OneM2M 개요 및 보안

부산대학교 최종석

2015.11.11

목차

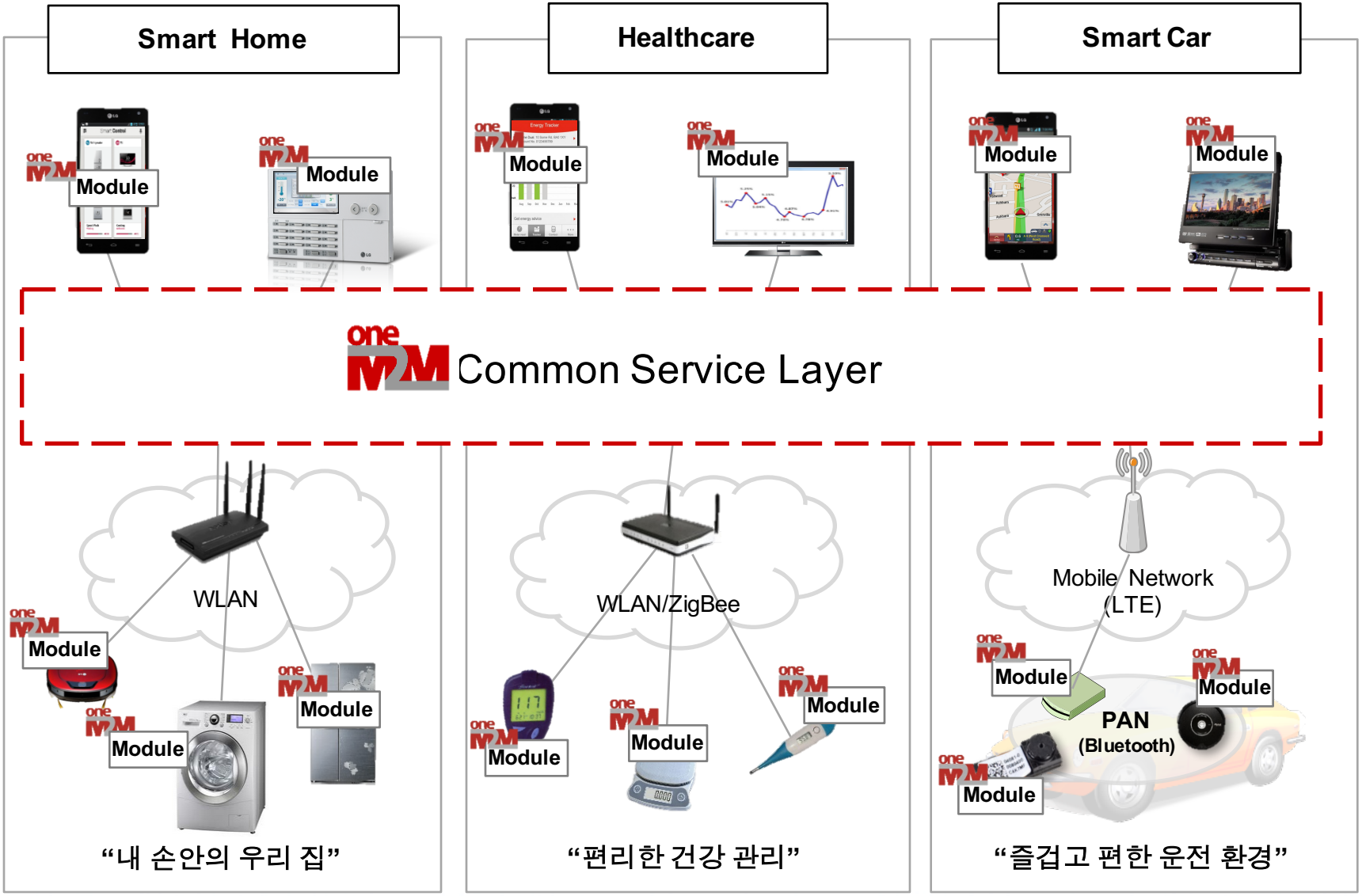
OneM2M 개요 및 보안

I. Introduction of OneM2M

1. Introduction
2. Detailed of CSE

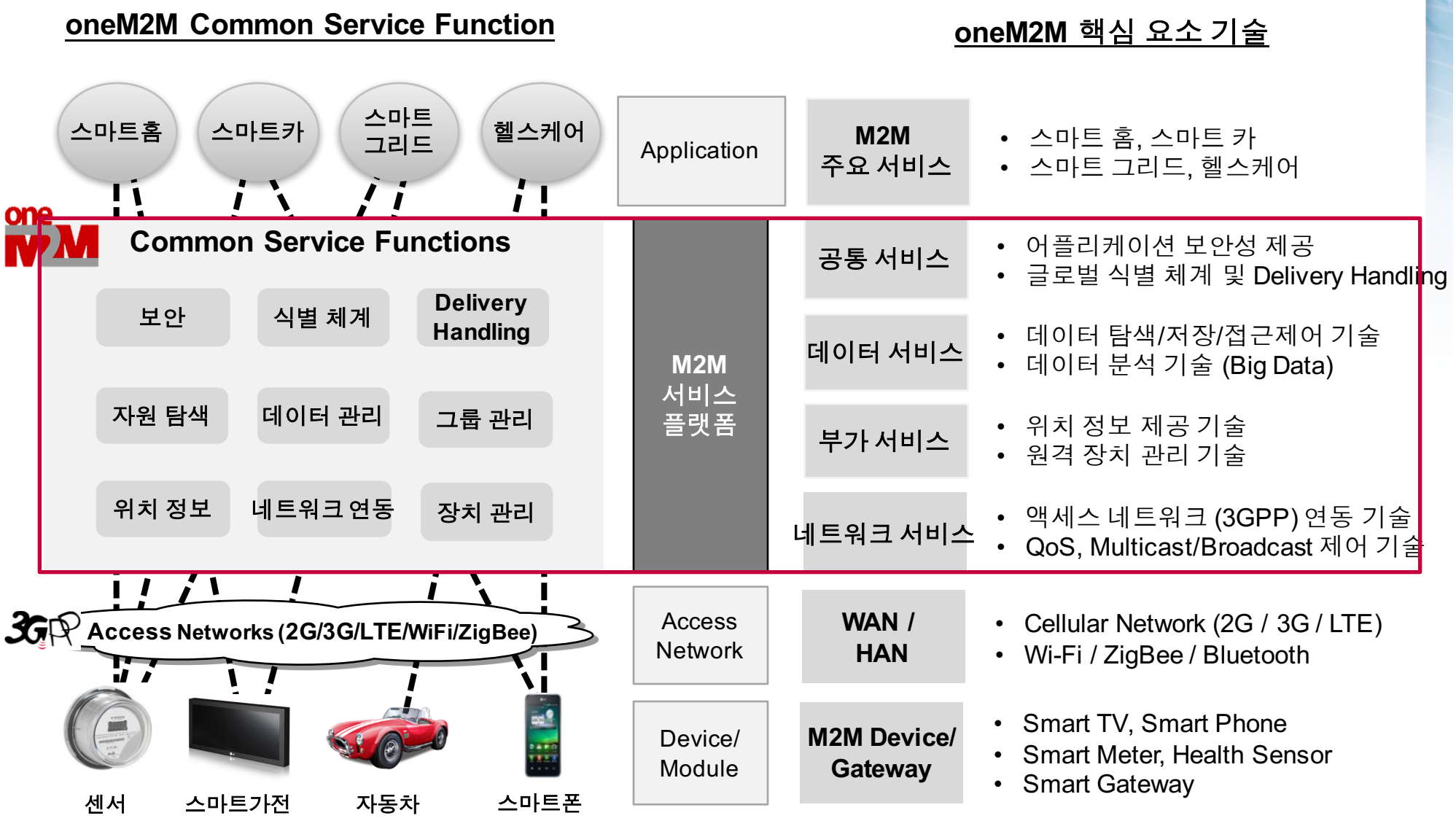
IoT 플랫폼 보안 - OneM2M 플랫폼

oneM2M 기술은 다양한 제품간 연결성을 바탕으로 새로운 제품 및 서비스로 손쉽게 확장 가능



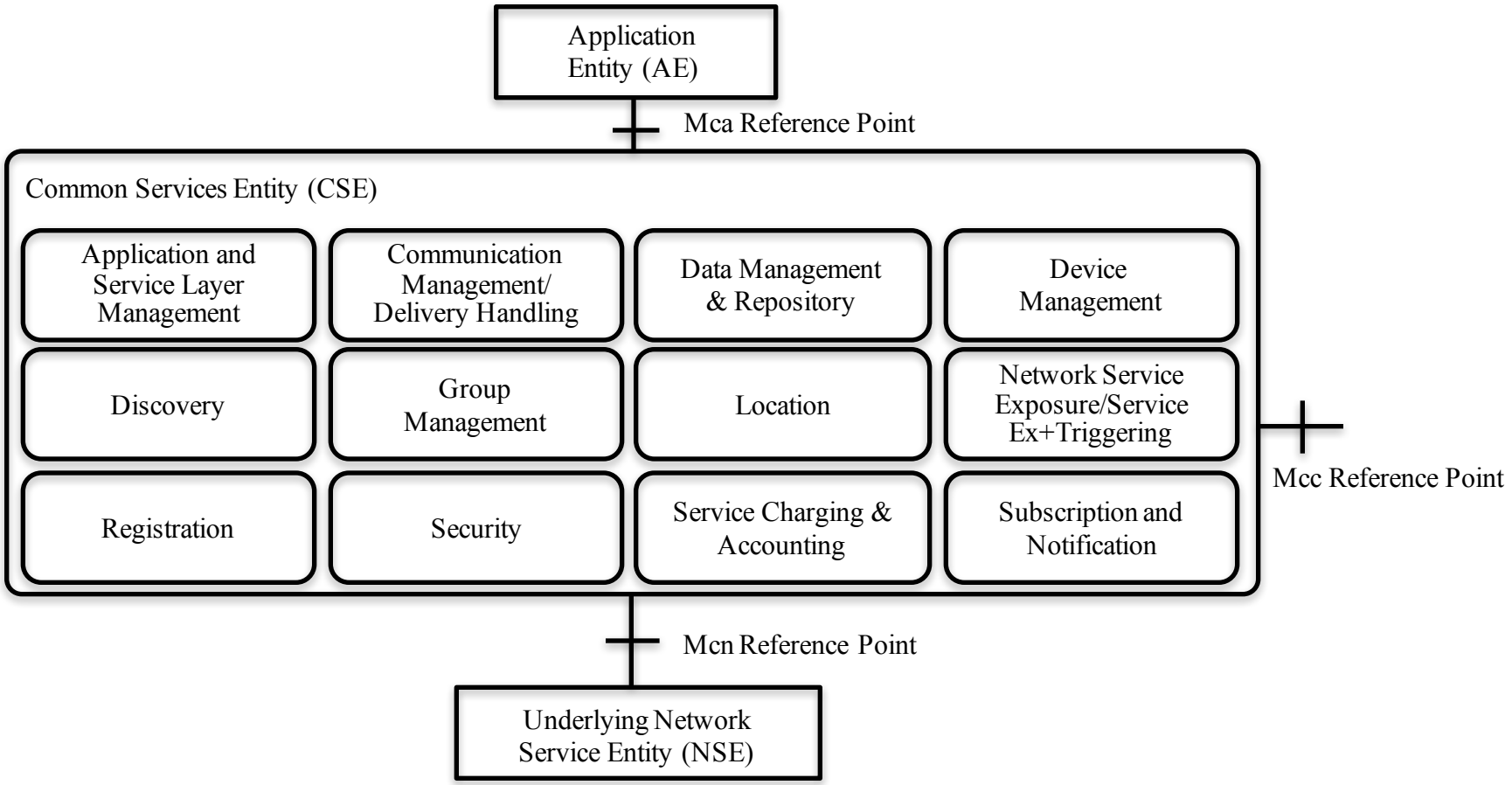
"플랫폼 공통화 → 고객의 가치 창조하는 새로운 **M2M** 서비스 창출 가능"

IoT 플랫폼 보안 - OneM2M 플랫폼



Common Service Functions

The services provided by the Common Services Layer in the M2M System.
Reside within a CSE and are referred to as Common Services Functions (CSFs).

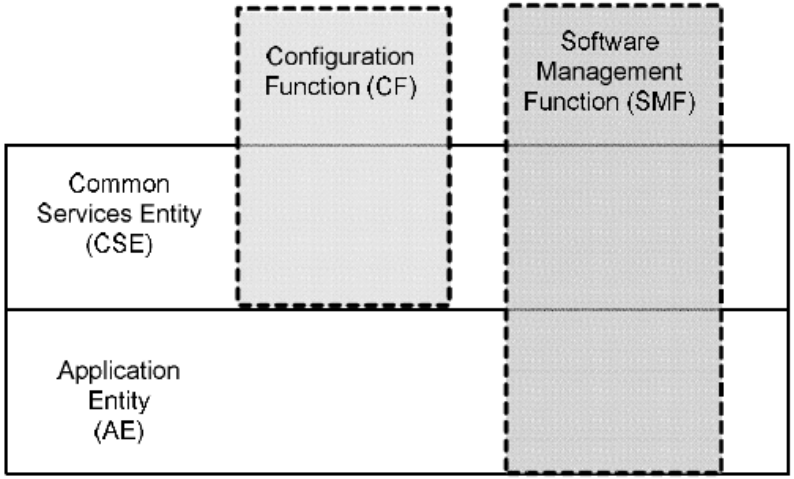


The CSFs provide services to the AEs via the Mca Reference Point and to other CSEs via Mcc reference point.
CSEs interact with the NSE via the Mcn reference point.

