Yongjing ZHANG (oneM2M WG5 chair / Huawei)
Jason YIN (oneM2M WG6 Vice-Chair / Huawei)
Christian Groves (Huawei)
Milan Patel (Huawei)

oneM2M device management and software/firmware update

1 Summary

This paper highlights the current state of the art of the work of oneM2M (www.oneM2M.org) with respect to device management and in particular secure software and firmware updates.

2 OneM2M background

The purpose and goal of oneM2M is to develop technical specifications which address the need for a common machine to machine (M2M) Service Layer that can be readily embedded within various hardware and software, and relied upon to connect the myriad of devices in the field with M2M application servers worldwide. A critical objective of oneM2M is to attract and actively involve organizations from M2M-related business domains such as: telematics and intelligent transportation, healthcare, utilities, industrial automation, smart homes, etc. There are currently 231 participating partners and members including regional standards bodies ARIB, ATIS, CCSA, ETSI, TIA, TSDSI, TTA and TTC. The Broadband Forum, CEN, CENELEC, GlobalPlatform, Home Gateway Initiative (HGI), New Generation M2M Consortium and Open Mobile Alliance (OMA) are also members.

There is a specific working group 5 "MAS" on Management, Abstraction and Semantics that deals with the technical aspects related to management of M2M entities and/or functions. It defines specifications related to the update of devices. Working group 4 "SEC" has the overall responsibility for all technical aspects related to security and privacy within oneM2M.

The Global Open Source IoT joint Forum (goiot-forum.org) is an open source implementation of the oneM2M specifications. News of oneM2M deployments can be found at: onem2m-in-the-news

3 Architecture

3.1 Generic Management Architecture

oneM2M TS-0001 "Functional Architecture" (WI-0002) describes the end-to-end oneM2M functional architecture, including the description of the functional entities and associated reference points. It focusses on service layer aspects and takes an underlying network-independent view of end-to-end-services.

The architecture defines a "Software Management Function" (Clause 6.2.1.2.1/[TS-0001]) as part of the application and service layer management (ASM) common service functions (CSF). It allows the management of the full lifecycle of a software package including states (e.g. Installing, Installed, Updating, Uninstalling and Uninstalled) and actions (e.g. Download, Install, Update and Remove).

The architecture furthermore defines a "Device Management function" (clause 6.2.4/[TS-0001]) DMG CSF. It provides management of device capabilities on M2M gateways and M2M devices, as well as devices that reside within an M2M area network.

Application Entities (AE) can manage the device capabilities and applications on those devices by using the services provided by the ASM/DMG CSF alleviating the need for the AE to have knowledge of the technology specific protocols or data models. In order to manage the service entities and device capabilities, the ASM/DMG CSF can utilize existing technology specific protocols (e.g. [BBF TR-069], [OMA-DM], and [LWM2M]) in addition to oneM2M native operation on the management resources across the Mcc reference

point. When the technology specific protocols are used to manage devices, the ASM/DMG CSF translates or adapts the management related requests from application entities to the technology specific requests of the corresponding technologies.

All services in the oneM2M system are represented as structured resources. There are two main resources associated with the management of devices and applications:

- Resource Type **mgmtObj**: Clause 9.6.15/[TS-0001] defines the <mgmtObj> resource which contains management data which represents individual M2M management functions. It represents a general structure to map to technology specific data model e.g. OMA DM, BBF TR-069 and LWM2M. It allows the specialisation of a <mgmtObj> type that indicates whether the resource relates to a software or firmware object. The create, read, update, delete (CRUD) procedures related to the <mgmtObj> resource are found in clause 10.2.8/[TS-0001]. The specialisation of the <mgmtObj> for *firmware* and *software* resources is contained in Annex D.2 and D.3 respectively.
- Resource Type **mgmtCmd**: Clause 9.6.16/[TS-0001] defines the <mgmtCmd> resource represents a method to execute management procedures or to model commands and remote procedure calls (RPC) required by existing management protocols (e.g. BBF TR-069), and enables application entities to request management procedures to be executed on a remote entity. This allows CRUD actions for software or firmware resources (among others). These procedures are described in clause 10.2.8/[TS-0001]. The use of <mgmtCmd> with its attributes or sub-resources allows the mapping of RESTful operations to RPC-like management technologies.

3.2 Trust Architecture

An important consideration in managing the lifecycle of firmware and software is the trust model between users and network entities. Clause 11/[TS-0001] describes the trust enabling architecture for establishing security and trust between all the parties involved in the M2M ecosystem. Four main infrastructure functions facilitate the trust model:

- M2M Enrolment functions (MEF), which manage the enrolment and configuration of M2M Nodes and M2M applications for access to M2M Services provided by an M2M Service Provider, prior to service operation. The credentials provisioned by a MEF can be used for Security Association Establishment Framework, End-to-End Security of Primitives or End-to-End Security of Data.
- M2M Authentication functions (MAF), which may facilitate identification and authentication of CSEs and AEs, End-to-End Security of Primitives and End-to-End Security of Data during M2M service operation. A single MAF may support all of the above security services or only a selection of them.
- Dynamic Authorization Systems and Role Authorities, which manage authorization privileges to access resources that may be assigned during operation.
- Privacy Policy Managers that assist in the management of privacy preferences expressed by data subject with respect to service requirements and applicable regulations.

