Secure and User-Friendly EV Charging

A Comparison of Autocharge and ISO 15118's Plug & Charge

June 12, 2019

Table of Contents

Figures

Abbreviation Key

Term	Description
CA	Certificate Authority
CCS	Combined Charging System
CPO	Charge Point Operator
CSMS	Charging Station Management System
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EIM	External Identification Means
EMAID	E-Mobility Account Identifier
EMP	E-mobility Provider
EMPS	E-mobility Service Provider
EV	Electric Vehicle
EVCC	Electric Vehicle Communication Controller
EVCCID	Electric Vehicle Communication Controller Identifier
ICE	Internal combustion engine
MAC address	Media Access Control address
MITM	Man-in-the-middle (attacks)
MO	Mobility Operator (aka: EMSP, EMP)
OCPI	Open Charge Point Interface
OCPP	Open Charge Point Protocol
OEM	Original Equipment Manufacturer (here: car manufacturer)
OFA	Open Fastcharging Alliance
OICP	Open InterCharge Protocol
PKI	Public Key Infrastructure
RFID	Radio-Frequency Identification
SLAC	Signal Level Attenuation Characterization
TLS	Transport Layer Security
VPN	Virtual Private Network

Introduction

The terms Autocharge and Plug & Charge are currently circulating in the electric vehicle (EV) industry. At first glance, both refer to the same user experience: offering a seamless and customer-friendly charging process that starts as soon as the EV driver plugs the charging cable into the EV — with no additional user steps required. To simplify the charging experience, the e-mobility industry is working to eliminate the hassle of using an external device to authorize the EV driver at a charging station. The act of paying with a credit card, using an app to scan a QR code, or finding that easy-to-lose RFID card can be a thing of the past.

In fact, the technology to make this vision into a reality is available now. Secure and scalable IT systems can seamlessly authenticate the user, automatically authorize him or her for the charging process, and settle the billing process after charging. The two main applications currently used for the Combined Charging System (CCS) are Autocharge and ISO 15118's Plug & Charge. But which hassle-free charging application is best suited for any given situation? Without further background knowledge, one might even confuse Autocharge with Plug & Charge (which is a term coined by the ISO 15118 standard). However, the two approaches differ drastically in their underlying security and complexity. The implementer not only needs to consider the necessary security level for a particular use case, but also must consider the related implementation and operational costs, along with the long-term viability, for the selected approach. This article will shed light on the differences between Autocharge and ISO 15118's Plug & Charge. The objective is to enable readers to decide which solution is favorable for each particular use case.

Autocharge

The term "Autocharge" describes a process that enables a charging station to authorize a CCS-equipped EV for charging based on the unique identifier that the EV sends to a charging station when it is plugged in. After a first-time registration by the charge point operator (CPO), all chargers in the network will instantly recognize a customer's vehicle and initiate charging automatically. There is not yet an industry-wide agreement on which type of identifier to use. However, it seems to be the case that most EVs use the media access control (MAC) address assigned to their communication controller. The MAC address is used as a network address for most network technologies including Ethernet, Wi-Fi, and Bluetooth.

One of the available publications on Autocharge is the paper which the Open Fastcharging Alliance (OFA) published on GitHub. Here, the mechanism behind Autocharge is outlined as follows:

1. The driver connects his/her EV to the charging station by plugging in the charging cable.

2. The EV sends its MAC address to the charging station.

3. Autocharge relies on the Open Charge Point Protocol (OCPP) version 1.5 and higher as a communication protocol between the charging station and a charging station management system (CSMS) in the cloud. The charging station uses OCPP's 'Authorize' request to send the MAC address it received from the EV to the CSMS.

4. The CSMS will then read the MAC address from the received Authorize request and check if the MAC address matches a whitelist of EV MAC addresses. In the case of a match, the CSMS then sends an Authorize response message back to the charging station. This confirms that the EV is allowed to charge and charging begins.

