Practical Considerations for Implementation and Scaling ISO 15118 into a Secure EV Charging Ecosystem

May 14, 2019

Disclaimer

digicert chargepoint+ eonTi™ Building Trust Transparently

Executive Summary

As Electric Vehicles (EVs) proliferate, EV drivers depend upon a reliable, scalable, and above all, secure charging infrastructure. Offering an exceptional driver experience is paramount to the growth of the EV industry because it lowers the resistance to entry for new users. Enhancing this experience should never compromise privacy or security. To ensure operation of the EV charging equipment, several charging infrastructure suppliers have developed networked Electric Vehicle Supply Equipment (EVSE), which communicates with a cloud-based service for management and operation. EV drivers may choose to join a particular network or access the EVSE anonymously as allowed by the policies of the network operators and the owners of the EVSE. Furthermore, some networks have roaming arrangements in place which allow EV drivers with an account on one network to charge on EVSE on another network. As this industry continues to evolve and innovate at a rapid pace, it is essential that a robust identity management system accommodate the growing needs of the EV charging industry.

Security and trust are essential for communication between EVs and the EVSE. In particular, secure EV-to-EVSE communication is a core competency and vital objective of the EV charging ecosystem. Paramount to this objective is the availability of a trust infrastructure, such as a Public Key Infrastructure (PKI), to authenticate the participants in a charging session as well as establish and maintain secure communications between the EV and the EVSE.

This paper provides a review of the International Organization for Standardization (ISO) 15118-2 standard (Road vehicles — Vehicle-to-Grid Communication Interface — Part 2: Network and application protocol requirements) [1], which specifies the communication requirements between the EV and the EVSE, and more precisely, the EV Communication Controller (EVCC) and the SE Communication Controller (SECC) (see Figure 1).

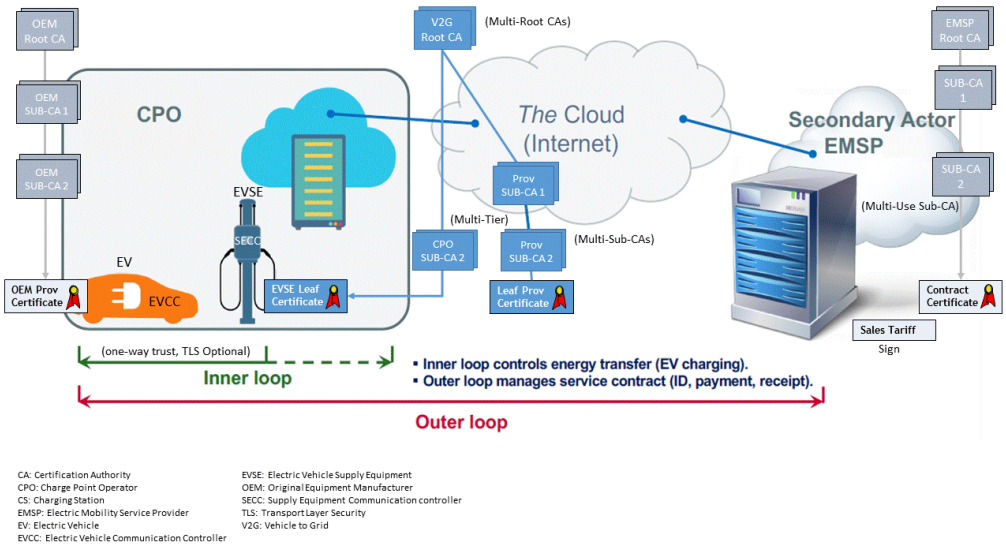
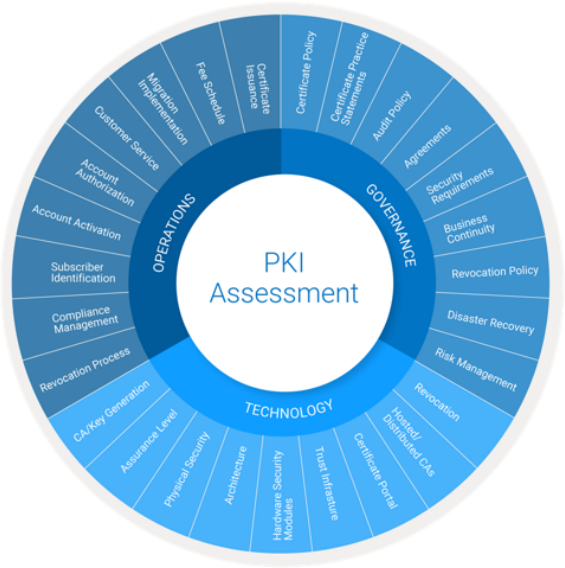


