[oneM2M] oneM2M 의 Trust Enablement Function(TEF) 표준문서 개발 현황

1. TEF 규격의 정의 및 작업 항목 개요

○ 작업항목 WI-0057 "TEF Interface 승인" : oneM2M TP#24 (2016.7)

- TEF(Trust Enabling Function)는 oneM2M의 생태계 구조 안에서 정의되는 entity들간의 security와 trust를 수립하는 목적으로 운영되는 기능을 정의한다. TEF에는 MEF(M2M Enrolment Function)와 MAF(M2M Authorization Function)가 포함되며, 이는 oneM2M 의 Trust Enabling Architecture(TS-0001)에 정의되는 부분이다.

- TP#24에 제출되어 승인된 해당 작업항목(WI-0057)은 퀄컴이 주도하고 있으며, 기존에 TS-0001(Functional Architecture) 및 TS-0003(Security Solution)에서 정의하고 있는 TEF를 구체화하여 TS 규격 문서로 개발하는 작업을 진행 중이다.

○ MEF와 MAF 간 프로토콜 정의 내용

- TS-0001 문서에 의하면, M2M 생태계에서 MEF는 M2M node를 운영하기 전 M2M 사업자의 서비스에 M2M 노드와 응용을 enrolment(등록)하고 configuration하는 기능을 담당한다. 한편 MAF는 M2M 서비스 운영 중 CSE와 AE의 identification 및 authentication, 종단 간 primitives 보안, 종단 간 data 보안 등을 가능하게 하는 중심 기능을 지정한다.
- MAF와 MEF는 서로 신뢰하는 주체들 (M2M 사업자 혹은 3rd party)에 의해 운영되는 것으로 (현재까지는) 정의되고 있다. 이들과 AE, CSE 등과는 서로 상호운영이 가능해야 하며 이들 간의 참조 점 정의, 새로운 일부 resource-type 정의, resource-type specific CRUD procedure 및 data types of the resource attributes은 추가로 정의되어야 함이 기존의 문서에 적시되어 있다.

○ MEF와 MAF 간 프로토콜 정의 내용

- WI-0057은 상기 추가로 정의해야 할 사항들과 함께 TEF에서 운영될 프로토콜 primitive들을 개발한다. TS-0003은 M2M entity들(AE 와 CSE 등)과 MEF(M2M Enrolment Function) 및 MAF (M2M Authorization Function) 간 연동을 전제한 security 프레임워크를 정의하고 있는데, (TS-0003 Security 개요: 별첨 참고) 해당 프레임워크는 다음의 security 프레임워크를 지정 하고 있다.
  - MEF-based Remote Security Provisioning Frameworks (RSPF)
  - MAF-based Security Association Establishment Framework (MAF-based SAEF)
  - End-to-End Security of Primitives (ESPrim)
  - End-to-End Security of Data (ESData)
- 이 중 MEF-based RSPF는 MEF와 MAF 간 상호통신을 필요로 한다. 상기의 security 프레임워크는 대개의 경우 (D)TLS에 기반하고 있으나 TEF 간 일부 파라미터는 전달이 곤란하여

이를 추가로 정의해야 한다는 것이 작업항목의 요점이다. 이에 따라 Mcc와 Mca에 운영할 별도의 프로토콜을 정의한다.