5. Optional: In case there is no matching whitelist entry, the CSMS will store the MAC address on the whitelist and send an Authorize response message to the charging station that denies the authorization. As a result, the charging station will indicate to the user that he or she needs to authorize the EV using one of the other available methods like RFID card or smartphone app. The user will then be able to use Autocharge for future charging sessions.

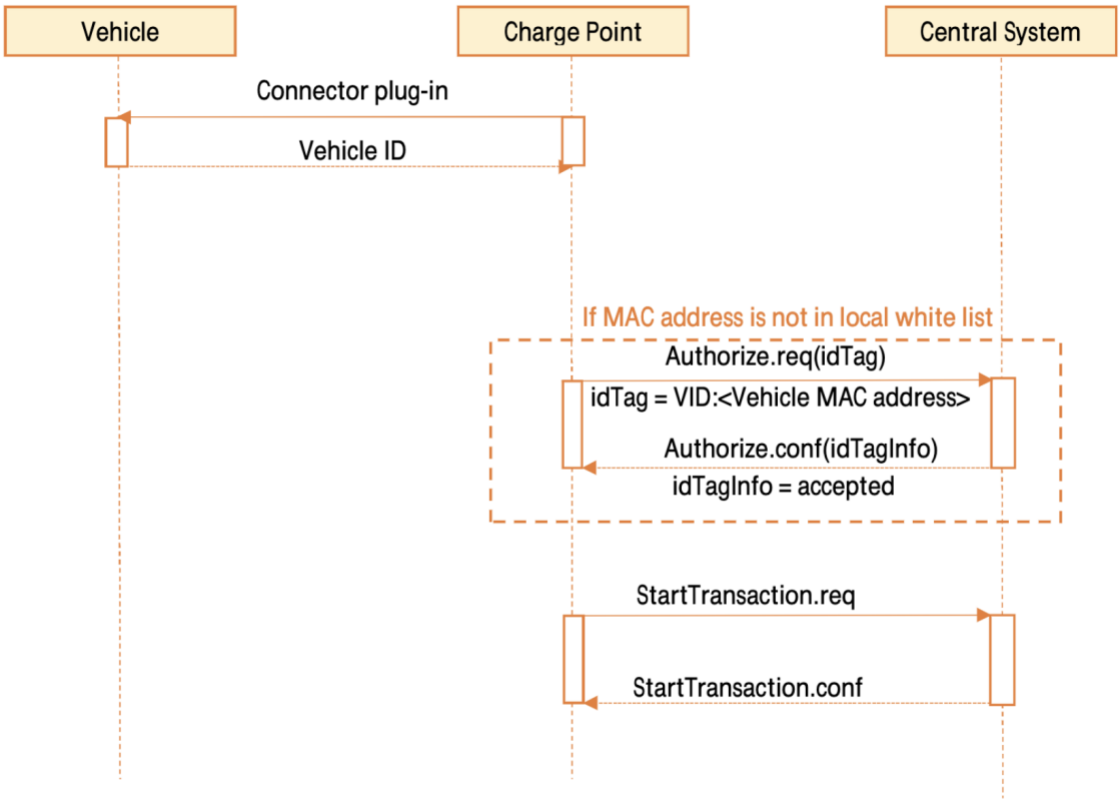

Figure 1: How Autocharge works with OCPP (© Open Fastcharging Alliance, 2019)

The mobility operator (MO) could give the user the opportunity to link his or her MAC address with the MO user account by using a communication channel other than OCPP, such as a smartphone application. Many, if not most, CPOs already maintain a whitelist of valid RFID tokens which they exchange with their roaming partners on a regular basis. For this, they use roaming protocols like OCPI or OICP. The same procedure applies to maintaining a whitelist of MAC address.

As the OFA paper states, currently only the Combined Charging System (CCS) provides the EV's MAC address. There are two ways for a charger to retrieve the EV's MAC address. The charging station manufacturer decides whether to retrieve the MAC address during the setup of the communication link, or after. The two options look like this:

1. During the setup of the communication link: the EV and charging station use the Signal Level Attenuation Characterization (SLAC) protocol, as outlined in the HomePlug Green PHY specification for powerline communication. Each SLAC message is transmitted in an Ethernet frame carrying the sender's MAC address.

