# 3GPP TR 33.812 V9.2.0 (2010-06)

*Technical Report*

# 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Feasibility study on the security aspects of remote provisioning and change of subscription for Machine to Machine (M2M) equipment (Release 9)

Keywords
SECURITY

# Contents

# Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

Y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

# Introduction

Machine to Machine (M2M) Communication is seen as a form of data communication between entities that may have no human interaction. One of the challenges with M2M communication is that deployed M2M equipments are managed remotely without any direct human interaction with the device.

This Technical Report considers the M2M Equipment as a device that could be a fully self-contained device or a device with interfaces to attach, for example, sensors and on-site service equipment. The current 3GPP system defines the use of a USIM/ISIM application in a UICC as a means of protecting users (until now mostly human users of mobile terminals) and network operators from fraudulent use of the network. Since some of the original assumptions on the use of a USIM/ISIM application in a UICC did not take into account the requirements of M2M Equipment and users, the current UICC based solution needs to be reviewed against the new assumptions that arise from M2M.

TR 22.868 presents a study on facilitating machine-to-machine (M2M) communication in 3GPP systems. This Technical Report goes along with the TR 22.868, evaluating from a security perspective the solutions that might address the M2M use cases. One of the challenges highlighted in TR 22.868 is the possible need to be able to provision (i.e. initialize and/or change the subscription of) M2M equipment remotely, i.e. without requiring a person to attend the location of the M2M equipment. This was captured in clause 6 of TR 22.868, as possible requirements that could facilitate M2M communications in 3GPP systems, and more specifically in clause 5.2.2 of TR 22.868 when handling large numbers of M2M equipment. TR 22.868 mentions only UICC-based solution for M2M use-cases and does not explicitly mention the need to investigate UICC-less-based solutions.

NOTE: For the reasons explained in the Definitions clause, the term MCIM is used as a generic term throughout this document and USIM or ISIM is considered as a type of the generic MCIM. However, whenever USIM and ISIM are referred to in the remainder of this document, they refer to the traditional USIM or ISIM that reside on the UICC.

# 1 Scope

The scope of this Technical Report is to study the remote subscription management for M2M Equipment (M2ME) when the Machine Communications Identity Module (MCIM) application resides in the UICC and when the MCIM application resides in the M2M equipment. The remote subscription management includes tasks such as remote subscription provisioning and/or remote change of subscription.

The scope of this study includes the definition of a trust model for remote subscription management for M2ME. Security threats and security requirements are identified, and an evaluation of the candidate solutions is presented.

The security implications of the following requirements are within the scope of the study (based on section 5.2.2 of TR 22.868)

1. The possibility to change subscription for M2MEs out in the field (e.g. after contract expiry) without direct human intervention.
2. The possibility to allocate the M2ME at initial power up to a network operator without direct human intervention.

Furthermore, this study includes the following items:

- an investigation of candidate security solutions architectures that allow remote subscription management to take place in a secure manner;
- an identification of current USIM/ISIM functionality that may need to be incorporated in a MCIM application, with or without changes to allow remote subscription management for the M2ME;
- an identification of functionality in the network, in the UICC or in the M2ME, that may need to be added due to the remote subscription management method;
- the study may identify principle requirements for protected storage and the execution environment (e.g. by collaborating with relevant working groups such as the OMTP Hardware group)

This study is beyond the scope of the first requirement identified in SA1 TR 22.868 since section 5.2.2 of TR 22.868 contains a requirement to have "Tamper Save/Theft proof terminal including a UICC".

# 2 References

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

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. 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] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 22.868: "Study on Facilitating Machine to Machine".

[3] Trusted Computing Group, "Mobile Reference Architecture and Mobile Trusted Module specifications", https://www.trustedcomputinggroup.org/specs/mobilephone/.

[4] Global Platform Device Application Security Management, http://www.globalplatform.org/specificationsdevice.asp.

[5] OMTP Trusted Environment: OMTP TR0, http://www.omtp.org/Publications/Display.aspx?Id=03f37406-be24-424b-b177-dd0cb9dbc719

[6] OMTP Advanced Trusted Environment: OMTP TR1, http://www.omtp.org/Publications/Display.aspx?Id=24ad518b-6dba-4155-ad51-3143bd43a234

[7] GSMA/EICTA Principles concerning handset theft, GSMA: Security Principles Related to Handset Theft 3.0.0

[8] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics".

[9] 3GPP TS 31.102: "Characteristics of the USIM Application".

[10] 3GPP TS 31.103: "Characteristics of the IP Multimedia Services Identity Module (ISIM) Application".

[11] 3GPP TS 31.101: "UICC-Terminal Interface, Physical and Logical Characteristics".

[12] ETSI TS 101 220: "Smart cards; ETSI numbering system for telecommunication application providers".

[13] OMA-TS-DM_Bootstrap-V1_2: "OMA Device Management Bootstrap" http://member.openmobilealliance.org/ftp/Public_documents/DM/Permanent_documents/

[14] OMA-TS-DM-Security-V1_2: "OMA Device Management Security" http://member.openmobilealliance.org/ftp/Public_documents/DM/Permanent_documents/

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [x] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [x].

**Trusted Environment**. The Trusted environment (TRE) with the M2ME provides some hardware and software protection and separation for the provisioning, storage, execution and management of MCIMs. A TRE can be validated at any time by an external agency that is authorised to do so.

**MCIM:** For the purposes of the present document the Machine Communication Identity Module (MCIM) is a term that indicates the collection of M2M security data and functions for a M2ME for accessing a 3GPP network. This may be an IMS network. MCIM may reside on a UICC or on a TRE.

NOTE: As USIM and ISIM are by definition located on the UICC, these terms cannot be used in the context of this TR when the corresponding security data and functions are intended to reside outside the UICC. MCIM can be used similarly as USIM and ISIM are used for accessing networks, the difference being that MCIM may reside on a UICC or on a TRE. For the purposes of readability where MCIMs are hosted by a UICC, the term MCIM can refer to applications such as USIM or ISIM. If terms USIM or ISIM are used then they refer to the traditional USIM or ISIM that reside on the UICC.

**M2M end user:** The entity using the M2ME. In general, a M2M end user might not have any direct contractual relationship with the MNO providing service to the M2ME.

**M2M subscriber:** The entity "owning" one or more M2ME(s) and having a contractual relationship with the MNO to provide service the M2ME(s).

**M2ME :** A M2ME is a device equipped for Machine To Machine Communication, which communicates through a PLMN.

**M2ME identity:** A permanent private identity that uniquely identifies each M2M Equipment. The M2ME identity is installed in the M2ME by the supplier. The M2ME identity follows the same format as the IMEI.

**Provisional Connectivity ID** (PCID): A temporary private identity that identifies each M2ME. The PCID, where required, should be installed in the M2ME by the supplier in order to allow the M2ME to register in a 3GPP network without being associated yet with any specific future selected home operator. The PCID follows the same format as the IMSI.

**TRE identity:** A permanent private identity that uniquely identifies each Trusted Environment. The TRE identity is installed in the TRE by the TRE supplier in order to be able to identify the TRE during provisioning of MCIMs.

## 3.2 Symbols

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

<symbol> <Explanation>

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

| | |
|---|---|
| ACL | Access Control List |
| ADSL | Asymmetric Digital Subscriber Line |
| AN | Access Network |
| AV | Authentication Vector |
| BOOTP | BOOTstrap Protocol |
| CCIF | Connectivity Credentials Issuing Function |
| DdoS | Distributed Denial of Service (attack) |
| DHCP | Dynamic Host Configuration Protocol |
| DM | Device Management |
| DPF | Downloading and Provisioning Function |
| DRF | Discovery and Registration Function |
| HO | Home Operator |
| ICF | Initial Connectivity Function |
| ICSP | Initial Connectivity Service Provider |
| IP | Internet Protocol |
| MCIM | Machine Communication Identity Module |
| MITM | Man In The Middle (attack) |
| MMI | Man-Machine Interface |
| M2M | Machine-to-Machine |
| M2ME | M2M equipment |
| NGN | Next Generation Network |
| OCSP | Online Certificate Status Protocol |
| OMA | Open Mobile Alliance |
| PCID | Provisional Connectivity IDentity |
| PfC | Platform Credential |
| PKCS | Public Key Cryptography Standard |
| PKI | Public Key Infrastructure |
| PN | Personal Network |
| PNM | Personal Network Management |
| PS | Packet Switched |
| PVA | Platform Validation Authority |
| RAM | Remote Application Management |
| RFM | Remote File Management |
| RO | Registration Operator |
| SHO | Selected Home Operator |
| TCG | Trusted Computing Group |
| TRE | Trusted Environment |
| VNO | Visited Network Operator |
| WLAN | Wireless Local Area Network |

# 4 Use cases and requirements

## 4.1 Use cases

SA1 has performed a study in TR 22.868 where they have identified a number of use cases (cf. TR 22.868, clause 4.4 [2]) covering the most important user requirements and also outlined some areas where they think improvements are needed. This section provides more detail on some of those use cases to clarify the security requirements on M2M systems.

Use Case 1: Traffic Cameras

Traffic cameras with cellular connectivity may be installed in locations such as motorway overpasses or remote stretches of roadway. Cameras may also require simultaneous secure local WLAN connectivity to the next camera down the road, e.g. when measuring average speed. It will be necessary to securely provision these cameras with subscription credentials. When cameras are deployed over a large area, it may be necessary to be able to select a carrier for a given camera after it has been deployed, and this selection process must be properly secured. Secure post-deployment changes in subscription data will also be needed.

Use Case 2: Metering

A change of utility by the residential customer may also require a change in operator. The utility itself may switch operators, requiring a change to many meters dispersed over a large geographical area in a limited timeframe. The management of these changes may require complex accounting mechanisms. Without the ability to remotely change subscription, a service person may need to visit each affected device. For commercial applications, obtaining physical access to deployed devices may be expensive, because of geography, extreme environmental conditions, or the need to interrupt a manufacturing process (e.g., petrochemical refining). Therefore, remote means to change subscription could be needed.

Use Case 3: Vending

Vending machines are subject to regular attacks on their contents, which increases the threat to other items of value in the machine. Vending machine connectivity may come from a Home NodeB or 3GPP I-WLAN access within the M2M subscriber premises. A change in the customer's choice of network operator may require an update to subscription data in many vending machines in a short time. The M2M subscriber may also change its preferred network operator.

Use Case 4: Asset / Cargo Tracking

Asset and cargo tracking will often require that the M2M equipment be placed in areas where physical access is difficult. Such placements would be part of a service provider's attempt to resist theft and tampering with the M2M equipment. These placements can make it difficult and costly to gain physical access to the M2ME to change subscription credentials. As noted in TR22.868, this is "practically impossible" under the current solution, and a means of securely re-provisioning MCIM applications over the air would therefore be very beneficial.

## 4.2 Use case analysis

The following issues can be identified from the use cases defined in TR 22.868 [2] and discussed above, and a number of features are proposed that could be beneficial to study in order to solve the identified issues.

**Issue 1: How to prevent theft of and tampering with subscription credentials**

In Use Cases 1, 2, and 3 of TR 22.868 [2], the problem is identified of how to ensure that the M2M equipment is tamper resistant, and in particular to ensure that the M2M subscriber's credentials cannot be removed by simply removing a UICC. The discussion in clause 4.1 also highlights the importance of tamper resistance. To solve this problem it would be beneficial to study the following options:

> Option 1: The UICC could be mechanically attached to the M2M equipment in such a way as to make it infeasible to remove the UICC, or where removing the UICC would render it permanently unusable. The USIM application would then still run and be managed in a secured, non-removable execution environment which is tamper resistant, namely the UICC.

Option 2: The MCIM application could be integrated within the M2M equipment in a protected module (i.e. without a physical UICC). That protected module would be required to provide for the MCIM application a secured execution and storage environment which is tamper resistant in the M2M equipment. Such an environment requires counter-measures against logical and physical attacks on the MCIM application, similar to counter-measures that are currently provided by a physical UICC.

Option 3: The USIM application is implemented on a removable UICC, but appropriate techniques could be applied to discourage or invalidate the UICC removal (i.e. making the UICC removal unproductive or even counterproductive for the attacker). These techniques may include physical countermeasures.

All of these options would have the feature that even if an attacker is able to steal the M2M equipment, s/he would not be able to tamper with or remove the subscription credentials from the M2M equipment.

**Issue 2: How to initially provision a new M2M equipment with a new USIM application from an operator of M2M subscriber choice**

If we assume that the UICC is mechanically attached to the M2M equipment as per **option 1** above, there are the following subcases:

a) The USIM application is provisioned to the UICC prior to being mechanically attached to the M2M equipment. In this subcase, the M2M subscriber selects his home operator upon ordering the M2M equipment from the supplier. The selection of home operator by the M2M subscriber is straightforward (no new provisioning processes are required). The M2M subscriber may select the home operator based on the M2M end user's needs/requests. The M2M subscriber might also play the role of a M2M end user.

b) The USIM application is provisioned to the UICC after being mechanically attached to the M2M equipment. This allows the M2M subscriber to select his home operator while receiving the M2M equipment from the supplier. Some form of security credential will need to be provisioned onto the UICC in advance to facilitate the provisioning of the initial USIM.

If we assume that the USIM application is integrated within the M2M equipment as per **option 2** above (i.e. not using a physical UICC), the following issues need to be addressed:

- How can the M2M subscriber select his chosen home operator after the M2M equipment has been delivered from the supplier?

- How can the M2M equipment be remotely and securely provisioned with a new MCIM application from the operator chosen by the M2M subscriber?

- How can the home operator ensure the trustworthiness of the M2M equipment?

To solve these issues it would be beneficial if it was possible to:

- Select the home operator of the M2M subscriber's choice

- Obtain a secure connection to a network for the purpose of registration and provisioning

- Register on-line with the chosen home operator for obtaining a subscription to that operator's networks. This includes the possibility of linking the new equipment to an existing subscription.

- Verify credentials for the M2M equipment's trustworthiness as a receptor of such provisioning service before the home operator allows provisioning of the M2M equipment to take place. The components to be verified for authenticity and/or integrity should include the secure module and the M2M equipment ("the platform"). Optionally, the home operator may choose to verify only the TRE e.g. using TCG [3].

- Initially download a MCIM application of the M2M subscriber's choice into a new M2M equipment, over a secured channel. It should also be possible to perform this initial download after the M2M equipment has been delivered to the M2M subscriber

- Deploy a large set of M2M equipments and associate them with a particular home operator. This could require batch registration and provisioning of M2M subscriptions.

- Operate a secure process for on-line provisioning and management that provides at least authentication of origin, confidentiality, data integrity and anti-replay protection.

If we assume that the USIM application is implemented on a removable UICC, as per **option 3** above, the selection of home operator by the M2M subscriber is implicit in the UICC chosen. This case is straightforward in the sense that it does not imply new processes, logistics and distribution for the chosen home operator. Hence it does not imply additional costs, nor new provisioning processes, for the chosen home operator. However, the process of choosing the home operator may have additional impacts e.g. that the M2M subscription might not be changeable to another operator without additional costs or physical replacement of the UICC.

**Issue 3: How to change subscription to a different operator**

Use Case 3 of TR22.868 [2] also describes the problem of when the M2M subscription needs to be changed to a different operator due to a change of power supplier, who happens to have a contract with a different mobile operator.

For this specific issue, the following subcases need to be considered:

a) Authorized change of subscription. A subcase for this is authorization for the change of the removable physical UICC

b) Unauthorized (i.e. fraudulent) change of subscription.

NOTE 1: In case, that the operator and the M2M user have a special contractual agreements e.g. if the equipment is subsidised, the possibility to change to another operator might be limited.

The usage of a removable UICC in the M2M equipment is conceptually straightforward to enable change of subscription. However, there may be issues with arranging the physical swapping of UICCs e.g. customer service calls.

NOTE 2: With reference to the specific Use Case 3 of TR 22.868 [2], the costs of replacing the UICCs of the M2M equipment are at the expense of the new power supplier that is willing to make business with a new mobile operator. Also, how to physically prevent, in an adequate and effective way, the unauthorized UICC removal from the M2M equipment cannot be considered within the scope of 3GPP.

A related issue is the possibility that another operator might try to migrate the current operator's M2M end users, with or without the consent of the end users but without the consent of the current operator.

NOTE 3: The issue below was proposed for the TR but it was not considered further as it was regarded to be out of scope of the TR.

**Issue 4: How to upgrade software and security credentials**

The number of M2M services, and use case scenarios, is expected to grow over time. Additionally some M2M services may have long product and service life cycles, e.g. smart meters. Security experts and cryptographers often discover new attacks on systems. This coupled with the constant improvements in computing capabilities, often force security managers to upgrade key lengths and modify security policies. In some instances there may be a need to upgrade algorithms. In some other instances, there may be a need to distribute security patches to address vulnerabilities in protocols and applications that are not known at the time of installation .

## 4.3 Requirements

### 4.3.1 Security requirements

From the analysis in clause 4.2, the following requirements can be derived:

I. It should be possible to prevent theft of or tampering with the subscription. The following options could be considered:

Option A: The physical UICC is mechanically attached to the M2M equipment (i.e. the UICC is not physically removable from the M2M equipment): At least one of the following solutions is required:

- A mechanism to logically bind a UICC with the M2ME, e.g. a device pairing mechanism (the implementation details of this may be out of scope of 3GPP).

- Additional mechanical protection mechanisms, of which implementation aspects are out of scope of 3GPP.

- Optionally network based restrictions of services assigned to a subscription (Service Profile).

Option B: The MCIM application is integrated within the M2M equipment in a trusted environment (TRE) (without a physical UICC). At least one of the following solutions is required:

- A secure execution environment;
- A secure storage environment that protects secrets;
- A mechanism to prevent the loading of unauthorised software on the M2M equipment, both for the case of operating system boot-up ("secure boot") and for the case of downloaded software that would cause the incorrect execution of the MCIM application;
- Sufficient physical protection against attacks;
- Support of at least one authentication algorithm and cryptographic mode of operation, preferably two authentication algorithms and mode of operation
- Tamper resistance;
- Secure storage and use of credentials that are established using secure methods (e.g. no plaintext input of credentials over the air);

NOTE: The network can also restrict the range of services the M2M can use e.g. by setting the M2M subscription to a data-only subscription with a limited low data volume in the network.

- Optional provision of means of detection and reporting (to a TBD network entity) of evidence of tampering on the MCIM functionality or the trusted environment (TRE) within the M2M equipment that provides such functionality;
- To fulfil other relevant requirements. Those relevant requirement might be originated from one or several of the following documents OMTP TR0 [5], OMTP TR1 [6], TCG [3], GSMA/EICTA Principles concerning handset theft [7] and other relevant industry standards on prevention against attack.
- Network based restrictions of services assigned to a subscription (Service Profile)

Option C: Physically removable UICC. At least one of the following solutions is required:

- A mechanism to logically bind a UICC with the M2ME, e.g. a device pairing mechanism (the implementation details may be out of scope of 3GPP)
- Additional mechanical protection mechanisms of which implementation details are out of scope of 3GPP
- Network based restrictions of services assigned to a subscription (Service Profile)

For the integrated MCIM option, it should be possible for the mobile operator to verify the secure execution environment prior to provisioning of the downloadable MCIM application.

- For the integrated MCIM option, it should be possible to securely initially provision a new MCIM application to the M2M equipment.
- For the mechanically attached UICC and integrated MCIM options, it may be required to securely change the subscription in the M2M equipment remotely.
- For the mechanically attached UICC and integrated MCIM options, it may be required to remotely upgrade security credentials, cryptographic contexts, cryptographic algorithms and methods.
- Data traffic sent or received by an M2M terminal should have the same protection against eavesdropping or modifications as traffic processed by any 3GPP UE.
- Exposure of subscriber authentication keys to unauthorised 3rd parties would have severe consequences for the GSM and UMTS industry and shall therefore be prevented.
- Any new security relevant functionality or process shall not jeopardise an operator's ability to fulfil obligations towards regulators and government authorities to guarantee secure authentication and billing.

### 4.3.2 Other Requirements

- It should be possible to find a viable business model with the technical solution.
- If the solution has an impact on existing subscriber management business processes, then the benefits of the solution should compensate for any additional cost and complexity of the new processes.
- If the solution has an impact on existing network infrastructure, then the benefits of the solution should compensate for any additional cost and complexity of the new infrastructure.
- If the solution has an impact on existing terminal architectures, then the benefits of the solution should compensate for any additional cost and complexity of the new terminal architectures.
- The MCIM should support a number of lifecycle states (e.g. installed but not activated, activated, suspended).
- It should be possible to securely update the software and firmware of the M2M equipment OTA.
- It may be required to prevent the replacement of one operator's MCIM application with that of another operator without the consent of all parties involved.
- Appropriate software isolation will be enforced between the secure environment or UICC and the main processing environment of the M2M equipment, and possibly within the secure environment or UICC itself.
- It should be possible for an operator who has a MCIM application installed in the M2M equipment to configure some aspects of the security policy of the M2M equipment.
- It should be possible for the MCIM application to be updated OTA.
- Initializing, bootstrapping, updating, and other related procedures should be automated, scalable, and efficient with respect to message exchanges and number of roundtrips, without compromises on security.
- Any solution must preserve the ability of an operator to fulfil obligations towards regulators and government authorities to guarantee secure authentication and billing.

## 4.4 Evaluation criteria

NOTE: The order to this list has no implications on the importance of the issue at stake. The following criteria are defined and they need to be used for evaluating candidate solutions:

1) **Security**: How well does the solution meet the security requirements listed above and other relevant threats presented in the threat analysis sections?
2) **Initial choice of operator**: How well suited is the solution to the M2M requirements relating to initial choice of operator?
3) **Operator change**: How well suited is the solution to the M2M requirements relating to operator change?
4) **Remote Management**: How well is the solution suited to remote management (provisioning and change) of subscriptions?
5) **Legal and regulatory impact**: How well does the solution address legal and regulatory requirements? (Note that as these requirements vary across countries, legal and regulatory requirements will have to be derived in order for this criterion to be meaningfully applicable.)
6) **Flexibility to adapt to new requirements**: How easy is it to adapt or extend the solution to address new requirements related to M2M?
7) **Viability of trust model**: Can the trust model be translated into a plausible business model?
8) **Suitability to mass market deployment**. Is the solution cost effective and scalable to the very large deployments envisioned within the M2M use cases?
9) **Impact on subscription management systems**: How much impact does the solution have on an operator's existing subscriber management systems? If new systems are required, what is their complexity?

10) **Impact on network infrastructure**: How much impact does the solution have on an operator's existing network infrastructure? If new infrastructure is required, what is its complexity?

11) **Impact on terminal**: How much impact does the solution have on the M2M terminal equipment? Can existing components be used, adapted or enhanced or do new components have to be developed?

12) **Impact on 3GPP specifications**: To what extent can existing specifications be re-used? What new specifications are needed?

The list of criteria is purposefully kept short but comprehensive to ensure that the analysis of solutions is manageable.

# 5 Candidate solutions

## 5.1 Alternative 1a: TRE based solution with remote subscription provisioning and change

### 5.1.1 MCIM

#### 5.1.1.1 Lifecycle of MCIMs

MCIMs should be able to exist in any one of the following lifecycle states:

**Installed**: an instance of a MCIM has been created and has an entry in the M2ME's registry

**Activated**: an instance of the MCIM is authorised for operational use.

**Selected**: this state marks the commencement of a session with a MCIM. Only an activated MCIM can be selected. When the session ends, the MCIM reverts to the Activated state.

**Blocked**: an instance of a MCIM has been temporarily de-activated and is not available for use. An example of this is when the status of an application-specific PIN becomes "blocked", as described in [8]. Unblocking of a MCIM causes it to be restored to the Activated state.

**Retired**: an instance of a MCIM is permanently unavailable for use, but is still instantiated in the M2ME. An example of this is where a credential is permanently deleted but some executable components of the MCIM that are used by other applications are still active.

**Deleted**: a MCIM is permanently removed from the M2ME's memory. Deletion may be applied to a MCIM that is in any of the above lifecycle states except for the Selected state.

The following figure 5.1.1.1-1 illustrates the state transition diagram for the MCIM lifecycle states. This can typically be viewed as a sequential process with certain possibilities for reversing a state transition or skipping states.

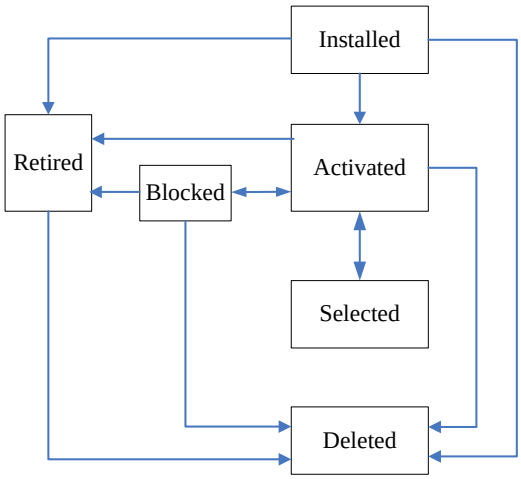


**Figure 5.1.1.1-1: MCIM lifecycle state transitions.**

NOTE: 3GPP specifications may place restrictions on the ability of multiple MCIMs to be active simultaneously.

### 5.1.1.2 Contents of a Typical Downloadable MCIM

A typical downloadable MCIM would include credentials, executables (including algorithms and a system of files and access control mechanisms) and data (e.g. file contents, security policy, etc). Further details can be found in the detailed example in B.2.4.

Sensitive objects within the MCIM package should be encrypted.

The download and provisioning service and M2ME could conduct a protocol conversation prior to provisioning a MCIM, to see which parts of the MCIM are already available in the TRE. This is particularly relevant if MCIMs are to be shared in the TRE.

Some standardisation of MCIM packaging will be necessary, so as to avoid proprietary implementations by different M2ME equipment suppliers and download and provisioning services. Further details on packing can be found in the detailed example in B.2.4.

NOTE1: Liberty Alliance protocols such as Advanced Client could be suitable candidates.

NOTE2: The provisioning of the MCIM application to the M2ME, likely requires the existence of
a) a TRE platform key for which the application secrets are sealed
b) a platform credential (issued by the PVA) certifying the public part of the platform key.

## 5.1.2 Trusted Environment (TRE)

### 5.1.2.1 Notes

Some of the functions in this section are described in more detail as security counter measures in the section on threat analysis.

Functions in this section are cross-referenced to the counter-measures that are described in the section on threat analysis. The cross-referencing takes the form [t*x* c*my*], where t*x* means threat #x and c*my* means counter-measure #y.

This section uses the term "stakeholder" to describe a person or entity who has an interest in the correct operation of the MCIM ecosystem. Typical stakeholders include operators, users, and M2M equipment suppliers.

### 5.1.2.2 General Functions of a TRE

A TRE [t1 cm1] should be a logically separate area in the M2M equipment with hardware support for this separation [t1 cm1, 2]. It is not necessarily a removable module, i.e. it can be functions within an IC or functions that are distributed

across a group of ICs. A TRE should define logical and physical interfaces to the outside world, including interfaces to specific functions in the M2ME. Such interfaces should be usable only under control of entities which are authorised to communicate directly with a TRE [t4 cm2, t6 cm1]. Such interfaces should not be able to compromise the confidentiality, integrity or availability of MCIMs or of a TRE [t4 cm3, t8 cm5].

A TRE should provide a root of trust for a secure storage and secure execution environment for multiple MCIMs and for certain functions concerned with the provisioning and management of MCIMs [t1 cm1, t2, cm3].

A TRE should be pre-provisioned in a secure, out-of-band facility with any required cryptographic keys and other credentials. Other security-critical functions of a TRE are also typically pre-provisioned onto the M2ME in the same way [t5 cm1, 2]. Other functions are typically provisioned by download after the M2ME is issued.

NOTE 1: The definition of which TRE functions may be downloaded after issue of the M2ME is FFS, if it is deemed within the scope of 3GPP to define that.

A TRE should provide a degree of protection against physical and logical attacks [t3 cm1, t4 cm1, 2, 3, 4]. Any tampering with a TRE or with secure functions in the M2ME should be detected and should result in lockdown of the TRE [t4 cm5, t6 cm5].

NOTE 2: A locked down M2ME might be re-provisioned again, when the correct state has been confirmed. The M2ME will not be reachable over the network while in locked down state.

