Exposing Network Capabilities to M2M Requirements

Approved Version 1.0 – 21 Jun 2018

Open Mobile Alliance

OMA-RD-ENCap-M-V1_0-20180621-A

Contents

Figures

Tables

1. Scope (Informative)

This document defines the requirements for Exposing Network Capabilities to M2M Applications and/or M2M Service Platforms through APIs.

In addition, it contains:

- Use cases where M2M Applications and/or M2M Service Platforms can leverage network capabilities to enrich the services or to streamline the operations.
- Gap analysis to identify any missing Network APIs to address the above use cases.

2. References

2.1 Normative References

[3GPP TR 22.853] 3GPP TR 22.853 V13.0.0 "Study on Service Exposure and Enablement Support (SEES) requirements (Release 13)", 3rd Generation Partnership Project, June 2014, URL: http://www.3gpp.org/

[3GPP TS 22.101] 3GPP TS 22.101 V13.6.0 "Service aspects; Service principles (Release 13)", 3rd Generation Partnership Project, September 2015, URL: http://www.3gpp.org/

[3GPP TS 22.368] 3GPP TS 22.368 V V13.1.0 "Service requirements for Machine-Type Communications (MTC) (Release 13), 3rd Generation Partnership Project, December 2014, URL: http://www.3gpp.org/

[3GPP TS 23.032] 3GPP TS 23.032 V12.0.0 "Universal Geographical Area Description (GAD) (Release 12)", 3rd Generation Partnership Project, September 2014, URL: http://www.3gpp.org/

[3GPP TS 23.682] 3GPP TS 23.682 V13.4.0 "Technical Specification Group Services and System Aspects;
Architecture enhancements to facilitate communications with packet data networks and applications (Release 13)", 3rd Generation Partnership Project, December 2015, URL: http://www.3gpp.org/

[Autho4API_10] "Authorization Framework for Network APIs", Open Mobile Alliance™, OMA-ER-Autho4API-V1_0, URL: http://www.openmobilealliance.org/

[oneM2M TR 0001] TR 0001 V0.0.5 "oneM2M Use Cases Collection", November 2013, URL: http://www.onem2m.org/

[oneM2M TS 0002] TS 0002 V1.0.1 "Requirements", oneM2M, January 2015, URL: http://www.onem2m.org/

[OSE] "OMA Service Environment", Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[RCC5139] "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)", M. Thomson, J. Winterbottom, February 2008, URL:http://www.ietf.org/rfc/rfc5139.txt

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt

[RFC5491] "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations", J. Winterbottom, M. Thomson, H. Tschofenig, March 2009, URL: http://www.ietf.org/rfc/rfc5491.txt

2.2 Informative References

[OMADICT] "Dictionary for OMA Specifications", Version 2.9, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_9, June 2012, URL:http://www.openmobilealliance.org/

[PresenceAPI_10] "OMA RESTful Network API for Presence v1.0", Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

For the purpose of this RD, all definitions from the OMA Dictionary [OMADICT] apply.

M2M Service Platform	It is a platform that enables the M2M service providers to provide common service functionalities for the machine to machine communication (M2M) allowing them to manage their customers' applications, devices, the communications between them and the collected data to be used efficiently for their customers. M2M Service Platform uses the network service capabilities exposed by the carriers through open access models (e.g. OMA network APIs).

3.3 Abbreviations

3GPP	3rd Generation Partnership Project
API	Application Programming Interface
DRX	Discontinuous Reception
M2M	Machine to Machine
OMA	Open Mobile Alliance
QoS	Quality of Service
RAT	Radio Access Technology

4. Introduction (Informative)

As M2M communications often have a different property from human-oriented communications, they are likely to have different requirements for exposure of network capabilities. At the same time, network capabilities and in particular those recently enhanced are not fully leveraged by different applications. This document bridges the gap between functionalities of current Network APIs and those that may be required by M2M Applications, by identifying the requirements that would enhance this exposure and would support APIs to allow access to these network capabilities.

Different standards bodies and entities, such as oneM2M, 3GPP, OMA and GSMA, have already started in one way or another to talk about the need of new network APIs to support different service exposure use cases and requirements. Therefore, this document defines the requirements for exposing network capabilities to M2M and other relevant applications.