Common Service Functions - ASM

Application and Service Layer Management(ASM)

The ASM CSF provides management capabilities for CSEs and AEs.
This includes capabilities to configure, troubleshoot and upgrade the functions of the CSE, as well as to upgrade the AEs.



The management functions include :

- **Configuration Function (CF)**: This function enables the **configuration of the capabilities and features of the CSE**.
- **Software Management Function (SMF)**: This function provides **lifecycle management for software components** and **associated artifacts** (e.g. configuration files) for different entities such as CSE and AE.

Common Service Functions - CMDH, DMR

The Communication Management and Delivery Handling (CMDH)

- The CMDH CSF provides communications with other CSEs, AEs and NSEs.
- The CMDH CSF decides at what time to use which communication connection for delivering communications and, when needed and allowed, to buffer communication requests so that they can be forwarded at a later time. This processing in the CMDH CSF is carried out per the provisioned CMDH policies and delivery handling parameters that can be specific to each request for communication.

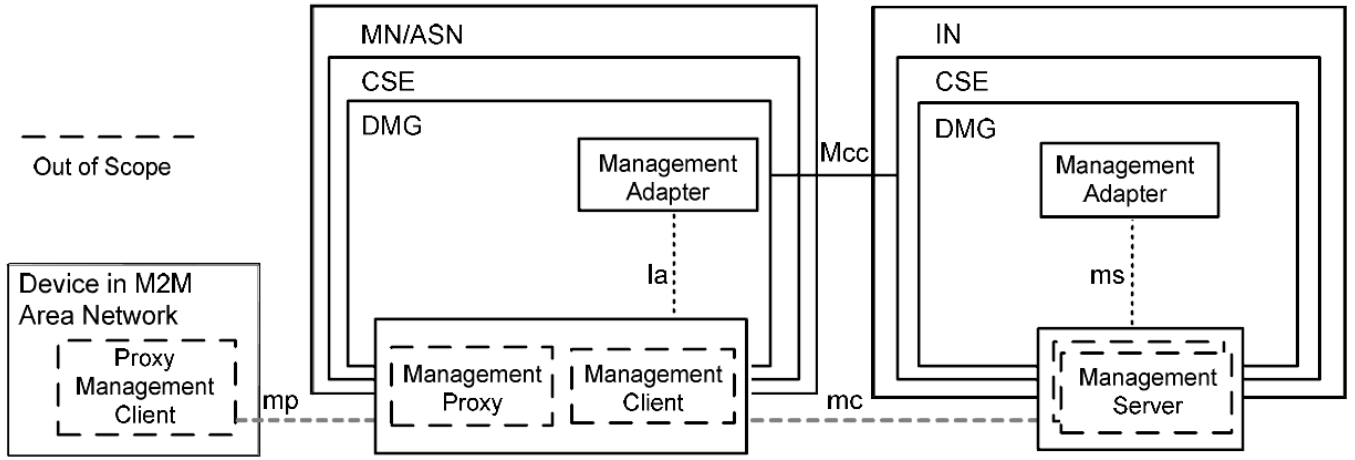
Data Management and Repository (DMR)

- DMR CSF is responsible for providing data storage and mediation functions.
- Ability to store data in an organized fashion so it is discernible.
- Provides the means to aggregate data received from different entities.
- Ability to grant access to data from remote CSEs and AEs based on defined access control policies, and trigger data processing based on data access.
- Ability to provide the means to perform data analytics on large amount of data to allow service providers to provide value-added services.

Common Service Functions - DMG

Device Management (DMG)

- The DMG CSF provides management of device capabilities on MNs (e.g. M2M Gateways), ASNs and ADNs (e.g. M2M Devices), as well as devices that reside within an M2M Area Network.



Discovery (DIG)

- The DIS CSF searches information about applications and services as contained in attributes and resources.

Common Service Functions - DIS, GMG, LOC

Discovery (DIG)

- The DIS CSF searches information about applications and services as contained in attributes and resources.
- The result of a discovery request from an Originator depends upon the filter criteria(e.g. a combination of keywords, identifiers, location and semantic information) and is subject to access control policy allowed by M2M Service Subscription.

Group Management (GMG)

- The GMG CSF is responsible for handling group related requests.
- The GMG CSF enables the M2M System to perform bulk operations on multiple devices, applications or resources that are part of a group. In addition, the GMG CSF supports bulk operations to multiple resources of interest and aggregates the results.

Location (LOC)

- The Location (LOC) CSF allows AEs to obtain geographical location information of Nodes (e.g. ASN, MN) for location-based services.

Common Service Functions - NSSE, REG, SEC

Network Service Exposure, Service Execution and Triggering (NSSE)

- The NSSE CSF manages communication with the Underlying Networks for obtaining network service functions on behalf of other CSFs, remote CSEs or AEs.
- The NSSE CSF uses the Mcn reference point for communicating with the Underlying Networks.

Registration (REG)

- The Registration (REG) CSF processes a request from an AE or another CSE to register with a Registrar CSE in order to allow the registered entities to use the services offered by the Registrar CSE.

Security (SEC)

The Security (SEC) CSF comprises the following functionalities:

- Sensitive data handling
- Security administration
- Security association establishment
- Access control including identification, authentication and authorization
- Identity management

Common Service Functions - SCA, SUB

Service Charging and Accounting (SCA)

- The Service Charging and Accounting (SCA) CSF provides charging functions for the Service Layer.
- The SCA CSF performs information recording corresponding to a chargeable event based on the configured charging policies.
- The SCA CSF sends the charging information transformed from the specific recorded information to the billing domain by the use of a standard or proprietary interface for charging purposes.

Subscription and Notification (SUB)

- The SUB CSF manages subscriptions to resources, subject to access control policies, and sends corresponding notifications to the address(es) where the resource subscribers want to receive them.

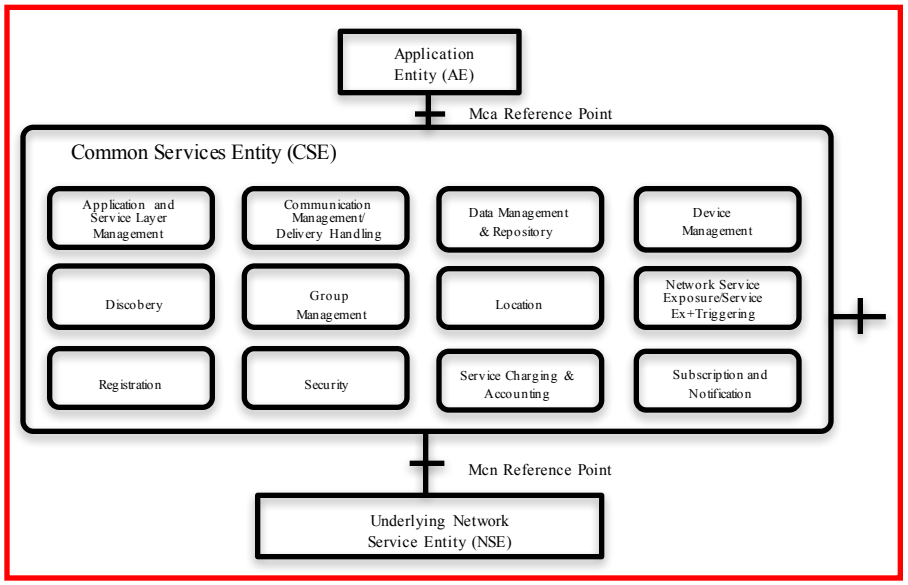
II. OneM2M Security

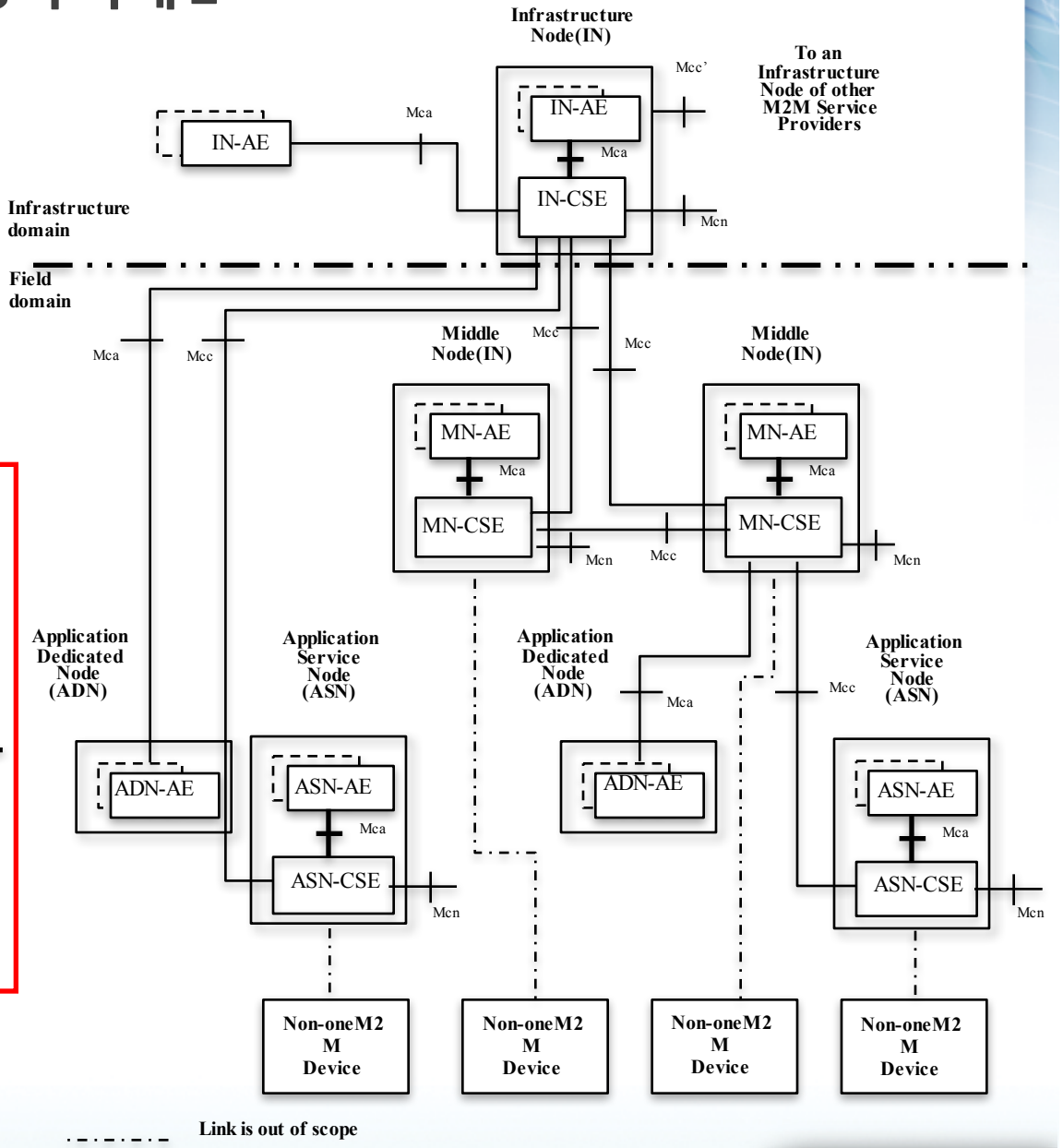
1. Security Framework
2. Security Procedures

IoT 플랫폼 보안

사물인터넷 플랫폼 보안 기술 정의 사례 2

- OneM2M 보안 기술
  - Privacy/Trust 관리 기술
  - 인증/인가 기술
  - 안전한 데이터 전송 기술
  - 시스템 보안 기술
  - Security Association 기술

