irdeto

Whitepaper

A holistic approach to solving EV's toughest ecosystem challenges

INCYDE irdeto utimaco

Table of Contents

EXECUTIVE SUMMARY

The electric vehicle market is experiencing rapid growth due to factors like global warming, the pandemic and geopolitical crises. This has led to substantial investments in Electric Vehicles (EVs) and charging infrastructure. Major car manufacturers are also committing to electrifying their fleets; however, the growth of the EV ecosystem has led to many challenges for drivers, including inconsistent charging experiences and payment methods.

Industry solutions like ISO 15118 and Plug and Charge rely on Public Key Infrastructure (PKI), involving multiple stakeholders and regulatory compliance to ensure security, when addressing these challenges and providing a seamless charging experience. The volume and robustness of PKI are critical considerations especially since Hardware Security Modules (HSMs) are used to secure the private keys.

Managed services like Irdeto's Keys & Credentials and CrossCharge, combined with Utimaco's HSM and Incyde's foundational security experience, offer solutions for seamless charging experiences all the while ensuring compliance with ISO 15118.

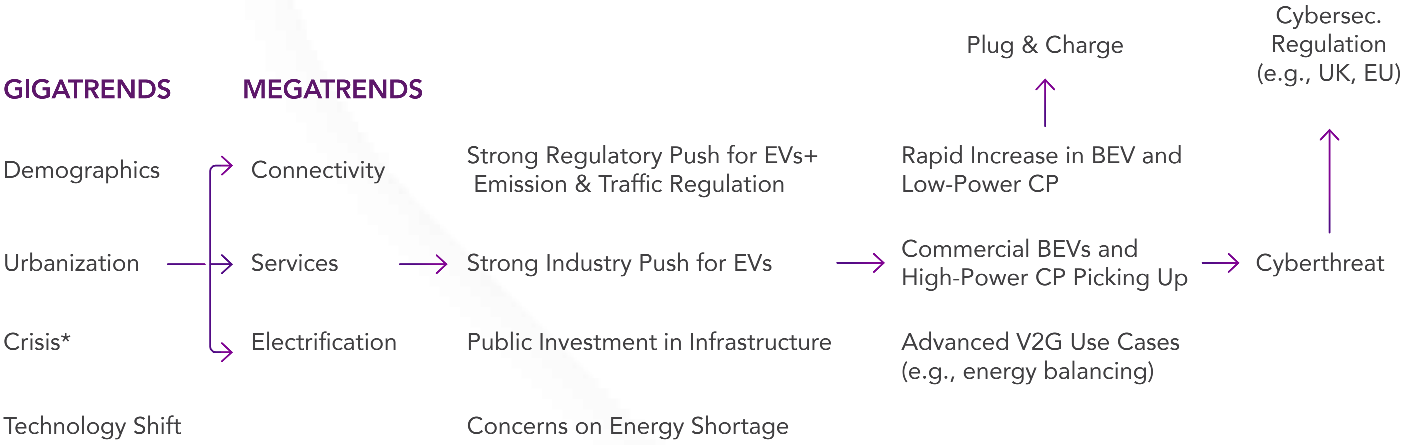
This whitepaper offers a holistic view of EV charging infrastructure, catering for Electric Vehicle Original Equipment Manufacturers (EV OEMs), Electric Vehicle Supply Equipment (EVSE) suppliers, E-Mobility Service Providers (EMSPs) and Charge Point Operators (CPOs). It is specifically designed to provide valuable insights and guidance to these key stakeholders in the electric mobility ecosystem.

Beginning with an introduction that outlines the purpose and objectives of the whitepaper, an exploration of the current state of the electric vehicle market follows, including growth projections and challenges faced by stakeholders. The whitepaper then delves into the specific requirements for developing a robust charging infrastructure, highlighting the importance of collaboration and partnerships among stakeholders.

To conclude, the future trends and innovations in the charging infrastructure space are explored, providing insights and recommendations for stakeholders to navigate this evolving landscape successfully.

1.INTRODUCTION

The EV market is booming. Global warming, pandemic and geopolitical crises have been driving significant public and private investments into EVs and their charging infrastructure. In the United States alone, the federal government is investing $7.5 billion dollars into charging infrastructure along the country's interstate network [1]. Also, most major car manufacturers have made public commitments for either full or significant electrification of their fleets within the next 5 to 10 years.


GIGATRENDS
MEGATRENDS
Demographics
Urbanization
Crisis*
Technology Shift
Connectivity
Services
Electrification
Strong Regulatory Push for EVs+ Emission & Traffic Regulation
Strong Industry Push for EVs
Public Investment in Infrastructure
Concerns on Energy Shortage
Plug & Charge
Rapid Increase in BEV and Low-Power CP
Commercial BEVs and High-Power CP Picking Up
Advanced V2G Use Cases (e.g., energy balancing)
Cybersec. Regulation (e.g., UK, EU)
Cyberthreat

** Climate + Post-Pandemic + Geopolitical/Energy*

Figure 1: Trends in the EV market

21 million BEV will be sold in 2026

General Motors	Mercedes-Benz	Stellantis	Volkswagen
All electric 2030	All electric 2030	70/40% electric EU/NA 2025	Last ICE platform 2026

Figure 2: Battery Electric Vehicles (BEV) to be sold in 2026

With this surge of investment, many market forecasts became obsolete very fast. According to Frost & Sullivan, the share of EVs in Europe will grow to 17% in 2025 and 36% by 2030 [2]; in contrast, the Americas' penetration is expected to grow to 10% and 27% respectively. In reality, these numbers are likely to be much higher though.

