Hewlett Packard Enterprise

Business white paper

HPE Universal IoT Platform oneM2M and beyond

Introduction

The market for IoT devices and applications, and the new business processes they enable, is enormous. Gartner estimates a 35.2 percent compound annual growth rate (CAGR) of non-consumer IoT devices from 2013 to 2020, reaching an installed base of 25 billion units in 2020.[1] BI Intelligence also predicts the number of devices connected via IoT technology will grow at a 35 percent CAGR from 2014 to 2019[2]. IDC estimates that the installed base of IoT is approximately 15 billion devices in 2016, growing to 28.1 billion devices by 2020.[3]

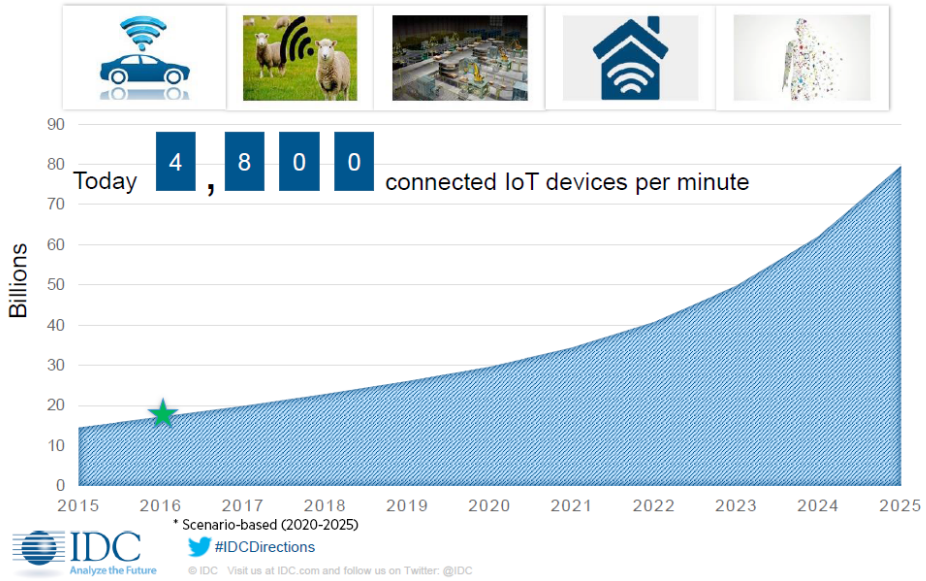

Figure 1: IoT connected device forecast

A key challenge for unlocking this huge potential traditionally has been a lack of consistent standards and interoperability between the different IoT systems. McKinsey estimates that inter-operability accounts for almost 40 percent of the value potential from the IoT applications.[4]

The HPE Universal IoT Platform addresses this key challenge of inter-operability with the adoption of the oneM2M standard, which is working to unify the global IoT community, by enabling the federation and interoperability of the different IoT systems, across multiple networks and domains. This paper explains the key benefits resulting from the adoption of the oneM2M standards and the additional advanced capabilities supported by the HPE Universal IoT Platform for effectively monetizing the IoT data.

Why oneM2M?

There are plenty of standards-related activities in the IoT industry led by different alliances and consortia, and many of them are quite mature in their own respective areas and domains. Adding to this challenge of multiple standards is the IoT market's distinct fragmentation, a highly distributed value chain with a lot of proprietary IoT device implementations which makes it nearly impossible for all of these devices to actually be able to talk to each other as envisaged with the Internet of Things.

AllSeen Alliance
The AllSeen Alliance is a cross-industry consortium dedicated to enabling the interoperability of billions of devices, services, and apps that comprise the Internet of Things (IoT).

OMA
Open Mobile Alliance (OMA) specifications support the billions of new and existing terminals across a variety of wireless networks, supporting machine-to-machine device communications for IoT.

3GPP
The 3rd-Generation Partnership Project (3GPP) unites telecommunications standard development organizations to standardize cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities. Specifically to IoT, they released the NB-IOT specification.

IEEE
The mission of the Institute of Electrical and Electronics Engineers (IEEE) IoT initiative is to serve as the gathering place for the global technical community working on IoT.

ITU
The purpose of the International Telecommunication Union (ITU) Global Standards for IoT is to provide a visible single location for information on and development of IoT standards, these being the detailed standards necessary for IoT deployment and to give service providers the means to offer the wide range of services expected from the IoT.

IPSO Alliance
The IPSO is an alliance that promotes and supports Smart Objects, and manages an IPSO Smart Object Registry. The objective is to develop, establish, and create the industry leadership of an "IPSO Platform" that includes the definition and support of Smart Objects with an emphasis on object interoperability on protocol and data layers and of Identity and Privacy technologies.

