http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.25, No.2, May 2020, pp.1-14
https://doi.org/10.7838/jsebs.2020.25.2.001

ISO 15118 충전 사용자 자동인증을 위한 교차인증서 기술의 적용에 관한 연구

A Study on the Application of Cross-Certification Technology for the Automatic Authentication of Charging Users in ISO 15118 Standard

이수정(Sujeong Lee)*, 신민호(Minho Shin)**, 장혁수(Hyuk-soo Jang)***

초 록

ISO 15118은 전기자동차와 전기차 충전기 사이의 통신을 정의하는 국제 표준이다. 또한 충전 서비스를 이용할 때 사용자를 자동인증하는 기술로써 Plug & Charge(PnC)를 정의하였다. PnC는 전기차 사용자 인증, 충전, 요금 청구 등의 모든 과정이 자동으로 처리되는 자동인증 기술을 말한다.

표준에 따르면 충전기와 CPS(Certificate Provisioning Service)의 인증서는 V2G(Vehicle to Grid) Root 인증서의 아래에 있어야 한다. 한국의 경우 한국전력공사가 자체적으로 PKI (Public Key Infrastructure)를 운영하고 있으므로 한전이 제공하는 충전기는 V2G Root 인증서의 아래에 있는 것이 어렵다. 따라서 서로 다른 Root 인증서를 가지고 있을 때에도 인증이 가능한 방법이 필요하다. 본 논문에서는 이를 위해 PnC 방식의 인증에 교차 인증서의 적용을 제안한다.

교차 인증서 자동인증은 서로 다른 Root 인증서를 가지더라도 인증이 가능하도록 Root CA의 교차 인증서를 발급하고 인증서 체인에 포함시켜 자동인증을 진행하는 것이다. 교차 인증서 기술을 적용하면 다른 Root 인증서의 아래에 있는 인증서의 검증을 가능하도록 해준다.

본 논문에서는 PnC 방식과 교차 인증서를 적용한 PnC 방식의 자동인증을 구현하여, 두 가지 방식이 모두 사용 가능함을 증명하는 개념 증명을 진행한다. 개발 요구사항과 인증서 프로파일, 사용자 인증 시퀀스를 작성하고, 이에 따라 구현, 실행한다. 이 실험을 통해 두 가지의 자동인증이 실행 가능하고, 특히 교차 인증서를 적용한 PnC 방식의 자동인증의 확장성이 뛰어남을 확인한다.

ABSTRACT

ISO 15118 is an international standard that defines communication between electric vehicles and electric vehicle chargers. Plug & Charge (PnC) was also defined as a technology to automatically authenticate users when using charging services. PnC indicates automatic authentication technology where all processes such as electric vehicle user authentication, charging and billing are automatically processed.

According to the standard, certificates for chargers and CPSs (Certificate Provisioning Services) should be under the V2G (Vehicle to Grid) Root certificate. In Korea, the utility

본 연구는 한국전력공사의 2016년 선정 기초연구개발과제 연구비에 의해 지원되었음(과제번호: R17XA05-50).

* First Author, Master of Science, Dept. of Security & Management Engineering, Myongji University (sujunglee223@gmail.com)

** Co-Author, Professor, Dept. of Computer Engineering, Myongji University(mhshin@mju.ac.kr)

*** Corresponding Author, Professor, Dept. of Computer Engineering, Myongji University(jang-h@mju.ac.kr)

Received: 2020-09-05, Review completed: 2019-11-06, Accepted: 2020-04-10

company operates its own PKI (Public Key Infrastructure), making it difficult to provide chargers under the V2G Root Certificate. Therefore, a method that can be authenticated is necessary even when you have different Root Certificates. This paper proposes to apply cross-certificate technology to PnC authentication.

Automatic authentication of Cross Certification is to issue a cross-certificate of the Root CA and include it in the certificate chain to proceed with automatic authentication, even if you have different Root certificates. Applying cross-certificate technology enables verification of certificates under other Root certificates.

In this paper, the PnC automatic authentication and cross certificate automatic authentication is implemented, so as to proceed with proof of concept proving that both methods are available. Define development requirements, certificate profiles, and user authentication sequences, and implement and execute them accordingly. This experiment confirms that two automatic authentication are practicable, especially the scalability of automatic authentication using cross-certificate PnC.

키워드 : 전기차, 전기차 충전인프라, 자동인증, 교차인증서, PKI
Electric Vehicle, Electric Vehicle Charging Infrastructure, Automatic Authentication, Cross Certification, PKI

1. 서 론

환경오염과 고갈되는 자원 등을 이유로 여러 국가에서 전기자동차에 집중하고 있다. 유럽, 미국, 중국 등이 배기가스 규제를 강화하고 전기자동차 산업을 성장시키려 한다. 특히 유럽은 내연기관 자동차를 모두 전기차로 전환하려는 장기계획을 수립하였다. 우리나라 역시 환경보호를 위한 움직임으로써 전기차 충전 인프라를 보급하고 전기차 운행 혜택을 확대하는 등의 정책을 운영하고 있다[4]. 또한 전기차 충전 인프라 간의 통신에 대한 표준들이 제정되었고, 이를 상용화하려는 움직임이 나타나고 있다.

ISO 15118은 전기자동차의 충전 절차를 제어하기 위해서 전기차와 충전기 사이의 통신을 정의하는 표준이다. 전기차를 충전하고자 할 때 충전 사용자를 자동으로 인증해주는 기술인 Plug and Charge(PnC)를 정의하고 있다. PnC는 전기차와 충전기가 연결되면 사용자 인증, 충전, 제어 등의 모든 충전 과정이 자동으로 처리되는 자동인증 기술로, 아직 상용화되지 않은 상태이다. 이때, 인증 수단으로 인증서를 사용한다. 이에 대한 자세한 내용은 ISO/TC22/SC31[2]을 참조한다.

