33rd Electric Vehicles Symposium (EVS33)
Portland OR, USA, June 14 - 17, 2020

Security Considerations for Safe & Efficient EV Charging

Jaeson Yoo, Daniel E.S. Kim, SangGyoo Sim

[1]*Autocrypt Co. Ltd.., Eusu Holdings Building, 20F, 25 Gukjegeumyung-ro 2-gil, Yeongdeungpo-gu, Seoul, South Korea 07327, jyoo@autocrypt.io*

Summary

As EVs and their charging infrastructure become more software-dependent, security considerations are becoming increasingly imperative as well. Using Public Key Infrastructure (PKI) to manage a trust-based platform is one way to address security and privacy, and the use of PKI for Plug & Charge (Pnc) enablement is a good case study to see how tomorrow's technology is evolving alongside security and convenience. From a business perspective, interoperability between PKI authorities is also an imminent concern that needs to be addressed. From a security perspective, a robust PnC ecosystem not only includes good technology, but also wide-ranging operational procedures to make sure that networks can operate safely and trust each other's security policies. Autocrypt Co. Ltd. Chief Evangelist and EVP of Business Development Jaeson Yoo illustrates how IT/IoT security can be applied in PnC charging, not only to ensure security and data integrity, but also to enable the viability of V2G business in the future.

1 Introduction

As EVs become increasingly software-dependent, EV chargers (EVSEs) are becoming software-dependent as well. Hardware can be expensive to install; they also represent a mechanical component that needs to be maintained and ultimately replaced with something else. RFID-based charging is a proven technology, but it is unlikely to support the amount of vehicles necessary for wider EV adoption. Lighter software components promise a future where more EVSEs can be installed with less cost, thereby making it possible for more EVs to be on the road.

Using PKI is expected to result in a more secure and convenient way for EV drivers to charge their vehicles in the future. While RFID provides convenience over credit cards, they can nevertheless be lost or stolen, leading to unauthorized charging, stolen identities, operational difficulties for charging service providers, etc. PKI, on the other hand, offers user authentication, and authorization for EV charging. In addition, mobility operators (MOs or E-Mobility Service Providers) can provide a streamlined charging service for their customers, allowing EV drivers to tap into charging networks outside the ones they are accustomed to. Indeed, this is one of the key factors for widespread EV adoption – the option to travel far and wide with electric vehicles.

Simply having a PKI system is inadequate for ensuring secure EV/EVSE charging with uninterrupted services, however. PKI itself is a secure process. But PKI servers are not immune to attacks if they are installed into network environments that are vulnerable. Therefore, the traditional considerations for IT Security cannot be overlooked when thinking of a secure PKI environment for EV charging. Moreover, many PKI infrastructure operators will need to establish trust with other operators if they are to provide interoperability with one another, leading to convenience for the EV drivers and service providers. Such trust

is not possible if any PKI infrastructure is negligent and therefore vulnerable to attacks. This is because interoperability provides a way for hackers to not only affect their original targets, but also other PKI authorities that are interconnected with them.

Since 2017, Autocrypt Co. has used its IT/IoT security experience to analyze how PKI technology can be implemented into the EV charging space. This paper will survey the potential benefits of using PKI for EV charging, the application that is currently available for this technology called Plug & Charge, and the security challenges that still lie ahead. Creating the right PnC environment can result in more EVSEs, therebyt creating more EV drivers and EV charging service providers.

2 Using PKI for a Trust-Based Platform

PKI was introduced in 1976 by Whitfield Diffie and Martin Hellman. According to Secure Socket Shell (SSH)—a network protocol that gives system administrators a secure way to access computers over an unsecure network—PKI is a "technology for authenticating users and devices in the digital world…[by having] one more more trusted parties digitally sign documents certifying that a particular cryptographic key belongs to a particular user or device."[1]

Over 40 years after Diffie and Hellman published their initial findings, PKI can be utilized as a trust-based platform to authenticate users, EVs, EVSEs, and other key stakeholders for EV charging. PKI provides a trust-based platform for various EV charging players, coming together for the sake of providing a secure way to provide convenience for EV charging. PKI can not only provide a way to authenticate users for service providers, OEMs and charging providers, but also provide a way to authorize the charging services when it happens.