IETF
The Internet Engineering Task Force (IETF) originally focused on running IP over IEEE 802.15.4 radios and has since then evolved into a much larger project, covering IPv6 adaptation layer (6LoWPAN), Constrained RESTful Environments (CoRE) to allow the integration of constrained devices with the Internet at the service level.

OIC/OCF
Unified as OCF in Feb 2016, it's an entity whose goal will be to help unify IoT standards so that companies and developers can create IoT solutions and devices that work seamlessly together.

Figure 2: IoT standards proliferation

The current IoT-related standards and technologies are highly fragmented. The fragmentation can be seen across different verticals/application domains where there is very little or no re-use of technologies. Given that multiple standards have always existed—many of them quite well established in their own areas more so around network/device connectivity—it is not realistic to expect the ecosystem to converge on a single standard considering the varied applications needs and diverse physical operating conditions for these connected devices. UBS's research report[5] has singled out standardization as one of the key prerequisites for the broad adoption of connected devices and claims that "adherence to a single standard will be key in enabling the success of the Internet of Things on a global basis". Overall, the importance of consistent standards and IoT interoperability to the market and consumers is undeniable.

While we have plenty of alliances already underway with the intention of establishing standards conducive to the implementation of IoT, oneM2M stands out as a unifying standard for most of these initiatives. The objective of oneM2M is to avoid competing standards, duplication, and conflicts stemming from alliances and consortia tackling similar or overlapping issues. oneM2M can be seen as a "standard of standards"; it is involved in concerted efforts to bring in interoperability among architectural layers across IoT applications spanning different industry verticals. oneM2M is helping this dire challenge of fragmentation in realizing the vision of IoT and stands out as the interoperability enabler for the entire M2M and IoT ecosystem[6].

oneM2M is the global standards initiative that was formed in 2012 and consists of eight of the world's preeminent Standards Development Organizations (SDO) viz. ETSI (Europe), ARIB (Japan), ATIS (U.S.A), TIA (U.S.A), CCSA (China), TSDSI (India), TTA (Korea) and TTC (Japan). These SDO Partners collaborate with six industry consortia (Broadband Forum, Continua Alliance, GlobalPlatform, HGI, Next Generation M2M Consortium and OMA) and has over 220 member organizations to produce and maintain globally applicable, access-independent technical specifications for a common M2M/IoT Service Layer. oneM2M is an open initiative; it actively encourages industry associations and forums with specific application requirements to participate, in order to ensure that the solutions developed support their specific needs.

HPE Universal IoT Platform and oneM2M

The HPE Universal IoT Platform is aligned with oneM2M industry standard and is designed to be industry-vertical and vendor-agnostic. It takes a truly horizontal approach, enabling connection and information exchange between heterogeneous IoT devices—standards and proprietary communication—and IoT applications. Its enables federating the various components of the end-to-end solution within the complex and fragmented eco-system, from device through to application—to sit on top of ubiquitous reliably managed connectivity, enable identification, development, and roll out industry-specific use cases.

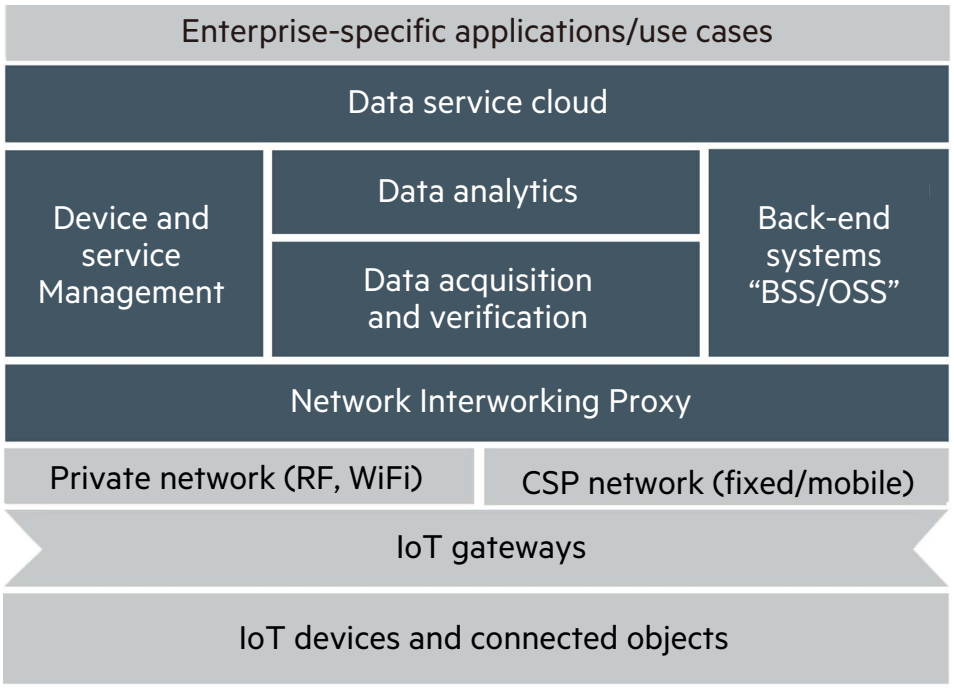

Figure 3: HPE Universal IoT Platform architecture

The HPE Universal IoT Platform comprises of the following key modules:

Device and service management
The device and service management (DSM) module is the nerve center of the HPE Universal IoT Platform. It manages the end-to-end lifecycle of the IoT service and associated gateways/devices and sensors, which includes application registration, communication policies, and remote management of the IoT gateways/devices. It provides a Web-based GUI for all the stakeholders to interact with the IoT platform. The hierarchical customer account modeling, coupled with the Role-Based Access Control (RBAC) mechanism, enables various mutually beneficial service models such as B2B, B2C, and B2B2C models.

Network Interworking Proxy
The Network Interworking Proxy (NIP) component in the HPE Universal IoT Platform provides a connected devices framework for managing and communicating with disparate IoT gateways/devices, and communicating over different types of underlying networks. With NIP, you get interoperability and information exchange between the heterogeneous systems deployed in the field and the uniform oneM2M-compliant resource model supported by the HPE Universal IoT Platform.

Data acquisition and verification

Data acquisition and verification (DAV) supports reliable bi-directional data communication between IoT applications and IoT gateways/devices deployed in the field. The DAV component uses the underlying NIP to interact and acquire IoT data and maintain it in a resource-oriented uniform data model aligned with oneM2M. This data model is completely agnostic to the device or application, so it is completely flexible and extensible. IoT applications in turn can discover, access, and consume these resources on the north-bound side using secure oneM2M-compliant Mca interface.

Data analytics

The data analytics (DA) module provides a creation, execution, and visualization environment for nearly all types of analytics including batch and real-time—based on complex event processing. It leverages the HPE Vertica technology for discovery of meaningful patterns in data collected from sensors in conjunction with your or other application-specific externally imported data. The data analytics engine enables the creation of data insights that can be used for business analysis and/or monetization by sharing insights with the partners.

Data service cloud

The data service cloud (DSC) module enables advanced monetization models, especially fine-tuned for IoT and cloud-based offerings. DSC supports mashup for new content creation providing additional insight by combining embedded IoT data with internal and external data from other systems. This additional insight can provide value to other stakeholders outside the immediate IoT ecosystem, enabling monetization of such information.

Back-end systems

The back-end systems (BSS/OSS) module provides a consolidated, end-to-end view of devices, gateways, and network information. This module helps IoT operators automate and prioritize key operational tasks, reduce downtime through faster resolution of infrastructure issues, and improve service quality. In addition, the IoT applications can consume a subset of these OSS/BSS from the Platform-as-a-Service, thereby avoiding the need for re-developing the OSS/BSS functionalities within the applications.

oneM2M benefits

Adoption of oneM2M for the HPE Universal IoT Platform was a natural choice and provides a number of benefits—a few of the keys ones being:

Enabling a horizontal IoT platform

oneM2M addresses the challenges of fragmentation, integration complexity, information sharing and high development cost with a horizontal-platform–based approach, providing a standardized, simplified, and unified layer as a service to various partners consuming and sharing information across various application domains. The access technology-independent horizontal platform enables reliable, end-to-end data control/exchange between M2M devices and customer applications by providing functions for remote provisioning and activation, authentication, data buffering, encryption/decryption, synchronization, aggregation, and device management. This enables rapid IoT application development using the underlying common service functions for multiple access technologies such as fixed line, cellular, Wi-Fi, ZigBee, Bluetooth®, LoRa, NB-IoT, etc.

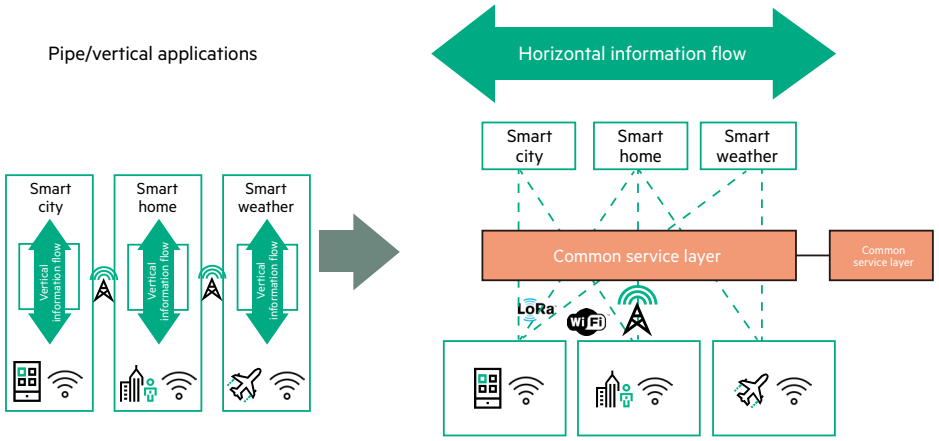

Figure 4: Horizontal IoT platform

A horizontal IoT platform provides the following key benefits:

- **Lower total cost of ownership (TCO):** Lower CAPEX with lower cost of development and deployment, and lower OPEX with scale of economies with horizontal service layer providing nearly all the common service functions
- **New revenue streams:** Enables new business opportunities with service offerings from cross sharing of resources and data across silos; helps address use cases and markets where cost was prohibitive earlier
- **Faster time-to-value** with accelerated development and deployment

The common service functions provided by the horizontal platform have been designed based on the analysis of a number of use cases across different application domains. Table 1 lists the collection of different use cases considered for defining the common service functions, confirming that the resulting horizontal platform could cater to a broad range of use cases having diverse communication and management requirements.

Table 1: oneM2M use case collection[9]

INDUSTRY SEGMENT	ONEM2M USE CASES							
Agriculture								
Energy	Wide-area energy-related measurement/ control system for advanced transmission and distribution automation	Analytics for oneM2M	Smart meter reading	Environment monitoring for hydro-Power generation using satellite M2M	Oil and gas Pipeline cellular/ satellite gateway			
Enterprise	Smart building							
Finance								
Healthcare	M2M healthcare gateway	Wellness services	Secure remote patient care and monitoring					
Industrial								
Public Services	Street light automation	Devices, virtual devices and things	Car/Bicycle Sharing Services	Smart parking	Information delivery service in the devastated area			
Residential	Home energy management	Home energy management system	Plug-In electrical charging vehicles and power feed in home scenario	Real-time audio/Video communication	Event triggered task execution	Semantic home control	Semantic device plug and play	
Retail								
Transportation	Vehicle diagnostic and maintenance report	Remote maintenance services	Neighbourhood alerting on traffic accident	Feel management service using digital tachograph				
Other	Extending the M2M access network using satellites	M2M data traffic management by underlying network operator	Optimizing connectivity management parameters with mobile networks	Optimizing mobility management parameters with mobile networks	Sleepy nodes	Collection of M2M system data	Leveraging broadcasting/ multicasting capability of underlying networks	Services provisioning for equipment with built-in device

Interoperability

As a unifying standard, oneM2M is enabling the federation and interoperability of the different IoT systems, across multiple networks and domains.

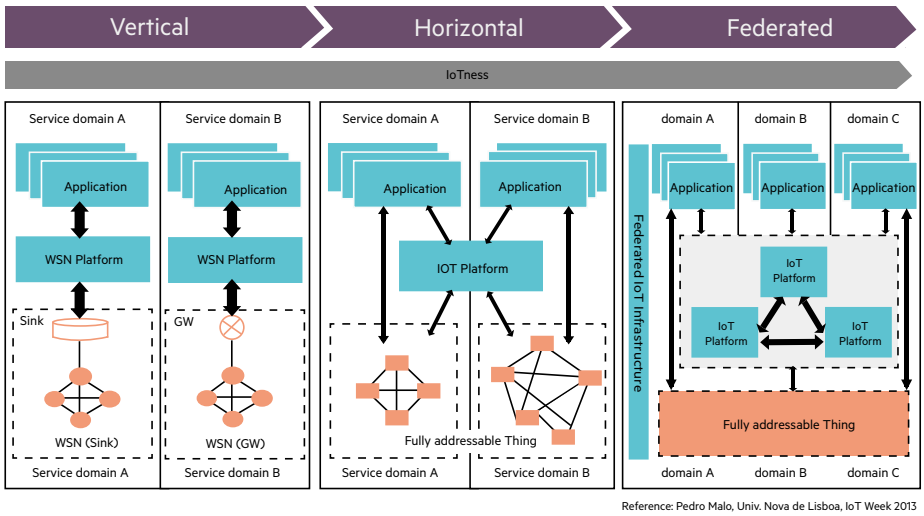

Figure 5: Towards the Internet of Things

Interoperability is a key requirement for any horizontal IoT platform supporting IoT applications across different verticals/domains and still benefit from all the predominant domain-specific standards and technologies. oneM2M is working on specifying the interoperability at different levels, which includes:

1. Device-to-platform interoperability—oneM2M Mca/Mcc
2. Platform-to-platform interoperability—oneM2M Mcc'
3. Service interoperability—oneM2M Mca
4. Data interoperability—oneM2M semantics

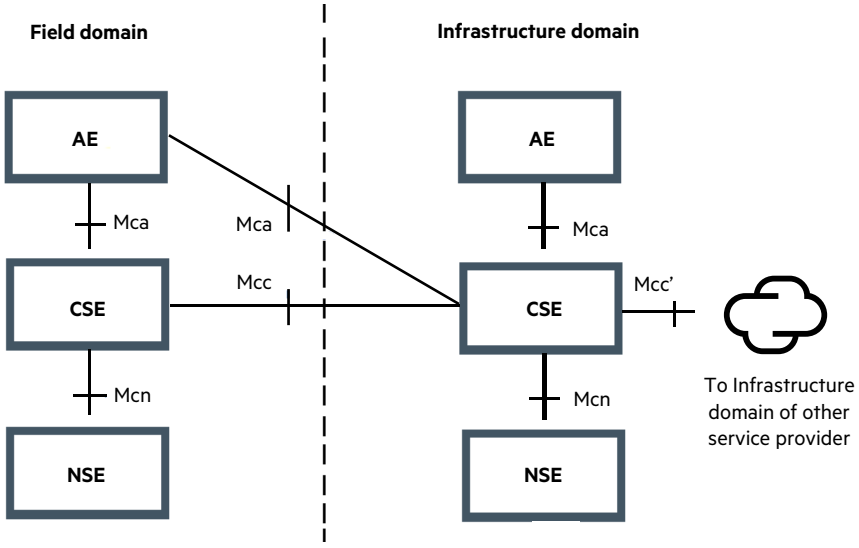

Figure 6: oneM2M functional architecture

oneM2M release 1[7] and the work-in-progress release-2 specifications[8] are already addressing interoperability for many of the common existing industry standards and technologies:

Protocol bindings

- **RESTful HTTP—release 2 (TS-0009)** specifies binding of oneM2M primitives to HTTP method, binding of oneM2M response status codes (successful/unsuccessful) to HTTP response codes and binding of oneM2M RESTful resources to HTTP resources
- **CoAP—release 1 (TS-0008)** specifies binding of oneM2M primitives to CoAP messages, binding of oneM2M response status codes to CoAP Response Codes and behavior of a CoAP client and server depending on oneM2M parameters
- **MQTT—release 1 (TS-0010)** specifies how the oneM2M Mca or Mcc request and response messages are transported across the MQTT protocol
- **WebSocket (TS-0020)**—oneM2M is working on specifying the binding for WebSocket protocol to transport serialized representations of oneM2M request and response primitives

Management enablers

- **OMA (TS-0005)** specifies the usage of OMA DM and OMA LWM2M resources and the corresponding messages to fulfil the oneM2M management-related requirements
- **BBF (TS-0006)** specifies the usage of the BBF TR-069 protocol and corresponding messages to fulfil the oneM2M management related requirements

Also, a number of other work programs have been identified in oneM2M for enabling interworking with other industry consortia/alliances, such as:

- **LWM2M Interworking (TS-0024)**—providing transparent transport of encoded LWM2M application objects between LWM2M endpoints and M2M Applications. It is also specifying full mapping of LWM2M objects in LWM2M endpoints to semantically enabled resources that are utilized by M2M applications. It should be noted that this interworking will also apply to ecosystems around LWM2M, for e.g. other alliances like IPSO have created LWM2M-compatible object descriptions related to smart city applications.
- **Home Appliances Information Model and Mapping (TS- 0023)**—describes the oneM2M-defined information model for home appliances, including the description of a method on how it is mapped with other information models from external organizations which include AllJoyn, OIC, HGi Smart Home Device Template (SDT), and ECHONET.
- **OIC Interworking (TS-0024)**—providing transparent transport of encoded OIC resources and commands in oneM2M resource types between OIC devices and M2M applications.
- **AllJoyn Interworking (TS-0021)**—oneM2M is working on identification of interworking scenarios between oneM2M and AllJoyn systems, which could result in new requirements on the oneM2M system.

Adoption of oneM2M provides for seamless interoperability with all of the above standards/technologies and benefits from the re-use of already existing solutions/technologies wherever possible. Continued focus from oneM2M around federation and interoperability helps mandate that the HPE Universal IoT Platform in future can be aligned with other emerging alliances and standards. For customers, this secures their investment in having a platform that is future technology-proof.