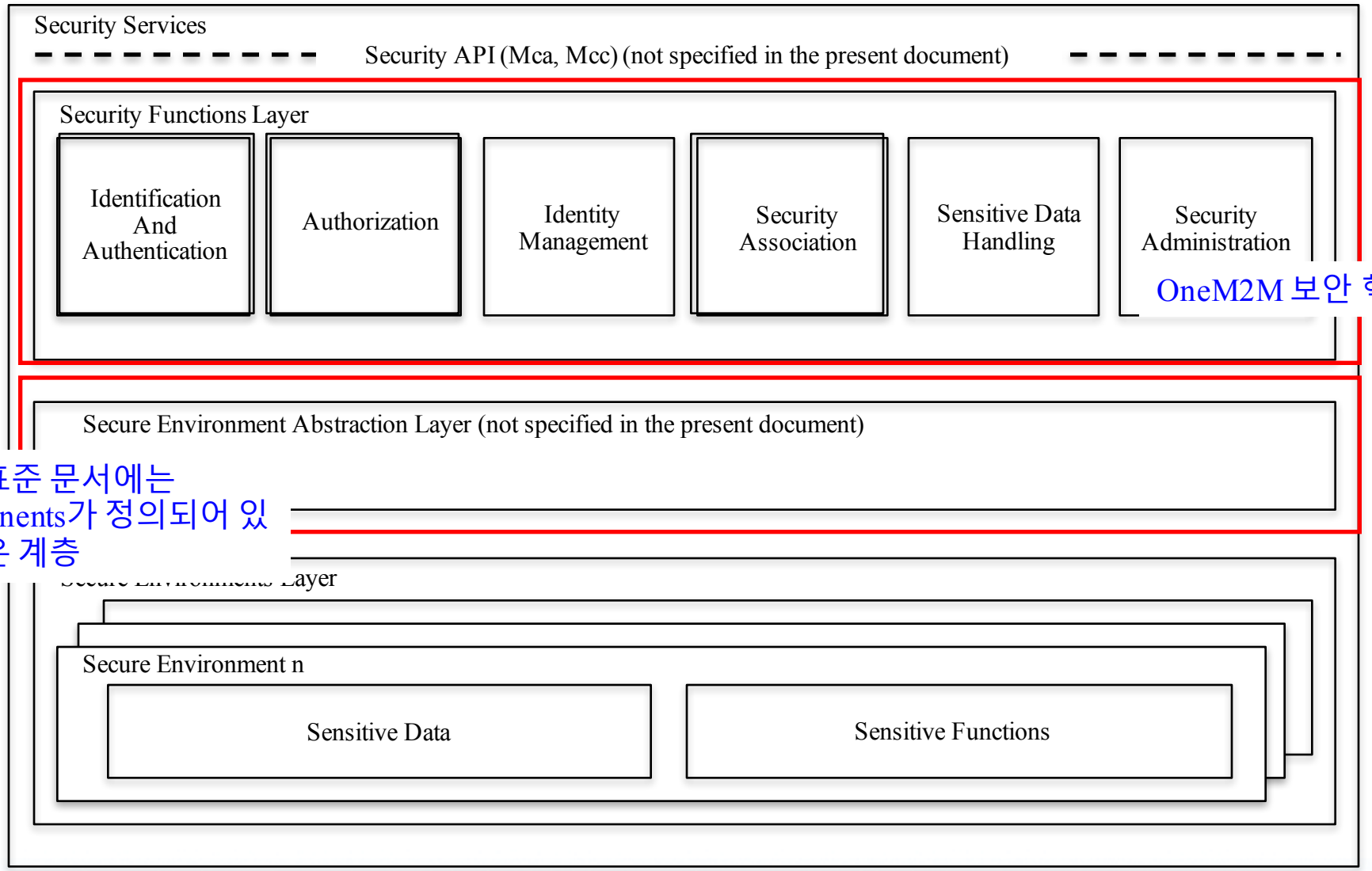




IoT 플랫폼 보안

사물인터넷 플랫폼 보안 기술 정의 사례 3

▪ OneM2M Security Architecture



OneM2M 보안 핵심계층

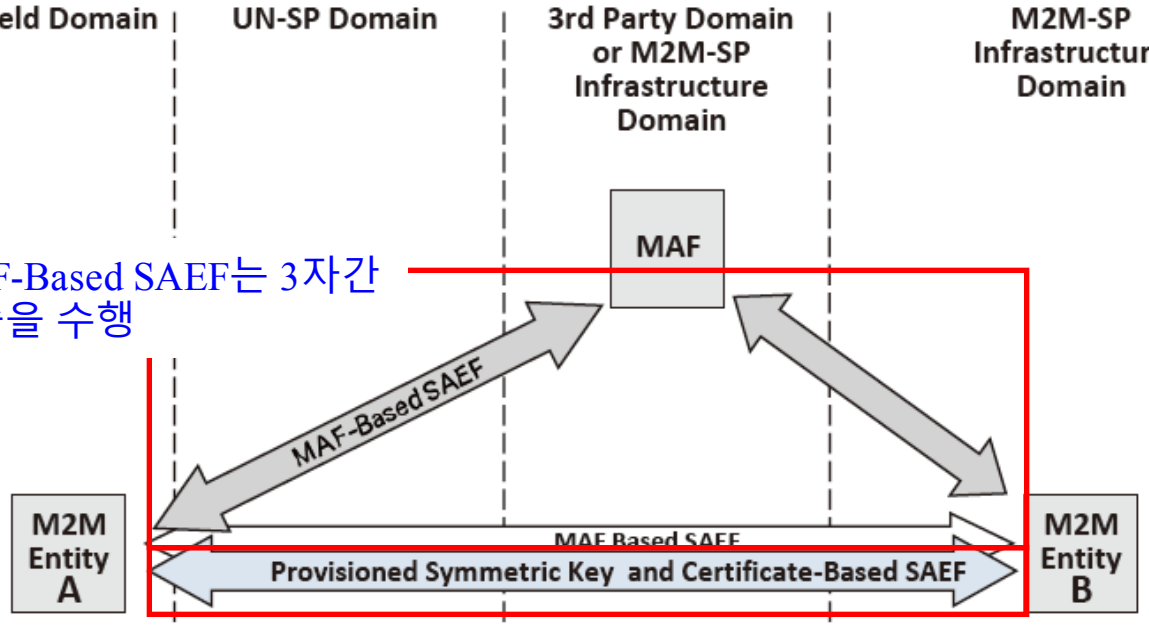
현재 표준 문서에는 components가 정의되어 있지 않은 계층

IoT 플랫폼 보안

OneM2M Security Functions Layer

▪ Authentication

- UN-SP : Underlying Network Service provider
- GBA : Generic Bootstrapping Architecture
- MEF : M2M enrolment function
- BSF : Bootstrap service function
- MAF : m2m authentication function
- RSPF : remote security provisioning framework
- SAEF : security association establishment framework



MAF-Based SAEF는 3자간 인증을 수행

Certificate-Based SAEF와 Symmetric Key-Based SAEF는 Entity 간의 인증을 수행

셋 중에 하나 사용

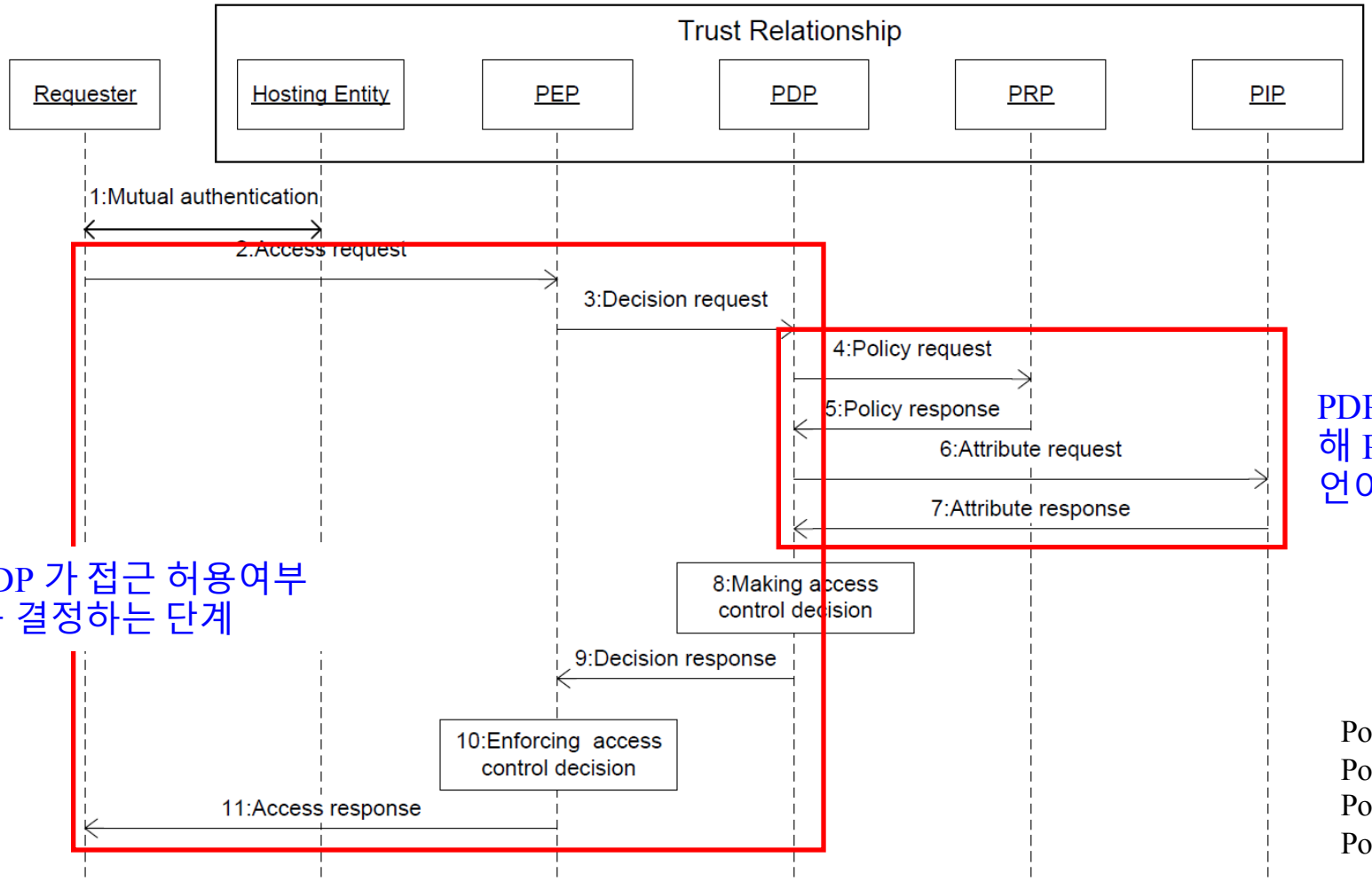
① Provisioned Symmetric Key Security Association Establishment Framework
   - ✓ 미리 제공된 대칭키를 이용하여 end-points간의 association 진행

② Certificate-Based Security security Association Establishment Framework
   - ✓ 개인 서명키와 인증서, 공개키를 이용하여 association

③ MAF Security security Association Establishment Framework
   - ✓ 3rd party service provider에 의해서 진행됨

OneM2M Security Functions Layer

▪ Authorization Procedure



PDP 가 인가를 하기 위해 PRP,PIP에게 정보를 언어오는 단계

PDP 가 접근 허용여부를 결정하는 단계

Policy Enforcement Point(PEP)
Policy Decision Point(PDP)
Policy Retrieval Point(PRP)
Policy Information Point(PIP)

OneM2M Security Framework

- General Introductions to the Security Frameworks
  - the Symmetric Key Security Framework
  - the Certificate-Based Security Framework
  - the Generic Bootstrapping Architecture(GBA) Framework

- Security Association Establishment Frameworks
  - Provisioned Symmetric Key Security Association Establishment Frameworks
  - Certificate-Based Security Association Establishment Frameworks
  - MAF(M2M Authentication Function)-Based Symmetric Key Security Association Establishment Frameworks

- Remote Security Provisioning Frameworks
  - Pre-Provisioned Symmetric Enrolee Key Remote Security Provisioning Framework
  - Certificate-Based Remote Security Provisioning Framework
  - GBA-based Remote Security Provisioning Framework