A TRE should support and enforce its own security policy [t6 cm3].

A TRE should perform security-related functions to support the DRF in its function of assisting the M2ME to discover and register itself at the SHO [t7 cm6]. Examples of such functions may include, but are not limited to, secure storage, retrieval, and use of the M2ME's PCID.

A TRE should perform security-related functions to support the PVA to validate the authenticity and integrity of the M2ME when required. Such validation should occurbefore a MCIM can be downloaded and provisioned into the M2ME [t1 cm4, t3 cm4, t7 cm5]. Computation of cryptographic signatures is one such function. Others are possible.

A TRE should be sufficiently secure as to allow the storage and execution of AKA functions that are currently implemented only in UICCs [t3 cm1].

A TRE should securely store the identity of the M2ME platform and should be capable of securely authenticating that identity to the issuing authorities using standardised protocols. The M2ME identity is embedded as part of a physically secure, out-of-band process that takes place before the M2ME is issued. The TRE may also have its own identity. If it does, the TRE should securely store this identity and may be capable of securely authenticating the TRE identity to the issuing authorities using standardised protocols [t1 cm3, t5 cm2].

A TRE should be able to perform user authentication and access control for single or multiple users, where relevant to the use case for that type of M2ME [t10 cm 1 - 11].

A TRE may provide a secure audit record of its transactions. Typically, these records would be protected against unauthorised access [t8 cm9].

A TRE should be able to be updated remotely by an authorised entity using secure protocols [t6 cm4].

NOTE 3: At the time of writing, UICC specifications are not fully capable of supporting the required functionality of a TRE, as described herein. However, if future enhancements are made to UICC specifications, it is possible that a TRE could be implemented on a UICC. See also candidate solution 1b in clause 5.2.

Future enhancements that can be considered for TREs include support for multiple isolated, trusted domains, each with or without MCIMs, and owned by a stakeholder [t8 cm1]. Such domains could be completely isolated from each other, or be isolated against tampering and unauthorized access but could provide inter-domain services. If such domains do provide services to each other, these domains may also provide inter-domain authentication functionality to each other, with the assistance of the TRE itself [t8 cm2, 3].

#### 5.1.2.3 TRE Functions Related to the Management of MCIMs

A TRE should be responsible, on behalf of the M2ME, for enforcing the security of the remote provisioning of MCIMs [t2 cm1, 3].

A TRE should check the integrity of MCIMs as part of a secure boot process whenever the TRE is reset. A TRE may also check the integrity of MCIMs at the start of each session with that MCIM. Detection of anomalies should result in that MCIM being placed into the "blocked" lifecycle state [t6 cm5, t8 cm8].

A TRE should allow MCIMs to share MCIM functions, e.g. cryptographic algorithms, but only where authorised by the security policies of the respective MCIMs and only where the MCIMs have been activated [t8 cm2].

The security of the process of transitioning MCIMs through their lifecycle stages shall be assured by a TRE [t3 cm3, t7 cm1, t8 cm6].

A TRE should maintain a registry of the MCIMs that it manages, so that (for example) an authorised entity can discover what MCIMs are supported in the M2ME and their current lifecycle stages and security status [t7 cm6, t8 cm7].

A TRE should enable authorised stakeholders to remotely discover the presence and lifecycle stages of supported MCIMs of that stakeholder [t7 cm6]. A TRE should also permit authorised functions within the M2ME to discover or verify the presence and lifecycle status of MCIMs.

A TRE should be able to support and enforce security controls relating to MCIMs. MCIM-specific security controls may be specified by a stakeholder such as the SHO. Where a security control is a discrete object, e.g, an ACL, it may be provisioned along with the MCIMs. Overall security controls governing the general usage and management of MCIMs may be provided by a stakeholder such as the M2ME equipment supplier [t2 cm4, t7 cm2 - 4, t8 cm3 - 4].

A TRE should support a secure update service for MCIMs and the use of standardised protocols such as OMA-DM or OTA RFM is preferred. Updates should only be accepted from an authorised, authenticated source [t7 cm7].

#### 5.1.2.4 TRE Functions Related to the Remote Provisioning of MCIMs

A TRE should be sufficiently secure to permit the on-line provisioning of MCIMs whose security is currently assured by provisioning the equivalent applications out-of-band onto UICCs [t3 cm1].

A provisioning protocol or suite of protocols is used to securely register a user on-line for service and to securely transport MCIMs from a download and provisioning service in the network to the M2ME [t2 cm1, 2]. Only a TRE should be responsible for enforcing the security aspects of that process [t2 cm3, t3 cm4]. The registration and provisioning phases should be cryptographically bound together [t2 cm5, t5 cm4, t12 cm2].

Where security controls, e.g. ACLs, are discrete objects that are provisioned along with a MCIM, a TRE should treat them as part of the MCIM for security purposes [t2 cm4, t3 cm5].

A TRE should perform all security processing required at the M2ME for remote provisioning and management protocols [t2 cm3, t3 cm4, t7 cm8].

The TRE should support all required functions for MCIM lifecycle management. The TRE should be able to verify that any instructions received as part of MCIM lifecycle management come from a valid, authorised source. This applies whether the instructions are pushed to the M2ME or pulled from the management server. A TRE should enforce the rule that an MCIM required for a given service can only be provisioned to an M2ME that acts on behalf of the M2ME subscriber who registered for that service. This implies that phases of the secure session between the TRE and the download and provisioning service should be bound to each other by some access control key/token [t2 cm5, t5 cm4, t12 cm2]. For instance, Liberty Alliance protocols separate the registration process from the actual provisioning process but bind them together with security tokens and identifiers.

The download and provisioning service can remotely query the system state of the M2ME to ensure that MCIMs will be stored only in a valid M2ME. This process may require handling platform validation information before the provisioning of MCIMs can proceed. A TRE's security policy may apply further conditions by specifying which provisioning-related events are permitted to drive a M2ME/TRE authentication [t1 cm4, t5 cm5].

NOTE: Full details and definitions of remote validation are not part of the present document.

## 5.1.3 Network architecture

### 5.1.3.1 Introduction

This network architecture uses a model consisting of services and technical functions that are necessary to build those services. Services are supplied to and consumed directly by the M2ME, for connectivity, provisioning and management of MCIMs, etc. In a typical architecture, it is likely that the various technical functions would be incorporated into a small number of Roles.

We define Roles as entities that provide services directly to the M2ME and with which the M2ME is able to communicate directly (with the exception of the regulator). Roles may be trading companies such as network operators, equipment suppliers, etc., or sub-divisions thereof.

Roles may perform one or more technical functions. In this document, where a Role is single-function, that function is described under that Role. Where a Role performs multiple functions, those are described in the technical functions section. The allocation of services and functions to a role can be done in many different ways and is determined by business as well as technical considerations.

NOTE: The grouping of technical functions into Roles herein is only one possible example and is not in any way definitive.

### 5.1.3.2 Principles of the Network Architecture

The following principles characterize the network architecture:

- Unified architecture to support MCIM provisioning and management for M2M equipments of different types and capabilities
- Separation of the connectivity services and MCIM management services
- Separation of initial and operational connectivity services
- Security of the MCIM management to be independent of the security of the initial connectivity service
- Requirement for IP connectivity for provisioning and management of MCIM credentials and applications
- Use of provisional connectivity IDs to obtain registration of the M2ME with the selected home operator through a secure connection via a visited network operator
- Validation of the authenticity and integrity of the M2ME as a trusted platform before provisioning takes place
- Support for re-provisioning due to change of selected home operators

### 5.1.3.3 Services

#### 5.1.3.3.1 Summary

Services are used directly by the M2M Equipment (M2ME) and/or M2ME Subscriber for remote management of MCIM functionality on an M2ME. They can be broadly categorized into three groups:

- Connectivity Services, subdivided into:
  - Initial network connectivity
  - Operational connectivity (including connectivity activation)
- Application Services, subdivided into
  - Discovery and registration
  - MCIM download and provisioning
- M2ME supply

An optional fourth service, Delayed Activation, is described in Annex B.1.

#### 5.1.3.3.2 Connectivity Services

##### 5.1.3.3.2.1 Initial Network Connectivity Service

The Initial Network Connectivity Service consists of 4 transactions:

- Initial network connectivity set-up
- AN-specific address resolution
- IP connectivity for provisioning and management of MCIMs
- IP connectivity for provisioning and management of M2M applications

Initial network connectivity set-up:

Before connection to a provisioning or management service can be achieved for the first time, i.e. before the operational MCIM(s) have been downloaded and activated, initial network connectivity must be achieved to an IP network. The M2ME is required to support bootstrapping functions for this purpose. Several different solutions to this problem may be required, depending on the type of equipment and on the type of AN that is available to the equipment for. Examples could include:

- Use of pre-provisioned preliminary credentials to access a visited 3GPP PLMN;
- Use of user-provided or pre-provisioned credentials to access a fixed-network or WLAN.

Other possibilities for equipment types and AN types are described in the use cases in the present document and in [2].

The process of providing initial 3GPP network connectivity to a M2ME should not require the VNO to support any new functions related to the acquiring of AVs from an ICO. This requires the ICO to support existing method of providing AVs, e.g. MAP. Therefore, standard AKA functions are required in the M2ME for the purpose of obtaining initial connectivity to a VNO's 3GPP network. Such initial AKA functions in the M2ME would typically include a preliminary credential (e.g. a PCID) as well as shared secret key(s) and cryptographic algorithm(s). These objects would typically be exchanged between the equipment supplier and the CCIF and pre-provisioned into the M2ME by the equipment supplier in a secure facility.

The initial AKA functionality (data and executables) may be stored and/or executed within the TRE. Bootstrapping credentials may also be provided for accessing non-3GPP networks, e.g. WLAN, but the precise nature of those credentials is out of scope.

Future enhancements to the M2ME's AKA functions for initial network connectivity may include the capability to download and replace the existing initial connectivity credential with a new one.

The M2ME should be allowed to use the initial network connectivity only for the purposes of provisioning and maintenance of MCIMs, and not for accessing other network services.

AN-specific address resolution:

Once initial IP connectivity is set up, the M2M equipment needs to know the address of one or more servers in order to proceed with the provisioning process. These addresses may be provided by any of several commonly used bootstrap mechanisms including BOOTP/DHCP for IP networks and OMA DM bootstrap for 3G networks. These mechanisms are not part of the initial connectivity, but can be used to provide a solution to the address resolution problem in cases where the necessary server address(es) cannot be preconfigured into the M2M equipment.

IP connectivity for provisioning and management of MCIMs:

Once initial IP connectivity has been established, IP connections to the registration, provisioning and management services can be achieved for the purpose of obtaining the operational network-access credentials and any additional needed configuration, such as security policies and software. The process for provisioning and management of operational credentials is independent of the AN being used. Furthermore, there is independence between the AN used for initial connectivity and the networks over which the operational credentials will be used. This allows any AN to be used to provision the operational network credentials and associated algorithms and software. For example, this

includes MCIM applications with the needed credentials and parameters. For example, any ANs that provide initial connectivity can be used to provision:

- Credentials for access to the operational network
- Authentication software and algorithms that operate on the afore-mentioned credentials

Examples of these include:

- a USIM application and an associated USIM credential that will be used by the M2M equipment for operational access to 3GPP;
- an ISIM application and an associated ISIM credential that will be used by the M2M equipment for operational access to an IMS, over any available AN.

IP connectivity for provisioning and management of M2M applications:

The provisioning and management of M2M applications may require IP connections to entities that are distinct from those used to provision and manage the operational credentials. The independence of this function from the AN will be as described above.

#### 5.1.3.3.2.2 Operational Connectivity

Operational connectivity is essentially identical to regular CS or PS connectivity provided in GSM, UMTS or EPS. The only difference is that M2M-specific filters may be applied in the M2M equipment and/or the network to restrict the sets of entities with which an M2ME can communicate. These filters could be realized by constraining communication to certain APNs in PS service. In a rental car tracking application, for example, the M2M equipment could be restricted to communicating with the M2M server of the car rental company.

Operational connectivity may also include a separate provisioning activity to set up (3GPP) network connectivity parameters such as SMS service centers and internet connectivity. Connectivity to an IMS may be required using the appropriate layers of the operational AN.

The owner of the M2M equipment should be able to change the IP connectivity subscription from one operator to another without having to go through an initial connectivity state.

### 5.1.3.3.3 Application Services

#### 5.1.3.3.3.1 Discovery and Registration Service

The discovery and registration service allows the M2ME to discover and securely register with the Selected Home Operator.

#### 5.1.3.3.3.2 MCIM Download and Provisioning Service

This service allows the M2ME to securely obtain the required MCIM application(s) and their parameters.

### 5.1.3.3.4 M2ME Supply Services

In this service the configured M2MEs are supplied to the M2ME subscriber. The M2MEs supplied should have all necessary root credentials installed and be capable of supporting the other services. All M2MEs must meet the relevant requirements and must support a TRE as described in section 5.1.2.

## 5.1.3.4 Technical Functions (in alphabetical order)

### 5.1.3.4.1 Connectivity Credential Issuing Function (CCIF)

CCIF is responsible for the generation of credentials required for initial network connectivity as described in clause 5.1.3.3.2.1. This function is required where unauthenticated connectivity may not be available to deployed M2MEs. This function could be provided by a central organisation or the M2MES. CCIF supports the following functions:

- Issuing initial network access credentials, e.g. preliminary IMSI numbers and preliminary keys, for each M2ME.

NOTE 1: For examples of preliminary credentials see annex B.

NOTE 2: Alternatives such as PCID and synthetic credentials could be possible.

- Helping the M2MES to configure the M2ME with the above credentials. Modes of such configuration may include:
  - CCIF generates credentials and sends to M2MES to embed during manufacture time; or
  - M2MES generates and embeds them and sends them to CCIF afterwards; or
  - M2MES generates and embeds them and they are communicated to CCIF via the M2M subscriber

#### 5.1.3.4.2 Discovery and Registration Function (DRF)

DRF helps the M2ME to discover and register with the SHO. Address resolution is included within DRF.

#### 5.1.3.4.3 MCIM Download and Provisioning Function (DPF)

This is a function for managing the downloading and provisioning of the MCIM applications and credentials to the M2ME.

In order to perform the secure provisioning of the MCIM applications and their parameters to the M2ME, the DPF needs to support the following functions:

- Receive some information (e.g. address) from SHO or RO (ICF) in order to access the M2ME, or alternatively rely on OMA-DM bootstrapping for inducing the M2ME to connect to the DPF
- Receive authorisation from the SHO or RO (ICF) to provision the M2ME. This could include a security token for communicating with the M2ME.
- Receive from the SHO the MCIM application and credentials package to be downloaded. Alternatively the DPF could generate this from stored rules and advise the SHO of the credentials that have been downloaded to the M2ME.
- Provision the MCIM application and credentials to the M2ME.
- Update previously downloaded MCIM applications or credentials and provisioning new applications as needed.
- Notify the SHO of the successful or failure of a provisioning event.

In addition to functions required to perform secure provisioning of the MCIM applications and their parameters to the M2ME, the DPF may support options to check the M2ME and/or TRE integrity prior to the provisioning. The DPF can obtain the verification data from the PVA and then, depending on relevant SHO security policies, allow or disallow the provisioning process.

#### 5.1.3.4.4 Initial Connectivity Function (ICF)

This function provides connectivity services (at layers above the basic network access provided by the VNO) to help with the post-purchase discovery of the SHO. The ICF:

- Provides IP connectivity for the M2ME to request downloading and provisioning of MCIM credentials and applications from a DPF via a Visited Network Operator (VNO) network.

In order to support this usage, the ICF may also:

- Authenticate the M2ME for connectivity functions, i.e. provide authentication vectors (AVs) to the connected VNO in order to allow the VNO to authenticate the M2ME at initial attach;
- Generate and transmit AVs or complete 3GPP attachment credentials to the M2M ES to allow for pre-configured credentials for temporary access, or;
- Receive AVs or complete 3GPP attachment credentials from either the M2M ES, the SHO or the M2ME subscriber.

### 5.1.3.5 Roles

#### 5.1.3.5.1 Summary

Examples of roles are given in this document are as follows:

1. M2M Equipment Subscriber
2. M2M Equipment Supplier (M2MES)
3. Registration Operator (RO)
4. 3GPP Visited Network Operator (VNO)
5. 3GPP Selected Home Operator (SHO)
6. Non 3GPP Initial Connectivity Service Provider
7. Platform Validation Authority (PVA)
8. Regulator

The mapping of technical functions onto roles that is used in the present document is described in the table below. It is only one example of a possible mapping and is in no way definitive.

**Table 5.1.3.5.1-1: Mapping of Roles to Technical Functions**

| ROLE | TECHNICAL FUNCTIONS INVOLVED |
|---|---|
| M2ME Subscriber | Single-function. Description of all functions is done at the Role level |
| M2ME Supplier | CCIF |
| Registration Operator | DPF, DRF, ICF |
| 3GPP Visited Network Operator | Single-function. Description of all functions is done at the Role level |
| 3GPP Selected Home Operator | Single-function. Description of all functions is done at the Role level |
| Non 3GPP Initial Connectivity Service Provider | Single-function. Description of all functions is done at the Role level |
| Platform Validation Authority | Single-function. Description of all functions is done at the Role level |
| Regulator | Single-function. Description of all functions is done at the Role level |

#### 5.1.3.5.2 M2ME Subscriber

The M2ME subscriber is the person or organization who receives M2M services under contract with an SHO, including services for connectivity and application registration and activation.

An M2ME subscriber must support selection of a SHO and deliver all the M2M equipment parameters to this SHO. An M2ME subscriber may support the following functions:

- Inform the RO of an impending subscription change from one SHO to another;
- Contact any relevant activation service provider;
- Provide the PVA with credentials needed for validation of the M2ME platform and/or applications provided by the M2ME, including those supporting MCIM remote management;
- Obtain credentials for the platform and/or applications from a trusted third party (e.g. M2MES or a third party that has a trusted relationship with the manufacturer or the supplier).

#### 5.1.3.5.3 M2M Equipment Supplier (M2MES)

The M2MES provides the M2M equipment to the subscriber. Typically the M2MES is a manufacturer. A M2MES may also be a business stakeholder in the initial connectivity service or in the application activation service. An M2MES may perform the CCIF to allow a credential for initial network access to be installed and securely stored in the M2ME

before downloading and provisioning of the MCIM takes place. A M2MES may provide a means for the M2ME subscriber to select the desired SHO, or for this to happen automatically when the equipment is connected to an access network.

NOTE: When the M2ME leaves the supplier, it is not normally associated with a SHO. However, some use cases may require the identity of the SHO and a corresponding discovery mechanism to be pre-configured in the equipment.

#### 5.1.3.5.4 Registration Operator

The purpose of this role is to provide initial connectivity to the M2ME and to provide registration and provisioning functions for the M2ME. This typically involves the Initial Connectivity, Discovery and Registration, and MCIM Download and Provisioning Functions.

#### 5.1.3.5.5 3GPP Visited Network Operator (VNO)

A VNO is any 3GPP operator that operates a network that is accessed for the purpose of initial registration and provisioning of the MCIM applications and credentials. The VNO and SHO may be the same operator, or they may be distinct operators. The VNO supports the following functions:

- Provide temporary 3GPP network access to the M2ME, where authentication using credentials such as a PCID may be required. A VNO may provide full or restricted connectivity during initial access.

- Provide open network access to the Discovery and Registration Function (DRF) when possible, i.e. where no credentials or authentication are required for this access. This function applies when the VNO will become the SHO after registration and provisioning, for example.

- Provide connectivity to SHO, when SHO and VNO are distinct operators.

#### 5.1.3.5.6 3GPP Selected Home Operator (SHO)

An SHO operates as follows:

- Has a subscription contract with the M2ME subscriber to provide operational connectivity services (and application services if it also takes on the role of an application service provider) for the M2ME;

- Authorises the DPF to provision M2MEs with MCIM parameters generated by, or generated on behalf of, the SHO;

- In case of re-provisioning and while there is an operational connection to an M2ME, provides connectivity services between the M2ME and a DPF for re-provisioning of a MCIM to the M2ME;

- In case of re-provisioning and while there is an operational connection to an M2ME, provides connectivity services for the attestation of the device with the help of the PVA for a re-provisioning of the MCIM application or credentials.

#### 5.1.3.5.7 Non-3GPP Initial Connectivity Service Provider

Non-3GPP Initial Connectivity Service Providers (ICSPs) are connectivity service providers such as fixed network service providers, IMS service providers, or WLAN providers that provide non-3GPP access to activation and registration services for the M2M equipment

#### 5.1.3.5.8 Platform Validation Authority (PVA)

The PVA is the authority responsible for validating the credentials used to verify the M2M equipment as a trusted platform. The PVA may also issue these credentials. The PVA supports the following:

- Validation of platform credentials that assert the authenticity and integrity of the M2ME as a platform to hold the MCIM application and credentials;

- Providing the DPF and SHO with information related to the success or failure of the validation of the M2ME.

- Obtaining new platform credentials when required, e.g. after a remote update of the M2ME.

The content and format of a PfC can have, e.g. the following variations. PfC may contain several parts some of which are device-specific and some common to a group of devices. E.g., (1) an M2M ES public key to act as the root of trust for verification (public, common), (2) a device-specific private key stored in the M2ME (secret, device-specific), (3) a certificate issued to the corresponding public key by the M2M ES (public, device-specific) asserting the expected system state of the M2ME. In this scenario, PfC needs to be obtained by PVA in advance of the manufacture in a secure manner; is embedded or initialized in the M2ME during manufacture; and can be provided along with other information during platform validation.

#### 5.1.3.5.9 Regulator

This is a governmental body or other legislative or regulatory entity governing the operation of the M2MEs and networks in a country or region.

### 5.1.3.6 Network Interactions for Remote Provisioning

#### 5.1.3.6.1 General

This section provides examples of the steps required for the M2ME to be remotely provisioned with an MCIM application and credentials. Both 3GPP access and non-3GPP access scenarios are described.

Remote provisioning using TRE as described in clause 5.1 can be implemented in various different ways, e.g. the DPF can be hosted by the RO or the SHO. Clauses 5.1.3.6 and 5.1.3.7 describe one example to implement remote provisioning and change when the DPF is hosted by the RO, and Annex B.2 describes another example when the DPF is hosted by the SHO. Annex B.2 also includes additional details of the network interactions using OMA DM.

#### 5.1.3.6.2 Overview of network architecture

Below we outline one example division of roles between the different entities. In this figure, the thick solid arrows indicate connections between the operators, service providers, and validation authorities, while the thin solid arrow indicates the air interface for the initial network access from the M2ME to the VNO's network. The dashed arrows indicate the IP connectivity between the M2ME and the RO (ICF) via the air interface provided by the VNO's network. The double dotted arrows indicate the connections between the M2ME and the RO (DRF) and DPF functions In this figure the DPF resides at the RO: it could also reside at the SHO (as is described in annex B).

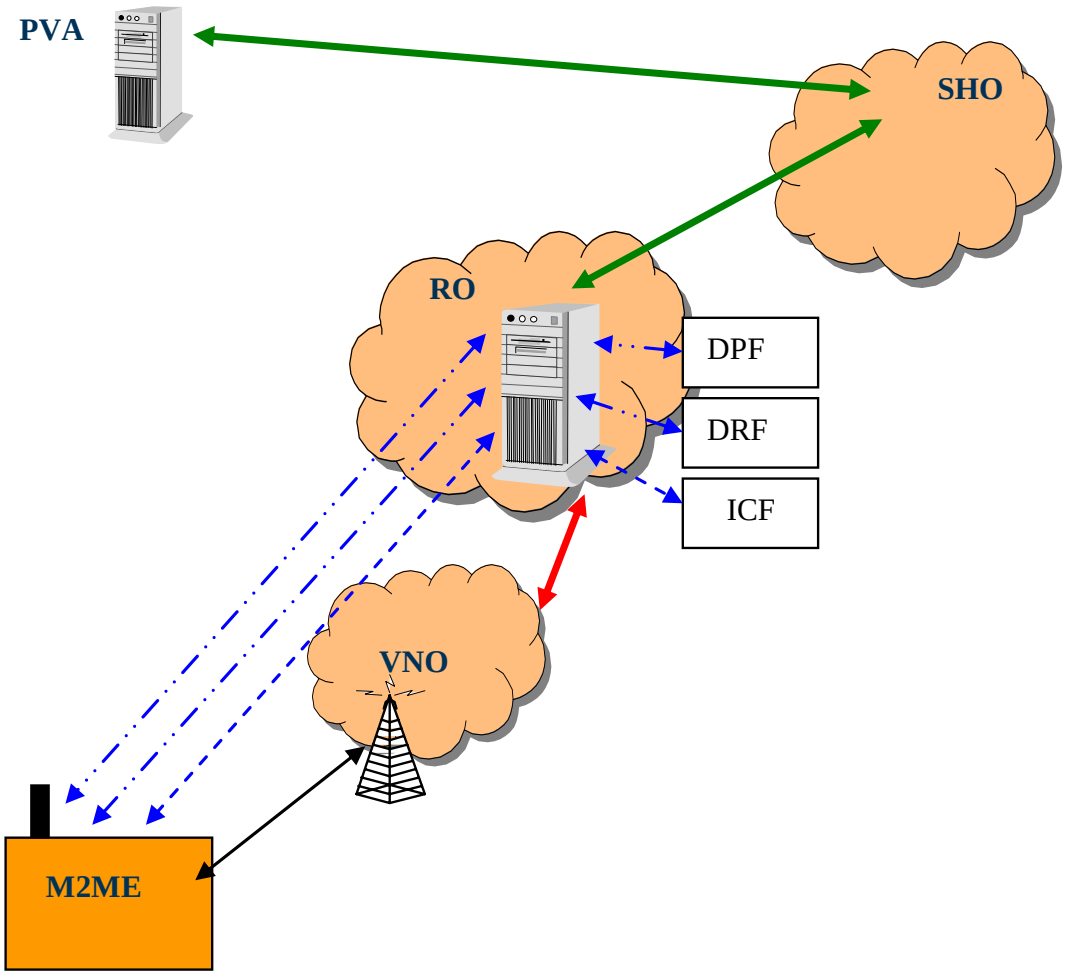


**Figure 5.1.3.6.2-1: Network authentication and MCIM Provisioning in the M2ME, in the case of 3G authenticated access.**

In some real-life situations, there may be only two operators physically present to provide access and services for an M2ME. In the interactions described in the coming clauses they would be an RO (incorporating ICF, DRF and DPF) and an SHO. In such cases, the RO could also serve as the VNO.

Further, in some cases the role of the PVA and the DPF may be hosted by the SHO as is done in the example provided in annex B. The VNO and SHO may be the same operator, although they will be logically separate entities until the M2ME has declared the identity of its SHO. There may be many alternative sets of network deployments which are not shown in this document.

### 5.1.3.6.3 Network Interactions for MCIM Provisioning in case of 3GPP Access

1. The M2ME uses the standard GSM/UMTS functions (GPRS/PS) to decode network information and attaches to the network of any VNO. In the attach message the M2ME sends a Provisional Connectivity ID (PCID) to the VNO. To avoid that the VNO needs to support special M2M functionality, the PCID has the same format as the IMSI. The "MCC" and "MNC" fields in the PCID will indicate to the VNO which entity it should contact to obtain authentication vectors to authenticate the PCID with.

2. The VNO contacts the RO (ICF function) and sends the PCID-IMSI to the ICF. Note that in some cases the RO and VNO may be the same operator.

3. Upon receiving the PCID-IMSI, the ICF queries the temporary-access credential associated with the PCID in its database. According to the credential, the ICF can generate AVs.

NOTE 1: If the ICF is not already in possession of the used PCID-IMSI and related temporary-access credential, it can obtain it from the CCIF.

4. The RO transfers AVs for the claimed PCID-IMSI to the VNO.

5. The VNO uses the AV to authenticate the M2ME through the AKA.

The step 1 to 5 describes the phase of initial attach.

6. The ICF request the DRF to bootstrap. Internally, the RO forwards the PCID and the IP address of the M2ME from its ICF to its DRF function.

7. According to the PCID-IMSI, the DRF queries the address of the DPF and the SHO which has contract with the M2ME in its database. Then it generates the Bootstrap message.

