|  |  |
| --- | --- |
| Input Contribution | |
| Meeting ID\* | SEC#35 |
| Title:\* | Discussion on Multicast Security |
| Source:\* | Wolfgang Granzow, Qualcomm, [wgranzow@qti.qualcomm.com](mailto:wgranzow@qti.qualcomm.com)  Phil Hawkes, Qualcomm, [phawkes@qti.qualcomm.com](mailto:phawkes@qti.qualcomm.com) |
| Uploaded Date:\* | 2018-05-21 |
| Document(s)  Impacted\* | TS-0003v3\_8\_0 and possibly TS-0001, TS-0004 and TS-0008 for Rel-3. |
| Intended purpose of  document:\* | Decision  Discussion  Information  Other <specify> |
| Decision requested or recommendation:\* | Decide how to address Multicast Security in Rel-3 |
| Template Version:23 February 2015 (Do not modify) | |

**oneM2M Notice**

The document to which this cover statement is attached is submitted to oneM2M. Participation in, or attendance at, any activity of oneM2M, constitutes acceptance of and agreement to be bound by terms of the Working Procedures and the Partnership Agreement, including the Intellectual Property Rights (IPR) Principles Governing oneM2M Work found in Annex 1 of the Partnership Agreement.

# 1 Background

This contribution addresses a discussion and Action Item in the PRO WG about the introduction of normative Annex B “Multicast group fan out procedure” into TS-0008v3\_1\_0 (CoAP protocol binding) which was agreed at the PRO#34 meeting.

Clause B.1 “Security” of TS-0008v3\_1\_0 states:

The multicast group fan out messages shall only be carried in UDP, not in DTLS. This means that the security modes defined for CoAP in this document are not applicable to multicast.

Clearly DTLS is not applicable when using CoAP for group communication over IP Multicast or 3GPP MBMS, as defined in RFC 7390 “Group Communication for the Constrained Application Protocol (CoAP)” [1]. However, the text highlighted above contradicts with what is stated in the Security Specification TS-0003:

On the Mca and Mcc reference points, security association establishment between a field domain AE or CSE, respectively, and an IN-CSE is mandatory.

On the Mcc' reference point, security association establishment between IN-CSE and IN-CSE is mandatory.

On the Mca reference point, security association establishment between AE and the CSE in the field domain is strongly recommended.

NOTE: Security Association Establishment on the Mca interface in a local domain is optional depending on risk assessment, for instance in scenarios where unauthorized access can be prevented by other security measures out of scope of the present document. This includes the following use cases:

* AE and CSE (i.e. Mca end-points) are securely integrated on the same physical device (i.e. an ASN).
* Secure communication is guaranteed by the Underlying Network (e.g. WLAN or VPN).
* Mca communication takes place on a wire (e.g. Ethernet) in a safe physical environment.

The purpose of this contribution is to trigger a discussion and decision if oneM2M wants to allow unsecured communication on the Mcc reference point when employing the multicast group fan out procedure, or how this issue can be resolved in the specifications for Release-3.

# 2 Multicast Security

## 2.1 CoAP group communication

Clause 5 “Security considerations” of RFC 7390 states the following:

… there is currently no security at the CoAP layer for group communication. Therefore, for sensitive and mission-critical applications (e.g., health monitoring systems and alarm monitoring systems), it is currently recommended to

deploy CoAP group communication with an application-layer security mechanism (e.g., data object security) for improved security. Application-level security has many desirable properties, including maintaining security properties while forwarding traffic through intermediaries (proxies). Application-level security also tends to more cleanly separate security from the dynamics of group membership (e.g., the problem of distributing security keys across large groups

with many members that come and go. Without application-layer security, CoAP group communication should only be currently deployed in non-critical applications (e.g., readonly temperature sensors). Only when security solutions at the CoAP layer are mature enough (see Section 5.3.3) should CoAP group

communication without application-layer security be considered for sensitive and mission-critical applications.

Clause 5.3.3 “Future Evolution” of RFC 7390 referenced above refers to ongoing IETF efforts to develop DTLS-based group communication [2], or alternatively, to use IPsec-based IP multicast security [3].

End-to-End Security of Primitives (ESPrim) defined in oneM2M TS-0003 represents a kind of object security which however currently is specified for unicast communications only.

The current ESPrim mechanism however could serve as basis for development of an object security mechanism suitable for CoAP group communication.

## 2.2 3GPP MBMS security

The 3GPP MBMS architecture is defined in 3GPP TS 23.246. Figure 1 shows the MPMS architecture for the Enhanced Packet Core (EPC) which allows MBMS broadcast only.

The BM-SC may be collocated with the MBMS-GW. The network bearer management decides whether to apply IP multicast distribution between MBMS-GW and NB/eNB, and down to the UE on the radio bearer, or whether to employ unicast transmission.



Figure 1: 3GPP MBMS reference architecture for the EPC (MBMS broadcast only) [3GPP TS 23.246]

The security architecture for 3GPP MBMS is defined in 3GPP TS 33.246. The 3GPP security architecture provides a method of authentication, key distribution and data protection for MBMS User Service. TS 33.220 Generic Bootstrapping Architecture (GBA) is used to agree the keys that are needed to run an MBMS User Service.

Encryption and integrity protection is performed for the bearers between BM-SC and UE.