4.1 Version 1.0

The OMA-RD-Encap-M-V1_0 captures the functional requirements for Exposing Network Capabilities to M2M and other relevant applications.

5. Exposing Network Capabilities to M2M release description (Informative)

5.1 End-to-end Service Description

Defining requirements for Network API to support network service exposure and exposing network capabilities will enable an M2M (or any other) application provider or service provider to have a clear view on how it can leverage existing and future available network capabilities and how to enrich the services or to streamline the operation.

These requirements will also help a Network Operator to promote effectively its existing and soon-to-be-made available network capabilities which subsequently will result in developing potential business opportunities in the market.

6. Requirements (Normative)

6.1 High-Level Functional Requirements

This section captures High-Level Functional Requirements of the ENCap-M2M.

Note that an M2M or any other Application and Service Platform are collectively referred to as a third-party.

Label	Description	Release
ENCapM-HLF-001	An OMA API SHALL enable a third-party to provide a Network Operator with information about predictable communication patterns of individual Devices or groups of Devices that are served by this third-party. Such communication patterns MAY include • Time and traffic volume related patterns (e.g. repeating communication initiation intervals, desired 'keep alive' time of data sessions, average/maximum volume per data transmission, etc.). **Informational Note:** This information may be used by the Network Operator to optimize resource usage. The relevant use case is found in Appendix B.1.	1.0
ENCapM-HLF-002	An OMA API SHALL enable a third-party to provide a Network Operator with information about predictable communication patterns of individual Devices or groups of Devices that are served by this third-party. Such communication patterns MAY include • Location and Mobility related patterns (e.g. indication of stationary Devices, predictable trajectories of Devices, etc.). **Informational Note:** This information may be used by the Network Operator to optimize resource usage. The relevant use case is found in Appendix B.2.	1.0
ENCapM-HLF-003	An OMA API SHALL enable a third-party to request sending a broadcast message in a specified geographic area expecting to reach a group of Devices that are registered with the third-party. **Informational Note:** The relevant use case is found in Appendix B.3.	1.0
ENCapM-HLF-004	An OMA API SHALL enable a third-party to request setting up data sessions with specified QoS (e.g. low latency or jitter) and priority handling to a Device that is registered with the third-party. **Informational Note:** The relevant use case is found in Appendix B.4.	1.0
ENCapM-HLF-005	An OMA API SHALL enable a third-party to be indicated when a Network Operator finds data transmissions have a risk of incapability to provide expected throughput and/or QoS in a specific area (e.g. due to forecasted high traffic load in that area). Additionally, an estimate may be given when the high traffic load is expected to be mitigated. **Informational Note:** The relevant use case is found in Appendix B.4.	1.0

Label	Description	Release
ENCapM-HLF-006	An OMA API SHALL enable a third-party to be informed/updated about status of a Device that is registered with the third-party. Such status information includes: • Indication of the roaming status (i.e. Roaming and No Roaming) and the serving network, when the Device starts/stops roaming, • Loss of connectivity of the Device, • Change or loss of the association between the Device and the USIM, • Communication failure events of the Device visible to the network (e.g. for troubleshooting). • Reporting when the Device moves in/out of a geographic area that is indicated by the third-party, • Reporting when the Device changes Routing Area / Tracking Area / Location Area / Cell. **Informational Note:** The area indicated by a third-party can be mapped to the area used for mobility management in a mobile network, i.e. a list of LAs/RAs/TAs in the 3GPP network. The third-party can define a geographical area as shapes (e.g. polygons, circles) or civic addresses (streets, districts…) as referenced by OMA Presence API [PresenceAPI_10] e.g. defined by shape areas of IETF RFC-5491 [RFC5491] or by civic addresses defined in IETF RFC-5139 [RCC5139].	1.0
ENCapM-HLF-007	An OMA API SHALL enable a third-party to request a one-time reporting or reporting at regular times on the number of Devices present in a certain area and the location of each Device as for a Location Based Service.	1.0
ENCapM-HLF-007a	An OMA API SHALL enable an application to subscribe to notifications about Device connections properties.	1.0
ENCapM-HLF-008	An OMA API SHALL enable a third-party to be notified about Device's connection properties. **Informational Note:** Connection properties of a Device describe the average data rate range or non-absolute value (e.g. high, medium or low) that the Device is likely to be able to obtain at the current location. The connection properties can, for example, be generated from the RAT type the Device is currently attached to, the load conditions at its current location and/or other parameters.	1.0
ENCapM-HLF-009	An OMA API SHALL enable a third-party to request for background data transfer to Devices that are registered with the third-party, indicating: • the desired time window for the data transfer, • the volume of the data expected to be transferred in a geographic area. **Informational Note:** The geographic area can be coded, for example, as specified by [3GPP TS 23.032].	1.0
ENCapM-HLF-010	An OMA API SHALL enable a third-party to get the information about: • one or more recommended time windows for the data transfer and, • for each time window the maximum aggregated bitrate for the set of Devices in the geographical area indicated by the third-party.	1.0