Trust and fraud prevention continue to be important considerations for EVs to become more prevalent in a carbon-free future. V2G Clarity, one of the co-authors of ISO 15118 that deals with secure communications between the EV and the EVSE, and Hubject, one of the leading e-roaming providers in the world, wrote in a 2019 whitepaper the following:

> The closer we get to a mass-market adoption of EVs, the more we need to shift our focus to fraud-protection. Whenever a new technology reaches a certain utilization rate, it becomes an interesting target for hackers to exploit. As an industry, we must adopt an authentication and authorization method that has fraud-protection built into the communication protocol.[2]

The emphasis on fraud-protection implies that all data that are generated to execute a variety of different EV charging transactions must be trustworthy to all the players operating within this ecosystem. Furthermore, the authors infer that fraud-protection is an essential component for an effective mass-market adoption of EVs. PKI can provide a communication protocol that has fraud-protection built into its design.

We believe that PKI will play an important role in the next phase of EV adoption, a critical component of which is how all of these vehicles will be charged in the future. PKI in wireless charging, for example, is expected to play a critical role when the technology is eventually rolled out for commercial use by EV drivers. When EVs beging to generate, store, and distribute electritcity back to the smart grid for V2G charging, PKI can be a way for EV charging stakeholders to authenticate users and authorize transactions. But these are technologies that are still a few years into the future. Plug-and-Charge technology, on the other hand, represents the first step toward a credit card- and RFID-free charging future the authors of this paper feel necessary for mass EV adoption.

2.1 PKI for Plug & Charge Technology

PnC technology refers to EV charging by simply plugging vehicles into EVSEs with no need for RFID verification. This technology has been in the mind of many OEMs and EV charging stakeholders for the past several years, precisely because it is a technologically feasible way to provide security and convenience for EV drivers when charging their vehicles. Using PKI, the EV and the EVSE can recognize one another in order to enable charging and other services. PnC technology is based on Ethernet communications, and is managed under ISO 15118 for Combined Charging Systems at up to 80 or 350 kilowatts.