The above functionalities are assumed to be operated by trusted parties (generally M2M Service Providers but possibly other trusted third parties). These functions are all detailed in oneM2M TS-0003 “Security Solutions” [TS-0003]. Whilst [TS-0003] doesn’t address any specific requirements regarding firmware/software update the general security framework can cover interactions over Mca and Mcc. For example, a <firmware> or <software> resource containing the package meta data (e.g. download URL) can be securely delivered to the platform (IN-node) or a device/gateway (ASN/MN-node), while the actual downloading of the firmware/software image is out-of-scope of oneM2M. If OMA/BBF DM technologies are used, then those (via Mcn reference point) technology specific security mechanisms shall be used to protect the update procedure.

4 Protocol

oneM2M TS-0004 “Service layer Core Protocol Specification” defines the communication protocol used in oneM2M systems. It specifies the common data formats, interfaces and message sequences to support

reference points(s) defined by oneM2M. It defines the data types related to the resources in TS-0001 including the <mgmtObj> and <mgmtCmd> resources in particular those related to firmware and software update (i.e. clause 6.3.4.2.13 & 6.3.4.2.22 / [TS-0004]). Procedures for management operations are described in a underlying network agnostic manner in clause 7/[TS-0004]. Common procedures and resource specific procedures for <mgmtObj> and <mgmtCmd> (i.e. clause 7.4.15 & 7.4.16 / [TS-0004]) are defined.

5 Technology specific management protocols

As discussed above the oneM2M architecture provides a technology agnostic approach to define resources and primitives which implement service functions. These primitives are eventually mapped to network specific protocols. oneM2M provides mappings to several technologies including: [BBF TR-069], [OMA-DM] and [LWM2M]. In general, oneM2M has specified a common set of management objects that are able to be mapped to underlying technology-specific management data models. This common model is specified in [TS-0001] Annex D, while the 1-1 mappings are specified in [TS-0005] and [TS-0006] respectively. However due to the capabilities inherent in the technology specific protocols 100% mapping is not possible. For example OMA status code 213 is not mapped to an oneM2m primitive code. There are also cases where a technology specific protocol does not support primitives defined by oneM2M, e.g. OMA DM 1.3 does not have a subscription mechanism for management object change (cl.5.4.1.5.1/[TS-0005]), LWM2M does not have objects for area network management (cl.6.3.5 & 6.3.6/[TS-0005]) nor does it have resource specific status codes (cl.6.4.6/[TS-0005]). oneM2M also defines new LWM2M objects (cl.6.6/[TS-0005]) to facilitate mapping. There are also cases where oneM2M provides resources but it is not possible to provide a mapping to technology specific management protocol resources due to that protocol itself being reliant on underlying transport technologies (cl. 7.1.2/[TS-0006]). In order to match some procedures, devices may have to alter their behaviour in order to be able to map notifications (cl.8.1.6/[TS-0006]).

Although the common model is not 100% compatible with other models, the added value is to provide a common API (via oneM2M Mca reference point) so that Application developers doesn't need to handle various management technologies. Besides, the oneM2M management object model (i.e. <mgmtObj> resources) may also be used directly (over Mca+Mcc reference point) without mapping to OMA/BBF technologies in principle, if the management task is not so complicated, e.g. to get the battery level of a device.The use of BBF device management is envisaged for fixed devices. The use of OMA device management is seen for mobile devices with LWM2M being used for constrained devices.

5.1 BBF Device Management

oneM2M TS-0006 defines the mapping between the oneM2M management model and the Broadband Forum CPE WAN management protocol [BBF TR-069]. It provides general management object data mapping and procedures between BBF and oneM2M specifications as well as specific details regarding software (clause 7.10/[TS-0006) and firmware (clause 7.9/[TS-0006]) resources.

Note: [BBF TR-069] has software/firmware image and software module management functions.

5.2 OMA Device Management

oneM2M TS-0005 clause 5 defines the mapping between the oneM2M management model and the OMA device management protocol (version 1.3 and 2) [OMA-DM]. It provides general management object data mapping and procedures for interworking between OMA and oneM2M specifications as well as specific details regarding software (clause 5.4.2.2/[TS-0005]) and firmware (clause 5.4.2.1/[TS-0005]) resources.

Note: Clause 8/[OMA-DM] describes a number of bootstrapping techniques including: factory bootstrap, smartcard bootstrap, client initiated bootstrap and server initiated bootstrap.

Clause 6/[TS-0005] covers the mapping between the oneM2M management model and the OMA LWM2M protocol. It provides general management object data mapping and procedures between OMA and oneM2M specifications as well as specific details regarding software (clause 6.3.3/[TS-0005]) and firmware (clause 6.3.2/[TS-0005]) resources.

Note: LWM2M describes a Bootstrap interface. See clause 5.2/[LWM2M].

6 References:

[TS-0001] oneM2M TS-0001“Functional Architecture” WI-0002

[TS-0003] oneM2M TS-003 “Security Solutions” WI-0007

[TS-0004] oneM2M TS-004 “Service Layer Core Protocol Specification” WI-0009

[TS-0005] oneM2M TS-0005 “Management Enablement (OMA)” WI-0010

[TS-0006] oneM2M TS-0006 “Management Enablement (BBF)” WI-0010

[BBF TR-069] Broadband Forum TR-069: "CPE WAN Management Protocol Issue": 1 Amendment 5, November 2013. TR-069

[OMA-DM] OMA-DM: "OMA Device Management Protocol", Open Mobile Alliance OMA DM Protocol

[LWM2M] LWM2M: "OMA LightweightM2M", Version 1.0, Open Mobile Alliance. OMA LWM2M.