Label	Description	Release
ENCapM-HLF-011	An OMA API SHALL enable a third-party application to request the Network Operator to trigger Devices to perform application-specific actions, e.g. initiating communications with the third-party **Informational Note:** Triggering is the means by which a third-party sends information to the Device via the Network Operator to trigger the Device to perform application specific actions that include initiating communication with the third-party. This function is required when an IP address for the Device is not available or reachable by the third-party. Refer to [3GPP TS 22.368] and [3GPP TS 23.682] for details in 3GPP. Trigger message contains information that allows the network to route the message to the appropriate Device and the Device to route the message to the appropriate application.	1.0

Table 1: High-Level Functional Requirements

6.1.1 Security

This section captures High-Level Functional Requirements – Security Items.

Label	Description	Release
ENCapM-SEC-001	An OMA API SHALL be able to provide a third-party with secure access to the exposed network services/capabilities.	1.0
ENCapM-SEC-002	It SHALL be ensured that the network services/capabilities are not disclosed to unauthorised parties and that user privacy (avoid e.g. trackable and traceable identity information of the concerned Device) is maintained subject to user agreement, Network Operator Policy, service agreement between Network Operator and third-party and regulation constraints.	1.0

Table 2: High-Level Functional Requirements – Security Items

6.1.1.1 Authentication

Application and user authentication is out of the scope of ENCap-M2M.

6.1.1.2 Authorization

Authorization is out of the scope of ENCap-M2M.

6.1.1.3 Data Integrity

Data Integrity is out of the scope of ENCap-M2M. It MAY rely on a bound protocol.

6.1.1.4 Confidentiality

Confidentiality is out of the scope of ENCap-M2M. It MAY rely on a bound protocol.

6.1.2 Charging

The OMA ENCap-M2M Enabler supports following charging requirements.

Label	Description	Release
ENCapM-CHG-001	An OMA API SHALL permit counting of the Network API invocations.	1.0
ENCapM-CHG-002	The ENCap-M2M Enabler SHALL permit generation of the needed information (e.g. Event Data Record) to properly document the invocation of NetAPI per Application/per third party. **Informational Note:** Charging information is generated for intra-operator use, and also for inter-operator settlements.	1.0

Label	Description	Release
ENCapM-CHG-003	At least the following list of Charging events for Monitoring SHALL be supported: • Monitoring Event configuration request, • Monitoring Event modification request, • Monitoring Event response messages, • Implicit or explicit Monitoring Event deletion request **Informational Note:** This does not exclude the generation of other types of events for other type of network and API functions.	1.0
ENCapM-CHG-004	An OMA API SHALL be able to provide a third-party with chargeable access to the exposed network services/capabilities.	1.0
ENCapM-CHG-005	Regarding ENCapM-HLF-010, the OMA API SHALL enable a third-party to get the information about the charging policy that will be applied to the third-party if the data are transferred within the recommended time window and if transmission rates stay below the limits of the respective maximum aggregated bitrate.	1.0

Table 3: High-Level Functional Requirements – Charging Items

6.1.3 Administration and Configuration

Administration and Configuration is out of the scope of ENCap-M.

6.1.4 Usability

Usability is out of scope of ENCap-M.

6.1.5 Interoperability

Not applicable.

