Matter 표준 프로토콜 Fabric 형성을 위한 커미셔닝 프로세스 분석 연구

홍서영, 지영민*, 권동우*
성결대학교, *한국전자기술연구원
hongsy20@sungkyul.ac.kr, *ym.ji@keti.re.kr, *dwkwon@keti.re.kr

Analysis study of commissioning process for building Fabric of Matter Standard Protocol

Seoyeoung Hong, Youngmin Ji*, Dongwoo Kwon*
Sungkyul Univ., *Korea Electronics Technology Institute (KETI)

요 약

최근 몇 년간 사람들의 삶을 편리하게 해주는 스마트홈(smart home)이라는 개념은 큰 주목을 받아왔다. 그러나 다양한 제조사가 서로 다른 통신 프로토콜을 사용하고, 개별적인 플랫폼을 운영하고 있기에 사용자는 하나로 통합된 스마트홈 시스템을 사용할 수 없다는 불편함이 존재한다. 따라서 장치와 시스템의 호환성 확보를 위해 통합 오픈 소스 연결 표준인 Matter가 등장하였다. 이는 인터넷 프로토콜(Internet Protocol, IP) 기반 개방형 스마트홈 연동표준으로 기존의 장치 제조사 중심의 스마트홈 산업의 주도권을 사용자 친화적으로 변할 수 있도록 한다. 본 논문에서는 Matter 표준을 준수하는 장치의 홈 구성 과정 중, 여러 기기가 상호 운용될 수 있는 환경인 Fabric 형성을 위한 커미셔닝 프로세스에 관한 분석 연구를 수행한다.

Ⅰ. 서 론

최근 몇 년간 사람들의 삶을 더욱 편리하게 해주는 스마트홈(smart home)이라는 개념은 큰 주목을 받아왔다. 그러나 다양한 제조사가 서로 다른 프로토콜을 사용하고, 개별 플랫폼을 운영하고 있기에 사용자는 하나로 통합된 스마트홈 시스템을 사용할 수 없다는 불편함이 발생한다.

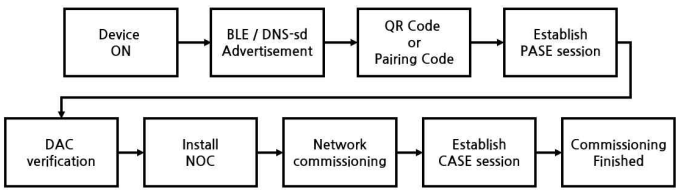
Matter는 이러한 문제점을 개선하기 위해 CSA(Connectivity Standards Alliance)가 주도하여 개발한 통합 오픈 소스 연결 표준이다[1]. 이는 보편적이고 잘 알려진 IP 기술을 활용한 개방형 스마트홈 연동표준을 목표로 하며, IoT 장치 간, 장치와 스마트홈 플랫폼 간 통신을 지원한다. Matter는 다양한 스마트홈 장치를 하나의 플랫폼에 연결해 원활하게 동작할 수 있도록 통합하며, 안전하게 통신할 수 있는 방식을 제공한다. 이를 통해 사용자들은 제조사와 관계 없이 장치를 구매할 수 있고, 스마트홈 기기, 플랫폼, 모바일 앱을 하나의 애플리케이션으로 연동하여 사용할 수 있다. 또한 기존의 C2C(Cloud to Cloud) 방식이 아닌 로컬 내 연결을 지원하기에 제어 신호의 속도가 빠르다는 장점을 가지고 있다. 이는 기존의 장치 제조사 중심의 스마트홈 산업의 주도권을 벗어나 사용자 친화적인 표준으로써 미래 스마트홈 산업의 발전에 긍정적인 영향을 줄 것으로 기대된다.

따라서 본 논문에서는 Matter 표준을 따르는 여러 기기가 상호 운용될 수 있는 환경인 Fabric 형성을 위한 커미셔닝(commissioning) 프로세스에 관한 분석 연구를 진행하고자 한다.

Ⅱ. 본론

2.1.커미셔닝

커미셔닝이란, Matter 기기가 홈에 구성되기 위한 과정으로 새로운 장치에 Fabric 사용자 인증 정보를 할당하는 프로세스를 말한다[2]. Fabric은 여러 Matter 노드가 상호 운영되는 환경이며, 커미셔닝 프로세스에는 커미셔닝을 수행하는 장치인 커미셔너(commissioner)와 커미션 중인 새로운 장치 커미셔니(commissionee)가 존재한다.