2. After the communication link is established: the EV and charger will either use DIN SPEC 70121 or ISO 15118 as the higher-level communication protocol. Both protocols initiate a communication session with a "Session Setup Request" message, which carries a field called

Electric Vehicle Communication Controller ID (EVCCID). This field contains the MAC address of the EVCC as six bytes.

It may make more sense to go with the second approach, as the EV should first initiate a communication session via the Session Setup Request before the charging station should try to authorize that EV for charging. The second approach is preferable from a security standpoint as well, which we'll see in the section of this paper dedicated to evaluating the security of Autocharge.

Fastned and EVgo are two CPOs that have publicly announced their support of Autocharge.

Key Benefits of Autocharge

As stated by the OFA, the main benefits of Autocharge are:

- Higher degree of user-friendliness over traditional authorization methods like RFID cards and smartphone apps
- Higher level of security compared to the widespread RFID technology (MIFARE Classic), as MAC addresses are not as easy to replicate as RFID cards
- Relatively simple implementation
- No major changes needed in backend IT systems, as Autocharge works with OCPP 1.5 and higher
- Functionality with all existing and future CCS vehicles on the market

Security Analysis of Autocharge

Currently, RIFD cards are the most widely-used way to authorize an EV for charging. The problem with RFID cards is that they can be copied with little effort. Given this concern for security, Autocharge is an important step in the right direction. It is much harder to change the MAC address that the EV automatically sends via the charging cable. Also, the user-friendliness factor is higher than fueling internal combustion engine cars (ICEs), where drivers are required to pay for fuel by cash or credit card.

Yet, given that the MAC address is used as an identification token for the charging and billing process, any misuse of this data must be prevented. Several man-in-the-middle (MITM) attacks must be considered when assessing the level of security that Autocharge provides. Potential MITM attacks include:

1. Changing the MAC address within the EV
2. Manipulating the MAC address on the way from the EV to the charger
3. Manipulating the MAC address on the way from the charger to the CSMS
4. Manipulating the MAC address on the way from the CSMS to the mobility operator (MO)

These attacks fall into the category of MAC spoofing[1], which is an attack used to hide one's digital identity or to imitate another. In order to avoid MAC spoofing, the following three cryptographic principles must be guaranteed:

- Confidentiality
  The content of a message (plain text) shall only be readable by the intended recipient(s) and not by any unauthorized third parties.

- Integrity
  An unauthorized modification of the sent message shall be avoided or at least detected.

- Authenticity
  Evidence that the communicating parties are truly the persons or entities which they claim to be must be part of the authentication process.

Confidentiality can be guaranteed by setting up an encrypted communication channel between each communicating party using Transport Layer Security (TLS). Integrity and authenticity can be realized by creating and verifying digital signatures. Public key infrastructures (PKIs) are a common technology used across a variety of industries to guarantee these two pillars of IT security.

Communication Protocols That Currently Enable Autocharge

- DIN SPEC 70121
- ISO 15118

DIN SPEC 70121 is a subset of an early version of the ISO 15118 standard that solely focuses on DC charging and does not support a secure communication via TLS. ISO 15118, on the other hand, supports TLS. However, TLS is only mandatory for the Plug & Charge identification mode, which we'll analyze in the following section. The other supported identification mode is called EIM, short for External Identification Means. EIM refers to those identification methods that involve additional user interaction, like presenting an RFID card to a reader at a charging station or scanning a QR code with a smartphone application. Whenever Autocharge is used based on ISO 15118, the EIM identification mode applies.

A secure communication channel between the charger and the EV then depends on whether or not both sides — EV and charger — support TLS. If, for example, the EV supports TLS, but the charging station does not, it is up to the car manufacturer's implementation how to proceed: either stop the communication (and charging process) due to an insecure communication link, or continue to make sure the driver can charge his or her EV and ignore the lower security level. The latter might currently be a more likely use case to not upset the driver. Hence, we might end up with an unencrypted communication between the EV and charger.