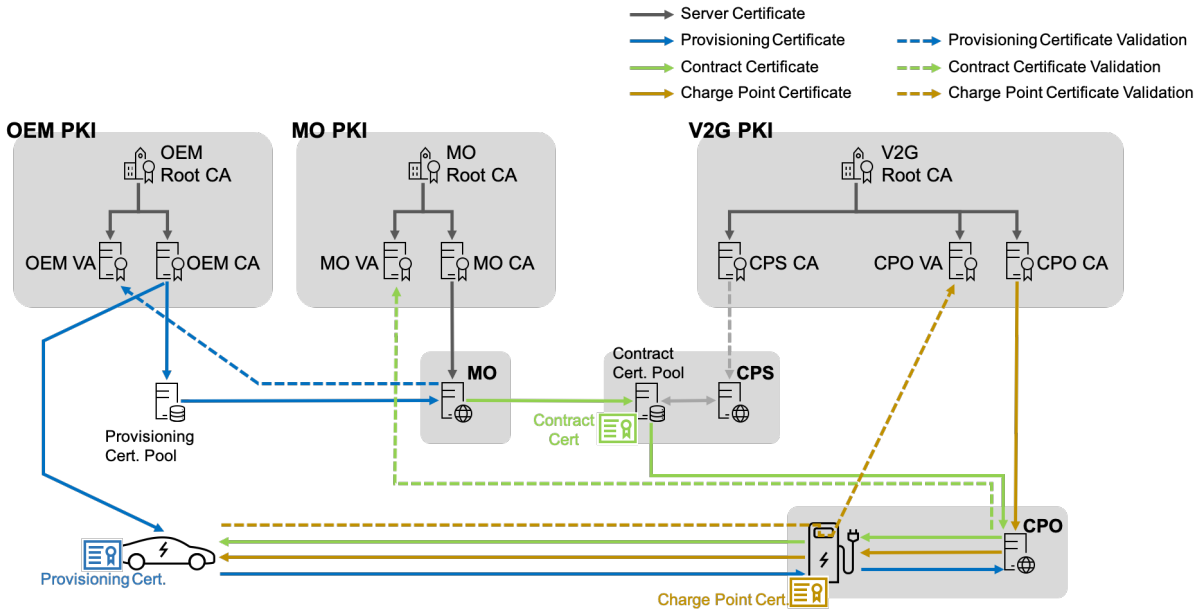

Figure 1: Plug & Charge PKI Architecture

2.1.1 Benefits of PnC

PnC allows for a lightweight software-based system without RFID. With embedded security modules, PnC requires data integrity when establishing direct connections. PnC ultimately offers user convenience, since it eliminates the need for physical cards to charge EVs. It also allows EV drivers to charge outside of their usual EV charging point network, an important issue for those who would like to use their EVs to take long-distance trips. This consideration can be especially attractive in markets like the E.U. and the U.S., where drivers may want to use their EVs to travel to different nations and states, respectively.

2.1.2 Security Considerations

A robust PnC ecosystem is based on the assumption that all stakeholders and generated data can be trusted. While eliminating the need for RFID provides convenience, it also places a heavier burden on embedded software to authenticate each other. ISO 15118 requires PKI to create a trust-based platform. Furthermore, PKI in PnC will be required to monitor and install important software updates.

Security is an important part of a PnC ecosystem to prevent fraud and unauthorized use. V2G Clarity and Hubject write:

> Currently, ISO 15118's Plug & Charge is the most secure and future-proof solution on the market. [PnC] uses a set of cryptographic algorithms and digital certificates issued to various market roles within the [PnC] ecosystem. Through this intricate web, Plug & Charge enables completely secure and tamper-proof communications between the EV and charging station – all while enabling the highest level of user convenience. [3]

The term "security" can be related to a variety of different applications in PnC, including trust between the different stakeholders, trust in the integrity of the data that is produced between these stakeholders, and data privacy for those who use this technology.

From a technology standpoint, PKI and encrypted communications provide the security foundation upon which to operate PnC on a basis of trust. As we will see in Sections 3 and 4 of this paper, however, there are additional business implementation challenges that must be overcome to enable PnC across the globe.

2.1.3 PnC Stakeholders

There are a variety of stakeholders required for PnC to become a viable business model in EV charging. The OEM provides the EV to the customer, and with it, a provisioning certificate to identify the vehicle. The

provisioning certificate is used to identify and authenticate the vehicle when connecting to the charging point, and the Charge Point Operator (CPO) provides the charging services.

The EV driver can register their account with an MO, which can authenticate the driver during the PnC process to provide contract certificates. For the sake of optimal delivery of services, as Contract Provisioning Service (CPS) is used as a pool of existing users who have charged using PnC before.

The following is an illustration of the stakeholders and their noteworthy roles in a PnC ecosystem:

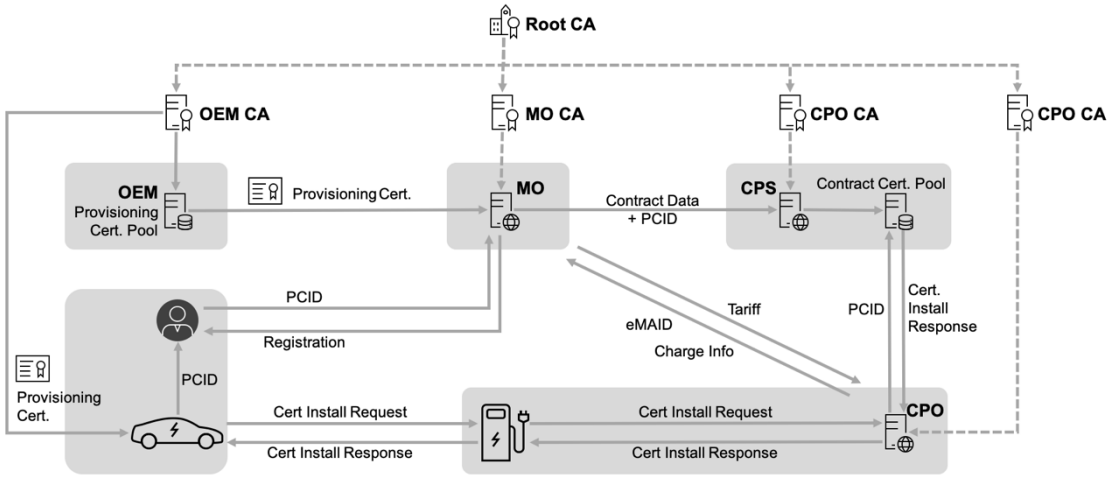

Figure 2: Plug & Charge - Overview

2.1.4 PnC Process

The following illustrates the PnC process under ISO 15118 using PKI authentication. Before any charging can begin, the car owner/user must first register with an MO, during which vehicle ownership can be verified. Once verified, the MO can create a User Agreement, which is used to create a Contract Certificate that is then transmitted to a Contract Certificate Pool. The EVSE can access this Pool to recognize existing customers in good standing, which it can then forward to the EVSE and EV, the latter of which is identified with its own unique provisioning certificate.

Assuming that the EV has been registered, the EV will request/receive the Contract Certificate to initiate charging. This certificate will be validated, and the sales tariff and the charging information will be then be transmitted to the MO.