The US EV charging infrastructure market is forecasted to rise from about 4 million currently to 35 million in 2030, according to a PwC analysis [3]. McKinsey estimates that the EU will need at least 3.4 million operational public charging points by 2030, even in the most conservative scenario. This means that on average, 6,000 public charging points a week would have to be installed in the European Union as a whole from 2021 to 2030 [4].

2. THE EV ECOSYSTEM AND ITS CHALLENGES

The EV ecosystem consists of seven major stakeholder groups, as illustrated in Figure 3:

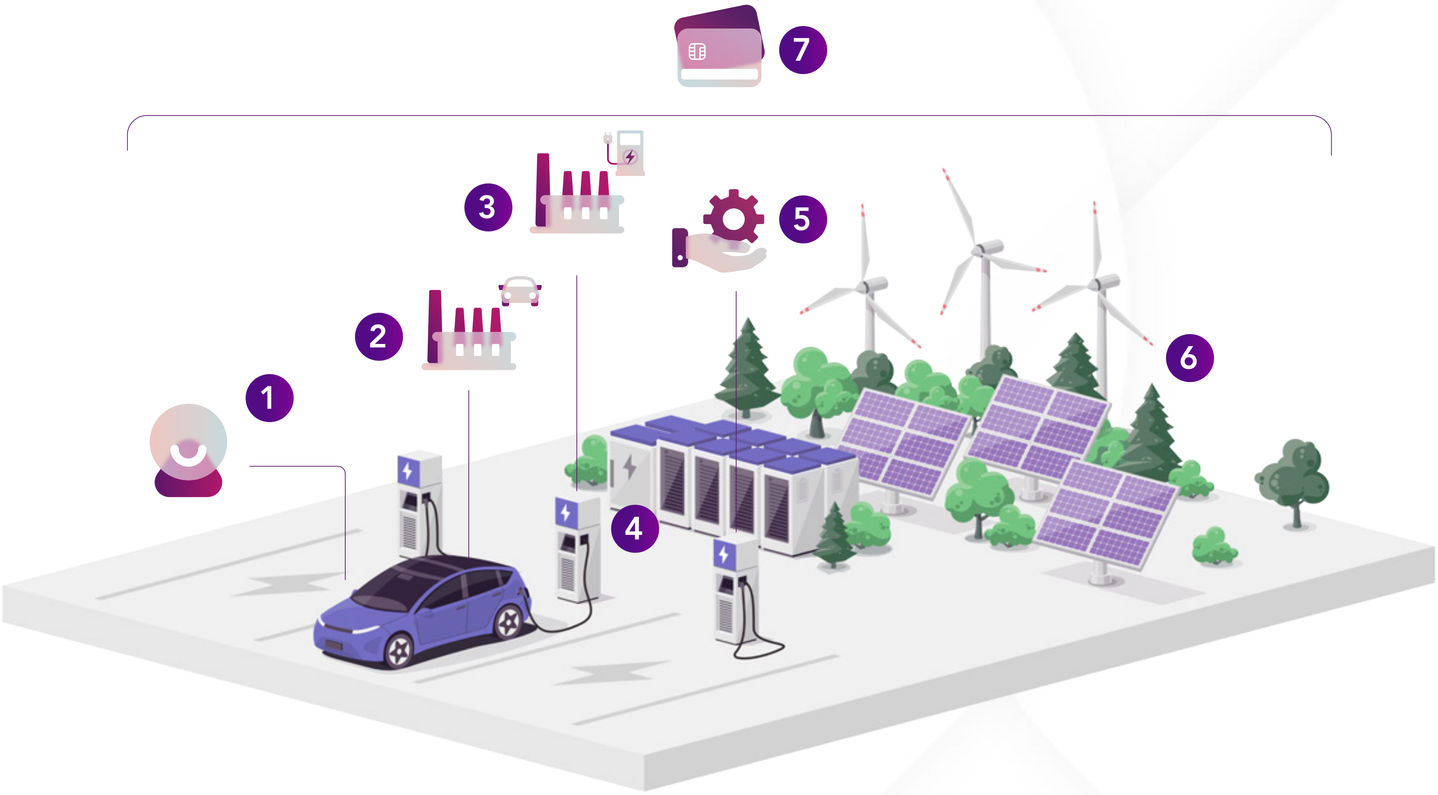


Figure 3: The EV ecosystem

1. Drivers
2. EV manufacturers
3. EVSE manufacturer (charging point manufacturers)
4. Charging point operators
5. Mobility services providers
6. Electricity providers
7. Roaming platforms and payment service providers (to facilitate the interactions between the major stakeholder groups).

The uncoordinated growth of the EV ecosystem has led to its fragmentation and some significant flaws in its initial design. For the driver, the charging experience is far from seamless and from what they are used to with the traditional internal combustion engines – charging point accessibility and compatibility, charging time and payment methods vary between charging point operators and are largely left for the driver to solve.

In some cases, the security and safety of the applied solutions leaves a lot to be desired. As an example of the inefficiency of the EV experience, it took an American citizen seven hours to complete the expected three-hour journey, from New York City to Hartford, Connecticut in 2021, as he needed to reroute to account for charging availability [5].

Similarly, the electricity grid suffers from a lack of seamless integration and compatibility. For consumers, accessing reliable and affordable electricity can be hindered by inconsistencies in grid infrastructure and the limitations of outdated systems. Power outages and voltage fluctuations are prevalent issues, impacting the reliability and quality of electricity supply. Moreover, the grid's vulnerability to cyber-attacks poses a significant threat to its security and resilience. In this context, Public Key Infrastructure (PKI) plays a vital role in the Vehicle-to-Grid (V2G) concept.