ISO 15118에 의하면, 충전기 인증서와 CPS 인증서는 같은 V2G(Vehicle to Grid) Root 인증서의 아래에 있어야 한다. 또한 전기차 역시 같은 V2G Root 인증서를 Trust anchor로 가지고 있어야 충전기와 CPS(Certificate Provisioning Service)를 인증하는 것이 가능하다. 하지만 충전기 인증서의 PKI를 독립적으로 운영하고자 하는 경우는 충전기 인증서가 해당 PKI의 Root 인증서 아래에 있게 된다. 그러나 이 경우에는 전기차가 해당 PKI의 Root 인증서를 갖고 있지 않기 때문에 충전기 인증서를 검증할 수 없게 된다. 따라서 V2G Root 인증서와 Non-V2G Root 인증서 사이의 인증 방법이 필요하다.

이 문제점은 교차 인증서 기술을 적용하면 해결하는 것이 가능하다. 교차 인증서 기술은 한 CA(Certificate Authority)가 다른 CA의 인증서를 발급하여 인증서의 검증 시 사용할 수 있도록 하는 기술을 말한다[3]. 교차 인증서 기술을 PnC에 적용하면 서로 다른 Root 인증서를 가진 Actor를 인증할 때, 교차인증서를 인증서 체인에 포함하여 인증을 진행하게 된다. 이 기술을 적용하게 되면 V2G Root 인증서와 Non-V2G Root 인증서 사이의 검증을 가능하게 한다. 또한 본 논문에서는 실제로 PnC 방법과 교차 인증서 기술을 적용한 PnC 방법을 둘 다 구현하여, 해당 기술을 실제로 사용 가능함을 증명하는 개념 증명(Proof of Concept)을 하고자 한다.

2. 배경 지식

본 장에서는 ISO 15118과 Plug and Charge의 특징 및 한계에 대해 살펴본다. 그리고 교차 인증서 기술의 적용을 제안한다. 본 장에서 다루는 내용은 ISO/TC22/SC31[2], Shin et al.[6, 7]를 참조한다.

2.1 ISO 15118

ISO 15118은 전기차와 충전기 간 통신규약을 정의하는 국제 표준이다. 이 표준은 Power Line Communication을 기반으로 통신하고 TLS(Transport Layer Security)를 사용하여 Transport 계층 이상의 모든 데이터를 암호화한다. 또한 PKI 기술을 사용하여 Actors를 인증한다. 전기차와 충전기 간에 TCP/IP 연결이 되면 TLS를 수행하여 충전기를 인증한다. 이 과정을 위해서는 충전기가 자신의 인증서 체인을 전기차에 전송하여야 한다. 또한 전기차는 충전기 인증서를 확인하기 위해 V2G Root 인증서를 가지고 있어야 한다.

충전 사용자를 인증하기 위해서 전기차는 계약 인증서 체인을 사용한다. 충전기는 계약 인증서 체인을 검증하고, 사용자의 서비스 인가 여부를 Secondary Actor와 통신하여 확인한다. 또한 충전기는 계약 인증서 체인의 Root 인증서를 가지고 있어야 한다.

전기차와 충전기가 충전 스케줄을 협상할 때는 충전 요금표 정보를 사용한다. 이때, 충전 사업자가 가격 정보에 서명하여 제공하여야 한다. 협상 후에는 전기차 충전을 진행한다. 충전 중에는 충전한 전력량을 양측이 확인하기 위해 Metering Receipt 정보를 주고받는다.

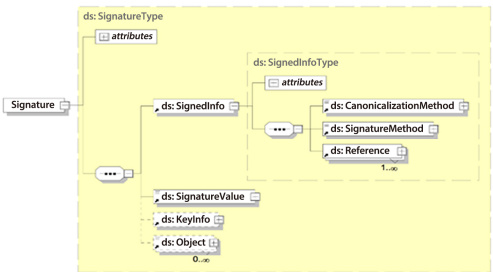
모든 충전 과정을 수행하기 위해서는 여러 개의 인증서를 사용하여야 한다. 또한 모든 인증서는 X.509v3을 따라 발급하여야 한다. 인증서를 사용하기 위해서는 모든 Actor가 <Table 1>에 정의된 기능을 사용하여야 한다.

〈Table 1〉 ISO15118 Certificate Requirements

Function	Requirement
Hash	SHA-256(NIST FIPS PUB 180-4)
Signature	ECDSA(secp256r1)
Key Length	256 bits(Elliptic Curve Cryptography)
Certificate Validation	Certificate Revocation List(CRL), Online Certificate Status Protocol (OCSP)

PnC 방식은 메시지를 주고받을 때 XML (Extensible Markup Language) 형태를 사용하고, ISO 15118에 메시지 내용에 대해 서명을 하는 방법과 암호화 방식이 정의되어 있다. 전기차는

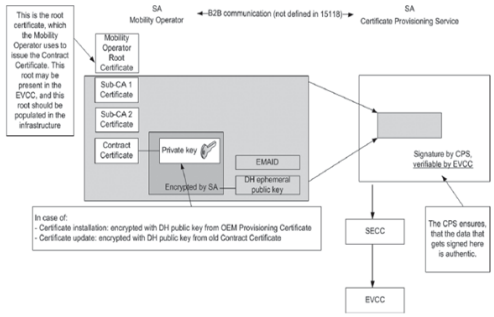
ISO 15118에 정의된 XML 서명 방식을 사용하여 자신을 인증하고 정보를 전달한다. 또한 충전사업자가 암호화한 자신의 비밀키를 안전하게 수신하는 것이 가능하다. XML 서명 방식은 Bartel et al.[1]에 정의되어 있다. <Figure 1>은 XML 서명의 구조를 보여준다.



〈Figure 1〉 XML Signature

서명할 메시지 내용에는 Reference ID를 적어야 한다. 이 Reference ID를 Reference 요소에 적어, 어떤 내용이 서명되어야 하는지 표시한다. 서명하기 위해서는 서명할 내용의 EXI(Efficient XML Interchange) 값을 SHA256으로 계산하고 Base64로 인코딩한 Digest 값을 Reference의 DigestValue에 넣는다. 그리고 SignedInfo에 대해 서명하고 그 값을 SignatureValue에 넣는다. 수신자는 DigestValue의 값을 사용하여 변조 여부를 확인한 뒤, SignatureValue의 값을 검증한다. 이에 관하여 자세한 내용은 Shin et al.[6]을 참조한다.