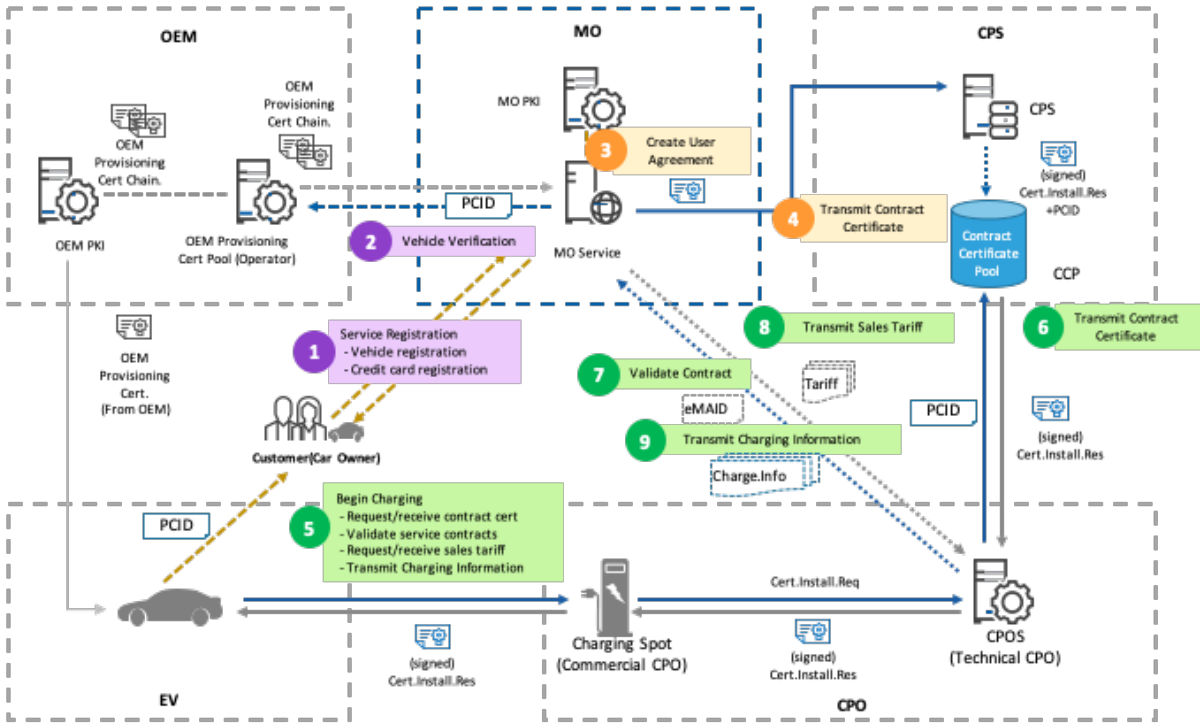

Figure 3: PKI Operations in Plug & Charge

3 Interoperability Between Root CAs for PnC

From a technical perspective, PnC can be a convenient and secure way to charge vehicles. However, PnC works with one single Root Certificate Authority (RootCA) to establish a PKI chain of trust. But it is difficult for a single RootCA to anchor all other lower authorities (SubCAs) throughout the global PnC ecosystem. For example, if an EV manufacturer exports its vehicles to a foreign market, they will have to connect to a RootCA that is not identifiable with its export market's RootCA (See illustraton below). Hence, interoperability between trusted RootCAs will be a crucial component for PnC's business viability.

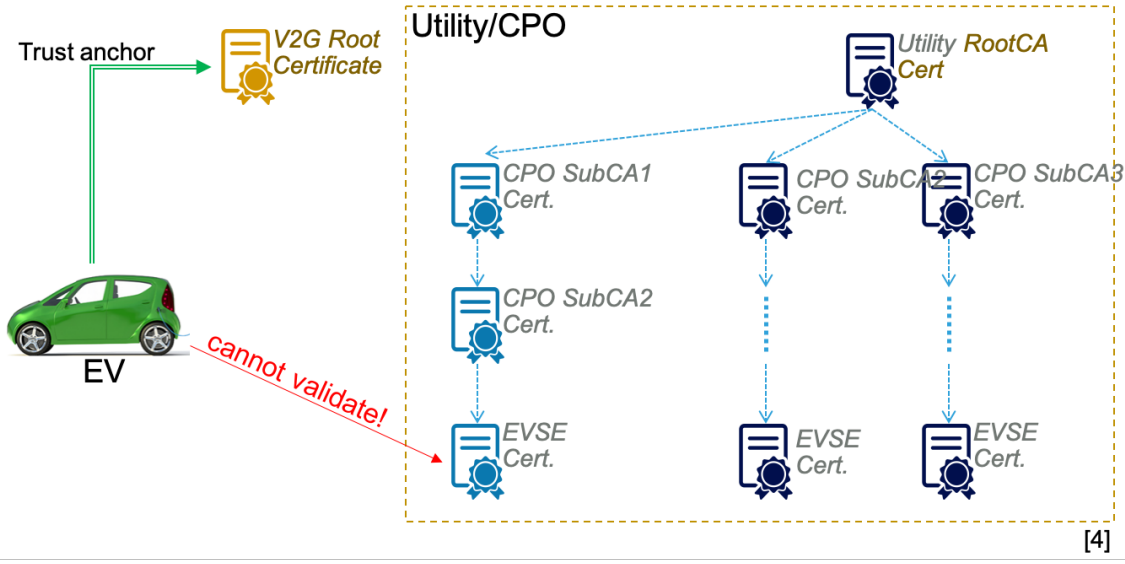

Figure 4: The Need for Interoperability Between EV and EVSE Under Utility PKI

3.1.1 Interoperability Option 1: OEMs Install All RootCAs

OEMs can install RootCAs within the vehicle for all regions in which they will be charged. However, this will require EV manufacturers to anticipate where all of its vehicles will be used, a difficult (if not impossible) task. Also, RootCAs can change over time, either through changing local market conditions or the vehicles themselves being re-sold to other regions/countries. Establishing a finite number of trusted RootCA with these kinds of variables is a severly restrictive ventures for OEMs when they roll their EVs out on to the roads.

