ETRI Creative Opinion
창의미래연구소

oneM2M Security Solutions

oneM2M-TS-0003-Security-Solutions-V-2014-08

ETRI 표준연구센터
박정수 (pjs@etri.re.kr)

ETRI

Mission

oneM2M is working to unify the Global M2M Community, by enabling the federation and interoperability of M2M systems, across multiple networks and topologies

By O. Elloumi

ETSI vs. oneM2M

ETRI Creative Opinion
창의미래연구소

By O. Elloumi

1. oneM2M architecture IS NOT an extension of ETSI M2M
2. Current oneM2M architecture USE SIMILAR, to ETSI M2M, architecture style : RESTFull, but oneM2M adopts full HATEOAS (Hypermedia as the Engine of Application State) principles, no mandated resource structure
3. However, other Service Oriented approaches ARE NOT EXCLUDED, in particular for componentization of the service layer.
4. oneM2M leverages underlying network capabilities: triggering, location, charging. While ETSI M2M assumes an IP capable network.
5. Extended capability set include: delivery handling, device triggering, location, Role based access control, M2M service subscription, etc.
6. Protocol binding include MQTT (in addition to HTTP and CoAP)

However an ETSI M2M platform could easily be upgraded to become oneM2M compliant. Interworking is also possible.

Security

By O. Elloumi

- ETSI TC M2M only addressed the security needs of M2M Service Providers: Protection of the M2M service infrastructure only
- Yet the purpose of an M2M Service Platform is to provide services to M2M Applications: Why not "Security as a Service"?
  - The goal in oneM2M is to leverage on security capabilities present in the M2M infrastructure (Service Layer or Underlying Network) to provide Security Services for M2M applications
- Some oneM2M Security Services:
  - Credentials deployments and management
  - Secure connection establishment and management
  - Authorization and Access Control, supporting roles and context attributes
- oneM2M Security Solutions:
  - Support of Symmetric (Pre-Shared Keys) and Asymmetric (PKI) credentials
  - Support of static trust scenarios, based on pre-provisioned credentials
  - Support of dynamic configurations, involving a Centralized Key Distribution

Contents

1. Scope
2. References
3. Definitions and abbreviations
4. Conventions
5. Security Architecture
6. Security Services and Interactions
7. Authorization
8. Security Frameworks
9. Security Framework Procedures and Parameters
10. Protocol and Algorithm Details

Contents

A. Mapping of 3GPP GBA terminology
B. General Mutual Authentication Mechanism
C. Security protocols associated to specific SE technologies
D. UICC Security framework to support oneM2M services (normative)
E. Precisions for the UICC framework to support M2M Services
F. Acquisition of Location Information for Location based Access Control (normative)
G. Access Control Decision Request

References [ch.2]

- **Normative references**
  - oneM2M TS-0001 "oneM2M Architecture"
  - Open Mobile API specification V2.0.2
  - GP TEE Client API
  - oneM2M TS-0004 “oneM2M Core Protocol” 외 43건 (그 중에 IETF 22건)

- **Informative references**
  - oneM2M Drafting Rules
  - oneM2M-TR-0004 Definitions and abbreviations
  - oneM2M TR-0008, Security Analysis Technical Report
  - oneM2M TS-0011 Definitions and Acronyms 외 11건

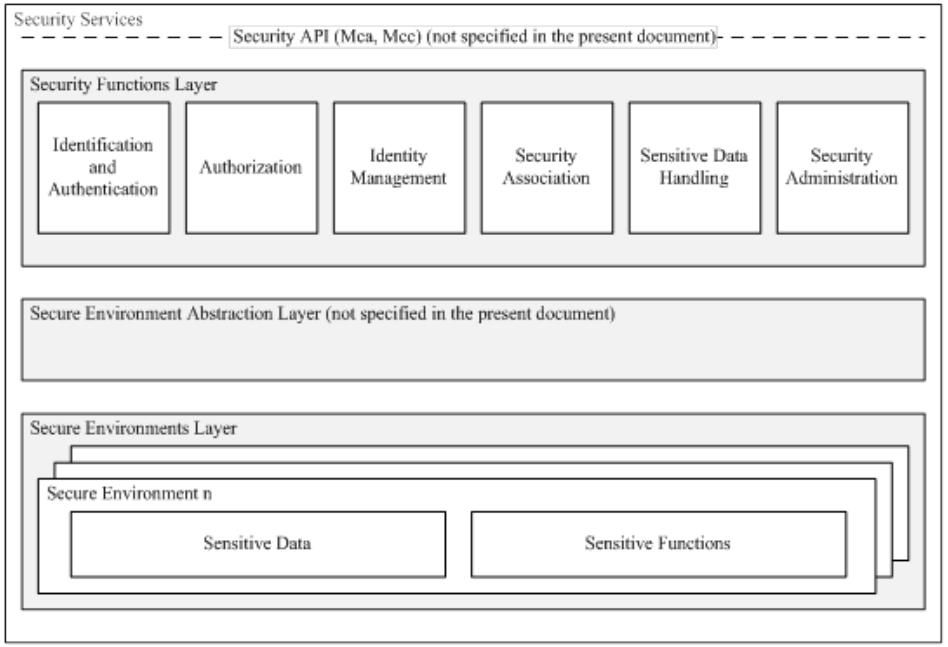
Abbreviations [ch.3]

- **Kc M2M Secure Connection Key**
- **Ke Enrolment Key**
- **Km Master Credential**
- **Kpm pre-provisioned credential for Master Credential provisioning**
- **Kpsa pre-provisioned credential for M2M SAE**
- **Ks temporary Key material referred to in GBA**
- **Ks_(ext/int)_NAF**
  - Derived key in GBA_ME or Derived key in GBA_U which remains on UICC
  - Ks..NAF Abbreviation of Ks_(int/ext)_NAF
  - Ks_NAF Derived key in the ME
  - Ks_ext_NAF Derived key in GBA_U sent to the ME
  - Ks_int_NAF Derived key in GBA_U which remains on UICC

Security Architecture [Ch.5.1]

ETRI Creative Opinion
창의미래연구소

- **Security Function layer**
  - A set of security functions
  - Exposed at reference point **Mca** and **Mcc**
  - Classified into six categories
- **Security Environment Abstraction layer**
  - Various security capabilities
  - To do the operation related to the SE by invoking from Security function layer
  - Physical access through the SE
  - Protection Level
    - 0: No protection
    - 1: Passive attack만 방지
    - 2: Remote attack 보호, local SW attack 보호
    - 3: Local HW attack 보호



- **Secure Environment layer**
  - To provide various security services over one or multiple secure environments
  - Sensitive data & sensitive functions

Security Architecture [Ch.5.1]

- **Six categories of Security Function Layer**
- **Identification & Authentication**
  - Identification: the process of checking if the identity provided for authentication is valid
  - Authentication: the process of validating if the identity supplied in the identification step is associated with a trustworthy credential
- **Authorization**
  - The authorization function is responsible for authorizing services and data access to authenticated entities according to provisioned access control policies and assigned roles
    - e.g., Access Control List (ACL), Role Based Access Control (RBAC)
  - Access control policy is defined as sets of conditions that define whether entities should be permitted access to a protected resource
  - Authorization evaluation process is based on the Service Subscription resource
  - After mutual authentication between the originator CSE or AE and hosting CSE