3. INDUSTRY SOLUTIONS

To address these industry-wide issues, in recent years there has been a collaborative effort to develop solutions to provide drivers with a seamless, secure and safe charging experience. One of the results is the ISO 15118 Road Vehicles – V2G communication interface standard [6]. Others include less-standardized solutions, such as Autocharge and closed ecosystem solutions, such as Tesla's Supercharger network.

3.1 Plug and Charge

One of the technologies introduced by the ISO 15118 is called Plug and Charge (PnC), which enables drivers to simply plug in and charge their cars at any public charging point without the need to use any traditional payment method, e.g., a credit card. It makes using different charging point operators as easy as using the roaming feature of the mobile network operators.

As for the charging point operators, PnC helps them to improve their top line from roaming users and reduce investment and operational costs related to traditional payment methods (credit card processing fees, credit card terminals). Mobility service operators can benefit too, as PnC makes it easier for them to cover multiple charging point operators and offer better service to their customers.

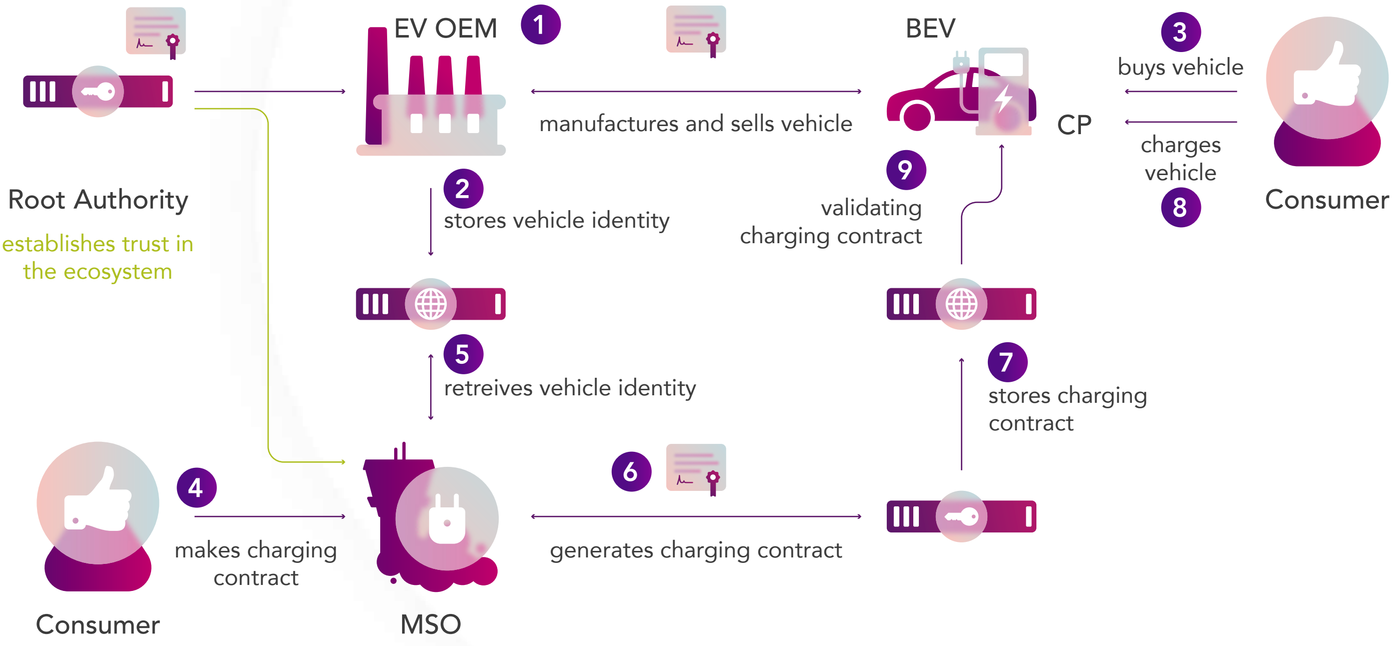


Figure 4: An overview on how PnC works

1. The EV manufacturer assembles a vehicle and issues it with a unique identity, known as the Provisioning Certificate Identifier (PCID). It is transmitted in the form of an X.509 certificate, called the provisioning certificate.
2. The provisioning certificates are then pushed into the Provisioning Certificate Pool (PCP) which is publicly available over the Internet.
3. A vehicle compatible with PnC and equipped with the PCID that has been published in the PCP can be bought by a consumer.
4. A consumer signs a charging contract with a mobility services provider. In the process, they advise the provider on the identity of their vehicle.
5. The mobility services provider retrieves the vehicle identity from the PCP.
6. A charging contract that is bound to that vehicle identity is generated. The contract is transmitted in the form of an X-509 certificate and contains the Electronic Mobility Account Identifier (EMAID) used for identification.
7. The contract is then stored to be used to initiate charging sessions.
8. When the consumer plugs the vehicle into a charging point and the contract is available, the charging starts

3.2 Challenges with PnC

The ISO 15118 requires all the ecosystem participants to embrace the standard ensuring interoperability between them. This imposes certain requirements on the ecosystem and each participant.

3.3 Becoming part of the ecosystem

The process of becoming part of the ecosystem consists of six steps as illustrated in Figure 5.

PLAN	Business case & management commitment Milestones & resources
BUILD	Implement support in the existing systems Acquire new systems, where applicable
V&V	Simulation Real world test
ASSESS	System compatibility test Evaluation of policies and procedures
LAUNCH	Commence production operation
OPERATE	Continue to establish commercial and technical arrangements with other ecosystem participants

Figure 5: The steps to ecosystem integration

The first step is to build a business case for entering the ecosystem and to seek management approval and support. Additionally, concrete milestones need to be defined and the required resources, including external parties, identified.

