



# ChargeUp Europe

## Public Key Infrastructure (PKI) for EV Charging

# ChargeUp Europe: A vision for Public Key Infrastructure (PKI) for EV Charging

[ChargeUp Europe](#) is the voice of the electric vehicle (EV) charging infrastructure industry. ChargeUp Europe has been formed to accelerate the switch to zero emission mobility and ensure a seamless driver experience with access to high quality, readily available charging infrastructure across Europe.

This paper outlines the importance of public key infrastructure (PKI) for EV charging. As e-mobility becomes mainstream the security of communications and transactions is ever more critical. To ensure the widespread rollout of EVs and EV charging around the globe, ChargeUp Europe calls for the development of a common global governance for EV charging PKI.

## (1) Public Key Infrastructure - Overview

### What is Public Key Infrastructure?

- Public Key Infrastructure (PKI) is a technology to authenticate users and devices in the digital world, with trusted parties digitally signing documents certifying that a particular cryptographic key belongs to a certain user or device.
- PKI facilitates the secure transfer of electronic information for a range of activities such as e-commerce and online banking.
- It is required for activities where regular passwords are an insufficient authentication method and more proof is required to confirm the identity of the parties involved in the communication and to validate the information exchange<sup>1</sup>.

### Why PKI and EV Charging?

- PKI is of major importance in the electric vehicle (EV) charging world. It addresses the needs of EV charging stations by providing trust. From user authentication to data protection, PKI can secure the EV charging process.
- PKI can be utilized as a trust-based platform to authenticate users, EVs, charging stations, and others. It can encrypt and authenticate data transfers such as station to vehicle, service provider and station-to-station, offering security across platforms.
- PKI offers a secure and convenient way to authorize charging services.
- PKI in the EV charging industry is also needed for securing the scaling of roaming e.g. via OCPI<sup>2</sup> where security aspects are currently managed in a manual way.


### What are some of the key elements of a PKI?

- A certificate authority (CA) stores, issues and signs digital certificates. A digital certificate is an electronic document used to prove the ownership of a public key. The presence of a CA allows others to rely upon signatures made about the private key that corresponds to the certified public key.

---

<sup>1</sup> Common examples of PKI security today are SSL certificates on websites so that site visitors know they're sending information to the intended recipient.

<sup>2</sup> OCPI - The Open Charge Point Interface protocol (OCPI) is a protocol that supports the connections between Mobility service providers and Charge Point Operators.

- 
- A registration authority (RA) verifies the identity of entities requesting their digital certificates to be stored at the CA;
  - A central directory is a secure location in which keys are stored and indexed;
  - A certificate management system oversees, amongst others, access to stored certificates and delivery of the certificates to be issued;

#### Why are the certificate authority (CA) and the root CA important?

- The CA has a critical role as a trusted third party—trusted both by the owner of the certificate and by the party relying upon the certificate.
- For this reason, it is important to have an independent CA managing the issue of the PKI to maintain the independence (neutral 3<sup>rd</sup> party) with the recipient of the data and/or transaction.
- The CA generally handles all aspects of the certificate management for a PKI, including certificate lifecycle management (e.g. revoking or re-issuing of certificates).
- A Root CA is a trusted CA that can verify the identity of a person and signs the root certificate that is sent to a user.

#### What are other industry sectors using PKI?

- **Air traffic/ “airport operations”** where there is one worldwide PKI structure/design (approved by all airline industry regulators). Any entity can run a certificate authority if they qualify according to very detailed rigorous technical criteria. The root CA (can be one entity per country or per industry, not limited) is controlled and earns the trust to be this root.
- **In e-commerce**, if a user purchases something using a browser and the merchant uses a safe store on a server that the browser presents between the parties (the “lock sign”) - once that is trusted the user can progress. If the merchant’s server is hacked then all its PKI certificates get revoked by the PKI operator who detects that the merchant has been compromised. This is an example of why the independence of the PKI authority is so important.