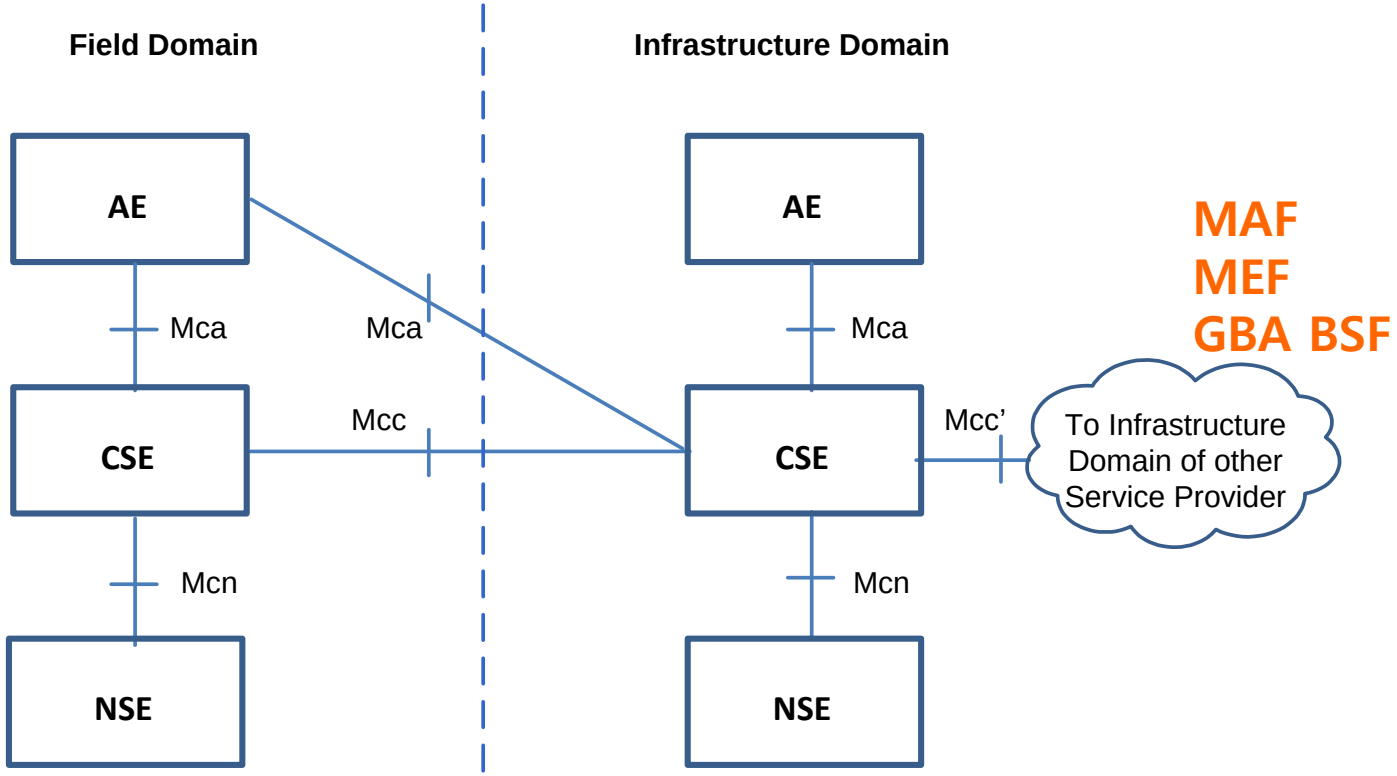
Security Architecture [Ch.5.2]

- **Identity Management**
  - oneM2M identifiers is treated as sensitive data that are accessible to AEs or CSEs and used independently of Authentication or Authorization functions.
  - Identity protection
- **Security Association**
  - Secure Connection via secure session establishment
  - Secure Connection via object security
- **Sensitive Data Handling**
  - Sensitive Functions in AEs/CSEs: cryptographic operations, bootstrapping methods, etc.
  - Secure Storage in AEs/CSEs through the Security API
- **Security Administration**
  - Security pre-provisioning
  - Remote security administration of SE
- **Trust Enabler security functions**
  - Two security functionalities within the infrastructure doamin
    - M2M Enrolment Function (MEF)
    - M2M Authentication Function (MAF)

Integration [ch. 5.3]

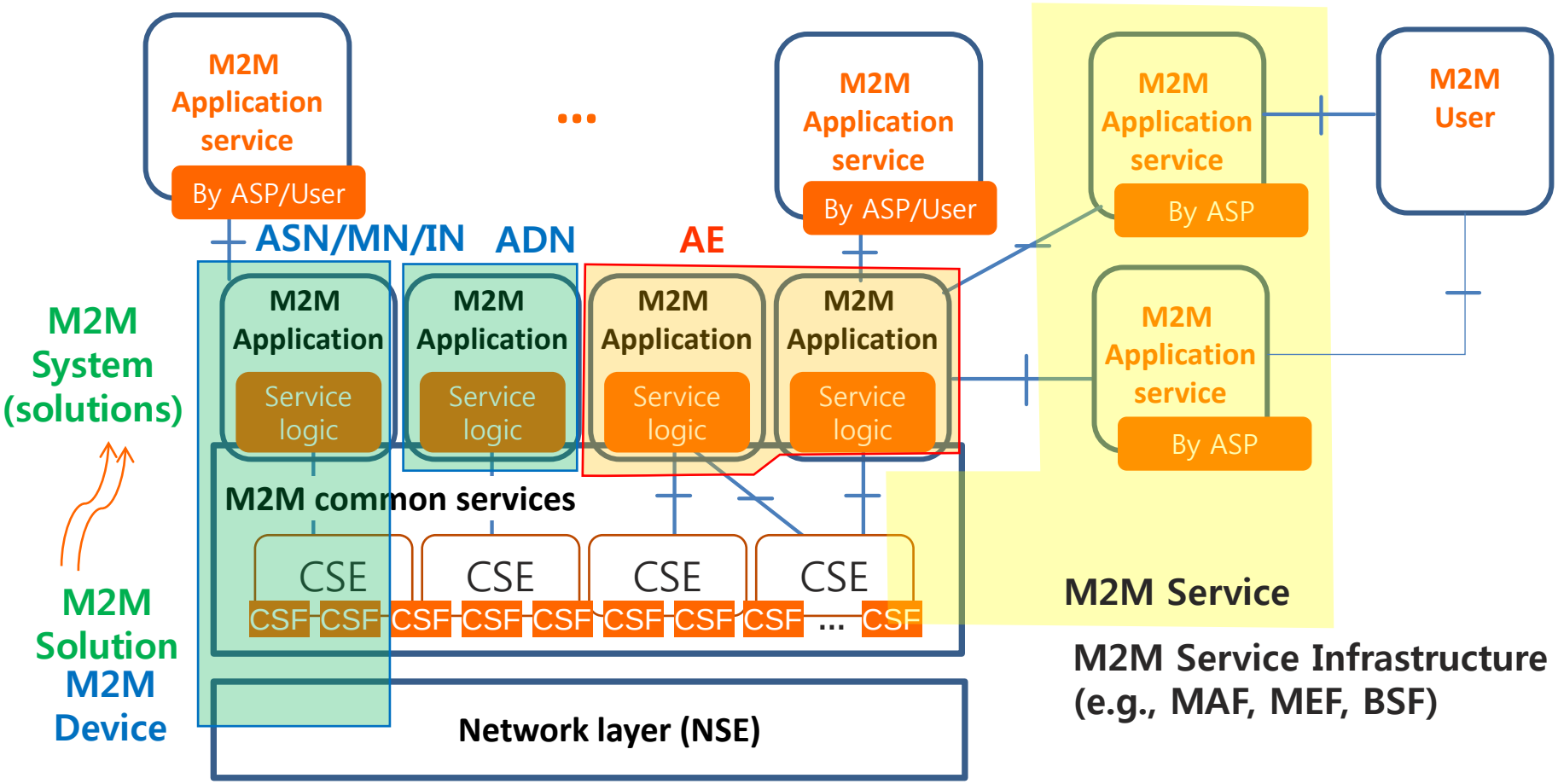
ETRI Creative Opinion
창의미래연구소

- **Integration within overall oneM2M architecture**
  - This document addresses the security over Mcc and Mca in hop-by hop scenario



