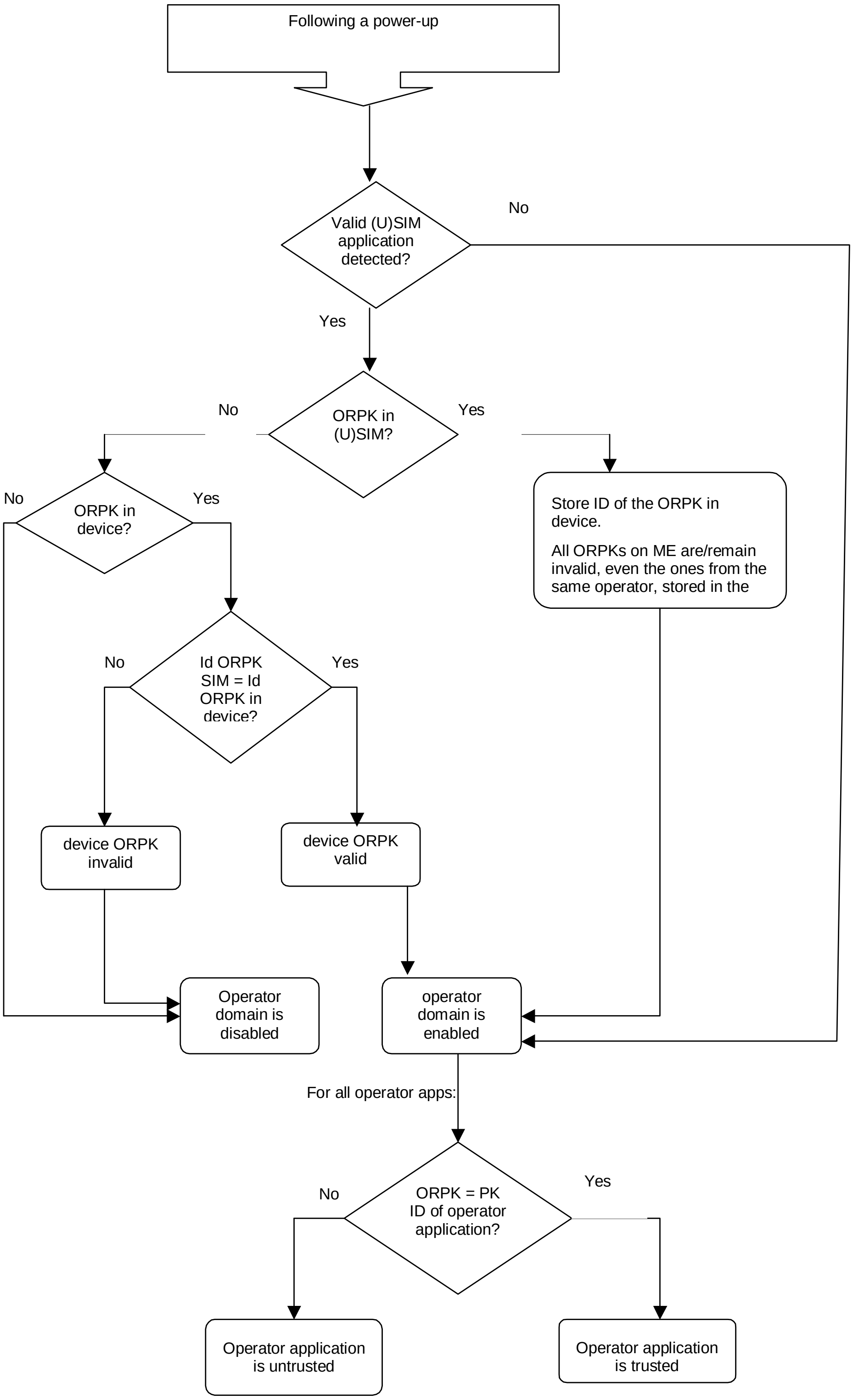
8.5.1.1 MExE device actions on detection of valid (U)SIM application ~~insertion~~ and/or power up~~.~~

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 ~~inserted~~ 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
Valid (U)SIM application detected?
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
Id ORPK SIM = Id ORPK in device?
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

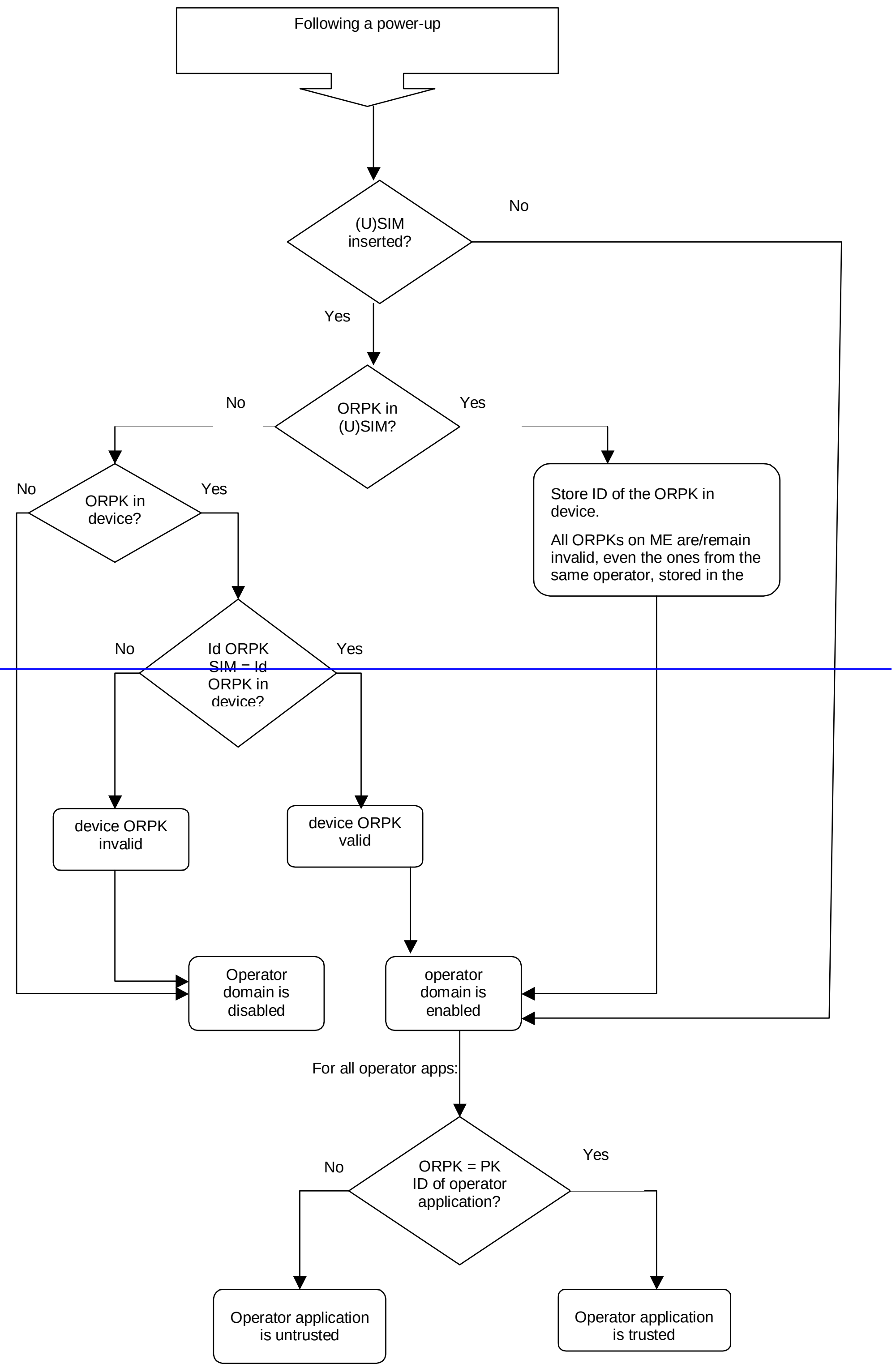

Following a power-up
(U)SIM inserted?
No
Yes
ORPK in (U)SIM?
No
Yes
ORPK in device?
No
Yes
Store ID of the ORPK in device.
All ORPKs on ME are/remain invalid, even the ones from the same operator, stored in the
Id ORPK SIM = Id ORPK in device?
No
Yes
device ORPK invalid
device ORPK valid
Operator domain 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.

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 ~~on removal of the~~ 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 ~~a~~ the valid (U)SIM application is ~~removed from~~ no longer present in the MExE device (without another valid (U)SIM application being ~~inserted~~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.

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 on the 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 [XY] respectively. The ME 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 (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

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 on the 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 [XY] respectively. Only one administrator root public key shall be valid on the MExE MS.

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.

If the Administrator root public key is stored in the (U)SIM, the administrator root public key can be downloaded to the MExE device as described in subclause 8.10.4 "Administrator root certificate download mechanism".

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.

8.8 Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device

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

All applications in the Domain are to be signed by a key which shall be verified back to a Third Party root public key on the MExE device. The Third Party root public keys shall be managed (e.g. addition/mark trusted/mark untrusted) by an administrator that is designated by the owner of the MExE device using the MExE administrator provisioning mechanism. A mechanism is required to be provided to enable the owner of the MExE device to dynamically assign an administrator. The mechanism shall support the following cases:

- the user is the owner;

- the owner is at a remote location. In this case the owner could be the operator, a service provider or a third party;

- the owner of the MExE-(U)SIM wants to be a temporary administrator.

8.8.1 Determining the administrator of the MExE device

The administrator of the MExE device shall be determined by the logical process shown in the flowchart in Figure 11 "MExE Release 98 administrator mechanism". During power-up the provisioned mechanism shall look for an administrator root public key that is stored on the MExE device.

- Administrator root public key is absent

  if the administrator root public key is absent, then the user shall automatically become the administrator of the MExE device.

- administrator root public key is present

  if an administrator root public key is present, this root public key shall be used for all remote administration authentication, implying that the owner of the administrator root public key is the administrator.

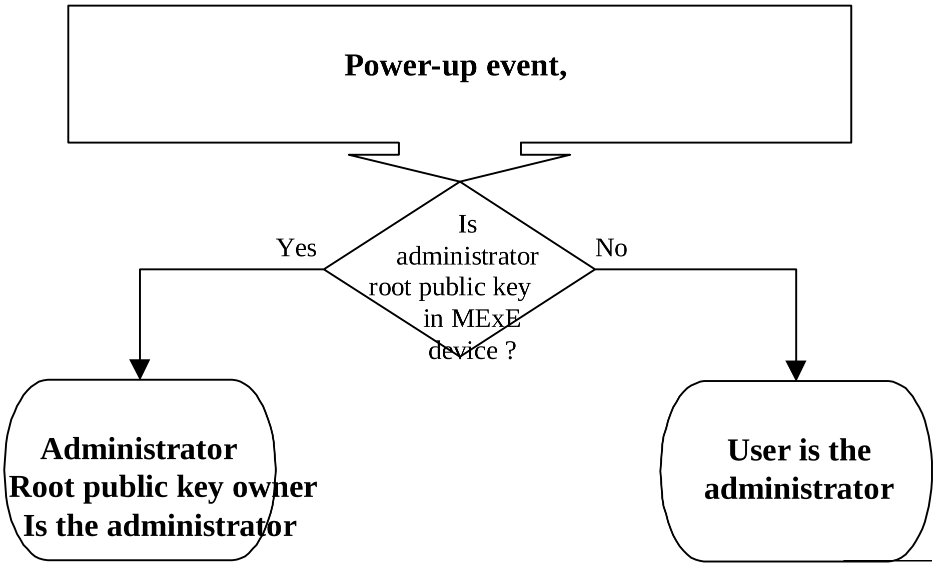

Power-up event,
Yes
Is administrator root public key in MExE device ?
No
Administrator Root public key owner Is the administrator
User is the administrator

Figure 11: MExE Release 98 administrator mechanism

The rest of the mechanism is subsequently defined, however it is a future release implementation, see Figure 12 "Enhanced administrator mechanism". This future enhanced administrator Mechanism shall be initiated after a power-up event is processed or when a MExE-(U)SIM is detected.

(The following subclauses assume that Third Party certificates can be added using the MExE-(U)SIM, however Third Party certificates may be added using a non-(U)SIM approach.)

8.8.1.1 Administrator of the MExE device is the user

If the administrator is the user, then a check shall be made to determine whether there is a MExE-(U)SIM. If a MExE-(U)SIM is present, then a check shall then be made to determine whether there is a certificate in the MExE-(U)SIM. The enhanced administrator Mechanism shall allow the MExE device to determine (via a format) what type of certificate is present:

- certificate present - third party (CP-TP)

  A certificate present in the MExE-(U)SIM shall be considered by the MExE device as a Third Party certificate, whilst that valid MExE-(U)SIM application is ~~inserted~~ present in the MExE device. The user shall be queried to allow or disallow the certificate as a Third Party.

- certificate present - administrator (CP-Admin)

  If a temporary certificate is present in the MExE-(U)SIM, the user shall be queried whether to allow the certificate on the MExE-(U)SIM to take temporary control of the third party domain. By temporary control, it is meant that once the card is removed the administrator reverts back to the user administrator settings. The above mechanism implies that the previous configuration settings for the administrator shall be saved, so that they may be restored. If the user disallows the MExE-(U)SIM certificate, the Third Party Domain shall not be able to use any of the network capabilities in the third party domain as identified in the network access section of the security Table 6 "Security domains and actions".