IoT 플랫폼 보안

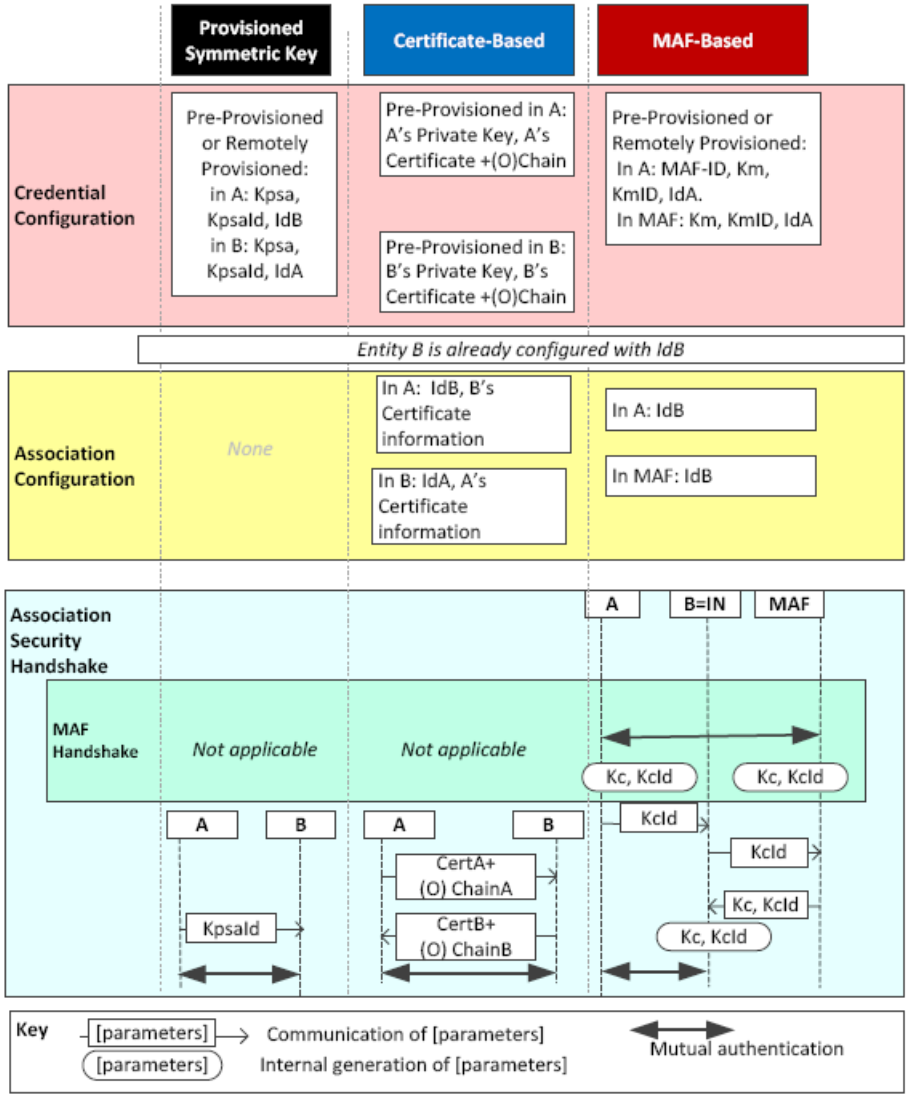
OneM2M Security Framework

Security Association Establishment Frameworks

– Credential Configuration
- 사전 파라미터 설정 단계

– Association Configuration
- 상대방 정보 송수신

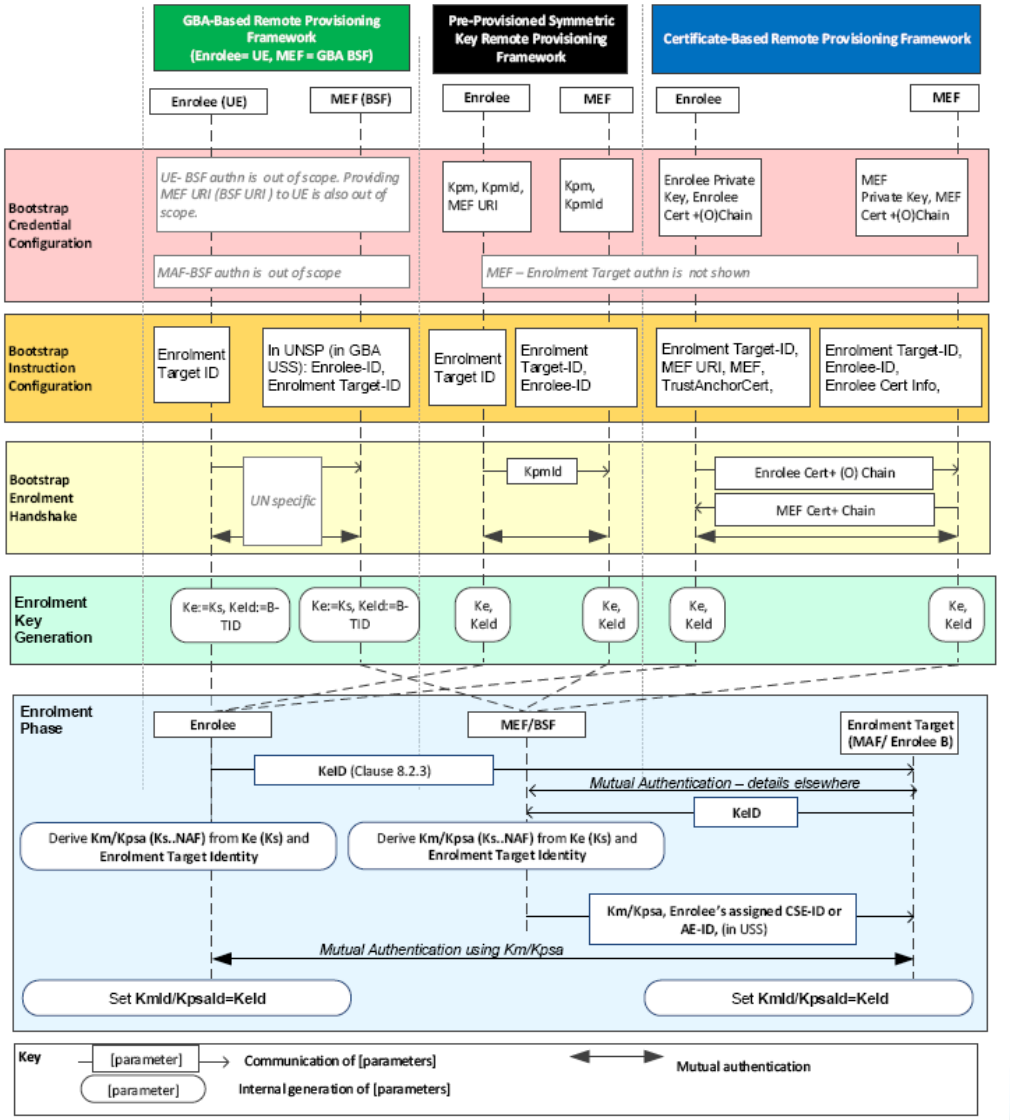
– Association Security Handshake
- 상호 인증



OneM2M Security Framework

Remote Security Provisioning Frameworks

- Bootstrap Credential Configuration
- Bootstrap Instruction Configuration
- Bootstrap Enrolment Handshake
- Enrolment Key Generation
- Enrolment Phase



III. OneM2M Identifiers

1. AllJoyn Internetworking
2. LWM2M Internetworking

M2M Identifiers on OneM2M

M2M Identifiers

- Application Entity Identifier(AE-ID)
- Application Identifier(App-ID)
- CSE-Identifier(CSE-ID)
- M2M Node Identifier(M2M-Node-ID)
- M2M Service Subscription Identifier(M2M-Sub-ID)
- M2M Request Identifier(M2M-Request-ID)
- M2M External Identifier(M2M-Ext-ID)
- Underlying Network Identifier(UNetwork-ID)
- Trigger Recipient Identifier(Trigger-Recipient-ID)
- M2M Service Identifier(M2M-Sev-ID)
- Service Role Identifier(SRole-ID)
- M2M Service Profile Identifier(M2M-Service-Profile-ID)

M2M Identifiers on OneM2M

- Application Entity Identifier(AE-ID)
  - **An Application Entity Identifier (AE-ID) uniquely identifies an AE resident on an M2M Node.**
  - **AE-ID is globally unique within/outside M2M SP domain**

- Application Identifier(App-ID)
  - **An Application Identifier (App-ID) uniquely identifies an M2M Application in a given context.**
  - **Two Type**
    - App-ID(Registered App-ID) : guarantee to be globally unique.
    - Non-Registered App-ID : not guarantee to be globally unique.

M2M Identifiers on OneM2M

CSE-Identifier(CSE-ID)

- A CSE shall be identified by a globally unique identifier, the CSE-ID, when instantiated within an M2M Node in the M2M System.
- The CSE-ID is globally unique, when used internally within/outside a specific M2M SP domain.
- The CSE-ID shall identify the CSE for the purpose of all interactions from/to the CSE within the M2M System.

M2M Node Identifier(M2M-Node-ID)

- An M2M Node, hosting a CSE and/or Application(s) shall be identified by a globally unique identifier, the M2M-Node-ID.
- The M2M System shall allow the M2M Service Provider to set the CSE-ID and the M2M-Node-ID to the same value.
- The M2M-Node-ID enables the M2M Service Provider to bind a CSE-ID to a specific M2M Node.
- Examples of allocating a globally unique M2M-Node-ID include the use of Object Identity (OID) and IMEI. For details on OID,

M2M Identifiers on OneM2M

M2M Service Subscription Identifier(M2M-Sub-ID)

- **The M2M-Sub-ID enables the M2M SP to bind application(s) to a particular M2M Service Subscription between an M2M subscriber and the M2M Service Provider.**
- **The M2M-Sub-ID is unique for every M2M subscriber.**
- **Characteristics:**
  - belongs to the M2M Service Provider;
  - identifies the subscription to an M2M Service Provider;
  - enables communication with the M2M Service Provider;
  - can differ from the M2M Underlying Network Subscription Identifier.
- **There can be multiple M2M Service Subscription Identifiers per M2M Underlying Network subscription. The M2M-Sub-ID shall not be exposed over any interface.**

M2M Identifiers on OneM2M

- M2M Request Identifier(M2M-Request-ID)
  - The M2M-Request-ID tracks a Request initiated by an AE over the Mca reference point, and by a CSE over the Mcc reference point
  - To enable an AE to track Requests and corresponding Responses over the Mca reference point, AEs shall include a distinct M2M Request Identifier per request

- M2M External Identifier(M2M-Ext-ID)
  - The M2M-Ext-ID is used by an M2M SP when services are requested from the Underlying Network.
  - allows the Underlying Network to identify the M2M Device (e.g. ASN, MN) associated with the CSE-ID.
    - For each CSE-ID, there is only one M2M-Ext-ID for a specific UNetwork-ID.
    - The mapping by the Underlying Network of the M2M-Ext-ID to the M2M Device is Underlying Network specific.
    - The Underlying Network provider and the M2M SP collaborate for the assignment of an M2M-Ext-ID to each CSE.

M2M Identifiers on OneM2M

- Underlying Network Identifier(UNetwork-ID)
  - The UNetwork-ID is used for identifying an Underlying Network. UNetwork-ID is a static value and unique within a M2M Service Provider domain.
  - For example, based on "policy", scheduling of traffic triggered by a certain event category in certain time periods may be allowed over Underlying Network "WLAN".

- Trigger Recipient Identifier(Trigger-Recipient-ID)
  - The Trigger-Recipient-ID is used to identify an instance of an ASN/MN-CSE on an execution environment.
  - For example, when 3GPP device triggering is used, the Trigger-Recipient-ID maps to the AppID
    - For pre-provisioned M2M-Ext-IDs, Trigger-Recipient-ID is provisioned at the Infrastructure Node along with the M2M-Ext-ID and the associated CSE-ID.
    - For dynamic M2M-Ext-IDs, Trigger-Recipient-ID specific to the Underlying Network is provisioned at each M2M device in the Field Domain. Such Trigger-Recipient-ID is conveyed to the IN-CSE during CSE Registration

M2M Identifiers on OneM2M

- M2M Service Identifier(M2M-Sev-ID)
  - The M2M-Serv-ID is an identifier of a M2M Service offered by an M2M SP.
  - It is an essential part of the M2M Service Subscription which stores a set of M2M-Serv-IDs pertaining to the set of subscribed services.

- Service Role Identifier(SRole-ID)
  - The Service Role Identifier shall be used for service access authorization.
  - In each M2M Service, one or multiple M2M Service Role(s) shall be defined by the M2M Service Provider.
  - An M2M Service Role is defined as a create permission pertaining to resource types which are associated with M2M Service.

M2M Identifiers on OneM2M

- M2M Service Profile Identifier(M2M-Service-Profile-ID)
  - An M2M Service Profile Identifier defines M2M Service Roles as well as applicable rules governing the AEs registering with M2M Nodes and the AEs residing on these nodes.
  - Every M2M Service Profile is allocated an identifier so it can be retrieved for verification purposes.
    - belongs to the M2M Service Provider;
    - identifies the M2M Service Roles as well as applicable rules governing AEs registering with an M2M node. The M2M Service Roles define the M2M Services authorized for the M2M Service Profile

IV. Accessing Resources

1. Blocking Mode
2. Non-Blocking Mode in Synchronous
3. Non-Blocking Mode in ASynchronous

Accessing Resources in CSEs

- Types of accessing resources
  - No Hop
  - 1 Hop
  - Multi Hops
- Non blocking accessing resources
  - Synchrous mode
  - Asynchrous mode