Integration [ch. 5.3]

- Integration within overall oneM2M architecture



Security services and Interactions [ch. 6]

ETRI Creative Opinion
창의미래연구소

- **High level sequence of events**

A. Enrolment phase

- M2M equipments typically require provisioning and configuration phases before being put in actual operation.
  - by a pre-provisioning in the manufacturing phase, or by means of a security bootstrapping procedure (i.e. remote security provisioning)
- Provisioning and configuration requires selection of the stakeholder (e.g., the M2M Service Provider)
- This Enrolment phase requires contractual agreements between the stakeholders.
- Enrolment phase may occur several times during the lifecycle of an M2M equipment

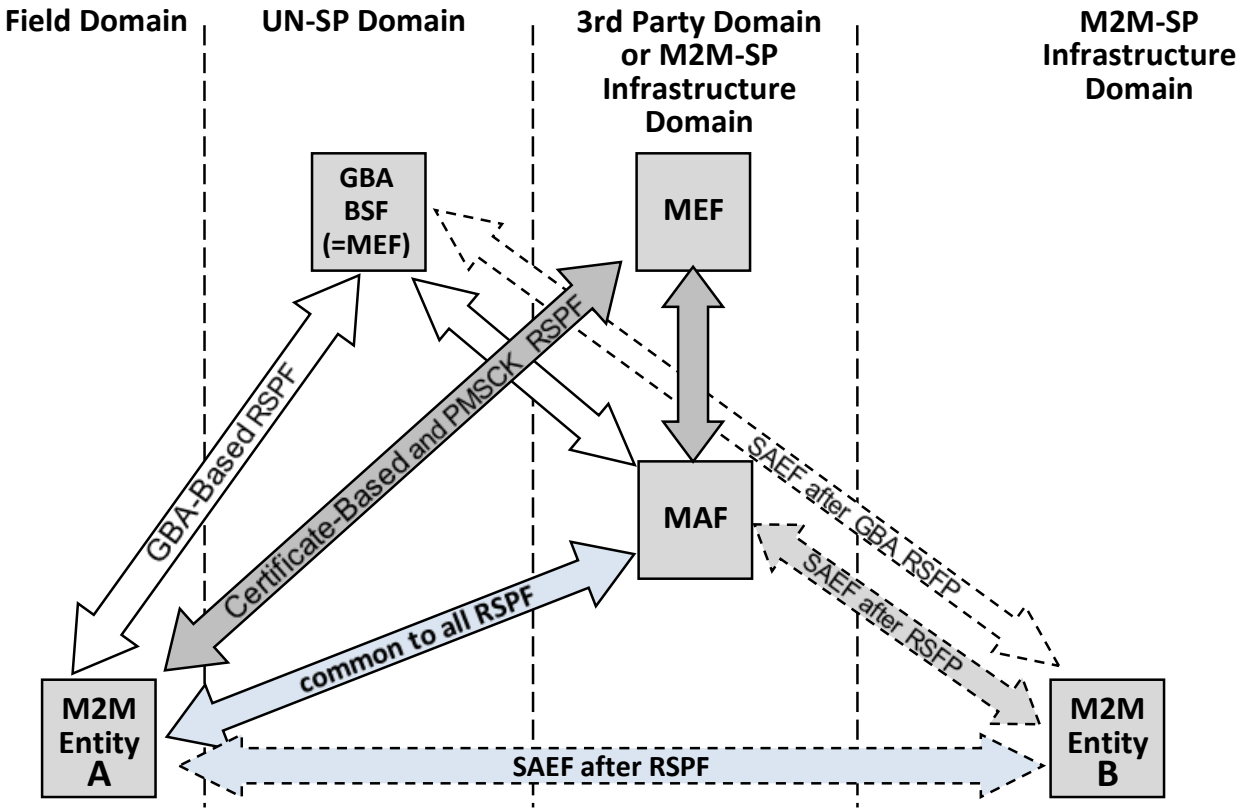
- Remote Security Provisioning Frameworks (RSPF)
  - Provisioned Symmetric Enrolee Key RSPF: A symmetric key for the mutual authentication between the Enrolee and M2M Enrolment Function(MEF)
  - Certificate-Based RSPF: Private signing keys and Certificates with the Public Verification Key
  - GBA-based RSPF: 3GPP or 3GPP2 symmetric keys

B. Operational phase

Security services and Interactions [ch. 6]

ETRI Creative Opinion
창의미래연구소

- Entities involved in Remote Security Provisioning in Fig. 6.1.2.1-1



Security services and Interactions [ch. 6]