In the second step, support for the standard needs to be implemented in the existing systems and, potentially, new systems need to be acquired. The latter often involves a proof of concept to ensure interoperability and fit for purpose of the internal systems. At the same time, policies and procedures need to be updated and possibly created in compliance with industry standards and regulations.

In the third step, the internal systems need to be verified and validated. It is a good practice to start verification validation as early as possible, using a simulated environment to reveal incompatibilities. When the simulation results start to look promising, further verification and validation activities in a real-world testing environment are recommended.

Once verification and validation activities are satisfactorily completed, an external audit or assessment may be necessary to complete the entry in the ecosystem. This may include compliance testing of the hardware and software systems as well as an evaluation of the policies and processes.

Finally, the participant can start the operation of the technical systems. Often, further steps are required to establish commercial and technical arrangements with other ecosystem participants to enable growth.

3.4 Requirements for ISO 15118

To improve the security of modern connected vehicles, the UN ECE Regulation mandates that vehicle manufacturers need to establish a Cyber Security Management System (CSMS) for type approval of new vehicles. These requirements can be addressed by applying ISO/SAE 21434 to follow a systematic development and test process. Although this is only required for vehicles, a systematic development and test process should be applied to the entire e-mobility ecosystem.

Establishing separate development and testing environments from productive environments is a critical measure to guarantee dependability, security and adherence to standards of software and hardware products. For products that must comply with international standards (such as ISO 15118), having a dedicated testing environment is especially significant to ensure thorough testing and readiness for deployment in a safe and controlled setting.

It enables the identification of potential issues without compromising the productive environment, minimizing the possibility of safety- and security-related incidents that may impact the end-users. Additionally, this satisfies necessary cybersecurity testing, as specified in the road vehicle cybersecurity standard ISO 21434.

4. PUBLIC KEY INFRASTRUCTURE

The security of ISO 15118 relies on digital certificates which are responsible for the identification of ecosystem participants and the encrypted communication between them. For example, each charge point and charging contract are represented by a unique certificate.

An underlying PKI must exist to generate, validate, renew and revoke the certificates. ISO 15118 specifies a PKI with a single Root Certificate Authority (CA) and five Tier-One Certificate Authorities (T1 CAs), one for each stakeholder group as illustrated in Figure 6.

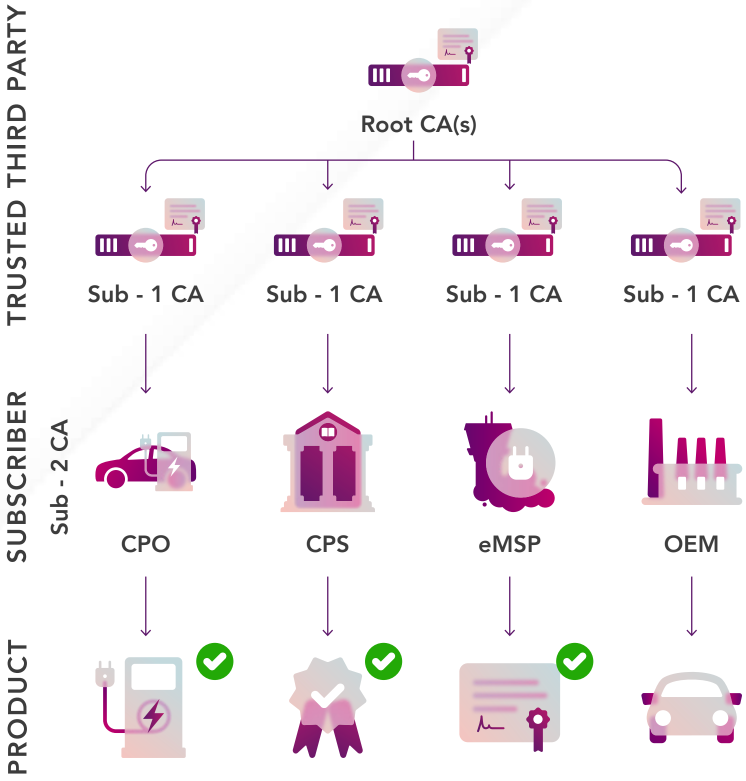


Figure 6: Public Key Infrastructure for ISO 15118

Currently, the Root CA in Europe is owned by CharIN and operated by Irdeto [7]. Each stakeholder who wants to participate in the ecosystem must operate their own CAs, enlist a company to operate them on their behalf or use the CAs offered by CharIN. Furthermore, each stakeholder must meet the requirements set out in CharIN's Certificate Policy (CP) which is verified during the onboarding process and includes a third-party audit and technical assessment of the generated certificates. The onboarding process is operated for CharIN by Irdeto and UL.

It is possible that the EV market will eventually have several ecosystems, each with their own Root CA. Interoperability between the different ecosystems can then be achieved through cross-signing at an appropriate level. For example, the T1 CAs of CharIN could be cross signed by those of an alternative ecosystem.

PKI would provide certain publicly accessible endpoints to ensure that the status of any certificate can be verified at any time. Part of this process would also include a Certificate Revocation List (CRL) service and an Online Certificate Status Protocol (OCSP) responder [8, 9].

4.1 Certificate provisioning and discovery

For the system to work, certificates need to be present in vehicles, charge points and backend systems. A charge point, for example, needs at least the following certificates:

1. A certificate to prove its own identity – in ISO 15118, this is called the Supply Equipment Communications Controller (SECC) Certificate.
2. A certificate proving the identity of the vehicle connected to it, called the OEM Provisioning Certificate.
3. A certificate containing payment information, called the Contract Certificate.
4. A root certificate or certificate to verify the authenticity of the OEM Provisioning Certificate and the Contract Certificate.