8. The DRF sends the Bootstrap message to the M2ME. In the message it includes the IP connectivity parameters (NAPDEF), the address of the DPF (Server URL), the context of the MCIM application provision and the context of the M2M application provision. If the provided PCID-IMSI already points to the RO, the RO could become the SHO , and then the IMSI is just continued to be used.

9. Triggered by the Bootstrap message, the M2ME contacts the DPF and includes relevant information of the M2ME and the TRE (e.g. platform validation info)

10. The RO (DPF function) connects to the SHO, and relays the M2ME/TRE info there.

The step 6 to 10 describes the phase of discovery and registration.

11. The SHO sends the validation info signed by the PfC and TRE identity to a PVA and requests a PVA to validate the authenticity and integrity of the TRE.

12. The PVA locally validates the authenticity and integrity of the M2ME, according to the requirements of the SHO.

13. The PVA sends the validation results back to the SHO, according to the SHO requirements.

14. The SHO encrypt the MCIM by using the PfC and generate the management object for M2M (e.g MCIMobj).

15. The SHO delivers the encrypted MCIM (e.g. within MCIMobj) to the RO (DPF) and authorizes provisioning of the MCIM application to the M2ME.

16. The RO (DPF) downloads a MCIM object to the M2ME.

17. The M2ME provisions the downloaded MCIM into the TRE. The TRE decrypts MCIMobj by using the TRE Platform Key to obtain the MCIM.

18. The M2ME reports the success/failure status of the provisioning to the RO (DPF).

19. The RO (DPF) reports the success/failure status of the provisioning back to the SHO

The step 11 to 19 describes the phase of MCIM application provision.

Thus the M2ME can attach to the network of the SHO by using the MCIM. Then the SHO provides the M2ME with operational service.

The procedure of how to initially provision the MCIM to the M2ME is executed as depicted in figure 5.1.3.6.3-1.

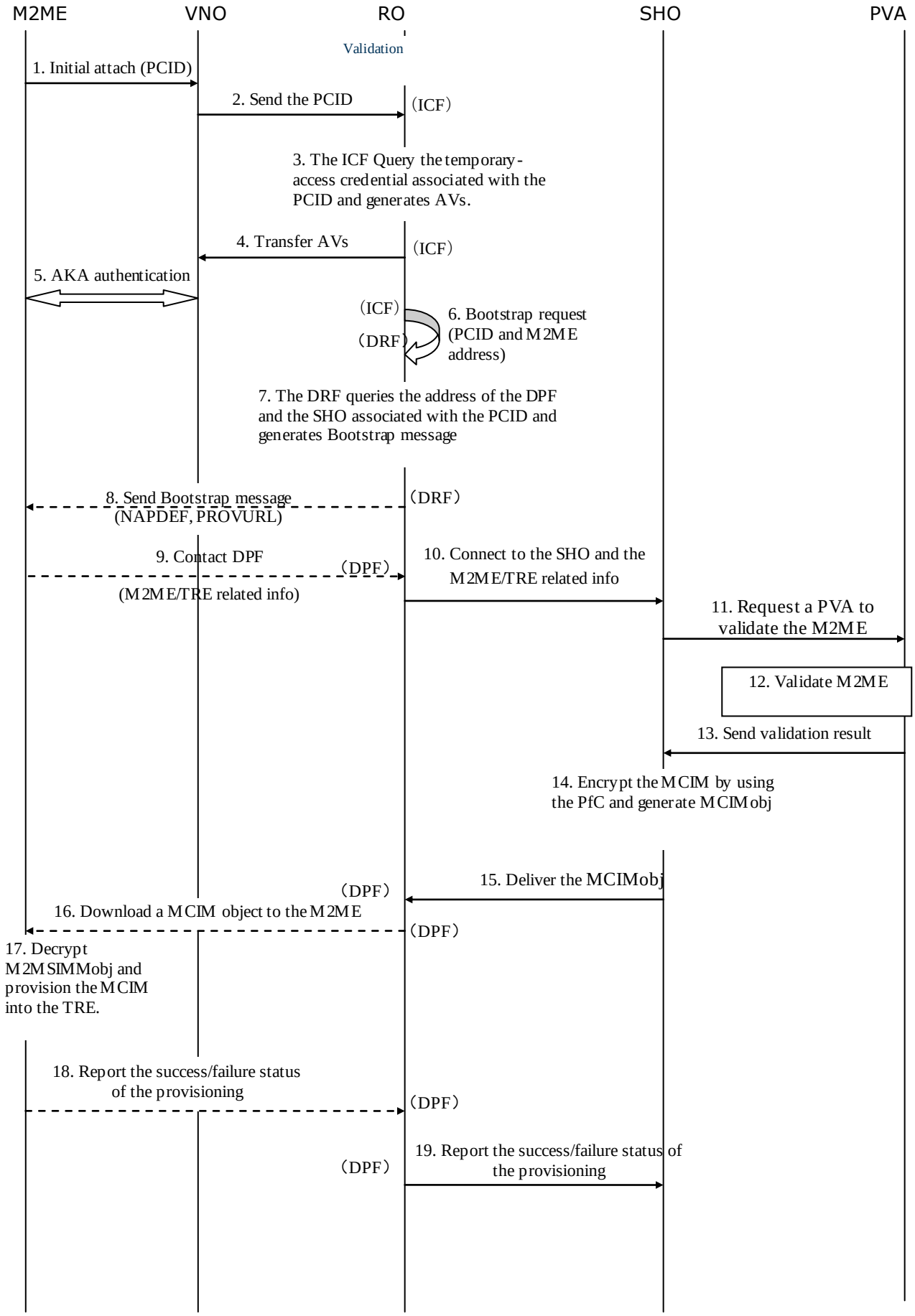
M2ME
VNO
RO
SHO
PVA
Validation
1. Initial attach (PCID)
2. Send the PCID
(ICF)
3. The ICF Query the temporary-access credential associated with the PCID and generates AVs.
4. Transfer AVs
(ICF)
5. AKA authentication
(ICF)
(DRF)
6. Bootstrap request (PCID and M2ME address)
7. The DRF queries the address of the DPF and the SHO associated with the PCID and generates Bootstrap message
8. Send Bootstrap message (NAPDEF, PROVURL)
(DRF)
9. Contact DPF
(DPF)
(M2ME/TRE related info)
10. Connect to the SHO and the M2ME/TRE related info
11. Request a PVA to validate the M2ME
12. Validate M2ME
13. Send validation result
14. Encrypt the MCIM by using the PfC and generate MCIMobj
15. Deliver the MCIMobj
(DPF)
16. Download a MCIM object to the M2ME
(DPF)
17. Decrypt M2MSIMMobj and provision the MCIM into the TRE.
18. Report the success/failure status of the provisioning
(DPF)
19. Report the success/failure status of the provisioning
(DPF)

**Figure 5.1.3.6.3-1: Procedure to initially provision the MCIM**

Note that the above steps must be further assured of appropriate types and levels of security. For example, steps 8 to 12 may be secured by use of the OMA DM protocol as is described in annex B. In another example, the steps involving the validation of the M2ME (and/or the TRE) may be done using the Online Certificate Status Protocol (OCSP) with the PVA acting as a server.

#### 5.1.3.6.4 Network Interactions for MCIM Provisioning in case of Non-3GPP Access

In this scenario, the M2ME communicates with a non-3GPP access network, which may be WLAN or DSL access (among others). The procedure is largely the same as above, with the following differences:

- The M2ME accesses a non-3GPP network provided by a non-3GPP ICSP. The M2ME is either authenticated using a non-3G mechanism (which is out of scope of this document), or given unauthenticated access for registration purposes.
- If unauthenticated access is provided, the RO's ICF is not needed, as the non-3GPP ICSP provides a direct IP connection to an RO (DRF).

After this stage, and until the M2ME connects to the network using MCIM credentials downloaded and provisioned from the SHO, all communication between the M2ME and the various network entities is done via the IP connectivity provided by the non-3GPP ICSP.

### 5.1.3.7 How to change to a new operator

#### 5.1.3.7.1 General

In this section we describe the process used to change from one SHO to another. It is worthwhile to discuss this situation in a little more depth, since the architecture used in this process may be to some degree orthogonal to the architecture presented in the previous section. This section first describes the design principles used for the architecture governing operator change. After this an extended role model is described, followed by a set of architecture proposals.

#### 5.1.3.7.2 Design principles

The following design principles were used to develop the architecture for operator change:

- Reuse as much as possible of initial provisioning architecture
- The new operator should be able to individually verify the integrity of the device just as in the case of initial provisioning
- The architecture should allow the option to have more than one MCIM stored in the device at a single moment. At most one MCIM can be active at any time.
- The owner of the device should control which MCIM in the device is used to provide connectivity.
- Selection of a new SHO should be possible at any time under control of the M2ME subscriber.

#### 5.1.3.7.4 Network architecture support for operator change

##### 5.1.3.7.4.1 General

In this section we illustrate how the architecture described in section 5.1.3 can facilitate a secure re-provisioning of MCIM due to a change of SHO.

##### 5.1.3.7.4.2 Re-provisioning using connectivity provided by old SHO

Re-provisioning may be performed using connectivity provided by the old SHO. The following is an example sequence of steps to achieve this goal:

1. The M2ME subscriber contacts the new SHO and transfers the M2ME's parameters. These parameter includes the data needed to re-provision the subscription, i.e. identity of the M2ME/TRE and authorization token by old SHO to avoid malicious overwriting of MCIM. This authorization token might be a token signed with a private key of the M2ME/TRE.

2. Transfer the M2ME's parameters from the new SHO to RO.
3. DRF sends the Bootstrap (via the old SHO) which instructs the M2ME to contact the DPF
4. M2ME connects to the DPF for provisioning of new MCIM. M2ME/TRE includes info needed, e.g. for platform validation.
5. RO (DRF) transfers the M2ME/TRE info to the new SHO
6. The new SHO requests the PVA to validate the TRE using the received M2ME/TRE info.
7. The PVA validates the TRE.
8. The PVA reports the successful status of the validation to the new SHO.
9. The new SHO sends its MCIM and the authorization token to the RO (DPF).
10. The RO securely sends the new MCIM and the authorization token to the M2ME using the connectivity provided by the old SHO. The M2ME validates the authorization token to ensure that the MCIM provisioning is authorized. This step should be atomic in the sense that the MCIM download should be complete before any other steps are initiated.
11. The M2ME sends a message to the old SHO indicating that the M2ME will discard the old SHO's credentials. This message is authorized with the authorization token to avoid that an attacker unregisters a M2ME.
12. The old SHO sends an acknowledgment to the M2ME indicating the receipt of message.
13. Before installing the new MCIM originating from the new SHO, the M2ME discards the current AVs and other MCIM credentials corresponding to the old SHO (e.g. overwrite the old MCIM).
14. The M2ME provisions the new MCIM from the new SHO into the TRE.
15. The M2ME reports the result of MCIM provisioning to the RO (DPF). If the provisioning to the new SHO fails, the M2ME firstly reverts to the pristine state and then performs another initial provisioning phase, as defined in this section.

NOTE: When the new MCIM is taken into use, in extreme cases, the new SHO, or its roaming partners, might not be able to provide coverage in the location of the M2ME. If the device cannot attach to any network within a predetermined time period, after taking a new MCIM into use, it should revert back to the previously used MCIM/network parameters. Therefore it might be beneficial if the current (old) SHO stores the credentials related to current active MCIM, for some time to resolve error scenarios, any such agreements should be done contractually. The credentials could be deleted when the old SHO can be sure that the M2ME has successfully changed to the new SHO. If such scenarios are covered by contractual agreements between old SHO and new SHO, the M2ME can be prevented from becoming unreachable.

16. The RO (DPF) reports the success/failure status of the provisioning to the new SHO.
17. The new SHO sends a message to the RO (DRF) to register the M2ME as 'subscribing to' the new SHO, for future discovery queries.

The procedure of re-provisioning of a new MCIM due to a change of SHO is executed as depicted in figure 5.1.3.7.4.2-1.

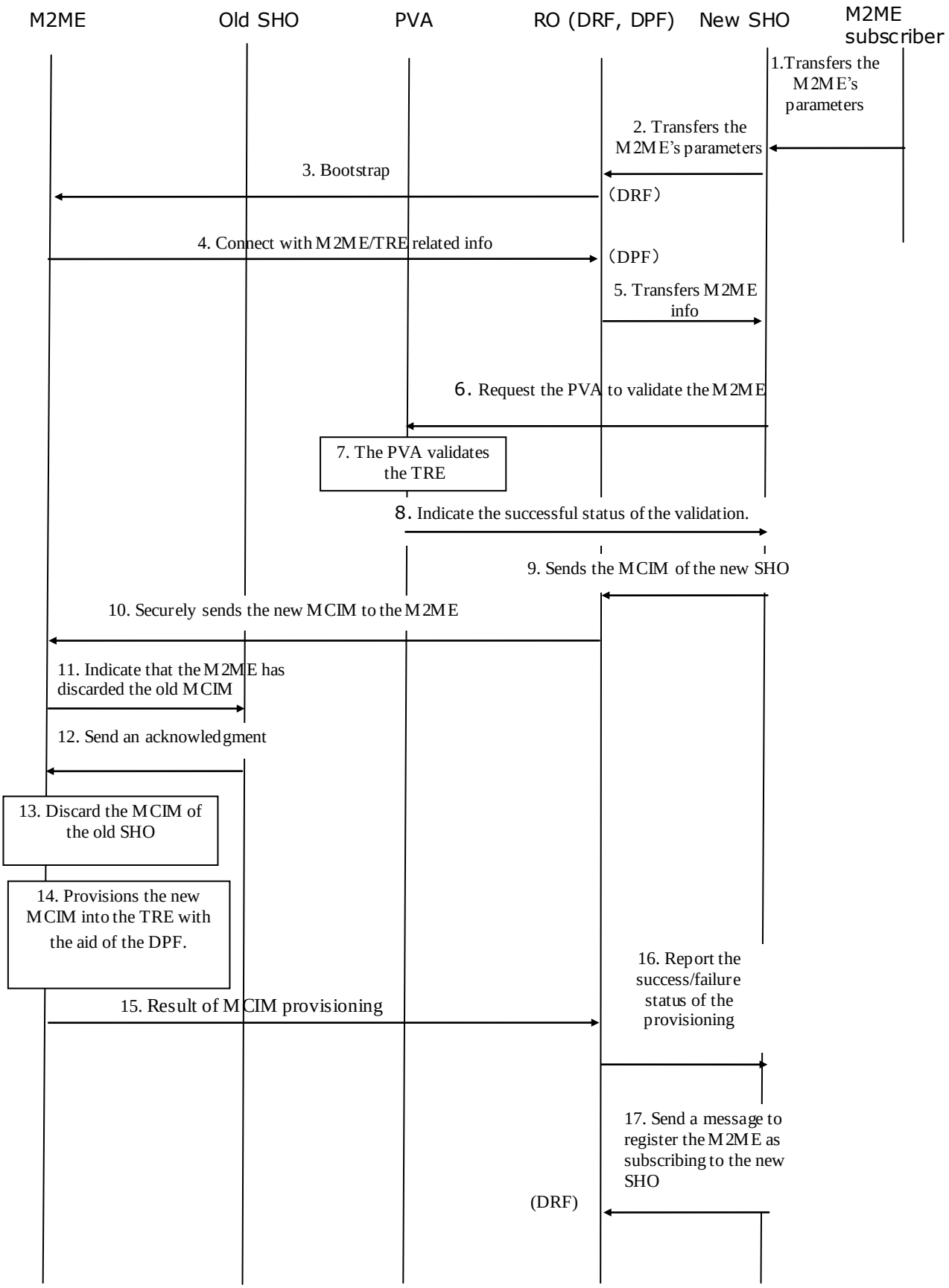
M2ME
Old SHO
PVA
RO (DRF, DPF)
New SHO
M2ME subscriber
1.Transfers the M2ME's parameters
2. Transfers the M2ME's parameters
3. Bootstrap
(DRF)
4. Connect with M2ME/TRE related info
(DPF)
5. Transfers M2ME info
6. Request the PVA to validate the M2ME
7. The PVA validates the TRE
8. Indicate the successful status of the validation.
9. Sends the MCIM of the new SHO
10. Securely sends the new MCIM to the M2ME
11. Indicate that the M2ME has discarded the old MCIM
12. Send an acknowledgment
13. Discard the MCIM of the old SHO
14. Provisions the new MCIM into the TRE with the aid of the DPF.
15. Result of MCIM provisioning
16. Report the success/failure status of the provisioning
17. Send a message to register the M2ME as subscribing to the new SHO
(DRF)

**Figure 5.1.3.7.4.2-1: Re-provisioning using connectivity provided by old SHO procedure**

In another variant of the above steps, the MCIM credentials for the old SHO and those for the new SHO may already be present in the M2ME before the subscription change takes place. In this case, these two separate sets of credentials need to be strictly separated, and neither of the two operators involved in the subscription change shall be allowed to obtain the other's MCIM credentials. Appropriate HW or SW isolation techniques must be used.

#### 5.1.3.7.4.3 Reverting to the pristine state

In this section we describe how the M2ME could change to a new operator by first reverting to the pristine state and then performing another initial provisioning phase. The basic idea here is that some entity contacts the M2ME and instructs it to perform a re-provisioning. This entity may be the owner or someone with similar management rights of the M2ME. The method could proceed as follows:

1. The M2ME subscriber contacts the new SHO and transfers the M2ME's parameters.
2. The new SHO transfers the M2ME's parameters to the RO which instructs the M2ME to perform a re-provisioning (see next step).
3. The M2ME removes the old SHO's MCIM and returns to the pristine state. Then it contacts the RO to receive the re-provisioning.
4. At this point, the M2ME can proceed according to the steps given in section 5.1.3.6.

Another possible case for going back to the pristine state could be if, e.g. during the provisioning activity, the M2ME has lost connectivity to the new SHO and is not either able to fall back to the old SHO either.

NOTE 1: The steps from 4 to 15 describe the procedure of initial provisioning the MCIM to the M2ME.

NOTE 2: As a future enhancement, the M2ME may also be able to download, install and use a new credential for the initial network access (i.e. credentials related to PCID). Once an M2ME has been provisioned, an updated initial network access credential could be delivered as a MCIM to the M2ME for future use in a SHO re-provisioning process. This way, the credential would be extracted, stored, and used exclusively in the TRE of the M2ME.
The initial network access credential could have an associated lifetime. During a MCIM re-provisioning process due to change of SHO, an M2ME may determine that its existing initial network access credential is about to expire. In this case, the M2ME may request and receive a new initial network access credential from a network entity (e.g. the DPF of the RO or the CCI function of a M2MES, etc). Alternatively, an appropriate network entity could initiate the replacement of the initial network access credential.

## 5.2 Alternative 2: UICC based solution with no remote subscription provisioning and change

### 5.2.1 General

This alternative simply consists in providing a removable-UICC to each deployed M2M equipment. In principle, it can apply without substantial differences for both the following cases:

- The UICC is a "traditional" one;
- The UICC has a new Form Factor, specifically designed to take in possible M2M peculiarity and/or requirements (e.g. high temperatures, long life duration, vibrations, etc..).

This approach rests on the following assumptions:

- a generic M2M solution studied within 3GPP should aim providing benefits for the MNOs represented in 3GPP and hence to all the parties (e.g. Vendors, smart card manufacturers) supporting the MNOs to provide services. Some possible M2M use cases were identified, but several others could certainly be added and there is not any official list of "M2M use cases" to be considered nor a list of those "to be ignored" for the purpose of this study. In this scenario, as M2M subscribers' *needs and requirements* are "use case"-specific and potentially divergent each other, whatever M2M solution fitting all possible (and potentially unknown) M2M scenarios in the same

optimal way is considered unrealistic. Moreover M2M subscribers are usually not directly represented in 3GPP. Based on this, M2M subscribers' *needs and requirements* in terms of M2M should be represented in 3GPP via MNOs (as this appears as the only practicable way forward.

- the generic M2M equipment getting access to the 3GPP Core Network falls within the category of 3GPP terminals. In other words, as in practice it is not possible to limit the application of M2M specific security requirements only to M2M equipment, the M2M security solutions shall not lower the 3GPP security when applied to 3GPP terminals, e.g. consumer mobile terminals.

The following subsections show how the Architecture under consideration fits the M2M scenario, providing benefits to the MNOs and hence to all the involved parties. In particular, it will be shown how it allows solving/counteracting the following issues:

- Initial provision of a new M2M equipment with a new USIM application from an operator of M2M subscriber's choice.
- Changing subscription to a different operator.
- Cloning prevention.
- Unauthorized removal of a UICC from the M2ME.

### 5.2.2 Initial provision of a new M2M equipment with a new USIM application from an operator of M2M subscriber's choice

From a MNO perspective this step is straightforward as it simply consists in inserting a UICC of *the operator of M2M subscriber's choice* in the M2M equipment.

This approach is also straightforward, for many use cases, from a *manufacturer of M2M equipments* point of view as the manufacture process is kept completely independent from the operator finally chosen by the M2M subscriber (exactly as is the case for 3GPP handsets). However, for some M2ME use cases, e.g. where very small devices are required, the requirement to provide a physical interface for UICC insertion may be problematic.

Possible technical and logistic issues deriving from this step do not seem to be a major issue from a MNO perspective, for many use cases: the initial insertion of the selected UICC may be carried over as part of the M2ME set-up/deployment phase, e.g. by properly trained people. However, for some use cases, the expense involved in physically provisioning large numbers of M2ME devices with respective UICCs may not be cost-effective

### 5.2.3 Changing subscription to a different operator

This potential issue arises when the M2M subscriber decides to move from a certain MNO#1 to a MNO#2.

From a MNO#1 perspective, this scenario simply means losing potential revenues and the opportunity to investigate the reasons behind the churn (or to perform appropriate "customer retention" actions to avoid it). From a MNO#2 perspective, this scenario means a new customer to serve and then new potential revenues. Under these circumstances, from a MNO perspective, the case where MNO#2 is not willing to perform the initial provision of the M2ME(s) in subject with its own UICC(s) does not seem a realistic option to be worried about. for many M2ME use cases.

The creation/management of the new subscription(s) within the MNO#2 network is welcomed by the MNO#2 as it presupposes potential new revenues; moreover it is also straightforward as the creation/management of the new subscription(s) is a widely proven process, implicit in the UICC(s) delivery and activation, for whatever 3GPP MNO.

However, for some M2ME use cases, e.g. many hundreds or even thousands of M2ME devices used for transmitting pictures of traffic from motorway bridges, the cost of physically replacing the UICCs of MNO#1 with those of MNO#2, may not be cost effective and may be an unwanted financial deterrent to change of MNO. Also, for some M2ME use cases, e.g. where very small devices are required, the requirement to provide a physical interface for UICC replacement may be problematic.

The alternative in subject allows changing the subscription of a M2ME to a different operator without impacts on the M2ME manufacturers.

## 5.2.4 Cloning prevention

In the M2M perspective, the "cloning" issue arises when a potential attacker attempts to get (directly or indirectly) the *security credentials and functions* securely stored in a genuine M2ME to reuse them in a "malicious" one or, simply, to perform other fraudulent scenarios (e.g. to get services at the M2ME subscriber's expenses).

The alternative in subject assumes the M2ME security *credentials and functions* securely stored in a UICC, i.e. in a tamper-resistant environment, that from a 3GPP MNO perspective is well proven and explicitly designed to prevent such a cloning issues, since GSM. For this reason the usage of a UICC is perceived as an adequate solution to store M2M *security credentials and functions*.

As a further measure to discourage possible cloning attempts in the M2M scenario, UICCs used within M2ME might have a specifically designed service profile in the core network, e.g. restricting their usage to the precise scope/purpose they were inserted in the genuine M2MEs (e.g. Speech Service "T11" could not be provisioned to a USIM/UICC to be used as authentication token in a vending machine).

## 5.2.5 Unauthorized removal and reuse of a UICC from the M2ME

It is envisaged that in some specific M2M use cases, there could be the interest for a potential attacker and/or for the legitimate M2ME end user to perform an unauthorized removal of the M2ME *security credentials and functions* securely stored within a certain M2ME, and then to reuse it in a different 3GPP terminal.

Another similar security threat would be the copy of security keys and authentication-related information exchanged on the interface connecting the UICC to the M2ME. The reuse of these data, without specifically involving the removal of the UICC, can also be counteracted by logical, physical means and / or in the mobile network.

Depending of the M2M use cases, and the security level that have to be achieved consequently for the M2ME, a combination of these solutions can also be used to ensure a sufficient prevention and protection against such attacks.

### 5.2.5.1 Physical protection

The alternative in subject assumes the M2ME security *credentials and functions* securely stored in a UICC. It is perceived that appropriate implementation-dependent measures can be put in place to physically prevent, in an adequate and effective way, any unauthorized removal of the UICC from the M2ME.

In many M2M use-cases, such as the use-cases described in section 4.1 (traffic cameras, metering, vending machine, asset / cargo tracking), no specific miniaturization and place constraints applies for the M2ME. Furthermore, for a large part of these equipments placed in public areas without specific supervision or in extreme environmental conditions, mechanical protection is already provided to protect the device from external unauthorized access or aggression: this is already done for many autonomous electronic devices, even if they do not have any cellular capabilities.

This physical protection can also protect the access to the UICC, and can be done in such a way to allow access for authorized personal only. The definition of the above-mentioned physical implementation-dependent measures is out of the scope of 3GPP.

### 5.2.5.2 Logical protection

In addition to physical protection mechanisms, logical protection can also be used when physical protection is not considered as sufficient. Logical protection can restrict the use of an UICC to a given M2ME: the M2ME would be authenticated by the UICC. This authentication can also be used to cryptographically protect further data exchanged on the UICC – M2ME interface, in order to provide confidentiality after the authentication step and prevent eavesdropping and copy of data on the interface.

Solutions of device pairing to securely associate the UICC and the M2ME are defined by ETSI and in certain cases extended by the 3GPP:

- The forthcoming ETSI TS 102.671, which specifies M2M UICC, list requirements for an optional feature for UICC to device pairing.
- This device pairing feature can be supported by 2 distincts technical mechanisms:
    - The CAT application pairing: similar to an IMEI-lock application.

- The Secure Channel pairing, standardized in ETSI TS 102.484: this mechanism defines how to handle a mutual authentication between the UICC and the terminal based on a shared key, and how to protect the communication channel after the authentication occurred. In order for the secure channel to be effective, the terminal should be trusted to securely store the shared key.

- Secrets loaded in UICC and M2ME before deployment, provided that they do not limit the possibility of change of subscription, can also be used to enable the Secure Channel.

- In the TS 33.110, 3GPP specifies as an extension of the Secure Channel standard, how to establishes a shared key in the UICC and the 3GPP terminal for enabling the Secure Channel, e.g. when M2ME and UICC are already deployed. This may impose to have a terminal trusted enough to store the secure channel symmetric key.

#### 5.2.5.3 Network protection

In addition to physical and logical protections, restriction measures can be configured in the mobile network to lower security threats regarding the unauthorized removal and reuse of the UICC or the copy and reuse of the security keys and authentication-related data (e.g. temporary identity).

Some examples of restriction measures:

- For specific IMSI, a systematic full authentication procedure can be enforced by the network.

- For specific IMSI, the available services can be restricted (no CS services, specific APN for PS services…).

- For specific IMSI, the location for network connection can be restricted to specific area and cells identity.

- Filtering mechanisms to allow only authorized protocol, services, and communication end-points, can be configured in the PS domain.

- Fraud detection system can also be used to monitor the behaviour of specific M2ME.

## 5.3 Alternative 3: UICC based solution with remote subscription change

### 5.3.1 Alternative 3a: IMSI change and key transfer between operators

#### 5.3.1.1 General

This clause presents a straight-forward mechanism that solves one of the most important requirements from M2M subscribers: i.e. the possibility to change MNO subscriptions in M2M equipments over air. This can be achieved without any requirements on 'virtual operators', 'temporary network connections', temporary ID:s, registration services etc.

#### 5.3.1.2 Principles

Initial provisioning of M2M Equipments is done with already existing methods or with any new method developed for M2ME manufacturers and/or M2M subscribers. The following steps describe the mechanism for change of MNO OTA. Note that the M2M subscriber in the following may in fact also be an M2ME manufacturer if it is the case that this is logistically favourable.