6.1.6 Privacy

Privacy is out of the scope of ENCap-M.

6.2 Overall System Requirements

None.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-RD-ENCap-M-V1_0-20180621-A	21 Jun 2018	Status changed to Approved by ARC Doc Ref # OMA-ARC-2018-0024-INP_ENCap_M2M_V1_0_RRP_for_final_Approval

Appendix B. Use Cases (Informative)

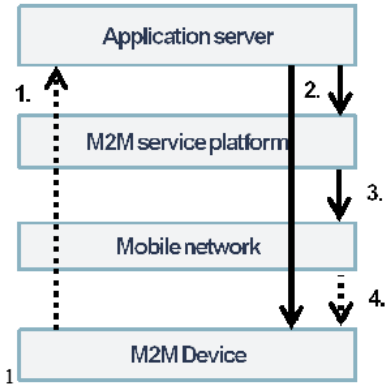
B.1 Optimization of Interworking between M2M applications and Mobile Network through Connectivity Management parameters

B.1.1 Short Description

This use case [oneM2M TS 0002] illustrates the case when changes to the M2M transmission patterns, such as sending of short data packets or frequent changes from active to idle mode or vice versa, are detected by M2M service platform and this information is passed to Mobile network to configure the connectivity parameters accordingly in order to optimize the mobile network utilization by M2M services and reduce the burden on the network.

An example would be when an M2M device has flood level sensor that communicates with the M2M application server via mobile network and the frequency of this communication, (frequently or less frequently), between these M2M entities, volume of data and mode switching, (active or idle), will depend on the level of the flooding situation.

1) The application server checks the measurement data from the M2M device taken by a water level sensor.
2) If the application server detects that the water level approaches the threshold, it sends a request to the M2M device to change the communication mode from normal to abnormal mode and also passes a message to M2M service platform to change the frequency of sending information to 'frequent'.
3) The M2M service platform detects the change of the data transmission interval from infrequent to frequent and passes this information to the mobile network.
4) The mobile network adjusts configuration parameters of the mobile network about the M2M device based on the current data transmission interval of the M2M device if required, e.g. the configuration parameters of a 3GPP network may include the connection keep time (e.g. the inactivity timer, the idle (dormant) timer), the radio reception interval, such as DRX (discontinuous reception) timer) etc.



Source: [oneM2M TR 0001]

Figure 1: Information Flow between Actors
– Connectivity Management Parameters –

B.1.2 Market benefits

A Network Operator will be able to optimize its resources and network capabilities by knowing the M2M communication and data packet transmission pattern. As such, this will reduce the burden on the network and cost, increase the efficiency and improve the revenue for the mobile operators.

On the other side, an M2M Application Provider or M2M Service Provider will be able to use network resources and network capabilities more efficiently and will have the revenue share by being more efficient and not causing network overloading.

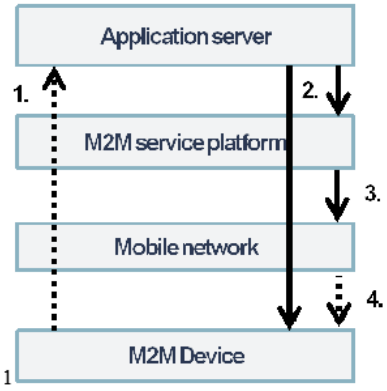
B.2 Optimization of Interworking between M2M and Mobile Network through Mobility Management parameters

B.2.1 Short Description

This use case [oneM2M TS 0002] illustrates the case when information about M2M device mobility characteristics, such as whether an M2M device is static or mobile, the speed it moves if it is mobile, location etc., are detected by M2M service platform and obtained from M2M applications on an M2M device with mobility sensors. This information is passed to Mobile network to configure the mobility parameters in order to allocate network resources accordingly and optimize the mobile network utilization by M2M services and reduce the burden on the network.

An example would be when an M2M device is in a car which one moment can be static, but the next moment is mobile, moving 70 mph. These two states of an M2M device have different requirements for network resources and capabilities and therefore the mobile operator has to interwork with the M2M service platform to have these mobility parameters.