Accessing Resouces in CSEs - No Hop

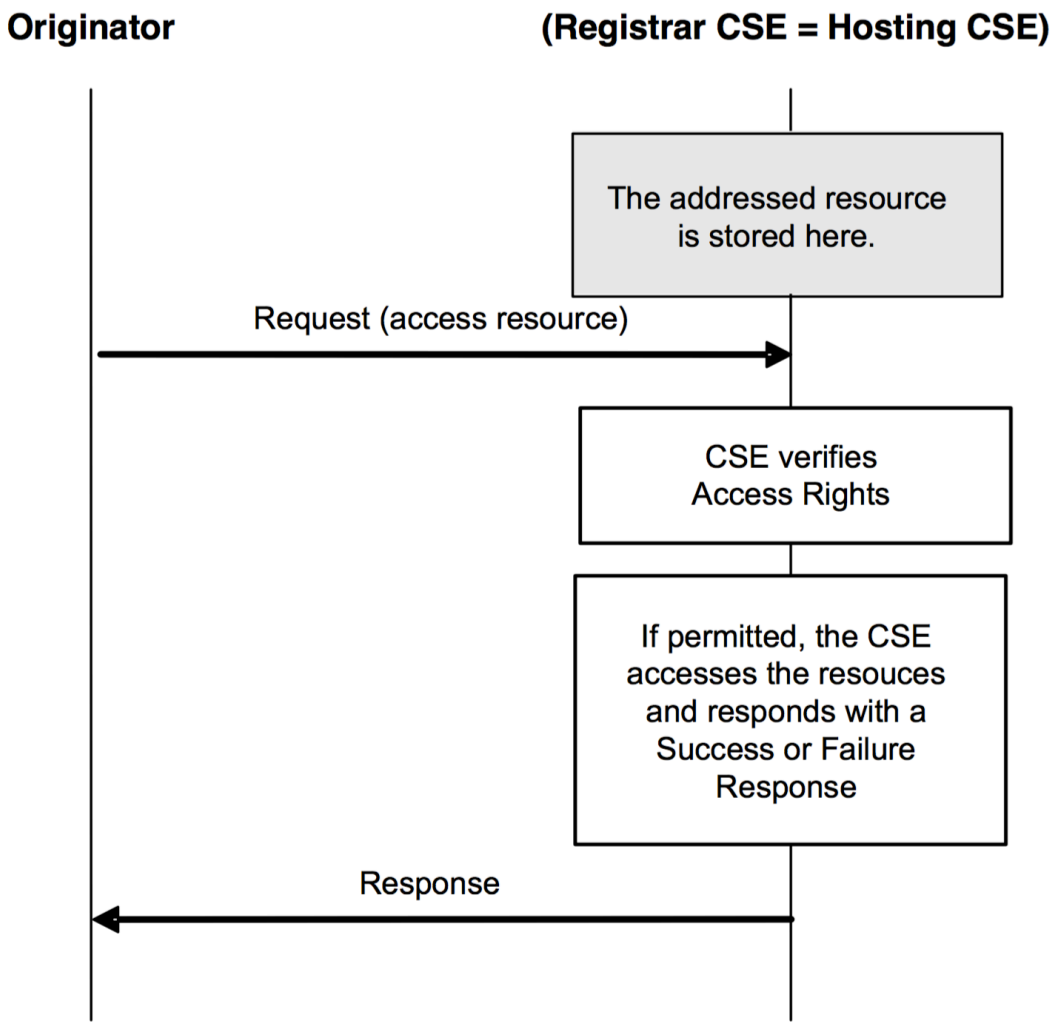


Figure 8.2.1-1: Originator accesses a resource on the Registrar CSE (No Hops)

Accessing Resouces in CSEs - 1 Hop

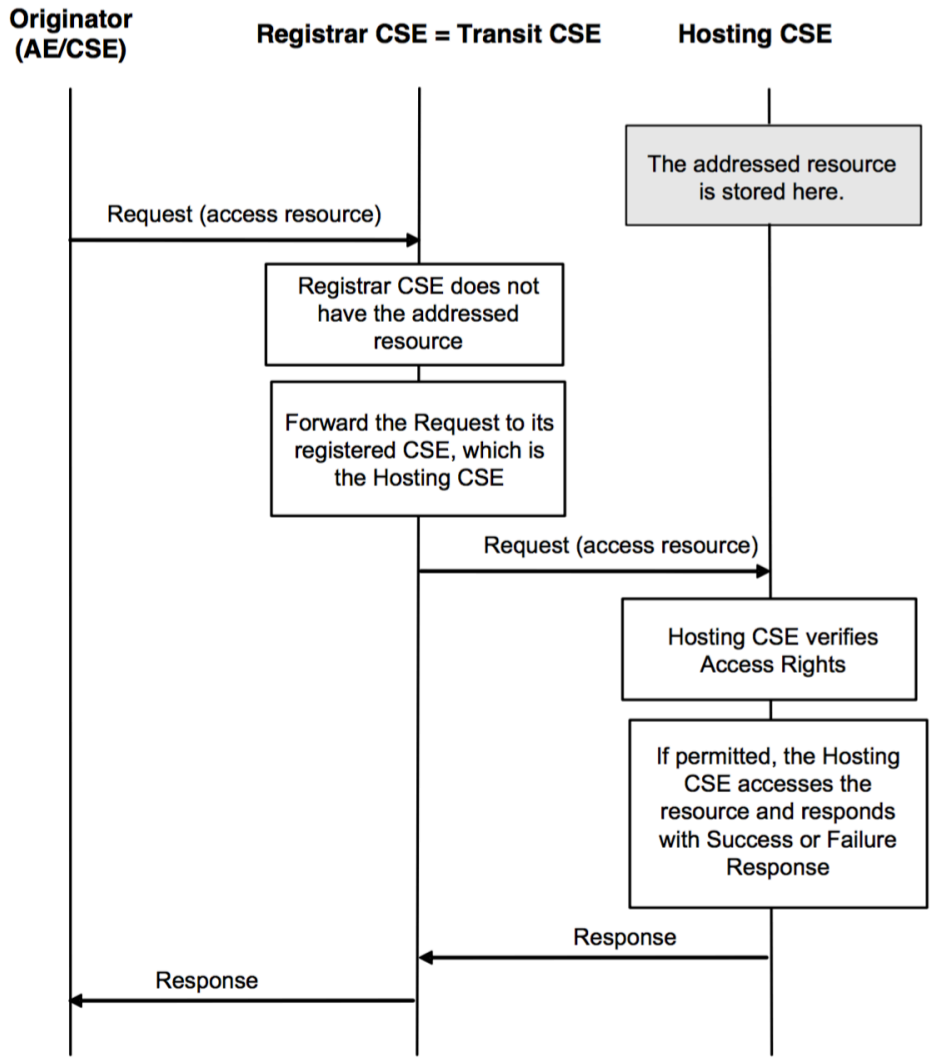


Figure 8.2.1-2: AE/CSE accesses a resource at the Hosting CSE (One Hop)

Accessing Resouces in CSEs - Multi Hop

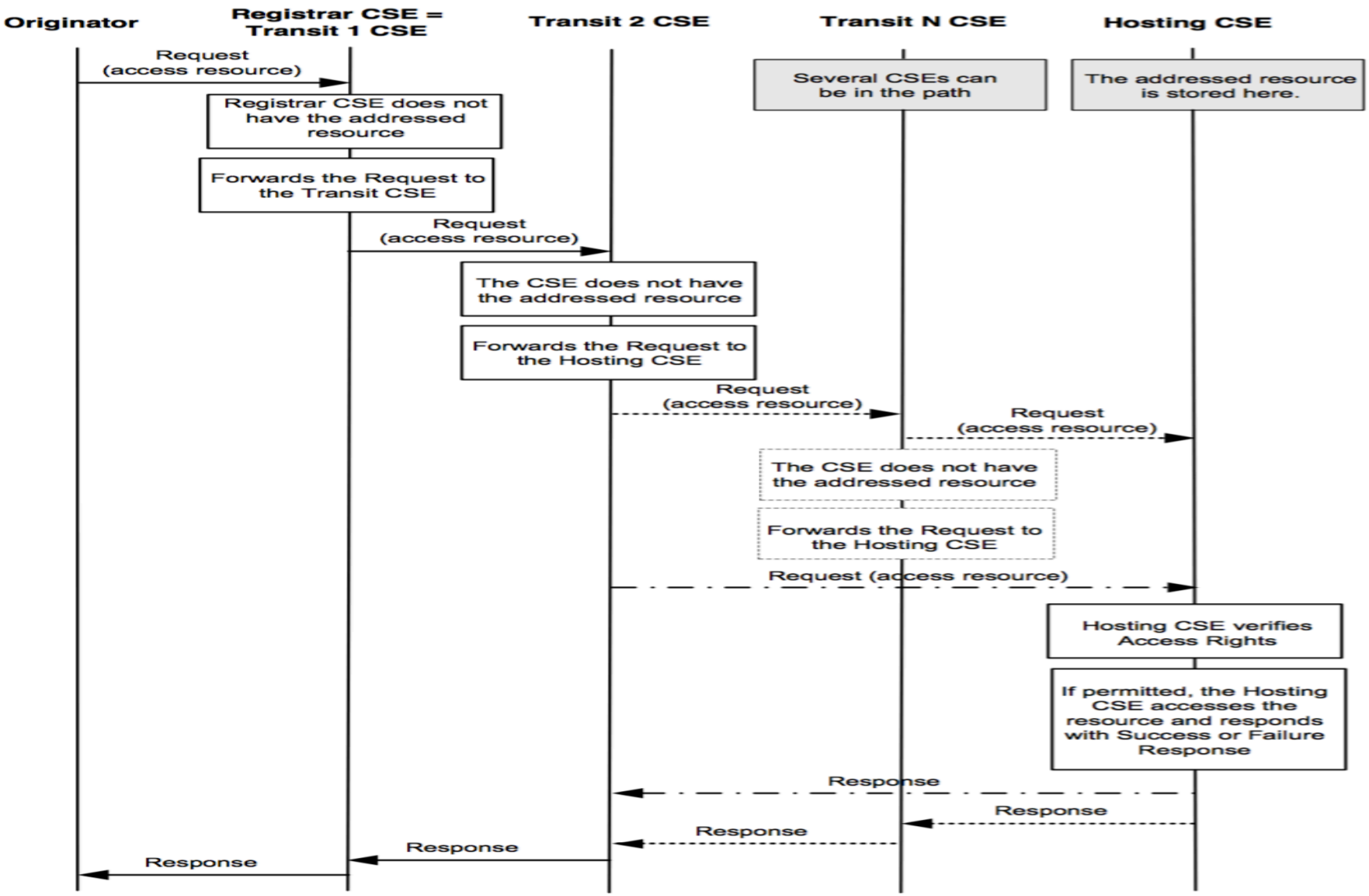


Figure 8.2.1-3: Originator accesses a resource at the Hosting CSE (Multi Hops)

Accessing Resources in Synchronous mode

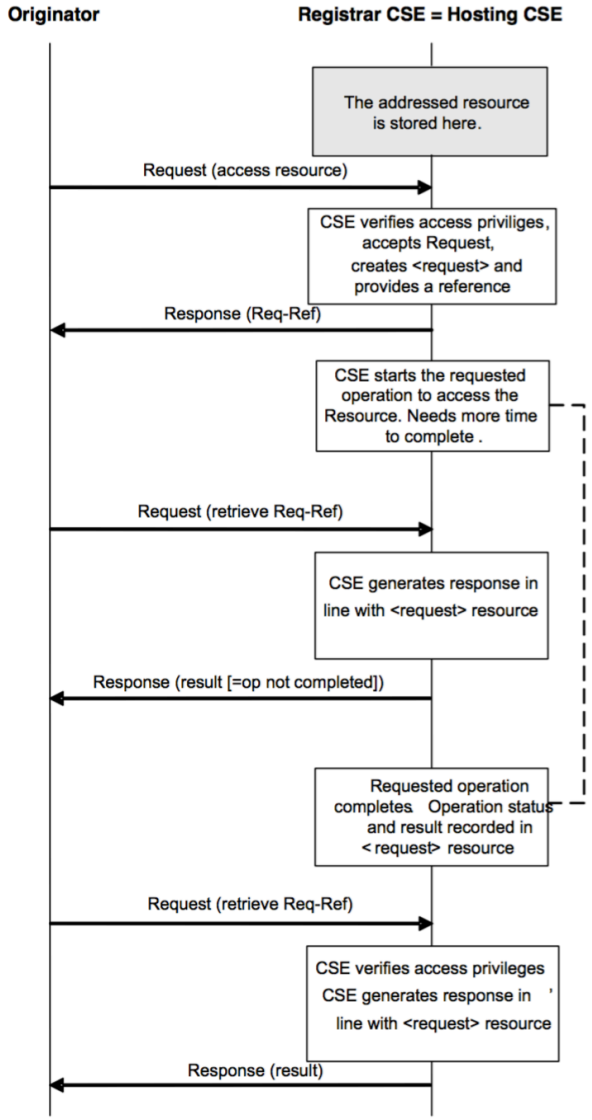


Figure 8.2.2.2-2: Non-blocking access to resource in synchronous mode (Hosting CSE = Receiver CSE), requested operation completed after the second but before the third request