3.1.2 Interoperability Option 2: Certificate Trust List

Alternatively, an authority can be designated to manage the Certificate Trust List (CTL) of all RootCAs that are trusted by EVs. Charging providers and OEMs can refer to this list in order to validate RootCAs that can be trusted. From a security perspective, however, the CTL presents a single point of vulnerability. More importantly, with so many stakeholders, it is likely difficult to designate such an important role to a single entity.

3.1.3 Interoperability Option 3: Cross Certification

Cross-certification refers to using mutual certificates to validate RootCAs that are not part of the original trust anchor. In the following example, the EVSE under Root "B" is using cross certification to support a vehicle under Root "A". The mutual certificate is produced by Root "A," and includes the SubjectDN and public key of Root B to validate the EVSE. Cross certification can be applied to existing ISO 15118 standards for PnC charging, and is the most viable way to achieve interoperability between two different RootCAs. However, if there are more than a few RootCAs that require interoperability, it does present a challenge for scalability. In such cases, a Bridge-CA operator to validate between multiple RootCAs can be considered to support scalability concerns. Autocrypt has initiated cross-certification tests with a few other EV charging market leaders, including Hubject GmbH.

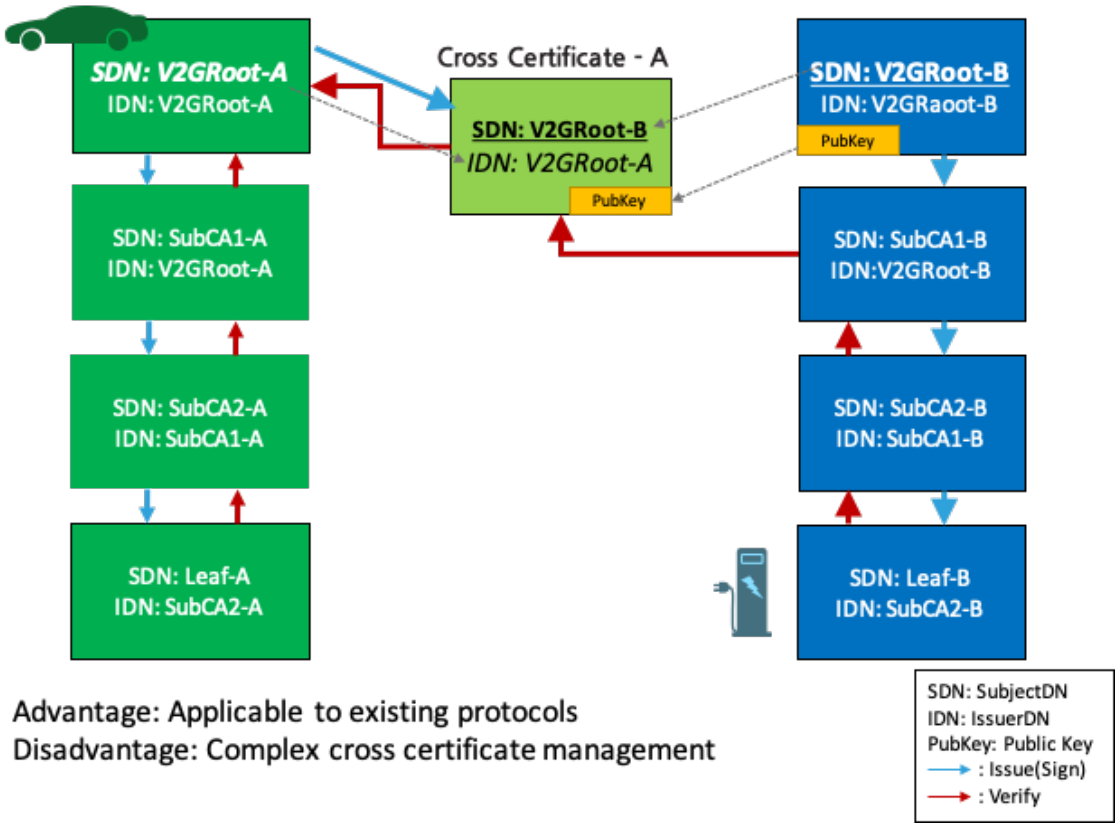

Figure 5: Technical Implementation: Cross-Certification

4 Business Implementation Considerations for PnC

PnC technology allows various different trust authoritites to provide security, privacy and convenience for EV charging. However, PnC does not, in and of itself, provide a way to be integrated into a real-world business setting. Instead, there are a variety of different technical and operational challenges that must be adequately addressed for the PnC market to be functional.

As mentioned, participation from a variety of different stakeholders is required to make PnC work. ISO 15118 covers communications between EV and the EVSE, which is transmitted using TLS encryption to form secure communication channels. ISO 15118 has not defined the communication for MOs, which provide key PnC services, and CPS operators, who are instrumental in providing a thriving business environment by storing existing customer information.

PKI in PnC is a process by which to establish trust in PnC's contract certification distribution system. However, integrating various players within the PnC ecosystem, which would include the multiple RootCA operators interoperating with one another, means that the environments in which the PKI systems are placed are important as well. Networks can be breached, and if they are, the PKI system within that network can be compromised. If the same PKI system is interoperable with another PKI, the latter may be vulnerable as well. As such, there needs to be a minimum security standard to which participants in a PnC system can be subject. As security requirements and vulnerabilities can evolve with time, there also needs to be periodically-updated auditing to which all stakeholders within a PnC ecosystem can comply.