ETRI Creative Opinion
창의미래연구소

- **High level sequence of events**

A. Enrolment phase

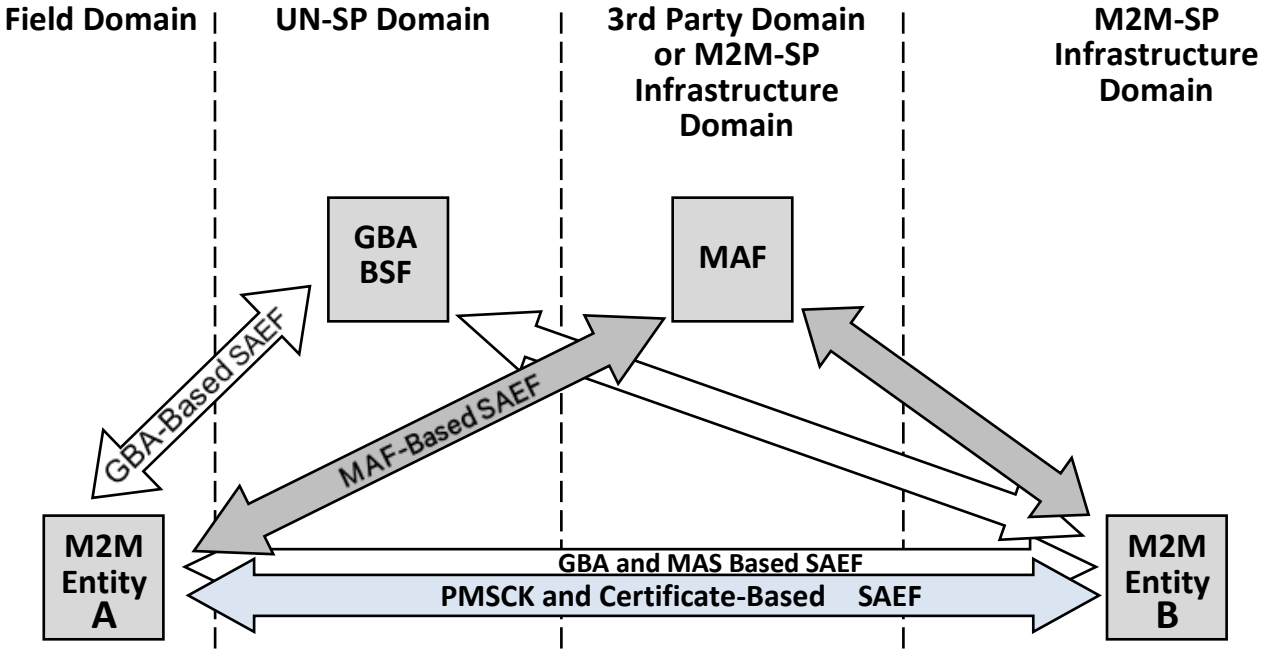
B. Operational phase

1. M2M Service Access
   - AEs and CSEs need to be mutually identified and authenticated with the M2M Service Infrastructure, in order to provide protection from unauthorized access and DoS attacks.
   - This mutual authentication enables to provide encryption and integrity protection for the exchange of messages across a single Mca, Mcc or Mcc' reference point.
   - Reference points in Security association establishment (SAE) procedure
     - SAE between a field domain AE or CSE, respectively, and an IN-CSE is mandatory.
     - SAE between IN-CSE and IN-CSE is mandatory.
     - SAE between AE and the CSE in the field domain is strongly recommended.
   - Authentication mechanisms for SAE in clause 8.2.1
     - Provisioned M2M Secure Connection Key SAEF: A symmetric key
     - Certificate-Based SAEF: private signing keys and Certificates with Public Verification Key
     - M2M Authentication Function (MAF) SAEF: the centralized key distribution server is MAF hosted either by a 3rd party service provider or by the M2M-SP itself. Using a symmetric key
     - GBA-Based SAEF: the centralized key distribution server is a Bootstrap Server Function (BSF) of the 3GPP Generic Bootstrap Architecture (GBA) hosted by the Underlying Network Service Provider. 3GPP or 3GPP2 symmetric keys are used to authenticate Field Domain entities.
2. Authorization to access M2M resources
   - Access control

Security services and Interactions [ch. 6]

ETRI Creative Opinion
창의미래연구소

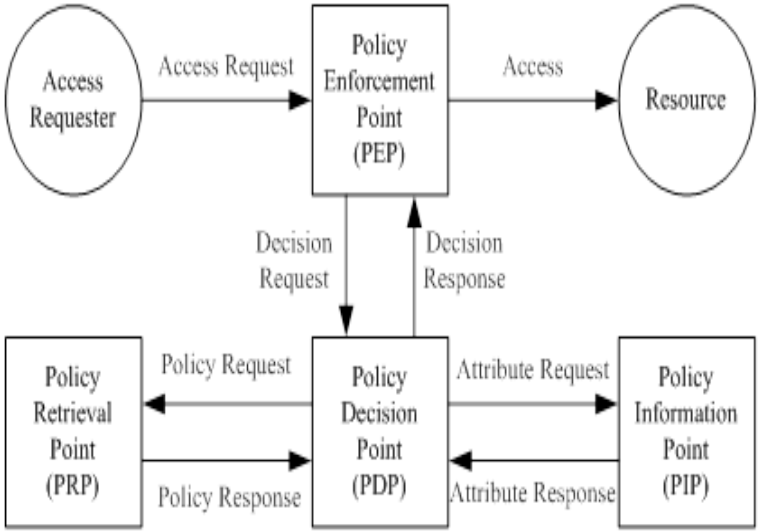
- Entities involved in Security Association Establishment in Figure 6.1.2.2-1

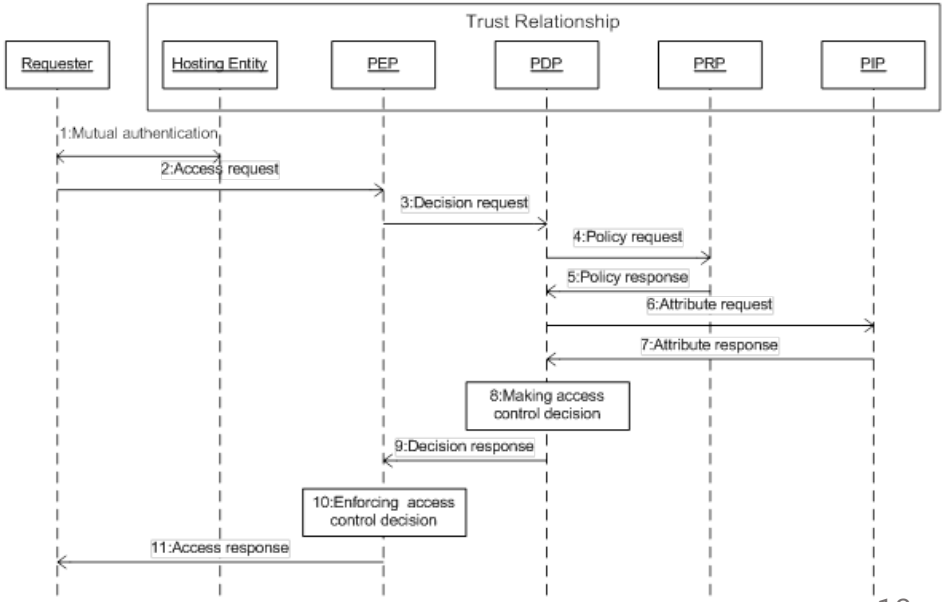


Security services and Interactions [ch. 6.2]

ETRI Creative Opinion
창의미래연구소

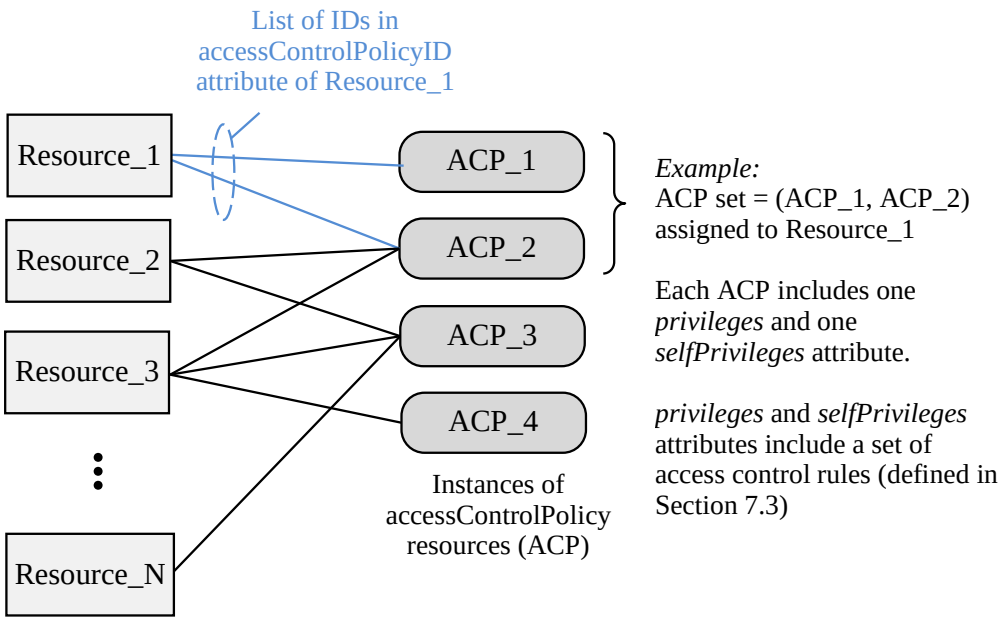
- **A high level Overview of the authorization architecture in Figure 6.2.2-1**
  - Policy Enforcement Point (PEP): making access control decision request
  - Policy Decision Point (PDP): Evaluation for access request
  - Policy Retrieval Point (PRP): Applicable authorization policies
  - Policy Information Point (PIP): Attributes for evaluating authorization policies
    - Release 1 does not support separation of PRP and PIP on different CSE from PDP.