Accessing Resources in Asynchronous mode

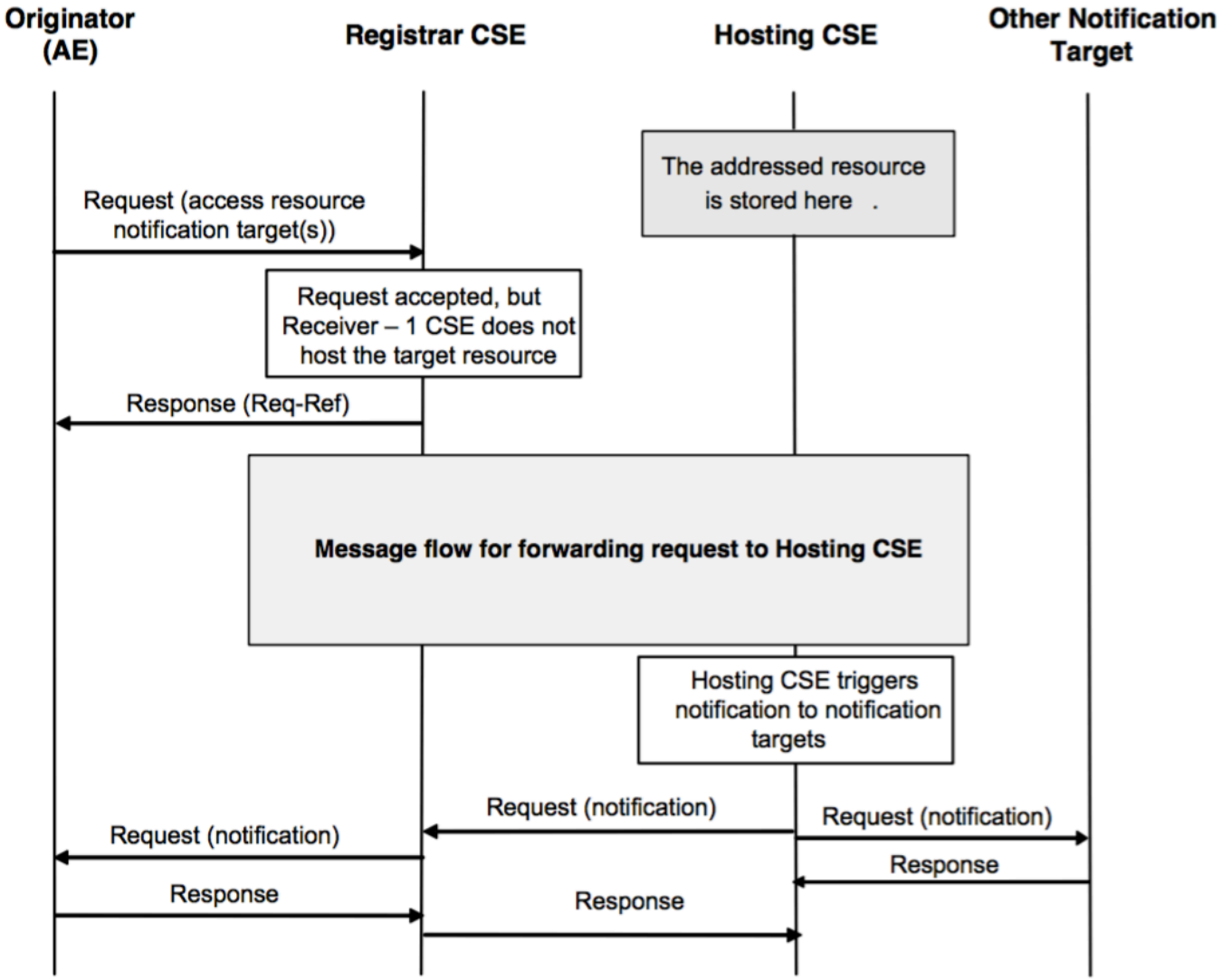
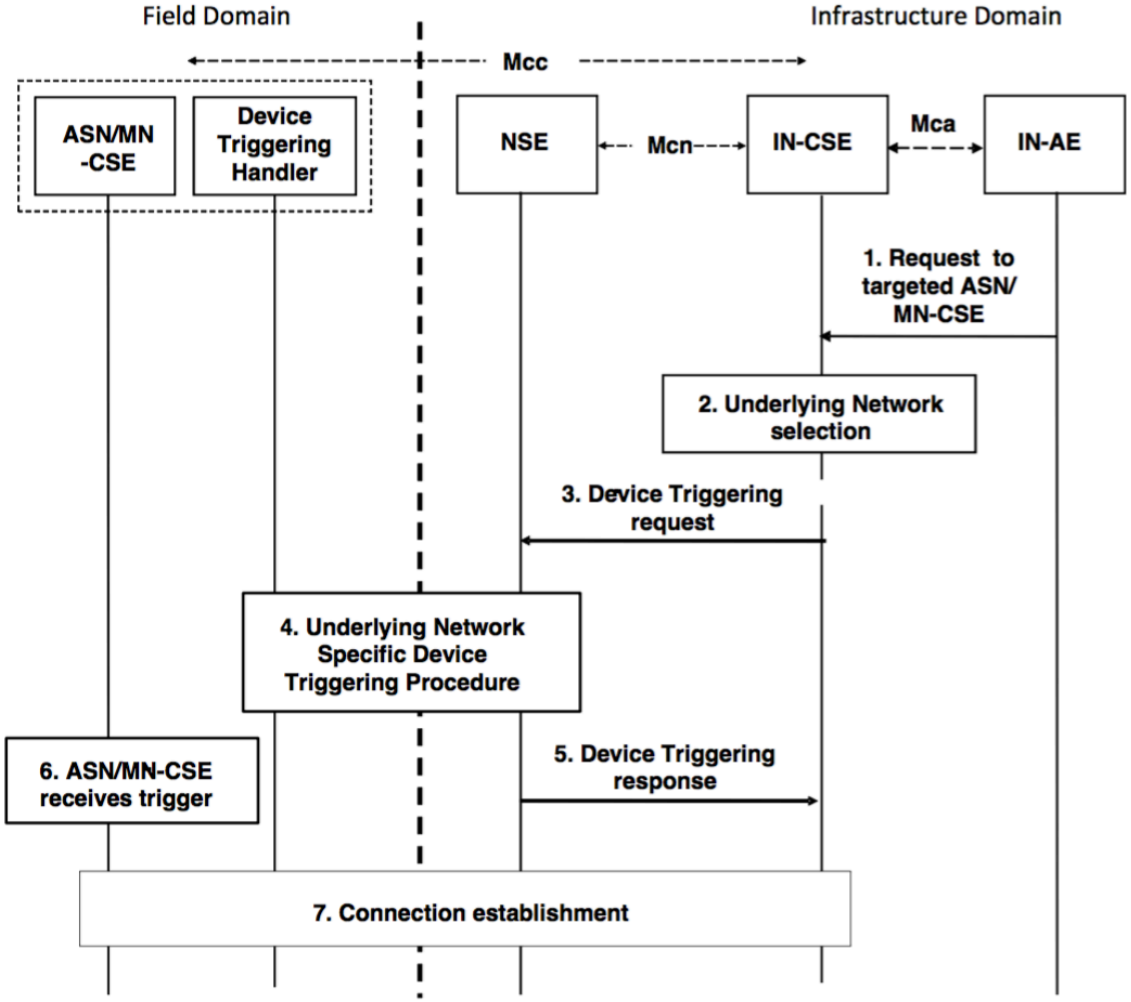


Figure 8.2.2.3-1: Non-blocking access to resource in asynchronous mode (Hosting CSE not equal to Receiver - 1 CSE), Originator provided targets for notification

V. Other Protocols

1. Device Triggering
2. Location Request
3. Notification of Re-Targeting

Device Triggering



NOTE 1: The IN and ASN/MN are assumed to be connected through the same Underlying Network.
NOTE 2: The Device Triggering Handler is a functional entity that receives the device triggering request, and it is dependent on the Underlying Network. The Device Triggering Handler is out of scope of the present document.

