

## Overview

# TR33.812: Proposal for TRE on a UICC

(Candidate Solution Alternative 1b)

---

**SA3#55 May 11-15 Shanghai, China**

**Discussion doc S3-090795**



# Agenda

- Background / motivation
- A description of the “TRE in the UICC” concept (1b)
  - Key Features
  - Comparison with Alternative 1a (“TRE integrated in the M2ME”)
- Threat analysis
  - Threats
  - Security Requirements
  - Comparison with Alternative 1a



# Background

- The TR 33.812
  - Discusses the scenario where the MCIM application resides in M2M equipment, but it does NOT limit how the MCIM application should reside in the M2M equipment
  - Definitions:
    - **TRE:** "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."
- The UICC's position
  - As a 'preferred environment for secure applications' by a large number of operators
  - And considering the investment in the infrastructure that has already been made
  - UICC and related specifications could need some further development for M2M TRE
- **Recall: Main focus of TRE and MCIM definitions in the TR**
  - Provisioning and Management of subscription credentials



## General TRE functions (from TR Alt 1a)

- Logical separate entity, with HW support for separation
- Defined interfaces to the outside world
- Include a Root of Trust (RoT) for secure storage and secure execution environment (SEE) for one or more MCIMs
- Provide protection against physical and logical attacks
- Support validation of M2ME towards PVA
- Enforce security of remote provisioning of MCIMs
- Remote discovery of MCIM lifecycle status



## Candidate Solutions

- 1) TRE based solutions
  - 1a) TRE based, with remote subscription provisioning and change
  - **1b) Future UICC-based solution ('TRE on UICC')\***
- 2) UICC based solution with no remote subscription provisioning and change
- 3) UICC based solution with remote subscription change
  - 3a) Ki transfer between operators
  - 3b) Pre-configured Ki list on UICC

\*presented in more detail in the following slides



## Alternative 1b – TRE on UICC

- What the TR (33.812 v1.3.0) already says referring to section 5.1.2.2:
  - “At the time of writing, UICC specifications are not fully capable of supporting the required functionality of a TRE, as described in clause 5.1.”
  - “However, if future enhancements are made to UICC specifications, it is possible that a TRE could be implemented on a UICC.”