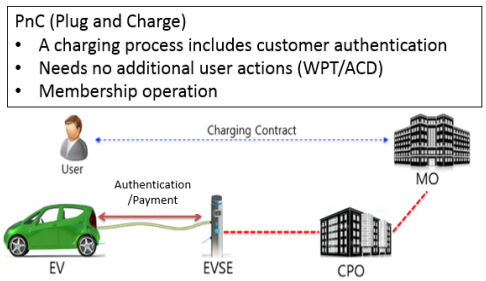
충전사업자는 전기차에 설치할 계약 인증서와 한 쌍인 비밀키를 암호화하여 전기차에 전달하여야 한다. 이때 ECDHE(Elliptic Curve Diffie Hellman Ephemeral) 키 교환 알고리즘을 사용한다. 이를 위해서는 먼저 충전사업자가 ECDHE를 사용하여 암호키를 생성하고, 그 키를 사용하여 계약 인증서와 한 쌍인 비밀키를 암호화한다. 그리고 이 정보를 포함한 계약 정보를 CPS에 전달하면 CPS가 이 정보를 ISO 15118 메시지에 넣은 후 전기차에 전달한다. <Figure 2>는 이 과정을 보여준다.



〈Figure 2〉 Provide Contract Certificate and Private Key

2.2 충전사용자 자동인증

ISO 15118은 Plug and Charge (PnC) 방법을 통해 충전사용자를 자동으로 인증하는 기능을 제안하고 있다. PnC란 전기차에 충전기의 플러그를 꽂으면 사용자 인증 및 인가, 충전 제어, 요금 지불 등의 과정이 모두 자동으로 수행되는 방식을 말한다. PnC 방법을 사용하면 ISO 15118에서 정의한 충전 프로세스에 사용자 인증이 포함되어 있기 때문에, 사용자의 추가적인 행동 없이 자동으로 인증을 수행한다. 충전서비스에 가입이 된 충전 사용자가 자신의 정보가 기재된 계약 인증서를 ISO 15118 메시지로 전달하면 이를 검증하여 인증하는 방식이다. PnC 방식은 충전 사용자의 추가적인 행동이 없어도 자동으로 사용자 인증을 진행할 수 있기 때문에, 사용자의 편의성이 향상된 방식이라고 할 수 있다. <Figure 3>은 PnC를 사용하는 인증이 어떻게 이루어지는지 보여준다.

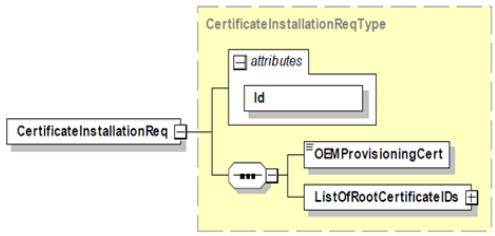


〈Figure 3〉 PnC(Plug & Charge)

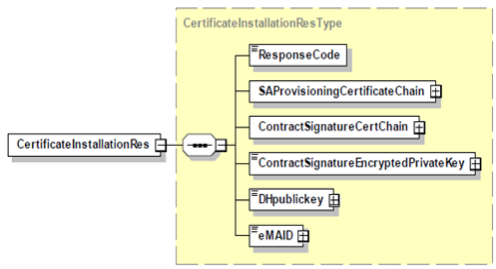
전기차는 PaymentServiceSelection 메시지를 사용하여 지불 방식을 EIM(External Identification Method)와 PnC 중 선택할 수 있다. EIM은 운전자가 자신을 인증할 수 있는 외부수단을 말한다. 신용카드, 현금, 회원카드 등을 예로 들 수 있다. PnC를 사용하기 위해서는 PaymentDetailsReq 메시지를 사용하여 eMAID(eMobility Account ID)와 계약인증서를 충전기에 전송해야 한다.

충전기와 Secondary Actors는 eMAID와 인증서 체인을 검증하고 문제가 없으면 PaymentdetailsRes 메시지를 통해 Challenge Text를 전달한다. 전기차는 AuthorizationReq 메시지를 통해 Challenge Text에 서명하여 충전기에 전달하고, 충전기는 이 서명을 검사하여 사용자를 인증한다.

전기차에 아직 계약 인증서를 설치하지 않았거나 계약 인증서를 갱신해야 하는 경우, 충전기를 통해 인증서를 수신할 수 있다. 계약 인증서를 설치하고자 할 때, 전기차는 CertificateInstallationReq 메시지를 통해서 충전기에 요청을 보낸다. 충전기는 CertificateInstallationRes 메시지를 통해 해당 인증서를 전송하고 전기차는 이 메시지를 검증 후 인증서를 설치한다. <Figure 4>와 <Figure 5>는 CertificateInstallationReq 메시지와 CertificateInstallationRes 메시지의 형식을 보여준다.

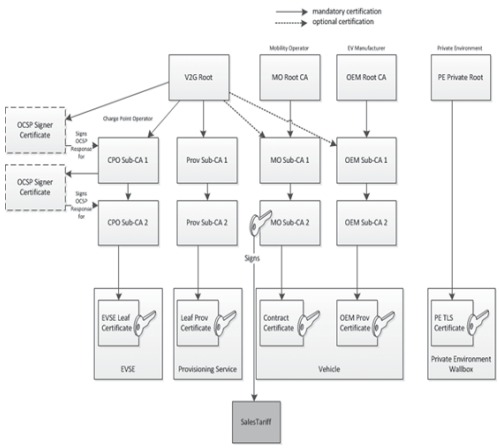


〈Figure 4〉 CertificateInstallaionReq



〈Figure 5〉 CertificateInstallationRes

인증서 갱신은 인증서 설치와 비슷한 방법으로 진행된다. 인증서 설치와 갱신의 차이점은 Req 메시지에 넣는 인증서가 각각 OEM(Original Equipment Manufacturer) Provisioning 인증서와 계약 인증서라는 점이다.