Authorization (ch.7)

- **Access control mechanism**
  - Attribute based access control (ABAC)
  - Relation between Resource Instances and Access Control Policies in fig.7.1.1-1
    - privileges: 이 리소스를 참조하는 리소스들에게 적용되는 규칙들의 집합
    - selfPrivileges: <accesscontrolPolicy> 리소스 자체에 적용되는 "access control rule" 집합



Authorization (ch.7)

ETRI Creative Opinion
창의미래연구소

- **Access control mechanism**
  - Logic to evaluate privileges in fig. 7.1.5-1

acrs = { *acr*(1), *acr*(2), ..., *acr*(*k*), ..., *acr*(K) }

acr(*k*) = {*acr*(*k*)_accessControlOriginators, *acr*(*k*)_accessControlOperations, *acr*(*k*)_accessControlContexts}

Set of originator parameters. Examples:
{CSE-ID1, AE-ID1, AE-ID2}
{all}

Set of allowed operations. Examples:
{Create, Retrieve, Update, Delete, Discover, Notify}
{Retrieve, Discover, Notify}

Set (list) of M_*k* context constraints (number of elements M_*k* can be different for each *acr*(*k*)):
{*acr*(k)_accessControlContext(k, 1), …
…,
acr(*k*)_accessControlContext(k, m), …

Set of time windows defined by start and end time
Example:
{daily 04:30 – 06:00, 11:30 – 12:30, 22:15 – 00:30}

Set of location regions defined by list of objects representing geographical regions
Example:
{geoRegion1, geoRegion2, geoRegion3}

Set of IP addresses or address blocks
Example (IPv4):
{212.75.201.105, 88.77.0.0/16, 116.27.123.0/24}

Security framework (ch.8)

- **The security frameworks**
  - Direct Security Frameworks
    - the Symmetric Key Direct Security Framework
      - each pair of entities that need to authenticate each other has to be provisioned with its own shared symmetric key
    - the Certificate-Based Direct Security Frameworks
      - Public Key Certificate Flavours: Raw public key certificate, device certificate, CSE-ID certificate, AE-ID certificate, FQDN certificate (in MEF/MAF)
      - Path validation and certificate status verification
      - Credential configuration for certificate-based security frameworks
        - Entity's private signing key, entity's certificate (chain), CSE-ID certificate & AE-ID certificate
      - Information needed for certificate authentication of another entity
        - A public key identifier, a globally unique identifier (e.gl, OID or URI or FQDN) and trust ancho certificate
      - Certificate verification
  - Centralized Security Frameworks
    - the GBA (Generic Bootstrapping Architecture) Framework

  - RSPF vs. SAEF

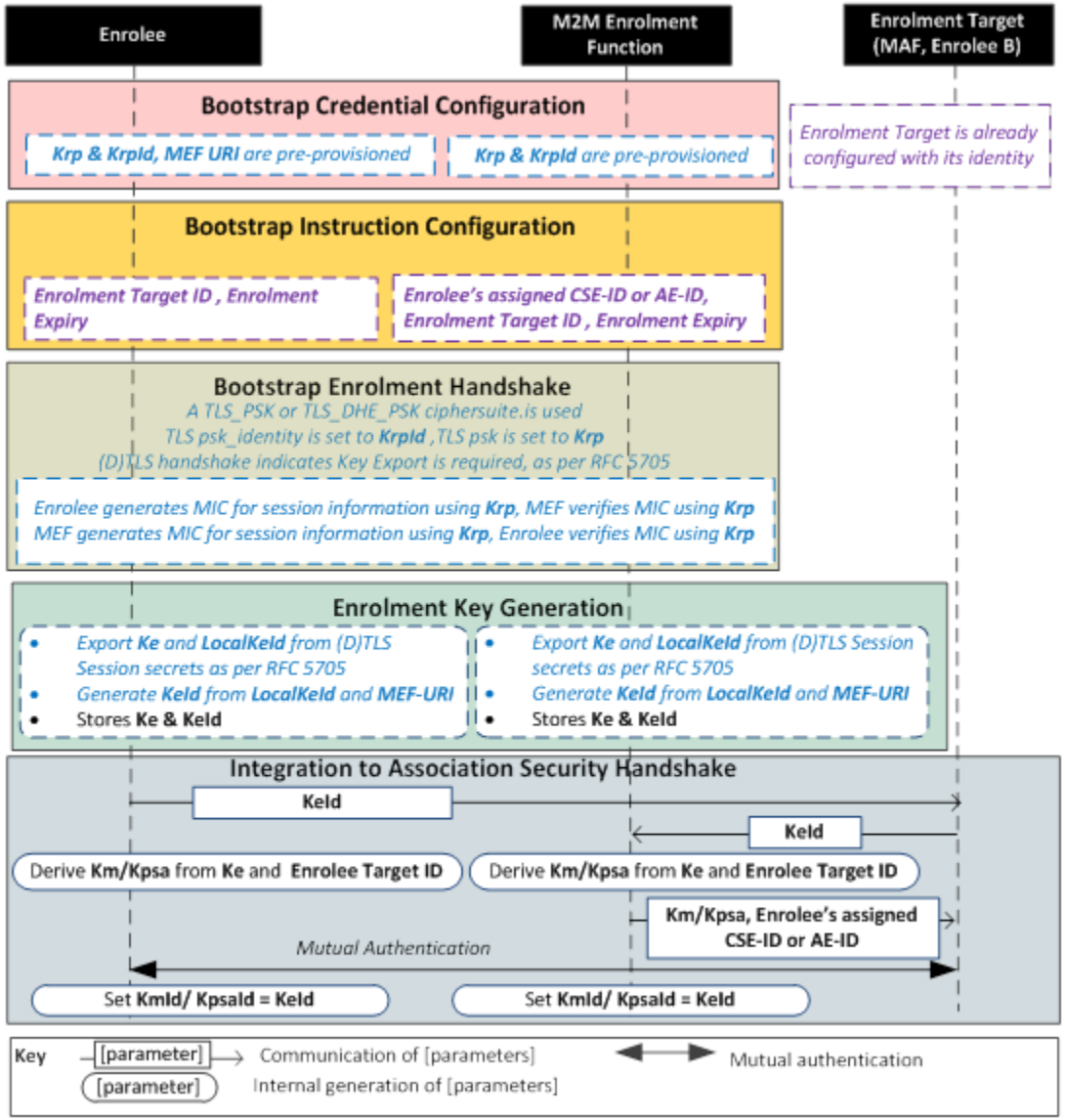
Remote Security provisioning framework (ch. 8.3)

- **The purpose of RSPF**
  - Security Bootstrap Frameworks enable the provisioning of a symmetric key shared between two entities
  - Either a CSE/AE and a M2M Authentication Function (MAF) or two CSEs/Aes
  - Usage of provisioned symmetric key
    - Provisioned Symmetric Key SAEF
      - Kpsa, KpsaID
    - MAF-based Symmetric Key SAEF
      - Km, KmId
- **Overview on RSPF**
  - Security bootstrap framework: Centralized RSPF
    - Pre-provisioned symmetric enrolee key RSPF
    - Certificate-based RSPF
    - GBA-based RSPF

Remote Security provisioning framework (ch. 8.3.2.1)