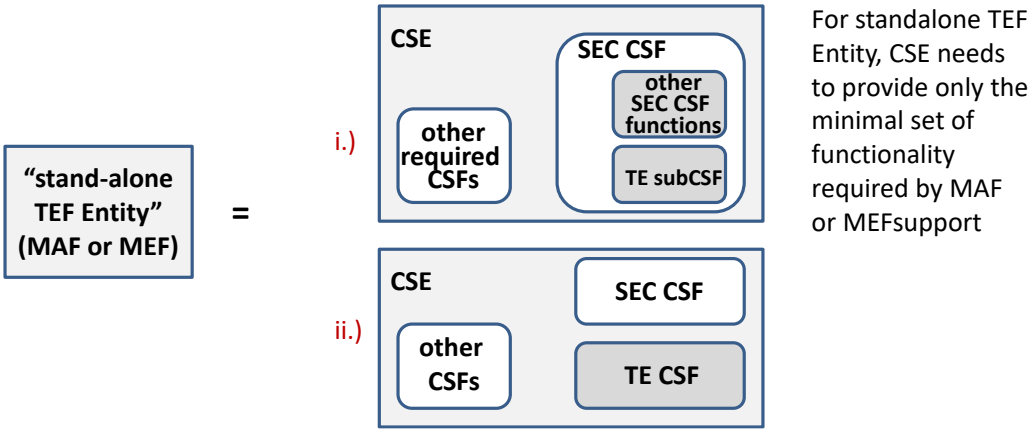
○ 작업 일정

- WI의 승인 이후 TP28에서 freeze, TP29에서 승인하는 일정을 목표로 추진 중이며, 예정대로 진행되면 해당 규격은 rel-3 규격 문서로 포함될 것으로 예상된다.
- Lead WG은 SEC(WG4)이며 TS 문서(TEF Interface Specification)로 개발 중인데, 본 작업 항목을 제안 한 퀄컴이 라포터/에디터로 진행 중이다.

2. TEF 기능의 독립화 방식을 지원하는 작업 항목 개정

○ oneM2M TP#25/ SEC WG (2016.10)에서 작업항목 WI-0057 revision

- 2016년 10월에 퀄컴은 작업 항목의 revision을 제출하였으며, 이를 통해 TEF modeling의 option 3을 추가하였다. 이는 "stand-alone TEF entity 방식"을 추가 제안한 것으로, 아래 [그림 1]에 보이는 예와 같이 기존의 SEC CSF와 별도로 TE CSF를 구현하는 것을 제안하여 승인되었다.
- 또 이로 인해 Trust enabling CSF가 생긴 것에 대응하는 message flow의 update와 향후 추진 방향을 정리하였다.



[그림 1] TEF의 구현 방식 (CSF기반의 구현 option - SEC CSF 의 내부 혹은 외부에 구현)

Ref: SEC-2016-0165R1

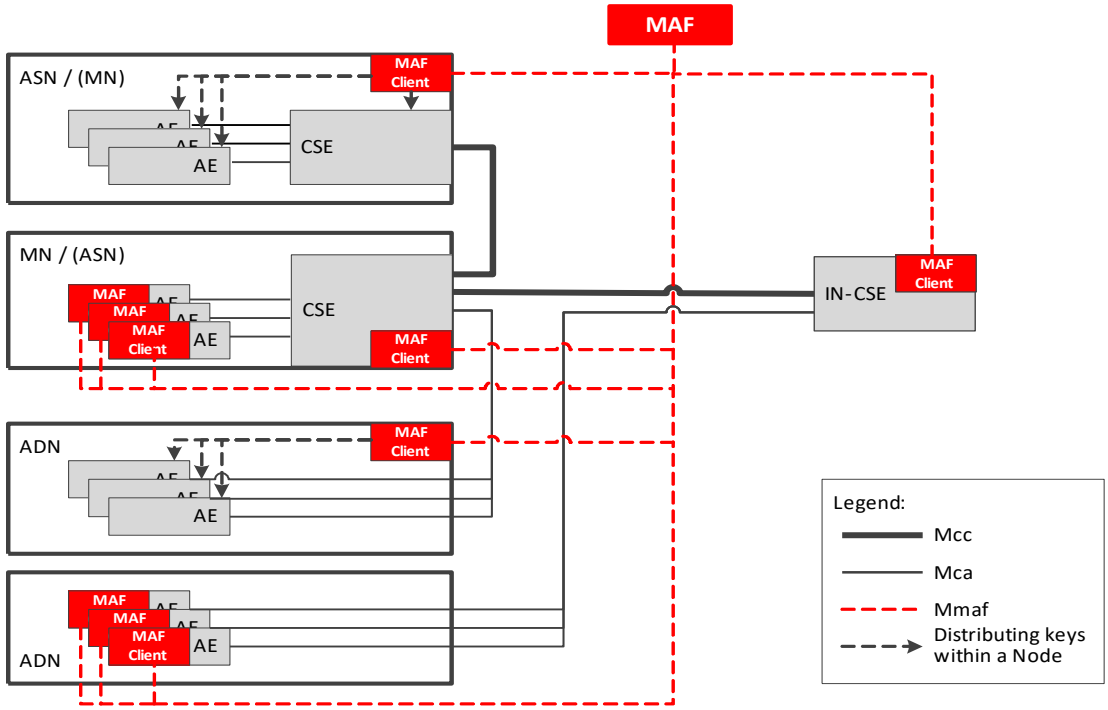
3. TP#26 (2016.12)의 TEF 관련 이슈 및 표준화 진행 정도

