|  |
| --- |
| **CHANGE REQUEST** |
| **102 725** | **Version**  | **0.5.0** | **CR** | **CRNum**  | **rev**  | 1 |
|  |
| ***CR Title:*** | Corrections related to the Secure Environment definitions |
|  |
| ***Source:*** | Motorola Mobility  |
|  |
| ***Work Item Ref:*** | RTS/M2M-00010ed211 | ***Date:*** | 06/26/2012 |
|  |
| ***Category:*** | F | ***Release:*** | 2 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(corresponds to a correction in an earlier release)****B*** *(addition of feature)****C*** *(functional modification of feature)****D*** *(editorial modification)* |
|  |
| ***Reason for change:*** | Correction related to Secure Environment is needed:* DeviceSecure Environment and M2M Node Secured Environment Domains are not adequately distinguished in the definitions and that leads to inaccuracies in 102 690..
* Secure Environment for M2M Application is missing
 |
|  |
| ***Summary of change:*** | Corrections related to the definition of M2M Node and Device/Gateway and their secure environments.  |
|  |
| ***Clauses affected:*** | 4 |
|  |
| ***Other deliverables*** ***affected:*** |  |
|  |
| ***Other comments:*** |  |

**Device Secure Environment (DSE):** An M2M Device relies on a resident Device Secure Environment that is capable of hosting the Secured Environment Domain(s) pertaining to any M2M Node that is hosted at the M2M Device.

A Device Secure Environment can be implemented as an Independent Security Element (e.g. a UICC) or as an integrated function in an M2M Device or M2M Gateway.

When more than one M2M Node is hosted on a single M2M Device, the Device Secure Environment needs to meet the security robustness requirements placed on the Secure Environment for each individual M2M Node. The Device Secure Environment needs to also ensure the cryptographic separation of the Secure Environment of different M2M Nodes, as required by the owners of the M2M Nodes. It is possible that an M2M Device or an M2M Gateway implements more than one Device Secure Environment, especially if security robustness requirements for different M2M Nodes are vastly different, or call for different implementations (e.g. one M2M Node implemented within UICC, while another is on another type of Secure Environment)

**Gateway Secure Environment (GSE):** When agreement reached for DSE, Repeat the definition of DSE for gateway.

**M2M Device**: a device that runs application(s) using M2M capabilities and network domain functions. A M2M device is made at least of one M2M Device Application and one M2M Communication Module. A M2M Device may contain one or more M2M Communication Module(s) and one or more M2M Device Application(s). An M2M Device relies on a resident Device Secure Environment (DSE) that hosts the Secure Environment(s) pertaining to one or more M2M Nodes hosted at the M2M Device.

**M2M Gateway**: equipments using M2M Capabilities to ensure M2M Devices interworking and interconnected to the Network and Application Domain. The M2M Gateway may also runs M2M applications. M2M Gateway functionality can be colocated with M2M Device(s). An M2M Gateway relies on a resident Gateway Secure Environment (GSE) that hosts the Secure Environment(s) pertaining to one or more M2M Nodes hosted at the M2M Gateway.

**M2M Network Device**: Madjid: the corresponding entity within the network is missing. We also need an M2M Network Device Secure Environment in parallel to DSE and GSE.

**M2M Node**: is a logical representation of the M2M component in the M2M Device, M2M Gateway or the M2M Core. Such components include one SCL, and optionally a M2M Service Bootstrap function and a M2M Service Connection function. An M2M Node is controlled and managed by the M2M service provider and its policies.

**M2M Node Secure Environment (NSE):** A Secure environment, within an M2M Device Secure Environment or M2M Gateway Secure Environment, or the M2M Network element dedicated to an M2M Node for the purpose of to performing M2M Node’s Sensitive Functions at the required level of robustness established for that M2M Node by its owner (M2M Service Provider). Sensitive functions pertaining to the M2M Node include but are not limited to the provisioning, derivation, storage and management of cryptographic keys which are used at the M2M service layer (in particular by local SCL). M2M applications interacting with the M2M Node are not necessarily secured within the domains of the M2M Node Secure Environment.

While the M2M Secure Environment must meet the security robustness requirements of its corresponding M2M Node, the details of the implementation of the environment are typically not standardized (e.g. hardware, versus software, etc).

Due to potentially high degree of variation between required security robustness levels for different M2M Nodes or different M2M services, it is possible for an M2M Device or M2M Gateway to implement multiple and different types of Secure Environments to host the M2M Node Secure Environment,

**Application Secure Environment**: The secure environment that protects the operation of an M2M application within the hosting M2M Device, M2M gateway or M2M Network device.

**Sensitive Data:** data which require protection from unauthorised disclosure or modification in accordance to the level of security robustness required

.

**Trusted Environment:** An instantiation of an M2M Device or M2M gateway Secure Environment (DSE or GSE) that is implemented as an integrated function (as opposed to Independent Security Element??). **TrE is considered to have cryptographically secure boundaries and interfaces (similar to a cryptographic module) but may or may not have a hardware instantiaion, i.e. may be** a logical entity within an M2M Device or M2M Gateway. An M2M Node Secure Environment (NSE) can be implemented on a TrE to performs Sensitive Functions, specifically for the purpose of Integrity Validation.

A Trusted Environment (TrE) requires a root of trust which is implemented as an integrated function in an M2M Device or M2M Gateway, so as to initiate the chain of trust for computation of software integrity values. The verification part of software integrity validation (IVal) is performed in a Secured Environment which can either be integrated in the Trusted Environment or securely connected to it.

The security properties of the TrE are provided by certain functions which are secure, for instance protected by physically non-removable secure hardware. Relying parties that trust the Root of Trust can also trust the functions of the TrE.

A TrE is initialised in a secure start up process when an M2M Device or M2M Gateway is initialised.

An M2M Device or M2M Gateway can support one or more TrEs.