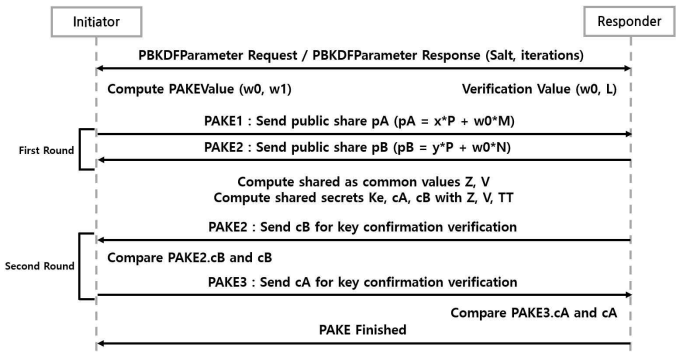
<그림 1> 커미셔닝 프로세스

<그림 1>은 커미셔닝 프로세스를 나타낸 것이다. 장치의 전원이 켜지면 블루투스 저전력 에너지(Bluetooth Low Energy, BLE), DNS-SD 등을 활용해 자신을 알리기 위한 광고를 시작한다. 커미셔너는 장치의 본체 혹은 별도의 위치에 존재하는 QR 코드를 스캔하거나 수동 페어링 코드를 입력하여 커미셔닝 프로세스에 필요한 인증 정보가 담긴 온보딩 페이로드(onboarding payload)를 얻는다. 두 기기의 커미셔닝은 커미셔너가 획득한 온보딩 페이로드의 Discriminator와 일치하는 커미셔니의 광고 속 Discriminator를 발견하면 시작된다.

커미셔닝은 PASE(Passcode Authenticated Session Establishment)와 CASE(Certificate Authenticated Session Establishment) 두 가지의 보안 세션을 설정한다. 이를 통해 안전한 방법으로 신원을 확인하고 키를 교환할 수 있으며, 최종적으로는 장치의 통신을 암호화할 수 있는 양쪽에 공유되는 세션 암호화 키를 생성한다. PASE 세션은 장치 인증 단계, 노드 운영 자격 증명 설치와 같은 신원 확인 과정에서의 통신에서 사용되고, CASE 세션은 커미셔닝 프로세스의 성공적인 완료 및 Matter Fabric 내 노드 간의 안전한 통신을 유지하기 위해 사용된다.

2.2. PASE

PASE는 커미셔닝 시작 전에 획득한 온보딩 페이로드 속 비밀번호를 기반으로 하는 첫 번째 세션 설정 과정이다. <그림 2>는 PASE 설정 과정으로 이는 PBKDF(Password-Based Key Derivation Function)를 활용한 PAKE(Password-Authenticated Key Exchange)를 통해 수행된다.



<그림 2> PASE Protocol

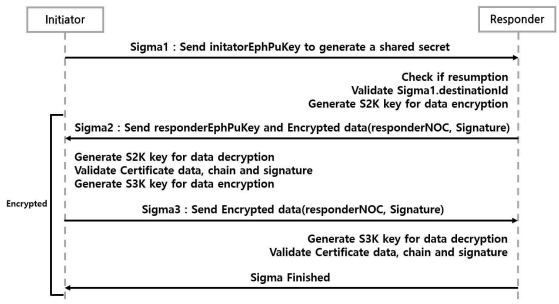
PBKDF는 비밀번호를 보호하는 데 널리 사용되는 방법으로 잘 알려진 비밀번호를 임의의 데이터인 솔트(Salt)와 사용자 지정 반복 횟수(iteration)의 반복적인 해싱을 통해 안전한 비밀번호로 변환한다. 커미셔너는 PBKDFParamRequest 명령을 통해 파라미터를 전달받으며, 이는 PAKE 프로토콜 실행 중에 사용된다.

PAKE는 비밀번호 공개 위험 없이 강력한 공유키 파생을 위해 두 당사자 간에 실행되는 프로토콜이다. Matter는 한 당사자만이 비밀번호를 직접적으로 사용하고, 다른 당사자는 검증 값을 사용하는 SPAKE2+ 프로토콜을 사용하며, 기본 그룹 타원곡선으로는 NIST P-256을 사용한다. 커미셔너는 PBKDF를 통해 획득한 비밀번호를 안전하게 변환하고, 이에 기반하여 PAKEValue 쌍을 생성한다. PAKE1, PAKE2에서 커미셔너와 커미셔니는 타원곡선에 기반한 각자의 공개 공유 키인 pA, pB를 계산하여 전달하고, 이 값을 활용해 공통의 값으로 도출되는 비밀 Z, V를 계산한다. 도출된 비밀은 프로토콜 실행 상태를 기록한 전사본 TT(Transcript)와 함께 공유키 Ke와 키 확인 값 cA, cB 생성에 사용된다. 키 확인 값 cB는 PAKE2, cA는 PAKE3에서 전송되며 각자 생성한 값과 비교하여 일치하는 경우, 공통의 공유키 Ke가 생성되었음을 알 수 있다. 커미셔니는 PakeFinished 메시지로 PAKE 프로세스가 완료되었음을 알리고, 커미셔너와 커미셔니는 공유키 Ke를 활용해 세션 암호화 키 I2RKey, R2IKey, AttestationChallenge를 생성한다. I2RKey, R2IKey는 각각 커미셔너와 커미셔니가 메시지를 암호화하고 복호화하는 데 사용되는 대칭 키이며, AttestationChallenge는 현재 세션 파악을 위한 키로 사용된다.