Figure 1: ISO 15118 PKI – Inner and Outer Loops

The paper also reviews the ISO 15118 PKI requirements for leaf Certificates (controlled within the inner loop of the PKI and issued under the vehicle-to-grid (V2G) Root CA), the OEM provisioned Certificates to authenticate the EV, and the contract Certificates from the EMSP for payment. Both sets of Certificates could be issued from the V2G Root CA but will likely be issued from an OEM Root and EMSP Root CA provider as shown in Figure 1. Although the current standard (First edition, 2014-04-01) may be workable for limited trial implementations, substantive gaps in the ISO 15118 PKI requirements require development in order for the PKI to scale to production levels (multi-root, multi-tier, and multi-Sub-CA).

The Assessment Overview

Eonti Inc. (Eonti), a leader in PKI implementations for critical infrastructures, and its partner, DigiCert, Inc. (DigiCert), the world's leading provider of TLS/SSL, IoT and PKI solutions, in collaboration with ChargePoint, Inc. (ChargePoint), performed a 360º PKI maturity assessment on the ISO 15118 PKI requirements. This in-depth assessment identified areas for improvement in the PKI requirements in order to provide reliable authentication between the EV and the EVSE and to maintain the integrity of contracts between the EV and the EMSP. The assessment's criteria, analysis, and processes were based on the Internet Engineering Task Force (IETF) guidelines, the National Institute of Standards and Technology (NIST) standards, and PKI best practices. The team evaluated the governance, technology, and day-to-day operations of the ISO 15118 PKI requirements and analyzed 21 specific categories of its proposed implementation (current state) taking into account the ecosystem's threat environment and risk posture.



Findings and Recommendations

Within each major assessment area (governance, technology, operations), the team identified shortfalls of underdeveloped or ad hoc policies and requirements. Subcategories under each major area were given a ranking, whose average was used to derive the assessment score (described later in this report). The key findings and recommendations are listed in

Table 1.

The recommendations provide a starting point to augment current requirements and should be addressed in a planned, predictable, and timely manner. When properly addressed, the results of the assessment provide a basic roadmap to help ISO 15118 meet its expanding need for Certificate based authentication and secure communications between the EV and the EVSE. The end target should be to improve the security strength and scalability of the ISO 15118 PKI.

Overall, with an average score of 1.3 out of 5 over the three major categories, the ISO 15118 PKI policies and requirements fail to adequately address necessary aspects of a functional, scalable, multi-root PKI. These shortfalls increase vulnerabilities and decrease interoperability at all levels. Although there have been claims of ISO 15118 PKI implementations that establish a standardized method for secure EV charging, for example, using terms such as "Plug and Charge Standard",

the issues identified in this paper raise enough concern for reviewers to question whether the current ISO 15118 standard can be the basis for a secure, scalable, and interoperable PKI.

Stakeholders would benefit by establishing a coalition with a diverse set of skills and experiences to address the recommendations, provide overall governance, and develop a standards-based solution that is not only secure, scalable, and interoperable, but also reduces implementation complexity and integration costs of the PKI within the EV charging ecosystem.

Table 1: Overall Assessment Key Findings

Assessment Area	Findings	Recommendations	Impacts
Governance **Score:** **1.4 out of 5**	• Insufficient requirements to determine a baseline level of trust for the PKI • Incomplete Certificate profiles due to vagueness; can lead to incompatible Certificates • Lack of Certificate revocation and key management processes creates vulnerability in the system	• Develop a baseline set of Certificate policies for all V2G root hierarchies • Require all CAs to complete a Certification Practice Statement • Complete the Certificate profiles • Develop the Certificate Revocation Policy and Key Management Policy	• Common level of trust across all root hierarchies within the ecosystem • Interoperable Certificates across the ecosystem • Improved integrity of Certificates and Private Keys
Technical **Score:** **1.6 out of 5**	• A mixed tier PKI system (i.e., 2 and 3-tier) • Lack of key management requirements exposes key usage vulnerabilities	• Analyze the challenges of a mixed tier PKI before production implementation • Create a common set of key management requirements across the ecosystem	• A simplified 2-tier PKI can save cost and complexity across the ecosystem. However, if needed, a 3-tiered system provides additional flexibility in assurance levels and geographical separations
Operations **Score:** **1.0 out of 5**	• Lack of requirements for identity proofing of Certificate requestors (i.e., subscribers) • Lack of access management controls applied to authorized subscribers for requesting Certificates • Lack of Certificate lifecycle management requirements • Lack of requirements for Certificate revocation • Lack of trusted time source at the EV nullifies Certificate • Unrealistic expectations of EV owners to update Certificates	• Develop baseline set of subscriber onboarding requirements to ensure only authorized subscribers obtain Certificates • Develop Certificate lifecycle management requirements for Certificate issuance, renewal, expiration, revocation • Develop Certificate revocation baseline requirements • Develop mechanism to support a trusted time source • Improve Certificate provisioning into the EV	• Increased assurance level of the PKI • Increased ease of use of EV Certificate provisioning