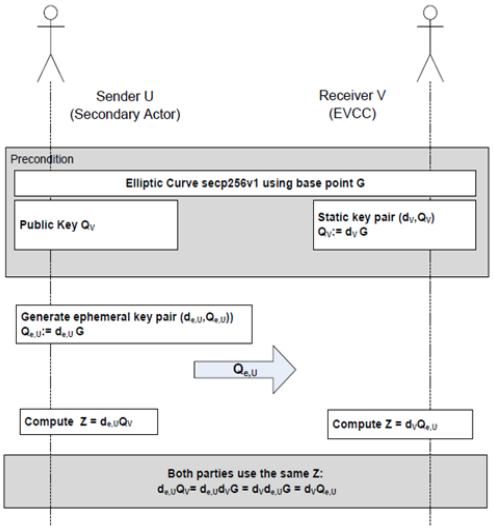


〈Figure 6〉 ISO 15118 Certificate Structure

<Figure 6>은 ISO 15118에서 사용하는 인증서의 구조를 보여준다. 모든 인증서 체인은 길이를 최대 3까지 가질 수 있다. 충전기의 인증서 체인은 TLS 연결 시 전기차에 전송되고, 충전기를 인증할 때 사용한다. 계약 인증서 체인은 해당 인증서의 Root 인증서를 제외한 체인이기 때문에, 전기차는 해당 Root 인증서가 없어 자체적으로 계약 인증서를 검증할 수 없다.

OEM Provisioning 인증서는 OEM이 운영하는 PKI의 아래에 있다. OEM Provisioning 인증서는 다음의 과정을 통해 전기차에 설치 및 사용된다.

(1) 전기차 생산 시, 전기차에 OEM Provisioning 인증서와 비밀키를 설치한다.
(2) 전기차 인수 시, 고객은 OEM Provisioning 인증서의 ID 정보(PCID)를 얻는다.
(3) 고객은 PCID를 사용하여 충전사업자(MO, Mobility Operator)와 계약한다.



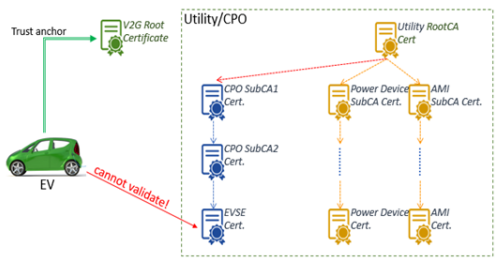
〈Figure 7〉 Elliptic Curve Diffie-Hellman Ephemeral Key Exchange

(4) 인증서 설치 시 OEM Provisioning 인증서를 사용한다.

ISO 15118에서 전기차가 인증서 설치를 요청하면 충전계약자는 해당하는 인증서와 비밀키를 생성하여 전달하는데, 이때 비밀키를 ECDHE를 사용하여 암호화한다. 먼저 충전계약자는 ECDHE를 사용하기 위해 임시 키 쌍을 생성하고 그 키쌍을 사용하여 세션키를 생성한다. 그리고 그 세션키를 사용하여 비밀키를 암호화하고 전기차에 전달한다. <Figure 7>은 비밀키를 암호화하기 위한 세션키를 생성하는 방법을 보여준다.

3. 교차 인증서

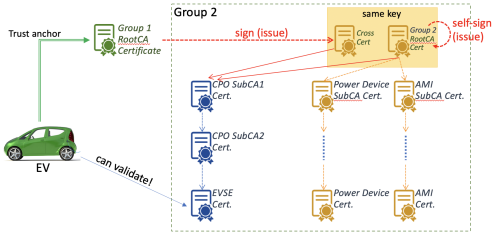
ISO 15118에 따르면 충전기 인증서는 V2G Root 인증서의 아래에 있어야 한다. 하지만 충전소의 PKI가 독립적인 경우 충전기 인증서는 다른 Root 인증서의 아래에 있게 된다. 하지만 전기차는 V2G Root 인증서만 가지고 있기 때문에, 독립적인 PKI의 충전기 인증서는 검증할 수 없다. 또한 충전기 인증서가 V2G Root 인증서의 아래에 있더라도, 전기차가 다른 V2G Root 인증서만 가지고 있다면 역시 검증할 수 없다. <Figure 8>은 독립적인 PKI의 충전기 인증서의 검증 문제를 보여준다.



〈Figure 8〉 Interoperability Problem

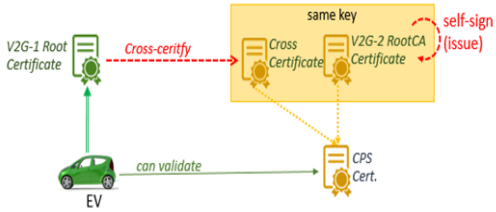
우리나라의 경우, 충전소의 운영자인 한국전력공사에서 자체적으로 PKI를 구축하여 사용하고 있기 때문에, 전기차가 충전기 인증서를 검증하는데 어려움이 있다. 그러므로 국내에서 PnC를 사용하기 위해서는 이 문제점을 해결하여야 한다. 이런 문제점을 해결하기 위해서 교차 인증서 기술을 PnC에 적용할 것을 제안한다.

교차 인증은 한 CA가 다른 CA의 인증서를 발급하여 인증서의 검증 시 사용할 수 있도록 하는 기술을 말한다[3]. 기존 CA 인증서의 공개키가 들어있지만, 다른 PKI의 Root CA가 서명한 인증서인 교차 인증서를 사용하게 된다. 두 PKI의 Root CA 간의 교차 인증을 예로 들 수 있다. <Figure 9>는 두 PKI 간의 교차 인증을 보여준다. <Figure 9>에서 그룹 1의 Root CA는 그룹 2의 Root 인증서와 같은 공개키를 가진 교차인증서를 발급한다. 그 후, 그룹 2의 멤버가 그룹 1의 멤버에게 자신을 인증할 때, 자신의 인증서 체인에 앞서 생성된 교차 인증서를 추가하여 구성한다. 그룹 1의 멤버는 그룹 1의 Root 인증서를 Trust Anchor로 가지기 때문에 이를 사용하여 그룹 2의 멤버 인증서 체인을 검증할 수 있게 된다.



〈Figure 9〉 Cross Certification

교차 인증을 V2G PKI와 CPS PKI 간에 적용하면, 전기차는 자신이 가진 V2G Root 인증서와 다른 V2G Root 인증서 아래의 CPS 인증서를 검증할 수 있다. <Figure 10>은 V2G 간에 교차 인증을 적용하여 CPS 인증서를 검증하는 과정을 보여준다.