1) The M2M device collects the mobility-related M2M information, e.g. engine is off, from sensors within the vehicle and sends it to the application server.
2) The application server gets the mobility characteristics (e.g. static, on the move, speed of movement etc.) based on the mobility-related M2M information of the M2M device and sends the current mobility characteristics to the M2M service platform.
3) The M2M service platform detects the change of the mobility characteristics and passes this information to the mobile network.
4) The mobile network adjusts configuration parameters of the mobile network based on the current mobility characteristics of the M2M device if required. These parameters include the location registration, traffic area where these M2M devices operate etc.



Source: [oneM2M TR 0001]

Figure 2: Information Flow between Actors
– Mobility Management Parameters –

B.2.2 Market Benefits

A Network Operator will be able to optimize its resources and network capabilities by having more information about M2M device mobility and location. As such, this will reduce the burden on the network and cost, increase the efficiency and improve the revenue for the mobile operators.

On the other side, an M2M Application Provider or M2M Service Provider will be able to use network resources and capabilities more efficiently and will have the revenue share by being more efficient and not causing network overloading unnecessarily.

B.3 Leveraging Broadcasting/ Multicasting Capabilities of Underlying Networks

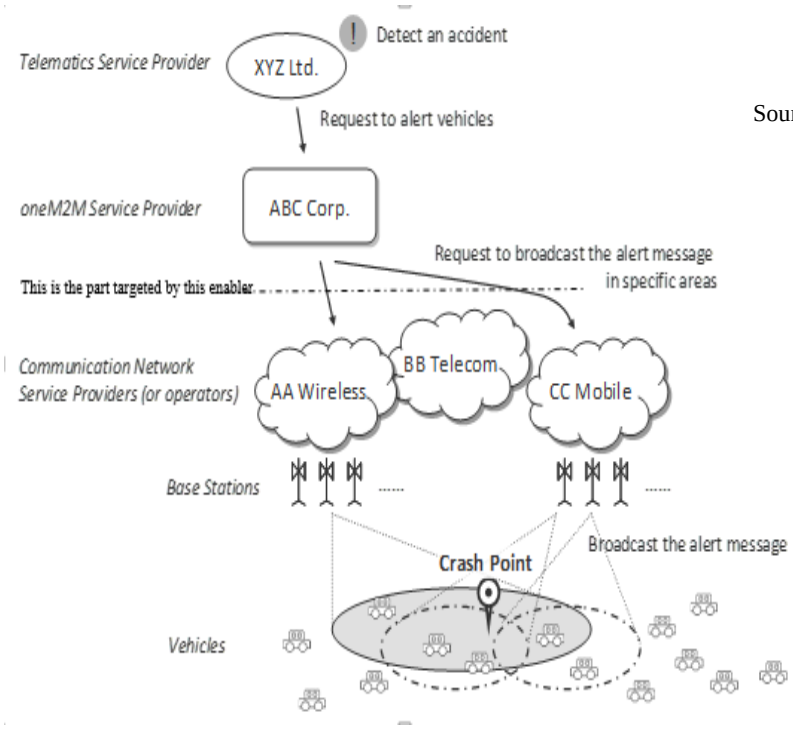
B.3.1 Short Description

This use case [oneM2M TS 0002] illustrates the case when mobile network broadcast/multicast capabilities are used by automotive telematics services to alert other road users or other vehicles of an accident in order to avoid more accidents or to avoid traffic jams.

By using these mobile network capabilities, automotive telematics services can alert vehicles within a specific area. To achieve this, automotive telematics services need to select the relevant vehicles that should receive alert messages based on their registered location, which requires continuous location management of vehicles. Moreover, the underlying communication network has to route large number of unicast messages with very short delay.

Other similar scenarios supported by this use case can be neighbourhood burglar alarm system that alerts the neighbours in case of a break-in and water delivery system monitoring that alerts water customers about bursts of water pipes.