Table of Contents

Executive summary I
THE ASSESSMENT OVERVIEW II
FINDINGS AND RECOMMENDATIONS II
References, definitions, and abbreviations 1
REFERENCES 1
DEFINITIONS 1
ABBREVIATIONS 2
Introduction 4
PKI assessment 4
ASSESSMENT METHODOLOGY 4
GOVERNANCE ASSESSMENT 7
KEY FINDINGS AND GAP ANALYSIS 7
TECHNOLOGY ASSESSMENT 9
OPERATIONS ASSESSMENT 12
REVIEW OF SIMILAR SECURITY MODELS FOR CRITICAL INFRASTRUCTURE 14
Conclusion and next steps 15
ABOUT EONTI 16
ABOUT DIGICERT 16
ABOUT CHARGEPOINT 16

Figures

Figure 1: ISO 15118 PKI – Inner and Outer Loops i
Figure 2: 360-degree PKI Assessment Model 5
Figure 3: Components and Elements 6

Tables

Table 1: Overall Assessment Key Findings iii
Table 2: Ranking Definitions 6

References, Definitions, and Abbreviations

References

Ref #	Reference Title
[1]	ISO 15118-2 standard (Road vehicles — Vehicle-to-Grid Communication Interface — Part 2: Network and application protocol requirements) (April 2014)
[2]	CA/Browser Forum, Version 1.6.2 (December 10, 2018), cabforum.org

Definitions

Term	Description
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and procedures, and to recommend necessary changes in controls or procedures.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's Authorization to receive specific categories of information.
Authorization	The process of giving individuals access to specific areas or systems based on their Authentication.
Certificate	A Certificate (or digital Certificate) is an encapsulation of a Public Key used to communicate purpose and prove ownership and validity. A Certificate is signed by a trusted Certification Authority (CA) to convey trust of the contents of the Certificate.
Certificate Policy (CP)	A set of requirements that address all aspects associated with the generation, distribution, accounting, compromise, and administration of digital Certificates.
Certificate Revocation List (CRL)	A list of revoked Certificates that is signed by an authorized CA (e.g., CRL Issuer). Relying Parties can lookup Certificate serial numbers in the CRL to determine if they have been revoked.
Certification Authority (CA)	An authority trusted by one or more users to create and assign Public Key Certificates. Optionally, the CA may create the subjects' keys.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing Certificates and providing access to them, in accordance with the CP governing the CA.
Hardware Security Module (HSM)	A physical computing device that safeguards and manages digital keys for strong Authentication and provides crypto processing.
Online Certificate Status Protocol (OCSP)	OCSP enables applications to determine the (revocation) state of identified Certificates in lieu of, or as a supplement to, checking against a periodic CRL. OCSP may be used to satisfy some of the operational requirements of providing more timely revocation information than is possible with CRLs and may also be used to obtain additional status information.

Private Key	In a Public Key cryptosystem, that key of an entity's Key Pair which is known only by that entity.
Public Key	A cryptographic key that is associated with a specific Private Key and may be made public. A given Public Key may be used by many entitites to support encryption and Digital Signature validation with asymmetric cryptographic algorithms.
Public Key Infrastructure (PKI)	A framework that is established to issue, maintain and revoke Public Key Certificates.
Relying Party	Any entity that trusts the data in a Certificate in making decisions.
Root CA	The Root CA is the highest level CA within a given hierarchy. A Root CA's Public Key Certificate will be self-signed.
Subordinate CA (Sub-CA)	All CAs under the Root CA.
Validity Period	The period starting with the date and time a Certificate is issued and ending with the date and time on which the Certificate expires or is revoked.