〈Figure 10〉 CPS Cross Certification

교차 인증을 PnC에 적용하게 되면 V2G PKI 간의 상호운용성이 향상된다. 또한, V2G PKI와 Non-V2G PKI를 함께 운영할 수 있다. 따라서 교차 인증의 적용은 PnC를 실제 환경에서 사용하기 위해서 필요한 기술이다.

4. 구현 및 평가

본 장에서는 ISO 15118에서 정의한 PnC와 교차 인증서 기술을 적용한 PnC의 사용이 가능함을 증명하고자 한다. 이를 위하여 개발 요구사항을 정의하고 실제 구현 및 평가를 진행한다. 이 장에서 다루는 내용은 ISO/TC22/SC31[2], Shin et al.[6, 7]를 기반으로 작성되었다.

4.1 구현 목적

현재 전기차 인프라와 관련하여 다양한 표준에서 PnC 기능을 정의하고 있고, 이를 위한 요구사항을 설명한다. 그러나 이와 관련된 표준이 복잡하고 여러 가지 표준을 함께 적용하여 PnC를 개발하여야 하는 어려움이 있다. 또한

PnC는 아직 상용화되지 않았기 때문에 구현하여 실행하는 것이 의미를 가진다. 본 논문에서는 PnC를 위한 인프라와 PnC 기능, 교차 인증 기술을 적용한 PnC 기능을 구현하여, PnC와 교차 인증 PnC의 사용이 둘 다 가능하다는 것을 증명하는 개념 증명을 수행한다.

4.2 개발 요구사항

PnC를 위한 인프라를 구현하기 위해서 각 Actor 별 PKI를 <Figure 11>에 따라 구현한다. 그리고 각 CA는 다음의 사항을 지켜야 한다.

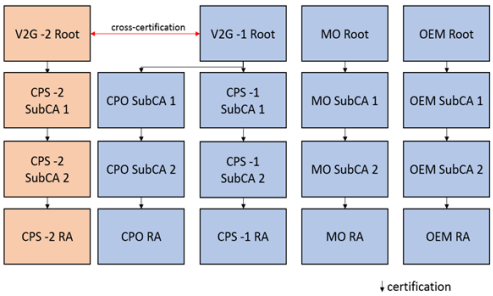
ECDSA (Elliptic Curve Digital Signature Algorithm)을 위한 키 쌍을 생성하고 PEM (Privacy Enhanced Mail) 형식 파일로 저장한다.

키 쌍을 이용하여 인증서 발급 요청을 위한 CSR(Certificate Signing Request) 생성 및 PEM 형식 파일로 저장한다.

인증서 발급 요청을 수신하면 해당 인증서를 발급하고 PEM 형식 파일로 저장하고 전송한다.

Root CA는 자신의 키로 자신의 인증서를 서명한 Self-signed 인증서를 제공한다.

V2G Root와 V2G-2 Root는 서로 교차 인증서를 발급하여야 한다.



〈Figure 11〉 PKI structure for PnC and Cross Certificate PnC

개념 증명에 사용할 각 인증서의 프로파일을 정의하였다. 실제 표준에서 사용되는 인증서 프로파일은 ISO/TC22/SC31[2]의 Annex F를 참조한다. 인증서 프로파일 중 Issuer, validity, Subject 요소를 정의하고, 다른 부분은 표준을 따른다. <Table 2>는 V2G Root 인증서, <Table 3>는 충전기 운영사업자(Charge Point Operator, CPO) 및 충전기(EV Supply Equipment, EVSE) 인증서, <Table 4>, <Table 5>는 CPS 인증서, <Table 6>은 충전사업자 인증서, <Table 7>은 OEM Provisioning 인증서의 프로파일 요소를 나타낸다. eMAID와 PCID의 Nation은 “KR”, Provider ID는 “MJU”를 사용하고, Unique ID는 임의의 값으로 설정한다. eMAID와 PCID의 형식은 ISO/TC22/SC31[2]의 Annex H를 참조한다.

〈Table 2〉 V2G Root Certificate Profile

Certificate Profile		V2G Root	V2G-2 Root
Issuer	country	"KR"	"KR"
	Organization	"MJU"	"MJU"
	Organization Unit	"HMCL"	"HMCL"
	Common Name	"MJU_V2G_RootCA"	"MJU_V2G-2_RootCA"
	Domain component	"V2G"	"V2G"
Validity		40 years	40 years
Subject	country	"KR"	"KR"
	Organization	"MJU"	"MJU"
	Organization Unit	"HMCL"	"HMCL"
	Common Name*	"MJU_V2G_RootCA"	"MJU_V2G-2_RootCA"
	Domain component+	"V2G"	"V2G"

* Common Name: Unique identifier of the subject.
+ Domain Component: Alternative information of the subject

〈Table 3〉 CPO, EVSE Certificate Profile

Certificate Profile		CPO Sub CA1	CPO Sub CA2	EVSE Leaf Cert
Issuer	country	"KR"	"KR"	"KR"
	Organization	"MJU"	"MJU"	"MJU"
	Organization Unit	"HMCL"	"HMCL"	"HMCL"
	Common Name	"MJU_ V2G_ RootCA"	"MJU_ CPO_ SubCA1"	"MJU_ CPO_ SubCA2"
	Domain component	"V2G"	"V2G"	"V2G"
Validity		4 years	2 years	3 months
Subject	country	"KR"	"KR"	"KR"
	Organization	"MJU"	"MJU"	"MJU"
	Organization Unit	"HMCL"	"HMCL"	"HMCL"
	Common Name	"MJU_ CPO_ SubCA1"	"MJU_ CPO_ SubCA2"	"MJU_ CPO_ LEAF"
	Domain component	"V2G"	"V2G"	"CPO"

