PUBLIC KEY INFRASTRUCTURE MARKET PRINCIPLES

At a glance:

This paper outlines the key market rules that should be implemented to deliver an open, interoperable and competitive Public Key Infrastructure (PKI) for EV charging. Ultimately, this will play an important part in ensuring that in Europe, a driver of any EV can charge on any (publicly accessible) charging station using any service provider. It follows up on previous ChargeUp Europe papers on PKI and also the relationship between PKI and ISO15118.

Introduction

As key services such as Plug&Charge and smart charging become more widely available for EV drivers, it is critical that the Public Key Infrastructure (PKI) security framework underlying these services is developed in a way which will ensures the highest level of security, interoperability, and fair competition.

This paper outlines the key market rules that should be implemented to deliver an open and competitive PKI for EV charging. It follows up on previous ChargeUp Europe papers on PKI and also the relationship between PKI and ISO15118:

- ChargeUp Europe Public Key Infrastructure (PKI) for EV Charging, 2021
- Plug&Charge, ISO 15118, Public Key Infrastructure (PKI), and the Need for Proper Governance, 2023

Current situation - Emerging services and Public Key Infrastructure (PKI)

PKIs have the power to set access, data exchange, and control security, amongst others. This must be controlled by a central system, that validates the market rules, audits PKIs, and governs the interoperability, non-discrimination, and usability of the trusted PKIs in their PKI ecosystem.

In particular, the Vehicle to Grid (V2G) Root Certificate Authority (CA), which is a PKI, is relevant to use Plug&Charge. At present there are two V2G Root CAs for EV charging available – the Hubject V2G Root PKI and Charin V2G Root PKI. Others are being developed by Gireve, SAE and Vedecom.

Given these available and emerging PKIs it is vital that there are clear rules to ensure interoperability, fair access and competition between PKIs and market players. Ultimately, this will play an important part in ensuring that in Europe, a driver of any EV can charge on any (publicly accessible) charging station using any service provider. To achieve this, we outline the key market rules required.

Key Principles for PKI market rules

1. GOVERNANCE – CODE OF CONDUCT

- Stakeholders should adhere to a code of conduct that promotes fair competition and prevents anti-competitive behavior. This will ensure that all stakeholders compete on a level playing field, promoting innovation and the best possible outcomes for consumers.

2. ROOT CERTIFICATE AUTHORITIES (CAs)

- It will be important to enable multiple Root CAs. This will ensure that if there are security or operational issues with one Root CA then others can continue and thus disruption will be minimal. In addition, having multiple Root CAs will ensure competition on service quality and price.
- These Root CAs shall meet agreed minimum requirements regarding reliability and security.

3. INTEROPERABILITY

- Clear rules on interoperability can deliver optimal functionality and a secure ecosystem so that any vehicle works with any station.
- For example, if an EV manufacturer exports its vehicles to a foreign market where another PKI is used, interoperability between trusted Root CAs will be crucial for the scale up and rollout of vehicles.
- To enable interoperability between different Root CAs, it needs to be ensured that all parties are relying on a similar (minimum) level of requirements and cyber-security, which should be developed and overseen by external, independent auditing organizations.
- There should be a common way for a Charge Point Operators (CPOs) and Mobility Service Providers(MSPs) to get the certificates from the CA to create interoperability in the ecosystem.

4. CONTRACTS – DRIVER CONTROL AND CHOICE

Installation and Non-discriminatory contract handling

- To ensure non-discriminatory access for services such as Plug&Charge, all EVs shall support contract certificate installation independent from which MSP the customer selects.

- If an EV supports Plug&Charge, the handling – namely the installation, update, removal, and prioritization of MSP contracts – in the EV needs to be defined so that the user has full control over their MSP contracts and is able to easily install, remove, update and prioritize contracts as they wish – e.g. through an easy process via their in-car or mobile display.

- EV-OEMs, therefore, need to provide all relevant information (including the Provisioning Certificate Identifier(PCID), which identifies the EV) to the customer in as simple a way as possible.

- This multi-contract handling should be supported by MSPs and EV OEMs.

5. DATA PROTECTION

- For the Plug&Charge functionality, supported by a PKI, contract certificates will be generated and issued by MSPs. Those contract certificates need to be installed in the EV.

- It is important that mechanisms are put in place to protect sensitive competitor data on installed contract certificates (i.e., anonymization of contract information).

6. TRUST

- To establish trust and confidence, there is a need to define criteria for trusted actors to join a PKI. Such a trusted actors list should be established and governed by a central, independent system.

7. PREVENTING ANTI-COMPETITIVE BEHAVIOUR

- EU regulation and governance rules should ensure that driver information and choice is prioritized. This will deliver a level playing field between MSP offers and ensure that every MSP (third-party or EV-OEM or CPO owned) can provide an equal, seamless (in-vehicle) user experience and functionalities for Plug & Charge and no "self-preferencing" occurs whereby the driver is bundled or locked-in to a specific service.

- Such bundling undermines the ability of EV drivers to choose and can lead to the market being dominated by a small number of large players, reducing competition on innovation, services, and pricing and reducing choice for the driver.