1) The M2M subscriber chooses an initial MNO = $MNO_A$ for his M2M operations. The subscription contract stipulates that the MNO must support a change to another MNO under certain, specified conditions upon which they have agreed. UICCs are distributed from $MNO_A$ to the M2M subscriber.

2) After initial service has started (or even before it has begun, if agreed in the contract) the M2M subscriber may decide to swap to another MNO = $MNO_B$.

3) $MNO_B$ delivers a list of IMSI to $MNO_A$, for all M2ME that shall change MNO.

4) $MNO_A$ changes IMSI in the USIM to the new IMSI obtained from $MNO_B$ for all relevant M2ME, using standardised OTA procedures. The last stage of the OTA procedure is to reset the USIM so that on next activation the new IMSI is presented to the M2M equipment

5) $MNO_A$ delivers a list to $MNO_B$ containing all M2ME with their new IMSI, subscriber key K, and the associated OTA key.

6) $MNO_B$ can now offer services to these M2ME. If it desired $MNO_B$ can as an option later also change the subscriber keys OTA.

7) If the M2M subscriber decides that a further operator change is required (e.g. to $MNO_C$) then the above procedure is repeated.

The procedure of remote subscription change in Alternative 3a is executed as depicted in figure 5.3.1.2-1.

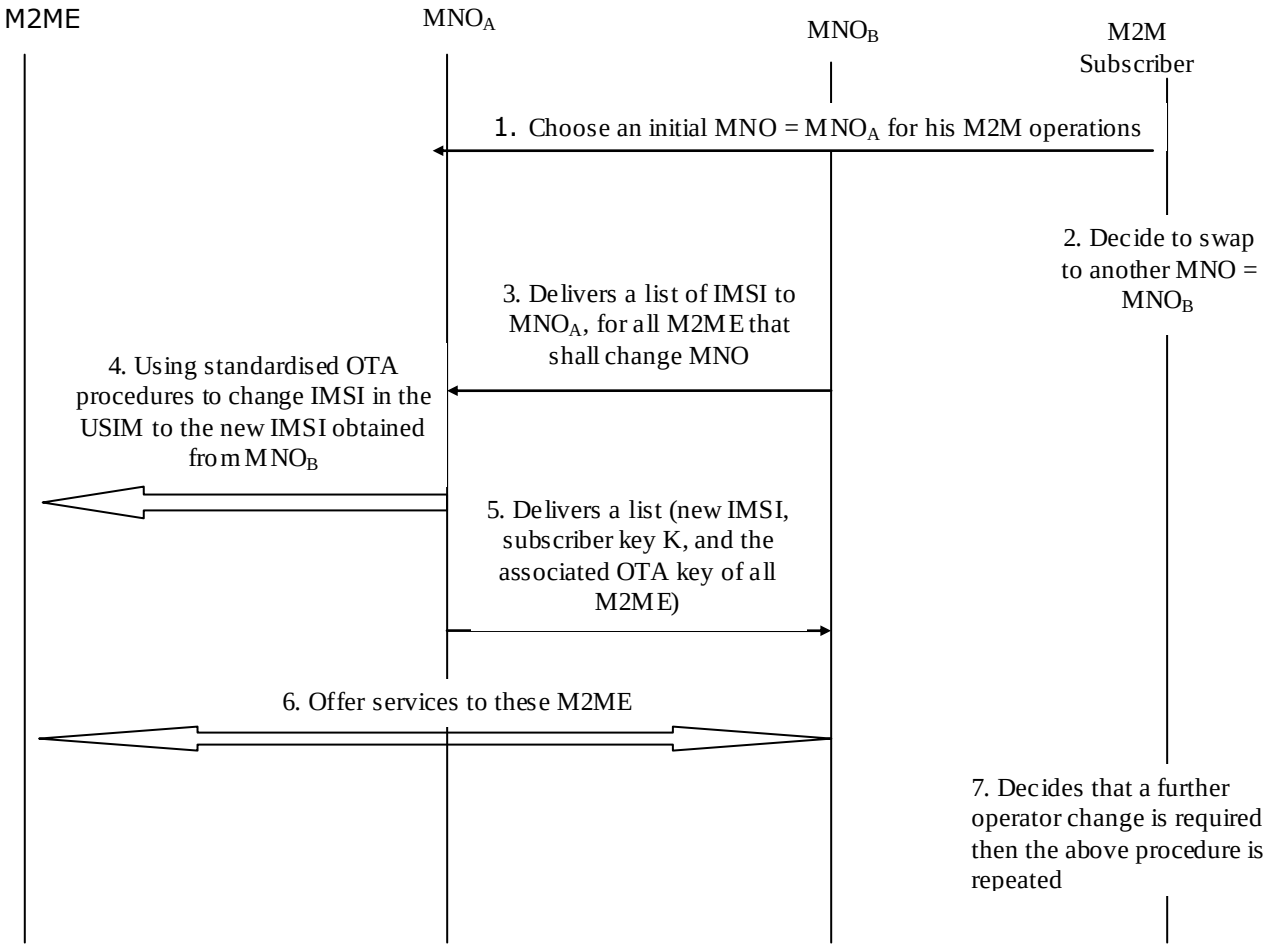


**Figure 5.3.1.2-1: K transfer between operators**

### 5.3.1.3 Requirements

This mechanism depends on the following requirements:

- The mechanism has to be supported by contractual agreements

- Involved operators must trust the entity that provisioned the initial subscriber key and OTA key on the UICC to ensure that the subscriber key and OTA key pair are not revealed to a third party. In addition, a particular operator in the chain of operators associated with an M2M USIM must trust all old operators and all new

operators associated with that USIM not to use the subscriber key value to compromise M2M communications associated with that particular operator.

- All involved operators must support a common AKA algorithm and sequence number management scheme. It is proposed that a Milenage profile (e.g. Milenage with OP set to 128 zeroes etc.) is prescribed for this. The scheme may be extended to allow the old operator to reconfigure OP parameters using OTA procedures based on requirements received from the new operator.
- All involved operators must use 3GPP (now partly ETSI SCP) specified OTA procedures (an M2M profile of OTA may be needed)
- A high degree of trust between operators is required.
- Transfer of control of the subscriber from one operator to another must be synchronised so that the subscriber is never without a valid subscription.
- It is required that operators who are part of the solution agree a base level of UICC security that all UICCs used by the operators achieve.
- It is required that inter-operator communications are protected to a high degree.

## 5.3.2 Alternative 3b: IMSI change and pre-configured key list on UICC

Editor's note: The description section should address the questions raised in TDoc S3-090233:

1. It is not clear who issues the UICC in this scenario. It may or may not be the M2M operator.

### 5.3.2.1 General

This clause presents a solution which can be seen as an extension of the mechanism in clause 5.3.1.

Like the mechanism in clause 5.3.1, the mechanism in this clause can be achieved without any requirements on 'virtual operators', 'temporary network connections', temporary IDs, registration services etc. However, the solution in this clause offers potential security advantages compared with the solution in clause 5.3.1.

### 5.3.2.2 Principles

Initial provisioning of M2M Equipment is done with already existing methods or with any new method developed for M2ME manufacturers and/or M2M subscribers. The following steps describe the mechanism for change of MNO OTA. Note that the M2M subscriber in the following may in fact be an M2ME manufacturer if it is the case that this is logistically favourable.

1. The M2M subscriber chooses an initial MNO = $MNO_A$ for his M2M operations. The subscription contract stipulates that the MNO must support a change to another MNO under certain, specified conditions upon which they have agreed.
2. $MNO_A$ acquires UICCs for the M2M devices which are preconfigured by the UICC manufacturer with an initial IMSI and an indexed list of subscriber key Key (K)/OTA key pairs. The first K/OTA key pair in the list is associated with the initial IMSI. The UICC manufacturer reveals the first K/OTA key pair to $MNO_A$ but keeps the remaining K/OTA key pairs secret.
3. After initial service has started (or even before it has begun, if agreed in the contract) the M2M subscriber may decide to swap to another MNO = $MNO_B$.
4. $MNO_B$ delivers a list of IMSIs to $MNO_A$, for all M2ME that shall change MNO.
5. $MNO_A$ changes IMSI in the USIM to the new IMSI obtained from $MNO_B$ for all relevant M2ME, using standardised OTA procedures. The OTA procedure associates the IMSI with the next K/OTA key pair in the list stored securely in the UICC. The last stage of the OTA procedure is to reset the UICC so that on next activation the new IMSI is presented to the M2M device.
6. $MNO_A$ delivers a list of new IMSIs to $MNO_B$ with the corresponding UICC IDs and the index values representing the K/OTA key pairs the IMSIs are associated with.

7. $MNO_B$ uses UICC ID and the index value to securely obtain the K/OTA key pair from the UICC manufacturer.
8. $MNO_B$ can now offer services to these M2ME.
9. If the M2M subscriber decides that a further operator change is required (e.g. to $MNO_C$) then the above procedure is repeated. Further operator changes are possible until the list of unused K/OTA key pairs is exhausted.

The procedure of remote subscription change in Alternative 3b is executed as depicted in figure 5.3.2.2-1.

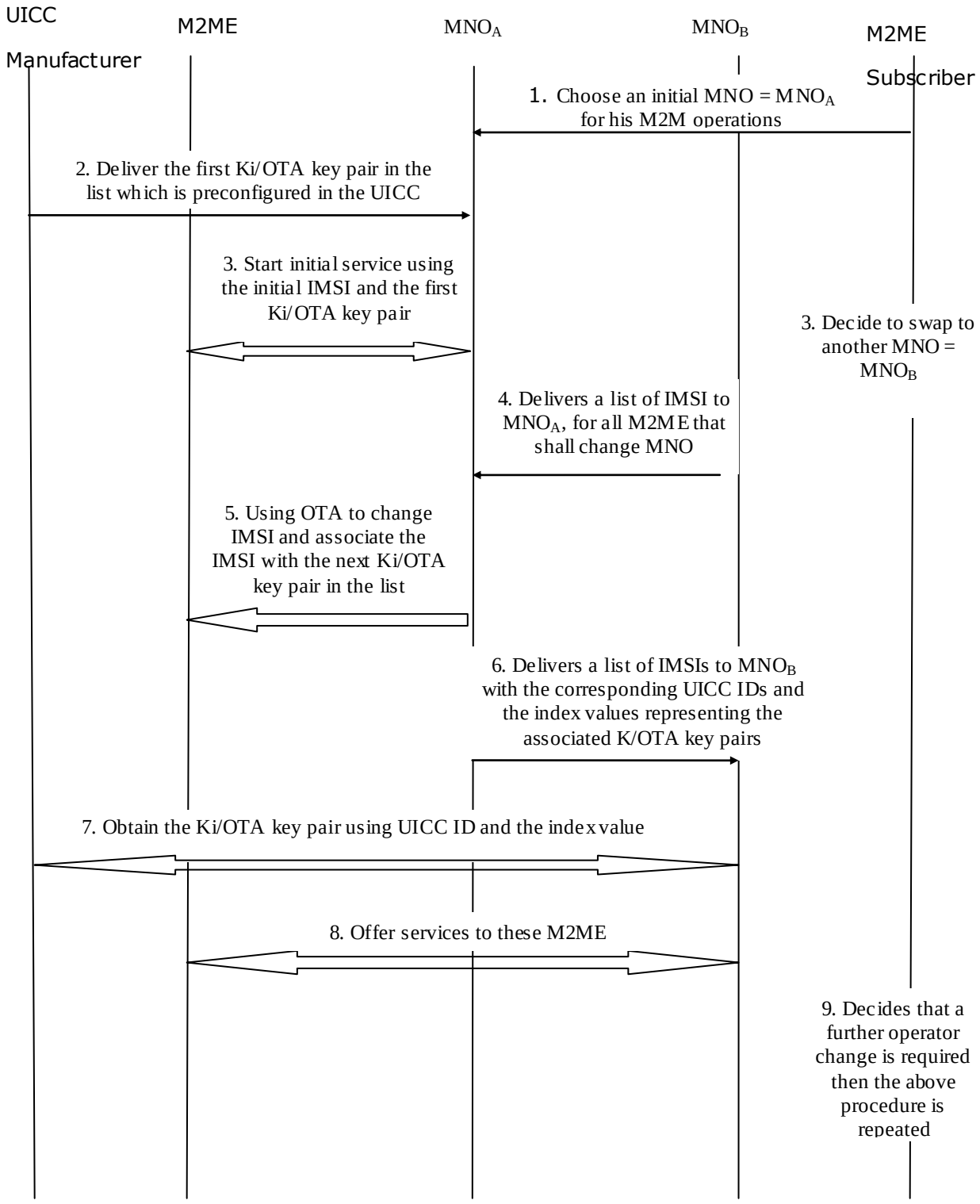

**Figure 5.3.2.2-1: Pre-configured Ki list on UICC**

### 5.3.2.3 Requirements and scheme variants

This mechanism depends on the following requirements:

- The mechanism has to be supported by contractual agreements.
- Involved operators must trust the UICC manufacturer to ensure that the specific K/OTA key pair associated with a specific operator is not revealed to another operator or any third party. A variant of the scheme is where the K/OTA key pairs are managed by an entity other than the UICC manufacturer. In this case the involved operators must trust this new entity and the UICC manufacturer. Another variant is where the OTA procedure for changing the subscription is carried out by the UICC manufacturer, or is delegated to a new entity which all involved operators trust. With this variant a common OTA key can be used for remote change of subscription instead of a per operator OTA key.
- It would be advantageous if all involved operators supported a common set of AKA algorithms and sequence number management schemes in their HLR/AuC. If Milenage is among the set of algorithms supported by involved operators a different set of randomly generated OP parameter values could be associated with each subscriber key/OTA key pair. The new operator would then obtain the new OP parameter values from the UICC manufacturer based on UICC ID and index value presented in step 7 above. When multiple AKA algorithms or sequence number management schemes are supported, the correct AKA algorithm and sequence number management scheme could be selected using the OTA procedures.
- It may be advantageous if all involved operators use 3GPP (now partly ETSI SCP) specified OTA procedures (an M2M profile of OTA may be needed).
- It may not just be IMSI, K and OTA keys than need to be changed when moving between operators – other UICC files and procedures may also need to be harmonised between the involved operators.
- The number of operator changes is limited by the number of pre-configured K/OTA key pairs on the UICC. If an operator tries to move a UICC to a new operator when there are no unused K/OTA key pairs, the OTA command should return a suitable error message.
- Acknowledged OTA procedures should be used to avoid that a UICC could become locked out during an operator change procedure.

NOTE: There may be several UICC manufacturers which provide UICCs. When changing operator, new MNO should identify which UICC manufacturer can supply the key pair associated with UICC. In case that UICCs are provided by several UICC manufacturers, how to identify which UICC manufacturer can provide the key pair associated with UICC is not described.

## 5.3.3 Requirements for removable UICC-based solution

If alternative 3a and alternative 3b both use removable UICC-based solutions for the initial provisioning of M2ME, some following issues should be taken into account.

- Initial provisioning of a new M2ME with a new USIM application from an operator of an M2M subscriber's choice.
- Cloning prevention.
- Unauthorized removal of a UICC from the M2ME.

### 5.3.3.1 Initial provisioning of a new M2ME with a new USIM application from an operator of the M2M subscriber's choice

From a MNO perspective this step is straightforward as it simply consists in inserting a UICC of the operator of the M2M subscriber's choice in the M2ME.

This approach is also straightforward, for many use cases, from an M2ME manufacturer's point of view, as the manufacturing process is kept completely independent from the operator finally chosen by the M2M subscriber (exactly as is the case for 3GPP handsets). However, for some M2ME use cases, e.g. where very small devices are required, the requirement to provide a physical interface for UICC insertion may be problematic.

Possible technical and logistic issues deriving from this step do not seem to be a major issue from a MNO perspective, for many use cases: the initial insertion of the selected UICC may be carried out as part of the M2ME set-up/deployment phase, e.g. by properly trained people. However, for some use cases, the expense involved in physically provisioning large numbers of M2MEs with respective UICCs may not be cost-effective

#### 5.3.3.2 Cloning prevention

In the M2M perspective, the "cloning" issue arises when a potential attacker attempts to get (directly or indirectly) the security credentials and functions securely stored in a genuine M2ME to reuse them in a "malicious" one or, simply, to perform other fraudulent scenarios (e.g. to get services at the M2ME subscriber's expenses).

The alternative in question assumes that the M2ME security credentials and functions are securely stored in a UICC, i.e. in a tamper-resistant environment, that from a 3GPP MNO perspective is well proven and explicitly designed to prevent such a cloning issues, since GSM times. For this reason, the usage of a UICC is perceived as an adequate solution to store M2M security credentials and functions.

As a further measure to discourage possible cloning attempts in the M2M scenario, UICCs used within an M2ME might have a specifically designed service profile in the core network, e.g. restricting their usage to the precise scope/purpose for which they were inserted in the genuine M2MEs (e.g. Speech Service "T11" could not be provisioned to a USIM/UICC to be used as authentication token in a vending machine).

#### 5.3.3.3 Prevention from unauthorized removal of a UICC from the M2ME

It is envisaged that in some specific M2M use cases, there could be the motivation for a potential attacker and/or for the legitimate M2ME end user to perform an unauthorized removal of the M2ME's security credentials and functions securely stored within a certain M2ME.

If those credentials and functions are securely stored in a UICC, it is perceived that appropriate implementation-dependent measures can be put in place to physically prevent, in an adequate and effective way, any unauthorized removal of the UICC from the M2ME. The counter-measures should not adversely affect the authorized removal of UICC.

The implementation details of the above-mentioned implementation-dependent measures is out of the scope of 3GPP.

# 6 Analysis

## 6.1 Threat Analysis

### 6.1.1 Methodology

#### 6.1.1.1 Risk-Level Matrix

The impacts of successful attacks are assessed here, based on NISCC criteria [NISCC] that are used widely in the UK.

NOTE: The same threat lists was used for all scenarios, but not all scenarios were fully analysed.

##### 6.1.1.1.1 Impact

The table below shows how values are assigned to the possible impacts of successful attacks on an unprotected system.

**Table 6.1.1.1.1-1 Impacts of successful attacks**

| | | |
|---|---|---|
| 1 | "minor impact" | Minor or no effect on the stakeholder, with resulting inconvenience very localised<br>No external impact or visibility of problems |
| 2 | "serious impact" | Failure of important revenue generating systems/processes and/or support systems/ processes.<br>impact would be noticeable to parties other than the stakeholder.<br>possible repercussions for revenue, penalty payments, market share and customer confidence |
| 3 | "Enterprise" | Irreparable damage to key systems/processes with probable widespread impact.<br>Ability of the enterprise to continue operations would be in jeopardy; major regulatory, licensing and legal implications<br>Impact would be very visible and would cause very severe cash flow problems and large-scale defection of major customers of the stakeholder |
| 4 | “National”<br>Note: this category is not used in the present document but is presented here for completeness | National Infrastructure - Severe damage to systems/processes that support important infrastructure requirements<br>National Security - Severe damage to systems/processes that support important national security/defence requirements |

### 6.1.1.1.2 Likelihood of Threat Occurring

Measures used to express the likelihood of a threat occurring are:

- Attackers’ skills and resources and minimum effort of carrying out an attack on an unprotected system
- Reasons and motivation of attacking, and the gained benefit as perceived by an attacker:

For the risk assessment, the likelihood of threats is estimated with values from "1" to "4", according to the level of threat to the stakeholders. The meaning of each assigned value is as follows:

**Table 6.1.1.1.2-1 Likelihood of Threat**

| | | |
|---|---|---|
| 1 | "low likelihood" | Attackers have low motivation and little opportunity and capability for launching and sustaining an effective attack |
| 2 | "moderate likelihood" | medium motivation, limited opportunity and capability |
| 3 | "substantial likelihood " | high motivation, limited opportunity and capability<br>or<br>medium motivation, significant opportunity and capability |
| 4 | “severe likelihood” | high motivation, high opportunity and capability |

#### 6.1.1.1.3 The Risk Matrix

This threat analysis uses a risk-level matrix to prioritize the various threats identified and their associated security requirements.

A risk-level matrix helps categorize the relatively priority of threats and associated security requirements. In the table above, four levels of threat likelihood (Probability) and three levels of impact are identified. Each level is associated with a number indicating the relative importance between the various levels. Impact level 4 ("National") is not used, as the application of this M2M technology does not give rise to impacts of such severity

Risk is calculated as Impact multiplied by Likelihood.

**Table 6.1.1.1.3-1 Risk Matrix**

| Threat Likelihood (Probability) | Impact | | |
|---|---|---|---|
| | **Minor (1)** | **Serious (2)** | **Enterprise (3)** |
| **Low (1)** | Risk = 1 (minor) | Risk = 2 (minor) | Risk = 3 (minor) |
| **Moderate (2)** | Risk = 2 (minor) | Risk = 4 (major) | Risk = 6 (major) |
| **Substantial (3)** | Risk = 3 (Minor) | Risk = 6 (major) | **Risk = 9 (critical)** |
| **Severe (4)** | Risk = 4 (major) | Risk = 8 (major) | **Risk = 12 (critical)** |

NOTE: in the above table, multiples 5, 7, 10, 11 cannot occur. 12 is the maximum risk level that can occur.

### 6.1.1.2 Definitions of Risk Level

The risk category for an unprotected system provides an indication of what security counter-measures are required. The result is classified into the following three categories:

| | | |
|---|---|---|
| Risk 1, 2, 3 | "minor risk" | No primary need for counter measures. |
| Risk 4, 6, 8 | "major risk" | Counter measures are required to minimize this risk as soon as possible. |
| Risk 9, 12 | "critical risk" | Counter measures are required to minimize this risk, with a high priority. |

Note that in this analysis there is no "moderate" or "medium" category for risk. This is because the process of choosing counter-measures to mitigate a "moderate" risk is too subjective. In this analysis there is no middle ground, i.e. counter-measures are either necessary or they are not.

## 6.1.2 Threats and Suggested Counter-Measures

### 6.1.2.1 Introduction

The descriptions of the attacks and the assessment of their likelihood and impact assume the lack of any security counter-measures. The risk analysis is therefore for a theoretical unprotected system and this allows the required counter-measures to be identified.

### 6.1.2.2 Generic threats

The threats described in this section apply to any potential solution to the remote management of a MCIM application on M2M equipment. The counter-measures used to address these threats may vary among the proposed solutions. Therefore this section describes only the threats themselves and leaves the description of the counter-measures and the resulting residual risk level to the analyses of the individual solutions.

**Table 6.1.2.2-1 Generic threats**

| THREAT # | BRIEF DESCRIPTION | RISK LEVEL |
|---|---|---|
| G1 | Copying the M2M subscriber's credentials to a different piece of M2M equipment with the intent of using it to make calls at the M2M subscriber's expense | critical |
| G2 | Copying the M2M subscriber's credentials to a different piece of M2M equipment with the intent of masquerading as the customer when enacting transactions, e.g. electronic payment, access to IT systems, etc | critical |
| G3 | Modifying the credentials to those of another M2M subscriber. This would typically be performed on a piece of stolen M2M equipment | critical |
| G4 | Performing an unauthorised migration of the M2M subscriber to another operator's network by modifying the credentials to a set that would apply to that M2M subscriber on the other operator's network | major |
| G5 | Adding a set of credentials that are not authorised by the M2M subscriber or the home operator | major |
| G6 | Rendering the M2M subscriber's credentials unusable, e.g. in an attack over an IP channel to the equipment | major |
| G7 | Rendering the credentials unusable due to exposure to environments that might normally be encountered by the M2M equipment, for example a magnetic or electrostatic field | major |
| G8 | Copying the credentials so as to be able to determine the derived ciphering and integrity keys used for traffic protection so as to be able to eavesdrop upon and/or tamper with communications between the M2M terminal and the network | major |

### 6.1.2.3 Threat analysis of Alternative 1: Non UICC based solution with remote subscription provisioning and change

The description of Alternative 1 assumes an implementation of the counter measures described in this section.

Some of the proposed counter-measures define the enforcement of security controls or metadata defining them. Security controls are security policies, or the embodiment thereof, that are small in terms of complexity and memory requirements. Specifically they are atomic in the sense that they do not depend on other policies (and thus do not require advanced policy evaluation). Furthermore, they are local in the sense that they can be enforced by information and means that are locally available in the M2ME.

NOTE 1: An example, of a Security Control could be a set of mechanisms and/or (meta)data to ensure the enforcement of a standardised policy concerning controlled access (in-band and out-of-band) to files protected by the TRE. The Security Control could embody the implementation of cryptographic methods for such protection and it could also include data/metadata objects such as PINs, ACLs and key identifiers. Such a Security Control could also control access to assets depending on the state of the M2ME.

The table below presents a convenient summary of the identified threats and the risk levels that have been assigned to them. The analysis of how these risk levels were calculated is provided after the summary.

**Table 6.1.2.3-1 Threats**

| THREAT # | BRIEF DESCRIPTION | RISK LEVEL |
|---|---|---|
| 1 | emulating the functions of a legitimate M2ME to obtain the illicit download of MCIMs | critical |
| 2 | attacking the MCIM provisioning process to obtain MCIMs | critical |
| 3 | Use of malicious software in the M2ME or host terminal to obtains MCIMs | critical |
| 4 | Use of logical or physical attacks against a TRE, to obtains and use a MCIM or secret keys that enable him to clone a TRE or MCIMs. | major |
| 5 | Replacing a TRE in a M2ME by another TRE or an emulation | major |
| 6 | modifying the functions of a TRE | major |
| 7 | attacking the permissions of an installed MCIM (to get unauthorised service or to steal data or for DoS) | major |
| 8 | another MCIM or malicious software extracts sensitive information from a MCIM | critical |
| 9 | obtaining sensitive information by monitoring interactions between a TRE and the M2ME | major |
| 10 | access to TRE or MCIM functions by masquerading as the legitimate user | critical |
| 11 | users lose access to networks, services or personalised data, due to malfunctions of MCIMs or of a TRE. | critical |
| 12 | Attackers find they can register falsely in order to obtain MCIMs | critical |

NOTE 2: In the following analysis, some counter-measures are not unique, i.e. they appear under more than one threat. This is intentional and although it causes some duplication, it is easier to present than, e.g,. a large table of threats and counter-measures.

**Threat #1**

Description of attack: An attacker emulates the functions of a legitimate M2ME, e.g., by extracting credentials and MCIMs from it, replicates them on another item of equipment and in subsequently uses those MCIMs to obtain service and uses the replicated credentials to obtain illicit downloads of MCIMs.

The effect on the M2ME subscriber is that the attacker can obtain service which is billed to the legitimate M2ME subscriber and can perform actions which are attributed to the legitimate M2ME subscriber. In the use cases (a), (b) and (c) in the present document, which involve M2ME functions in UEs, the attack could amount to identity theft.

Likelihood: 3

Impact: 3

Risk Level: 9 (critical)

Counter-Measures:

1. The M2ME should support at least one TRE. A TRE should be a root of trust for the secure storage and secure execution environment for multiple MCIMs and for security-related functions concerned with the provisioning and management of MCIMs.

2. A TRE should be a logically separate area in the M2M equipment with hardware support for this separation.

3. Each TRE should have a unique, authenticable and revocable identity, e.g. as provided by a valid X.509 certificate and associated private key, for proving its authenticity as a true TRE.

NOTE 3: This function is intended for use in bootstrapping the secure provisioning process

4. The DPF can remotely query the system state of the M2ME, either directly or via the PVA, to ensure that MCIMs will be provisioned only in a valid M2ME. This process may also require remote validation of a TRE and also possibly the M2ME platform, before the provisioning of MCIMs can proceed.

NOTE 4: Full details and definitions of remote validation are not part of the present document.

5. If the services accessible by using the MCIM are filtered in the network (e.g. only one APN with restricted IP connectivity allowed), then the incentive to obtain and use such MCIM and the possible impact are reduced.