Built on a Resource Oriented Architecture

oneM2M is based on Resource Oriented Architecture, where the real-world entities (Gateways, devices, sensors) are uniformly represented as resources, where a resource could be any component of a device/application on a device that is worth being uniquely identified and linked to. Resources are identified based on Uniform Resource Identifiers (URIs), and representations retrieved through resource interactions contained as links to other resources, so that applications can follow links through an interconnected web of resources. Note that in addition to the hierarchical URI, oneM2M also supports a non-hierarchical URI to enable IoT applications to access and interact with resources without the need to know the topology of the underlying resource model.

A Resource Oriented Architecture simplifies the development of IoT applications by providing a uniform interface for interacting with resources and retrieving their representations, irrespective of:

- The type of the underlying gateway/device and their topology.
- The type of the vertical/application domain, which could be smart cities, industrial control, home automation, connected health, intelligent transportation, etc.
- The communication protocol used between the gateway and devices in personal area network. For e.g. ZigBee, Bluetooth, RFID etc.
- The application/communication protocol used by the gateways/devices, for e.g. MQTT, LWM2M, CoAP or any other proprietary protocol.
- The network communication technology used, for e.g. cellular, LoRa, Wi-Fi, or fixed line, etc.

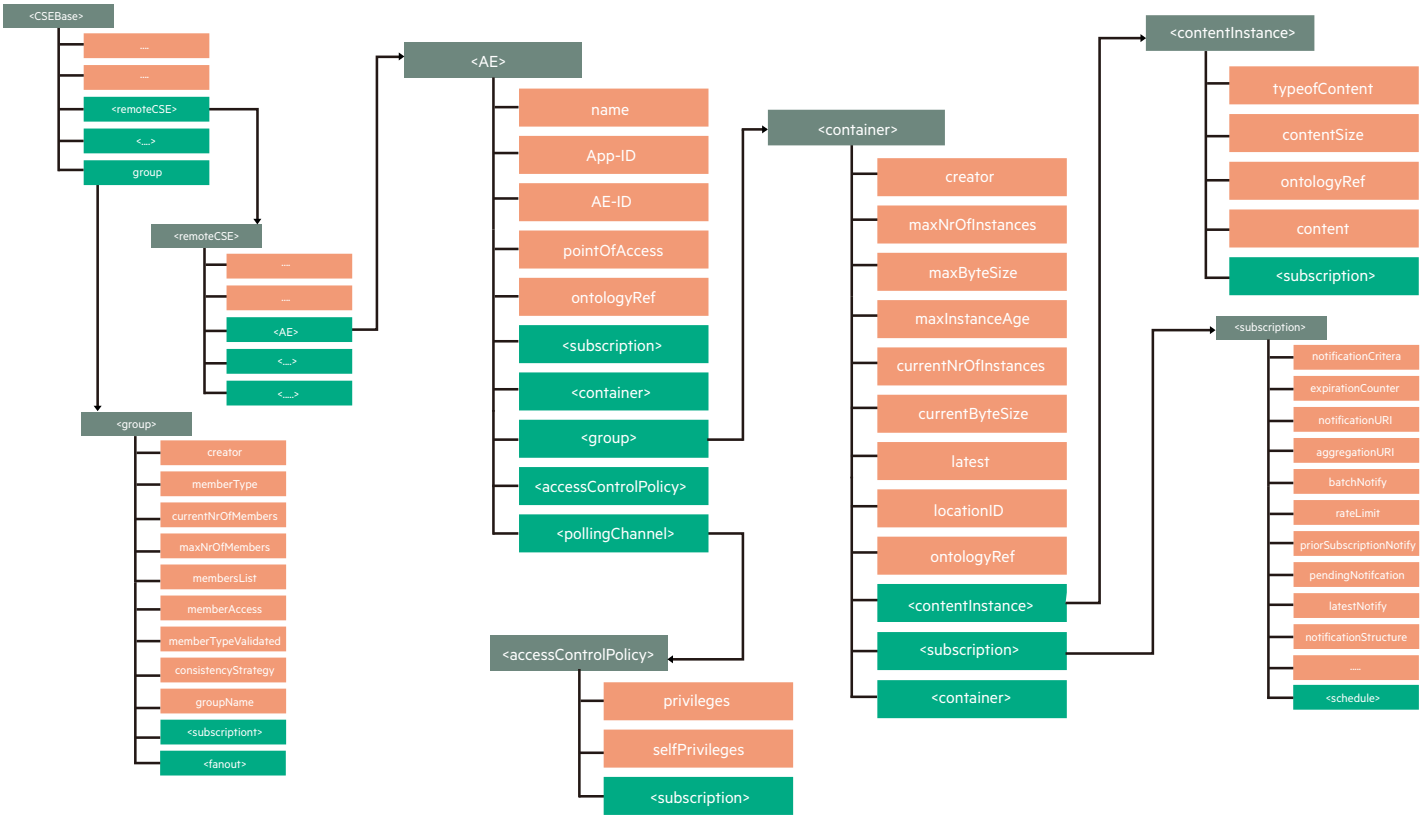

Figure 7: oneM2M hierarchical resource tree

Applications access/interact with the resources using a simple request/response mechanism with “Create”, “Retrieve”, “Update”, “Delete”, and “Notify” commands (CRUDN), enabling discovery of access policies, device info, and resources on the devices; fetching device information by retrieving resources; controlling devices by changing resources and monitoring resources observing the changes on the properties of resources. oneM2M provides for multiple protocol bindings (HTTP, WebSockets, MQTT, CoAP, etc.) to access and interact with this common resource model. For e.g. a Web-based IoT application could use RESTful HTTP based interface.