ETRI Creative Opinion
창의미래연구소

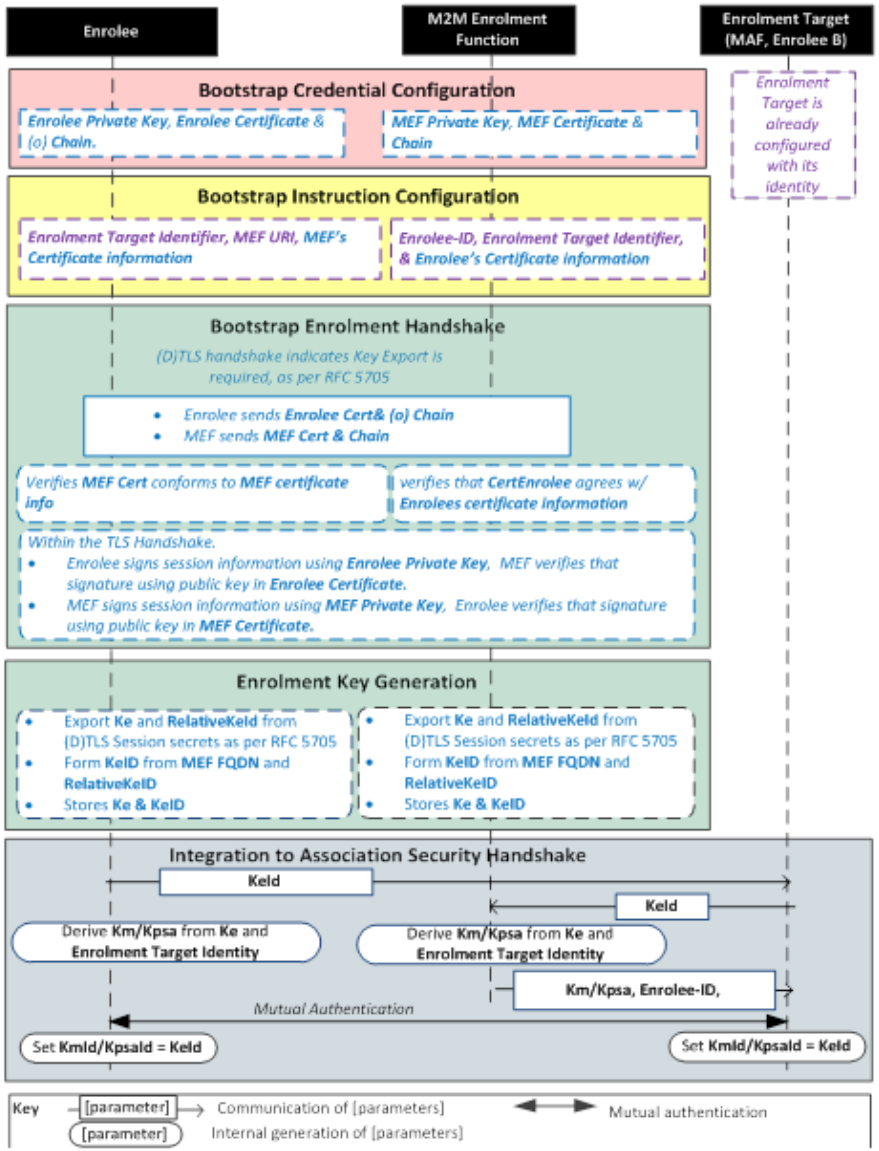
- Pre-Provisioned Symmetric Key RSPF in fig. 8.3.2.1-1



Remote Security provisioning framework (ch. 8.3.2.2)

ETRI Creative Opinion
창의미래연구소

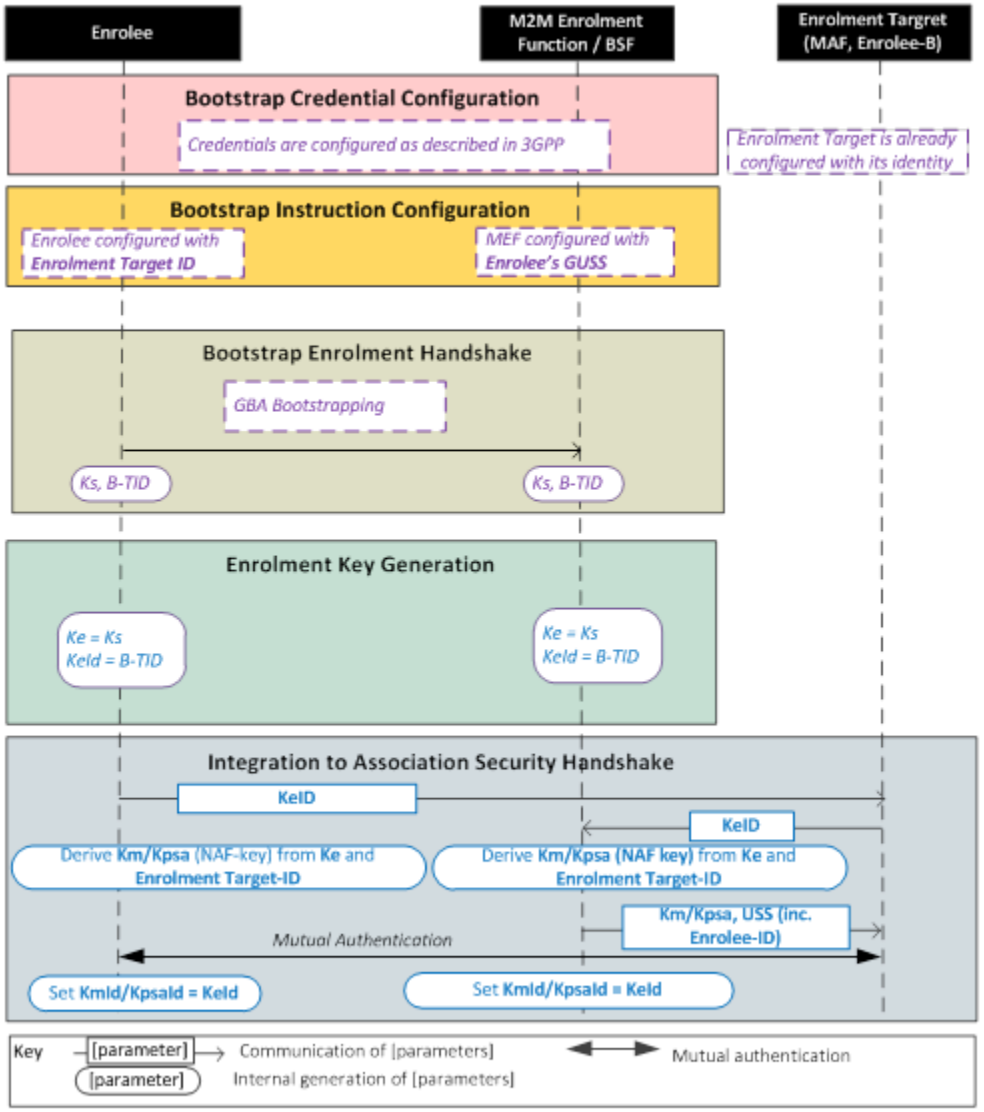
- Certificate-Based RSPF in fig. 8.3.2.2-1



Remote Security provisioning framework (ch. 8.3.2.3)

ETRI Creative Opinion
창의미래연구소

- GBA-Based RSPF in fig. 8.3.2.3-1



Security Association Establishment Frameworks(ch. 8.2)

