전기차 충전기에서 Matter DAC와 OCPP 정체성의 안전한 바인딩기법에 관한 연구

김진현, 김기형*
아주대학교, *아주대학교

dbchre@ajou.ac.kr, *kkim86@ajou.ac.kr

ASecure Binding of Matter DAC and OCPP Identities for EVSE Systems

Kim Jin Hyun, Kim ki Hyung*
ajou Univ., *ajou Univ.

요 약

전기차 충전기(EVSE)가 집 안에서는 Matter 기반 스마트홈에, 바깥으로는 OCPP 기반 클라우드 과금·운영 시스템에 동시에 연결되는 구조가 점점 보편화되고 있다. 그러나 Matter는 디바이스 정품성과 Fabric 멤버십(DAC/NOC)에 초점을 맞추고, OCPP는 충전기 식별자(CPID), TLS, 사용자·계약 정보에 기반해 세션 인가와 과금을 수행하므로, 두 정체성이 서로 독립적으로 관리될 때 DAC 클론, 충전기 교체, CPID 설정 오류 상황에서 기기 신뢰와 과금 신뢰가 어긋나는 보안 공백이 발생할 수 있다.

본 논문은 EVSE별 Matter 정체성(DAC/NOC)과 OCPP 정체성(CPID/TLS)을 해시와 서명으로 하나의 튜플로 묶는 “DAC–OCPP 바인딩 자격증명(Binding Credential)”을 제안한다. 이 자격증명을 온보딩 시점에 생성해 백엔드에 저장하고, 충전 세션 시작 시 현재 구성과 비교·검증함으로써 클론·스왑·오구성을 정체성 불일치 이벤트로 탐지하는 방법을 보인다. 또한 EVSE·브릿지·CSMS 단에 배치하는 구현 방안과 소프트웨어 테스트베드 기반 평가 계획을 통해, 제안 기법이 Matter–OCPP 융합 EVSE 환경에서 기기 신뢰와 과금 신뢰를 연결하는 실용적인 보안 구성요소가 될 가능성을 논의한다.

Ⅰ. 서 론

전기차 충전기(EVSE)는 이제 단순한 전력 설비가 아니라, 로컬 스마트홈과 클라우드 운영 시스템을 동시에 잇는 노드로 동작한다. 가정용·상업용 충전기는 집 안에서는 스마트홈 허브나 HEMS(Home Energy Management System)와 연동되고, 외부로는 충전 사업자의 CSMS(Charging Station Management System)와 연결되어 과금, 모니터링, 펌웨어 업데이트를 수행한다.

표준 관점에서 보면, 스마트홈 영역에서는 Matter가 EVSE를 공식 기기 타입으로 포함하면서 로컬 네트워크에서 충전 제어를 담당하고, 백엔드 영역에서는 OCPP가 사실상 표준으로 자리 잡아 충전 세션 관리와 과금 기능을 담당한다. 따라서 하나의 EVSE가 “로컬에서는 Matter, 클라우드에서는 OCPP”라는 하이브리드 구조로 운용되는 것은 자연스러운 진화 방향이다.

문제는 두 프로토콜의 \emph{신뢰 모델}이 서로 다르다는 점이다. Matter는 디바이스 인증서(DAC)와 운영 인증서(NOC)를 통해 “이 기기가 정품인가, 이 Fabric의 합법적인 멤버인가”를 검증한다. 반면 OCPP는 충전기 식별자(CPID), TLS, 사용자·계약 정보를 기반으로 “어느 충전기에서, 어떤 계약으로, 누구에게 얼마를 청구할 것인가”를 결정한다. 실제 구현에서는 Matter 쪽 정체성과 OCPP 쪽 정체성이 별도 설정·운영되기 때문에, DAC 클론, 충전기 교체(swap), CPID 설정 오류(misbinding)가 발생하면 기기 정품성에 대한 신뢰와 과금·운영에 대한 신뢰가 서로 어긋나는 보안 공백(trust gap)이 생길 수 있다.

본 논문은 이러한 공백을 줄이기 위해 EVSE별 Matter 정체성(DAC/NOC)과 OCPP 정체성(CPID/TLS)을 하나의 정체성 튜플로 정의하고, 이를 해시와 서명으로 고정하는 “DAC–OCPP 바인딩 자격증명”을 제안한다. 핵심 아이디어는 EVSE가 처음 온보딩될 때 “정상 정체성 스냅샷”을 만들어 서명해 두고, 이후 각 충전 세션 시작 시 현재 구성과 비교하여 정체성 불일치 여부를 검증하는 것이다.

Ⅱ. 본론

2.1 하이브리드 EVSE 환경과 문제 시나리오

하이브리드 EVSE 환경은 다음과 같이 단순화할 수 있다.

- 로컬 도메인: EVSE 또는 브릿지가 Matter Fabric에 가입해 DAC/NOC를 보유하고, 스마트홈 허브·앱이 Matter 명령으로 충전기를 제어한다.
- 클라우드 도메인: 동일 EVSE가 OCPP를 통해 CSMS에 연결되어 CPID와 TLS 설정을 가지며, 사용자·계약 정보에 따라 세션 인가와 과금이 이루어진다.

이때 Matter와 OCPP 정체성 사이를 직접 묶어주는 표준 메커니즘이 없기 때문에, 다음과 같은 문제가 현실적으로 발생할 수 있다.

1. **DAC 클론**: 정품 EVSE A에서 DAC를 추출해 다른 위치의 EVSE B에 주입하면, Matter 입장에서는 B도 정품처럼 보이나 OCPP 입장에서는 다른

CPID·위치에서 트래픽이 발생한다.