○ oneM2M TP#26에 제출된 3개의 문서 채택

- TP26에서는 퀄컴이 제출한 skeleton 문서, scope 문서, main body - base line 문서가 모두 승인되었고, SEC/ARC joint session을 통한 interface discussion을 진행하였다. 이를 통해 합의한

일정으로 TP26에 뒤이어서 (SEC26.1 등 추가회의를 통해) "MAF and MAF Interface Specification"draft를 만들 것을 예고하였다.

- 현재 버전의 body에서는 MAF와 MAF client 간의 참조점은 Mmaf로, MEF와 MEFclients 간의 reference point는 Mmef로 하여, 이를 정의하는 TS를 개발하고 있다. 추가되는 MAF 기능과 해당 interface Mmaf가 [그림 2]와 같이 제시되어 있다.



[그림 2] TS-0003 (Security Solution) oneM2M security 구조 개요

4. oneM2M TP#27 (2017.2)의 TEF 진행

○ DM based MEF (SEC-0017R2, 퀄컴)

- 2017년 2월 (TP#27)에 퀄컴은 TS-0032 v0.0.2(MAF&MEF)에 대해 입력하고 resource type에 대한 정의를 진행하였다.

- 퀄컴이 입력한 기고서가 제안하는 것은 MEF interface의 resource 정의라고 볼 수 있는데, 해당 내용이 특히 MAS WG의 device configuration 문서에 영향을 주므로 이를 상호 조율/동기화시키는 작업이 중요하게 다루어졌고, MAS WG 과의 협력 세션에서 논의되었다.

- MAS WG 의 TS-0022(WI-0030)은 2017년 2월 약 85%의 완성율을 보이고 있으며 현재 문서 구조를 일부 조정하고 authentication profile, credential 등에 대한 부분을 정리하고 있다.

- Qualcomm은 MEF의 운용에 있어 MEF client가 등록을 위해 임의 시점에 credential을 필요로 할 수 있다는 점을 지적하여 management of credential이 필요하며, 이는 remote management에

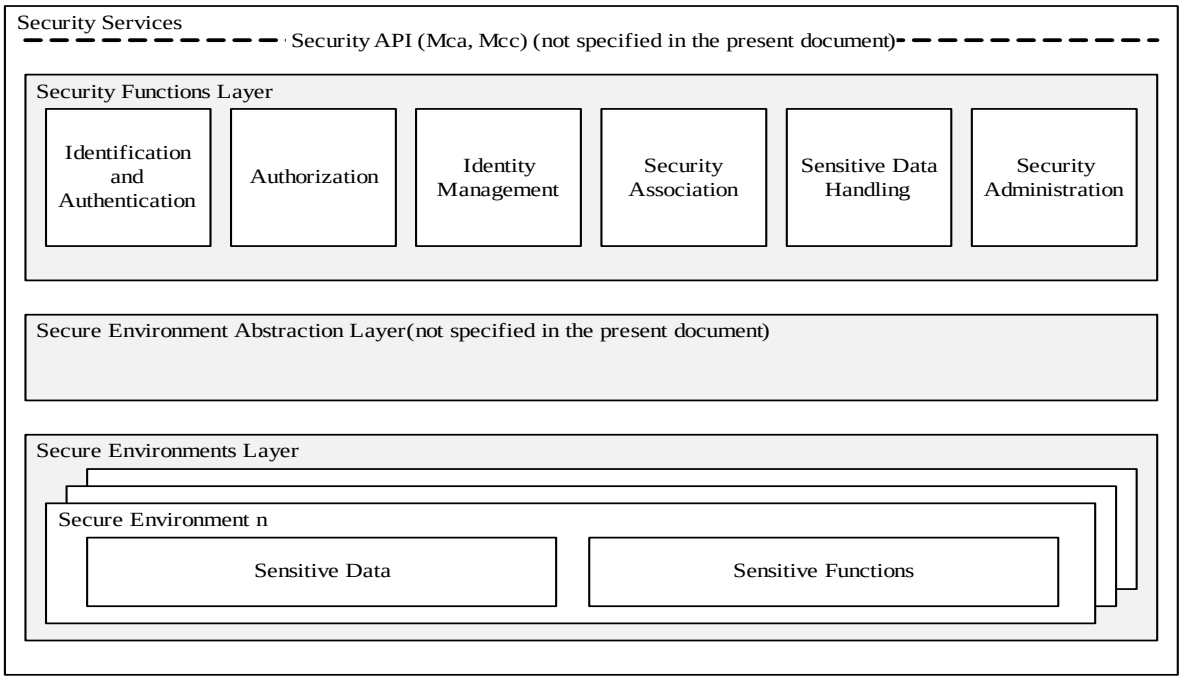
해당함을 적시한다.