1) A sensor in the car, as part of Telematics Service Provider, detects an accident and Telematics Service Provider requests from M2M Service Provider to alert other vehicles in the area or heading towards the area where the accident happened
2) M2M service provider sends a request to service providers/mobile operators to alert subscribed vehicles in the specified area using mobile network broadcast/multicast service
    - The request contains the payload to be delivered to vehicles, which for example can contain the alert level, e.g. serious and urgent, location and time of the accident, and a message to drivers in that specific area to slow down or change the route in case of traffic jam;
    - The request from the M2M service provider also contains information about targeted receivers and about specific area, e.g. area to be covered, the type of devices to be alerted, the option whether the alerting should be repeated, the repetition interval, and stopping conditions.
3) Upon the reception of this request, the mobile operator authenticates the M2M service provider and authorizes the request
4) Mobile operator delivers the message to targeted receivers using broadcast/multicast service on behalf of M2M service provider



Source: [oneM2M TR 0001]

Figure 3: Information Flow between Actors – Message Broadcast –

B.3.2 Market Benefits

M2M Service Provider will be able to use underlying network resources and capabilities more efficiently and will be able to deliver its services to subscribers and other participants in timely manner and based on specific geographic locations.

On the other hand, mobile operators will be able to increase the usability of broadcast and multicast services and as such increase the revenue share.

B.4 M2M Data Traffic Management by Underlying Network Operator

B.4.1 Short Description

This use case [oneM2M TS 0002] illustrates the case when underlying network and M2M entities (e.g., M2M service platform, M2M application servers, and M2M devices) interact to avoid loss of M2M traffic based on the data traffic condition (e.g. current traffic congestion status) provided by information of underlying network.

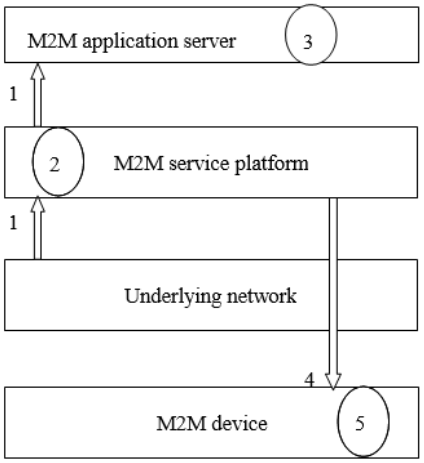
Based on this information, the underlying network operators (e.g. mobile network operators) try to manage the M2M data traffic in their networks in conjunction with M2M entities in order to avoid losing the M2M communication data packets in the networks.

The M2M service platform and/or M2M application servers will react upon the reception of this information from the mobile operator by changing their configurations, such as changing data transmission schedules or suspension of sending data over the underlying networks for some time.

1) The mobile network sends the data traffic condition information to the M2M service platform.
2) After the M2M service platform receives the data traffic condition information from the mobile operator, it forwards this information to the M2M application server.
3) After the M2M application server receives the information from the M2M service platform it starts controlling M2M data transmission.

4) After the M2M service platform receives the data traffic condition information from the underlying network in step 1, it may send M2M data transmission configuration information to the M2M device.

5) After the M2M device may receive M2M data transmission configuration information from the M2M service platform, it may control M2M data transmissions accordingly.



Source: [oneM2M TR 0001]

Figure 4: Information Flow between Actors – Data Traffic Management –

B.4.2 Market Benefits

A Network Operator will be able to monitor and manage the M2M data traffic over its network more efficiently to prevent potential traffic congestion and any impact on network performance. As such, the mobile operator will keep the network up and running, increase the efficiency and improve the revenue.

On the other side, an M2M Application Provider or M2M Service Provider will be able to use network resources and capabilities more efficiently and will have the revenue share by coordinating the efforts with mobile operators to better control the M2M data traffic and not causing network overloading unnecessarily.

Appendix C. Gap Analysis (Informative)

The idea of this annex is to look at existing Network APIs that have been specified by OMA in the past many years and to analyse their usability in the context of ENCap-M2M.

This gap analysis will also be used to see if additional work is needed and tries to identify new APIs that would be required to address the ENCap-M2M requirements.

C.1 Inventory of OMA Network APIs

The link below provides a repository of OMA APIs developed so far. These OMA APIs expose fundamental capabilities such as SMS, MMS, Location Services, Payment and other core network assets in a standardized way.

http://technical.openmobilealliance.org/Technical/technical-information/oma-api-program/oma-api-inventory

C.2 Analysis of requirements vs. existing OMA RESTful APIs

This section analyses the coverage of existing OMA Network RESTful APIs for each ENCap-M requirement. The idea here is to list most relevant APIs and related description.