〈Table 4〉 CPS Certificate Profile

Certificate Profile		CPS Sub CA1	CPS Sub CA2	Leaf Prov Cert
Issuer	country	"KR"	"KR"	"KR"
	Organization	"MJU"	"MJU"	"MJU"
	Organization Unit	"HMCL"	"HMCL"	"HMCL"
	Common Name	"MJU_ V2G_ RootCA"	"MJU_ CPS_ SubCA1"	"MJU_ CPS_ SubCA1"
	Domain component	"V2G"	"V2G"	"V2G"
Validity		4 years	2 years	3 months
Subject	country	"KR"	"KR"	"KR"
	Organization	"MJU"	"MJU"	"MJU"
	Organization Unit	"HMCL"	"HMCL"	"HMCL"
	Common Name	"MJU_ CPS_ SubCA1"	"MJU_ CPS_ SubCA2"	"MJU_ CPS_ LEAF"
	Domain component	"V2G"	"V2G"	"CPS"

〈Table 5〉 CPS-2 Certificate Profile

Certificate Profile		CPS-2 Sub CA1	CPS-2 Sub CA2	CPS-2 Leaf Cert
Issuer	country	"KR"	"KR"	"KR"
	Organization	"MJU"	"MJU"	"MJU"
	Organization Unit	"HMCL"	"HMCL"	"HMCL"
	Common Name	"MJU_ V2G-2_ RootCA"	"MJU_ CPS-2_ SubCA1"	"MJU_ CPS-2_ SubCA2"
	Domain component	"V2G"	"V2G"	"V2G"
Validity		4 years	2 years	3 months
Subject	country	"KR"	"KR"	"KR"
	Organization	"MJU"	"MJU"	"MJU"
	Organization Unit	"HMCL"	"HMCL"	"HMCL"
	Common Name	"MJU_ CPS-2_ SubCA1"	"MJU_ CPS-2_ SubCA2"	"MJU_ CPS-2_ LEAF"
	Domain component	"V2G"	"V2G"	"CPO"

〈Table 6〉 MO Certificate Profile

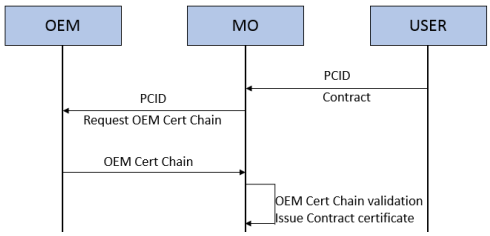
Certificate Profile		MO Root	MO Sub CA1	MO Sub CA2	Contract Cert
Issuer	country	"KR"	"KR"	"KR"	"KR"
	Organization	"MJU"	"MJU"	"MJU"	"MJU"
	Organization Unit	"HMCL"	"HMCL"	"HMCL"	"HMCL"
	Common Name	"MJU_ MO_ RootCA"	"MJU_ MO_ RootCA"	"MJU_ MO_ SubCA1"	"MJU_ MO_ SubCA2"
	Domain component	"V2G"	"V2G"	"V2G"	"V2G"
Validity		2 years	2 years	2 years	1 year
Subject	country	"KR"	"KR"	"KR"	"KR"
	Organization	"MJU"	"MJU"	"MJU"	"MJU"
	Organization Unit	"HMCL"	"HMCL"	"HMCL"	"HMCL"
	Common Name	"MJU_ MO_ RootCA"	"MJU_ MO_ SubCA1"	"MJU_ MO_ SubCA2"	EMAID
	Domain component	"V2G"	"V2G"	"V2G"	"V2G"

〈Table 7〉 OEM Certificate Profile

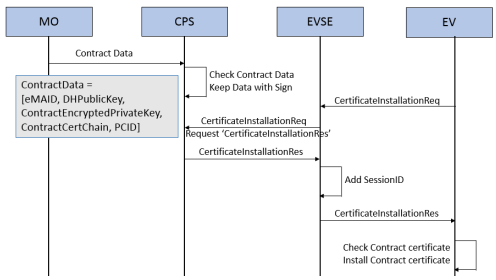
Certificate Profile		OEM Root	OEM Sub CA1	OEM Sub CA2	OEM Prov Cert
Issuer	country	"KR"	"KR"	"KR"	"KR"
	Organization	"MJU"	"MJU"	"MJU"	"MJU"
	Organization Unit	"HMCL"	"HMCL"	"HMCL"	"HMCL"
	Common Name	"MJU_OEM_RootCA"	"MJU_OEM_RootCA"	"MJU_OEM_SubCA1"	"MJU_OEM_SubCA2"
	Domain component	"V2G"	"V2G"	"V2G"	"V2G"
Validity		2 years	2 years	2 years	1 year
Subject	country	"KR"	"KR"	"KR"	"KR"
	Organization	"MJU"	"MJU"	"MJU"	"MJU"
	Organization Unit	"HMCL"	"HMCL"	"HMCL"	"HMCL"
	Common Name	"MJU_OEM_RootCA"	"MJU_OEM_SubCA1"	"MJU_OEM_SubCA2"	PCID
	Domain component	"V2G"	"V2G"	"V2G"	"OEM"

PnC 방식을 사용해서 인증하기 위해서는 다음과 같은 일련의 단계를 거쳐야 한다. “계약인증서 발급단계” 에서는 사용자가 충전사업자와 계약할 때 전기차의 PCID를 충전사업자에게 제시하고 충전사업자는 OEM에게 PCID와 매칭되는 OEM 인증서의 체인을 요청한다. 이 때 충전사업자는 사전에 OEM Root 인증서를 Trust Anchor로 가지고 있어야 한다. OEM이 해당 인증서 체인을 전달하면 충전 사업자는 수신한 인증서 체인을 검증한 뒤 올바르면 계약 인증서를 발급한다. <Figure 12>는 계약 인증서의 발급 시퀀스를 보여준다.