The communication path between the charger and the CSMS (and between CSMS and MO) also needs to be encrypted. As stated earlier, Autocharge relies on the OCPP version 1.5 and higher. OCPP 2.0 is the first version that supports TLS. This said, in order to guarantee confidentiality with OCPP 1.5 or 1.6 (the only available releases before 2.0 came out), the CPO would have to make sure the charger and CSMS communicate via a Virtual Private Network (VPN), which itself takes care of establishing a TLS connection.

[1] https://en.wikipedia.org/wiki/MAC_spoofing

As a result, confidentiality can only be achieved with Autocharge if the EV and charger communicate via ISO 15118 and if TLS is used between each communicating party. This leaves us with the remaining task of verifying the integrity of the MAC address and the authenticity of the EV as the sending party. This is something Autocharge cannot provide. If someone manages to change the MAC address, then there is no way to automatically detect this data manipulation.

In the end, a malicious third party could access and use anyone's account. It is up to the CSMS operator to evaluate the likelihood of such an attack and the resulting financial risk that could arise for both the driver and the CSMS operator itself. The only possibility for a CPO to prevent unauthorized access via spoofed MAC addresses is to maintain a blacklist of such MAC addresses. However, as a result, both the rightful owner of the MAC address and the EV sending the spoofed MAC address would be blocked from charging at the charging stations managed by that CPO. As you can see, although Autocharge appears to be a reasonable approach, it may not be the most secure solution to user-convenient charging.

ISO 15118's Plug & Charge

The solution to the above situation is to rely on digital signatures and public key infrastructures. This security paradigm is built into the Plug & Charge identification mode, as defined by ISO 15118. Plug & Charge allows for utmost user-convenience combined with the highest level of data security.

Overview of Security Mechanisms within Plug & Charge

Verifying authenticity and data integrity are features that can only be realized through asymmetric cryptography, which uses a key pair composed of a private and a public key. Both keys are mathematically linked to each other in such a way that a message encrypted with a public key can only be decrypted with its corresponding private key, and vice versa, as illustrated in the image below. The private key must be kept secret and is only used to create digital signatures by the entity to which it belongs. The public key is distributed to peers in the same ecosystem and used to verify the signature that was created with the associated private key. This process ensures that the EV and charging station establish trust in the authenticity and integrity of the messages they send to each other.

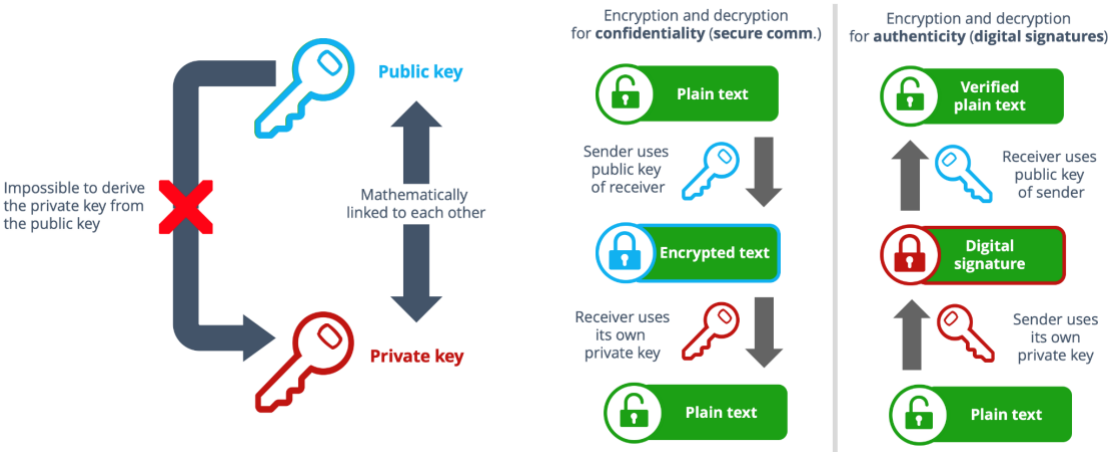

Figure 2: Relationship between private and public keys in asymmetric cryptography (© V2G Clarity, 2019)

ISO 15118 follows a hybrid approach that uses asymmetric-key algorithms to create and verify digital signatures and to agree upon a symmetric key. This can then be used to encrypt/decrypt all messages during a charging session with a symmetric-key algorithm.