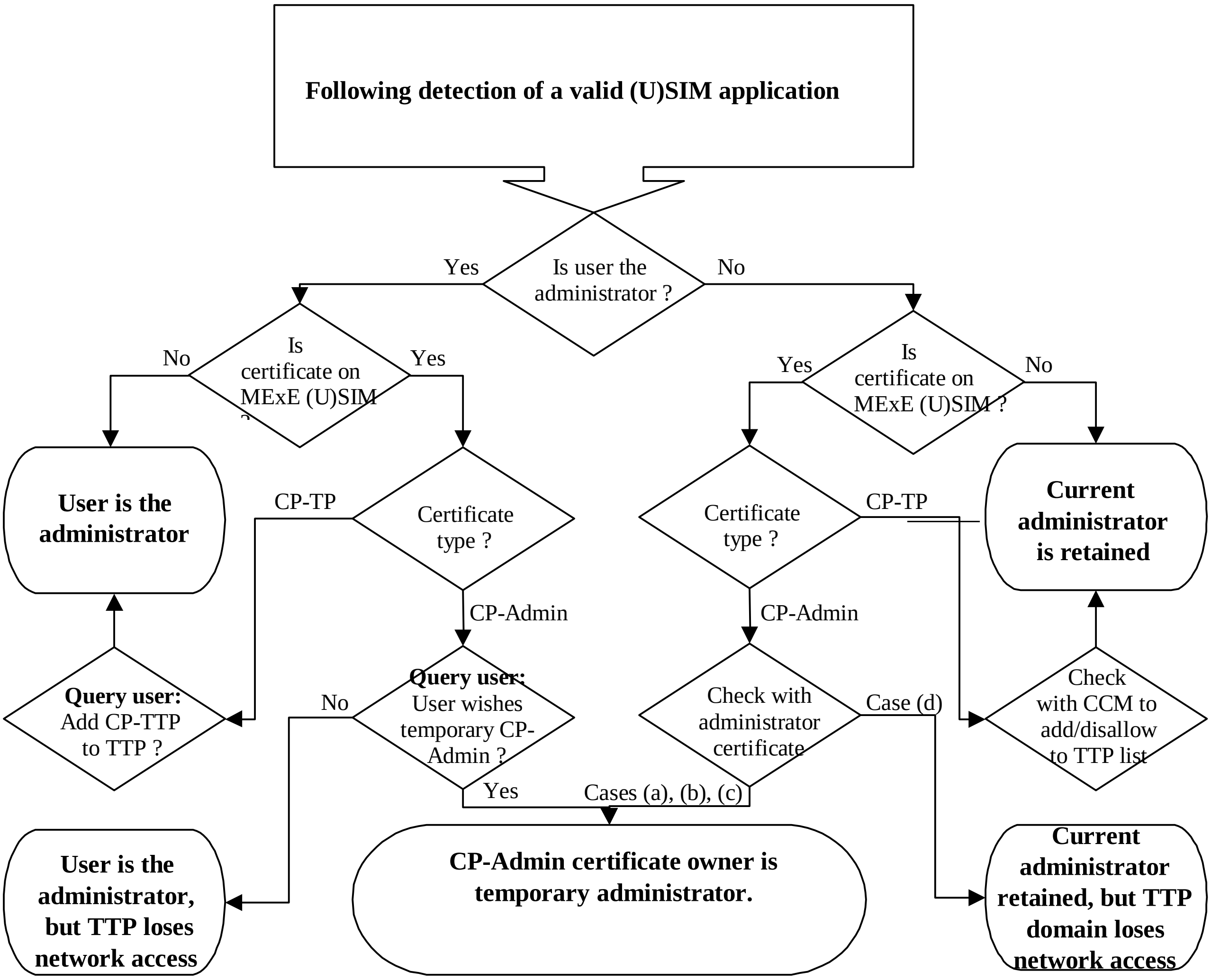
If a certificate is not present on the MExE-(U)SIM and the administrator is the user, the user shall continue to be the administrator and may make use of all functionality.

8.8.1.2 Administrator of the MExE device is not the user

If the administrator is not the user, then a check is made to determine if there is a MExE-(U)SIM. If a MExE-(U)SIM is present, then a check is made to see if there is a certificate in the MExE-(U)SIM. If a certificate is present in the MExE-(U)SIM, then a comparison is made of the certificate’s root public key on the MExE-(U)SIM with the root public key on the MExE device for the following cases:

- Case (a): they are the same;
- Case (b): they are not the same, but the MExE device certificate is cross-certified with the MExE-(U)SIM certificate (a cross-certificate exists on the MExE device);
- Case (c): they are not the same, but the MExE device certificate has a line of trust back to the MExE-(U)SIM certificate domain;
- Case (d): they are not the same.

If the owner of the public key in the certificate on the MExE-(U)SIM is to be a temporary administrator (CP-Admin), then in cases (a), (b) and (c), the temporary administrator shall be the owner of the CP-Admin root public key. In case (d), the Third Party domain shall not use any of the network capabilities in the third party domain as identified in the network access section of the security Table 6 "Security domains and actions". If the certificate is to be a Third Party, then the certificate (CP-TP) shall be verified with the CCM and based on the content and permissions of the CCM, the certificate shall be added to the Third Party list or rejected.


Following detection of a valid (U)SIM application
Is user the administrator ?
Yes
No
Is certificate on MExE (U)SIM ?
No
Yes
Is certificate on MExE (U)SIM ?
Yes
No
User is the administrator
Certificate type ?
CP-TP
CP-Admin
Certificate type ?
CP-TP
CP-Admin
Current administrator is retained
Query user: Add CP-TTP to TTP ?
Query user: User wishes temporary CP-Admin ?
No
Yes
Check with administrator certificate
Case (d)
Cases (a), (b), (c)
Check with CCM to add/disallow to TTP list
User is the administrator, but TTP loses network access
CP-Admin certificate owner is temporary administrator.
Current administrator retained, but TTP domain loses network access

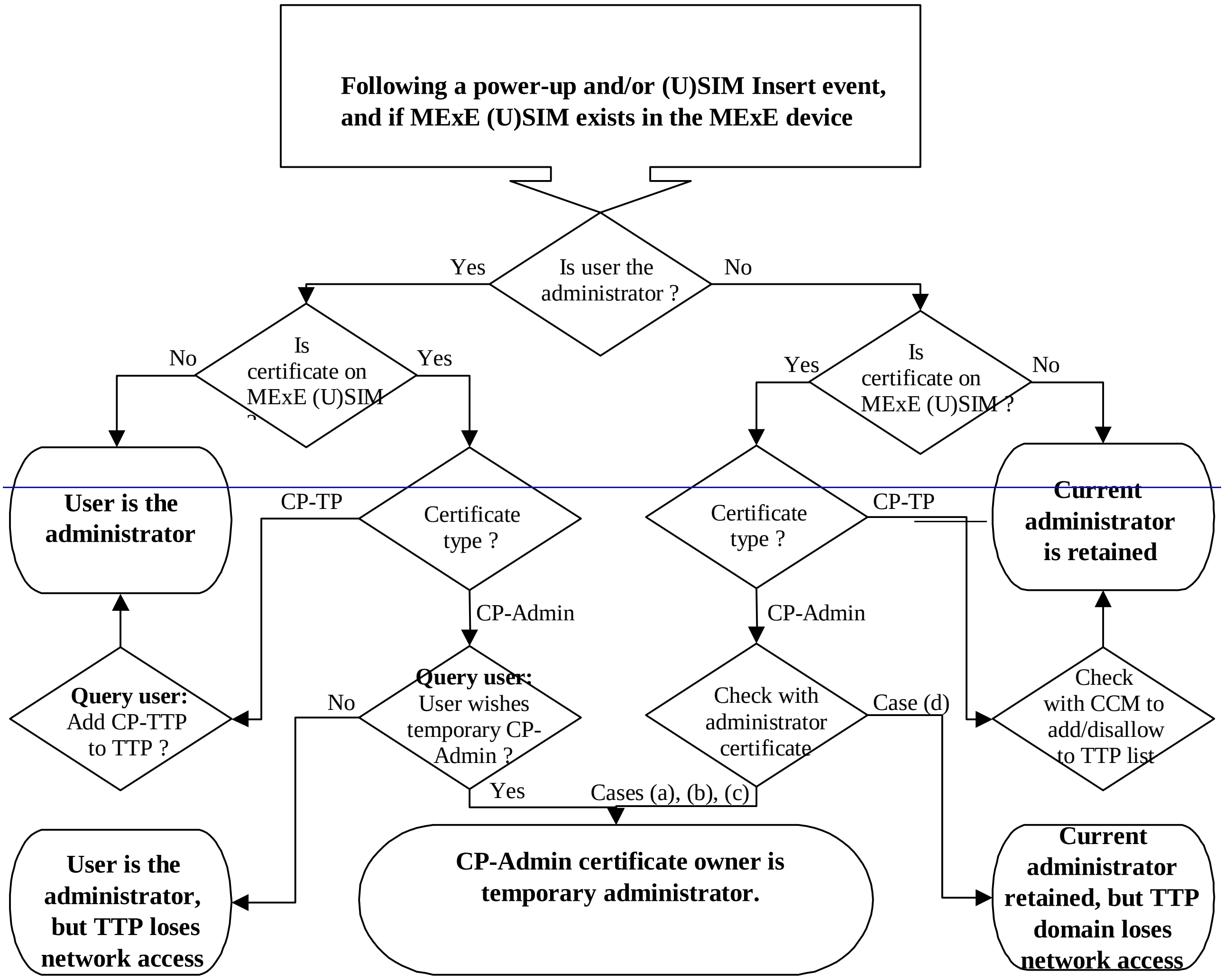

Following a power-up and/or (U)SIM Insert event, and if MExE (U)SIM exists in the MExE device
Is user the administrator ?
Yes
No
Is certificate on MExE (U)SIM ?
No
Yes
Is certificate on MExE (U)SIM ?
Yes
No
User is the administrator
Certificate type ?
CP-TP
CP-Admin
Certificate type ?
CP-TP
CP-Admin
Current administrator is retained
Query user: Add CP-TTP to TTP ?
Query user: User wishes temporary CP-Admin ?
No
Yes
Check with administrator certificate
Case (d)
Cases (a), (b), (c)
Check with CCM to add/disallow to TTP list
User is the administrator, but TTP loses network access
CP-Admin certificate owner is temporary administrator.
Current administrator retained, but TTP domain loses network access

Figure 12: Enhanced administrator mechanism

3GPP TSG-T2 #13
Pusan, Korea
14-18 May 2001

T2-010384

3GPP TSG-T2 MExE
Whistler, Canada
March 27th - March 29th 2001

T2-010042

CR-Form-v3

CHANGE REQUEST

⌘	**23.057**	**CR**	**081**	⌘	rev	**-**	⌘	Current version:	**4.1.0**	⌘

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:	⌘	Administrator mechanism		
Source:	⌘	T2		
Work item code:	⌘	MEXE-ENHANC	***Date:*** ⌘	15/05/2001
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 administrator mechanism requires to be updated to reflect the fact that MExE (U)SIM may now contain administrator certificates. The currently described mechanism originates from the date when it was presumed that they the administrator certificate could not be carried on the MExE-(U)SIM, and still refers back to Release 98.
Summary of change:	⌘	The mechanism is still retained in two parts. The first part is clarified to determine who the administrator of the MExE device is, by now first checking the MExE-(U)SIM, and secondly checking the MExE device. The text is also cleaned up to remove references to some "future mechanism" as it is now supportable with MExE-(U)SIMs carrying certificates. Note that corrections to terminology (i.e. SIM, MExE ME) are corrected in a different CR.
Consequences if not approved:	⌘	The current ambiguous text may lead inconsistent implementations

Clauses affected:	⌘		
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.

8.8.1 MExE administrator d~~D~~etermin~~in~~ation~~g~~ mechanism~~the administrator of the MExE device~~

The administrator of the MExE device shall be determined by ~~the~~ a two part logical process with the first part shown in the flowchart in Figure 11 "MExE ~~Release 98~~ administrator determination mechanism". The second part of the logical process is in Figure 12 "MExE administrator determination mechanism, for MExE-(U)SIM supporting third party certificates".

During power-up or MExE-(U)SIM insertion event, the provisioned mechanism shall look for an administrator root public key that is stored on the MExE-(U)SIM.

8.8.1.1 Determining the administrator of the MExE device

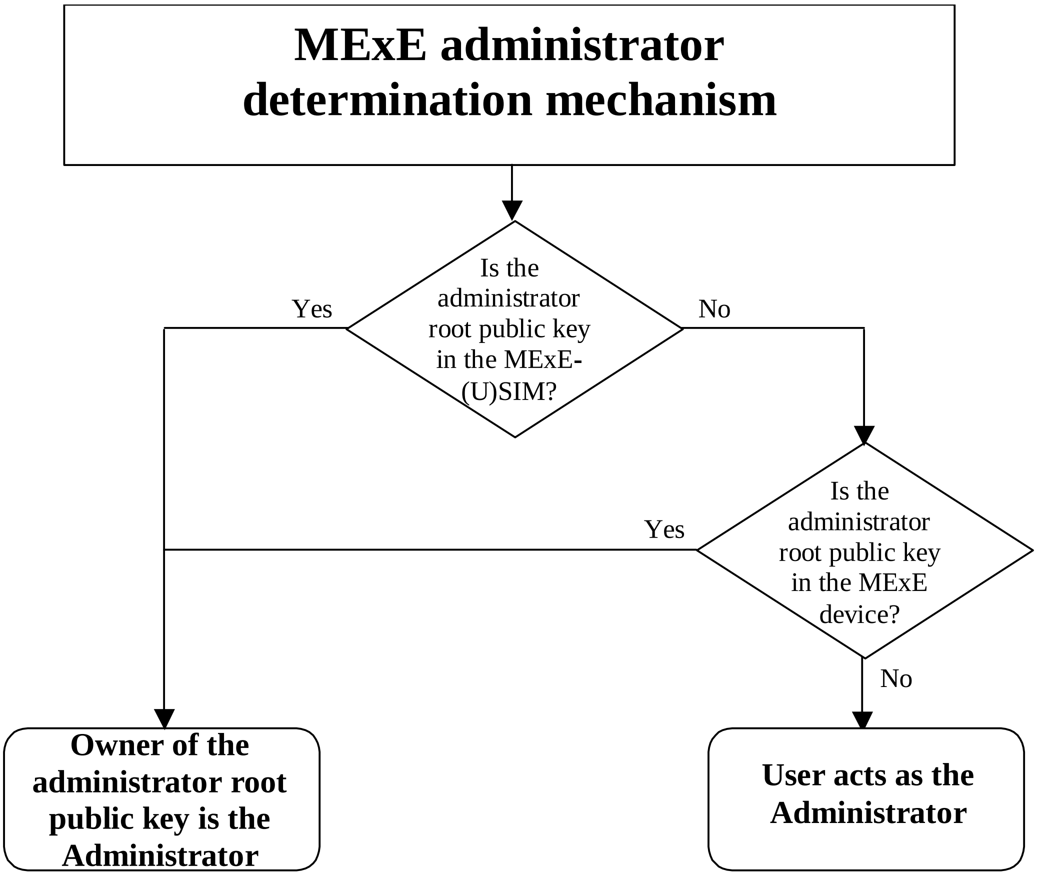
~~During power-up the provisioned mechanism shall look for an administrator root public key that is stored on the~~ If an administrator root public key cannot be found on the MExE-(U)SIM, the provisioned mechanism shall look for one on the MExE device. This leads to the following two cases: ~~MExE device.~~

- ~~Administrator~~ administrator root public key is absent

  if the administrator root public key is absent, then the user shall automatically become the administrator of the MExE device.