“계약인증서 설치단계”에서는 충전 사업자가 Contract Data를 생성하고 CPS에게 전달한다. Contract Data에는 eMAID, ECDHE 공개키, 암호화된 계약 비밀키, 계약 인증서 체인,



〈Figure 12〉 Contract Certificate Issuance

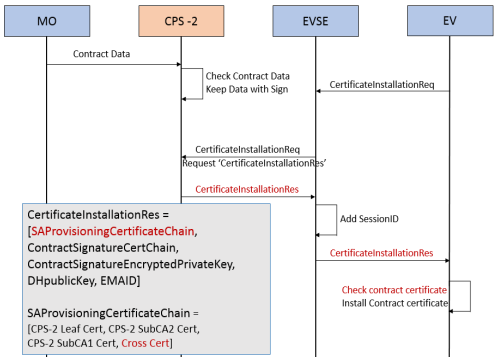


〈Figure 13〉 Contract Certificate Installation

PCID로 구성된다. CPS는 받은 Contract Data의 계약 인증서 체인을 검증한다. 인증서 체인이 유효하면 Contract Data에 서명한 후 저장한다. 이 뒤에 전기차가 충전기에게 인증서 설치를 요청하면 충전기는 CPS에게 CertificateInstallationRes 메시지의 생성을 요청한다. CPS는 전달받은 OEM Provisioning 인증서를 검사하고 해당 PCID와 매칭되는 Contract Data를 검색한다. 그 Contract Data를 사용하여 CertificateInstallationRes 메시지를 생성한 뒤 충전기에 전달한다. 그러면 충전기는 수신한 메시지에 Session ID를 추가하고 전기차에 전달한다. <Figure 13>은 계약 인증서의 설치 시퀀스를 보여준다.

만약 교차 인증서을 사용하여 계약인증서를 설치하는 경우는 교차 인증서를 인증서 체인에 포함시켜서 전송해야 한다. 본 논문에서는

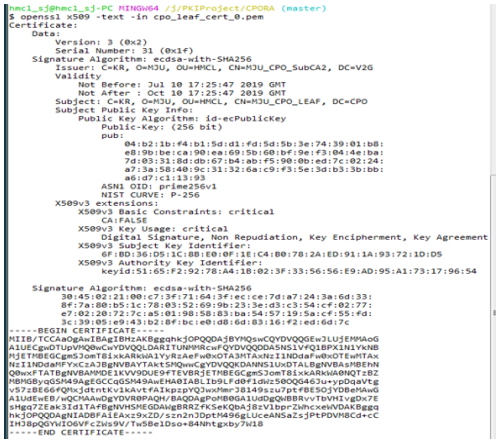
다른 V2G Root 인증서의 아래에 있는 CPS-2가 서명한 계약 인증서를 전기차에 전송하여, 검증 및 설치가 가능함을 확인하고자 한다. <Figure 14>는 교차 인증서를 사용한 계약 인증서 설치 시퀀스를 보여준다. CPS 인증서 체인은 CertificateInstallationRes 메시지의 SAProvisioningCertificateChain 요소에 들어가는데, 이 부분에 교차 인증서를 추가한다. 또한 전기차가 이를 검증하는 것이 가능하도록 하여야 한다.



〈Figure 14〉 Contract Certificate Installation by Cross-certification

4.3 구현 결과 및 평가

3.2절에서 정의한 요구사항에 따라 V2G, 충전소, 충전사업자, OEM PKI를 개발하였다. 또한 키 쌍과 CSR 생성, 인증서 발급, 인증서 검증, Contract Data 생성 등의 기능을 개발하였다. ISO 15118 메시지 생성과 전기차, 충전기 관련 기능은 RISEV2G 프로젝트[5]를 참조하였다. 각 CA, RA는 TCP 소켓을 통해 통신을 한다. 또한 3.2에서 정의한 인증서 프로파일을 준수하여 인증서를 발급하였다. <Figure 15>는 그 중 충전기 인증서의 상세 내용을 보여준다.

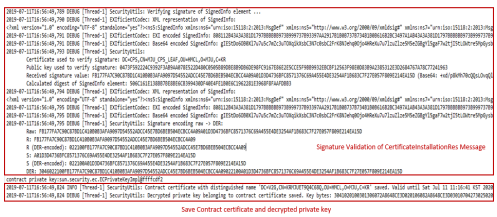


〈Figure 15〉 EVSE Certificate

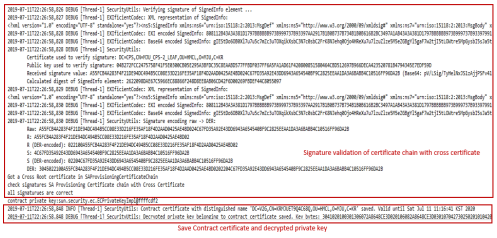
〈Figure 16〉 Contract Certificate Data Generation

충전 사업자는 OEM에게 OEM Provisioning 인증서 체인을 요청하여 받은 뒤, 계약인증서를 발급 및 저장한다. 그 후, 충전 사업자는 CertificateInstallationRes 메시지 생성을 위해 필요한 정보를 Contract Data 메시지에 넣고 CPS에게 전달한다. <Figure 16>은 CPS가 수신한 Contract Data를 검사하고 메시지 생성 및 서명하여 저장하는 과정을 보여준다. 이 과정에서 XML Object인 V2GMessage를 생성하고, EXI 인코딩을 하여 Byte array로 저장한다.

전기차가 충전기에게 인증서 설치를 요청하면 충전기는 CPS에게 CertificateInstallationRes 메시지를 요청한다. CPS는 OEM 인증서를 검사한 뒤, 그 인증서의 PCID를 사용하여 CertificateInstallationRes 메시지를 검색한 후 충전기에 전송한다. 이 때 CPS의 Root 인증서와 충전기의 Root 인증서가 같으면 CPS 인증서 체인을 {Sub CA2 인증서- Sub CA1 인증서 -Leaf 인증서}로 구성한다. 만약 서로 다른 Root 인증서의 아래에 있으면 앞의 체인에 교차인증서를 추가한다. 충전기는 받은 메시지에 SessisonID를 추가하여 전기차에게 전송한다. <Figure 17>, <Figure 18>은 수신한 CertificateInstallationRes 메시지를 검사하고 유효하면 계약인증서와 비밀키를 저장하는 과정을 보여준다. 이후 ISO 15118에 정의된 PnC 충전 시퀀스에 따라 전기차의 충전이 진행된다.