2. **EVSE 교체(swap)**: 현장에서 EVSE A를 제거하고 B를 설치하되, 설정 편의를 위해 CPID_A를 그대로 재사용하면, CSMS는 “CPID_A=원래 장비”로 믿지만 실제 물리 장비는 B로 바뀐다.

3. **CPID 설정 오류(misbinding)**: 설치자가 여러 EVSE와 CPID를 섞어 잘못 매핑하면, 과금·로그 데이터가 잘못된 충전기에 귀속된다.

이 세 가지는 공격이든 실수든 공통적으로 “Matter에서 보는 기기 정체성과 OCPP에서 보는 충전기 정체성이 일치하지 않는 상황”이라는 점에서 보안·신뢰 문제를 유발한다.

2.2 DAC–OCPP 바인딩 자격증명

제안 기법은 EVSE별로 Matter·OCPP 정보를 하나의 정체성 튜플로 묶고, 이를 CSMS 서명으로 고정해 두었다가 나중에 다시 비교하는 방식이다.

1. **정체성 튜플**
   EVSE x에 대해 다음을 묶어 정적 정체성으로 본다.
   `ID_x = (DAC_x, NOC_x, CPID_x, TLS_x, meta_x)`
   여기서 meta_x는 설치 위치, 설치 시각 등 선택적인 정보이다. 세션별 사용자·계약 ID는 기존 OCPP 인가 흐름에서 별도로 처리한다.

2. **온보딩 시 바인딩 생성**
   EVSE가 Matter Fabric에 가입하고 OCPP로 CSMS에 등록되는 시점에, CSMS는 ID_x를 직렬화·해시한 뒤, 자체 서명키로 서명한 값을 “바인딩 자격증명 BC_x”로 생성한다. (ID_x, BC_x) 쌍은 백엔드 DB에 저장되며, “이 EVSE의 정상 정체성 스냅샷” 역할을 한다.

3. **충전 세션 시작 시 검증**
   충전 세션이 시작되면 CSMS는 현재 관측되는 정보로부터 ID_x^{current}를 만들고, 저장된 BC_x를 검증해 얻은 해시와 ID_x^{current}에 대한 해시를 비교한다. 해시가 같으면 MATCH, 다르면 MISMATCH로 판정한다. MISMATCH는 DAC 클론, EVSE 교체, CPID 오구성 등 정체성 변형이 있었음을 의미하며, 운영자가 추가 분석을 수행할 수 있다.

2.3 사용자 관점 확장과 구현 방향

바인딩 자격증명은 백엔드 내부 로직으로만 사용해도 의미가 있지만, 사용자 경험 측면으로 확장할 수도 있다. 예를 들어 모바일 앱에서 충전기를 선택하거나 QR 코드를 스캔할 때, “현재 이 물리 충전기가 등록된 정체성과 일치하는지”를 CSMS에 질의하고, 그 결과를 “Charger Identity Card” 형태로 보여줄 수 있다. 사용자는 충전기 이름·위치와 함께 “검증 완료” 또는 “정체성 불일치 가능 성 있음” 표시를 보고, 낯선 장소에서 이상 징후를 직관적으로 인지할 수 있다.

구현 측면에서는 바인딩 검증 로직을 EVSE, 브릿지, CSMS 중 어디에 둘지 선택해야 한다. EVSE 단에 배치하면 로컬에서 바로 차단할 수 있지만 하드웨어 제약이 있고, CSMS 단 배치는 필드 수정이 적은 대신 주로 모니터링·경고 용도에 가깝다. 현실적인 도입 전략으로는 CSMS 단에서 탐지·로그용으로 먼저 도입한 뒤, 필요에 따라 EVSE·브릿지 펌웨어로 점진 확장하는 방식을 고려할 수 있다.

Ⅲ. 결론

Matter–OCPP 하이브리드 EVSE 환경에서 하나의 충전기는 동시에 두 개의 신뢰 도메인에 속한다. Matter는 DAC/NOC를 통해 기기 정품성과 Fabric 멤버십을, OCPP는 CPID/TLS와 사용자·계약 정보를 통해 과금·운영을 담당하지만, 두 정체성이 별도로 관리될 때 DAC 클론, EVSE 교체, CPID 설정 오류와 같은 상황에서 기기 신뢰와 과금 신뢰가 어긋나는 보안 공백이 발생할 수 있다.

본 논문은 이 공백을 줄이기 위해 EVSE별 Matter 정체성과 OCPP 정체성을 하나의 튜플로 정의하고, 온보딩 시점에 해시+서명 기반 바인딩 자격증명을 생성·저장한 뒤, 충전 세션 시작 시 현재 구성과 비교·검증하는 “DAC–OCPP 바인딩 자격증명” 기법을 제안하였다. 이를 통해 DAC 클론·EVSE 교체·설정 오류를 정체성 불일치 이벤트로 탐지할 수 있고, 나아가 Charger Identity Card와 같은 사용자 인터페이스나 운영 경고 정책으로 확장할 수 있음을 논의하였다.

향후에는 Matter SDK와 OCPP 시뮬레이터를 이용한 테스트베드를 구축해, 제안 기법 적용 시 탐지율과 지연 시간, 시스템 부하 등을 정량적으로 측정하는 것이 필요하다. 또한 EVSE·브릿지·CSMS 각각에 바인딩 로직을 배치했을 때의 장단점과 운영 정책을 비교 분석하고, 표준화 논의와 연계하는 방향의 연구도 가능하다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음 (IITP-2025-RS-2021-II211835, GIST ITRC).

참 고 문 헌

[1] Connectivity Standards Alliance, “Matter 1.3 Core Specification,” 2024.

[2] Open Charge Alliance, “OCPP 2.0.1 Specification,” 2020.

[3] ISO, “ISO 15118: Road vehicles – Vehicle to grid communication

interface,” 2019.

[4] EVBoosters, “Plug & Charge Explained,” 2024.