A Resource Oriented Architecture with linkable resources is one of the key steps towards building a scalable interaction model on top of the basic network connectivity for any IoT application and is a strong foundation for having a semantically enabled Internet of Things.

Security

oneM2M provides the guidelines and security solutions for addressing the diverse security needs resulting from the delivery of cross-domain interactions and services. It defines the following high layers:

Secure functions layer: Contains a set of security functions that are exposed at reference point Mca and Mcc, such as identification and authentication, authorization, security association, sensitive data handling, and security administration.

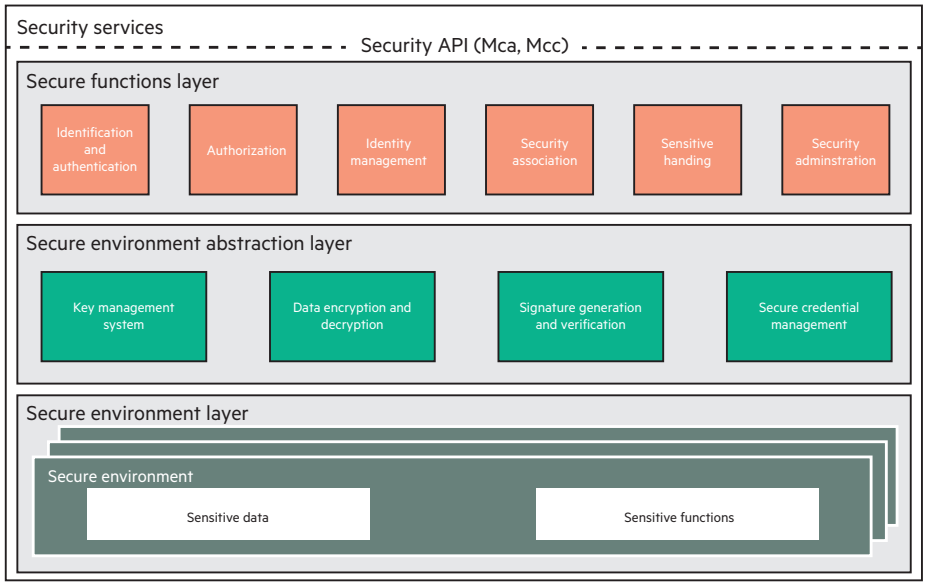

Figure 8: High-level overview of oneM2M security architecture

Secure environment abstraction layer: This is used by the secure functions layer and implements various security capabilities such as key derivation, data encryption/decryption for application message security, signature generation/verification, manage security credential from/to the secure environments.

Secure environment layer: This layer contains one or multiple secure environments that provide various security services related to sensitive data (SE capability, security keys, local credentials, security policies, identity information etc.) storage and sensitive function (data encryption/decryption) execution.

The authorization function is aligned with the Resource Oriented Architecture and manages data access to authenticated entities according to provisioned access control policies and assigned roles. Access Control Policy (ACP) is defined as sets of conditions that define whether entities should be permitted access to a protected resource. Access/management for a given resource is authorized upon satisfying at least one ACP rule in one of the linked ACPs. For e.g. an ACP rule is satisfied if the "who", "what" and "which" are satisfied by the requesting entity. The system provides for a flexible model for defining the ACP allowing for associating the same ACP with multiple resources, enabling easy sharing of resources for multiple applications.