**Threat #2**

Description: an attacker attacks the MCIM provisioning process to obtain and use MCIMs that are not intended for use by the attacker. This includes:

- corrupting or eavesdropping on the on-line provisioning process externally to the M2ME or internally to the M2ME;
- MITM attacks;
- Spoofing one or more of the entities involved in the provisioning process

Likelihood: 4

Impact: 3

Risk Level: 12 (critical)

Counter-Measures:

1. The M2ME should support a secure provisioning process and protocol for authorised service providers to register users for a MCIM-enabled service and to provision MCIMs remotely, in-band.
2. A secure provisioning protocol is required to transport all components of MCIMs, including network-access credentials, from a DPF in the network to the M2ME.
3. In the M2ME, only a TRE should be responsible for assuring the security aspects of the provisioning process, and of the subsequent storage and usage of MCIMs, such that sensitive data cannot leak from the provisioning channel to an insecure or unauthorised function within the M2ME.
4. The provisioning protocol should:
   - allow mutual authentication of M2ME (TRE and possibly M2ME platform) and DPF
   - provide for authenticity of origin, data integrity, confidentiality, uniqueness and assurance of freshness.
   - be adequately and demonstrably resistant to known attacks including eavesdropping, replay, DDoS, data corruption, masquerading (as a TRE or as a DPF), MITM;
   - have the capability to securely register a user for the service online;
   - support a way for the service provider to provision discrete security control objects (e.g. an ACL) related to the use and management of an installed MCIM
5. an attacker should be prevented by cryptographic means from interrupting or hijacking a provisioning session
6. A M2ME subscriber must go through the registration phase of provisioning in order to obtain a download of MCIMs.
7. If the services accessible by using the MCIM are filtered in the network (e.g. only authorised services of the legitimate M2ME subscriber allowed), then the incentive to obtain and use such MCIM and the possible impact are reduced.

**Threat #3**

Description: By use of malicious software in the M2ME or host terminal, an attacker obtains and uses a MCIM that is not intended for him, either on the same terminal or on a different one.

Likelihood: 3

Impact: 3

Risk Level: 9 (critical)

Counter-Measures:

1. A TRE should be sufficiently secure as to be suitable for the storage and execution of AKA functions which are currently implemented in UICCs.

2. A TRE should support features that are similar to some aspects of 3GPP ME personalisation, e.g. a MCIM could be locked to a M2ME (and possibly to a TRE) and unable to be replaced by an unauthorised MCIM. It should not be possible for this feature to be nullified by an unauthorised entity.

NOTE 5: The above function is analogous to, but not identical to, SIM-lock. Applicability of 3GPP ME personalisation specifications is FFS

3. A TRE should assure the security of the lifecycle stages of multiple MCIMs whether owned by the same or multiple stakeholders. Such MCIMs may be in different lifecycle stages.

4. In the M2ME, only a TRE should be responsible for assuring the security aspects of the provisioning process, and of the subsequent storage and usage of MCIMs, such that sensitive data cannot leak from the provisioning channel to an insecure or unauthorised function within the M2ME.

5. The provisioning protocol should:

   - allow mutual authentication of M2ME (TRE and possibly M2ME platform) and DPF

   - provide for authenticity of origin, data integrity, confidentiality, uniqueness and time-stamping of messages.

   - be adequately and demonstrably resistant to known attacks including eavesdropping, replay, DDoS, data corruption, masquerading (as a TRE or as a DPF), MITM;

   - have the capability to securely register a user for the service online;

   - support a way for the service provider to provision security controls related to the use and management of an installed MCIM

6. If the services accessible by using the MCIM are filtered in the network (e.g. only authorised services of the legitimate M2ME subscriber allowed), then the incentive to obtain and use such MCIM and the possible impact are reduced.

7. The PVA should be able to validate the authenticity and integrity of the M2ME (and the TRE) on behalf of a requesting entity such as a SHO or a DPF. The security properties of this validation of the M2ME shall be guaranteed by the TRE

**Threat #4**

Description: By use of logical or physical attacks against an instance of a TRE, an attacker obtains and uses a MCIM that is not intended for him or obtains secret keys that enable him to clone a TRE or MCIMs.

Likelihood: 3

Impact: 3

Risk Level: 9 (critical)

Counter-Measures:

1. The design and implementation of a TRE should provide a proven degree of protection against physical and logical attacks against objects including cryptographic keys, datafiles and security-related executable code. This includes direct monitoring of components and their interfaces and side-channel attacks. SA3 discussed and investigated potential protection and evaluation approaches in section 6.2.

NOTE 6: The precise method of specifying and assuring the “proven degree of protection” offered by a TRE is not part of the present document.

2. Logical interfaces to a TRE should be usable only under the control of an entity which is authorised to communicate directly with a TRE.

3. Use of logical interfaces to a TRE should not compromise the confidentiality, integrity or availability of the MCIMs or of a TRE.

4. A TRE should support and enforce its own security policy

5. If the services accessible by using the MCIM are filtered in the network (e.g. only authorised services of the legitimate M2ME subscriber allowed), then the incentive to obtain and use such MCIM or secret and the possible impact are reduced.

**Threat #5**

Description: an attacker replaces a TRE in a M2ME in order to commandeer use of that M2ME and/or its host terminal. The replacement TRE may be a real TRE or an emulation

Likelihood: 2

Impact: 2 (or possibly 3, if the detailed method of attack is widely publicised)

Risk Level: 4 or 6 (major)

Counter-Measures:

1. Security-critical elements of all TREs should be pre-provisioned in a secure, out-of-band facility.

2. A TRE should have its own embedded, unique identity that is typically associated with the identity of the M2ME platform that, where used, is also embedded in a TRE. A TRE should be capable of securely authenticating those identities to the issuing authorities using standardised protocols. The issuing authorities can validate a TRE's identity as being that of a valid, issued, TRE and M2ME. Those identities are embedded as part of a physically secure, out-of-band process that takes place before the M2ME is issued.

3. Provisioned MCIMs and the messages used to provision the MCIMs should be securely bound and mapped to the identity of the TRE for which they have been issued.

NOTE 7: This may be achieved by ensuring that cryptographic tokens used to remotely provision or manage MCIMs are cryptographically bound to that TRE's identity

4. The provisioning function should ensure that MCIMs are delivered only to the correct, valid and authentic TRE/M2ME. This implies that the DPF can authenticate a TRE and that the phases of the registration and provisioning sessions are bound together and to a TRE by cryptographic means.

5. The DPF can remotely query the system state of the M2ME, either directly or via the PVA, to ensure that MCIMs will be stored only in a valid M2ME. This process may require handling platform validation information, before the provisioning of MCIMs can proceed.

6. The PVA can validate the authenticity and the integrity of the M2ME and the TRE. The security properties of this validation of the M2ME shall be guaranteed by the TRE.

NOTE 8: All M2ME-internal functions required to support the PVA to perform this task should be performed within the M2ME's TRE.

NOTE 9: Full details and definitions of remote validation are not part of the present document.

**Threat #6**

Description: an attacker modifies the functions of a TRE in order to perpetrate a DoS attack or to control the functions or behaviour of a TRE to his advantage.

Likelihood: 2

Impact: 2 (or possibly 3, if the detailed method of attack is widely publicised)

Risk Level: 4 or 6 (major)

Counter-Measures:

1. Logical interfaces to a TRE should be usable only under the control of an entity which is authorised to communicate directly with that TRE.

2. Use of logical interfaces to a TRE should not compromise the confidentiality, integrity and availability of the MCIMs or of a TRE.

3. a TRE should support and enforce its own security controls

4. Changing or upgrading of the access control-related firmware of a TRE should be possible, using a secure channel and only by an authorized remote management system, which may be under the control of the entity that is responsible for ownership of that TRE. The identity of controlling entities for each of a TREs in a M2ME should be specified in a global security controls that are embedded in the M2ME and in protected storage in the M2ME E/S's TRE (or if stored external to a TRE, then by cryptographically secured storage),. In order to remotely modify an identity, authorisation by appropriate entities, including the stakeholder owner of a TRE whose identity is to be modified, as well as appropriate M2ME subscriber, may be required.

4. Any tampering with a TRE or its functions of the M2ME protected by a TRE should be detected by that TRE itself. Detection of anomalies should result in that TRE entering an un-trusted state and should result in shutdown of that TRE.

**Threat #7**

Description: an attacker modifies or defeats the permissions to access an installed MCIM e.g. in order to obtain unauthorised service or to gain access to private data stored with or in a MCIM or as a DoS attack (i.e. disabling it or de-selecting it)

Likelihood: 2

Impact: 3 if the attack becomes distributed and/or or publicised and/or if the private data gained is sensitive or of monetary value.

Risk Level: 6 (major)

Counter-Measures:

1. A TRE should assure the security of the transition of a MCIM through its lifecycle stages, according to instructions from the stakeholder (typically the SHO) that authorizes such lifecycle transition, and/or according to the MCIM's and/or TRE's security controls.

2. Where the M2ME subscriber has a subscription relationship with a particular SHO, a TRE should provide certain user access control functionality for managing MCIMs belonging to that SHO. How a TRE may control access to the user-related functions of MCIMs (e.g. providing file system for user data, for example) should be defined globally in that TRE according to security controls specified by the M2ME E/S. It may also be further defined by individual security controls specifiable by the M2ME subscriber and/or the SHO.

3. On behalf of the SHO, a TRE should store, monitor and enforce MCIM-specific security controls that may be a component of a MCIM. MCIM security controls should include MCIM functions that the M2ME subscriber cannot over-ride and may also include functions which the M2ME subscriber can over-ride. Over-riding of a security control by the M2ME subscriber should be performed by the M2ME subscriber issuing an authorized command. Such authorized command may also require the M2ME subscriber to authenticate itself to a TRE.

NOTE 10: Examples of security controls which the user should not be able to over-ride are those which relate to the lifecycle management and operational use of an SHO's MCIM. An example of a user-over-ride-able security control is the phonebook, where the M2ME subscriber may wish to over-ride the security controls that were set by the M2ME supplier, so as to prevent remote access by the M2ME supplier to phonebook entries.

4. On behalf of a M2ME subscriber, a TRE should store, monitor and enforce such MCIM management security controls as may be specified by the M2ME subscriber

5. A TRE should provide suitable, secure mechanisms for the SHO to validate the integrity of MCIMs that the SHO owns.

6. Where permitted by security controls of e.g. the SHO, a TRE should support a secure discovery service by which another entity, such as a DRF, can 'discover' the identifiers and lifecycle status of MCIMs that are loaded on that TRE.

7. A TRE should support the remote upgrade/update of SHO's MCIMs, but only after authorization from the SHO and, where applicable, only if permitted by the security controls of the MCIM, and/or the M2ME E/S, and/or the M2ME subscriber.

8. In the M2ME, only a TRE should be responsible for assuring the security aspects of the provisioning process and of the subsequent storage and usage of MCIMs.

9. The same provisioning function can also be used for de-provisioning and/or updating MCIMs, to support the complete MCIM lifecycle management process.

10. The provisioning protocol should enable the M2ME to verify that management instructions come from a valid source.

11. The M2ME should support the use of standardised, trusted protocols for upgrade/update of MCIMs Examples could be OMA DM, OTA RFM and OTA RAM

**Threat #8**

Description: another MCIM or malicious software extracts sensitive information from or corrupts a MCIM either in error or in order as an attack.

Likelihood: 3

Impact: 3

Risk Level: 9 (critical)

Counter-Measures:

1. A TRE should provide logical isolation for the environments in which the MCIMs of different stakeholders are stored and executed.

2. If a TRE permits MCIMs it manages to interact or share a specified set of its functions with another MCIM managed by the same TRE, this should be allowed only where that is permitted by the security controls of the MCIM that is being requested to share its functions and only where both MCIMs are in the "activated" lifecycle state and where such MCIMs belong to the same stakeholder. That TRE should verify that commands and responses between such MCIMs are origin-authenticated.

3. A TRE should be able to support and enforce the security controls of MCIMs.

4. On behalf of a M2ME subscriber, a TRE should store, monitor and enforce such MCIM management security controls as may be specifiable by the M2ME subscriber.

5. Interfaces to a TRE should be usable without compromising the Confidentiality, Integrity and Availability of the MCIMs or of that TRE.

6. A TRE should assure the security of the transition of MCIMs through their various lifecycle stages.

7. A TRE should maintain a registry of the MCIMs that it manages, including information about their current lifecycle and security status.

8. The executable code of a MCIM should be integrity checked by a TRE at boot time and whenever a TRE is reset and optionally at the start of each session with that MCIM. The integrity of the file system may also be checked. Detection of anomalies should result in the MCIM entering an un-trusted state and the MCIM should be permanently blocked. In such situation the M2ME could go to pristine state and start re-provisioning of the MCIM.

NOTE 11: In pristine state only ICO connectivity is possible, if such coverage is available.

9. A TRE may provide a secure audit record of its transactions. Records would typically be protected against unauthorised access

**Threat #9**

Description: an attacker obtains sensitive information by monitoring interactions between a TRE and the M2ME.

Likelihood: 2

Impact: 2

Risk Level: 4 (major)

Counter-Measures:

1. A TRE should not reveal its authorisation values to any other functions on the M2ME.
2. Interactions between a TRE and any other trusted components in the M2ME should take place over secure channels.
3. Operations that require secure communications with a TRE should not take place in untrusted components of the M2ME or the host terminal.
4. If the services accessible by using the MCIM are filtered in the network (e.g. only authorised services of the legitimate M2ME subscriber allowed), then the value of the information gathered this way by the attacker may be of much lower interest to the attacker.
5. Interactions between a TRE and another component in the M2ME that is not trusted should be designed so that these interactions do not contain any sensitive information and should assume compromise of the non-trusted component.

**Threat #10**

Description: an attacker gains access to TRE or MCIM functions by masquerading as the legitimate user

Likelihood: 3

Impact: 3, if publicised

Risk Level: 9 (critical)

Counter-Measures:

1. A TRE should be able to perform user authentication and access control for single or multiple users, where relevant to the use case for that type of M2ME.or should be designed so that no user authorisation is required for correct operation.
2. A TRE should support user authentication services, where required by MCIMs and where user authentication is necessary.
3. A TRE should allow a MCIM to invoke its own M2ME subscriber authentication process, using, for instance, an application-specific credentials such as password or certificate, specified by the MCIM's security controls.
4. Monitoring of interactions between a TRE and one of its users should be prohibited unless explicitly permitted by the user. Such permission should require user authentication.
5. Transfer of credential values from e.g. credential entry devices or smart card reader to a TRE should be protected from eavesdropping, e.g. by a secure tunnel that provides at least confidentiality and anti-replay.

NOTE 12: Counter-measures 4 and 5 above might not be applicable or have usability issues in some cases, and they might be costly to implement.

6. A TRE should block itself or a MCIM after *n* consecutive incorrect entries of its own or the MCIM's credential, respectively. This should disable all trusted applications and functions for which that credential is an access condition.
7. As a default policy, a TRE should not accept authentication attempts from a remote M2ME subscriber, except where such commands are allowed under that TRE's security controls and are embedded in secure, standardised, protocols (e.g. OTA) that are compatible with the TRE, and which originate from a remote security server. This will ensure that a remote attacker is not able to lock the platform by intentionally providing invalid authentication credentials to it.
8. void.

NOTE 13: The above item is void as otherwise the numbering would be confused, since there is cross-referencing in the TRE functionality section.

9. If user authentication is supported, a TRE should be capable of supporting a monotonic timer that is protected from tampering which will set the user authentication status to non-verified after a specified period of inactivity. This may be required by security controls of specific MCIMs.

10. A TRE should be configured with M2ME subscriber authentication parameters (multi-factor preferred). On booting or rebooting the M2ME, a TRE should force authentication of the M2ME subscriber before the M2ME subscriber is allowed to use the device's functionality to whose access is controlled by that TRE. Alternatively, the authentication could be invoked only when a functional part of a TRE is invoked, in which case, the authentication status should then persist for the duration of the user-TRE session and should apply to all applications under that TRE's control.

NOTE 14: The M2ME subscriber may be a consumer or a remote administrator, depending on the nature of the use case.

11. A TRE should not allow a M2ME subscriber to reduce the user-authentication protection of that TRE below an acceptable security level specified in the global security controls of that TRE. For example, the M2ME subscriber may not disable the credential verification process if the TRE's security controls prohibit that

NOTE 15: The above counter-measure is FFS, from the viewpoint of ease-of-use vs. security, since with a hardware UICC, the user can suspend the credential verification process that applies to MCIM functions.

12. Only a TRE should be responsible for the security aspects of managing M2ME subscriber's access to MCIMs' usage and management functions.

**Threat #11**

Description: a user loses access to networks and services and/or loses personalised data, due to a malfunction or erasure of a MCIM or a malfunction of a TRE's firmware.

Likelihood: 3

Impact: 3 (the M2ME E/S's business would suffer if prominent people lose their service access or data)

Risk Level: 9 (critical)

Counter-Measures:

1. It should be possible for an authorised entity to reset a TRE's MCIM management functions to factory settings and for users to re-establish their access to that TRE and to MCIMs

NOTE 16: A secure backup service for sensitive credentials, e.g. Ki, is regarded as impractical to implement.

**Threat #12**

Description: attackers find that they can register using a stolen or as yet un-registered identity in order to obtain MCIMs.

Likelihood: 3

Impact: 3

Risk Level: 9 (critical)

Counter-Measures:

1. The registration procedure must be trust-worthy. How this is achieved is out of scope.

2. The provisioning process should be securely bound to the registration.

### 6.1.2.4 Threat analysis of Alternative 2: UICC based solution without remote subscription provisioning and change

Editor's Note: To be completed.

#### 6.1.2.4.1 Introduction

The descriptions of the attacks and the assessment of their likelihood and impact assume the lack of security counter-measures not introduced earlier. The risk analysis will therefore allow suitable counter-measures to be identified.

The alternative analysed here assumes that a UICC and application eg USIM is used. The UICC is intended to be standard or, potentially, with a new Form Factor, specifically designed for M2M purposes.

#### 6.1.2.4.2 Summary of Threats and Assigned Risk Levels

The table below presents a convenient summary of the identified threats and the risk levels that have been assigned to them.

**Table 6.1.2.4.2-1 Threats**

| THREAT # | BRIEF DESCRIPTION | RISK LEVEL |
|---|---|---|
| 1 | UICC is removed from M2ME A and inserted into M2ME B | Minor/Major, depending on the specific M2M use case |
| 2 | UICC is inserted into Rogue M2ME | Minor/Major, depending on the specific M2M use case |
| 3 | Radio interface session keys may be copied/inserted on an exposed UICC–M2ME interface. Although the session keys used in M2M applications may have a quite limited scope to justify such an attack, the requirements to protect keys (crossing the UICC-ME interface) may, in some specific use cases, be higher for M2M devices than for personal devices, due to, for instance, the unguarded, unattended nature of the M2M devices,. | Minor/Major depending on the specific M2M use case |

#### 6.1.2.4.3 Threats and Counter-Measures

### 6.1.2.5 Threat analysis of Alternative 3: UICC based solutions with remote subscription change

#### 6.1.2.5.1 Alternative 3a: IMSI change and key transfer between operators

##### 6.1.2.5.1.1 Introduction

The descriptions of the attacks and the assessment of their likelihood and impact assume the lack of security counter-measures not introduced earlier. The risk analysis will therefore allow suitable counter-measures to be identified.

The alternative analysed here assumes alternative 3 based on the use of UICC or a M2M UICC as defined by ETSI SCP (i.e. including use of new form factor). If alternative 3 should be used without UICC, threats and solutions involving TrE, described at other places in this TR, would apply.

##### 6.1.2.5.1.2 Summary of Threats and Assigned Risk Levels

The table below presents a convenient summary of the identified threats and the risk levels that have been assigned to them.

**Table 6.1.2.5.1.2-1 Threats**

| THREAT # | BRIEF DESCRIPTION | RISK LEVEL |
|---|---|---|
| 1 | Original MNO refuses to assist in transferring subscription to new MNO | minor |
| 2 | Original MNO attacks old subscribers after they have been transferred to new MNO | minor |
| 3 | New MNO eavesdrops on subscribers' traffic with old MNO (recorded before they were transferred to new MNO). | minor |
| 4 | Users lose access to services, due to malfunctions in transferring subscribers from old MNO to new MNO. | minor |
| 5 | Sensitive information can be obtained by a third party by monitoring interactions between the old MNO and the new MNO | minor |

#### 6.1.2.5.1.3 Threats and Counter-Measures

**Threat #1**

Description of attack: Original MNO refuses to assist in transferring M2M users to a new MNO that the subscriber has chosen. The original MNO could claim any motive, like having lost credentials for the actual user. The effect on the M2M subscriber is difficulty to smoothly change operator.

Likelihood: 1

Impact: 2

Risk Level: 2 (minor)

Countermeasures:

1. The M2M subscriber must have a tight contract with the MNO to force the current one to cooperate with the new one, when the subscriber wants to change operator. The contract may have clauses to protect the MNO as well. Only under agreed conditions shall MNO change be possible. A standard contract for the M2M area could be developed to support the M2M business area. Liability clauses can be part of the contract.

**Threat #2**

Description: Original MNO attacks old subscribers after they have been transferred to new MNO.

As the old MNO knows credentials like the subscriber key of the transferred subscriber, he is able to eavesdrop on the traffic for this user in the future. The old MNO may also use a false base station to attract the user and divert and/or eavesdrop on his traffic. Furthermore the old MNO may masquerade as the user towards the new MNO.

There is a substantial risk for bad will or repercussions if it should be discovered that an MNO is recording traffic belonging to other MNOs.

Also note that M2M service profiles as a rule are heavily restricted, with typical limitations like: on traffic type (e.g. only GPRS), on volume (e.g. one SM /month), on called number (e.g. only to fixed service center, not international etc.), on serving networks (e.g. roaming not allowed) etc. This heavily reduces the potential for meaningful fraud, thus reducing likelihood for this particular threat.

Likelihood: 1

Impact: 3

Risk Level: 3 (minor)

Countermeasures:

1. The new MNO may optionally change to a new subscriber key by OTA procedure to minimise the risk for eavesdropping and masquerading. An M2M profiled USIM/UICC could be defined with access conditions that allows this option.

2. The new MNO may later optionally change IMSI for his new users by OTA procedure to make it more difficult for old MNO to locate and identify the transferred users in the new MNO network. The IMSIs used in the transfer process may thus be regarded as temporary 'dummies' used only for the migration period.

3. The new MNO may monitor the new users' traffic with use of a fraud detection system to detect any anomalies.

4. Severe rules may be stipulated in contracts to discourage old MNO to keep any records of old credentials. This can be supported by liability clauses and possibly even with third party inspections.

**Threat #3**

Description: New MNO eavesdrops on subscribers' traffic with old MNO (before they have been transferred to new MNO). The attack assumes that the new MNO 'proactively' has monitored and recorded users' (encrypted) traffic with old MNOs. After they have been transferred to the new MNO he may use the now divulged subscriber keys to decrypt and read the previously recorded traffic. It may be a hard problem for the (potentially new) MNO to find in advance the potentially interesting terminals with a current MNO. Historic M2M traffic probably does not have sufficiently interesting content to motivate preparing for 'post-eavesdropping'. There is a substantial risk for bad will or repercussions if it should be discovered that an MNO is recording traffic belonging to other MNOs.

Likelihood: 1

Impact: 1

Risk Level: 1 (minor)

Countermeasures:

- Any recording of competing MNOs' traffic should already be forbidden by most national jurisdictions. However, it could be further stressed in contracts between M2M subscribers and MNOs that any such recording leading to potential, subsequent eavesdropping, after keys have been transferred, is strictly forbidden.

**Threat #4**

Description: Users lose access to services, due to malfunctions in transferring subscribers from old MNO to new MNO. This could happen if the change of IMSI somehow fails and the modified USIM is not known or 'reachable' for either old or new MNO. Also if the new MNO decides to change subscriber key and/or IMSI using the OTA procedure after the transfer a similar problem may result if the process goes wrong.

Likelihood: 1

Impact: 2

Risk Level: 2 (minor)

Countermeasures:

1. The administrative procedures and document for transferring keys between operators must be well defined and secure.

2. A common M2M profile for the Milenage authentication algorithm should be specified and be implemented in all USIMs dedicated for use in the M2M area. (Alternatively old MNO would have to give his Milenage parameters to new MNO).

3. It has to be specified which USIM parameters, if any, need to be deleted or modified by old MNO in connection with transfer. Likewise it has to be investigated if any USIM parameters must be modified or inserted by new MNO. Access control conditions for read/write must be set accordingly for all relevant EF and for all USIM dedicated for use in the M2M area.

**Threat #5**

Description: If the transfer of sensitive information (IMSIs, Keys) between operators is intercepted by a third party a number of threats can be performed, like eavesdropping and masquerading.

Likelihood: 1

Impact: 2

Risk Level: 2 (minor)

Countermeasures:

1. The administrative procedures and documents for transferring keys between operators must be well defined and secure.
2. New MNO can optionally change IMSI and/or subscriber keys.
3. Fraud detection system can be used to monitor the new subscribers' traffic to discover any masquerading activities.

## 6.2 Security comparison of UICC and non-UICC approaches

### 6.2.1 General

Due to issues identified in section 4.1.2, there is a need to have a M2M equipment providing:

- secure execution environment
- secure storage,
- tamper-resistance

Moreover, it should be possible for operator or third entity to check that all those requirements are together satisfied by the M2M equipment.

The usage of M2ME with or without UICC has been reviewed by different angels in the following clauses.

### 6.2.2 M2M equipment with UICC

The smart card is a tamper resistant device. It has a primary role of storing credentials and performing sensitive cryptographic computations. The smart card contains hardware and software countermeasures to protect against invasive and non-invasive attacks performed to retrieve secrets and obtain sensitive data during execution of computations. For example the smart card contains physical encapsulation of critical circuitry.

Certification, such as Common Criteria, is a means to guaranty a security level for an execution environment. Smart card industry is familiar with certification processes since certification is often mandated in banking to guaranty security.
Some companies noted, that this is true, but actually the vast majority of SIM cards are NOT Common Criteria certified.

Smart card benefits from rich experience to provide security and to resist against software and hardware attacks, e.g. banking, identity, wireless communications…

Consequently, UICC in M2M equipment is a tamper-resistant device providing secure execution environment and secure storage for M2M equipment.

### 6.2.3 M2M equipment without UICC

No consensus has been found on the following issues in 6.2.3.

In case of M2M equipment without UICC, there is a need to secure the M2M equipment.

The following issues can be identified to secure part of the M2M equipment without UICC:

- What are the boundaries of the part of the M2M equipment to secure?
  On the other hand, this can be described. A secure execution environment is certainly required and this, and attendant hardware and software, can help define the boundary.

- How to describe the means to secure the part of the M2M equipment in order to provide secure storage and secure execution?
  On the other hand, it was noted that many new phone processors have secure execution environments, for example TI M-shield and ARM Trustzone processors. There are phones of the market now supporting secure execution environments. There have been phones supporting hardware enforced secure storage for a number of years now

  - By means of requirements on the M2M equipment? Or by means of specifications defining the security mechanisms to be implemented in the M2M equipment?
    On the other hand, a high level security architecture and some security requirements can do this. Essential components of such security requirements for a tamper-resistant trusted environment in a phone are relatively well-known too, and are expected to be incorporated into the TR relatively easily in the near future.

- In case that there is no specification of the security mechanisms to implement:

  - What will be the level of confidence in the countermeasures of the solution against software and physical attacks? All M2M equipments may not secure the same functions. Generic tests could not be applied.
    On the other hand, the same is true for smartcards – there are NO security requirements on smartcards standardised in 3GPP at all, the only thing giving confidence is the fact that the operator chooses his smartcard supplier. We can have a similar approach for USIM on M2M terminals – if an operator does not like a certain terminal type, they don't accept its USIM as valid. The draft architecture in 33.812 would allow for this. In the smartcard world, implementation is not specified by 3GPP or ETSI, but the secure protocols for remote management are and this could include adoption of the specifications of other bodies such as Liberty Alliance and OMA. It is the province of other industry and inter-industry bodies to specify things such as CC protection profiles, if required. OMTP also provides some very comprehensive requirement specifications for such secure execution environments.

  - M2M equipments would not have the same level of security
    On the other hand, UICCs do not all have the same level of security either.

- In case that a certification is required:
  It should be noted that this section assumes that Common Criteria is the only form of certification – this is not the case. There are valid models for self-certification to agreed robustness rules as is done for terminals supporting Digital Rights Management (DRM) technology

  - What will be the scope of the target of evaluation of the solution to secure part of the M2M equipment without UICC?
    On the other hand, taking the term "target of evaluation" loosely, a TOE could be semi-formally defined for the secure execution environment on a processor supporting this, and attendant s/w and h/w (e.g. the secure boot mechanism on the terminal)

  - Do Protection Profiles exist for this type of solution?