There are a variety of different organizations that establish what a secure PKI infrastructure is, and monitor/audit them for certificate seals. WebTrust has been established to provide safe PKI practices for government and financial service transactions. TISAX provides seals for automotive parts suppliers. Market leaders like Hubject has undergone auditing by ISO 27001 to give peace-of-mind to any organization looking to use Hubject's V2G RootCA services, including for PnC enablement.

In terms of pure business enablement, Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE) has established a guide for OEMs, CPOs, MOs, and CPS operators for PnC implementation. Included in this guide are baseline requirements for any organization that is running a adequately secure PKI infrastructure.

4.2.1 VDE Application Guide VDE-AR-E 2802-100-1

The VDE Application Guide VDE-AR-E 2802-100-1 (VDE) can serve as a blueprint for establishing a PnC ecosystem. According to V2G Clarity, the VDE "closes specification gaps and serves as the blueprint for establishing a complete and well-orchestrated Plug & Charge ecosystem."[5] V2G adds:

> To actively participate in the Plug & Charge ecosystem with your product or service, you'll need to set up the corresponding business processes and implement the interfaces to other market roles in this interconnected system architecture.[6]

Two concepts that establish security and secure operational procedures for a PnC environments are Certificate Policy and Certificate Practice Statement.

4.2.2 Certificate Policy

VDE defines the certificate policy as "a technically neutral document [that] can be shared with third parties as necessary for the purpose of assessing the level of security."[7]

> [The Certificate Policy] describes the requirements applicable to the issue and use of certificates and should be written to be as generic as possible in order to allow flexibility for the specific technical solution on the basis of an operator's existing organisational, technical and structural conditions.
>
> However, the certificate policy should also be as precise as possible so as to achieve interoperability with regard to certificate and data exchange formats…Furthermore, it should be clear when the certificate policy is created how many sub-CAs are to exist in the PKI, as any change in the number necessitates revisions to the certificate policy document, which should be avoided at all times for reasons of time and cost.[8]

The certificate policy is designed to get different PnC stakeholders—MO/CPO/OEM/ V2G root operators—to establish common ground from which to operate PnC ecosystems, including those that will be interoperable between different global markets and service sectors. ISO 15118 is currently discussing how many sub-CAs can exist for interoperable ecosystems using the cross-certification method.