Figure 7 illustrates how the SECC Certificate, OEM Provisioning Certificate and the root certificates are used to establish a secure connection between the charge point and the vehicle using the Transport Layer Security (TLS) protocol. TLS implies that the traffic between the two endpoints is encrypted using asymmetric cryptography and can only be decrypted by the receiving entity.

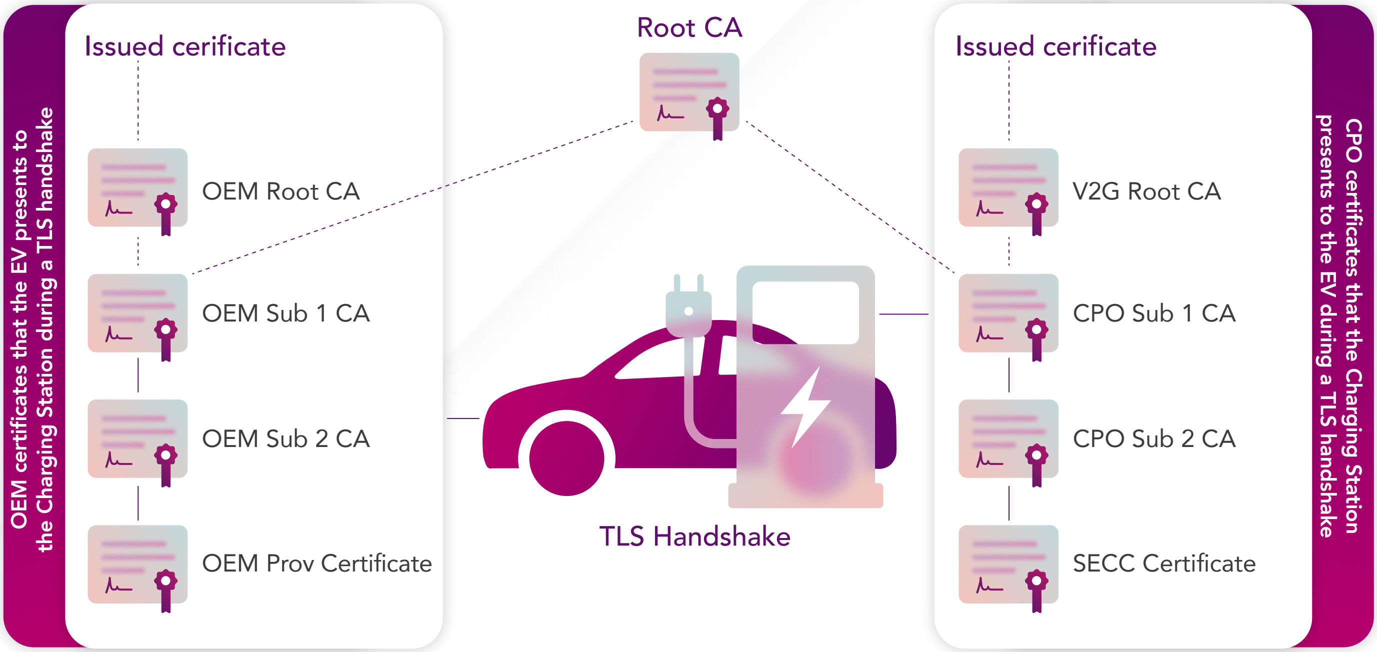

OEM certificates that the EV presents to the Charging Station during a TLS handshake
Issued cerificate
OEM Root CA
OEM Sub 1 CA
OEM Sub 2 CA
OEM Prov Certificate
Root CA
TLS Handshake
Issued cerificate
V2G Root CA
CPO Sub 1 CA
CPO Sub 2 CA
SECC Certificate
CPO certificates that the Charging Station presents to the EV during a TLS handshake

Figure 7: How certificates help establish a secure connection

Both the SECC and root certificates need to be provisioned into the charge point, either at manufacturing time (by the charge point manufacturer) or over the air by the charge point operator. The OEM Provisioning Certificate is provided by the vehicle upon connection with the charge point and the Contract Certificate can either be provided by the vehicle or downloaded from an online Contract Certificate Pool based on the vehicle's identity.

Thus, in addition to generating the certificates, they must be distributed to the correct points of use. The distribution itself is not solved by a standard PKI but requires either a full Key Lifecycle Management System with appropriate integrations, Certificate Pools or another means of delivery.

4.2 Volume

The number of certificates that need to be managed is also an important consideration as the volume can be estimated based on the predicted number of charge points and electric vehicles.

By 2026, the number of EVs globally is expected to reach 18 million [10] and the number of charge points the same, in Europe and North America alone [11]. Assuming one active contract certificate and one identity certificate per vehicle, one identity certificate per charge point and a handful of root certificates, the expected number of active certificates in 2026 is about 150 million, again for Europe and North America. It is expected that the global number of certificates for charging will be one order of magnitude greater.

4.3 Robustness

The charging infrastructure built today is expected to last for the decades to come. In contrast some certificates will be relatively short-lived, with a lifetime from months to several years, others will have a lifetime of several decades.

High volumes combined with long lifecycles, short response times and the criticality of the application pose three additional and critical requirements for the PKI.

- The first one is scalability both in terms of volume and the number of requests served by the public Application Programming Interface (API).
- The second one is business continuity, implying disaster recovery not only for the PKI system and assets, but also the operational processes.
- The third one is compliance with the requirements of the ecosystem and industry best practices, such as WebTrust and ISO 27001 [12].

4.4 Hardware security modules as a root of trust in your PKI environment

Hardware Security Modules (HSMs) are designed to provide a secure physical and logical environment for storing and using private keys. Typically, they include tamper-proof hardware that prevents unauthorized access to the keys, as well as software and firmware that enforce security policies and access controls.