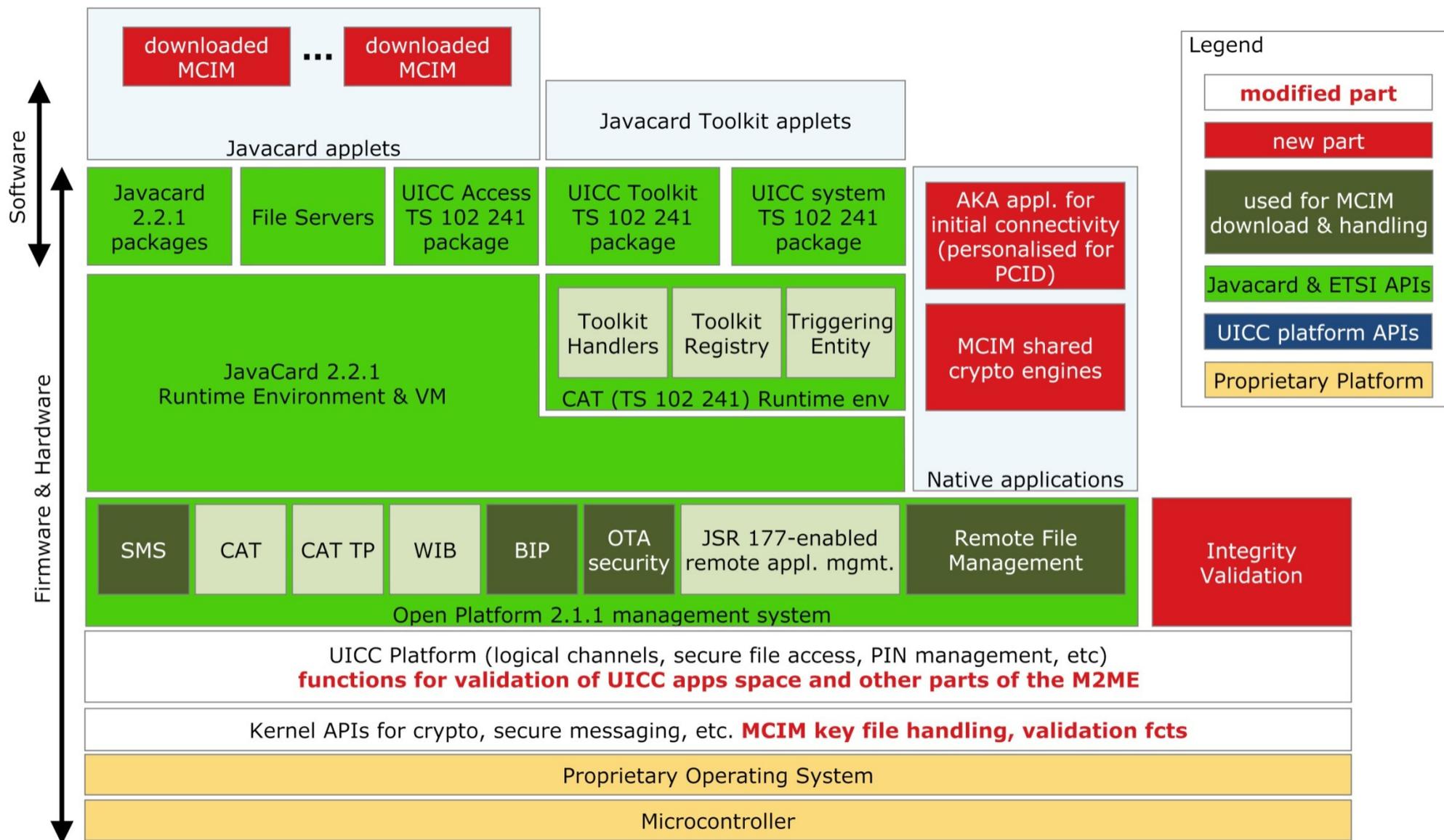


# TRE on UICC: Key Features

- Cryptographic Functions
  - Protected storage
  - Pre-provisioned private key (for TrE\_ID)
  - Generation of session keys using the private key
  - **New: validation of MCIM-related updateable code in TrE**
- Connectivity Functions
  - Network attach to VNO using PCID
  - Establish IP connectivity using RO
  - **New: support for interactions with DRF (discovery, registration) and DPF (end-end secure download).**
- MCIM Support
  - Initial provisioning of MCIM (**new: download encrypted MCIM credentials, data, app from DPF. Decrypt MCIM credentials (e.g. keysets), data, exec code. Extract and install them.**)
  - Use of MCIM to perform AKA or cert-based authentication towards SHO (**new: under supervision of SHO: deprecate/delete old MCIMs, replace/re-provision new MCIMs, remote discovery of MCIM lifecycle states**)
  - Support for protocols (e.g. OMA-DM, Liberty Alliance, Global Platform...) for discovery, registration and/or download/provisioning/replacement and/or management of MCIMs. **New: 3GPP/ETSI spec work to standardize some of these.**



# TRE-on-UICC Architecture (example)





## Comparison to Alternative 1a

- Can make use of many UICC features and much existing infrastructure
- Global Platform already defines logically separate domains on a smart card. These might need to be enhanced for TRE to be implemented as a special domain with required flexibility for ownership and for sub-domains
- Provides some flexibility for subscription management similar to 1a
- Some functionality required outside UICC, but protected by UICC (transport of via M2ME from network to UICC)
- ETSI/3GPP interfaces between UICC and ME need to be studied to see if they are adequately secure and, if necessary, further developed



## Selected Security Threats (section 6.1.2.3)

### Threat #5

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 - 3

Risk: 4 to 6 (major)

### Threat #11

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

Risk: 9 (critical)

### Threat #3

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: 9 (critical)



## Threat #5 – Replacement / Simulation of TRE

### Alternative 1a

Threat can be addressed by:

- TRE needs to have a unique embedded identity
- TRE must be able to authenticate this identity
- Validation of the TRE identity must be possible
- TRE identity must be securely stored in the M2ME

### Alternative 1b

Threat can be addressed by:

- UICC is known to be highly resistant to simulation and tampering
- UICC needs to be protected against physical removal or replacement (it is not currently known how this can be done in a standardized way, even using MFF UICC)

Keypoint: Alternative 1b may benefit from the protection provided by the UICC's physical design but how to make it un-removable is a problem



## Threat #11 – Malfunction of TRE Causing Connectivity Loss

### Alternative 1a

Threat can be addressed by:

- TRE must provide functions to be reset to factory settings
- Authorization for this process is necessary

### Alternative 1b

Threat can be addressed by:

- UICC provides proven stable secure environment for execution of services
- Some functions of the TRE could be remotely updated within the UICC using 23.048, RFM/RAM, Java, Global Platform. Method can be complex and limitations likely to apply

Keypoint: In 1b the remote secure reset is protected by the UICC O/S, but this may introduce limitations and may require further specification work



## Threat #3 – Use of Malicious Software in M2ME

### Alternative 1a

- TRE securely stores and executes AKA functions
- TRE protects and assures security of MCIM provisioning and storage process.
- TRE supports PVA in the validation of the authenticity and integrity of the M2ME.

### Alternative 1b

- Critical SW will run protected in the UICC
- Secure MCIM download, storage, execution and management
- But relatively weak computing power and limited storage may bring problems
- Compromise of channels to UICC could be undetected by UICC, leading to an undetected compromise of the M2ME
- **New for UICC: the UICC should run startup validation of its own updateable code which is involved with MCIM functionality.**

**Keypoint:** Alternative 1b may provide better physical protection against physical attempts to tamper with the S/W. However, it may be vulnerable to attacks on the interface between the M2ME to the UICC since the UICC by itself cannot control the security of the interface. The required validation is new functionality.



## Some More Limitations of Solution 1b

- These issues apply to all UICC-based solutions
- There is no standardized non-removable format of UICC. Even MFF UICC is said by SCP to be removable (e.g. by de-soldering or connectorizing).
- “Burying” the UICC deep within the M2ME (to make it non-removable) could place adverse constraints on M2ME design, production-line procedures and in the field maintenance.
- Real estate required for UICC (including package, power supply, clock, etc) compared to embedded functions.



## Conclusion

- Alternative 1b is for a TRE on (MFF) UICC
  - Aims to make use of established UICC infrastructure
  - Key features can be derived from requirements for TRE (Alt.1a)
  - Needs some improvements to current UICC specifications (e.g. GP, SCP) and will require some UICC O/S changes.
- May mitigate some security threats better than Alternative 1a
- Removability and size will be issues to contend with
- Might not provide the same flexibility as Alt. 1a
- Alt. 1a provides better integrity protection (see threat #3)
- Is SCP/3GPP secure interface between UICC and ME adequate?
- Optimum download protocol to UICC via M2ME is FFS