〈Figure 17〉 Contract Certificate Installation in EV



〈Figure 18〉 Contract Certificate Installation in EV via Cross-Certification

3.2에서 정의한 개발 요구사항을 반영하여 PKI 프로젝트를 개발하고 RISEV2G 프로젝트를 수정하였다. 개발한 PKI 프로젝트를 통하여 정의된 인증서 프로파일을 따르는 인증서를 발급하였음을 확인하였다. 또한 앞서 정의한 자동인증 시퀀스를 따라 프로젝트를 실행하여 전기차에 계약 인증서 체인을 설치하고 자동인증을 수행하는 것을 성공하였다. 따라서 PnC 방식을 사용한 자동인증과 교차 인증서를 적용한 PnC 방식을 사용한 자동인증의 개념 증명이 둘 다 성공하였다고 할 수 있다.

5. 결 론

전기자동차의 사용률이 점차 증가하고 있고, 때문에 전기자동차의 충전 인프라의 보급을 위한 움직임이 활발하게 나타나고 있다. 이런 상황에서 전기자동차 충전 사용자의 편의성을 향상시키는 사용자 자동인증 기술 연구는 앞으로의 충전 인프라 보급과 발전에 기여할 수 있다. 또한 현재 전기차 충전 인프라에 관련하여 다양한 국제, 국내 표준이 정의되어 있으므로 이 표준들을 준수할 필요성이 있다.

본 논문에서는 전기자동차와 충전기 사이의 통신을 정의한 ISO 15118 국제 표준을 분석하였고, 사용자 자동 인증 기술의 구현에 어떤 부분이 필요한지 알아보았다. 특히 Plug & Charge 방식을 사용하여 어떻게 충전하는지 분석하였다.

ISO 15118에 따르면 충전기 인증서와 CPS 인증서는 V2G Root 인증서의 아래에 있어야 한다. 그러나 자체적으로 PKI를 구축하여 충전기 또는 CPS를 운영하고 자 하는 경우 표준을

준수할 수 없게 된다. 실제로 한국의 경우 한국전력공사에서 충전사업자와 충전소 운영자의 역할을 수행하는데, 이미 자체적으로 구축한 PKI를 사용하고 있어 V2G Root 인증서의 아래에 있는 것이 어렵다.

이런 문제를 해결하고 확장성을 높이기 위해 교차 인증서 기술을 PnC 방식의 자동인증에 적용하고자 한다. 교차 인증서 기술을 PnC 방식에 적용하면, 서로 다른 V2G Root 인증서의 아래에 있는 경우 또는 V2G가 아닌 PKI의 Root 인증서 아래에 있더라도 인증서를 검증할 수 있다.

ISO 15118에 정의된 PnC 사용자 자동인증이 아직 상용화되지 않았기 때문에, PnC 방식의 인증이 실제로 사용 가능함을 증명하고, 교차 인증서를 적용한 PnC 방식의 인증 역시 사용 가능함을 증명하기 위한 개념 증명을 실시하였다. 이를 위한 개발 요구사항과 각 인증서의 프로파일을 정의하였다. 그리고 PnC 방식을 사용한 인증의 수행 시퀀스를 정의하여 프로젝트를 구현하고 실행하였다.

그 결과, PKI들은 정의된 요구사항을 만족하였고, 정의된 인증서 프로파일을 준수하는 인증서를 발급하였다. 또한 PnC 방식의 사용자 자동인증과 교차 인증서를 적용한 PnC 방식의 사용자 자동인증을 시퀀스에 따라 수행하였고 자동인증이 실제로 사용할 수 있다는 것을 확인하였다. 따라서 PnC 방식과 교차 인증서를 적용한 PnC 방식을 사용하는 사용자 자동인증 기술은 실제의 전기차 충전 인프라에 적용이 가능하다고 할 수 있다.

References

[1] Bartel, M., Boyer, J., Fox, B., and La-Macchia, B., and Simon, E., “XML Signature Syntax and Processing Version 1.1.,” World Wide Web Consortium, 2013.

[2] ISO/TC22/SC31, “Road vehicles-Vehicle-to-Grid Communication Interface-Part 2: Network and application protocol requirements,” ISO 15118-2, 2014.

[3] Lloyd, S., “Understanding Certification Path Construction,” PKI Forum, 2002.

[4] Park, J., Jo, H., Kim, M., and Kim, S., “A study of Strategy for Spread of Green IT,” The Journal of Society for e-Business Studies, Vol. 17, No. 2, pp. 39-62, 2012.

[5] “Risev2g project,” (2017 Jul 21), https://github.com/eclipse/risev2g(accessed 2019 Mar 3).

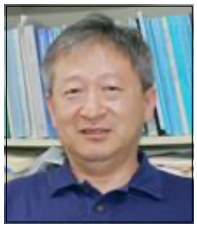
[6] Shin, M., Lee, S., and Zhang, S., “Outlook of communication standards for the Managements of Electric Vehicle Charging Stations and User Authentication,” 2019 IEEE Transportation Electrification Conference, 2019.

[7] Shin, M., Lee, S., and Zhang, S., “Standard Developments of Electric Vehicle Charging Infrastructure,” The 3rd International Conference on Electric Vehicle, Smart Grid and Information Technology, 2018.

저 자 소 개

이수정 (E-mail: sujunglee223@gmail.com)
2017년 명지대학교 컴퓨터공학 (학사)
2019년 명지대학교 보안경영공학학과간협동과정 (석사)
관심분야 전기자동차, PKI, 자동인증

신민호 (E-mail: mhshin@mju.ac.kr)
1998년 서울대학교 계산통계학과 (학사)
2003년 메릴랜드 주립대학교 전산과 (석사)
2008년 메릴랜드 주립대학교 전산과 (박사)
2007년~2010년 다트머스대학 연구원
2010년~2011년 삼성종합기술원
2011년~현재 명지대학교 컴퓨터공학과 교수
관심분야 보안, 개인정보보호, 블록체인



장혁수 (E-mail: jang-h@mju.ac.kr)
1975년~1983년 서울대학교 산업공학과 (학사)
1990년 오하이오 주립대학교 전산과 (박사)
1990년~1992년 경북대학교 전자공학과 교수
1992년~현재 명지대학교 컴퓨터공학과 교수
관심분야 컴퓨터시스템, 스마트그리드