HSMs are essential for PKI as they provide a secure environment for generating, storing and managing private keys, which are a critical component of PKI. Private keys are used to create digital signatures to authenticate users in PKI and as a result, must be kept secure to prevent unauthorized access and potential misuse.

In addition, HSMs enable a secure way to manage the lifecycle of digital certificates, which are used in PKI to establish trust between parties. They ensure that certificate issuance, revocation and renewal processes are performed securely and in compliance with industry standards.

Some of the benefits of UTIMACO HSMs are:

- Providing secure generation, storage and usage of keys inside the tamper protected HSM.
- Generating high-quality true random numbers to ensure the uniqueness of keys.
- Configuring role-based access control and separation of functions.
- Providing two-factor authentication with smart cards.
- Enabling the lifecycle management of digital certificates.
- Ensuring efficient key management and HSM administration, including firmware updates via remote access.
- Providing a software simulator for evaluation and integration testing before deployment into production.

5. MANAGING THE COMPLEXITY OF ISO 15118 TO DELIVER SEAMLESS CHARGING EXPERIENCES

Irdeto's Keys & Credentials and CrossCharge managed services are solutions designed for delivering seamless, ISO 15118-compliant charging experiences. Enabled by the Utimaco HSMs and complemented by professional services from the developers of the standard's underlying concepts at Incyde, the solution meets the needs of all ecosystem participants.

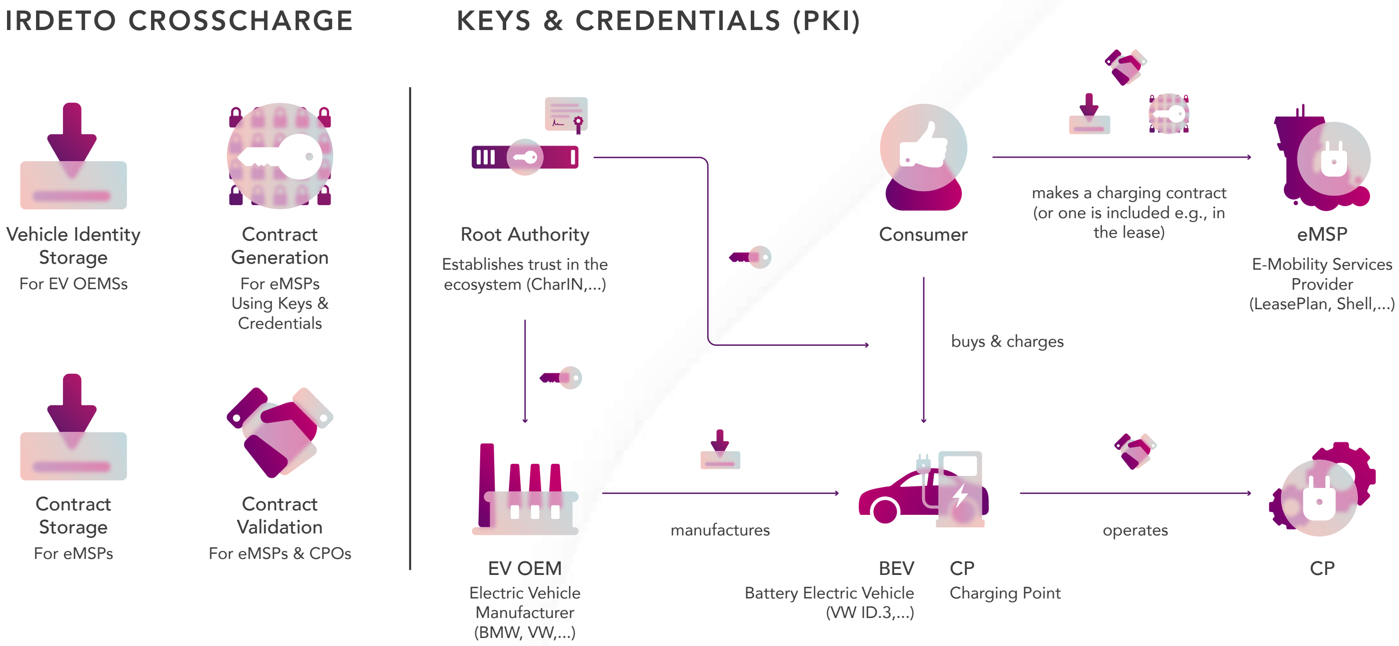

IRDETO CROSSCHARGE
KEYS & CREDENTIALS (PKI)
Vehicle Identity Storage
For EV OEMSs
Contract Generation
For eMSPs Using Keys & Credentials
Contract Storage
For eMSPs
Contract Validation
For eMSPs & CPOs
Root Authority
Establishes trust in the ecosystem (CharIN,...)
Consumer
makes a charging contract (or one is included e.g., in the lease)
eMSP
E-Mobility Services Provider (LeasePlan, Shell,...)
buys & charges
EV OEM
Electric Vehicle Manufacturer (BMW, VW,...)
manufactures
BEV
Battery Electric Vehicle (VW ID.3,...)
CP
Charging Point
operates
CP

Figure 8: Illustration of Irdeto's services

Irdeto Keys & Credentials is a key lifecycle management service, which includes a PKI. Irdeto already operates the PKI for CharIN's European V2G Root. Within the context of CharIN, Irdeto provides the operation of Tier-1 and Tier-2 Sub-CAs as a service and manages the onboarding process with the CharIN or other PKIs. In the US, Irdeto operates its own Root CA with cross-certification arrangements with other roots. Alternatively, Keys and Credentials can be used to establish a completely new Root CA, with possible cross-signing arrangements with other roots.