- administrator root public key is present

  if an administrator root public key is present, this root public key shall be used for all remote administration authentication, implying that the owner of the administrator root public key is the administrator. Note that the owner of the administrator root public key could be the user.


MExE administrator determination mechanism
Is the administrator root public key in the MExE-(U)SIM?
Yes
No
Is the administrator root public key in the MExE device?
Yes
No
Owner of the administrator root public key is the Administrator
User acts as the Administrator

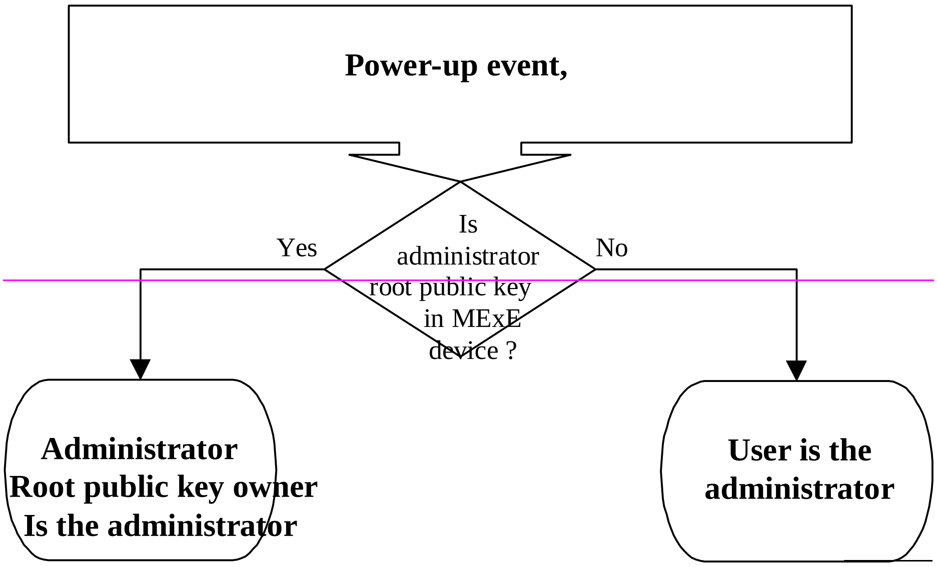

Power-up event,
Is administrator root public key in MExE device ?
Yes
No
Administrator Root public key owner Is the administrator
User is the administrator

Figure 11: MExE ~~Release 98~~ administrator determination mechanism

8.8.1.2 Determining the administrator of the MExE device, for MExE-(U)SIM supporting third party certificates

The ~~rest~~ second part of the administrator determination mechanism is subsequently defined~~, however it is a future release implementation,(~~ see Figure 12 "~~Enhanced~~ MExE administrator mechanism, for MExE-(U)SIM supporting third party certificates")~~. This future enhanced administrator Mechanism~~ and shall be initiated after a power-up or MExE-(U)SIM insertion event is processed ~~or when a MExE (U)SIM is detected~~.

~~(~~The following subclauses 8.8.1.2.1 "Administrator of the MExE device is the user" and 8.8.1.2.2 "Administrator of the MExE device is not the user" assume that Third Party certificates can be added using the MExE-(U)SIM, however Third Party certificates may be added using a non-(U)SIM approach~~.~~(e.g. inserted at the time of manufacture, signed package download etc.).

8.8.1.2.1 Administrator of the MExE device is the user

If the administrator is the user, then a check shall be made to determine whether there is a MExE-(U)SIM. If a MExE-(U)SIM is present, then a check shall then be made to determine whether there is a certificate in the MExE-(U)SIM. The ~~enhanced~~ second part of the administrator determination ~~M~~mechanism shall allow the MExE device to determine (via a format) what type of certificate is present:

- certificate present - third party (CP-TP)

  A certificate present in the MExE-(U)SIM shall be considered by the MExE device as a Third Party certificate, whilst that MExE-(U)SIM is inserted in the MExE device. The user shall be queried to allow or disallow the certificate as a Third Party.

- certificate present - administrator (CP-Admin)

  If a temporary certificate is present in the MExE-(U)SIM, the user shall be queried whether to allow the certificate on the MExE-(U)SIM to take temporary control of the third party domain. By temporary control, it is meant that once the card is removed the administrator reverts back to the user administrator settings. The above mechanism implies that the previous configuration settings for the administrator shall be saved, so that they may be restored. If the user disallows the MExE-(U)SIM certificate, the Third Party Domain shall not be able to use any of the network capabilities in the third party domain as identified in the network access section of the security Table 6 "Security domains and actions".

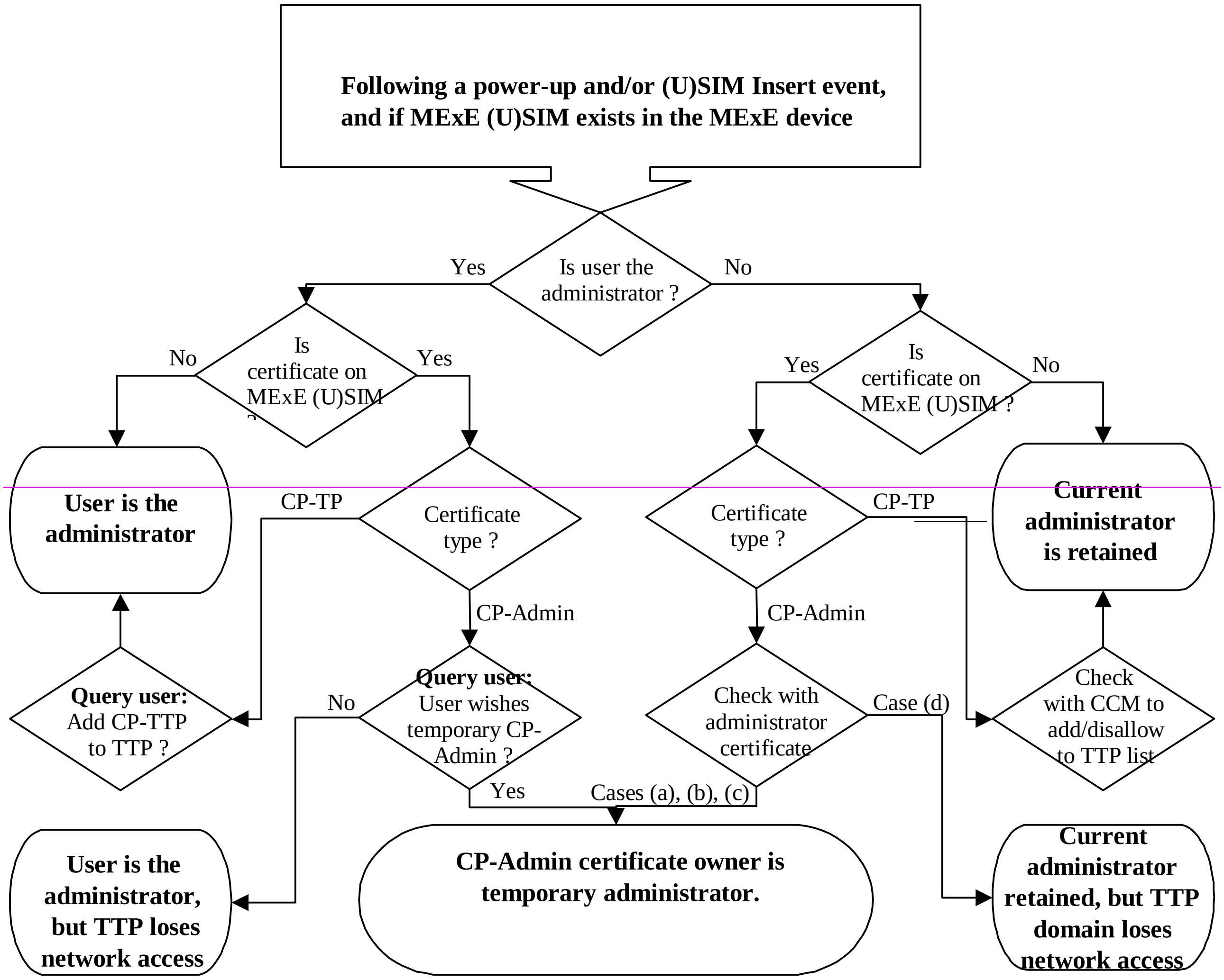
If an administrator certificate is not present on the MExE-(U)SIM and the administrator is the user, the user shall continue to be the administrator and may make use of all functionality.

8.8.1.2.2 Administrator of the MExE device is not the user

If the administrator is not the user, then a check is made to determine if there is a MExE-(U)SIM. If a MExE-(U)SIM is present, then a check is made to see if there is a certificate in the MExE-(U)SIM. If a certificate is present in the MExE-(U)SIM, then a comparison is made of the certificate's root public key on the MExE-(U)SIM with the root public key on the MExE device for the following cases:

- Case (a): they are the same;
- Case (b): they are not the same, but the MExE device certificate is cross-certified with the MExE-(U)SIM certificate (a cross-certificate exists on the MExE device);
- Case (c): they are not the same, but the MExE device certificate has a line of trust back to the MExE-(U)SIM certificate domain;
- Case (d): they are not the same.

If the owner of the public key in the certificate on the MExE-(U)SIM is to be a temporary administrator (CP-Admin), then in cases (a), (b) and (c), the temporary administrator shall be the owner of the CP-Admin root public key. In case (d), the Third Party domain shall not use any of the network capabilities in the third party domain as identified in the network access section of the security Table 6 "Security domains and actions". If the certificate is to be a Third Party, then the certificate (CP-TP) shall be verified with the CCM and based on the content and permissions of the CCM, the certificate shall be added to the Third Party list or rejected.


Following a power-up and/or (U)SIM Insert event, and if MExE (U)SIM exists in the MExE device
Is user the administrator ?
Yes
No
Is certificate on MExE (U)SIM ?
No
Yes
Is certificate on MExE (U)SIM ?
Yes
No
User is the administrator
Certificate type ?
CP-TP
CP-Admin
Certificate type ?
CP-TP
CP-Admin
Current administrator is retained
Query user: Add CP-TTP to TTP ?
Query user: User wishes temporary CP-Admin ?
No
Yes
Check with administrator certificate
Case (d)
Cases (a), (b), (c)
Check with CCM to add/disallow to TTP list
User is the administrator, but TTP loses network access
CP-Admin certificate owner is temporary administrator.
Current administrator retained, but TTP domain loses network access

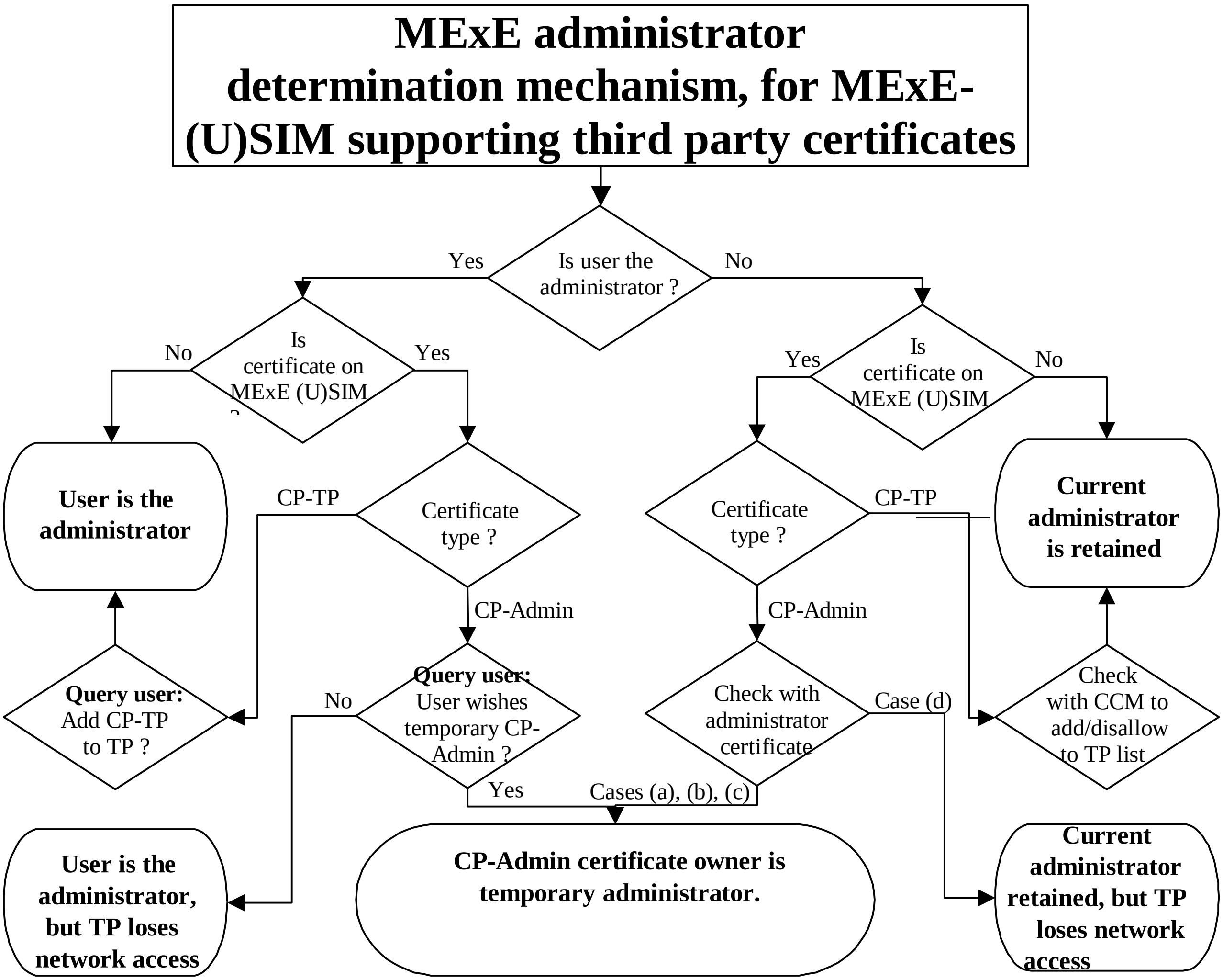

MExE administrator determination mechanism, for MExE-(U)SIM supporting third party certificates
Is user the administrator ?
Yes
No
Is certificate on MExE (U)SIM ?
No
Yes
Is certificate on MExE (U)SIM
Yes
No
User is the administrator
CP-TP
Certificate type ?
Certificate type ?
CP-TP
Current administrator is retained
CP-Admin
CP-Admin
Query user: Add CP-TP to TP ?
No
Query user: User wishes temporary CP-Admin ?
Check with administrator certificate
Case (d)
Check with CCM to add/disallow to TP list
Yes
Cases (a), (b), (c)
User is the administrator, but TP loses network access
CP-Admin certificate owner is temporary administrator.
Current administrator retained, but TP loses network access