  - What is the expertise of companies providing the solution to perform certification of this type of solution?
    On the other hand, terminal manufacturers that engage in either government products or in products supporting strong DRM have experience in evaluating products for robustness of implementation. In addition, such expertise can also be brought in by recruitment or by professional services.

- What is the level of security of the secured part of the M2M equipment against software and physical attacks compared to the security level offered by the other solutions, and in particular those which are UICC-based?
  On the other hand, some believed that terminals with an integrated USIM solution can meet the required levels of security. Further, we do not see that there is any reason why the terminal cannot in principle be made just as secure as a UICC. With respect to some forms of side channel attack, e.g. power and timing analysis, the integrated USIM solution may well provide more resistance than a UICC due to the higher number of contemporaneous processes masking critical cryptographic operations

- If the selected solution to protect a part of the M2M equipment relies on the addition of a specific hardware element to M2M equipment, what is the benefit compared to UICC-based solutions?
  On the other hand, the addition of specific hardware elements may not be required. However, even if it is required, the solution would have the advantage over UICC-based solutions of not exposing a physical UICC-ME interface that could be attacked. The solution is also likely to have other advantages, e.g. cost, power consumption, provisioning efficiency, size. In some implementations, an advantage is that it does not require the terminal to support a physical UICC interface. There are use cases in TR33.812 that describe terminals that would not be supplied with a UICC connector as standard

### 6.2.4 Security Assurance for USIM application integrated into M2M equipment

Traditionally USIM applications have been required to be instantiated within a removable UICC. Operators buy and own the UICCs of their subscribers and can therefore impose their own requirements on their UICC suppliers. Apart from the occasional security failing (e.g. the weak COMP-128 algorithm) this model has served operators well and it is to be expected that there will be some concern at the suggestion that the USIM application could be integrated into the M2M equipment itself (an M2M equipment that will not be owned by the operator) instead of in a UICC. One of the major concerns that operators have with the USIM application being integrated into the M2M equipment (with "an integrated USIM") is that the integrated USIM will not be as robust as a USIM within a UICC. Operators also have concerns for reasons other than security and these reasons must also be taken into account.

This sub-section examines methods whereby operators could be given assurances that integrated USIMs are indeed sufficiently robust.

The methods by which operators are given assurance about the robustness of their UICCs is first examined. The following points can be made:

1. Security assurances are gained because the operator chooses their UICC supplier and can therefore choose a supplier that meets the operator's security requirements. Since operator revenues will suffer if the UICC security is broken, the operator has an incentive to choose a reputable and competent supplier.

2. If the supplier turns out not to be reputable and competent, the operator can move, with a certain delay, to an alternative supplier.

3. Further, the operator may choose to have a very small number of UICC suppliers and can therefore spend a reasonable amount of time auditing each supplier, or alternatively requiring the supplier to get themselves audited against an agreed standard, such as the GSMA Smartcard Supplier Accreditation System.

4. Finally, UICC suppliers generally release new products at a lower rate than terminal suppliers and have a smaller range of platforms on which UICCs are built than most terminal suppliers. There is therefore a relatively small range of UICCs and UICC platforms and again this gives the operator the chance to spend some time examining each candidate

5. Further, the UICC is a system with relatively limited complexity when compared with MEs. Therefore, it can be assessed for security and robustness with less effort than that which would be required for an M2ME. Even though UICCs are growing more complex, they are likely to remain less complex than an ME).

There seem to be two forces at work here:

a Market forces, in that operators have an incentive to choose good UICC suppliers or their revenues will suffer, and that operators can reasonably easily change bad UICC suppliers, and UICC suppliers therefore have an incentive to produce robust UICCs or they will not be chosen by operators

b The opportunity for due diligence (because of the relatively small number of UICC platforms) and audit, which operators may choose to carry out themselves (because of the relatively small number of UICC suppliers), or require their suppliers to get themselves audited to

It might be thought that these two methods do not give operators assurance if the USIM application is integrated into the M2M equipment, for the following reasons:

- The operator does not own the M2M equipment and cannot therefore impose their own security requirements on the M2M equipment supplier

- As the operator does not own the M2M equipment, operator market forces cannot be used to safeguard standards of security

- There are more terminal suppliers than smartcard suppliers, and terminal suppliers typically have more frequent update of products and platforms that smartcard supplies do. There is therefore too large a range for the operator, or any entity, to carry out sufficient due diligence on the terminal suppliers or their products and platforms.

However, the following points can be made in response:

1. Although the operator may not be the final owner of an M2M equipment with an integrated USIM, the operator may choose to use their expertise in terminal sourcing on behalf of final owners and so be a distributor of such terminals, i.e. buy these terminals themselves and then sell onto the final owners in the same way that many operators today are distributors of consumer terminals. Operator market forces can in this way be brought to bear on the M2M terminal market.

   a However, it should be noted that the UICC is primarily a security device, and security can be a very significant factor in purchasing decisions. The M2M equipment is not primarily a security device and security cannot therefore be such a significant factor.

   b Further, operators will not be the only purchasers of M2M equipments. There may be some very significant non-operator purchasers of M2M equipments such as those within the automotive industry. Operator market forces may not in reality be that significant.

   c Finally, its clear that the operator is no longer in sole control of the security of their USIM applications via direct relationship with their UICC providers, and that the operator is now dependent on other entities, including other operators, equipment suppliers and possibly certification agencies.

2. Although the operator may not be the owner of the entire M2M equipment, it may become a sole 'owner' of certain functionality (an " operator compartment") – such as one that manages and performs integrated USIM functionality - of the M2M equipment, by use of available technologies (e.g. the trusted mobile platform technology from the Trusted Computing Group TCG [3] and [4]. The operator who has ownership of the integrated USIM functionality can exclude interfering actions on it by any other stakeholder of the M2M equipment.

   a However, the feasibility of operator controlled M2ME functionality is yet be studied or proven if the M2ME has to support multiple operator compartments or if transfer of control of an operator compartment from one operator to another is required.

3. There are technologies (such as those described within TCG specifications) available that enable the operator to audit the trustworthiness (e.g. authenticity and integrity) of software responsible for all or selected functionality (such as the application and USIM security functionality) in a remotely located terminal during the time of its deployment. Use of such technologies can increase the operational trustworthiness of the M2M equipment.

4. Although the present number of consumer terminal suppliers is more than the number of smartcard suppliers, M2M equipments may be a niche market with fewer suppliers.

5. Further, although the number of consumer terminal suppliers is relatively large, the number of terminal hardware suppliers is actually quite small, and this is also likely to be the case for M2M equipments. If the architecture of M2M equipments with integrated USIMs is designed so that the security of the integrated USIM application mainly or totally depends on certain isolated portions of the terminal hardware, e.g. a hardware-embodied Trusted Environment (TRE) within such terminals, then this further reduces the number of entities that an operator or other relying party needs to conduct very detailed due diligence upon (though the requirement to still audit the final terminal supplier is admitted),

6. Requirements for terminal supplier audit can be used (as they often are on smartcard suppliers) as can requirements on the robustness of the terminal implementation, in the following way:

   a The M2M equipment, and especially the TRE within such a terminal, can be required to authenticate itself (as Alternative 1) requires), e.g. by means of a public key certificate. There could be a central body overseeing issuance of such certificates (though not perhaps issuing them itself) and imposing requirements on terminal suppliers or the suppliers of TREs, if the TRE is a physically discrete component.

   b Operators or other USIM-issuing entities could be required to refuse to issue USIM applications into terminals that do not have a certificate from the PKI of this overseeing central body.

   c The requirements imposed by the central body could include the terminal supplier (and TRE supplier, if applicable) having successfully passed an audit on their processes.

d These requirements could also include security requirements on the robustness of the terminal implementation that the terminal supplier self-certifies to ("robustness rules"). If it is found that M2M equipments from a supplier do not in fact meet the security requirements, then measures could be imposed on the terminal supplier in order to ensure corrections are made as soon as possible.

e However, it's not clear which entity would take on this central role nor what the infrastructure requirements would be. The cost of running this infrastructure may result in the overall cost of the integrated M2M-USIM option being greater than the cost of using UICCs. There may be difficult legal issues.

By these means it seems that the power of market forces and of audit and due diligence, the chief means by which security standards are upheld for smartcard suppliers, can also be used with respect to suppliers of M2M equipments.

# 7. Evaluation of Candidate Solutions

## 7.1 General

In the following three subsections, the scores of evaluation of the three network architecture alternatives are given, using the evaluation criteria described in section 4.3.

## 7.2 Alternative 1: TRE based solution with remote subscription provisioning and change

"+" means a positive comment

"-" means a negative comment

| EVALUATION CRITERION | COMMENTS |
|---|---|
| 1 **Security** | + It incorporates device integrity validation performed from within the TRE.<br>+ If the TRE is non-removable, an embedded TRE addresses issues such as unauthorised removal/replacement of TREs and attacking the TRE's interfaces.<br>- Uses a broadly defined (for evaluation purposes) embedded TRE for storing authentication credentials, rather than a well-defined dedicated security module such as a UICC. This makes it more difficult assess the level of security provided.<br>- Based on security technology which is yet to be proven as a satisfactory way of protecting authentication credentials.<br>- Requires all involved operators to trust the M2ME/TRE and M2ME/TRE supplier to provide a secure environment for storing authentication credentials, unless there is a central body certifying M2MEs/TREs or M2ME/TRE suppliers.<br>- Requires all involved operators to trust the PVA to validate the trusted environment before downloading an MCIM to it.<br>- Individual operators have limited control over the M2MEs which they accept onto their network and as a consequence may have a low level of assurance about the security level provided by the M2ME/TRE and the M2ME/TRE supplier.<br><br>- A specific M2ME may only be able to support a limited set of cryptographic algorithms. This reduces the diversity of authentication algorithms between operators, and makes it difficult for an individual operator to introduce a new authentication algorithm. This may have a negative impact on the overall level of security offered, and goes against the principle that individual operators should be free to select their own authentication algorithms.<br><br>- If operator-specific security applications other than MCIMs need to be downloaded and executed in the M2ME, then procedures will be needed to ensure that these applications can be securely isolated between operators. |
| 2 **Initial choice of operator** | + The choice of SHO can be made after deployment of the M2ME.<br>- The choice of initial connectivity operator (ICO) has to be made at the time the M2ME is manufactured (assuming the ICO uses 3GPP access). |
| 3 **Operator change** | + This is provided for using OMA DM protocols.<br>- There will be a problem if the new operator does not have a contract or trust relationship with the M2MES or PVA.<br>+ Supports an unlimited number of operator changes.<br>+ No physical interaction by operator for initialization, maintenance, and invalidation.<br>-Mechanisms for downloading and managing other files, in addition to IMSI and key K procedures will need to be defined between MNO (still FFS in section 5.1.1.2 what should be the content of an MCIM). |
| 4 **Remote management** | + This is provided for using OMA DM protocols. |
| 5 **Legal and regulatory impact** | - May be difficult for operator to provide assurance to regulator that M2M subscriptions cannot be cloned or tampered with due to lack of operator control on TRE compared to a UICC based solution.<br>- This solution may not allow network operators to sufficiently manage their legal risk. It may require network operators to trust many third parties or be excluded from the market.<br>- Use of this solution would require network operators to support TRE-based subscription management infrastructure or be excluded from the market. Since M2MEs which include a TRE for storing subscription credentials will be a new phenomenon in some countries (phones with similar credential protection techniques are already used in countries with CDMA systems) regulatory bodies should be consulted |
| 6 **Flexibility to adapt to new requirements** | + Allows flexibility to the owners/subscribers of the M2ME in terms of provisioning and subscription management. This assumes that a sufficient number of network operators trust this solution.<br>- Future subscription management requirements may require new M2ME subscriber management capabilities that are not available in already deployed M2MEs of the type described in this solution. This would require M2ME replacement, if the new TRE functions could not be installed by a remote upgrade. |
| 7 **Viability of trust model** | - Requires all involved operators to have trust in the M2ME/TRE and associated PVA. This may be a viable trust model in some scenarios e.g. when operator change is only required between a relatively small group of operators that have a business relationship that would allow them to place trust in a common set of M2ME/TRE manufacturers and their corresponding PVAs. However, it seems infeasible to establish a single, globally trusted PVA that *all* operators would trust. Possibly a model is required similar to that of multiple CAs today. |
| 8 **Suitability to** | + Mostly suitable (providing the need to trust a central authority is not a constraint). |

| | |
|---|---|
| **mass market deployment** | - Need to choose an ICO at time of device manufacture could be an issue (assuming the ICO uses 3GPP access). |
| 9 **Impact on subscription management systems** | - Major impact: Significant new technical capabilities including OMA DM and PKI need to be supported. Also, business procedures for subscription management are radically changed. |
| 10 **Impact on network infrastructure** | Same comment as item 9. |
| 11 **Impact on terminal** | - Major impact: TRE must be supported. This can be based on currently available trusted computing technology and/or secure execution environment, and it is a significant change to require that terminals support embedded trusted computing technology to protect mobile subscription credentials.<br>- Costs of design, development, components and certification for the TRE.<br>+ Eliminates the need for some discrete components such as UICCs and their connection devices, power supplies and external clocks.<br>+ Potential problems with respect to removable credential storage and physical interface are reduced (e.g. 'card not found' errors).<br>+ Avoids mechanical and form-factor constraints on the M2ME casing that normally result from requirements to be able to open/close part of the casing to insert a UICC a minimal number of times. |
| 12 **Impact on 3GPP specifications** | - Various new specifications required, however some re-use of existing specs should be possible (e.g. OMA DM). |

## 7.3 Solution Alternative 2: UICC based solution with no remote subscription provisioning and change

"+" means a positive comment

"-"Means a negative comment

"U" means that it was impossible to evaluate the solution, due to insufficient information in the description of the solution

| EVALUATION CRITERION | COMMENTS |
|---|---|
| 1 **Security** | Editor's Note: It is FFS whether methods to physically prevent UICC removal need to be described in this TR. It is also FFS whether the case needs to be covered that the UICC can only be physically removed by authorised personnel e.g. by protecting it inside a locked enclosure which can be unlocked by unauthorised personnel only. |
| 2 **Initial choice of operator** | |
| 3 **Operator change** | Operator change: This alternative does not address the issue described in TR22.868, i.e. how to effect a remote change of operator on M2MEs. This architecture requires the M2ME to be visited by personnel in order to replace the UICC.<br>+ It can be performed by physically replacing the UICC in the M2ME.. This procedure uses existing process and does not impact on M2ME manufacturers<br>- It relies on direct human interaction with device |
| 4 **Remote management** | This architecture requires the M2ME to be visited by personnel in order to replace the UICC.<br>+ Some limited functionality (but not operator change) is provided for using existing OTA protocols<br>- It relies on direct human interaction with device |
| 5 **Legal and regulatory impact** | + Due to the vast M2M business, the appropriate protection against unauthorised removal, of the UICC is defined and implemented case by case, taking also into account possible applicable regulatory requirements (e.g. on fair competition).<br><br>+ May help *"MNO's to fulfil their obligations towards regulatory and other governments to guarantee secure authentication and billing"* (GSMA SCaG), if the security issues listed in 1 above are addressed (and the existing M2M business shows that they can be adequately addressed).<br>+/- No risk to "lock out" new operators that are. not willing to trust central authority or invest in new infrastructure. |
| 6 **Flexibility to adapt to new requirements** | + Automatic tracking and alignment with consumer UICC developments<br>+ This solution can be applied with traditional UICC (as currently shown by the existing M2M market) and also with UICCs with a new Form Factor, specifically designed to take in possible M2M peculiarity and/or requirements |
| 7 **Viability of trust model** | |
| 8 **Suitability to mass market deployment** | |
| 9 **Impact on subscription management systems** | + No impact |
| 10 **Impact on network infrastructure** | + No impact |
| 11 **Impact on terminal** | The requirement to provide a physical interface for UICC replacement may be problematic for use cases where very small devices are required.<br>- Dependent on how the security issues in 1 above are addressed<br>+no impact unless measures used to remove threat of unauthorised UICC removal are implemented |
| 12 **Impact on 3GPP specifications** | + no impact: the exiting M2M market relies on this solution. The appropriate implementation-dependent measures that may be needed to implement (depending on the specific M2M use case) to avoid possible unauthorised UICC removal are out of the scope of 3GPP. |

## 7.4 Alternative 3

### 7.4.1 Alternative 3a: IMSI change and key transfer between operators

"+" means a positive comment

"-"Means a negative comment

"**U**" means that it was impossible to evaluate the solution, due to insufficient information in the description of the solution

| EVALUATION CRITERION | COMMENTS |
|---|---|
| 1 Security | +/- Complying with some of the security requirements in section 4.3.1, that apply to UICC-based solutions, could be a problem, as follows:<br>- unauthorised removal or exchange of the UICC may be possible.<br>+ However, if UICC removal or exchange needs to be prevented for security reasons, then mechanical or logical binding of the UICC to the M2ME is feasible using existing techniques such as soldering, a strongbox, or the ETSI secure channel standard.<br>- Radio interface session keys may be copied/inserted on an exposed UICC–M2ME interface. The requirements to protect the UICC-ME interface for things like CK/IK may be higher for M2M devices than for personal devices, due to 1) the unguarded, unattended nature of the M2M devices, and also that 2) many M2M devices may have a gateway capability, so a compromise may increase the impact of key exposure over the UICC-ME interface for specific use cases. The ETSI/3GPP secure channel specifications (ETSI TS 102 484 / 3GPP TS 33.110), which require a shared secret or other type of credential, may be used to protect the UICC-M2ME interface if required. It is FFS to what extent these countermeasures are useful and needed for M2ME. Or physical security mechanisms may be used to protect the UICC-M2ME interface if required<br>- Operators would have to trust other operators to provide subscriber/OTA key pairs for whole populations of devices, which exceeds the current trust model.<br>- Operators would have to trust other operators to destroy previous subscriber keys.<br>- requires the new operator to trust the UICCs of the old operator.<br>- Individual operators have limited control over the UICCs which they accept onto their network and as a consequence may have a low level of assurance about the security level provided by the UICC and the UICC supplier.<br>- If operator-specific security applications need to be provisioned on the UICC, then procedures will be needed to ensure that these applications can be securely isolated between operators.<br>- It is difficult for individual operators to keep the details of the authentication algorithm(s) they use confidential which is a desirable security requirement.<br>- The scheme reduces the diversity of authentication algorithms between operators, and makes it difficult for an individual operator to introduce a new authentication algorithm. This may have a negative impact on the overall level of security offered, and goes against the principle that individual operators should be free to select their own authentication algorithms.<br>- The case where OTA keys are shared between MNO involves new important security threats.<br>- Means for exchanging authentication keys between operators AuC while keeping the right confidentiality level are not described |
| 2 Initial choice of operator | - The initial operator can be used for initial connectivity only. This would allow the choice of selected home network to be made after deployment of the M2ME. The initial choice of operator has to be made at the time that the UICC is installed, which (for a non-removable UICC) happens during manufacture of the M2ME. For a removable UICC, installation of the UICC could be done at any time after manufacture and even after deployment of the M2ME but that could be expensive and difficult to achieve in some use cases. The most favourable stage for inserting the UICC has to be considered from logistical, economical and security points of view. |
| 3 Operator change | + this is provided for using OTA protocols<br>- There is a concern that the background transfer of ownership of a population of M2MEs from an old operator to a new operator could be performed when some of those M2MEs are not network-attached. In that case, those M2MEs would then be unable to attach to any network.<br>- a common minimum UICC profile must be agreed within the MNO community<br>U: it is not explained how a new operator can join the scheme, i.e. how to establish trust with the existing set of operators<br>- Many other files, in addition to IMSI and key K (and possibly OTA keys) will need to be changed. Data under ADM protection inside the USIM, non-standardized data, and procedures will need to be changed and aligned between MNO.<br>- After each change of operator, the 1st authentication with the new operator will lead to a synchronization failure, which might not be desirable. To prevent this, a specific procedure should be established between MNOs to transmit SQN values managed in their AuC. |
| 4 Remote management | + this is provided for using OTA protocols<br>- remote application management is needed to handle the case where UICC applications are not shareable between operators. This adds complexity to the overall system management and brings some risks regarding interoperability.<br>- The OTA increased capabilities (servers) that would be needed to manage the UICC (i.e. downloading of keys, applications, files) are likely to be a costly solution. |
| 5 Legal and regulatory impact | U: in general, UICC based solutions are well understood and accepted by regulators but it is not yet known if this alternative would require any further re-assessment |
| 6 Flexibility to adapt to new requirements | - Standard OTA mechanisms are likely to be replaced by IP-based mechanisms.<br>+ It can be assumed however that any new such OTA mechanisms have similar or same functionality regarding remote managing of USIM fields in a secure way.<br>- This solution would require network operators to support new inter-operator subscription management infrastructure or be excluded from the market. That requirement could be viewed |

| | |
|---|---|
| | adversely by some regulatory bodies.<br>+ Changes in subscription management will not create any new requirements on the M2ME itself, i.e. such changes will only impact the UICC. However, UICC replacement is lower cost than replacement of entire M2ME<br>- However, the use of field-replaceable UICCs could be a security issue, due to the risk of unauthorised replacement. |
| 7 Viability of trust model | - Goes beyond current trust models, see criterion 1 above. Viability of new requirements is FFS |
| 8 Suitability to mass market deployment | + mostly suitable<br>- need to choose initial connectivity operator at time of device manufacture (if that is logistically needed) could be an issue |
| 9 Impact on subscription management systems | + minimal impact |
| 10 Impact on network infrastructure | + minimal impact |
| 11 Impact on terminal | - Need to use multiple secure algorithms will require large memory UICCs, which may not be a cost-effective solution. |
| 12 Impact on 3GPP specifications | + minimal impact<br>- the option which proposes the change of Milenage OPc parameters needs new standardization effort on the USIM application. |

### 7.4.2 Candidate Solution Alternative 3b: Pre-configured K list on UICC

"+" means a positive comment

"-"Means a negative comment

"U" means that it was impossible to evaluate the solution, due to insufficient information in the description of the solution

| EVALUATION CRITERION | COMMENTS |
|---|---|
| 1 Security | - Complying with some of the security requirements in section 4.3.1, that apply to UICC-based solutions, could be a problem, as follows:<br>- unauthorised removal or exchange of the UICC may be possible. However, if UICC removal or exchange needs to be prevented for security reasons, then mechanical or logical binding of the UICC to the M2ME is feasible using existing techniques such as soldering, a strongbox, or the ETSI secure channel standard.<br>- there may be a problem in meeting the requirement "Exposure of subscriber authentication keys to unauthorised 3rd parties would have severe consequences ….". The UICC supplier, or another central authority, is required to act as a long-term key-escrow for sequences of key-pairs for future operator-changes, whereas currently keys can be destroyed very soon after batches of UICCs are personalised and the corresponding keys sent to the recipient operator.<br>+ meets the other security requirements listed in section 4.3.1, that apply to UICC-based solutions<br>- Requires all involved operators to trust the installed UICC and UICC supplier to provide a secure environment for storing authentication credentials.<br>- Radio interface session keys may be copied/inserted on an exposed UICC–M2ME interface. Although the session keys used in M2M applications may have a quite limited scope, the requirements to protect keys (crossing the UICC-ME interface) may, in some specific use cases, be higher for M2M devices than for personal devices, due to 1) the unguarded, unattended nature of the M2M devices, and also that 2) many M2M devices may have a gateway capability, so a compromise may increase the impact of key exposure over the UICC-ME interface for specific use cases. The ETSI/3GPP secure channel specifications (ETSI TS 102 484 / 3GPP TS 33.110), which require a shared secret or other type of credential, may be used to protect the UICC-M2ME interface if required. It is FFS to what extent these countermeasures are useful and needed for M2ME. Alternatively physical security mechanisms may be used to protect the UICC-M2ME interface if required and these mechanisms can have more strength on an M2M device than on a consumer device.<br>- Individual operators have limited control over the UICCs which they accept onto their network and as a consequence may have a low level of assurance about the security level provided by the UICC and the UICC supplier.<br>- If operator-specific security applications need to be provisioned on the UICC, then procedures will be needed to ensure that these applications can be securely isolated between operators.<br>- It is difficult for individual operators to keep the details of the authentication algorithm(s) they use confidential which is a highly desirable security requirement.<br>- The scheme reduces the diversity of authentication algorithms between operators, and makes it difficult for an individual operator to introduce a new authentication algorithm. This may have a negative impact on the overall level of security offered, and goes against the principle that individual operators should be free to select their own authentication algorithms.<br>- The case where OTA keys are shared between MNO involves important new security threats. |
| 2 Initial choice of operator | + The choice of SHO can be made after deployment of the M2ME, if the initial operator is used for initial connectivity only.<br>- The initial choice of operator has to be made at the time that the UICC is installed, which (for a non-removable UICC) happens during manufacture of the M2ME. For a removable UICC, installation of the UICC could be done at any time after manufacture and even after deployment of the M2ME but that could be expensive and difficult to achieve in some use cases. The most favourable stage for inserting the UICC has to be considered from logistical, economical and security points of view. |
| 3 Operator change | + this is provided for using current OTA protocols<br>- For the case that subscription change is done by OTA, there could be a problem if the new operator does not have a contract or trust relationship with the UICC supplier or central authority responsible for managing the distribution of Ki/OTA key pairs<br>- there is a concern that the background transfer of ownership of a population of M2MEs from an old operator to a new operator could be performed when some of those M2MEs are not network-attached. In that case, those M2MEs would then be unable to attach to any network.<br>+/- If OTA based operator change is not possible for either of the reasons above, then operator change by UICC swap may be possible, although that solution clearly does not fulfil any requirement to be able to change the subscription remotely. However, the use of field-replaceable UICCs could be a security issue, due to unauthorised replacement.<br>- Many other files, in addition to IMSI and key K (and possibly OTA keys) will need to be changed. Data under ADM protection inside the USIM, non-standardized data, and procedures will need to be changed and aligned between MNO. |
| 4 Remote management | + This is provided for, using OTA protocols<br>-/+ Supports a finite number of operator changes limited by the number of Ki/OTA key pairs initially loaded onto the UICC but the number of possible operator changes can be made large enough to satisfy all practical operator change scenarios. |

| | |
|---|---|
| 5 Legal and regulatory impact | - There is some potential for a non-removable UICC approach to "lock out" new operators that are e.g. not willing to trust the central authority or invest in the new infrastructure needed to manage the functionality associated with the preconfigured Ki list.<br>U: in general, UICC based solutions are well understood and accepted by regulators but it is not yet known if this solution would require any further re-assessment<br>- Use of this solution means that network operators would be required to support specific subscription management infrastructure and special UICC capabilities, or be excluded from the market Likewise, UICC suppliers could be required to adopt a new role and infrastructure for long-term key escrow. Those requirements could be viewed adversely by some regulatory bodies. |
| 6 Flexibility to adapt to new requirements | - use of standard OTA is a limitation, as it is likely to be replaced by IP-based mechanisms<br>+ It can be assumed however that any new such OTA mechanisms would have similar or the same functionality regarding remote management of USIM fields in a secure way.<br>+ Changes in subscription management will not create any new requirements on the M2ME itself, i.e. such changes will only impact the UICC. However, UICC replacement is lower cost than replacement of entire M2ME<br>- However, the use of field-replaceable UICCs could be a security issue, due to unauthorised replacement. |
| 7 Viability of trust model | - Requires all involved operators to have trust in a central authority which, in this case, may be a UICC supplier. This is, in principle, a viable trust model, although it exceeds the current trust model, as described under “security”. The general need to trust a central authority seems to be a common requirement of some solutions which supports remote operator change. |
| 8 Suitability to mass market deployment | + Mainly suitable (assuming the need to trust a central authority is not a constraint)<br>- the need to chose initial connectivity operator at time of device manufacture could be an issue |
| 9 Impact on subscription management systems | + Moderate impact: new technical capabilities and business processes would be needed to support remote subscription management. However, these can be based on extension/adaptation of existing systems |
| 10 Impact on network infrastructure | + as per “Impact on subscription management systems” |
| 11 Impact on terminal | + No significant impact is foreseen |
| 12 Impact on 3GPP specifications | - Some changes will be required to UICC specifications to enable the key indexing features to be activated remotely and securely. |

# 8 Summary and conclusions

## 8.1 Summary of the report methodology and solutions presented

### 8.1.1 General

This technical report presents a study of the feasibility of securely and remotely managing USIM/ISIM/MCIM applications for M2M equipment within a 3GPP system. Security aspects of some M2M use cases are analysed. A number of security and other requirements are derived from this analysis, and evaluation criteria are derived from these security requirements. A variety of solutions for securely and remotely managing USIM/ISIM/MCIM applications for M2M equipment are then presented, these are:

Alternative 1: TRE-based solution with remote subscription provisioning and change

Alternative 2: UICC-based solution with no remote subscription provisioning and change

Alternative 3a: UICC-based solution with remote subscription change; K transfer between operators

Alternative 3a: UICC-based solution with remote subscription change; Pre-configured K list on UICC

A threat analysis methodology is described and applied to each of the proposed solutions. Both general threats which apply to any potential solution as well as threats specific to the proposed alternatives are considered. Each alternative is then evaluated according to the criteria given earlier.