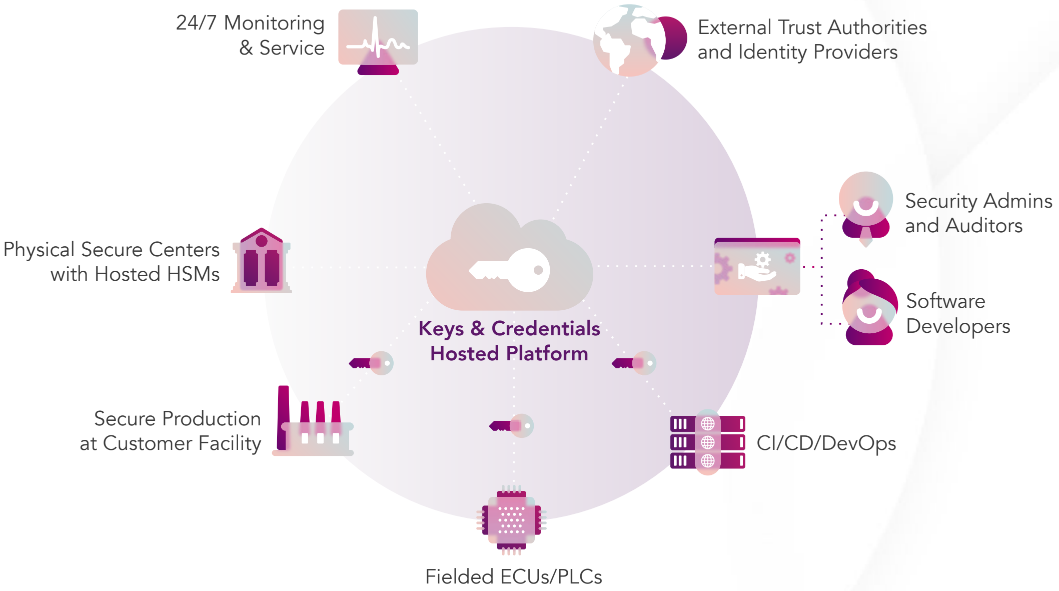
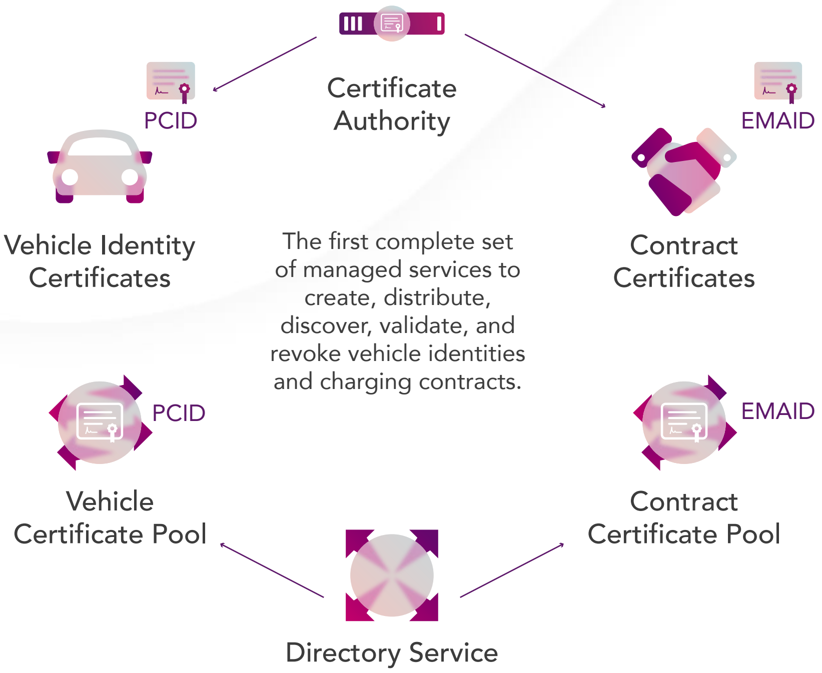

24/7 Monitoring & Service
External Trust Authorities and Identity Providers
Security Admins and Auditors
Software Developers
Physical Secure Centers with Hosted HSMs
Keys & Credentials Hosted Platform
Secure Production at Customer Facility
CI/CD/DevOps
Fielded ECUs/PLCs

Figure 9: Hosted platform of Irdeto's Keys & Credentials

As an additional advantage, Keys & Credentials is not limited to certificates. As a full key lifecycle management service, it can be used to manage all the secure material required by an embedded system, such as an electric vehicle or a charging point. This includes, for example, symmetric keys and JTAG passwords. Keys & Credentials manages the entire lifecycle of the material, from generation and initial provisioning at the factory to renewal and revocation in the field.


Certificate Authority
PCID
Vehicle Identity Certificates
EMAID
Contract Certificates
The first complete set of managed services to create, distribute, discover, validate, and revoke vehicle identities and charging contracts.
PCID
Vehicle Certificate Pool
EMAID
Contract Certificate Pool
Directory Service

Keys & Credentials is complemented by CrossCharge, the first complete set of managed services to create, distribute, validate and revoke vehicle identities and charging contracts. The services are illustrated in Figure 10.

Figure 10: Irdeto's Keys & Credentials, complimented by CrossCharge

6. SUMMARY AND OUTLOOK

The collaboration between Irdeto, Utimaco, and Incyde solutions address the challenges of the EV charging ecosystem by providing seamless and secure charging experiences through ISO 15118-compliant solutions, robust PKI infrastructure and comprehensive key and identity management services. These solutions contribute to the standardization, interoperability and security of the EV charging ecosystem, ultimately enhancing the experience for drivers and supporting the growth of electric mobility.