Abbreviations

Term	Description
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DNSSEC	DNS Security Extensions
ECC	Elliptic Curve Cryptography
EV	Electric Vehicle
EVCC	Electric Vehicle Communication Controller
EVSE	Electric Vehicle Supply Equipment
HSM	Hardware Security Modules
ICAO	International Civil Aviation Organization
ICT	Information Communication and Technology
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology

OCSP	Online Certificate Status Protocol
PKD	Public Key Directory
PKI	Public Key Infrastructure
SA	Secondary Actor (e.g. EMSP, Utility, Clearinghouse)
SECC	Supply Equipment Communication Controller
Sub-CA	Subordinate Certification Authority

Introduction

The ISO 15118-2 specification creates the requirements for the network and application protocol layers of the V2G communication interface between the EV, the EVSE, and one or more Secondary Actors (SAs). The ISO 15118 PKI that provides the authentication Certificates is anchored by the V2G Root CA. V2G herein refers to the concept set forth in the ISO 15118 proposed PKI to create a trusted communication channel between EVs, EVSEs, and SAs. This document presents the key findings of an assessment of the ISO 15118 proposed V2G PKI for EV charging systems.

PKI Assessment

The focus of this assessment is on the ISO 15118 PKI requirements as they relate to a PKI's governance, technical, and operations points of view and includes:

- A presentation of the key findings of the assessment of the ISO 15118 proposed PKI for EV charging ecosystem (EVs, Charging Stations, Charging Station Operators, E-Mobility Service Providers, etc.)
- Results of the review of the ISO 15118 PKI as it relates to similar security models found within critical infrastructures
- Recommendations to advance the standard to successfully be able to operate a large-scale, standard, global PKI to serve the EV charging ecosystem
- Identification of best practices and best of breed technical solutions for deployment of a large-scale EV charging ecosystem

Assessment Methodology

The DigiCert and Eonti team reviewed the PKI requirements defined in ISO 15118 using their 360-degree PKI assessment methodology (see Figure 2). The assessment employed a comprehensive, multi-step approach working with PKI experts and stakeholders to review the published ISO 15118 PKI requirements (the governance), the PKI's architecture (the technology components), and how the standard would be deployed in the real world (the operations of the PKI). The assessment also identified the PKI priorities and goals of the ecosystem and tailored the methodology to include suggested clarifications and/or enhancements to meet the objectives of the PKI. The structure of the PKI assessment:

- Covered three areas of focus: Governance, Technology, Operations
- Divided each focus area into subcategories for an in-depth view of the PKI
- Made observations between the ISO 15118 PKI requirements and industry best practices
- Communicated key findings and identified recommended mitigating controls

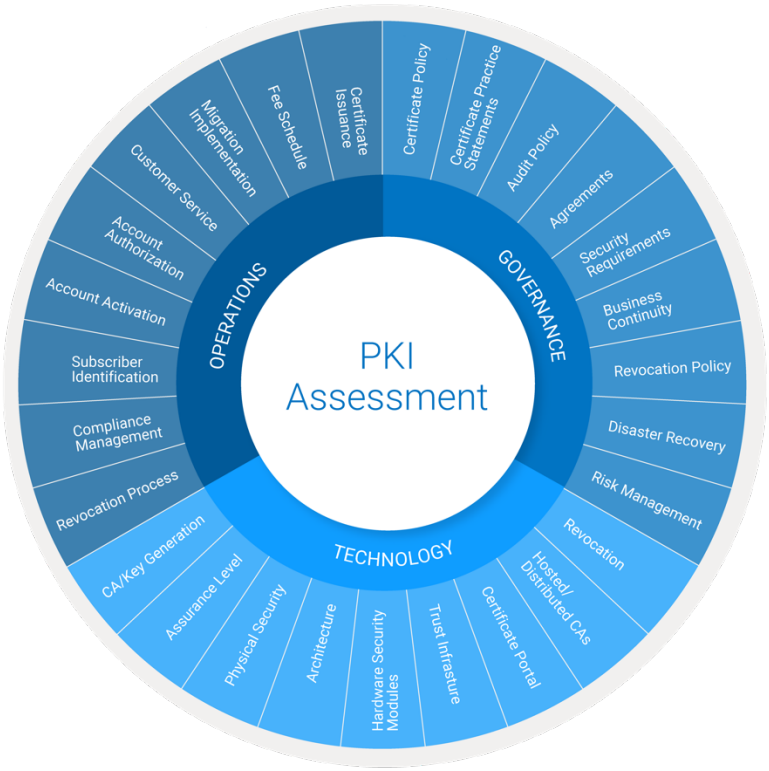


Figure 2: 360-degree PKI Assessment Model

Within each major focus area, several subcategories were evaluated to determine the PKI's current state observations and measured it against PKI best practices to identify key findings and recommendations (see Figure 3). For this assessment, the team arrived at current state observations by a review of the industry's PKI strategies, requirements, and policies put in place by the EV community via the ISO 15118 standard.