The cryptographic mechanisms that come into play during ISO 15118's Plug & Charge can be summarized as follows:

- Transport Layer Security (TLS v1.2) protocol is used to establish the encrypted communication session.
- A key agreement protocol, called Elliptic Curve Diffie-Hellman (ECDH), is used to mutually agree upon a shared (symmetric) TLS session key that is valid for one charging session.
- Symmetric block cipher AES-128-CBC (ISO 15118-2) and AES-128-GCM (ISO 15118-20) are deployed to encrypt and decrypt all messages during a charging session using the symmetric TLS session key.
- Elliptic Curve Digital Signature Algorithm (ECDSA) will then verify the authenticity of the sender and the integrity of the received message (using SHA-256 as a cryptographic hash function).

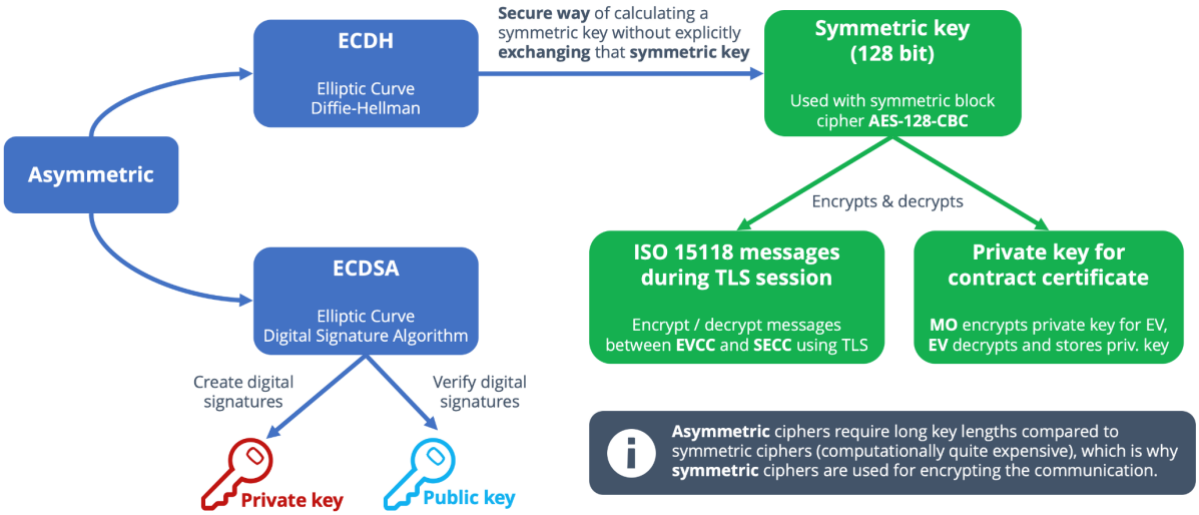

Figure 3: The hybrid cryptosystem approach used in ISO 15118 (© V2G Clarity, 2019)

In order to make sure that a specific public key belongs to a certain entity (like a particular EV or charging station), we need to rely on the concept of digital certificates. A digital certificate is an electronic document used to verify that a public key belongs to an authorized party. It is, therefore, also known as a public key certificate. A digital certificate's authenticity is bound to a digital signature that was created by a trustworthy third party called a certificate authority (CA). Acting as a trusted third-party, every CA is responsible for validating the digital identity of a certificate holder before issuing the corresponding certificate.

ISO 15118 outlines the complete ecosystem of digital certificates that need to be in place to enable Plug & Charge. These X.509 certificates are the same ones that are used in everyday Internet technology. Public key infrastructures (PKIs) come into play to verify the digital certificates within Plug & Charge. A

PKI is a tree-like, hierarchical structure of trusted CAs. These CAs manage the creation, storage, distribution, and revocation of digital certificates. One example of a common PKI is a building's security system where you present an ID card to a card reader at the door to enter. A certificate stored on the card lets the reader verify whether or not you're allowed access to the building.