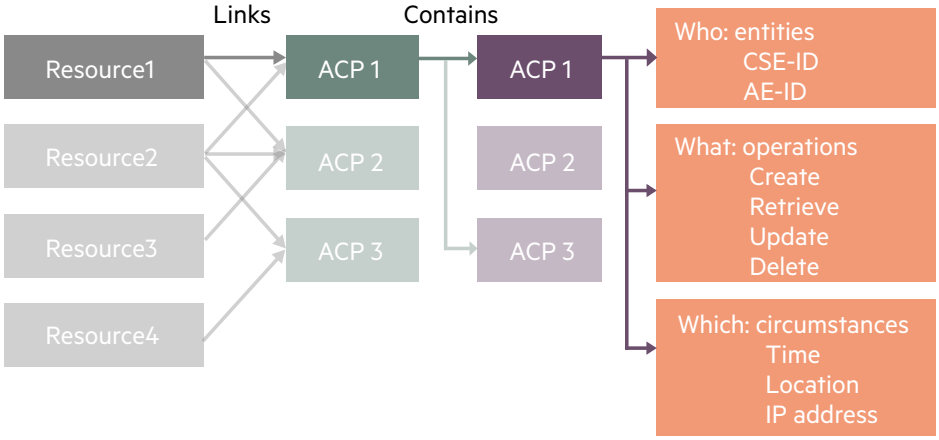

Figure 9: oneM2M Access Policy Control (ACP) model

Semantically enabled IoT

In order to fully realize the benefits of Internet of Things, we need an ecosystem where applications can collaborate and exchange data across industry domains, which means:

- M2M data needs to be made understandable without prior knowledge about the data or devices
- M2M data and devices should be discoverable in real time as complex relationships between the various resources change with time in an IoT environment
- Data interaction should be offered on higher level of abstraction (physical/virtual entity modeling)
- Privacy and confidentiality of the information source should be maintained while still providing the required semantic context

oneM2M is working together with other consortiums to address these challenges and build a standardized vocabulary/ontology to semantically annotate the data (for describing the "Things" and their associated contexts). The ontology will be interoperable to allow applications to discover, exchange and analyze semantic information across different vertical domains while ensuring the confidentially and privacy of the information sources. For e.g. a smart lighting application can manage the luminosity levels of the street lighting based on the data collected from the transportation domain, weather warnings, and parking occupancy within the given area. This will enable development of truly collaborative IoT applications wherein data collected within each of the service domains and represented semantically is interpreted and consumed by another domain seamlessly and securely.

Effective data monetization

The end game with IoT is to securely monetize the vast treasure troves of IoT-generated data to deliver value to enterprise applications, whether by enabling new revenue streams, reducing costs, or improving customer experience. Effective monetization of data will not be achieved with mere consumption of the IoT data—data needs to be categorized based on the value, services need to support instant interactions based on the data values, and data should be exchanged across multiple domains for maximizing the value. Built on top of the oneM2M resource-oriented architecture the HPE Universal IoT Platform enables this data monetization with the data service cloud (DSC) component, which enables mashups where users can create applications mixing real-world devices, such as sensors, with virtual services on the Web. The DSC component also manages partner services, defines and enforces policies on the services consumed, and tracks the consumption of data. In addition, the data analytics component helps detect anomalies in data, enabling preventive actions; it helps detect patterns and trends in data for improving business efficiency or sharing insights with partners, all directed towards effective monetization of the data.

Built on top of oneM2M industry standards along with additional advanced capabilities to meet the business requirements, with the HPE Universal IoT Platform architecture, you get an industry-, vertical-, and client-agnostic solution with greater scalability, modularity, and versatility. This enables you to manage your IoT solutions and deliver value through monetizing the vast amounts of data generated by connected devices and making it available to enterprise-specific applications and use cases.

References

[1] Forecast: Internet of Things, Endpoints and Associated Services, Worldwide, Gartner, 20 October 2014, **gartner.com/doc/2880717/forecast-internet-things-endpoints-associated**

[2] Business Insider: The Internet of Everything, 2015 Slide Presentation, **businessinsider.in/THEINTERNET-OF-EVERYTHING-2015-SLIDE-DECK/articleshow/45695215.cms#-1**

[3] IDC Report—The Internet of Things: Getting Ready to Embrace Its Impact on the Digital Economy, **idc.com/getdoc.jsp?containerId=prUS25658015**

[4] McKinsey Report **mckinsey.com/business-functions/business-technology/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world**

[5] UBS investment research report "Who Are the Enablers of 'The Internet of Things'?" **http://max.book118.com/html/2015/0819/23705417.shtm**

[6] onem2m-whitepaper-january-2015—The Interoperability Enabler for the Entire M2M and IoT ecosystem, **onem2m.org/images/files/oneM2M-whitepaper-January-2015.pdf**

[7] oneM2M technical release 1 specifications, **onem2m.org/technical/published-documents**

[8] oneM2M technical work-in-progress release 2 specifications, **onem2m.org/technical/latest-drafts**

[9] oneM2M Use Case Collection **etsi.org/deliver/etsi_tr/118500_118599/118501/01.00.00_60/tr_118501v010000p.pdf**

Learn more at
hpe.com/go/IoT4CSP

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-5470ENW, May 2016