The subcategories where further subdivided into their components, which were also further reduced into their basic elements. This detailed examination of a PKI allows the team to provide a comprehensive review of the PKI, identify any missing requirements, and determine the effectiveness of each subcategory.

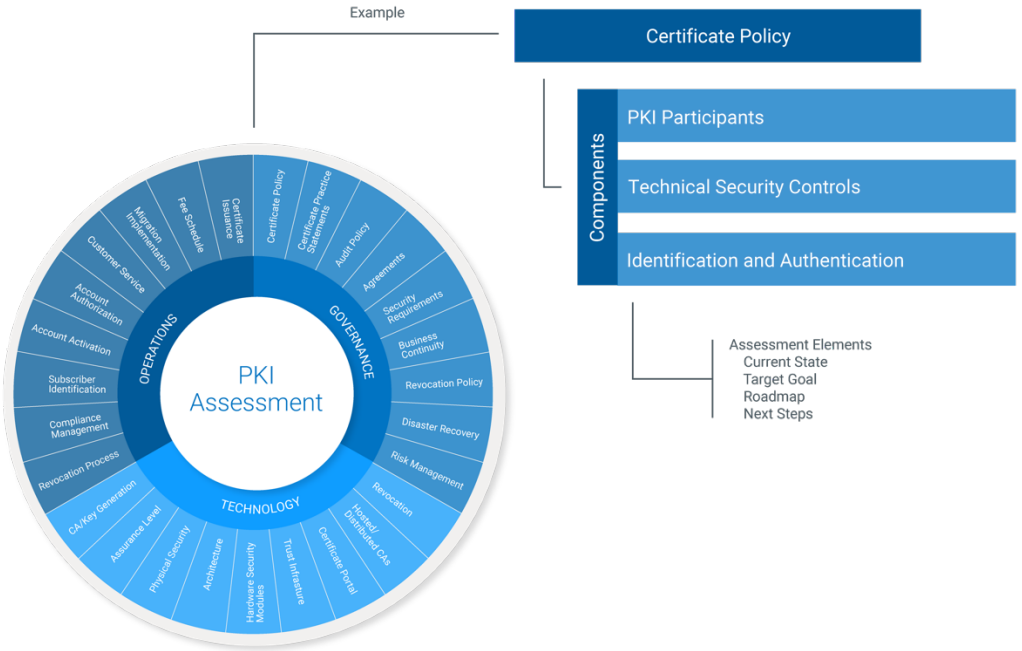


Figure 3: Components and Elements

The current state evaluation of each subcategory is mapped to rankings ranging from "Undeveloped" to "Specialized" as shown in

Table 2. These rankings were based on the documentation review by security experts and stakeholders in order to succinctly summarize the assessment results and to quickly identify strengths and weaknesses within the PKI requirements. The values assigned to the rankings ranged from 1 for Undeveloped to 5 for Specialized.

Table 2: Ranking Definitions

UNDEVELOPED	AD HOC	ESTABLISHED	OPTIMIZED	SPECIALIZED
▪No capability exists ▪No automation or systems (highly manual) ▪No defined roles	▪Basic capability ▪Ad Hoc / Informal manual processes ▪Some roles defined ▪Basic integration between organizations / stakeholders (e.g., enterprise, business unit, suppliers, partners) ▪Manual analytics	▪Defined capabilities ▪Formal processes ▪Defined roles & responsibilities ▪Regular integration between organizations / stakeholders ▪Some centralized repositories ▪Inconsistent adoption of systems	▪Advanced capabilities ▪Formal and dynamic processes ▪Specialization of roles and skills ▪Consistent adoption / integration of systems ▪Close integration between organizations / stakeholders ▪Some advanced analytics	▪Market leading capabilities ▪Highly adaptive processes ▪Advanced skill sets ▪Highly integrated systems ▪High automation ▪Advanced and predictive analytics

The collective research and analysis covered all three major focus areas and helped to evaluate how the ISO 15118 PKI requirements would be implemented. The current state of the PKI was mapped against best practices.