## 2.3 IP Multicast security

When using IP Multicast in a plain IP network, security may be provided on the network layer as extensions to IPSec [4] as specified in RFC 5374 [5].

There is furthermore a aeries of specifications issued by IETF MSec group (<https://datatracker.ietf.org/wg/msec/about/>), e.g. RFC 3740 (The Multicast Group Security Architecture) [6] and RFC 6407 (Group Domain of Interpretation) [7].

The Multicast Group Security reference architecture [6] features of three functional areas

* Multicast security policy management
* Group Key Management
* Multicast data handling (includes group authentication, data encryption, data integrity protection)

None of these functions are currently addressed in oneM2M TS-0003.

# 3 Architecture issues related to multicast

The recent introduction of multicast group fanout procedures into TS-0001 and TS-0004 represents a major addition to the oneM2M communication paradigm.

In this procedure, multicast may be employed when an operation (CRUD request) on a <fanOutPoint> virtual resource is performed where its parent <group> resource also has <localMulticastGroup> children assigned which identifies “multicast capable” CSEs.

The CSE which hosts the <group> resource (parent of <fanOutPoint> addressed in the CRUD request) is denoted *Group Hosting CSE* in this context. The CSE which hosts a <localMulticastGroup> resource is denoted *as Member Hosting CSE*. A Member Hosting CSE is hosting the resources to which the issued CRUD request applies.

According to clause 10.2.7.13.1 of TS-0001v3\_11\_0, “if at least two Member Hosting CSEs support the same multicast capability (i.e. MBMS or IP Multicast), the Group Hosting CSE determines to create multicast group, and performs all the actions: assign the multicast type based on the multicast capability, and allocate multicast address and multicast address type to the member resources of the multicast group”.

For IP multicast, the underlying network associated with the Group Hosting CSE requires multicast capability. Multicast capability aspects related to a Group Hosting CSE do not seem to be addressed in TS-0001 at all. It likely requires addition of a *multicastCapability* attribute to the <*CSEBase*> resource type.

A Group Hosting CSE acts as transmitter of request primitives sent to a multicast address. It receives response primitives in unicast mode from each involved Member Hosting CSE.

A Member Hosting CSE acts as receiver of request primitives arriving on a multicast address. It transmits response primitives in unicast mode to the Group Hosting CSE.

There are rather different requirements which apply to multicast transmitters (Group Hosting CSE) compared to multicast receivers (Member Hosting CSE). These aspects should be addressed in TS-0001.

TS-0001 presently does not define any applicable mapping of these types of CSEs onto the 3GPP MBMS architecture. To some extent this is touched in TS-0026 (3GPP Interworking). The relation of multicast functionality to the Mcc interface is not defined anywhere yet.

There are a number of limitations, which are likely different depending whether MBMS or IP Multicast technology is employed, such as, e.g.

* For 3GPP based MBMS:
  + Group Hosting CSE must be an IN-CSE in order to provide an interface to a Broadcast/Multicast Service Center (BM-SC)
  + Member Hosting CSEs corresponds to a UE
* For IP Multicast
  + In general, in case WAN communication assumed, a Group Hosting CSE must have access to an IP Multicast capable backbone (e.g. Mbone).
  + Member Hosting CSEs corresponds to a oneM2M field node

The mapping of oneM2M entities onto the 3GPP MBMS architecture 3GPP TS-23.246 and IP Multicast Architecture needs to be defined in TS-0001 before a security architecture for multicast on the oneM2M service layer can be developed.

# 4 Conclusions

From the above discussion we propose the following way for a´ward for Rel-3 and Rel-4:

* For Rel-3,
  + for multicast group fanout based on 3GPP MBMS,
    - add text to TS-0003 (and TS-0001?) that no security mechanism is defined on the oneM2M Service Layer (on Mcc reference point), and 3GPP MBMS security as defined in 3GPP TS 33.246 is employed
    - add also text stating that security between the Group Hosting CSE and the BM-SC is not defined for Rel-3.
    - Include a reference into TS-0008 to the section in TS-0003 that includes this new text
  + for multicast group fanout based on IP multicast,
    - include a statement/disclaimer into TS-0003 (and TS-0001?) that IP multicast should be used only with network layer or link layer security below the oneM2M Service Layer.
* For Rel-4,
  + extend the specification of the ESPrim mechanism to become generally applicable to group communication
  + this includes specification of group security association mechanisms and likely extensions to MAF and MEF procedures for management and provisioning of group credentials.

## **References:**

[1] RFC 7390, “Group Communication for the Constrained Application Protocol (CoAP)”

[2] Keoh, S., Kumar, S., Garcia-Morchon, O., Dijk, E., and A. Rahman, "DTLS-based Multicast Security in Constrained Environments", Work in Progress, draft-keoh-dicemulticast-security-08, July 2014.

[3] Migault, D. and C. Bormann, "IPsec/ESP for Application Payload", Work in Progress, draft-mglt-dice-ipsec-forapplication- payload-00, July 2014.

[4] RFC 4301, “Security Architecture for the Internet Protocol”

[5] RFC 5374, “Multicast Extensions to the Security Architecture for the Internet Protocol”

[6] RFC 3740 The Multicast Group Security Architecture

[7] RFC 6407 Group Domain of Interpretation (GDOI)