The motivation for establishing a PKI is to provide a framework for verifying the digital identity of people and devices, enabling confidential communication, and guaranteeing controlled access to resources. In the case of ISO 15118, the X.509 certificates act as digital identities that are essential to authenticate and authorize access to charging services provided by market participants in the Plug & Charge ecosystem. The charging station, for example, authenticates itself to the EV in order to establish a trusted communication channel via TLS. This is the same principle as when we surf the web: the web server authenticates itself to your browser before showing the web page. In the case of EV charging, once TLS is set up, the EV authenticates and authorizes itself for charging using what is called a contract certificate. We'll explore contract certificates in the following section. When designing the Plug & Charge ecosystem, the concerns of the individual market roles are separated so that the required PKIs are able to operate independently.

The image below shows the set of CAs and certificates that are required and must be managed to enable secure and trusted communication among all involved parties.

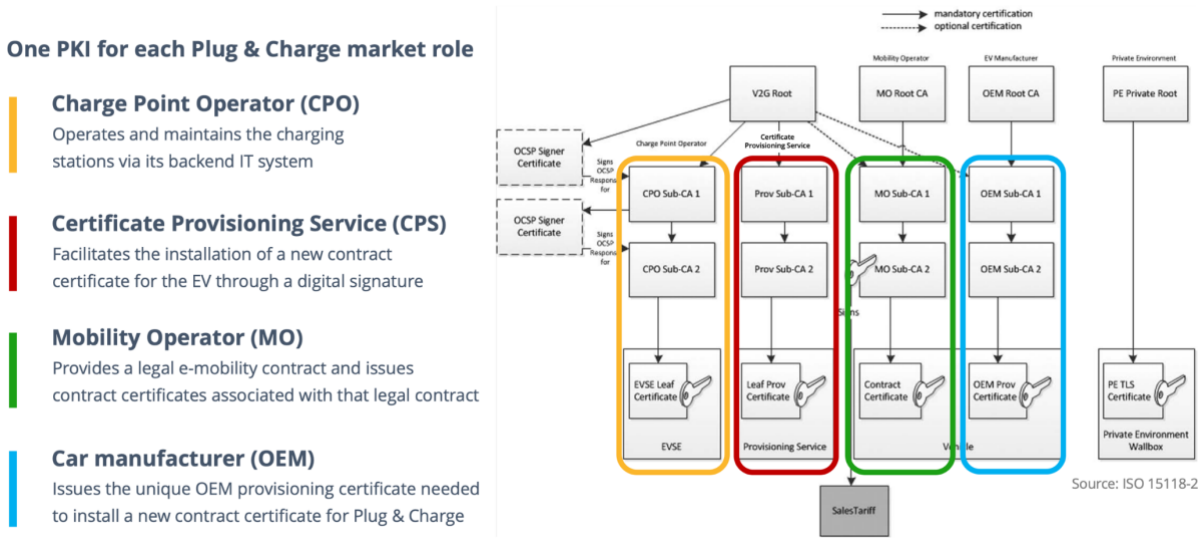

Figure 4: Public key infrastructures outlined in ISO 15118 (© V2G Clarity, 2019)

Seamless Authentication and Authorization with a Contract Certificate

This section will walk you through the authentication and authorization process that Plug & Charge follows using a contract certificate. Before the charging station permits the EV to charge its battery using Plug & Charge, the EV needs to present a valid contract certificate (and associated sub-CA certificates — see MO Sub-CA1 and MO Sub-CA2 in the image above). This will allow it to be authorized for charging. The charging station or CSMS will have the corresponding Root CA certificate on hand to verify each and every signature along the chain of MO certificates. An example for such a contract certificate, given in the X.509 format, is shown in the image below:

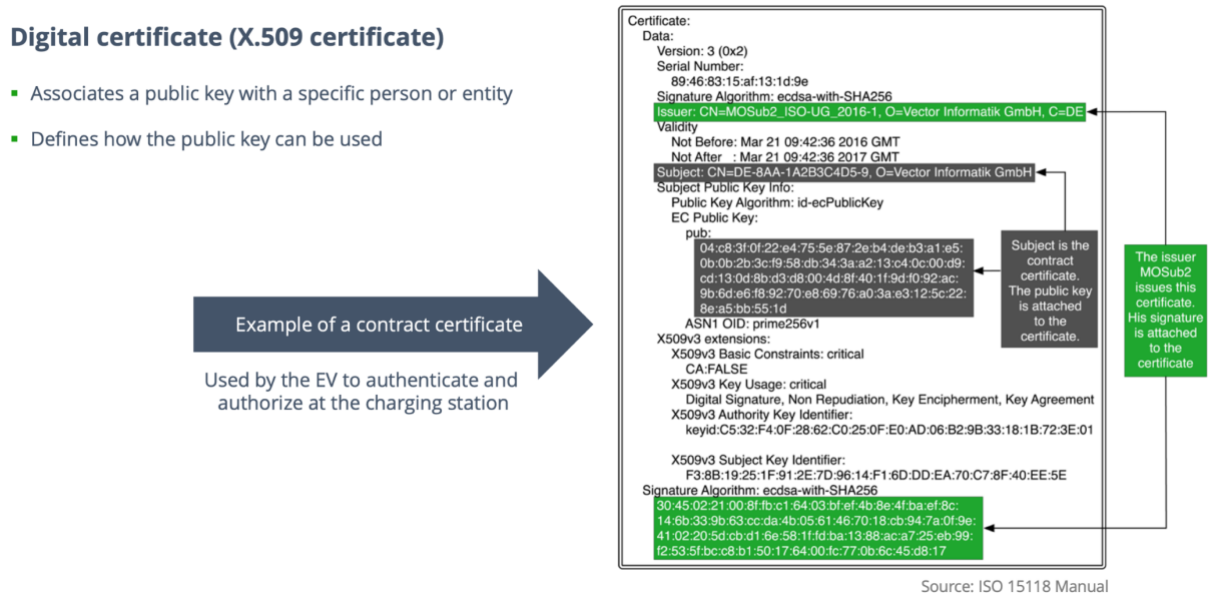

Figure 5: Example of a contract certificate (© V2G Clarity, 2019)

Each contract certificate is linked to a billing account via a unique identifier, also known as the E-Mobility Account Identifier (EMAID). You can see an example of such an EMAID in the 'Subject' field in the image above. Here, the EMAID is 'DE-8AA-1A2B3CD5-9'. The owner of the EV needs to sign up with a mobility operator to create a billing account. Synonyms for the mobility operator (MO) are e-mobility service provider (EMSP) and e-mobility provider (EMP). The MO will then take care of provisioning the contract certificate to the EV through a series of well-orchestrated steps that are outlined in a specification called VDE application guide (VDE-AR-E 2802-100-1).

If the EV does not yet have a valid contract certificate installed, it can do so using its backend telematics services or it can use the certificate installation service provided by the ISO 15118 standard. When conducting the installation of a contract certificate via the charging infrastructure (using ISO 15118), the EV's unique OEM[2] provisioning certificate comes into play. The EV will use this provisioning certificate to authenticate and authorize itself at the charging station for this installation process.

After the EV has presented its contract certificate and MO Sub-CA certificate(s) to the charging station, the charging station and/or CSMS need to conduct a series of checks, such as:

- Verifying the signatures along the chain of MO certificates
- Making sure each certificate is valid regarding its validity period
- Making sure no certificate has been revoked (e.g. due to a compromised private key)
- Verifying that the e-mobility contract associated with the EMAID, which is part of the contract certificate, is still valid (the authorization will be through the MO that issued the contract certificate)

[2] OEM is short for Original Equipment Manufacturer and specifically refers to car manufacturers in the domain of ISO 15118.

If all checks pass, the EV is authorized and can start charging its battery according to the schedule that was agreed upon through the charging station.