Figure 8.4.2.1-1: Device Triggering general procedure for CSE

Location Request

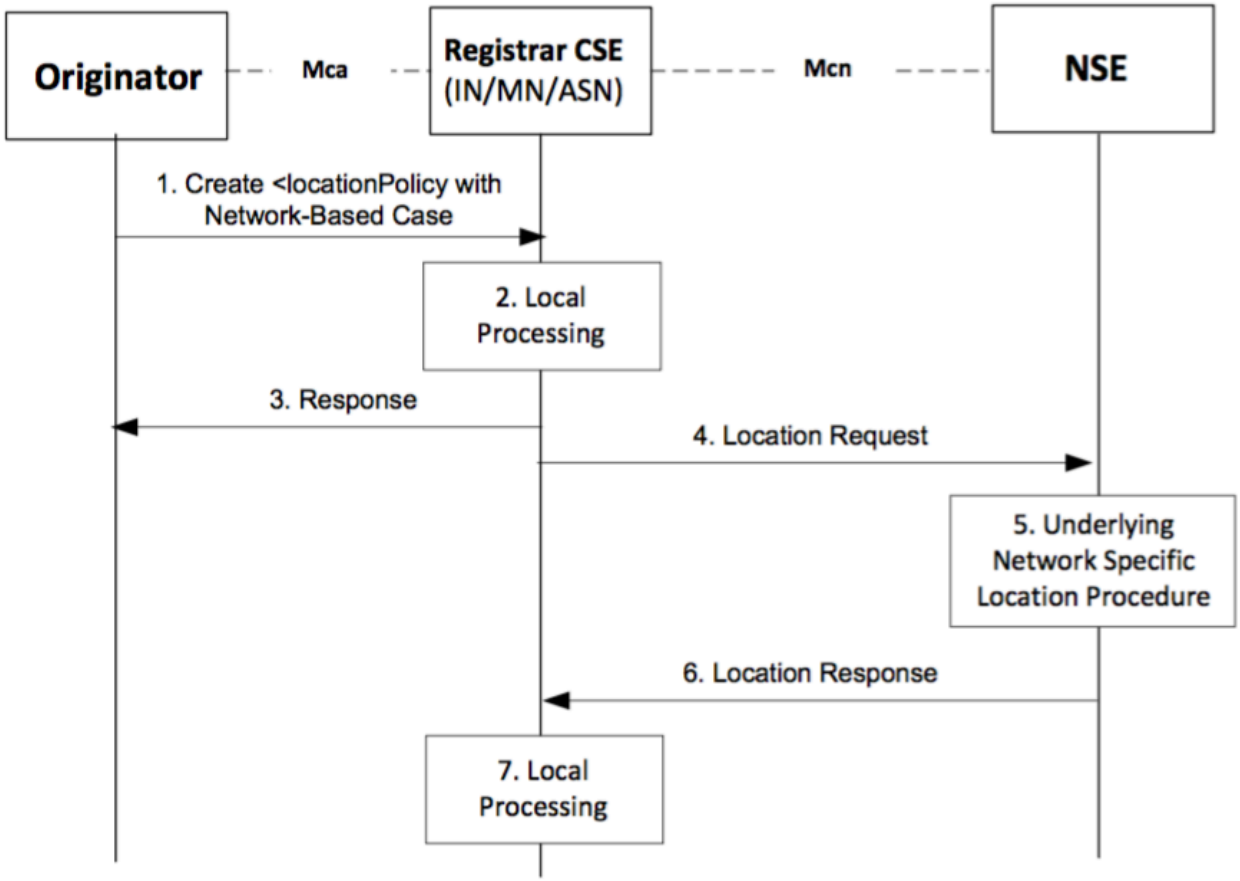


Figure 8.5.2-1: General Procedure for Location Request

Notification of Re-Targeting

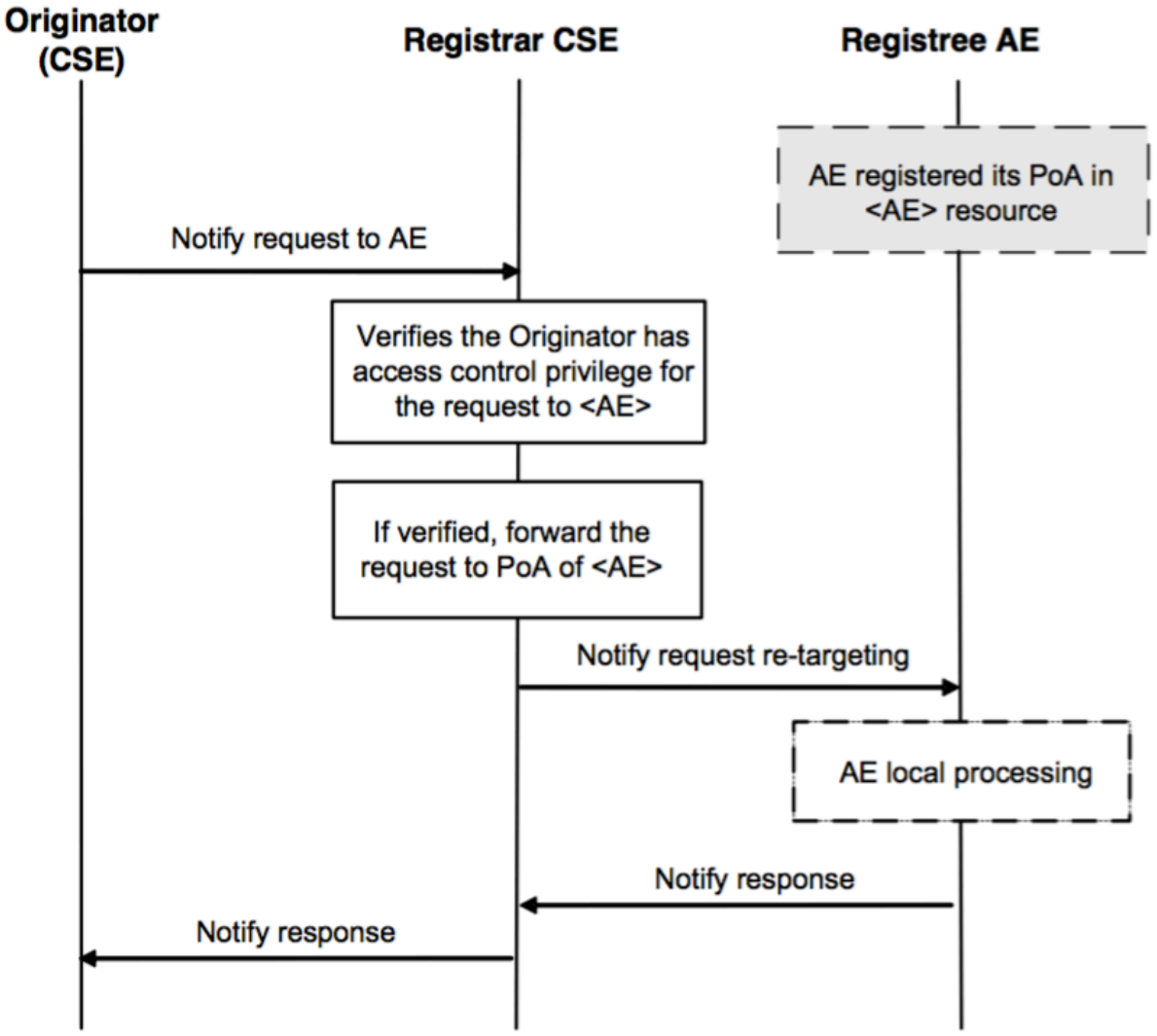


Figure 9.3.2.3-1: Re-targeting a notification request to an AE

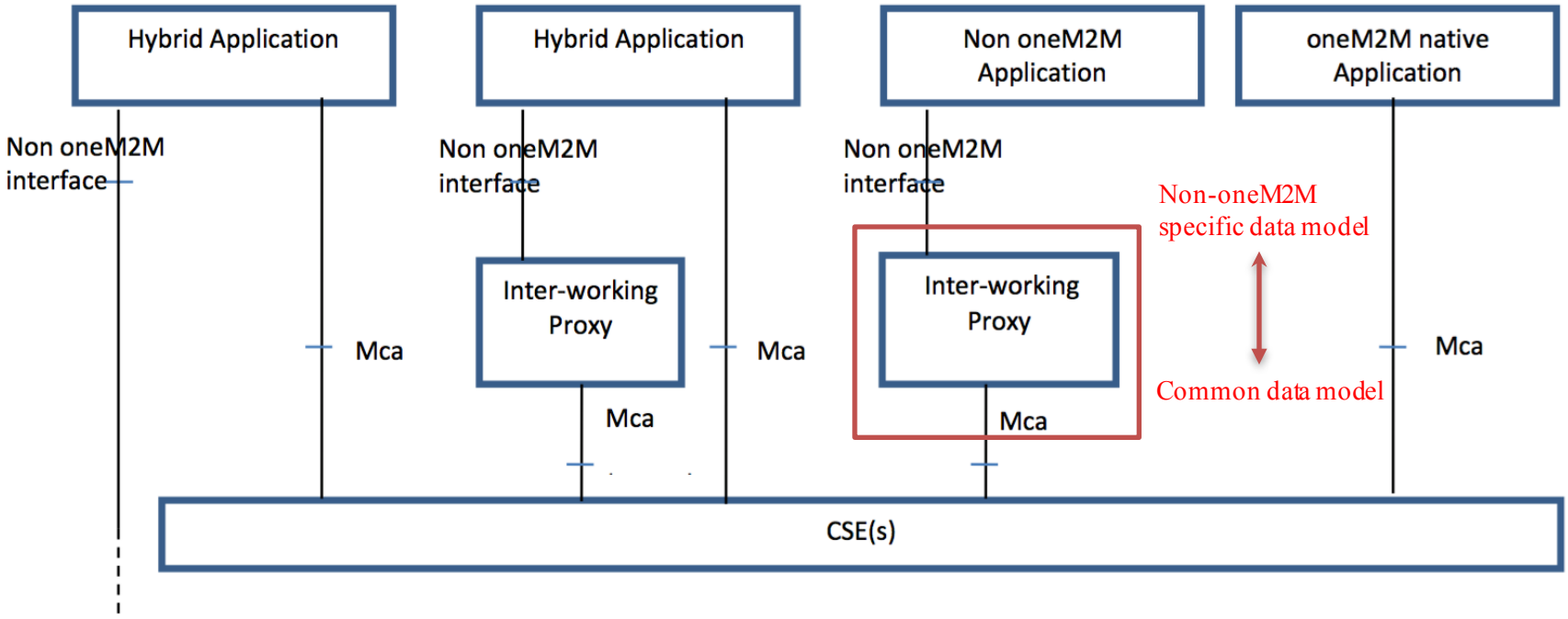
VI. OneM2M Internetworking

1. AllJoyn Internetworking
2. LWM2M Internetworking

oneM2M Interworking - Non oneM2M Entity

Non oneM2M Entity Interworking

- oneM2M 에서는 non oneM2M Entity와의 연동을 위해 IPE(Interworking Proxy Entity)를 정의
- 타플랫폼의 Specific Data Model을 IPE에서 oneM2M에서 정의된 Common Data Model으로 Mapping
  - oneM2M Entity는 IPE에서 Mapping한 Common Data Model에 접근하여 연동

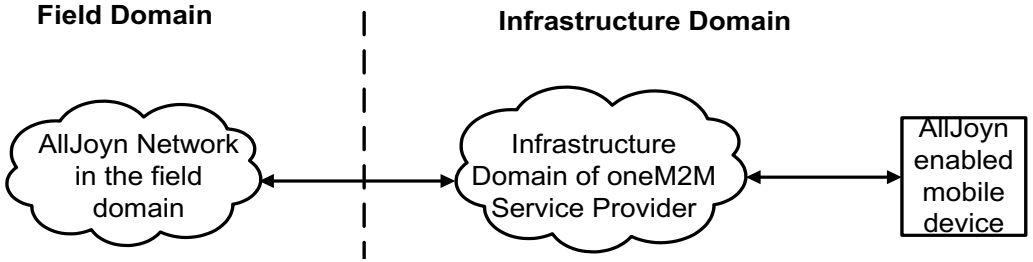


oneM2M Interworking - AllJoyn

AllJoyn Interworking

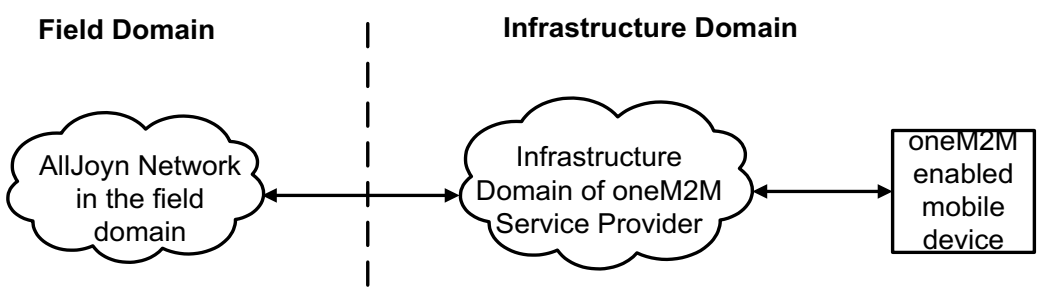
▪ 연동 시나리오

1



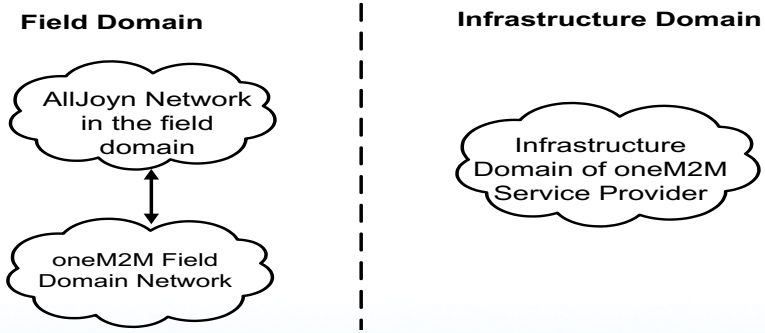
AllJoyn enabled mobile device controls AllJoyn Network through oneM2M

2



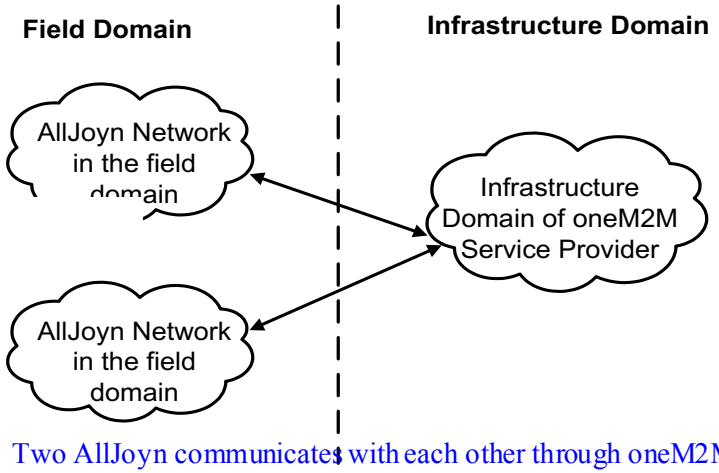
oneM2M enabled mobile device controls AllJoyn Network

3



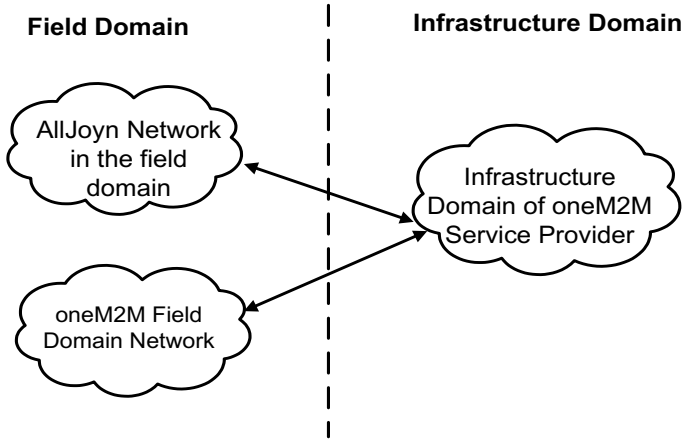
AllJoyn Network directly communicates with oneM2M field domain Network

4



Two AllJoyn communicates with each other through oneM2M

5



AllJoyn Network communicates with oneM2M through oneM2M

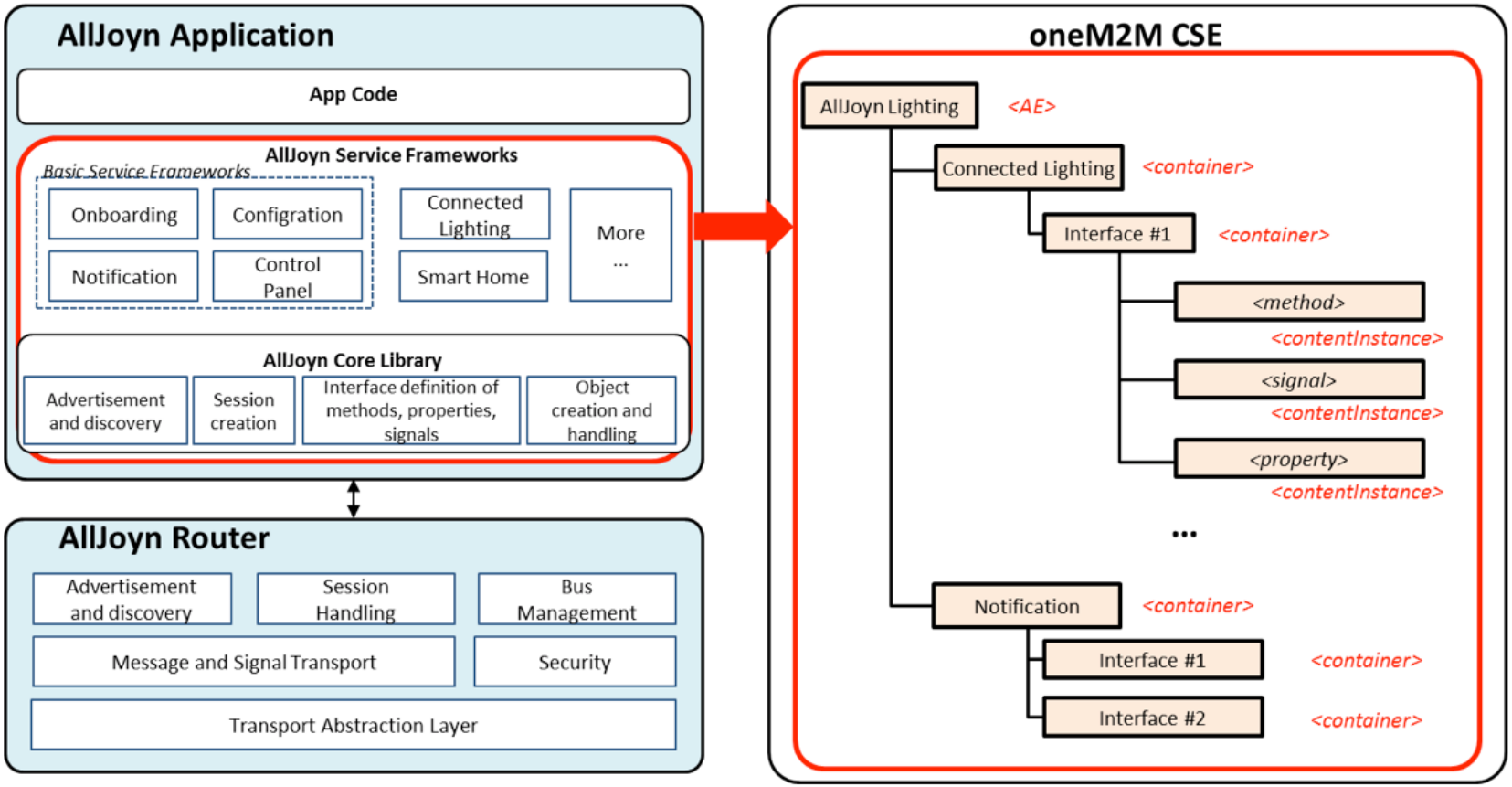
oneM2M Interworking - AllJoyn

AllJoyn Interworking

▪ Service Mapping

– 기존 <container> Resource Type Mapping

- AllJoyn의 methods, signals, properties까지 접근제어 정책을 적용할 수 없음
  ➔ <containerInstance>는 container의 accessControlPolicy를 따름