#### What is the relationship between PKI and ISO15118?

- In many discussions relating to EV charging, PKI and ISO15118 (the standard which enables plug&charge (PnC) and other functionalities) often become intertwined. It is very important to highlight that PKI is separate from ISO15118. PKI will be important for communication and data transfer for a wide range of EV charging processes, as listed in the section above.
- However, ISO15118 will need a PKI to enable its use of certificates for securing features like identification and authentication of the driver to authorize the EV charging and activation of the charging process.
- In particular, ISO 15118 uses certificates that are created and managed by the PKI throughout the lifecycle of the certificate.

## (2) Developing a PKI for EV charging

### A Global and independent approach

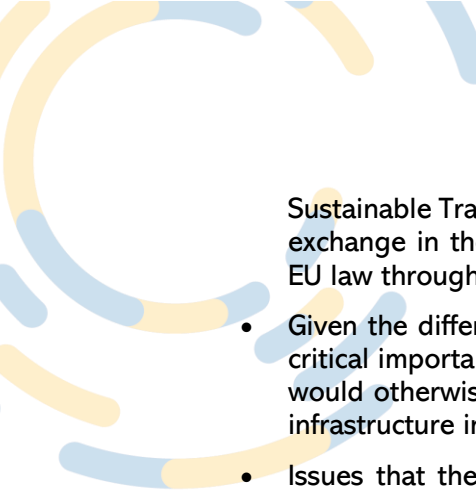
- For EV charging, as a fast growing, global industry, there is a need for a global PKI solution supported by a common governance structure that is designed to operate and serve worldwide all EVs, charging stations and EV charging service networks.
- The governance should lay out the rules and guidelines for trust/authentication between the EV and the station, network, service provider and station-to-station, offering trust across platforms.
- It will be important for charge point operators, mobility service providers, OEMs and other stakeholders that there is a common vision, governance, definitions, and requirements for PKI across EV charging domains and across geographical locations so that e-mobility can scale consistently and rapidly.
- The governance should look at two overarching issues in particular: (1) technical requirements to deliver a reliable approach to establishing digital trust and protecting electronic exchanges, including the integrity and privacy of consumer data and (2) management and market rules to provide clarity for operators.
- The design of this PKI governance for the EV charging industry needs to be done in a qualified, balanced, and neutral industry coalition rather than through a single organisation.

### Key elements for a global governance approach

- While a common governance approach is optimal, it will also 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 CA's will ensure competition on service quality and price.
- Interoperability between root CA's is key. For example, if an EV manufacturer exports its vehicles to a foreign market, interoperability between trusted root CAs will be crucial for the scale up and rollout of vehicles.
- It is critical to have a neutral root CA to ensure independence of data handling. This principle should be embedded in governance and legislation.
- Certificates servicing should however be left to the market as a business, as already happens already in other industry segments.
- Multiple PKIs are viable but will certainly add a layer of complexity and cost. Interoperability must be ensured so that for example, if an EV is connected to a certain PKI and the charging point to another, they can communicate and carry out transactions.

### Recommendations to deliver PKI for EV charging through EU leadership

- We support the development, through a neutral industry coalition, of a common global approach to PKI governance.
- The European Union should however take the opportunity of its Green Deal agenda and rapidly accelerating EV adoption to take the lead to develop a PKI governance framework that could eventually be adopted at a global level.
- This PKI governance framework should be developed in the context of the Alternative Fuels Infrastructure Regulation revision and through the expert work ongoing in the



Sustainable Transport Forum sub-group on governance and standards for communication exchange in the electromobility ecosystem. This could then eventually be embedded in EU law through a Delegated Act.

- Given the different interests of commercial parties in the EV charging ecosystem it is of critical importance that the EU facilitates the process of the creation of this framework. It would otherwise be a lost opportunity and possibly slow down the further rollout of EV infrastructure in Europe.
- Issues that the governance framework should address include topics such as defining criteria for trusted actors to join a PKI and end-to-end interoperability which will be fundamental for the enabling fast rollout of EV charging and the best EV driver experience.
- Clear rules on interoperability can deliver the best functionality and secure ecosystem so that any vehicle works with any station. To realise this, it will be important to have certainty around the de jure and de facto open protocols and standards that the industry can work with as minimum requirements, such as OCPI, OCPP<sup>3</sup>, ISO15118.

---

<sup>3</sup> The Open Charge Point Protocol (OCPP) is an open-source communication protocol for EV charging stations and network software companies. It enables EV charging stations to communicate with central management systems from different vendors