Any level of security is only as good as the weakest implementation, meaning: the validity of these digital identities needs to be checked at outlined above before granting access to the charging infrastructure. There are automatic processes in place that make sure a corresponding CA will issue a new certificate once the previous one has expired or been revoked.

For more in-depth information about Plug & Charge, V2G Clarity[3] is a trusted and comprehensive resource on the topic.

Market Support of ISO 15118 Plug & Charge

The image below shows a number of major industry players have either already implemented or are in the process of implementing ISO 15118 and Plug & Charge. This is mainly because ISO 15118 is an internationally agreed-upon industry standard that facilitates interoperability and helps to secure financial investment of each involved market role via future-proof technology.

Figure 6: Selection of companies that support ISO 15118 Plug & Charge (© Hubject, 2019)

[3] If you'd like to venture more deeply into cryptographic mechanisms, PKIs, and the use of certificates for each associated market role, take a look at the available online courses provided by V2G Clarity at https://v2g-clarity.com/courses/.

Conclusion

In this whitepaper, we compared two methods for authorizing an EV for charging: Autocharge and ISO 15118's Plug & Charge. Both enhance the charging experience in terms of security and user friendliness.

Both also offer an option to eliminate RFID cards from use. As of today, RFID cards currently remain the most widespread method of EV charging authorization. The downside of RFID cards is that they are easily replicable and not convenient to the user.

Autocharge is a step into the right direction, as it eliminates the need for external identification tokens like RFID cards or smartphone apps and it enhances the overall level of security. It is far more difficult to spoof a MAC address than to copy an RFID card. Although Autocharge introduces a higher barrier for hackers, it is not a secure method to protect against man-in-the-middle attacks.

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

When a MAC address is not considered to be trustworthy (in cases when it is used in more than one EV or has been spoofed), there is no clear process in place for replacing that MAC address. Autocharge does not define a particular process for how to deal with this situation beyond maintaining blacklists of invalid MAC addresses. Additionally, the authenticity and integrity of a MAC address cannot be protected by digital signatures.

Depending on the use case and the security requirements, Autocharge may be a reasonable solution to allow minimum complexity for an automated authorization. The decision for Autocharge should include a thorough analysis of the required security level and the potential short and long-term business risks and impact. ISO 15118's Plug & Charge is considerably more complex than Autocharge, which also means that it includes higher implementation and operational costs. However, the added complexity of Plug & Charge means that there is a far higher level of data security and protection against fraud and misuse of credentials. It is up to the CPO and site owner to decide which is the enduring solution for their particular use case.

About V2G Clarity

Over the last decade, V2G Clarity has become a recognized e-mobility consultancy after developing the widely-used RISE V2G software and co-authoring the ISO 15118 and related international standards. We work with companies and research institutions across the globe to integrate ISO 15118's promising Plug & Charge feature into their products and innovations.

Our mission has been to help bring convenient, secure, and user-friendly electric vehicle charging to a global audience. We genuinely believe ISO 15118 and Plug & Charge will transform electric vehicle charging. With our online courses, the "ISO 15118 Manual" eBook, and consulting within the industry, we hope to contribute to making this vision a reality.

About Hubject

Hubject simplifies electric vehicle charging. Through its Interoperability platform, called "intercharge", the eMobility specialist connects charge port operators and eMobility service providers, thus providing standardized access to charging infrastructure regardless of network. With over 100,000 connected charging stations and more than 300 B2B partners across 26 countries, intercharge is the world's largest cross-provider of charging networks for electric vehicles. Hubject is also a trusted consulting partner to automakers, charging providers and other EV-related businesses looking to launch eMobility services or implement Plug&Charge using ISO 15118. Thus, Hubject enables eMobility to make a breakthrough worldwide. Founded in 2012, Hubject is a joint venture of the BMW Group, Bosch, Daimler, EnBW, innogy, Siemens and the Volkswagen Group. Hubject's headquarters is located in Berlin, with business units in Los Angeles and Shanghai.

Contribution and Review

Special thanks for contribution and review to Dr.-Ing. Andreas Heinrich (Daimler) and Ronald Heddergott (Carmeq).