High Level Requirement/Exposing network capability	Relevant OMA RESTful Network API	Further work required	Comments
ENCapM-HLF-001	Not found	A new API is needed to address predictable communication patterns.	New API to be proposed
ENCapM-HLF-002	Not found	A new API is needed to address the predictable communication pattern	The suggested API above can be also used for this requirement.
ENCapM-HLF-003	SOAP API for message broadcast	A new RESTful API for broadcasting messages is needed	There is a SOAP API for message broadcast that can be REST-ified if required. There is another API, Messaging API that supported sending messages from 1-unlimited users where the address is a mandatory parameter. To check what oneM2M wants
ENCapM-HLF-004	RESTful Network API for Quality of Service 1.0	More work may be needed for this requirement	Current QoS 1.0 API only supports bandwidth adaptation during an ongoing call
ENCapM-HLF-005	RESTful Network API for Quality of Service 1.0	More work may be needed for this requirement	Existing API does not support this requirement
ENCapM-HLF-006	RESTful Network API for Terminal Status 1.0 RESTful Network API for Terminal Location 1.0 RESTful Network API for Presence 1.0	New resources may be needed, in RESTful Network API for Terminal Status, to address reporting when the Device changes Routing Area / Tracking Area / Location Area / Cell.	The requirement is not fully but partially covered by the existing APIs. The capability is missing to address reporting when the Device changes Routing Area / Tracking Area / Location Area / Cell.

ENCapM-HLF-007	RESTful Network API for Terminal Location 1.0	A new API may be needed to address the reporting on a number of Devices present in a certain area.	The requirement is not fully but partially covered by the existing API. The capability is missing to address the number of Devices present in a certain area. With the existing terminal location 1.0 API you can't specify the number of devices in a specific area ZonalPresence can also be considered for this.
ENCapM-HLF-008	Notification Channel 1.0	A new API may be needed to address Device's connection properties.	RESTful Network API for Notification Channel 1.0 may be reused by a new API. The same API as for requirements for HLF-001/002 could be used or a new API may be needed
ENCapM-HLF-009	Not found	A new API is needed to address background data transfer.	If needed, Notification Channel 1.0 may be extended to enhance the requirement fully.
ENCapM-HLF-010	RESTful Network API for Quality of Service 1.0	More work is needed in this case since this requirement is addressed partly only.	QoS API can be used to define the maximum aggregated bitrate for the set of Devices
ENCapM-HLF-011	Not found	A new API is needed to address Device Triggering.	It can be confirmed that a new API is needed for this requirement.
ENCapM-SEC-001	N/A	No further work is needed.	The existing architecture and security mechanisms can be applied.
ENCapM-SEC-002	Autho4API_10	No further work is needed at this stage	This requirement can be supported by OMA Authorization Framework for Network APIs [Autho4API_10] since the main requirement here is to prevent access of unauthorized parties to network resources/capabilities.
ENCapM-CHG-001/002/003	N/A	Further study may be needed to ensure the support of this requirement.	These three requirements are not to support new APIs. They require certain features, capabilities and formats to be supported if a RESTful API is used

NCapM-CHG-004/5	N/A	Further study may be needed to ensure the support of this requirement.	These two requirements are not to support new APIs. They require certain features, capabilities and formats to be supported if a RESTful API is used

C.3 Summary

This section provides a summary and a conclusion of the findings about new and existing APIs needed to address ENCap-M2M requirements. In addition, this section also provides the APIs that are being proposed to be developed in the next phase of the ENCap-M2M work.

Upon completion of this Gap Analysis, it can be concluded that new APIs are needed to address most of the requirements to support exposure of network capabilities to M2M.

The table in section C.2 identifies some of the existing APIs and suggests some new APIs to perform specific tasks as defined by the ENCap-M2M requirements, but the given list is not an exhausted list and can serve as a guide for potential new work items only.

Overall, there were identified 8 new APIs that OMA members would need to consider in future in order to enrich the OMA API portfolio and enhance network capability exposure. There were 5 existing APIs that could partly or fully be used to address some of the ENCap-M2M requirements.