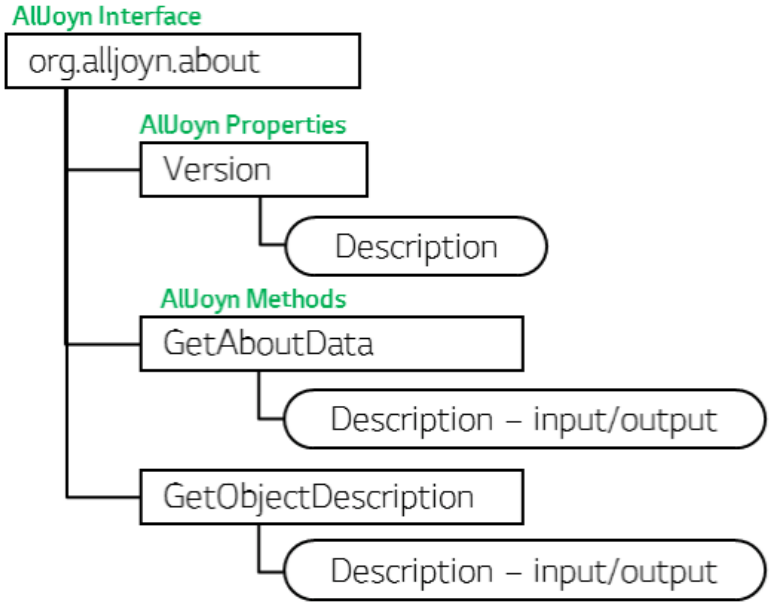
oneM2M Interworking - AllJoyn

AllJoyn Interworking

▪ Service Mapping

– Newly defined Resource Type

- AllJoyn 연동을 위한 새로운 oneM2M Resource Type 정의
  → 새로운 Resource Type 정의에 대한 비용 발생



[About interface]
org.alljoyn.About

[Properties]
- Version

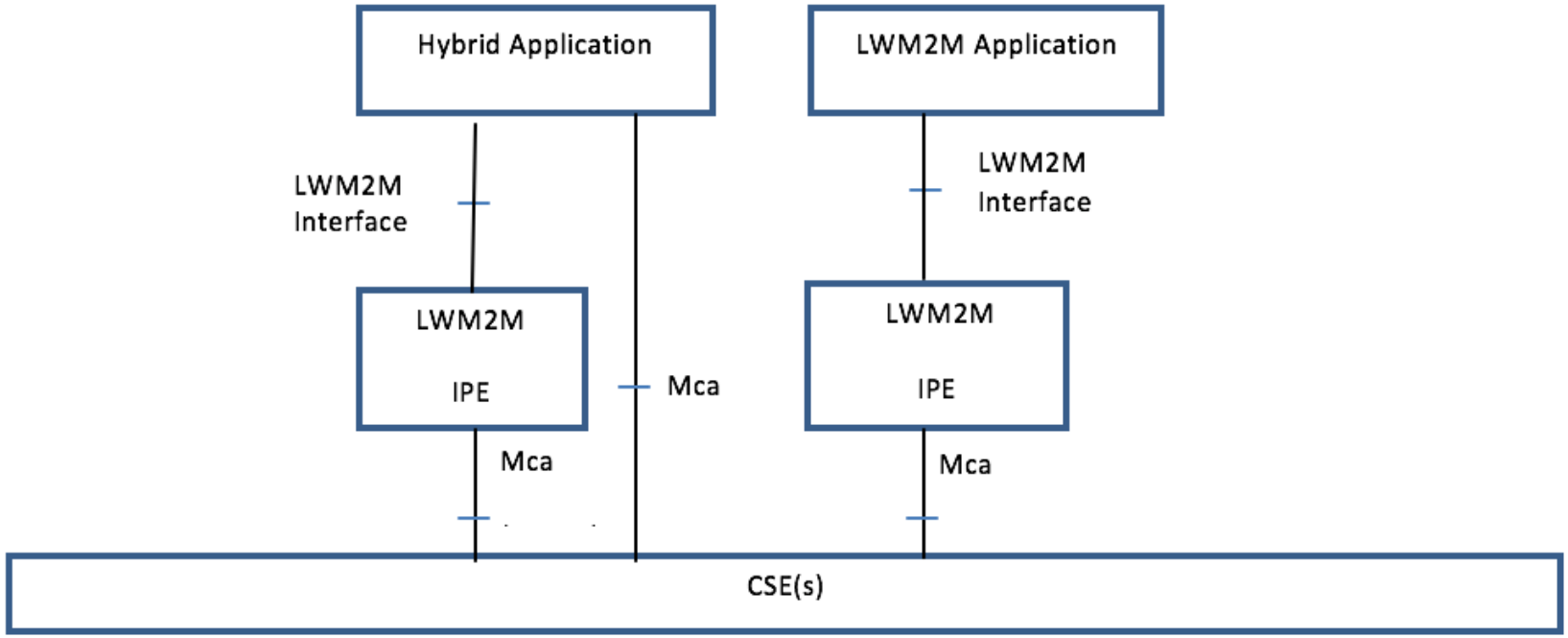
[Methods]
- GetAboutData
- GetObjectDescription

[Signals]
- Announce

oneM2M Interworking - LWM2M

LWM2M Interworking

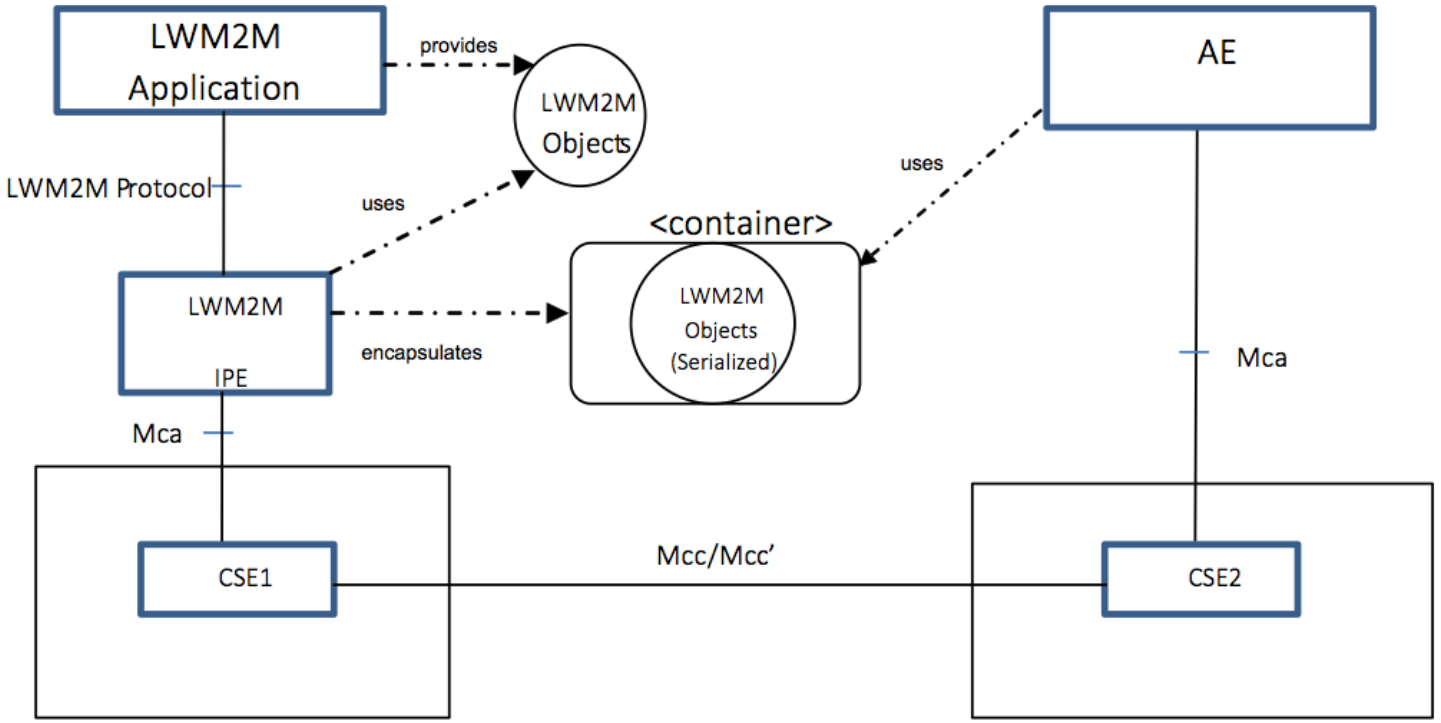
- 연동 시나리오
  - LWM2M Interworking Proxy Entity(IPE) 를 통한 연동
    - 기본적으로 TS-0001에 정의된 non-oneM2M Entity 와 CSE 간의 연동을 참조



oneM2M Interworking - LWM2M

LWM2M Interworking

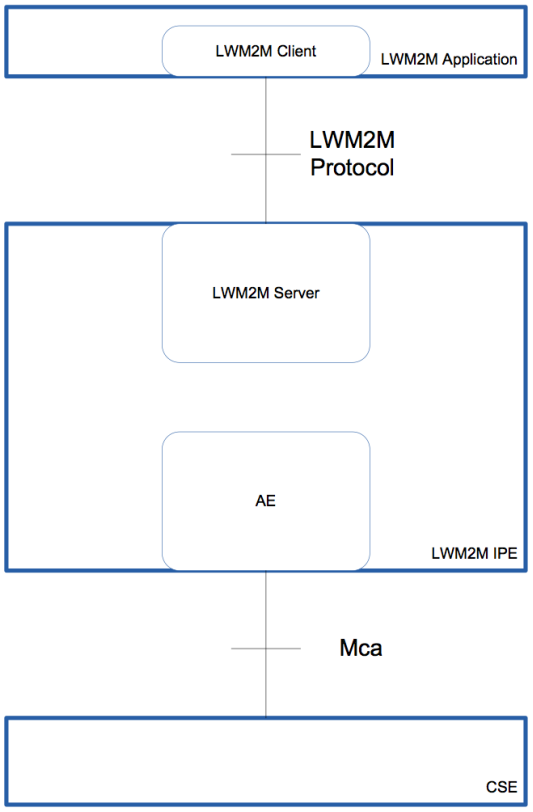
- 연동 방법
  - LWM2M IPE를 통해 LWM2M Object를 <container> 리소스로 encapsulates
  - IPE가 생성한 <container> 에 접근을 통해 연동 가능



oneM2M Interworking - LWM2M

LWM2M Interworking

- **Interworking Proxy Entity(IPE)**
  - LWM2M Server와 AE로 구성된 Entity
    - **LWM2M Server**
      : LWM2M Client와 LWM2M 프로토콜을 통해 LWM2M Object를 전달 받음
    - **AE(Application Entity)**
      : CSE 등과 통신하기 위한 Entity



oneM2M Interworking - LWM2M

LWM2M Interworking

- LWM2M IPE 에서 지원하는 프로토콜
  - Device and Endpoint Lifecycle
  - Object Discovery
  - Object Transport and Interworking
  - Object Subscription and Notification
  - Object Security
  - Client Pre-provisioning
  - IPE Administration
- 프로토콜에 대한 oneM2M Mapping

LWM2M Errors Client Registration Interface	oneM2M Resource Operation Response
Register 2.01 Created: 4.00 Bad Request 4.03 Forbidden	create <AE>, create <Node> 2001 Created All other codes 4105 Conflict
Update 2.04 Changed 4.00 Bad Request 4.04 Not Found	update <AE>, update <Node> 2004 Changed All other codes 4000 Not Found
De-register 2.02 Deleted 4.04 Not Found	delete <AE>, delete <Node> 2002 Deleted 4004 Not Found

감사합니다

Q & A