Assessment components with current states identified as “Undeveloped” or “Ad Hoc” should be looked at as items to address in the near term to reach a target goal of Established. Components with current states identified as “Established” should be considered as following best practices. Components marked as “Optimized” meet requirements for solutions that automate PKI functions, management, and renewal processes to ultimately achieve a “Specialized” state for its PKI.

This document results in a comprehensive look at the ISO 15118 PKI requirements detailing a 360-degree view with predicted needs, existing capabilities, gaps, and a set of next steps.

Governance Assessment

PKI governance is a complex concept and is often associated with principles such as transparency, participation, and accountability. A PKI will not function effectively without appropriate governance. Without policies that clearly define roles and responsibilities, PKI participants will not be able to recognize when a compromise occurs and when to revoke a Certificate, or worse, they will not able to determine if Certificates are valid. In the context of the PKI, the achievement of good governance is a critical foundation for achieving the required level of trust. The governance assessment employed by the DigiCert/Eonti team reviewed the following subcategories:

- The CP and CPS to govern the PKI
- Audit policy and requirements for the crucial components of the PKI
- Security policies which describe personnel, physical, telecommunications, logical, and cryptographic key management security requirements
- Revocation policy which describes the PKI Certificate revocation and status checking requirements
- Ancillary agreements such as a supplier agreement and Root CA hosting agreement
- Business continuity and disaster recovery plan which provides recovery method procedures
- Risk management processes to protect components of the PKI

Key Findings and Gap Analysis

In terms of governance, the Algorithms and Protocols defined by the standard approach a ranking of “Established,” all other governance elements however, such as Certificate Policy documentation, Audit Policies, and Certificate Revocation Policies failed to meet the criteria of an established approach. This is concerning because PKI implementations conceived without appropriate governance, especially underdeveloped or ad hoc PKI implementations, rarely fulfill their security objectives. In our experience, proper PKI governance with well thought out security requirements that have been properly vetted are a prerequisite to a successful implementation.

The following table provides a high-level view of the governance assessment results.

Governance Assessment Key Findings (Current State Observations)

Governance	Current State	Undeveloped	Ad Hoc	Established	Optimized	Specialized
Certificate Policy (CP)						
A CP document describes a set of rules, policies, and procedures by which a PKI is governed for a given community (e.g., EV charging ecosystem). The CP provides a central document where users of the Certificates (e.g., the Relying Party) can determine the level of assurance (i.e., trust) to place in the integrity and use of the Certificate. While there are some PKI requirements stated in ISO 15118, there is not a sufficient set of requirements to determine the level of trust of the PKI due to lack of: • Existing CP to govern Root CA issuance under ISO 15118 PKI compliance • Identity proofing of participants (e.g., Root CAs, Sub-CAs, end-entities, etc.) • Cross-certification requirements to determine how Root CAs will trust each other • Requirements for issuance and revocation of Certificates • Audit requirements for the PKI components • In a multi-root system, such as the one proposed by ISO 15118, it is essential to have a common set of rules, protocols, and technologies to serve as a starting point for roots participating in the ecosystem as seen in the approach the CA/Browser Forum takes in their Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [2].			●			
Certification Practice Statement (CPS)						
The CPS, is generated by the operators of CAs (e.g., Root CAs, Sub-CAs) within the PKI and describes how the CAs are operated in compliance with the PKI's CP. Currently, there is no CPS template defined to govern operations of CAs under ISO 15118 compliance. Creation of the CPS template requires completion of the ISO 15118 PKI CP.		●				
Audit Policy						
Currently there are no formal PKI Audit policies for the ISO 15118 PKI. Unless the PKI is deployed and operated in accordance with the PKI's CP, and is shown to remain compliant through periodic audits, the security intended to be provided by the PKI will not be realized and Relying Parties will not have enough information to determine the level of trust in the PKI.		●				

Algorithms and Protocols					
The algorithm and protocol requirements of the ISO 15118 PKI are very specific, e.g.,: • SHA 256 for the Hash Algorithm • ECDSA for the Signature Algorithm • User Datagram Protocol A best practice approach would be to provide flexibility via a range (e.g., SHA 2 to SHA 3, or equal to or greater than SHA 256) instead of limiting to specific algorithms and protocols.		●			
Business Continuity and Disaster Recovery					
There are no requirements specified in ISO 15118 for how CA operators should handle disruption to their Certificate issuance, Certificate revocation, or Certificate status processes.	●				
Certificate Revocation Policy					
There are only a few (3) Certificate revocation requirements in ISO 15118. Additionally, all the Certificate profiles list the CRLDistributionPoints and the Authority Information Access (for OCSP) as optional. Certificate revocation should be a mandatory and well defined process to maintain the assurance level and integrity of ISO 15518 PKI issued Certificates.		●			
Risk Management					
There are no requirements specified in ISO 15118 for how CA operators should handle risk management processes. There are no: • PKI asset management and risk management controls • CA Certificate rollover requirements • Metrics defined to measure risk management performance A best practice approach would be to outline a baseline set of requirements for risk management across all CAs within the ecosystem.	●				