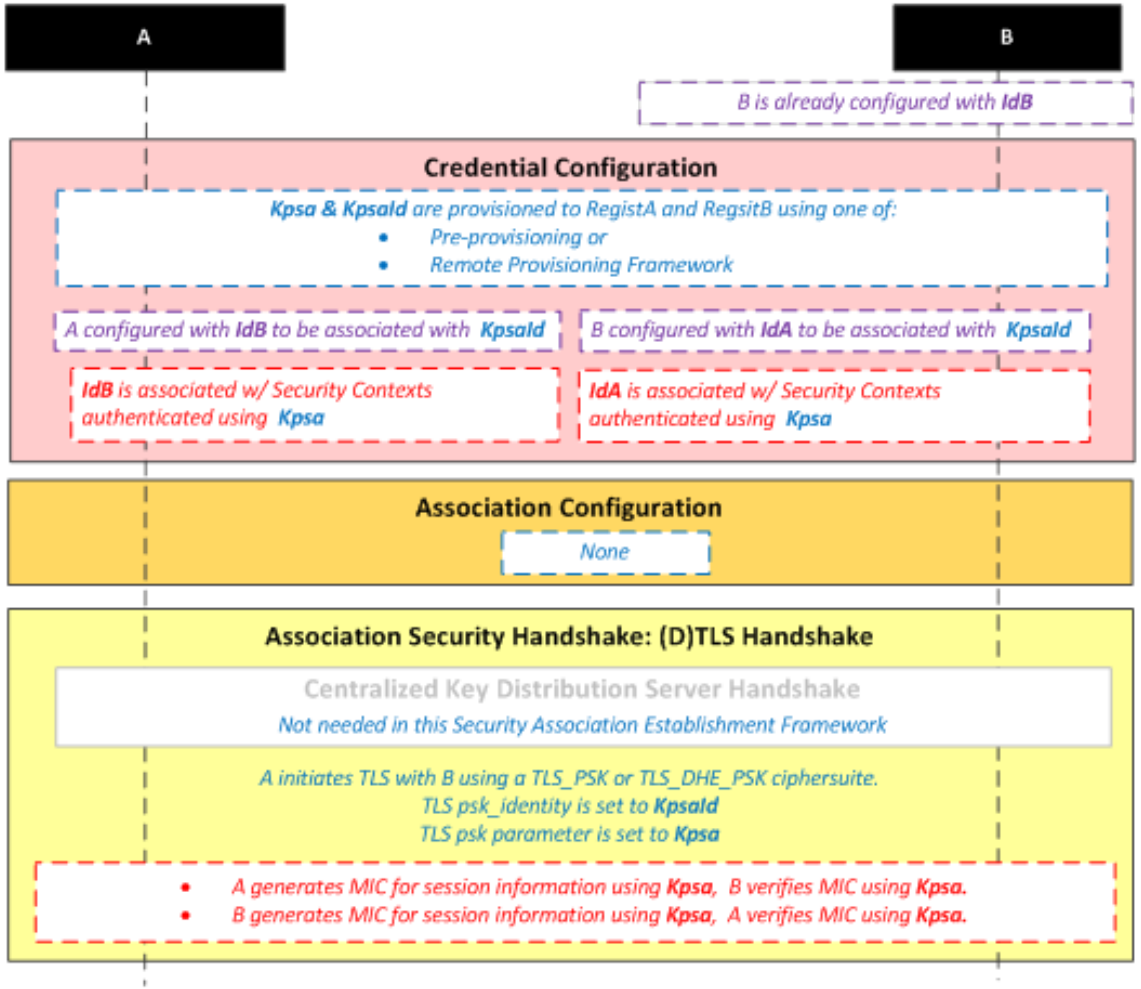
ETRI Creative Opinion 창의미래연구소

- **In the present document, security associations are restricted to single hop on Mcc, Mcc' or Mca reference point.**
- **The oneM2M system supports the following Security Association Establishment Frameworks:**
  - Direct Security Association Establishment Frameworks:
    - Provisioned M2M Secure Connection Key Security Association Establishment
    - Certificate-Based Security Association Establishment
  - Centralized Security Association Establishment Frameworks
    - GBA based Security Association Establishment
    - M2M Authentication Function (MAF)-based Security Association Establishment.
- **Procedural aspects of the SAEF**
  - Credential Configuration
  - Association Configuration
  - Association Security Handshake
    - Central Key Distribution Server Handshake

Security Association Establishment Frameworks (ch. 8.2.2)

ETRI Creative Opinion 창의미래연구소

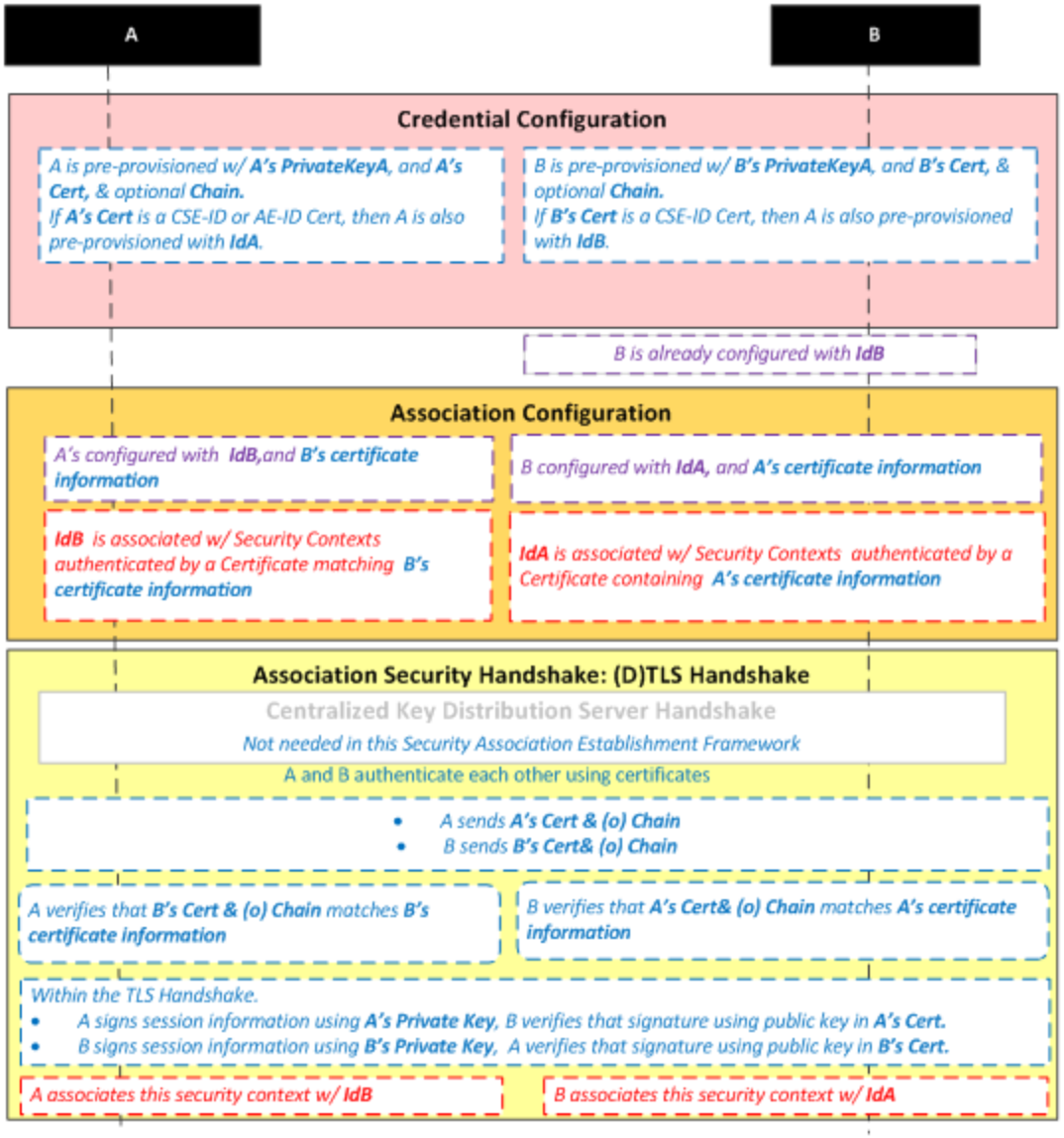
- **Direct SAEF**
  - Provisioned Symmetric Key SAEF
  - Using the Pre-Provisioned Secure Connection Key SAEF in fig. 8.2.2.1-1



Security Association Establishment Frameworks (ch. 8.2.2)