Figure 12: MExE ~~Enhanced~~ administrator determination mechanism, for MExE-(U)SIM supporting third party certificates

3GPP TSG-T2 #13
Pusan, Korea
14-18 May 2001

T2-010386

3GPP TSG-T2 /ETSI SMG4
Whistler, Canada
272th - 29th March 2001

T2-MExE-010046

CR-Form-v3

CHANGE REQUEST

⌘	**23.057**	**CR**	**082**	⌘	rev	**-**	⌘	Current version:	**4.1.0**	⌘

*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:	⌘	Clarification of note 10 in table 6		
Source:	⌘	T2		
Work item code:	⌘	MEXE-ENHANC	***Date:*** ⌘	2001-05-15
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 requirement is unclear.
Summary of change:	⌘	Text in note changed to “Access request **requires** no user permission.” (the word "requires" is missing).
Consequences if not approved:	⌘	The text is ambigious.

Clauses affected:	⌘	8.2.1		
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://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.

8.2.1 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 subclause 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 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 1. Start/stop radio 2. Turn on/off device 3. Write time and/or date 4. Activate a user profile 5. 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] 1. Send APDU **2.** 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 1. Run algorithm **2.** Verify CHV/2 or UNBLOCK CHV/2 **3.** Activate/deactivate CHV **4.** Modify CHV/2	No		
Network property access 1. Get IMSI 2. Get home network 3. Select network	Yes	No	
Network services access 1. Initiate a voice/data connection [3] 2. Accept a voice/data connection [3] 3. Call forward [4] 4. Multiparty call [4] 5. Call deflection [4] 6. Explicit call transfer [4] 7. Terminate an existing connection 8. Hold an existing connection 9. Resume an existing connection 10. Send point-point message (e.g. SMS, USSD) [4] 11. Generate DTMF 12. Query network status 13. Get signal level 14. Get call list 15. 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 subclause 8.8.1 "Determining the administrator of the MExE device"*			

	MExE Security Domains		
Actions	**Operator**	**Manufacturer**	**Third Party**
User private data access [1]			
1. Read	Yes[2]		
2. Write	Yes[2]		
3. Get properties	Yes[2]		
4. Delete	Yes[2]		
5. Get Location Information	Yes[2]		
6. Read stored SMS	Yes[2]		
7. Delete stored SMS	Yes[2]		
8. Modify user preferences	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.*			
MExE security functions access			
1. Install a certificate for a given domain	Yes [5]		
2. Uninstall a certificate for a given domain	Yes [5]		
3. Replace a certificate for a given domain	Yes [5]		
4. Data encryption API			
5. Verify a signature API	Yes		
6. Compute a digital signature API	Yes		
7. Hash a content API	Yes		
8. Non repudiation API	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			
1. Get application list	Yes[8]		
2. Launch an application	Yes[8]		
3. Get application status	Yes[8]		
4. 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		
1. Install a MExE Executable			
2. Uninstall a MExE executable			
Terminal data access			
1. Get manufacturer software version	Yes		
2. Read time and date	Yes		

	MExE Security Domains		
Actions	**Operator**	**Manufacturer**	**Third Party**
Peripheral access 1. Sound generation to speaker (e.g. via stream) 2. Set speaker volume 3. printer access 4. Monitor the power state 5. Change the power state **6.** Activate/ access Serial port (RS232, IrDA, Bluetooth, USB …) access **7.** Activate/access Parallel port 8. Activate/access Smart card other than (U)SIM card (Send APDU, Slot management)	Yes		
Input output User interface access 1. Input device (keyboard, mouse …) **2.** Output device (display) **3.** Output notification device(smart icon, sound, light, vibrator …)	 Yes[10] Yes[10] Yes		
[10] – *Access request requires no user permission.*			

The lists in the groups in Table 6 "Security domains and actions" are not exhaustive, and other actions which are of the same category shall be included in the group for the purposes of requesting user permission.

This subclause identifies the permissions for MExE executables in the 3 security domains (operator, manufacturer and Third Party). The permissions do not apply to untrusted MExE executables which are not permitted to execute within the domains.

3GPP TSG-T2 #13
Pusan, KOREA
14-18 May 2001

T2-010390

CR-Form-v3

CHANGE REQUEST

⌘	**23.057**	**CR**	**083**	⌘	rev	**-**	⌘	Current version:	**4.1.0** ⌘

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

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

Title:	⌘	MExE Device Administrator		
Source:	⌘	T2		
Work item code:	⌘	MEXE-ENHANC	***Date:*** ⌘	15-May-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 specific role of the MExE device Administrator with regards to third-party certificates is not always clear in the specification.
Summary of change:	⌘	This CR proposes several small editorial modifications to help clarifying the relationship between the Administrator and the Third-Party certificates.
Consequences if not approved:	⌘	Misunderstanding of the MExE Administrator role.

Clauses affected:	⌘	Sub-clause 8.5.3, 8.5.4, 8.6 and 8.8	
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.

8.5.3 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, ~~T~~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.

8.6 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.~~

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.

8.8 Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device

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

All applications in the Third-Party security d~~D~~omain are to be signed by a key which shall be verified back to a Third Party root public key on the MExE device. The Third Party root public keys shall be managed (e.g. addition/mark trusted/mark untrusted) by an administrator that is designated by the owner of the MExE device using the MExE administrator provisioning mechanism. A mechanism is required to be provided to enable the owner of the MExE device to dynamically assign an administrator. The mechanism shall support the following cases:

- the user is the owner;
- the owner is at a remote location. In this case the owner could be the operator, a service provider or a third party;
- the owner of the MExE-(U)SIM wants to be a temporary administrator.

3GPP TSG-T2 #13
Pusan, KOREA
14-18 May 2001

T2-010395

CR-Form-v3

CHANGE REQUEST

⌘	**23.057**	**CR**	**084**	⌘	rev	**-**	⌘	Current version:	**4.1.0** ⌘

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:	⌘	Quality of Service Support		
Source:	⌘	T2		
Work item code:	⌘	MEXE-ENHANC	***Date:*** ⌘	15-May-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 a contradiction between section 4.13 and section 9 about the optionality of QoS support in MExE device.
Summary of change:	⌘	Aligned content of 4.13 with section 9. Added a cross-reference to section 9 in 4.13.
Consequences if not approved:	⌘	Possible confusion about QoS support in MExE .

Clauses affected:	⌘	Sub-clause 4.13
Other specs affected:	⌘	□ Other core specifications ⌘ □ Test specifications □ O&M Specifications
Other comments:	⌘	Ideally, section 4.13 should only contain a reference to section 9.

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.

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, ~~T~~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.

~~For MExE devices supporting bearers defined by QoS, the MExE execution environment shall support QoS management.~~ 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.

9 Quality of Service

Support of quality of service for MExE devices supporting bearers defined by QoS as defined in this subclause is optional.

QoS aware MExE executables may be executing on the MExE device. To ensure correct operation with the QoS provisioning of the bearer network(s) the associated API's and the MExE QoS manager shall be supported by MExE device supporting bearers defined by QoS – see Figure 14 "Logical MExE device QoS manager elements". Non QoS aware MExE executables shall operate with the defined QoS by the user or the network.

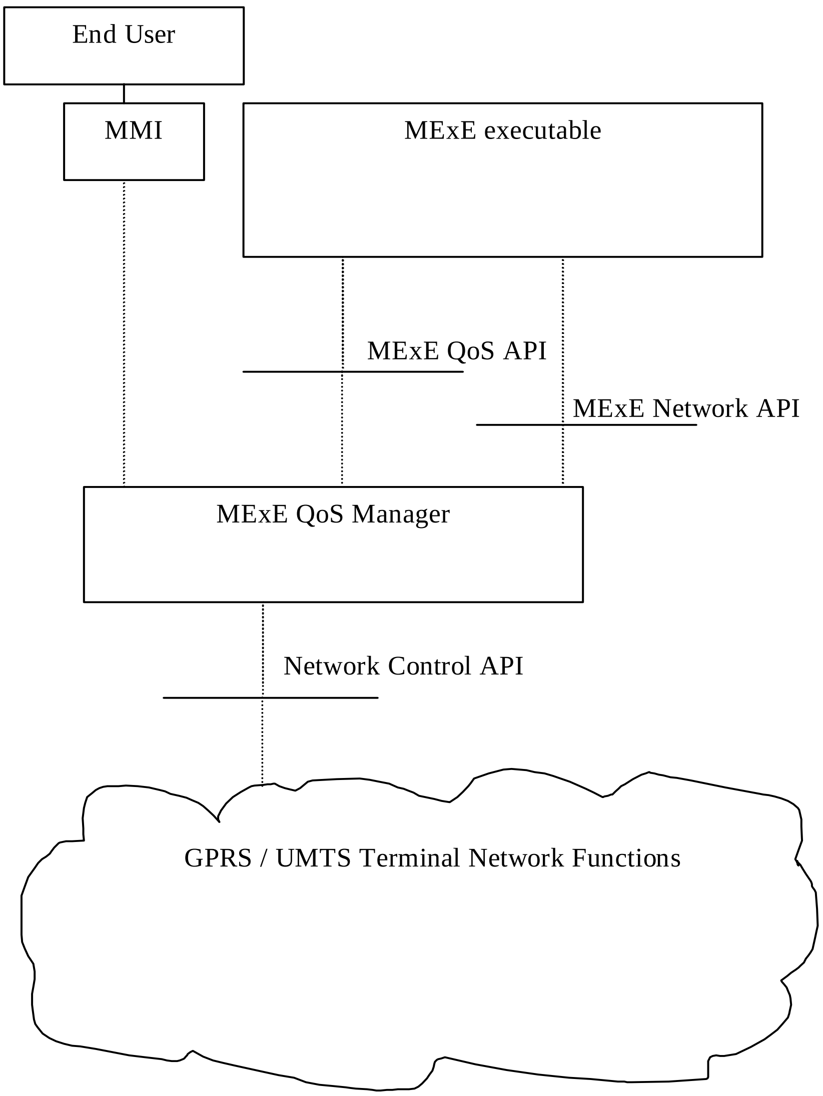


Figure 14: Logical MExE device QoS manager elements

9.1 MExE QoS support

In the logical architecture depicted in Figure 14 "Logical MExE device QoS manager elements", a conceptual entity, a MExE QoS manager exists between the MExE executable and the Network Control API. A QoS API for MExE executables is provided and an API to the network is provided. The MExE QoS functions accommodate standard methods of end to end QoS provisioning.

For a MExE device supporting bearers defined by QoS, it is recommended that the MExE device shall support the following basic QoS operations:

- The end user should be able to manage the QoS directly via the MMI.

For MExE devices supporting bearers defined by QoS, the MExE device shall optionally support the following basic QoS operations:

- a mapping between the QoS requirements of the MExE executable and the network layer;
- MExE executables shall be able to indicate and interpret QoS values of the network via the MExE QoS Manager;
- MExE executables shall be able to modify the QoS dynamically;

- MExE executables shall be able to react to changes in the provided QoS;

MExE introduces two new elements to cater for QoS – the MExE QoS manager and the QoS API. The MExE QoS manager shall handle the fact that the network may not have QoS capabilities.

9.2 MExE QoS manager

As a conceptual entity, the MExE QoS manager is responsible for:

- Managing the QoS streams for MExE executables;
- Notification of the negotiated and delivered QoS to the end user / MExE executable.

The MExE QoS manager shall support the MExE QoS API according to the bearer supported by the MExE device, and provide functions such as:

- insert additional QoS signalling parameters;
- add the functionality of the MExE QoS API at best effort, if the network does not support it directly;
- translate between the QoS parameters from the MExE executable and those of the network;
- monitor the QoS delivered by the network and manage QoS requests between the MExE executable and the network;
- be informed by the MExE executable of the requested QoS traffic class ;
- be informed by the MExE executable of the lowest QoS traffic class which can be accepted by the MExE executable;
- attempt to re-negotiate the QoS if it falls below the lowest QoS traffic class.

The MExE QoS manager may request information from the network regarding the QoS available.

The MExE QoS manager does not need to know the end user's subscribed QoS, this is held within the network and used to validate a requested QoS level.

The MExE QoS manager may also be accessed through the MExE device's MMI.

9.3 Network control API

The network control API shall provide the QoS manager with access to the network specific QoS control (e.g. as defined for GPRS/UMTS in [29] and [30]).

The MExE QoS manager may perform some QoS control, even if it is not provided in the network control.

9.4 MExE QoS API

The MExE QoS API provides the MExE executable with an interface to the QoS management. It does not require the MExE executable to have any knowledge of the underlying network, or how QoS is implemented in the network.

The QoS API shall provide the MExE executable with a standard set of parameters. Refer to [28] for details of these parameters (see note).

NOTE: The FLOWSPEC parameters, defined by the IETF Integrated Services Working Group, provide the QoS information required by QoS capable network elements.

Table 10 "Example parameters" shows the set of example parameters.