Technology Assessment

PKI technology includes the CA hardware and software, physical security components, the revocation architecture, and personnel administering the PKI's issuance and management of digital Certificates. In addition, a key challenge in deploying a PKI is the technology is deeply intertwined with governance. The PKI technical model assures that the rules set forth in the governance policies can be enforced by technical means. In addition to the requirements set by the Certificate policies, the technology must incorporate basic, modern concepts such as security-by-design and privacy-by-design, especially in the age of the General Data Protection Regulation (GDPR)[1].

[1] https://eugdpr.org/

The PKI technology assessment includes review of:

- The CA hierarchy and architecture components
- The assurance level associated with the PKI
- Physical security protection of PKI components
- Disaster Recovery
- Key Management
- Protocols and Algorithms
- Certificate Revocation architecture

Regarding technology, the CA Hierarchy and Architecture, as well as the implementation of the Algorithms and Protocols approach a ranking of "Established." However, all other factors failed to meet the criteria of an established approach according to the assessment. The implications of these findings are broad and carry the potential to impact production implementations throughout the ecosystem, which will depend on PKI provider selection of robust and compatible PKI technology. Understanding the risks of incompatible and inadequate technology due to vague or underdeveloped requirements is something the ecosystem cannot ignore.

The following table provides a high-level view of the technology assessment.

Technology Assessment Key Findings (Current State Observations)

Technology	Current State	Undeveloped	Ad Hoc	Established	Optimized	Specialized
CA Hierarchy & Architecture						
ISO 15118 PKI requirements allow for mixed tier (2 or 3 tier) PKI implementations. However, the standard does not explain the reason for a 3 tiered system. Typically in a 3 tiered system, the first Sub-CA (Sub-CA1) is used as a policy CA to separate a mixture of assurance levels and / or geographical regions using the next tier Sub-CA (Sub-CA2). However, the 3 tiered system comes at a cost of additional hardware (e.g., HSMs, CAs, etc.), additional management (e.g., more CAs and more CPSs), additional Certificate storage required at the EVCC, and additional processing time of the Certificate chain validation. An analysis of the reasoning for using a 2 tier or a 3 tier PKI is needed to determine if a 2 tier or a 3 tier system is the best model or if a mixed (2 and 3 tier) system is needed.			●			
Assurance Level						
There are no requirements for the level of assurance (trust) that the CAs are trying to achieve. Relying Parties should know the extent to which a Certificate may be trusted to actually represent that the entity named in the Certificate is the same entity engaging in the transaction. Level of assurances relies on the trustworthiness of the identity proofing process and the credential management function.		●				

Physical Security					
Physical security requirements are needed that apply equally to all Root CAs and Sub-CAs within the ecosystem, including any remote access used to administer the CAs, so that: • CA equipment is protected from unauthorized access while the cryptographic module is installed and activated • Access controls reduce the risk of equipment tampering even when the cryptographic module is not installed and activated • CA cryptographic modules are protected against theft, loss, and unauthorized use	●				
Disaster Recovery Infrastructure					
Not recovering quickly from a CA failure (e.g., due to key compromise or unusable CA cryptographic material) prevents the CA from signing the next scheduled CRL or OCSP updates, thus preventing Relying Parties from checking the Certificate status of Certificates issued by the CA. A disaster recovery analysis is needed for ISO 15118, based on the CA architecture and CA Certificate Validity Periods, to determine how to minimize the impact of a CA failure on Certificate validation throughout the ecosystem.	●				
Key Management					
Key management requirements are needed to provide ISO 15118 PKI implementers with the common set of requirements for: • Key lifecycle management (generation, distribution, destruction) • Flexibility of key ranges, e.g., ECC 256 or 384 bit keys • Secure storage of keys • Key backup and recovery • Key compromise		●			
Protocols and Algorithms					
The ISO 15118 PKI requirements are algorithm specific, such as: • Hash Algorithm: SHA 256, Signature Algorithm: ECDSA • Protocol: TLS A best practice approach is to provide a range in selection of protocols and algorithms for flexibility. For example, hash algorithm SHA 256 or higher, TLS 1.2 or 1.3, etc.			●		
Certificate Revocation Infrastructure					
Certificate revocation appears to be optional in ISO 15118. Therefore, there are no requirements specified for: • CRL and/or OCSP infrastructures • CRL and OCSP Certificate profile • Secure time source required by the Relying Party validating the Certificate • Certificate revocation process	●				

