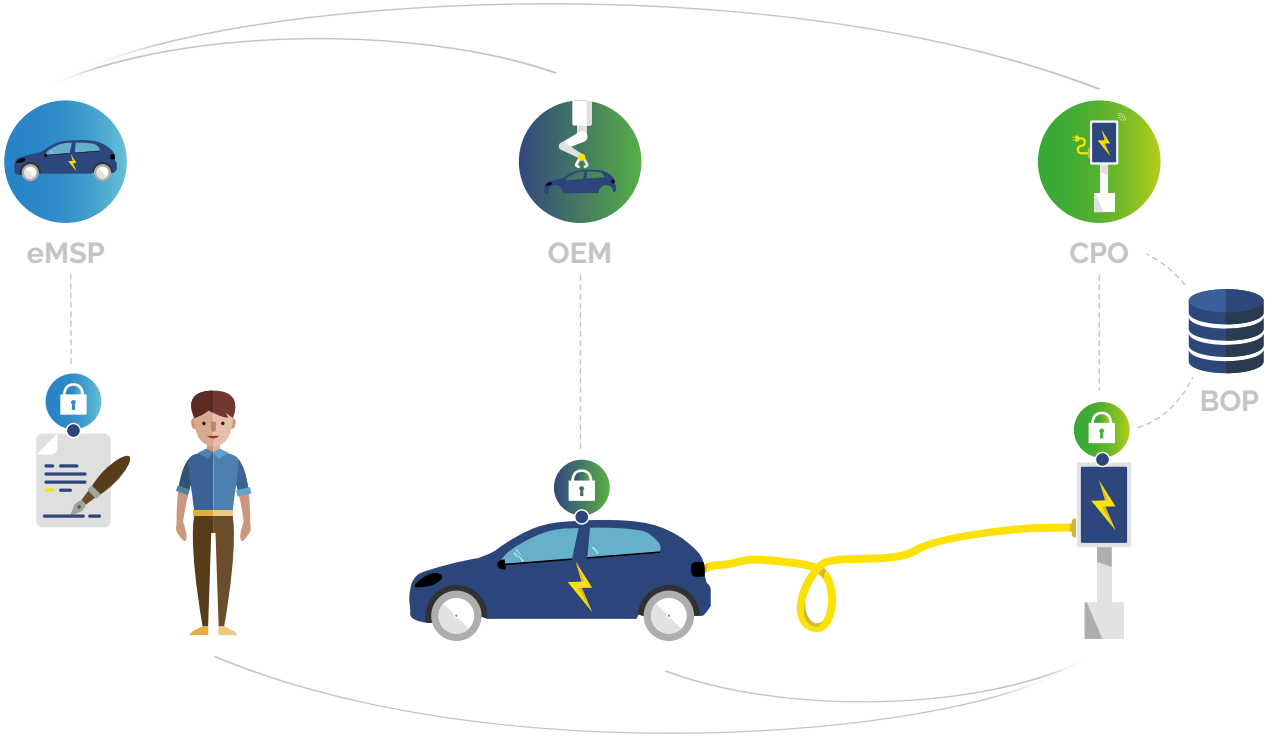

ISO 15-118 is a standard that describes a protocol of communication between vehicle and charging station to bring new features. The "Plug and Charge" feature is its most visible improvement: it enables a driver to start a charging session on its EV by plugging in the cable, without having to use a badge, a credit card or a mobile application. The user is identified automatically by the connection between the vehicle and the charging point. 15118 is an opportunity for the electromobility ecosystem.

It provides simplicity for EV drivers, makes progress in energy optimisation, reduces costs, and enhance (cyber)security.