In the rapidly evolving landscape of EV charging, the future holds promising developments, with ISO 15118 poised to shape the next generation of charging capabilities. As the adoption of EVs continues to soar, the focus will shift towards innovative solutions that enhance charging convenience, grid integration, and overall sustainability.

ISO 15118's forward-looking features, such as bi-directional communication and control, open doors to advancements like V2G technology. This transformative concept enables EVs not only to draw power from the grid but also to contribute surplus energy back to it, empowering vehicles to become integral components of a dynamic energy ecosystem. Moreover, ISO 15118's PnC functionality (which streamlines authentication and payment processes) paves the way for seamless interoperability across charging networks, setting the stage for a future where charging an EV becomes as effortless as plugging in.

6.1 ISO15118 beyond PnC

ISO 15118 also extends its influence beyond V2G and PnC functionalities, offering a broader spectrum of benefits to the EV charging ecosystem. The protocol's comprehensive communication capabilities enable advanced features like smart charging and demand response.

Smart charging leverages ISO 15118's bi-directional communication to optimize charging schedules based on factors such as energy prices, grid conditions and renewable energy availability, ensuring efficient and cost-effective charging.

Additionally, ISO 15118 enables seamless integration with energy management systems, allowing EV charging to be coordinated with renewable energy generation and grid demands. This integration facilitates the integration of EVs as flexible assets within the broader energy ecosystem.

6.2 Post-quantum and EV charging

Post-quantum technology and its implications for EV charging are also becoming increasingly significant. As quantum computers continue to advance, they pose a potential threat to the security of conventional cryptographic algorithms used in various industries, including EV charging infrastructure.

Post-quantum cryptography aims to develop encryption methods that are resistant to attacks from quantum computers, ensuring protection against potential cyber threats. In the context of EV charging, this technology plays a vital role in safeguarding sensitive information such as payment transactions, user authentication and data privacy. This intersection of post-quantum technology and EV charging ensures that the growing electric mobility sector is equipped with advanced security measures to maintain the trust and confidence of both its stakeholders and users.

6.3 Other value-added services for EV charging

The evolution of payments and value-added services for EV charging holds great potential to transform the current landscape. Streamlining payment processes, such as integrating contactless payment methods, mobile wallet options or even automated payment systems, can enhance the user experience and remove barriers to adoption.

Moreover, value-added services like real-time charging station availability, reservation systems, personalized charging plans and rewards programs can incentivize EV drivers and optimize charging infrastructure utilization. These advancements not only simplify the charging experience but also encourage greater usage of EVs by providing added convenience and benefits. By improving payment options and introducing value-added services, the EV charging ecosystem can foster a seamless, user-centric and economically viable environment that propels the transition to electric mobility.

EV charging infrastructure plays a crucial role in advancing sustainability efforts by facilitating the transition away from fossil fuel-dependent transportation systems. EVs offer lower emissions, reduced air pollution and improved energy efficiency compared to traditional internal combustion engine vehicles.

Furthermore, strategically planned and well-distributed charging infrastructure ensures convenient access to charging stations, encouraging more individuals to embrace electric mobility. As the grid becomes increasingly powered by renewable energy sources, such as solar and wind, EV charging can leverage these clean energy options, further reducing carbon emissions and dependence on non-renewable resources.

The development of robust EV charging networks, integrated with smart charging technologies and renewable energy integration, contributes significantly to the overall sustainability of our transportation sector and fosters a greener future.

7. ABOUT US

Irdeto is the world leader in digital platform security offering cyber services and technology solutions that protect platforms, digital assets and software applications across multiple industries. Irdeto's products meet the rapidly changing mobility demands and exceed cybersecurity regulations for automotive, rail and beyond.

Irdeto provides solutions throughout the product lifecycle to prevent cyberattacks and help protect assets for connected cars, charging infrastructure, commercial fleet, rail and construction equipment. With a rich heritage of security innovation and rapid adaptation to the changing demands of the cyber security space, Irdeto is the preferred partner to empower a secure world where people can connect with confidence.

Incyde, specializes in combining their deep branch-specific knowledge with cybersecurity expertise to deliver customized and efficient concepts for businesses.

They have a strong focus on applied cybersecurity, providing comprehensive support in managing industrial cyber defense, ensuring that they respect the unique operating systems and requirements of each of their clients.

Their services cover the entire project process, integrating security-by-design principles and leveraging IT/OT expertise within the operational life cycle. They conduct thorough system maturity analysis, verify IT/OT security concepts, perform risk assessments and KRITIS audits and actively contribute to the development of future security standards.

Additionally, they offer managed Test PKI, enabling the creation of secure and reliable testing environments. By setting robust IT/OT security strategies and actively managing security projects, they emphasize the continuous nature of security and the importance of effective communication and partnerships.

They also possess extensive experience in automotive security and compliance with ISO 15118, ensuring the implementation of stringent security measures for connected vehicles and their communication protocols. As a trusted partner, they offer personalized and comprehensive cybersecurity solutions tailored to your specific needs.

UTIMACO is a global platform provider of trusted cybersecurity and compliance solutions and services with headquarters in Aachen (Germany) and Campbell, CA (USA).

UTIMACO develops on-premises and cloud-based hardware security modules, solutions for key management, data protection and identity management as well as data intelligence solutions for regulated critical infrastructures and Public Warning Systems.

As one of the world's leading manufacturers in key market segments, UTIMACO has over 500 employees around the globe creating innovative solutions and services to protect data, identities and communication networks with responsibility for global customers and citizens. Customers and partners in many different industries value the reliability and long-term investment security of UTIMACO's high-security products and solutions.