ETRI Creative Opinion 창의미래연구소

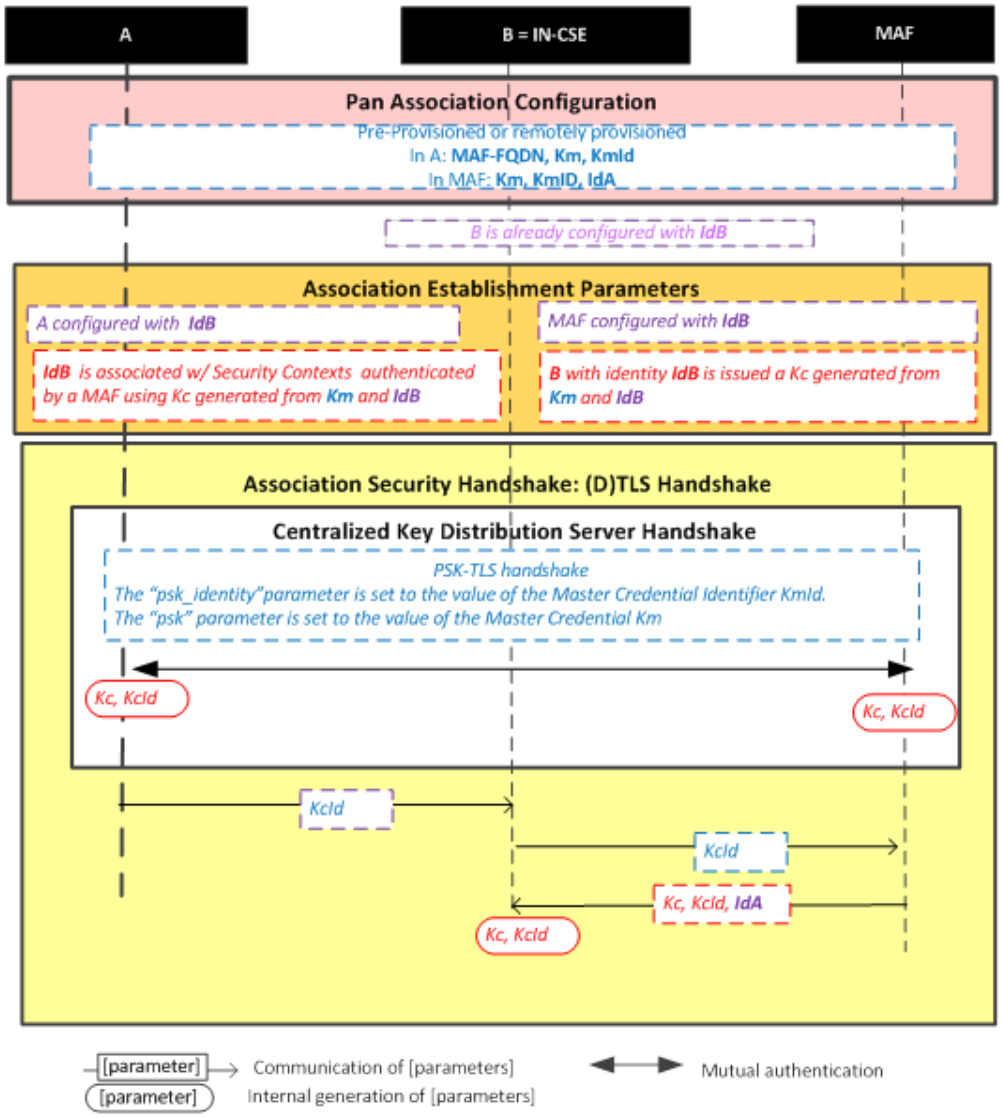
- **Direct SAEF**
  - Certificate-Based SAEF
  - Using the Certificate-Based SAEF in fig. 8.2.2.2-1



Security Association Establishment Frameworks (ch. 8.2.3)

ETRI Creative Opinion 창의미래연구소

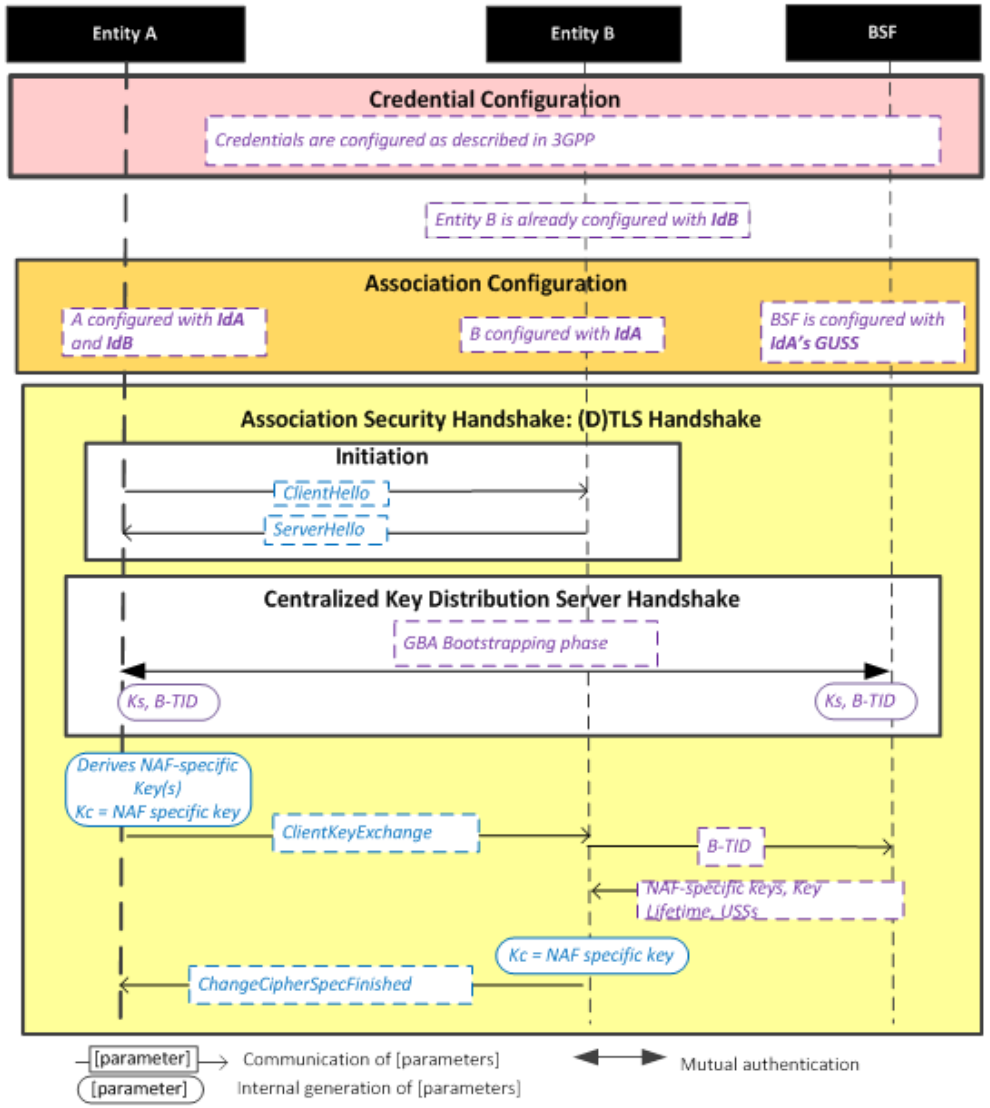
- **Centralized SAEF**
  - MAF-Based Symmetric Key SAEF
  - Using the MAF-Based Symmetric Key SAEF in fig. 8.2.3.1-1



Security Association Establishment Frameworks (ch. 8.2.3)

ETRI Creative Opinion 창의미래연구소

- **Centralized SAEF**
  - GBA-Based SAEF
  - Using the GBA-Based SAEF in fig. 8.2.3.2-1



Thank you

무지무지 감사합니다.

발표자 _ 박정수

이메일 _ pjs@etri.re.kr

연락처 _ 042-860-6514