PASE 프로토콜을 통해 생성된 세션 암호화 키는 장치 증명과 노드 운영 자격 증명을 설치하는 과정의 통신에서 사용되며, 공개키 인프라(Public Key Infrastructure, PKI) 구조를 사용한다. 모든 Matter 장치는 장치 증명을 위해 X.509 v3 형식의 장치 증명 인증서(Device Attestation Certificate, DAC)를 가지고 있다. 커미셔너는 커미셔니로부터 해당 인증서를 전달받아 장치의 신원을 검증하고, 이에 대한 적절한 개인 키 보유 여부를 확인한다. 장치 증명이 완료되면 커미셔니에게 CSR(Certificate Signing Request)을 요청하며, 이에 대한 응답을 기반으로 노드 운영 자격 증명서(Node Operational Certificate, NOC)를 생성하고 이를 루트 인증서와 함께 커미셔니에게 설치한다. 노드 운영 자격 증명서는 Matter Fabric 내 노드가 해당 장치를 식별할 수 있도록 한다. 장치 증명과 노드 운영 자격 증명 설치가 성공적으로 이루어진 경우, 커미셔너는 커미셔니에게 운영 네트워크를 설정하고 PASE 세션은 종료된다.

2.3. CASE

CASE는 장치에 설치된 노드 운영 자격 증명을 사용해 세션 내 후속 통신을 안전하게 보호하기 위한 두 번째 세션 설정 과정이다.



<그림 3> Basic CASE Protocol

<그림 3>은 기본 CASE 설정 과정으로 본 논문에서는 재개의 경우가 아닌 기본 CASE 설정 과정만 포함한다. 이는 SIGMA 프로토콜과 IPK(Identity Protection Key)를 사용해 더 나은 신원 보호를 제공하며, 노드 운영 인증서를 교환하고 동일 Fabric에 존재하는지 확인하는 과정이 포함된다. 또한 새로운 세션 설정 외에 이전 세션의 정보를 활용하여 빠르게 세션을 재개할 수 있는 수단인 재개(resumption) 메커니즘을 제공한다.

CASE 세션은 일시적으로 타원 곡선 공개 키를 교환하여 공유 비밀을 생성하며, 신원 증명을 위해 노드 운영 인증서를 교환하고 해당 인증서에 대한 개인 키 보유 여부도 확인한다. 커미셔너는 통신을 시작하기 위해 임시 키와 식별자를 생성해 Sigma1 메시지를 전송하고, 이를 수신한 커미셔니는 메시지 필드 값을 확인하여 재개인지 아닌지 확인한다. 재개가 아닌 경우 설치된 노드 운영 인증서를 순회하며 Sigma1의 destinationID 값과 일치하는 Fabric과 인증서를 발견하고, 서명과 함께 해당 정보를 암호화하여 전송한다. 데이터 암호화와 무결성 보호를 위해 Sigma2, Sigma3에서는 공유 비밀을 사용해 S2K, S3K 임시 키를 생성하며, 이는 세션 설정이 완료되면 폐기된다. 커미셔너와 커미셔니는 수신한 인증서에 담긴 데이터의 일치성 여부와 체인의 유효성 검증을 수행한다. 위의 과정이 성공적으로 완료되면 세션 내 후속 통신을 보호하기 위한 세션 암호화 키 I2RKey, R2IKey, AttestationChallenge를 생성하며, 커미셔니는 자신이 속한 운영 네트워크의 Fabric 내 다른 노드처럼 서로 통신하고, 동작할 수 있다.

Ⅲ. 결론

본 논문에서는 Matter 장치가 상호 운영될 수 있는 환경인 Fabric 형성을 위한 커미셔닝 프로세스에 관한 분석 연구를 진행하였다. Matter는 기기 간 연결성 및 호환성을 강조하며, 안전한 통신을 위해 향상된 보안 기능을 제공한다. 이를 위해 비밀번호 기반 신원 인증을 위한 PASE 세션과 인증서 활용 후속 통신을 위한 CASE 세션을 도입하여 기기 간 통신 과정을 보안 측면에서 안전하게 강화하고 있다.

그러나 현재 커미셔닝 프로세스에서는 암묵적으로 커미셔너에 대한 신뢰를 부여하고, 이를 검증하는 단계가 포함되어 있지 않다. 또한 잠재적인 위험은 Matter 장치에서 발생한다고 가정하고 있다. 이는 악성 커미셔너 혹은 컨트롤러가 Fabric 내 장치에 액세스하고, 악의적으로 공격할 수 있다는 것을 시사한다. 따라서 커미셔닝 프로세스에서 커미셔너의 신뢰성을 검증하는 단계가 포함되는 방향으로 개선이 필요할 것으로 생각된다.

ACKNOWLEDGMENT

본 연구는 산업통상자원부(MOTIE)와 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (No. 20212020800120)

참 고 문 헌

[1] IOT (2024) CSA. Available at: https://csa-iot.org/.

[2] Connectivity Standards Alliance. Matter Specification Version 1.2, Oct 2023.