Many key aspects of this report, such as the requirements and evaluation criteria, already exist in a compact form and therefore need not be repeated here. The descriptions of the proposed solutions themselves can be quite long, however, so each of them is briefly summarized below.

### 8.1.2 Alternative 1: TRE based solution with remote subscription provisioning and change

This solution relies on a trusted environment (TRE) within the M2M equipment. Among other features, a TRE should also be able to validate the M2M equipment and perform user authentication. A TRE hosts one or more MCIMs, which are remotely provisioned over the air. MCIMs can exist in one of several lifecycle states. A TRE will manage the transitions between these states and enforce security controls on the MCIMs.

The solution also includes a network architecture which defines a variety of functions, roles and services. A role performs one or more functions. The mapping of functions to roles is not specified, though some natural groupings are evident. Services are provided by one or more functions to the M2M equipment and/or subscriber.

The basic services described are initial and operational connectivity, application, and M2ME supply. The goal of initial connectivity is to provide an IP connection over which the M2ME can be provisioned with credentials and other data required to access the operational network, which may provide any standard 3GPP connectivity. Application services are concerned with supplying the required MCIMs to the M2ME, while the goal of M2ME supply is to physically deploy a functional M2ME to the subscriber.

Several functions form a part of this solution. The Connectivity Credential Issuing Function (CCIF) is responsible for generating credentials required for initial network access. The Discovery and Registration Function (DRF) helps the M2ME to discover and register with the SHO. The MCIM Download and Provisioning Function (DPF) manages the downloading and provisioning of MCIMs to the M2ME. The Initial Connectivity Function (ICF) provides IP connectivity to allow the M2ME to discover the SHO.

These functions are performed by one of the following roles: M2ME subscriber; M2ME supplier; Registration, Visited Network, and Selected Home Operators; Non-3GPP Initial Connectivity Service Provider; Platform Validation Authority (PVA); and Regulator. Most of these roles are self-explanatory. The registration operator provides initial connectivity as well as registration and provisioning functions to the M2ME. Non-3GPP Initial Connectivity Service Providers provide non-3GPP access to activation and registration services for the M2ME. The PVA is the authority responsible for validation of credentials used to verify the M2ME as a trusted platform based on a platform credential supplied by the M2ME before downloading of the MCIM takes place. A Regulator may governs the operation of the M2MEs and networks in a country or region.

The solution provides examples of the interactions among the defined roles that are necessary for an M2ME to be remotely provisioned with an MCIM application and credentials. The process of changing to a new SHO is also detailed. Two variants are presented: moving directly from one SHO to another and using the intermediate step of reverting to the original, or pristine, state.

Lastly, the solution presents a trust model describing the tasks that each role is expected and trusted to do by the others.

### 8.1.3 Alternative 2: UICC-based solution with no remote subscription provisioning and change

This solution consists of providing a removable UICC to each deployed M2M equipment. Either a standard UICC or one having an M2M-specific form factor may be used. Initial provisioning consists of inserting into the device a UICC from the operator selected by the M2M subscriber. The same process is also employed to change a subscription to a different operator. This alternative is the solution currently used for the existing 3GPP M2M business.

### 8.1.4 Alternative 3a: UICC-based solution with remote subscription change; Ki transfer between operators

This alternative presents a mechanism which allows an over-the-air change of MNO in a deployed M2M equipment. The change mechanism comprises the following steps:

- The new operator B provides a list of IMSIs of M2MEs to be changed.

- The current operator A uses standardised over-the-air procedures to change the IMSIs as requested.
- Operator A provides operator B with a list of the new IMSIs along with associated subscriber keys Ki and OTA keys.

The alternative describes the following requirements:

- Each operator must trust that the others will protect the Ki and OTA key pairs and not use them to compromise the M2M communications.
- All involved operators must also support a common Milenage profile and specified OTA procedures.

### 8.1.5 Alternative 3b: UICC-based solution with remote subscription change; Pre-configured Ki list on UICC

This solution also provides a mechanism to allow over-the-air change of MNO in a deployed M2M equipment. An M2M equipment is provided with a UICC containing an initial IMSI and an indexed list of Ki/OTA key pairs. The first such pair is associated with the initial IMSI, while the others are kept secret by the UICC manufacturer. The process of changing operators is similar to that of Alternative 3a:

- The new operator B provides a list of IMSIs of M2MEs to be changed.
- The current operator A uses standardised over-the-air procedures to change the IMSIs as requested. During these procedures, the new IMSI is associated with the next Ki/OTA pair stored in the UICC.
- Operator A provides operator B with a list of the new IMSIs along with the index values of the new Ki/OTA key pairs.
- Operator B uses these index values to obtain the next Ki/OTA pair from the UICC manufacturer.

The alternative describes a few requirements. Each operator must trust the UICC manufacturer to protect the Ki/OTA pairs. Use of a common Milenage profile and specified OTA procedures would be advantageous.

Two variants are also mentioned, where Ki/OTA pairs are managed by an entity other than the UICC manufacturer and where the OTA procedures are performed by an entity other than an involved operator.

## 8.2 Summary of the solution evaluations against the use cases and against the evaluation criteria

### 8.2.1 Summary of the solutions evaluated against the use cases

NOTE: There are many more use cases, and for such use cases, the evaluation result might be different from what is presented in this clause.

The use cases in section 4.1 were developed in order to derive security requirements and in turn, evaluation criteria for the candidate solutions - they were not developed to directly assess the candidate solutions. Nonetheless, as the use cases were considered sufficiently representative to be used as a source of security requirements, they can also be considered sufficiently representative for there to be some value in assessing how the candidate scenarios could be used to implement them.

The four use cases in section 4.1 are (see section 4.1 for full descriptions):

- Use Case 1: Traffic Cameras
- Use Case 2: Metering
- Use Case 3: Vending
- Use Case 4: Asset / Cargo Tracking

#### 8.2.1.1 Alternative 1: TRE based solution with remote subscription provisioning and change

For all four use cases, Alternative 1 is capable of fulfilling the totality of common requirements, as follows:

- M2MEs can be subscribed to network operators after deployment of the M2MEs.
- It is not necessary for any personnel to visit the M2MEs in order to initially provision or to change the network subscription.
- Network subscriptions of single M2MEs or of large, widely dispersed populations of M2MEs can be changed in a short time.
- - Addresses the requirements of "track and trace" use cases, as pointed out by 3GPP WG SA1 in [2].

In order to meet the requirements of the four use cases, Alternative 1 requires new infrastructure in the CN, and requires the use of a standardised authentication algorithm. The use of Milenage was disputed in this study. Alternative 1 requires the existence of a TRE in the M2ME, which provides a secure environment for the storage and execution of MCIMs and which assures the security of the subscription download processes, which is the main issue of the Alternative 1.

Use of a TRE to store 3GPP subscription credentials represents a change from established and ad proven security procedures, which rely on a UICC.

#### 8.2.1.2 Alternative 2: UICC-based solution with no remote subscription provisioning and change

Alternative 2 can meet all four use cases, and indeed there are implementations of this solution in the market already for use cases 1, 3 and 4 at least.

Alternative 2 provides a market and time proven solution for secure subscription credentials and operator specific data (algorithms, applications, etc.) storage in a tamper resistant device.

However, use of Alternative 2 presents some issues:

- This alternative does not support remote provisioning and subscription change. This means that physical contact with the M2ME will be needed in order to change operators. Physical contact will also be needed to perform the initial choice of operator if this choice must be made after the device is deployed.
- Removable UICCs may also be subject to unauthorized removal in some M2M use cases unless additional protection mechanisms are used.

#### 8.2.1.3 Alternative 3a: UICC-based solution with remote subscription change; IMSI change and key (K) transfer between operators

Alternative 3a can be used to implement all four use cases, except that it does not allow for *remote* choice of initial operator after the M2ME has been deployed. As M2MEs operate in exposed environments, the unauthorised removal of the UICC can become an issue. The exchange of subscriber/OTA keys among operators will require the establishment of trust relations among those operators. It may be challenging for a new operator to join a group with a pre-existing set of such relations Also, especially in the context of alternative 3a, where operators are required to exchange K/OTA key pairs, a large infrastructure for the establishment of trust relationships has to be established to enable the exchange of subscriber/OTA key pairs among operators.. Since a UICC is used, there may be concerns with UICC removal for some use cases. However, this alternative provides for remote change of subscription, which means that the UICC can, if required, be physically attached to the M2ME so that it is very difficult or impossible to remove.

The requirement to have a UICC may also mean that M2MEs cannot be below a certain size, which may lead to devices/modules that are too big for variants of the use cases where very small embedded M2MEs are required. The use of the new Industrial Form Factor UICC may address this concern,.

#### 8.2.1.4 Alternative 3b: UICC-based solution with remote subscription change; Pre-configured K list on UICC

Alternative 3b can be used to implement all four use cases, except that it does not allow for *remote* choice of initial operator after the M2ME has been deployed. Since a UICC is used, there may be concerns with unauthorised UICC removal for some use cases. However this alternative provides for remote change of subscription, which means that the UICC can be physically attached to the M2ME so that it is very difficult or impossible to remove.

The requirement to have a UICC may also mean that M2MEs cannot be below a certain size, which may lead to devices/modules that are too big for variants of the use cases where very small embedded M2MEs are required. The use of the new Industrial Form Factor UICC may address this concern, though this may mean the UICC is then non-removable. According to the evaluation of 3b, UICC-swap may be required for cases where the OTA key-change procedure fails.

Implementations of alternative 3b would have to ensure that the number of different operators to which the UICC can be assigned during its lifetime was high enough to cover the operator change requirements required by some variants of the use cases.

## 8.3 Conclusions

The Scope of this TR is given in section 1 of this document, extracts of which are given below for convenience.

The aim of this TR is to study "*an investigation of candidate security solutions architectures that allow remote subscription management to take place in a secure manner*" and by implication to assess whether these are feasible or not.

Three basic candidate solutions (numbered 1 to 3) for remote provisioning and management of subscriptions in M2MEs have been developed and evaluated within this TR, with solution 3 having two variants (3a and 3b) giving 4 candidate solutions in all. See section 8.1 above for a summary of each of these solutions.

These solutions are evaluated against the criteria developed within this TR in section 7 of this report, and against the use cases in section 4.1 (from which the evaluation criteria were derived) in section 8.2.1.

Each candidate presents a different trade-off among many factors such as security, standardization impact, ease of deployment, and ability to meet the use cases.

Even if Alternative 1 is compatible with the intended M2M uses cases, it has the most complicated network architecture, and the greatest difference with existing subscription management methods, It gives rise to important security concerns. Integration of the MCIM within the M2ME creates concerns about the ability of an M2ME to adequately protect the sensitive data within an MCIM.

Alternative 2 is the solution already specified for ensuring all 3GPP UE network authentications and represents the solution currently in use to address the existing M2M business of MNOs. It has the least impact on subscription management methods and network infrastructure. Change of subscription without human intervention does not seem to be possible with this solution, but the existing M2M business of MNOs shows that the technical and logistical issues deriving from this aspect are not a major issue, at least from a MNO perspective.

Alternatives 3a and 3b lie between 1 and 2 in terms of the trade-offs within the three main headings. They use a UICC but the change of subscription is achieved without human intervention. This requires changes in the subscription management systems and/or the UICC; thereby raising concerns on security. Thus, the security level is lowered compared to the standard UICC solution corresponding to the Alternative 2.

There were different points of view in SA3 with respect to the relative importance of these trade-off factors, and no final recommendation on a particular solution or solutions is given is this TR:

- Alternatives 1 and 3b require new specification work before being widely used in 3GPP networks and they have important security concerns. It needs to be shown how the security and complexity issues can be solved in an economical and practical manner.

- Alternative 2 does not require any new specification work. It is already being used for M2M use cases and provides a satisfactory level of security.

- Alternative 3a does not require any specification work for interaction with M2MEs and only requires specification of mechanisms for inter-operator IMSI/K sharing. Though implementations of Alternative 3a are possible, there are many concerns about security issues and also issues of inter-operator trust. Discussion of this alternative in a forum such as the GSMA may help to address the issues of inter-operator trust presented by this alternative.

# Annex A (informative): Collection of views expressed by external bodies

## A.1 GSMA SCaG

GSMA MNOs provided their concerns and recommendations related to "SIM usage in M2M application" in LS from GSMA ScaG sent to TSG SA and TSG WGs SA1, SA3 and CT6; confer S3-081005. At the time of receiving the LS the TR was version 0.4.0.

The GSMA MNOs concerns and recommendations are the following ones (Extract of LS S3-081005):

- *GSMA MNOs, represented by ScaG, aim to consider not only technical topics, but also end-to-end business processes and requirements. Furthermore, one of the major concerns of MNOs is the potential weakening of the well-established and trusted SIM-based GSM/3G security architecture. Extended OTA (any kind and via any bearer of over the air data download to the USIM) capability to facilitate download of new subscriber keys and possibly authentication algorithms represents such a potential weakening of security.*

- *While until now, only the smartcard based SIM, which is well accepted by users and appropriate to fulfil the regulators' directives for the consumer market, is standardised, there is a demand by the M2M market for a new Form Factor, as currently discussed at ETSI SCP. According to the information available today, ScaG is confident the new form factor to be standardised by ETSI SCP will meet the M2M market demand without requiring subscription download.*

- *For MNOs, it is of utmost importance that any new security relevant functionality or process must maintain the current GSM/3G security level, not only with respect to the technology, but also with respect to the end-to-end business processes. For example, a potential need to expose subscriber authentication keys (Kis) and/or authentication algorithms to any 3rd party, would have severe consequences for the GSM/3G industry, e.g. not allowing MNOs to fulfil their obligations towards regulatory and other governmental authorities to guarantee secure authentication and billing.*

- *Any new security relevant functionality or process must not harm the overall GSM or/and 3G security concept, by e.g. requiring functionalities which are not compliant with the entire security architecture and design of GSM and 3G.*

## A.2 GSMA SG

GSMA MNOs provided their concerns related to "Remote USIM Management on M2M Equipment" in LS from GSMA SG sent to TSG WG SA3 in May 2009, confer S3-091069. The review of the TR was based on version 1.3.0.

The GSMA SG concerns are the following ones (Extract of LS S3-091069):

*The security of the 3GPP standards is based on the control and protection of the UICC. Operators purchase UICCs from specialist manufacturers and specify the necessary cost effective security requirements and procedures. 3GPP defined technology is dependent on the business relationship between the Operators and the UICC supplier, and change to this relationship has the potential to significantly change the risk model.*

*Although significant progress has been made by some manufacturers in recent years, the security of devices is such that they have been compromised in many ways in the past. It has therefore been very beneficial for user authentication credentials to be stored in a security element (UICC) that is separate from the mobile equipment.*

*The only proposal in the TR that was acceptable to GSMA SG representatives was the Alternative 2 where operator change was performed by physical replacement of the UICC in the device.*

*GSMA SG also questioned the requirement to have physical binding of the UICC to the M2M ME that prevented removal of the UICC as detailed in section 4.2. SG believes that a logical secure association between the UICC and the ME could be achieved so that the UICC could only be used in the M2M equipment.*

-

# Annex B (informative): Details and options for Alternative 1

## B.1 Delayed Activation

There may a considerable delay (perhaps weeks or even months) between provisioning (U)SIM functionality into the M2M equipment and the first use of any connectivity. In the legacy credentials case, it may be undesirable for the operator providing the initial connectivity service to have live subscriptions in his network without any activity over an extended period of time. Therefore, a service may be useful (but not mandatory) by which an M2M user can indicate to the Registration Operator (Initial Connectivity Function) that the M2M equipment is going to be switched on so that the subscription can be activated in the network. Such a service could be realized over an appropriately protected web portal.

## B.2 Detailed example for Network Interactions using decentralized Registration Operator and OMA DM

### B.2.1 Overview

Section B.2.2 describes the steps unique to the initial provisioning, i.e., the first change of operator. Section B.2.3 then describes the general steps performed at every change of operator. The first initial change of operator hence proceeds as follows. The steps in B.2.2 are performed such that the M2ME is preconfigured with all essential data needed, and such that the device can establish IP connectivity to the RO. The change of operator from the RO to the first SHO is then performed according to Section B.2.3.

The architecture in the example assumes that every SHO owns a DPF and a DRF in their own networks.

The architecture also assumes that the role of the PVA is performed by the TRE manufacturer.

NOTE: We use here the concept of TRE manufacturer for distinguishing between the general M2ME manufacturer responsibilities and the specific responsibilities for creating and personalizing the TRE. In practice the TRE manufacturer could be the manufacturer of the modem part of the M2ME.

The suggested procedures allow an abstraction at the SHO to be independent of the specifics of the TRE. The TRE specifics, e.g. Java or STIP or Native, can be handled by the OMA DM (DM is designed the take care of this and can handle different devices, brands, etc)

### B.2.2 Establishing Initial IP Connectivity

#### B.2.2.1 Manufacture pre-credential installation phase

During manufacture, a TRE is initialized with an asymmetric key pair $\{PrK_{TRE}, PuK_{TRE}\}$, additionally corresponding certificate signing request is created. In this architecture it is assumed that the TRE supplier assumes the role of the PVA, i.e., the TRE supplier certificate, denoted $Cert_{PVA}$, is trusted by all parties. The SHO has securely obtained the necessary PVA certificate ($Cert_{PVA}$). However, the means for the secure delivery is out of scope in the present study. Hence, the TRE Supplier creates the TRE certificates $Cert_{TRE}$, by signing the certificate requests with the private key corresponding to $Cert_{PVA,}$. The certificate is inserted into the TRE, together with the corresponding key pair. Additionally, the certificate of the RO, also called SHO[0] or current SHO, is installed as a trusted root certificate for authenticating the RO towards the TRE. The certificate is denoted $Cert_{SHO[0]}$.

NOTE 1: As the $Cert_{PVA}$ is.trusted by all parties, one could consider using $Cert_{PVA}$ for authenticating the RO. However, this is not plausible as the administrator of $Cert_{PVA}$ should not be signing certificates of operators. Moreover, using $Cert_{PVA}$ for this purpose would not be secure as then anyone getting his certificate signed by $Cert_{PVA}$ could play the role of RO towards the TRE.

NOTE 2: To simplify the manufacture procedure, alternatively, secure push can be used to authenticate the RO. In such implementations, the requirement to install the $Cert_{SHO[0]}$ in the TRE is removed. The use of secure push would be contractually agreed between the RO and the M2ME/TRE manufacturer to reduce the requirement on support of secure push for all M2MEs.

In the TRE, necessary algorithms for key derivation are installed, the TRE is also assumed to have an identity denoted by TRE_id. Hence, tuple {$PrK_{TRE}$, $Cert_{TRE,}$, $Cert_{SHO[0]}$, TRE_id} is available inside the TRE after manufacture time.

NOTE 3: $PuK_{TRE}$ is included within $Cert_{TRE.}$. TRE_id is globally unique. This can be achieved using the vendor name; vendor given number format.

NOTE 4: To improve the security it might be beneficial to create two asymmetric key pairs, replacing $PrK_{TRE}$ above, one used for signatures, and one used for encryption.

Depending on business agreements, either the TRE Supplier or the RO creates a set of unique network-access credentials for the TRE including network-access credentials {PCID, K}. The credentials are shared between the TRE manufacturer and the RO such that they can be inserted in the ROs HLR/AuC resp. HSS, and into the TRE by the TRE manufacturer.

NOTE 5: The current SHO (the RO at this stage), needs to be able to map a TRE_id to a subscription to enable operator change.

The M2ME is purchased and delivered to the M2M subscriber. On delivery, {TRE_id, $Cert_{TRE}$, SHO_id} is given to the M2ME Subscriber, where SHO_id denotes the identity of the current SHO, i.e., SHO[0], i.e., the identity of the RO.

### B.2.2.2 Initial Attach

It is recommended that the M2ME uses a PCID which has the same format as a currently used IMSI, so that the VNO does not have to be M2M-aware and can use the existing and known protocols and nodes. The “MCC” and “MNC” fields in the IMSI will indicate to the VNO/SHO which entity it should contact to obtain authentication vectors to authenticate the IMSI with.

NOTE 1: The shortage of IMSI numbers is a known issue for M2M communications where the number of M2M capable devices is expected to be considerable, and it is not only relevant for the present TR but also to M2M communications in general. Possible future enhancements could include, for instance, that PCIDs (IMSIs) no longer required by a M2ME could be re-allocated. Furthermore, a group of M2MEs could share the same PCID. We have to consider that the core network will not allow concurrent connectivity to M2MEs with same PCIDs. NOTE 2: Depending on the actual contractual agreements, the operator may just confirm the IMSI data used in the initial attach and only provide the missing IP connectivity parameter details. This would mean that the M2ME already has a viable MCIM to this operator’s network.

If no packet switched network parameters are available in the M2ME, then the M2ME can only get cellular connection when turned on and no IP connectivity. When the M2ME attaches to the RO, i.e., SHO[0], for the first time, the DRF is triggered to initiate an OMA DM Bootstrap, e.g., by using Automatic Device Detection (ADD) and e.g. via SMS. The bootstrap provides the M2ME with a Network Access Point Definition (NAPDEF) for the access network in question to enable IP connectivity (packet switched bearers) on the M2ME.

The M2ME can at this stage establish IP connectivity. However, the connectivity might be restricted by the policies of the current SHO, e.g. to only allow connectivity to provisioning services.

After the initial attach phase, the provisioning of the MCIM and change of selected home operator (from the RO to the first SHO) are according to Section B.2.3.

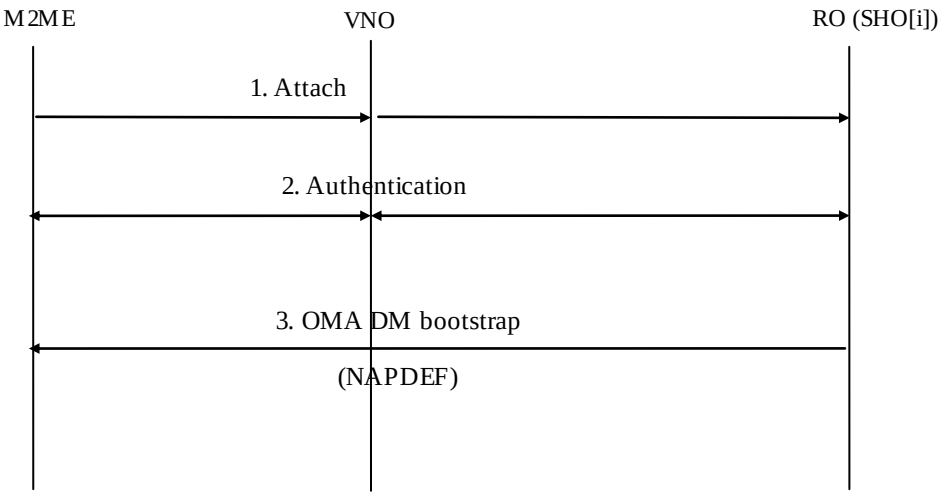


**Figure B.2.2.2-1: Initial attach**

## B.2.3 Change of Selected Home Operator

### B.2.3.1 Procedure

The general steps performed at each operator change are illustrated in Figure B.2.3.1-1. Description of the steps in the figure is described in clauses B.2.3.2 – B2.3.5.

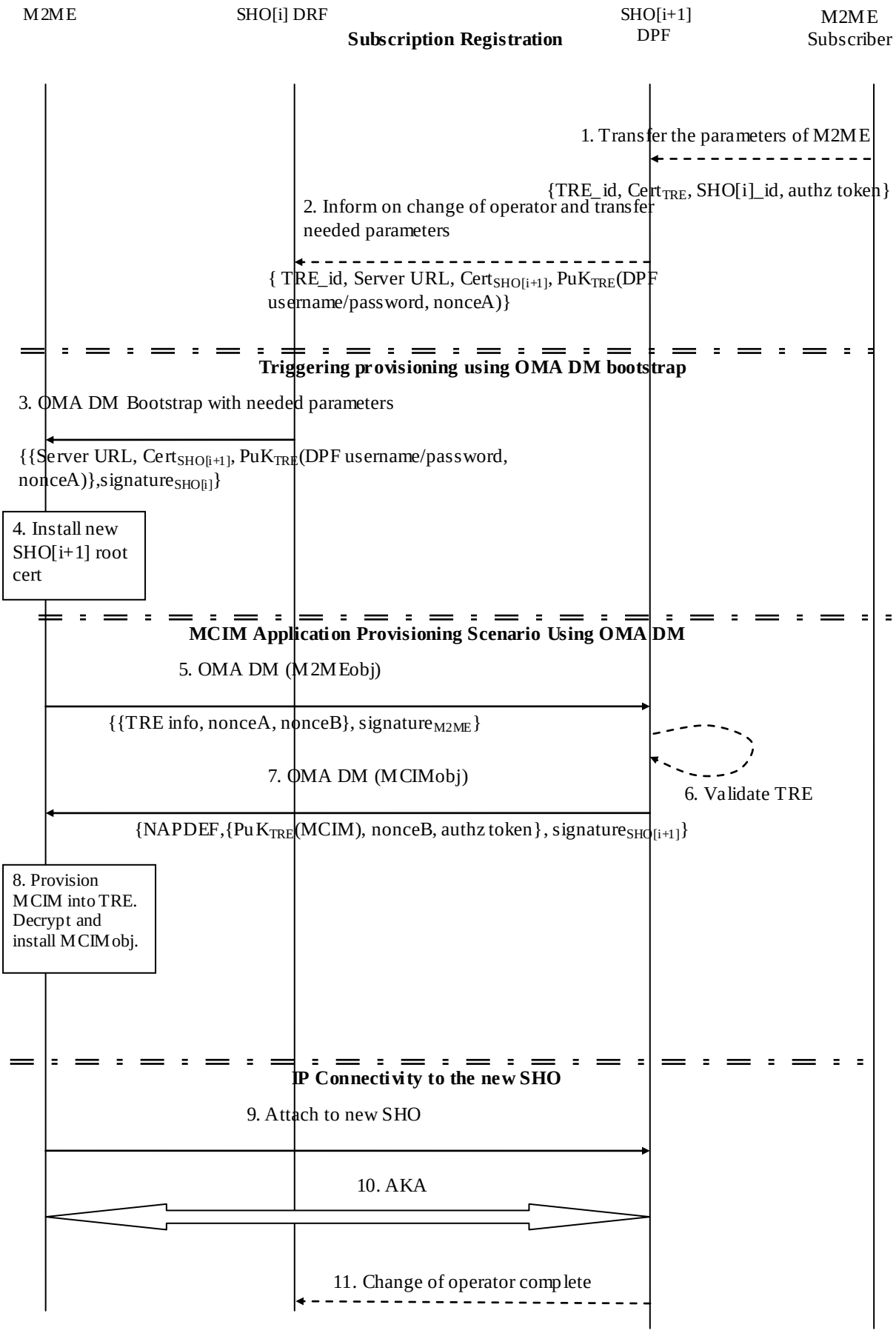


**Figure B.2.3.1-1: Change of selected home operator**

### B.2.3.2 Subscription Registration

Subscriber registration can be done in several different ways. In the context of this example we will assume that the M2ME is shipped to the end customer before the new SHO has been chosen. As stated in the previous section, the M2ME is shipped together with {TRE_id, $Cert_{TRE}$, SHO[i]_id}. Before registering the subscription the SHO[i] has to receive the {TRE_id, $Cert_{TRE}$, SHO[i]_id}. The data may also come from the manufacturer of the TRE, but the subscriber need to provide some data, which enables the SHO to obtain those data.