Table 10: Example parameters

Parameter	Units	Type
Token Bucket Rate	bytes /sec	32-bit IEEE floating point number
Token Bucket Size	bytes	32-bit IEEE floating point number
Peak Data Rate	bytes/sec	32-bit IEEE floating point number
Minimum Policed Unit	bytes	32-bit integer
Maximum Packet Size	bytes	32-bit integer
Latency	micro secs	32-bit integer
Delay Variation	micro secs	32-bit integer
Service Type		service type

As a minimum the following three parameters shall be supported by the MExE QoS manager:

- Token Bucket Rate;
- Token Bucket Size;
- Peak Data Rate.

NOTE: The discussion of UMTS bearer service parameters as well as radio access bearer parameters is still going on. Especially the bitrate parameters and reliability parameter are under discussion [28].

If the MExE executable does not provide a full set of QoS parameters, then the MExE QoS manager shall the provide QoS parameters based on information available to it (e.g. from the MMI settings), see subclause 9.5 "Sources of Bearer Service Parameters".

9.5 Sources of bearer service parameters

A set of QoS parameters (QoS profile) specify the service provided to the user by the network. At bearer service establishment or modification different QoS profiles have to be taken into account. This is based on:

- The MExE device capabilities;
- The MExE device or the TE within the terminating network;
- A QoS profile in the QoS subscription (describes the upper limits);
- Default QoS profile (of the user or network);
- A Network specific QoS profile characterising for example the current resource availability or other network capabilities.

9.6 QoS streams

Several MExE executables may be executing in the MExE device, each with a different QoS requirement. Also, a MExE executable may operate several QoS streams, each with different parameter settings. The MExE QoS manager within the MExE device shall be able to deal with each stream independently.

9.7 QoS security

Only the end user, MExE executable or the network using a QoS stream should be able to modify the QoS of that stream.

3GPP TSG-T2 #13
Pusan, KOREA
14-18 May 2001

T2-010397

CR-Form-v3

CHANGE REQUEST

⌘	**23.057**	**CR**	**085**	⌘	rev	**-**	⌘	Current version:	**4.1.0**	⌘

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:	⌘	Administrator Determination Mechanism		
Source:	⌘	T2		
Work item code:	⌘	MEXE-ENHANC	***Date:*** ⌘	16-May-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 Administrator determination mechanism does not always clearly say which type of certificate it deals with.
Summary of change:	⌘	Added certificate type and the fact that the certificate contains a root public key wherever the specification generically refers to certificate in the Administrator determination mechanism.
Consequences if not approved:	⌘	Misunderstanding of the mechanism which could potentially lead to implementation not complying with the specification.

Clauses affected:	⌘	Sub-clause 8.8.1.1 and 8.8.1.2		
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘	
Other comments:	⌘	This document supercedes T2-010379		

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.

8.8 Provisioned mechanism for designating administrative responsibilities and adding third parties in a MExE device

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

All applications in the Domain are to be signed by a key which shall be verified back to a Third Party root public key on the MExE device. The Third Party root public keys shall be managed (e.g. addition/mark trusted/mark untrusted) by an administrator that is designated by the owner of the MExE device using the MExE administrator provisioning mechanism. A mechanism is required to be provided to enable the owner of the MExE device to dynamically assign an administrator. The mechanism shall support the following cases:

- the user is the owner;
- the owner is at a remote location. In this case the owner could be the operator, a service provider or a third party;
- the owner of the MExE-(U)SIM wants to be a temporary administrator.

8.8.1 Determining the administrator of the MExE device

The administrator of the MExE device shall be determined by the logical process shown in the flowchart in Figure 11 "MExE Release 98 administrator mechanism". During power-up the provisioned mechanism shall look for an administrator root public key that is stored on the MExE device.

- Administrator root public key is absent

  if the administrator root public key is absent, then the user shall automatically become the administrator of the MExE device.

- administrator root public key is present

if an administrator root public key is present, this root public key shall be used for all remote administration authentication, implying that the owner of the administrator root public key is the administrator.

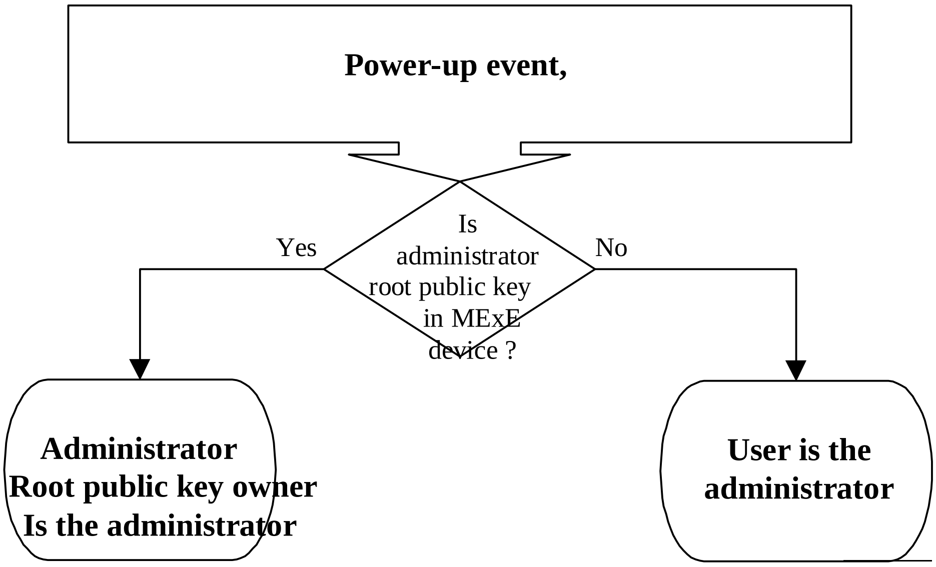

Power-up event,
Is administrator root public key in MExE device ?
Yes
No
Administrator Root public key owner Is the administrator
User is the administrator

Figure 11: MExE Release 98 administrator mechanism

The rest of the mechanism is subsequently defined, however it is a future release implementation, see Figure 12 "Enhanced administrator mechanism". This future enhanced administrator Mechanism shall be initiated after a power-up event is processed or when a MExE-(U)SIM is detected.

(The following subclauses assume that Third Party certificates can be added using the MExE-(U)SIM, however Third Party certificates may be added using a non-(U)SIM approach.)

8.8.1.1 Administrator of the MExE device is the user

If the administrator is the user, then a check shall be made to determine whether there is a MExE-(U)SIM. If a MExE-(U)SIM is present, then a check shall then be made to determine whether there is a Third Party or an Administrator certificate containing a root public key in the MExE-(U)SIM. The enhanced administrator Mechanism shall allow the MExE device to determine (via a format) what type of certificate is present:

- certificate present - third party (CP-TP)

  ~~A~~ If a Third Party certificate containing a root public key is present in the MExE-(U)SIM then this certificate shall be considered by the MExE device as a Third Party certificate, whilst that MExE-(U)SIM is inserted in the MExE device. The user shall be queried to allow or disallow the certificate as a Third Party.

- certificate present - administrator (CP-Admin)

  If a temporary Administrator certificate containing a root public key is present in the MExE-(U)SIM, the user shall be queried whether to allow the certificate on the MExE-(U)SIM to take temporary control of the third party domain. By temporary control, it is meant that once the card is removed the administrator reverts back to the user administrator settings (i.e. the Administrator becomes the User). The above mechanism implies that the previous configuration settings for the administrator shall be saved, so that they may be restored. If the user disallows the MExE-(U)SIM certificate, the Third Party Domain shall not be able to use any of the network capabilities in the third party domain as identified in the network access section of the security Table 6 "Security domains and actions".

If a certificate is not present on the MExE-(U)SIM and the administrator is the user, the user shall continue to be the administrator and may make use of all functionality.

8.8.1.2 Administrator of the MExE device is not the user

If the administrator is not the user, then a check is made to determine if there is a MExE-(U)SIM. If a MExE-(U)SIM is present, then a check is made to see if there is a Third Party or an Administrator certificate containing a root public key in the MExE-(U)SIM.

If an Administrator certificate containing a root public key is present in the MExE-(U)SIM, then a comparison is made of this~~e~~ certificate's root public key ~~on the MExE-(U)SIM~~ with the Administrator root public key on the MExE device for the following cases:

- Case (a): they are the same;
- Case (b): they are not the same, but the MExE device certificate is cross-certified with the MExE-(U)SIM certificate (a cross-certificate exists on the MExE device);
- Case (c): they are not the same, but the MExE device certificate has a line of trust back to the MExE-(U)SIM certificate domain;
- Case (d): they are not the same.

If the owner of the public key in the certificate on the MExE-(U)SIM is to be a temporary administrator (CP-Admin), then in cases (a), (b) and (c), the temporary administrator shall be the owner of the CP-Admin root public key. In case (d), the Third Party domain shall not use any of the network capabilities in the third party domain as identified in the network access section of the security Table 6 "Security domains and actions".

If the certificate is to be a Third Party certificate containing a root public key, then the certificate (CP-TP) shall be verified with the CCM and based on the content and permissions of the CCM, the certificate shall be added to the Third Party list or rejected.

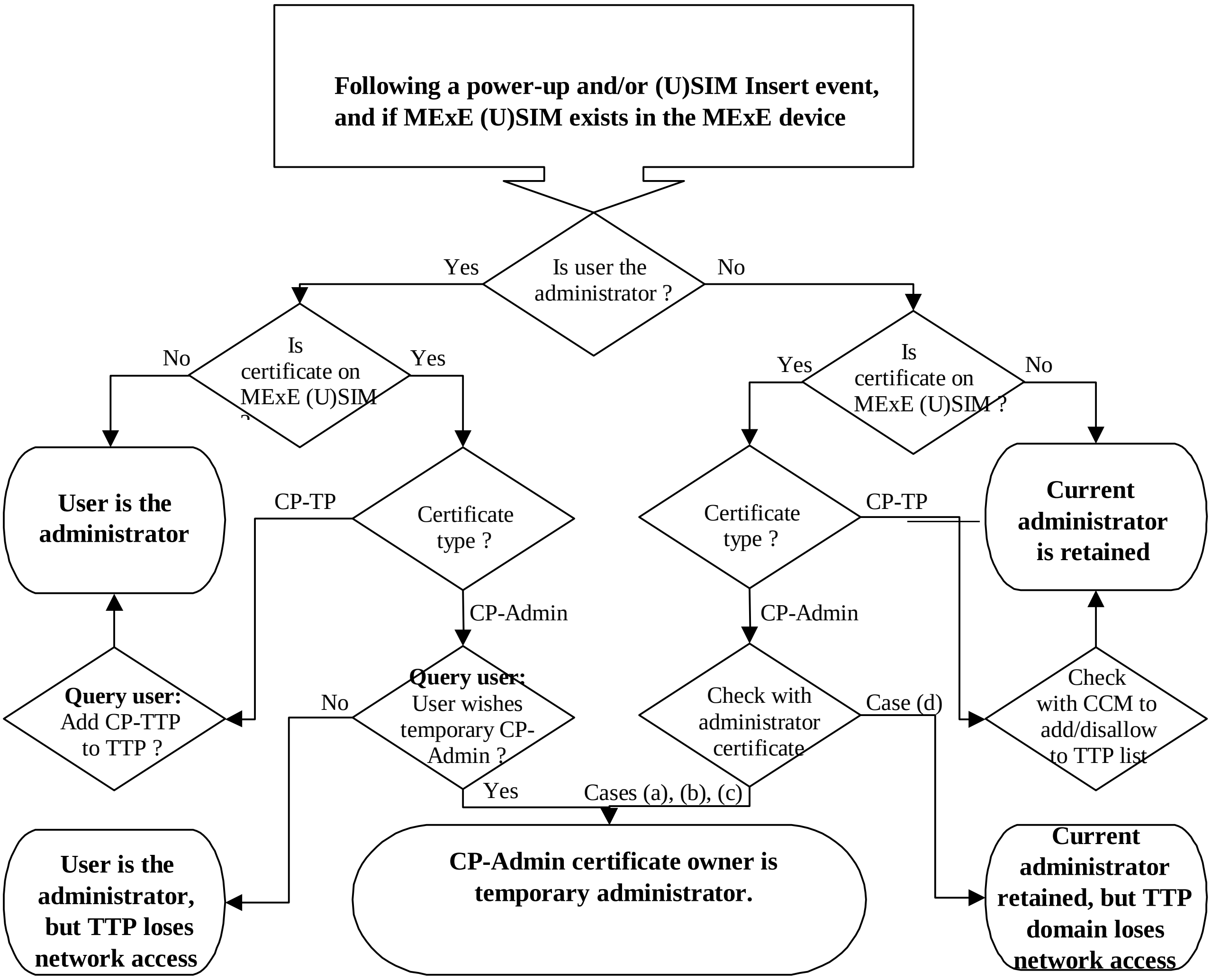

Following a power-up and/or (U)SIM Insert event, and if MExE (U)SIM exists in the MExE device
Is user the administrator ?
Yes
No
Is certificate on MExE (U)SIM ?
No
Yes
Is certificate on MExE (U)SIM ?
Yes
No
User is the administrator
Certificate type ?
CP-TP
CP-Admin
Certificate type ?
CP-TP
CP-Admin
Current administrator is retained
Query user: Add CP-TTP to TTP ?
Query user: User wishes temporary CP-Admin ?
No
Yes
Check with administrator certificate
Case (d)
Cases (a), (b), (c)
Check with CCM to add/disallow to TTP list
User is the administrator, but TTP loses network access
CP-Admin certificate owner is temporary administrator.
Current administrator retained, but TTP domain loses network access

Figure 12: Enhanced administrator mechanism

3GPP TSG-T2 #13
Pusan, Korea
14-18 May 2001

T2-010405

3GPP TSG-T2 MExE
Whistler, Canada
27th-29th March, 2001

T2-MExE-010043

CR-Form-v3

CHANGE REQUEST

⌘ **23.057 CR 086** ⌘ rev **-** ⌘ Current version: **4.1.0** ⌘

*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:*** ⌘	15/05/2001
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

(Note: the text in 8.5.1.2 concerning the removal of the (U)SIM not affecting the status of operator root public keys on ME device is handled in a separate CR).

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: ⌘

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 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.