- 해당 내용은 TS-0022 가 정의하고 있는 resource type 중 <mgmtObj> 부분을 참조하여, 다음 내용을 반영해 줄 것을 제안하였다.
- 기본적으로, MEF 는 3가지 종류의 interaction을 지원가능
  - Mmaf <symmKeyReg> operation
  - EST (RFC7030)을 사용하는 certification 등록(MEF는 EST 서버역할)
  - 기타 DM 기능 사용
- 그외 MAS와의 동기화를 위한 action이 제안되었고, TS-22 및 TS-32의 영향, TS-01로의 영향등에 대해 추가로 검토할 것이 요구되었다.

[별첨] oneM2M 의 security 구조 개요

○ oneM2M Security Solution 규격서 TS-0003을 참조

- TS-0003은 M2M security architecture를 다음 그림과 같이 정의
- security layers:
  - security serviced layer, security function layer, secure environment abstraction layer, secure environments layer로 나눔.
  - 이중 secure function layer가 Mcc 및 Mca 인터페이스 에 나타나는 6가지 기능 집합임 (Identification, Authentication, Authorization, Security Association, Sensitive Data Handling and Security Administration.)
  - secure service layer 는 Access management, sensitive data handling, security association establishment, security administration, identity protection 의 서비스를 제공함



- layer 간 상호작용:

• M2M CSE들 간의 절차 이전에 하부의 Network Service Layer의 connectivity setup이 이루어짐. 이로부터 시작하여 CSE 계층의 독립적인 Security Provisioning and Security Association Establishment procedure가 가동됨

• Service layer 레벨에서는 이 결과 TLS 혹은 DTLS 세션이 만들어져 인접한(hop-by-hop) AE/CSE 간의 데이터 교환을 보호한다. 만일 untrusted 중간노드를 통해 정보를 전송할 때 프라이버시를 보호할 필요가 있는 AE 들은 그들 간 direct security association을 지원하여 교환되는 자원의 암호화를 할 수 있음.

- Enrolment phase:

• M2M 장치는 일반적으로 provisioning과 configuration 이후 operation에 들어감. 이의 과정을 실현하는 데는 몇 가지 방법과 경우가 있으나 기본적으로 M2M service provider를 선택하여 접속하는 것이 핵심. 이때 3rd party 혹은 UN-SP domain에서 이들의 enrolment를 지원하는 기능이 MEF 및 MAF

• Security Association Establishment Framework 에 따르면 다음과 같은 절차들이 가능함

(1) Provisioned Symmetric Key Association Establishment Framework

(2) Certificate-based Security Association Establishment Framework

(3) M2M Authentication Function (MAF) Security Association Establishment Framework

안재영 (ETRI 초연결통신연구소 책임연구원, ahnjy@etri.re.kr)