**Step 1**

The M2ME Subscriber registers for a subscription at the selected new SHO, denoted SHO[i+1], e.g., via a web interface. Information that needs to be provided to the new SHO is {TRE_id, $Cert_{TRE}$, SHO[i]_id, authorization token}. The SHO[i+1] stores the information obtained from the M2ME Subscriber. The authorization token is used to ensure that the MCIM provisioning is authorized. This authorization token might be a token signed with a private key of the M2ME/TRE.

The new SHO, i.e. SHO[i+1], generates MCIM credentials, which are stored in the HLR/AuC or in the HSS and are additionally protected using the TRE public key, i.e., $PuK_{TRE}$, see subsection B.2.3.6, and inserted into the DPF.

NOTE 1: The new SHO may wait to prepare the credentials for the M2ME until being contacted by the OMA DM backend system. However it seems more advantageous (e.g. when bulk provisioning is to be performed) to have the new SHO prepare the (wrapped) credentials as result of the registration of the devices and their respective platform credentials in advance at the new SHO. Both approaches are possible and the final decision can be left to the discretion of the new SHO.

**Step 2**

Based on the SHO_id, the new SHO, i.e., SHO[i+1], makes a registration at the SHO[i]. I.e. it i informs the current SHO, i.e., SHO[i], that it now has a subscription with the M2ME. The new SHO provides the current SHO with data to be included in the OMA DM bootstrap message to be sent from the DRF.

The data given from the new SHO to the current SHO is {TRE_id, Server URL, $Cert_{SHO[i+1]}$, $PuK_{TRE}$(username/password to the OMA DM (DPF) server, nonceA)}, where nonceA is used to prevent replay attacks. As this is sensitive data not to be exposed to the current SHO, it is encrypted using the public key of the M2ME, i.e., $PuK_{TRE}$. The protection format used is described in Subsection B2.3.6.

The current SHO maps the TRE_id to a subscription, and updates its registers in the DRF with information on how the M2ME should discover the new SHO.

### B.2.3.3 Triggering provisioning using OMA DM bootstrap

This section provides one example of how the current SHO can bootstrap information to the M2ME about how to find the provisioning server (DPF) of the new SHO.

NOTE 1: OMA DM provides a bootstrap mechanism based on connectionless OTA push. This mechanism can be used if no IP connectivity parameters are pre-configured in the M2M equipment. At least two configuration contexts can be identified: the context for provisioning the MCIM application, and the context for provisioning M2M applications.

**Step 3**

The OMA DM Account management object (DMAcc) (sent in Bootstrap message) defines the server URL of the DPF to which the M2ME (OMA DM client) will initiate the connection

The TRE will authenticate the DRF server using the trust root certificate of the current SHO, i.e. $Cert_{SHO[i]}$, which has been previously installed in the TRE. The DRF (OMA DM server) will sign the bootstrap message using XML signatures and $Cert_{SHO[i]}$ which can be verified by the TRE. Client authentication of the Bootstrap message is defined in OMA-TS-DM_Security-V1_2 [14] and OMA-TS-DM_Bootstrap-V1_2[13].

NOTE 3: As noted in Section B.2.2.1, the RO (SHO[0]), may be authenticated using secure push.

There is also a requirement for the M2ME (OMA DM client) to authenticate the DPF server during the MCIM provisioning activity. This is achieved by including the certificate of the new SHO, i.e. $Cert_{SHO[i+1]}$, in the bootstrap

message. The DRF server further signs the bootstrap message using the private key corresponding to the trusted server certificate, i.e. $Cert_{SHO[i]}$.

NOTE 4: This has been done before (MS) by the addition of a "CertificateStore" characteristic, but could also be conveyed in a more subtle way, e.g. by including the public key hash in the Server URL parameter, or by the addition of a VENDORCONFIG characteristic in the bootstrap message.

**Step 4**

Thus, the data sent in the bootstrap is {{Server URL, $Cert_{SHO[i+1]}$, $PuK_{TRE}$(username/password to the OMA DM (DPF) server, nonceA)},$signature_{SHO[i]}$}. When the TRE of the M2ME receives the bootstrap message, the TRE verifies that the signature of the current SHO is correct. The certificate of the new SHO, i.e., $Cert_{SHO[i+1]}$, is installed as a new trusted root certificate. The encrypted data is decrypted and saved for usage in the provisioning phase after checking the nonce for replay attacks.

### B.2.3.4 MCIM Application Provisioning Scenario Using OMA DM

The following steps outlines the provisioning steps in the context of OMA DM.

It is assumed that two OMA DM management objects have been defined; the M2MEobj and the MCIMobj. The first one is used to carry information about the M2ME and its TRE to the DPF (OMA DM Server), see Step 5, and the latter is used to transport the MCIM parameters (and possibly code) to the TRE of the M2ME, see Step 7.

NOTE 1: The standardization of OMA DM management objects is a relatively simple process and can be done in 3GPP (SA3) if so desired. OMA may then register the defined object to become a publicly registered OMA DM management object.

**Step 5**

When the M2ME has received and verified the DRF bootstrap message (see B.2.3.3), it prepares the M2MEobj with information about the TRE of the M2ME. The nonce, i.e. nonceA, received in the bootstrap message is included in the object. Additionally, the M2ME creates a second nonce, i.e. nonceB, which is included in the M2MEobj. Information about the TRE is also included and denoted TRE_info and contains information about which type of TRE that is used in the M2ME. Finally, the TRE signs the data in the M2MEobj with $PrK_{TRE}$. The data, {{TRE_info, nonceA, nonceB}, $signature_{M2ME}$}, is packaged in theM2MEobj and is sent to the DPF. The two nonces, nonceA and nonceB, are included to prevent replay attacks.

The DPF (OMA DM server) receives the OMA DM management object for M2ME (M2MEobj), verifies the signature and validates that the provisioning request relates to an ongoing M2M provisioning. This is done by verification that nonceA is the same as the nonce given to the SHO[i] in step 2.

**Step 6**

The OMA DM back-end system contacts the PVA to verify that the TRE platform and TRE certificates can be trusted.

NOTE 2: It is assumed that SHO[i+1] trusts the root certificate of the TRE manufacturer. The validation can then be performed locally by the new SHO, i.e., SHO[i+1], by verification of the signature I.e., there is no need for SHO[i+1] to contact the PVA for the validation.

**Step 7**

The DPF retrieves the wrapped platform credential for the M2ME, denoted $PuK_{TRE}$(MCIM), and prepares the MCIMobj for provisioning by the OMA DM Server. Included in the object is the following data {{$PuK_{TRE}$(MCIM), nonceB, authorization token}, $signature_{SHO[i+1]}$}, where nonceB is the nonce received in the M2MEobj from the M2ME. The packet switched network parameters to allow IP connectivity in the SHO network (NAPDEF) are also included. The MCIMobj is sent to the M2ME.

**Step 8**

The M2ME receives the MCIMobj, the OMA DM client in the M2ME locally provisions the MCIM blob to the TRE The TRE can verify that the MCIM blob comes from the correct SHO by verifying the signature, and by checking the registration nonce, i.e. nonceB, one achieves protection against replay attacks.

The encrypted blob with the parameters is decrypted inside the TRE and the parameters are extracted and securely installed.

NOTE 3: To limit the security requirements on the OMA DM server the OMA DM server only receives an encrypted binary blob. The encrypted binary blob contains the MCIM application information including the IMSI, the key Ki, an algorithm identifier and possible algorithm constants or algorithm code packaged for the device that can only be opened using the platform key that the M2ME holds in its TRE (e.g. a value of OP_C if MILENAGE is the selected algorithm). OMA DM includes support for XML Encryption and XML Signatures and hence these can be straightforwardly applied. The binary blob is a PKCS-formatted envelope for the device, externally formatted to be further sent to theTRE for decryption, validation and deployment.

NOTE 4: When the new MCIM is taken into use, in extreme cases, the new SHO, or its roaming partners, might not be able to provide coverage in the location of the M2ME. If the device cannot attach to any network within a predetermined time period, after taking a new MCIM into use, it should revert back to the previously used MCIM/network parameters. Therefore it might be beneficial if the current (old) SHO stores the credentials, e.g. current active MCIM and $Cert_{TRE}$, for some time to resolve error scenarios, any such agreements should be done contractually. The credentials could be deleted when the old SHO can be sure that the M2ME has successfully changed to the new SHO. If such scenarios are covered by contractual agreements between SHO[i] and SHO[i+1], the M2ME can be prevented from becoming unreachable.

### B.2.3.5 IP Connectivity

**Step 9 and step 10**

The M2ME connects to the new SHO using the new provisioned MCIM and establish IP connectivity by running the normal AKA procedure and using the IP connectivity parameters received in step 7.

**Step 11**

The new SHO (SHO[i+1]) informs the old SHO (SHO[i1) of successful completion of operator change. At this point old SHO can delete/deactivate the credentials related to the M2ME.

### B.2.3.6 Form of data protection

The data that needs to be protected and then provisioned should have the form:

*data = tag | payload_length | payload | version | padding_data*

- The *tag* is to indicate what kind of information is contained in the payload e.g. algorithm, update, or MCIM.

- The padding_data is to make up the data length to a suitable length for encryption.

For the protection of the provisioned data a pair of symmetric secret keys is used, denoted as the integrity key PIK and the confidentiality key PCK. Two distinct keys should be used for performance reasons. Those keys are protected with the public key $PuK_{TRE}$. The protection should be straightforward and use well-known algorithms e.g. AES-CBC for encryption and HMAC-SHA 1 as the integrity protection algorithm. The data should be protected as follows:

*Protected_data = (ENC_PCK (data) | MAC_PIK (ENC_PCK(data))*. E.g. the MCIM Object described in figure B.2.3.1-1 step 7 has the following content:

$PuK_{TRE}$ *(PIK|PCK)* | *Protected_data*, which may be also used in a shortened form $PuK_{TRE}$ *(Protected data)*.

## B.2.4 Example: Algorithm and MCIM data details

The *data* in B.2.3.6 should contain the equivalent to the following information as specified by [11] TS 31.101:

EFICCID; EFDIR, EFPL and EFARR

The *data* in B.2.3.6 should contain the following information as specified by [9] TS 31.102 chapter 4.2 for the USIM case:

- IMSI

- Ciphering and Integrity Keys
- Ciphering and Integrity Keys for Packet Switched Domain
- Higher Priority PLMN search period
- USIM Service Table
- Access Control Class
- Forbidden PLMNs
- Location Information
- Administrative Data

NOTE 1: The administrative data gives also an indication to the machine whether some machine features should be enabled during normal operation, for details see [9] chapter 4.2.

- Emergency Call Codes
- Packet Switched location information
- Key for hidden phone book entries
- Initialisation values for Hyperframe number
- Maximum value of START
- Access Rule Reference
- Network Parameters
- Operator PLMN List

Other information specified by [9] chapter 4.2 may be part of the *data*.

The *data* in B.2.3.6 should contain the following information as specified by [10] TS 31.103 chapter 4.2 for the ISIM case:

- IMS private user id
- Home Network Domain
- IMS Public user identity
- Administrative data
- Access Rule Reference

Further information as specified in chapter 4.2 in [10] may be part of the *data*, depending on the actual supported usage scenarios defined by the SHO e.g. P-CSCF Address for local breakout support, ISIM Service Table for support of optional services or GBA support.

The *data* may also contain further additional information not specified here.

For algorithm usage appropriate authentication and key agreement algorithm with AES CBC should be used.

## B.2.5 Example of potential OMA DM Management Object

The following section describes as example of a potential OMA DM management object that could be used to remotely manage subscription on a M2ME. In the description, the following notation is used

| Character | Meaning |
|---|---|
| + | One of many occurrences |
| * | Zero or more occurrences |
| ? | Zero or one occurence |

Nodes under the TRE node are used for sending validation data to the OMA DM provisioning server. Nodes under the Prov node, are used to provision the MCIM in the M2ME. The following nodes and leaf objects are possible under the MCIM management node:

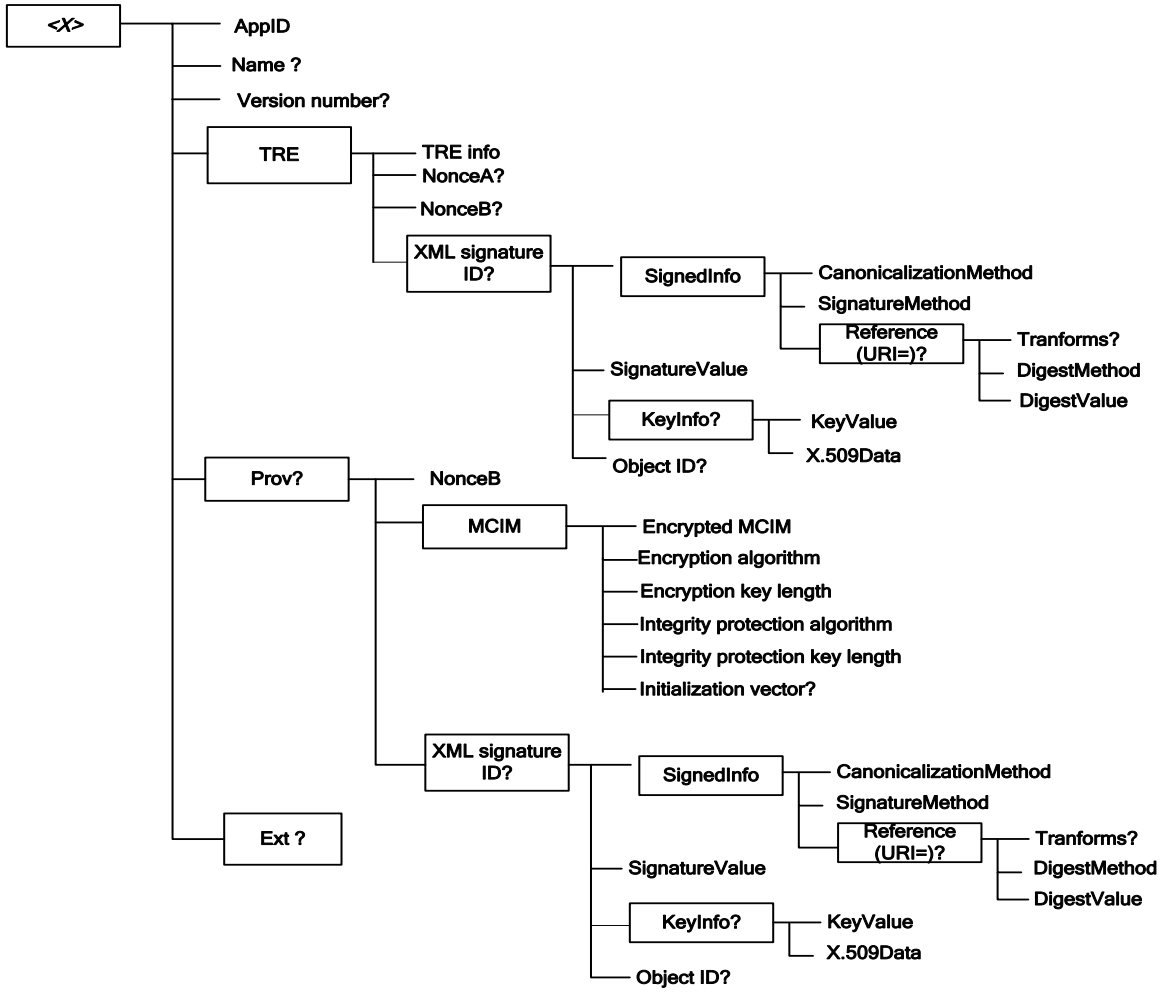


**Figure B.2.3.8-1: The Communication Continuity Object**

Management Object parameters:

-**Node: /<X>:** The interior node is mandatory if the UE supports update of MCIM parameters via OMA DM.

-/<X>/**AppID:** The AppID identifies the type of the application service available at the described application service access point. The value is globally unique.

-/<X>/**Name:** The Name leaf is a name for the MCIM parameters.

-/<X>/**TRE**/**TREinfo:** contains information about the TRE.

-/<X>/**TRE/NonceA:** contains nonce used

-/<X>/**TRE/NonceB:**

-/<X>/**TRE/XML signature ID:** The node identifies an XML signature used to authenticate/ integrity protect the MCIM.

-/<X>/ **TRE /XML signature ID/SignedInfo:** contains or references the signed data and specifies what algorithms are used.

-/<X>/ **TRE /XML signature ID/CanonicalizationMethod:** used by the `SignatureValue` element and are included in `SignedInfo` to protect them from tampering.

-/<X>/ **TRE /XML signature ID/SignatureMethod:** used by the `SignatureValue` element and are included in `SignedInfo` to protect them from tampering.

-/<X>/ **Prov/XML signature ID/Reference :** One or more `Reference` elements specify the resource being signed by URI reference

-/<X>/ **Prov/XML signature ID/Reference/Transforms:** specifies any transforms to be applied to the resource prior to signing.

-/<X>/ **Prov/XML signature ID/Reference/DigestMethod :** specifies the hash algorithm before applying the hash

-/<X>/ **Prov/XML signature ID/Reference/DigestValue :** contains the result of applying the hash algorithm to the transformed resource(s).

-/<X>/ **Prov/XML signature ID/SignatureValue:** contains the Base64 encoded signature result - the signature generated with the parameters specified in the `SignatureMethod` element - of the `SignedInfo` element after applying the algorithm specified by the `CanonicalizationMethod`.

-/<X>/ **Prov/XML signature ID/KeyInfo:** optionally allows the signer to provide recipients with the key that validates the signature, usually in the form of one or more X.509 digital certificates. The relying party must identify the key from context if `KeyInfo` is not present.

-/<X>/ **Prov/XML signature ID/KeyInfo/KeyValue:** identifies the key used for the signature, if not included, the relying party must identify the key from context.

-/<X>/ **Prov/XML signature ID/X.509Data:** one or more X.509 digital certificates used to tie key used for the signature to a identity.

-/<X>/ **Prov/XML signature ID/Object ID:** optionally contains the signed data if this is an *enveloping signature*.

-/<X>/**Prov/MCIM/Encryption algorithm:** The Encryption algorithm leaf contains the name of the symmetric encryption algorithms used to encrypt the MCIM, this encapsulates mode of operation etc.

-/<X>/ **Prov/MCIM /Encryption key length:** The Encryption key length contains the symmetric key length used to encrypt the MCIM.

-/<X>/ **Prov/MCIM /Integrity protection algorithm:** The Integrity protection algorithm leaf is contains the name of the algorithm used for the integrity protection of the MCIM.

-/<X>/ **Prov/MCIM /Integrity protection key length:** The Integrity protection key length leaf contains the key length used for the protection of the MCIM.

-/<X>/ **Prov/MCIM /Initialization vector:** The Initialization vector leaf contains any potentially used IV used to protect the MCIM.

-/<X>/ **Prov/XML signature ID:** The data under this node has the same structure as **-/<X>/TRE/XML signature ID**, and is hence not described further

**/<*X*>/Ext/:** The Ext is an interior node for where the vendor specific information about the MCIM MO is being placed (vendor meaning application vendor, device vendor etc.). Usually the vendor extension is identified by vendor specific name under the ext node. The tree structure under the vendor identified is not defined and can therefore include one or more un-standardized sub-trees.

## B.2.6 Example of potential ASN.1 encoded MCIM

This section shows a potential ASN.1 definition used to transport MCIM parameters and potential software to the TRE. In the example the following parameters are used:

- the subscriber key (denoted akakey);
- the IMSI;
- the MCIM service table (denoted mst), the functionality corresponds to the USIM service table;

the forbidden PLMN list (denoted fplmn);

- the access control class (denoted acc);
- administrative data, e.g., information concerning the mode of operation according to the type of USIM (denoted ad);
- the maximum value of $START_{CS}$ or $START_{PS}$. This value is used to control the lifetime of the keys (denoted thresh).
- the de-personalization control keys associated with the OTA de-personalization cycle (denoted dck)
- the co-operative network list used for the multiple network personalization services (denoted cnl)

Additionally, the proposed definition allows an optional inclusion of software, represented by the element MCIMSWCODE, enabling the possibility to download and update algorithms etc. in the TRE.,Below is the definition called the MCIMProtocol is illustrated:

```
MCIMProtocol DEFINITIONS
  AUTOMATIC TAGS ::=
BEGIN

  MCIMBLOB ::= SEQUENCE {
   version   MCIMVersion,
   effields  SEQUENCE OF EFDATA,
   code    MCIMSWCODE OPTIONAL
   }

  MCIMVersion ::= INTEGER { v1(0) }

  EFIDS ::= INTEGER {akakey(1),   -- akakey does not exist as an EF in any 3GPP
specifications
              imsi(28423),  -- EF='6F07'H=28423
              mst(28472),   -- EF='6F38'H=28472
       fplmn(28539), -- EF='6F7B'H=28539
       acc(28536),   -- EF='6F78'H=28536
       ad(28589),  -- EF='6FAD'H=28589
       thresh(28508), -- EF='6F5C'H=28508
       dck(28460),   -- EF='6F2C'H=28460
       cnl(28466)} -- EF='6F32'H=28466


  EFDATA ::= SEQUENCE {
   efid   EFIDS,
   efbytes   OCTET STRING
   }
   -- efbytes are the big endian representation of the AKA key
   -- otherwise the bytes from the EF fields in 3GPP TS 31.102 V9.0.0


  MCIMSWCODE ::= SEQUENCE {
   swcodeLength   INTEGER,
     swcodeBinary   OCTET STRING
   }

END
```

## B.3 Trust Model

A trust model is presented so that it is clear what reliance the roles have on each other. The trust model takes the form of statements about the tasks that each role is expected and trusted to perform. Where this trust and expectation of one role is held by particular other roles, this is mentioned. Standard trust relations that already exist within mobile networks are not described in detail. Expectations that are part of most commercial arrangements (e.g. that bills will be paid, contracts complied with) are also not mentioned. In order to avoid duplication, expectations *upon* roles are given (e.g. what A is trusted to do by B) but not the expectations upon others that each roles holds (i.e. the list of roles trusted by the SHO are not given).

The roles that are discussed in this trust model are:

- M2ME Subscriber
- M2ME Supplier (M2MES)
- Platform Validation Authority (PVA)
- Registration Operator (RO)
- 3GPP Visited Network Operator (VNO)
- 3GPP Selected Home Operator (SHO)

Additionally, technical functions that are discussed include:

- Initial Connectivity Function
- Discovery and Registration Function (DRF)
- Download and Provisioning Function (DPF)

The roles/technical functions and the trust that is placed on them by other roles/technical functions are as follows.

**Role: M2M Equipment Subscriber**

The M2ME subscriber is trusted to be in legitimate possession of any credentials that the M2ME subscriber is required to use. A possible credential here is a password. Other schemes are also possible, such as certificates.

**Role: M2M Equipment Supplier (M2MES)**

The M2MES which manufactures the M2M equipments that host the TRE is trusted by the RO (including its DPF function) and the SHO to

- Manufacture equipment that meets relevant security requirements on MCIM hosting in the TRE
- Generate and provision PCIDs in accordance with industry guidelines
- Generate and provision other initial connectivity credentials (e.g. algorithm, key K) in accordance with standards
- Securely transmit initial connectivity credentials and PCID to chosen RO
- Generate device credentials in line with industry guidelines/standards
- Supply correct information to the PVA to enable it to verify the identity and compliance of the M2ME.

**Role: Registration Operator (RO)**

The RO is trusted by the M2ME subscriber (and SHO, where applicable) with respect to particular M2ME to carry out the Technical Functions of DRF and DPF, as described below.

**Technical Function: Initial Connectivity Function**

The ICF of an RO is trusted by the M2MES and VNO to:

- Securely receive and store initial connectivity credentials and PCIDs from M2MESs that have chosen the RO

- Securely generate (if not received from M2MES) authentication vectors for PCIDs registered with the RO
- Securely store and manage authentication vectors for PCIDs registered with the RO
- Securely transmit authentication vectors for specific PCIDs to VNO on request from VNO
- Securely maintain keys (K) and parameters

**Technical Function: Discovery and Registration Function (DRF)**

The DRF of a RO is trusted by the M2ME subscriber, VNO, and SHO to

- Correctly discover the SHO and route the M2ME to the SHO

**Technical Function: Downloading and Provisioning Function (DPF)**

The DPF of an RO is trusted by the M2ME User/Subscriber to

- Securely generate USIM keys and parameters, if instructed to do so by RO
- Securely store and manage generated keys, if instructed to do so by RO
- Carry out specified activities (e.g. using the PVA to authenticate the M2ME) prior to MCIM download
- Securely receive USIM keys and parameters from the SHO, or alternatively to generate same and transmit them to the SHO for operational use.
- Securely download and provision the USIM keys (K) and parameters to the M2ME.

**Role: Visited Network Operator (VNO)**

The VNO is trusted by the M2ME User/Subscriber, Equipment Supplier, RO and SHO, following the standard trust model for 3GPP network operators.

**Role: Selected Home Operator (SHO)**

The SHO is trusted by the M2ME User/Subscriber to accept requests to register the User's M2ME if obliged to by contract with the User/Subscriber.

**Role: Platform Validation Authority (PVA)**

The PVA is trusted by the SHO and by the RO or its DPF to

- Correctly authenticate the identity and compliance status of M2ME and report status back to RO (or DPF of the RO).

# Annex C (informative): Change history

| Change history | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** |
| 2008-09 | SA#41 | SP-090480 | -- | -- | Presentation to SA for information | --- | 1.0.0 |
| 2009-12 | SA#46 | SP-090829 | -- | -- | Presentation to SA for Approval | 1.0.0 | 2.0.0 |
| 2009-12 | SA#46 | SP-090901 | -- | -- | Removal of contentious text is 8.2.1.1 and 8.2.1.2 | 2.0.0 | 2.1.0 |
| 2009-12 | SA#46 | -- | -- | -- | Publication of SA-approved version | 2.1.0 | 9.0.0 |
| 2010-04 | SA#47 | SP-100095 | 004 | - | Correct clause number error in section 5.3.2.1 | 9.0.0 | 9.1.0 |
| 2010-04 | SA#47 | SP-100095 | 005 | - | Change the names “M2M operator” and “M2ME operator” in Alternative 3a and Alternative 3b | 9.0.0 | 9.1.0 |
| 2010-04 | SA#47 | SP-100223 | 008 | 1 | some corrections | 9.0.0 | 9.1.0 |
| 2010-04 | SA#47 | SP-100095 | 011 | - | Adding definition of M2ME to TR | 9.0.0 | 9.1.0 |
| 2010-04 | SA#47 | SP-100095 | 013 | - | Removal of editor’s note on Alternative 2 and correction of figure text | 9.0.0 | 9.1.0 |
| 2010-04 | SA#47 | SP-100095 | 014 | - | Removal of “TBD” in Alt 1 evaluation | 9.0.0 | 9.1.0 |
| 2010-04 | SA#47 | SP-100095 | 015 | - | Removal of editor’s note in Annex A | 9.0.0 | 9.1.0 |
| 2010-04 | SA#47 | SP-100095 | 017 | 1 | Adding definitions of various identities | 9.0.0 | 9.1.0 |
| 2010-04 | SA#47 | SP-100095 | 003 | 1 | Use Cases corrections and Evaluation Criteria clean-up | 9.0.0 | 9.1.0 |
| 2010-04 | SA#47 | SP-100223 | 018 | 1 | MCIM lifecycle state transitions | 9.0.0 | 9.1.0 |
| 2010-04 | SA#47 | SP-100095 | 009 | 1 | Incorrect abbreviation | 9.0.0 | 9.1.0 |
| 2010-04 | SA#47 | SP-100095 | 012 | 1 | Clean up of Alternative 1 | 9.0.0 | 9.1.0 |
| 2010-04 | SA#47 | SP-100095 | 016 | 1 | Removal of editor’s note on handling of validation information | 9.0.0 | 9.1.0 |