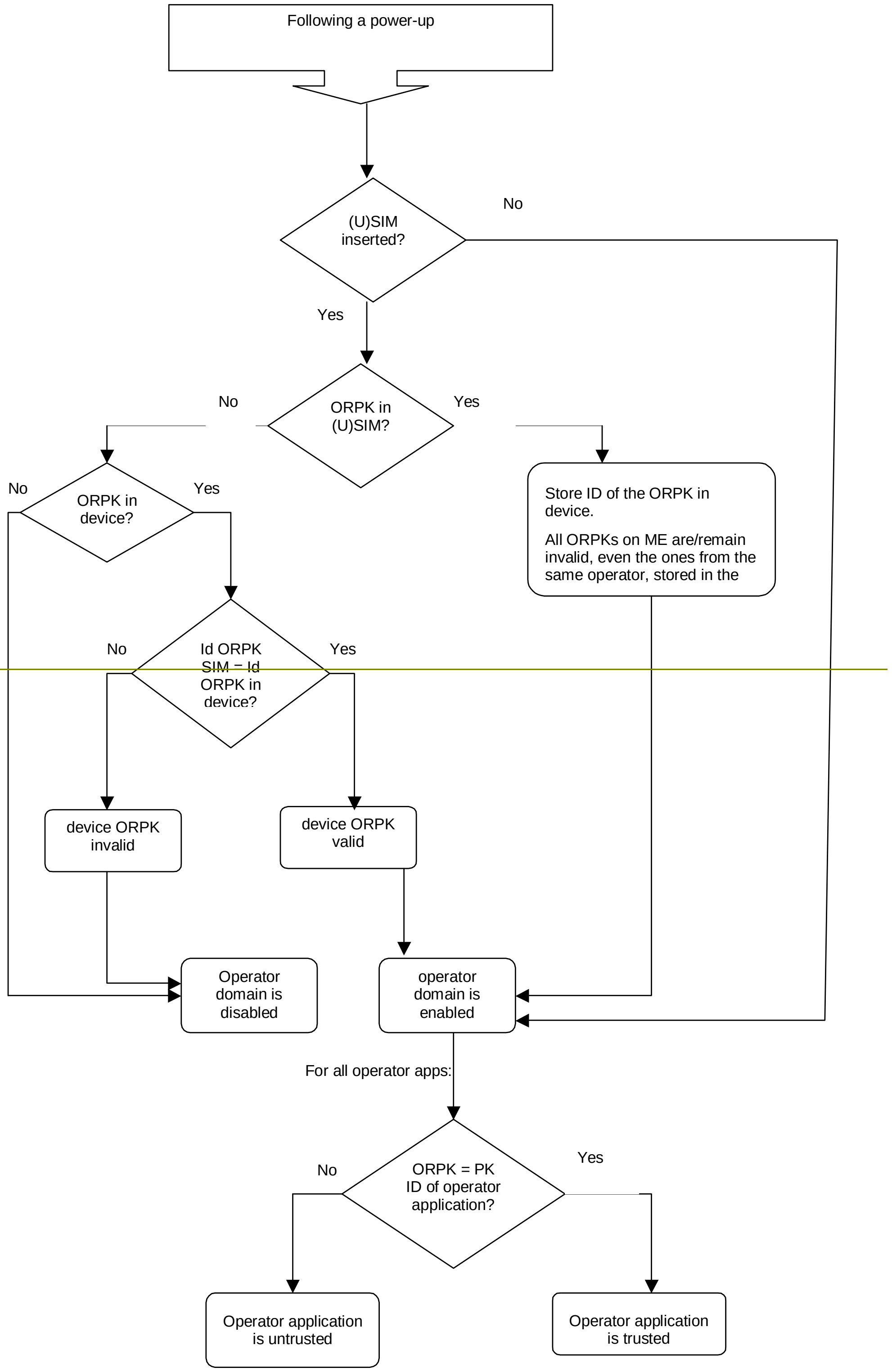
An application signed by an operator shall not be able to execute in the Operator Domain unless the root public key of that operator is installed in the MExE device (either ME or MExE-(U)SIM) and is marked as trusted.

8.5.1.1 MExE device actions on (U)SIM insertion and/or power up.

The requirements in this subclause ensure that the operator domain on the ME belongs to the same operator as the operator that issued the (U)SIM inserted 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 deviceshall 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
Id ORPK SIM = Id ORPK in device?
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

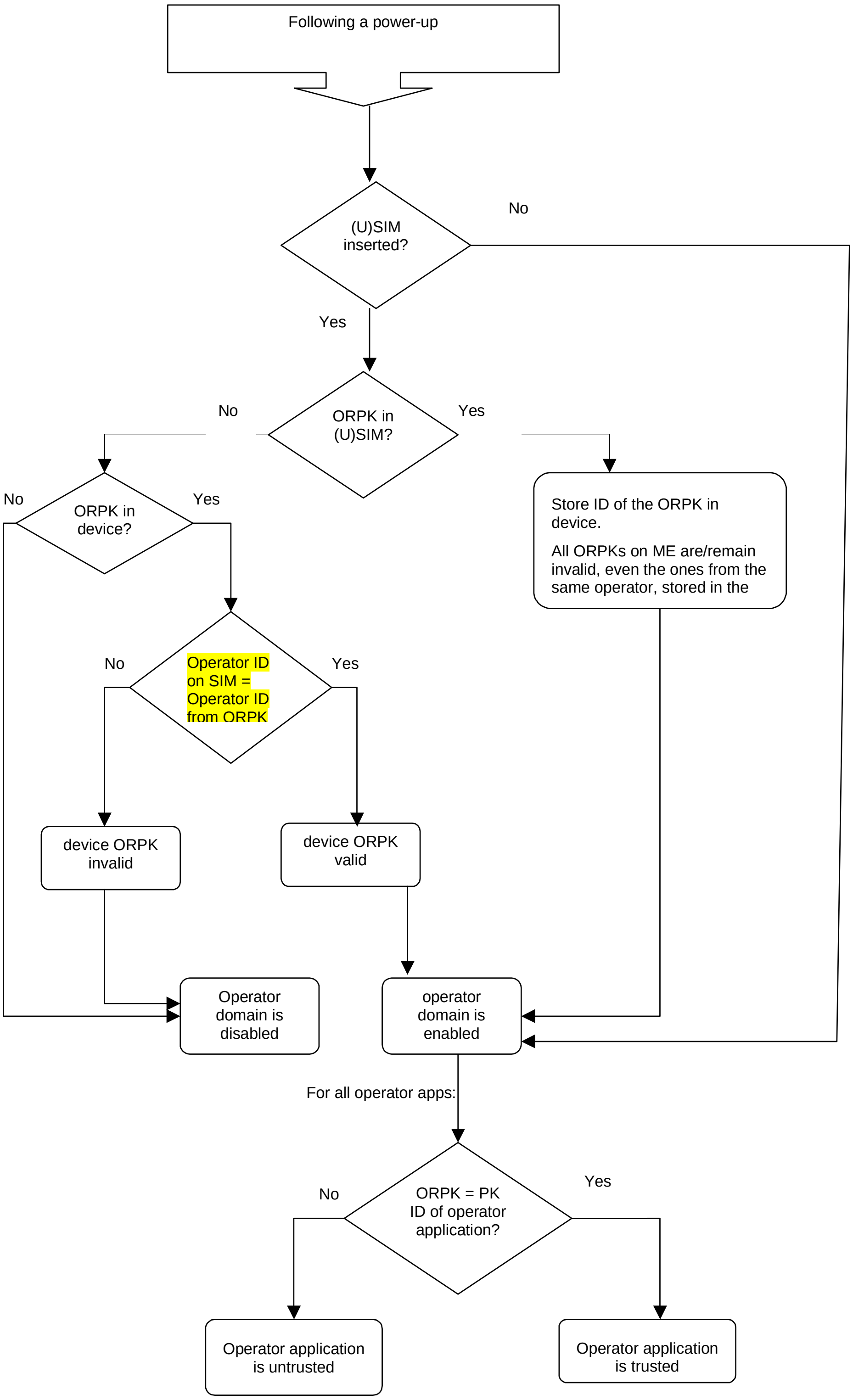

Following a power-up
(U)SIM inserted?
No
Yes
ORPK in (U)SIM?
No
Yes
Store ID of the ORPK in device.
All ORPKs on ME are/remain invalid, even the ones from the same operator, stored in the
No
ORPK in device?
Yes
No
Operator ID on SIM = Operator ID from ORPK
Yes
device ORPK invalid
device ORPK valid
Operator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

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 on removal of the (U)SIM~~

~~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.

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 (if there is support for public key management on the (U)SIM) and in the MExE device. 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 (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

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 (if there is support for public key management on the (U)SIM) and in the MExE device. 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.

If the Administrator root public key is stored in the (U)SIM, the administrator root public key can be downloaded to the MExE device as described in subclause 8.10.4 "Administrator root certificate download mechanism".

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,-until a new RPK for that secure domain is validated.

When the new RPK is validated, the currently running MExE executables (under the old RPK) in that secure domain shall be terminated.

3GPP TSG-T2 /ETSI SMG4
Busan, South Korea
14th - 18th May 2001

T2-010406

CR-Form-v3

CHANGE REQUEST

⌘	**23.057**	**CR**	**087**	⌘ rev	**-**	⌘	Current version:	**4.1.0** ⌘

*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: ⌘	Executable integrity		
Source: ⌘	T2		
Work item code: ⌘	MEXE-EHANC	***Date:*** ⌘	15.05.2001
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 specification is overly burdensome on classmarks that support security domains, and defines implementation details not requirements.
Summary of change: ⌘	Modifications to section 8
Consequences if not approved: ⌘	Sub-optimal performance for Classmarks which support security domains.

Clauses affected: ⌘	8.11	
Other specs affected: ⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘
Other comments: ⌘	This CR is based on T2-010396.	

8.11 MExE executable ~~pre-launch signature verification~~integrity

If the 3 MExE security domains defined in subclause 8.1 "Generic security" are not supported, then the pre-verification of MExE executables at launch time described in this subclause 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. ~~As a~~Authentication of a MExE executable at the time of download does not ensure that the ~~integrity of that~~ 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.~~, all MExE executables shall be authenticated immediately prior to each and every launch.~~

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 section 8.11.1)
- Optimised pre-launch signature verification (see section 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.

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

8.11.1 Full signature verification

Full signature verification assumes that the procedure of validation for downloaded MExE executables and certificates is used. For more details see section 8.4 “Certification and Authorization Architecture”.

~~Authentication of MExE executables prior to being launched shall be performed by performing a full signature verification, or by performing an optimised authentication mechanism to reduce launch time overheads (see 8.11.1 "Optimised pre-launch signature verification").~~

~~NOTE: The definition of full signature verification requires further elaboration.~~

8.11.2 Optimised pre-launch signature verification

This is an optional feature ~~added~~ which is used to eliminate the potentially excessive overhead of checking a signature again after initial full certificate verification has already been performed.~~each time an application is launched~~.

To use this process the MExE device shall create a hash of the executable object (executable object fingerprint) as if checking the signature. This shall be stored in a protected verified application list, along with indication of the domain permissions for the application. The hash used shall be the same type as that used for signing the object. When launching an application or downloading an applet, the hash shall be performed as for when computing the signature. The verified application list shall then be checked; if the hash value is present and the entry has not expired then the application or applet may execute. If no list entry exists for this object, or the entry has expired, the process shall then proceed with the full signature verification. Note that the lists for applications and applets should be separate and that an implementation determines management policy for the lists (e.g., ageing policy, which entries to delete when trying to add a new entry to a full list etc.). One restriction imposed that shall be enforced is that the maximum number of uses for an entry before it is marked invalid is limited to some maximum value.

In the event that a new CCM is received by the MExE device, all verified application list entries shall be marked invalid unless some mechanism to determine the validity of an authorising certificate entry for each application is provided by the MExE device implementation.

3GPP TSG-T2 #13
Pusan, KOREA
14-18 May 2001

T2-010554

CR-Form-v3

CHANGE REQUEST

⌘	**23.057**	**CR**	**088**	⌘ rev	**-**	⌘ Current version:	**4.1.0**	⌘

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: ⌘	Clarifications on call control and signed packages			
Source: ⌘	T2			
Work item code: ⌘	MEXE-ENHANC		***Date:*** ⌘	18-May-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: ⌘	Editorial clarifications for a better understanding of the MExE specification: 1) Specific support of call control is actually identified in section 5.3 and for WAP classmarks only. 2) JAR files are an example of signed packages and are essentially used by Java based MExE classmarks
Summary of change: ⌘	Reference to section 5.3 added and clarification on which MExE classmark is concerned by call control. Clarification on JAR files.
Consequences if not approved: ⌘	Misunderstanding of the specification leading to possible non-compliant implementations.

Clauses affected: ⌘	Subclauses 4.10 & 8.10.2	
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://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.

4.10 User control of application connections

Support of the user control of application connections is mandatory.

This subclause 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 ~~and Java~~ classmark MExE devices is identified in subsequent ~~subclauses~~subclause 5.3 “Call control”, the security aspects of connection control are identified in subclause 8 "Security", and the user control of connection authorisation is identified in 4.7 "User profile".

8.10.2 Installation of root certificates in a signed data package

Root certificates in a signed package (whose signature verifies as described in subclause 8.5 "Root Public keys" to the Manufacturer root, Operator root, or the Administrator root), may be installed to the root public key store on the MExE device. Note that the certificate thus packaged does not necessarily belong to the manufacturer domain. The types of certificate that can be present and installed by packages are given in Table 9 "Allowed certificate types in signed packages". The MExE device shall store the root public key as indicated by the certificate type.

When a certificate containing an Administrator root public key is thus contained in a signed package, the signed package (e.g. a JAR file in the case of Java based MExE classmarks) shall contain two files: the Administrator root public key and the CCM.