15-118 WILL IMPROVE EV DRIVER EXPERIENCE OF CHARGE

ISO 15-118 will not only improve the experience of charging for the EV driver, but it will also help the entire e-mobility ecosystem, enhancing available services and securing operators exchanges:

1. **Improved user experience**: New features for EV-drivers will bring simplicity in the user journey. The "plug & charge" feature is a good example: No badge, no smartphone app, no credit card… "you plug, you charge"
2. **Enhancing smart charging**: Smart-charge refers to processes where charging is driven to optimise the balance between energy delivery constraints, opportunities, prices, and the EV driver's mobility need and flexibility. ISO-15118 that allows a secured and enriched communication between EVs and charging station is a good base for new "smart-charge" use cases.
3. **Introducting cyber-security in e-mobility**: ISO-15118 is the first standard that introduces "Cybersecurity" in the electromobility ecosystem. Security is essential for the expansion of the EV industry. ISO 15-118 standard could guarantee that issues like payment fraud, identity theft and system hacking are tackled.
4. **High power charging standard**: ISO-15118 is a key element of the CCS standard (Combined Charging System) that simplifies the physical connexion between vehicle and charging station, with only one plug for both AC and DC. CCS will be, with CHAdeMO, the main standard for "High Power Charging", which is the capacity to charge up to 350kW.

The ISO-15118 standard is based on certificates and requires a clear policy. This communication is supposed to take place in a given context: first, the charging station must be connected to a CPO back-end system (BOP) and be authenticated by certificates. Vehicles must also be authenticated by certificates. Those vehicle certificates are delivered by Car-Makers and must be accessible and trusted by Mobility-Operators. For "plug & charge" features, the user must have a valid subscription to an eMSP offer, described in a certificate. These certificates are delivered by e-Mobility Operators (eMSP) and must be accessible and trusted by Charging-Points-Operators and by Car-Makers. The certificates must circulate between actors. This circulation process is usually called "pool mechanism".

15118 SHOULD BE ESTABLISHED IN AN OPEN, FREE, ROBUST AND FAIR MARKET

Since the actors systems authentication and security is based on certificates, actors have to agree on **WHO** are the trusty certificates providers (the "Root Certificates Authorities") and **HOW** they have to provide certificates. This implies an agreement on a common set of basic rules (market rules) and requirements (Certificate policies).

The 15118 standard needs some contextual elements among which a well-governed "cyber security environment". GIREVE is working on establishing a robust governance with one main goal: the electro-mobility industry must be rooted in an open, free, robust and fair market. It means:

NO MONOPOLY
Nurture healthy competition, limit the impact of actor exit (bankruptcy, security breach etc.) on the global scale

HIGH SECURITY
Payment security and fraud prevention. Protection against cyber attacks

COST REDUCTION
Reduce operating costs for the benefit of EV-Drivers

GIREVE'S 15118-RELATED PROJECTS WITH PARTNERS

"Recommendation on communication security for roaming electric vehicle charging PKI architectures related to ISO 15118 charging station-vehicle communication standard"

PKI symposium & PKI roundtable (2019), pilot and prototyping action plan to compare different architectures on which to set up a multi-certificate authorities organisation.

Management of the working group "Authentication and security" that includes the 15118 cyber security topics.

We contribute to the "PKI CharIn task Force" that aims to define a certificate policy, at least for 15118.

GIREVE'S 15118-RELATED SERVICES

ROAMING AND AUTHORISATION MECHANISM

In the 15118 Plug & Charge use case, the user doesn't authenticate itself (usually using an RFID badge). The vehicle itself has the user-contract ID stored in a secured onboard controller for authentication. When plugged-in, the charging station doesn't read the badge, but receives a contract ID through the power cable!

The roaming authorisation features were up to now, based on RFID badges. They must be extended to 15118 contract-based authorisations.

GIREVE's platform is already compliant with this authorisation mechanism.

THE CERTIFICATE AUTHORITIES CHAIN (ROOT-CA AND SUB-CA)

The Root Certificate Authority (Root-CA) is the highest actor in the certificates issuing chain. It authenticates delegate sub-authorities (Sub CA) which can authenticate other delegate sub authorities …. In ISO 15-118 this authorities chain is limited to three levels.
The overall trust principles are based on this chain: all its parts must be trusty and secure. They must implement the commonly defined Market Rules and meet the common Certificate Policy requirements.

CERTIFICATE ISSUING

eMSP, CPO, OEM etc. have to deliver certificates. They can do it by themselves (and thus become a Sub-Certificate-Authority) or use a "certificate-as-a-service" provider: an efficient way to improve their time-to-market by avoiding the cost and time of acquiring complex skills and knowledge related to cryptography and cybersecurity.