4.2.3 Certificate Practice Statement

If the Certificate Policy describes the "what," the Certificate Practice Statement establishes how a PKI system will be secured. According to VDE, Certificate Practice Statement "defines rules for the practice of certification and describes in detail how the requirements of the certificate policy are fulfilled…and governs organisational processes and technical methods for operating a PKI."[9]

The VDE's RFC 3647 establishes the following as the considerations that an organization must consider when writing its Certificate Practice Statement

- Introduction
- Publication and repository responsibilities
- Identification and authentication
- Certificate life-cycle operational requirements
- Facility, management and operational controls
- Technical security controls
- Certificate, CRL and OCSP profiles
- Compliance audit and other assessment
- Other business and legal matters
- References[10]

The Certificate Practice Statement provides a roadmap for different PKI infrastructure to trust one another for PKI's secure transmissions of authentication via encrypted communications. In order to take advantage of technological advantages that come with PnC, the stakeholders need a way to find a baseline on which to assure themselves that other actors are doing what is minimal for prioritizing network security. And as interoperability becomes a required component for executing new technologies like PnC, these players need to find a way to measure themselves against each other in terms of preserving security and privacy.

5 Conclusion on Security Considerations

PKI provides an accessible way to achieve advanced security for non-RFID communications. Through PKI, Ethernet communications can be made secure for not only PnC charging, but other methods like wireless and V2G charging. However, endpoint modules and PKI infrastructure need to be continually fortified to address evolving network and IoT vulnerabilities. As stakeholders continue to define these standards, it is important to focus not only on convenience, but also security and privacy protection.

Although using PKI for EV charging is expected to change the charging landscape in the future (starting with PnC), the technology itself is inadequate for business implementations. OEMs, CPOs, MOs, and CPS operators need to establish specific technological implementations necessary to ensure secure transactions and privacy protection with PKI. The oncoming demand for interoperability between various RootCA authorities is an issue that needs to be solved by leading authorities like ISO 15118, OCPP, etc.

While a well-established PKI system can enable new technology, the network environment and operational policies need to be put into place for PKI to be integrated into new technologies like PnC. VDE establishes the Certificate Policy and Certificate Practice Statement as starting guidelines, but it is up to stakeholders to determine for themselves what the minimal requirements are. And there needs to be a trusted third-party organization like ISO 27001, TISAX, or WebTrust to confirm that these minimal requirements are being followed with periodic audits.

Many future technologies like PnC is based on the presupposition that open communications between software components is the best way to derive new convenient features while preserving security and privacy. But in order for there to be open communications between organizations, there needs to be trust. Moreover,

this trust cannot be taken for granted by verbal reassurances, but monitored and audited throughout the course of business. PnC stakeholders needs to define what the requirements for this trust are, hold each other accountable, and find ways to preserve the trust, in order to take advantage of the openness that comes with software-enable features in EV charging.

References

[1] https://www.ssh.com/pki

[2] https://v2g-clarity.com/wp-content/uploads/2019/06/Whitepaper-Autocharge-vs-ISO15118-Plug-and-Charge.pdf (2019)

[3] *Ibid.*

[4] Minho Shin, "Using Cross-certification in ISO 15118" (2019)

[5] https://v2g-clarity.com/knowledgebase/basics-of-plug-and-charge/

[6] *Ibid.*

[7] VDE-ARE-E 2802-100-1, "The Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118" (English Translation)

[8] *Ibid.*

[9] *Ibid.*

[10] *Ibid.*

Author

Jaeson Yoo serves as Chief Evangelist and EVP of Business Development for Autocrypt Co. Ltd. With over nine years of IT Security consulting and public speaking experience for automobiles, IoT, PKI authentication, web security and data encryption, Jaeson brings Autocrypt's proprietary and market-proven core technologies closer to partners and customers all over the globe. Jaeson is a magna cum laude graduate of Occidental College, and is a member of Phi Beta Kappa.