Table 9: Allowed certificate types in signed packages

Signature on Package	Allowed Certificate types in package
Administrator	Third Party
Manufacturer	Administrator, Manufacturer, Operator, Third Party
Operator	Administrator, Operator, Third Party

3GPP TSG-T2 #13
Pusan, KOREA
14-18 May 2001

T2-010555

CR-Form-v3

CHANGE REQUEST

⌘	**23.057**	**CR**	**089**	⌘ rev	**-**	⌘ Current version:	**4.1.0** ⌘

*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:	⌘	More Abbreviations		
Source:	⌘	T2		
Work item code:	⌘	MEXE-ENHANC	***Date:*** ⌘	15-May-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:	⌘	Missing abbreviations in the abbreviation definition list.
Summary of change:	⌘	Addition of DTMF, SIM, USIM and XML abbreviations.
Consequences if not approved:	⌘	Missing explanation of abbreviations.

Clauses affected:	⌘	Sub-clause 3.2	
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://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

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

3.2 Abbreviations

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

AA	Attribute Authority
API	Application Programming Interface
APDU	Application protocol data unit
CA	Certification Authority
CC/PP	Composite Capability/Preference Profiles
~~Diff-serv~~	~~Differentiated Services~~
CGI	Common Gateway Interface
CCM	Certificate Configuration Message
CLDC	Connected Limited Device Configuration
CP-Admin	Certificate Present (in the MExE (U)SIM) - Administrator
CP-TP	Certificate Present (in the MExE (U)SIM) - Third Party
DHCP	Dynamic Host Configuration Protocol
Diff-serv	Differentiated Services
DTMF	Dual Tone Multiple Frequency
GSM	Global System for Mobile Communication
GPRS	General Packet Radio Service
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transport Protocol Secure (https is http/1.1 over SSL, i.e. port 443)
IETF	Internet Engineering Task Force
IP	Internet Protocol
JAD	Java Application Descriptor
JAM	Java Application Manager
J2ME	Java 2 Micro Edition
J2SE	Java 2 Standard Edition
JNDI	Java Naming Directory Interface
JTAPI	Java Telephony Application Programming Interface
JAR file	Java Archive File
JVM	Java Virtual Machine
KVM	K Virtual Machine
ME	Mobile Equipment
MIDP	Mobile Information Device Profile
MIDlet	MIDP Application
MMI	Man-Machine Interface
MSE	MExE Service Environment
MT	Mobile Termination
OCF	OpenCard Framework
OEM	Original Equipment Manufacturer
QoS	Quality of Service
PDP	Packet Data Protocol
RDF	Resource Description Format
RFC	Request For Comments
SAP	Service Access Point
SIM	Subscriber Identity Module
SMS	Short Message Service
SSL	Secure Socket Layer
TE	Terminal Equipment
TLS	Transport Layer Security
TP	Third Party
UDP	User Datagram Protocol
UE	User Equipment
UI	User Interface
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
USIM	Universal Subscriber Identity Module

USSD	Unstructured Supplementary Service Data
VM	Virtual Machine
WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WDP	Wireless Datagram Protocol
WMLS	Wireless Markup Language Script
WSP	Wireless Session Protocol
WTA	Wireless Telephony Applications
WTAI	Wireless Telephony Applications Interface
WTLS	Wireless Transport Layer Security
WTP	Wireless Transaction Protocol
WWW	World Wide Web
XML	Extensible Markup Language

Further abbreviations are given in 3GPP TS 22.057 (MExE stage 1) [2] and GSM 01.04 [1].

3GPP TSG-T2 #13
Pusan, KOREA
14-18 May 2001

T2-010556

CR-Form-v3

CHANGE REQUEST

⌘	**23.057**	**CR**	**090**	⌘	rev	**-**	⌘	Current version:	**4.1.0** ⌘

*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:	⌘	CC/PP Working Group Web Page
Source:	⌘	T2
Work item code:	⌘	MEXE-ENHANC **Date:** ⌘ 15-May-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 World Wide Web Consortium (W3C) CC/PP Working Group has set up a Web page linking together all CC/PP documents, including the two documents currently referenced by the MExE specification. It would therefore be beneficial to all MExE specification readers to learn about this Web page.
Summary of change:	⌘	References [15] and [16] have been modified to show the address of this Web page.
Consequences if not approved:	⌘	Current text links are incorrect and would mean that the reference document could not be located

Clauses affected:	⌘	Clause 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://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.

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: "MExE Stage 1 Description".

[3] Personal Java 1.1.1 or higher, Sun Microsystems http://www.javasoft.com/products/personaljava/

[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: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects Service Aspects; The Virtual Home Environment"

[13] ISO 639 International Standard - codes for the representation of language names.

[14] 3GPP TS 22.101: "3rd Generation Partnership Project; Service Aspects; Service Principles".

[15] CC/PP Exchange Protocol based on HTTP Extension Framework; W3C ~~http://www.w3.org/TR/NOTE-CCPPexchange~~http://www.w3.org/Mobile/CCPP

[16] Composite Capability/Preference Profiles (CC/PP):A user side framework for content negotiation; http://www.w3.org/Mobile/CCPP~~ http://www.w3.org/TR/NOTE-CCPP.~~

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

[18] JDK 1.1 security http://www.javasoft.com/products/jdk/1.1/docs/guide/security/index.html

[19] Java 2 security http://www.javasoft.com/products/jdk/1.2/docs/guide/security/index.html

[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: ftp://ftp.isi.edu/in-notes/rfc1321.txt

[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: Authentication framework".

[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: "3rd Generation Partnership Project; Technical Specification Group Services and system Aspects QoS Concept and Architecture (3GPP TS 23.107)".

[29] 3GPP TS 24.007: "3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile radio interface signalling layer 3; General Aspects (3GPP TS 24.007)".

[30] 3GPP TS 24.008: "3rd Generation Partnership Project; Universal Mobile Telecommunications System; Mobile radio interface layer 3 specification, Core Network Protocols – Stage 3 (TS 24.008)".

[31] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Core Network; Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service Description; Stage 2 (3GPP TS 23.060)".

[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 Internet X.509 Public Key Infrastructure January 1999.

[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: http://www.w3.org/XML

[37] Resource Definition Framework (RDF) Model and Syntax, W3C Recommendation.
URL: http://www.w3.org/RDF

[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.

3GPP TSG-T2 #13
Pusan, KOREA
14-18 May 2001

T2-010557

CR-Form-v3

CHANGE REQUEST

⌘	**23.057**	**CR**	**091**	⌘	rev	**-**	⌘	Current version:	**4.1.0**	⌘

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:	⌘	Using WBXML when transporting CC/PP over WSP			
Source:	⌘	T2			
Work item code:	⌘	MEXE-ENHANC	***Date:***	⌘	15-May-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:	⌘	When transporting the UAProf over WSP, the WAP specification requires the UAProf to be encoded according to the WBXML specification. This should be mentioned in the MExE specification.
Summary of change:	⌘	This CR proposes to add to the MExE specification a comment making clear WBXML is required.
Consequences if not approved:	⌘	It would not be clear that CC/PP is encoded with WBXML

Clauses affected:	⌘	Clause 2, sub-clauses 3.2 & 4.6.2		
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://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.

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: "MExE Stage 1 Description".

[3] Personal Java 1.1.1 or higher, Sun Microsystems http://www.javasoft.com/products/personaljava/

[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: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects Service Aspects; The Virtual Home Environment"

[13] ISO 639 International Standard - codes for the representation of language names.

[14] 3GPP TS 22.101: "3rd Generation Partnership Project; Service Aspects; Service Principles".

[15] CC/PP Exchange Protocol based on HTTP Extension Framework; W3C http://www.w3.org/TR/NOTE-CCPPexchange

[16] Composite Capability/Preference Profiles (CC/PP):A user side framework for content negotiation; http://www.w3.org/TR/NOTE-CCPP.

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

[18] JDK 1.1 security http://www.javasoft.com/products/jdk/1.1/docs/guide/security/index.html

[19] Java 2 security http://www.javasoft.com/products/jdk/1.2/docs/guide/security/index.html

[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: ftp://ftp.isi.edu/in-notes/rfc1321.txt

[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: Authentication framework".

[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: "3rd Generation Partnership Project; Technical Specification Group Services and system Aspects QoS Concept and Architecture (3GPP TS 23.107)".

[29] 3GPP TS 24.007: "3rd Generation Partnership Project; Technical Specification Group Core Network; Mobile radio interface signalling layer 3; General Aspects (3GPP TS 24.007)".

[30] 3GPP TS 24.008: "3rd Generation Partnership Project; Universal Mobile Telecommunications System; Mobile radio interface layer 3 specification, Core Network Protocols – Stage 3 (TS 24.008)".

[31] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Core Network; Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service Description; Stage 2 (3GPP TS 23.060)".

[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 Internet X.509 Public Key Infrastructure January 1999.

[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: http://www.w3.org/XML

[37] Resource Definition Framework (RDF) Model and Syntax, W3C Recommendation.
URL: http://www.w3.org/RDF

[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

3 Definitions and abbreviations

3.1 Definitions

3.2 Abbreviations

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

AA	Attribute Authority
API	Application Programming Interface
APDU	Application protocol data unit
CA	Certification Authority
CC/PP	Composite Capability/Preference Profiles
Diff-serv	Differentiated Services
CGI	Common Gateway Interface
CCM	Certificate Configuration Message
CLDC	Connected Limited Device Configuration
CP-Admin	Certificate Present (in the MExE (U)SIM) - Administrator
CP-TP	Certificate Present (in the MExE (U)SIM) - Third Party
DHCP	Dynamic Host Configuration Protocol
GSM	Global System for Mobile Communication
GPRS	General Packet Radio Service
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transport Protocol Secure (https is http/1.1 over SSL, i.e. port 443)
IETF	Internet Engineering Task Force
IP	Internet Protocol
JAD	Java Application Descriptor
JAM	Java Application Manager
J2ME	Java 2 Micro Edition
J2SE	Java 2 Standard Edition
JNDI	Java Naming Directory Interface
JTAPI	Java Telephony Application Programming Interface
JAR file	Java Archive File
JVM	Java Virtual Machine
KVM	K Virtual Machine
ME	Mobile Equipment
MIDP	Mobile Information Device Profile
MIDlet	MIDP Application
MMI	Man-Machine Interface
MSE	MExE Service Environment
MT	Mobile Termination
OCF	OpenCard Framework
OEM	Original Equipment Manufacturer
QoS	Quality of Service
PDP	Packet Data Protocol
RDF	Resource Description Format
RFC	Request For Comments
SAP	Service Access Point
SMS	Short Message Service
SSL	Secure Socket Layer
TE	Terminal Equipment
TLS	Transport Layer Security
TP	Third Party

UDP	User Datagram Protocol
UE	User Equipment
UI	User Interface
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
USSD	Unstructured Supplementary Service Data
VM	Virtual Machine
WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WBXML	WAP Binary XML
WDP	Wireless Datagram Protocol
WMLS	Wireless Markup Language Script
WSP	Wireless Session Protocol
WTA	Wireless Telephony Applications
WTAI	Wireless Telephony Applications Interface
WTLS	Wireless Transport Layer Security
WTP	Wireless Transaction Protocol
WWW	World Wide Web

Further abbreviations are given in 3GPP TS 22.057 (MExE stage 1) [2] and GSM 01.04 [1].

4 Generic MExE aspects

4.1 MExE classmark 1 (WAP environment)

4.2 MExE classmark 2 (PersonalJava environment)

4.3 MExE classmark 3 (J2ME CLDC environment)

4.4 Multiple classmark support

4.5 High level architecture

4.6 Capability and content negotiation

4.6.1 Capability negotiation characteristics

4.6.2 CC/PP over WSP (Classmark 1)

In Classmark 1, according to the WAP User Agent Profile Specification [17], the CC/PP description is encoded with WBXML [45] after which it is carried over by ~~using CC/PP over~~ WSP, [17].

3GPP TSG-T2 #13
Pusan, Korea
14-18 May 2001

T2-010404

3GPP TSG-T2 MExE
Whistler, Canada
27th-29th March, 2001

T2-010558

CR-Form-v3

CHANGE REQUEST

⌘	**23.057**	**CR**	**092**	⌘	rev	**-**	⌘	Current version:	**4.1.0** ⌘

*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:	⌘	Clarification of root public keys		
Source:	⌘	T2		
Work item code:	⌘	MEXE-ENHANC	***Date:*** ⌘	12/05/2001
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: ⌘

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.

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

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 (U)SIM insertion and/or power up.

The requirements in this subclause ensure that the operator domain on the ME belongs to the same operator as the operator that issued the (U)SIM inserted 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 deviceshall behave as dictated by Figure 7 "Terminal behaviour on power up" below.

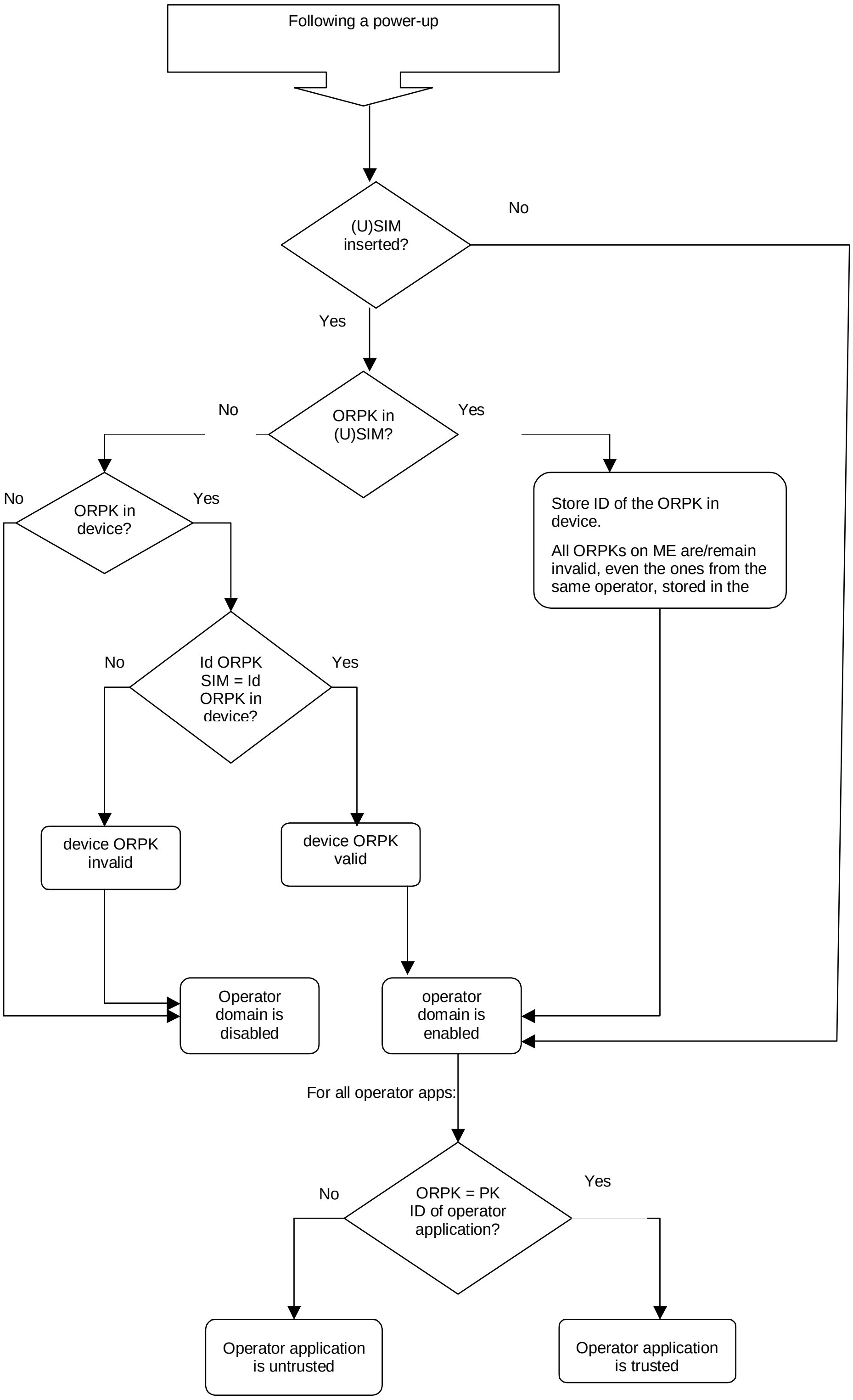

Following a power-up
(U)SIM inserted?
No
Yes
ORPK in (U)SIM?
No
Yes
ORPK in device?
No
Yes
Store ID of the ORPK in device.
All ORPKs on ME are/remain invalid, even the ones from the same operator, stored in the
Id ORPK SIM = Id ORPK in device?
No
Yes
device ORPK invalid
device ORPK valid
Operator domain 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.

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 on removal of the (U)SIM

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.

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

8.5.3 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 (if there is support for public key management on the (U)SIM) and in the MExE device. 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 (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

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 (if there is support for public key management on the (U)SIM) and in the MExE device.

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.

If the Administrator root public key is stored in the (U)SIM, the administrator root public key can be downloaded to the MExE device as described in subclause 8.10.4 "Administrator root certificate download mechanism".

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 #13
Pusan, Korea
14-18 May 2001

T2-010408

3GPP TSG-T2 #12
Whistler, Canada
March 27-29, 2001

T2-MEXE-010041

CR-Form-v3

CHANGE REQUEST

⌘ **23.057 CR 093** ⌘ rev **-** ⌘ Current version: **4.1.0** ⌘

*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: ⌘ Certificate Chain Verification Diagram

Source: ⌘ T2

Work item code: ⌘ MEXE-SEC

Date: ⌘ 15/05/2001

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 specification does not clearly specify a procedure for checking the signatures on an application. There are a number of areas that remain ambiguous.

Summary of change: ⌘ This CR proposes a certificate chain verification diagram and relevant text to verify newly downloaded applications on to the terminal.

Consequences if not approved: ⌘ Unclear definition of digital signature verification procedure will then remain in MExE specification

Clauses affected: ⌘ 3.1, 3.2, 8.4.2

Other specs affected: ⌘
□ Other core specifications ⌘
□ Test specifications
□ O&M Specifications

Other comments: ⌘

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.

3.2 Abbreviations

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

AA	Attribute Authority
API	Application Programming Interface
APDU	Application protocol data unit
CA	Certification Authority
CC/PP	Composite Capability/Preference Profiles
Diff-serv	Differentiated Services
CGI	Common Gateway Interface
CCM	Certificate Configuration Message
CLDC	Connected Limited Device Configuration
CP-Admin	Certificate Present (in the MExE (U)SIM) - Administrator
CP-TP	Certificate Present (in the MExE (U)SIM) - Third Party
CRL	Certificate Revocation List
DHCP	Dynamic Host Configuration Protocol
GSM	Global System for Mobile Communication
GPRS	General Packet Radio Service
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transport Protocol Secure (https is http/1.1 over SSL, i.e. port 443)
IETF	Internet Engineering Task Force
IP	Internet Protocol
JAD	Java Application Descriptor
JAM	Java Application Manager
J2ME	Java 2 Micro Edition

J2SE	Java 2 Standard Edition
JNDI	Java Naming Directory Interface
JTAPI	Java Telephony Application Programming Interface
JAR file	Java Archive File
JVM	Java Virtual Machine
KVM	K Virtual Machine
ME	Mobile Equipment
MIDP	Mobile Information Device Profile
MIDlet	MIDP Application
MMI	Man-Machine Interface
MRPK	Manufacturer Root Public Key
MSE	MExE Service Environment
MT	Mobile Termination
OCF	OpenCard Framework
OEM	Original Equipment Manufacturer
OCSP	Online Certificate Status Protocol
ORPK	Operator Root Public Key
QoS	Quality of Service
PDP	Packet Data Protocol
PKI	Public Key Infrastructure
RDF	Resource Description Format
RFC	Request For Comments
RPK	Root Public Key
SAP	Service Access Point
SCVP	Simple Certificate Verification Protocol
SMS	Short Message Service
SSL	Secure Socket Layer
TE	Terminal Equipment
TLS	Transport Layer Security
TP	Third Party
UDP	User Datagram Protocol
UE	User Equipment
UI	User Interface
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
USSD	Unstructured Supplementary Service Data
VM	Virtual Machine
WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WDP	Wireless Datagram Protocol
WMLS	Wireless Markup Language Script
WSP	Wireless Session Protocol
WTA	Wireless Telephony Applications
WTAI	Wireless Telephony Applications Interface
WTLS	Wireless Transport Layer Security
WTP	Wireless Transaction Protocol
WWW	World Wide Web

Further abbreviations are given in 3GPP TS 22.057 (MExE stage 1) [2] and GSM 01.04 [1].

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 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".

Note that blanket permission cannot be used for uninstalled MExE executables e.g. applets, WMLS.

Table 8: User Permissions

	User Permissions		
Permission Type	Description	Invocation	Revocation
blanket permission	The user gives blanket permission to the MExE executable for the specified action, and the MExE executable subsequently uses the user's original permission for the identified subsequent actions whenever the MExE executable is running.	Typically such permission would be given at MExE executable configuration or run time.	The blanket permission maybe revoked by the user at any time. The user permission no longer applies once the MExE executable has been removed.
session permission	The user gives permission to the MExE executable for the specified action during a specific run time session of an MExE executable, and the MExE executable subsequently uses the user's permission for the identified subsequent actions whilst the MExE executable session is still running.	Typically such permission would be given at MExE executable run time.	The session permission maybe revoked by the user at any time. The user permission no longer applies once the MExE executable run time session has terminated.
single action permission	The user gives a single permission to the MExE executable for the specified action; if the MExE executable subsequently wishes to repeat the action it must again request the user's permission for the identified subsequent action.	Typically such permission would be given at MExE executable run time.	The user permission no longer applies once the action has terminated.

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.

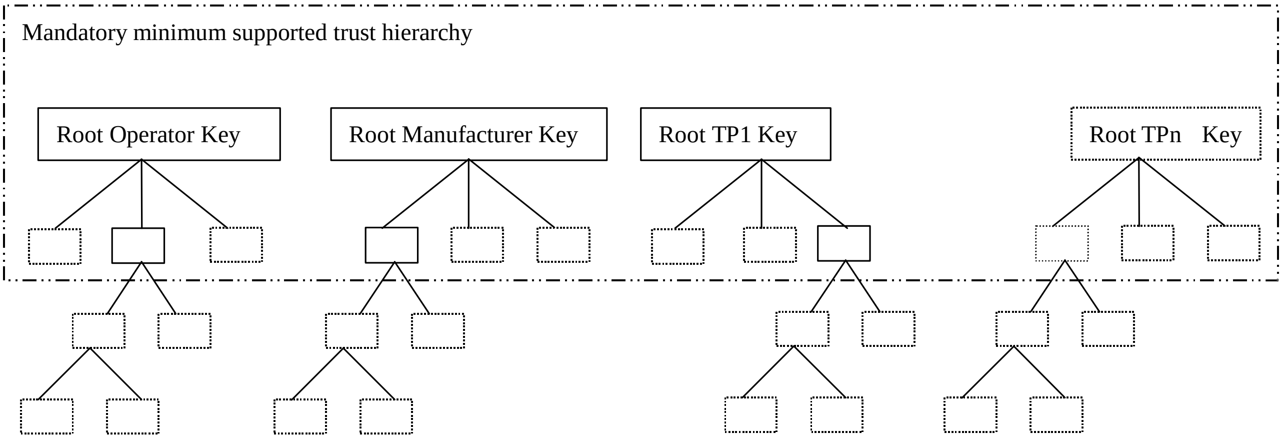


Figure 6: Trust hierarchy

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.

8.4.3 Certificate Chain Verification

This section 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* – Checks whether the executable contains a signature together with the corresponding end entity certificate.

Valid Application Signature* – 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* - 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.

*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 section "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 X 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 X shows an example of the certificate chain verification procedure.

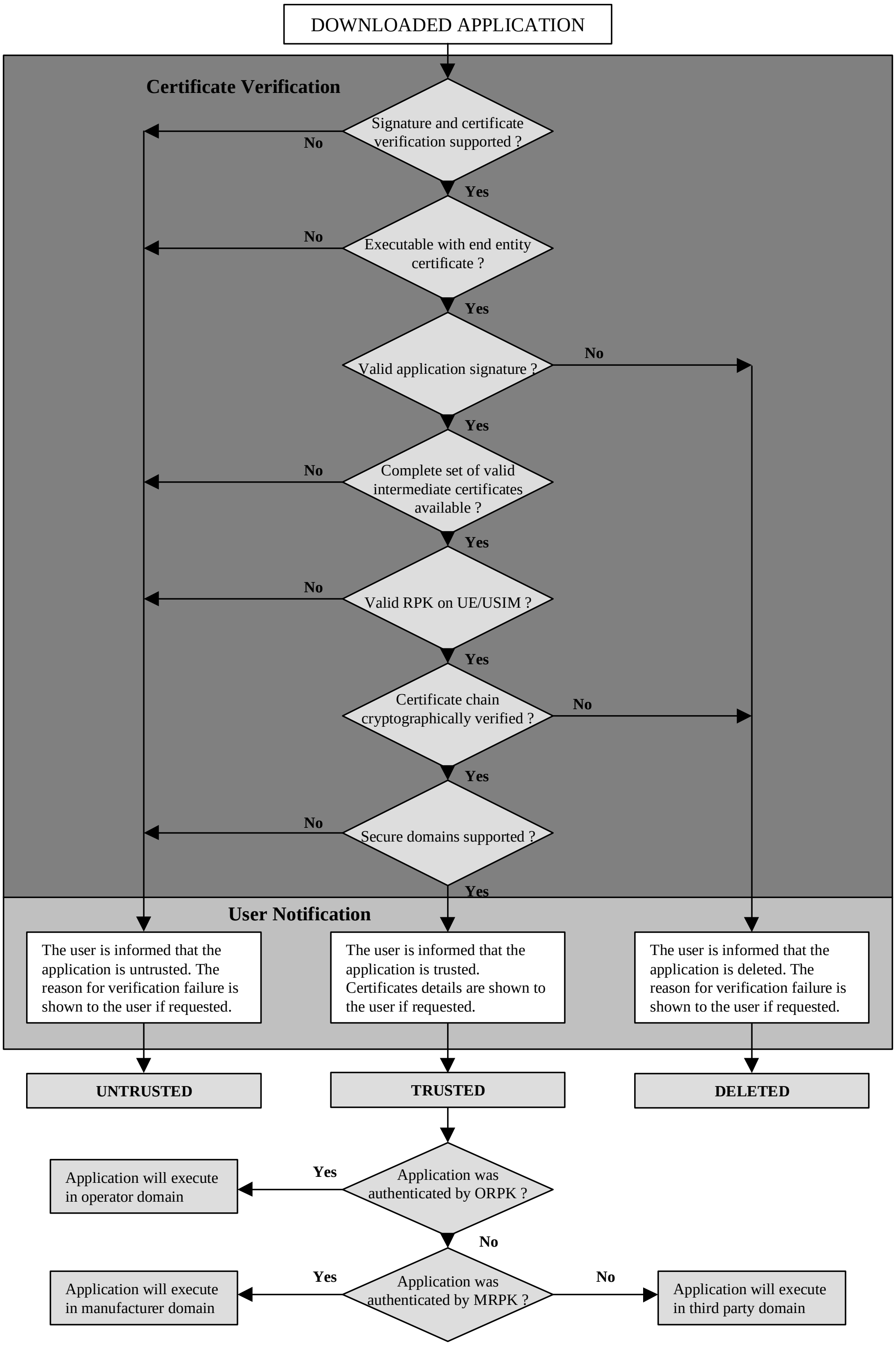

DOWNLOADED APPLICATION
Certificate Verification
Signature and certificate verification supported ?
No
Yes
Executable with end entity certificate ?
No
Yes
Valid application signature ?
No
Yes
Complete set of valid intermediate certificates available ?
No
Yes
Valid RPK on UE/USIM ?
No
Yes
Certificate chain cryptographically verified ?
No
Yes
Secure domains supported ?
No
Yes
User Notification
The user is informed that the application is untrusted. The reason for verification failure is shown to the user if requested.
The user is informed that the application is trusted. Certificates details are shown to the user if requested.
The user is informed that the application is deleted. The reason for verification failure is shown to the user if requested.
UNTRUSTED
TRUSTED
DELETED
Application was authenticated by ORPK ?
Yes
Application will execute in operator domain
No
Application was authenticated by MRPK ?
Yes
Application will execute in manufacturer domain
No
Application will execute in third party domain

Figure X "Certificate Chain Verification Diagram"