Operations Assessment

PKI operations (i.e., Certificate management) are a crucial part of a PKI implementation and represents the bulk of the effort in continually maintaining the assurance level and integrity of the PKI. Effective Certificate management is a combination of well-defined policies and the right tools and automation to implement them. Operations best practices for Certificate management help simplify and streamline PKI implementations, enabling relying parties to trust in the infrastructure and its compliant devices, applications, and services.

The operations assessment includes review of:

- PKI account Authorization approval process
- Certificate requests and issuance process
- Customer service participants
- Certificate tracking and renewal process
- Management of the revocation process
- CA Certificate rollover migration implementation

One of the most overlooked areas of maintaining a successful PKI implementation is the operations and day-to-day management of certificate lifecycle, key generation and delivery, certificate revocation, etc. Lack of consistent PKI management requirements across the ecosystem can lead to serious downtime and loss of revenue for stakeholders. Regarding the operations requirements of the Standard, all factors failed to meet the criteria of an established approach. The following table provides a high-level view of the operations assessment results.

Operations Assessment Key Findings (Current State Observations)

Operations	Current State	Undeveloped	Ad Hoc	Established	Optimized	Specialized
Identity and Access Management						
There are no requirements for identity proofing of Certificate requestors (i.e., subscribers) or access management controls applied to authorized subscribers for requesting Certificates.		●				
Certificate Lifecycle Management						
Certificate lifecycle management requirements are needed in ISO 15118 for: • Certificate issuance • Monitoring and tracking • Renewal, Expiration, and Revocation Additionally, Certificate expiration is not supported at the EV due to lack of a trusted time source. Also, expecting vehicle owners to update Root Certificates in their EVs is unrealistic and would require the EV automaker to provide a Certificate installation process easy enough for EV owners to use.		●				

Certificate Revocation					
Certificate revocation appears to be optional in ISO 15118. Therefore, there are no requirements specified for Certificate revocation process, i.e.,: • Circumstances for revocation • Who can request revocation • Revocation request procedure • Revocation status issuance	●				
Certificate Repository					
Implementation of ISO 15118 will employ multiple Root CAs and Sub-CAs. Relying Parties will need a trusted source from which to retrieve the CA Certificates, especially if switching between root domains and their Sub-CAs is automated between the EVCC and the SECC. A secure Certificate repository can serve to distribute Certificate revocation information (e.g., CRLs) or serve as an out-of-band validation mechanism.	●				
Incident Response					
Incident response requirements are needed in ISO 15118 to develop and maintain each Root CA's security management and incident response plans that include reacting to vulnerabilities or compromises impacting the ecosystems use of Certificates.	●				
PKI Compliance and Audit					
Compliance Audit policies are needed to govern all Root CAs participating in the ecosystem PKI, in order to ensure that the CAs are in compliance with the CPs of ISO 15118 and are operating in accordance with the CA generated CPS. The Audit policy should specify the qualifications of auditors, the frequency of the Audits, the topics covered by the Audit (e.g., CP and CPS), the actions to be taken as a result of deficiency, and communications of the results.	●				
Cross-Certification					
There are no requirements for cross-certification of Root CAs in ISO 15118, thus all Root CAs will be seen as of equal assurance level by the Relying Party (e.g., EVs), regardless of the actual assurance level of the Root CA. Without a common baseline for PKI requirements and a compliance Audit policy, assurance levels between each Root CA will vary. An attacker will use the weakest link in the set of trusted roots to attack the ecosystem. A cross-certification policy for the V2G roots will extend the trust relationship between the root domains evenly when applied with a compliance Audit policy.	●				

Review of Similar Security Models for Critical Infrastructure

Successfully designed and deployed PKIs for similar critical infrastructures typically have rankings of Established or Optimized in an overwhelming majority of the 21 PKI categories under which ISO 15118 was reviewed. Examples of successfully deployed and managed critical infrastructure PKIs include:

- AeroMACS - The Aeronautical Mobile Airport Communication System (AeroMACS) deploys a wireless broadband technology for data communication and information sharing on the airport surface for both fixed and mobile applications. The AeroMACS PKI provides Certificates for aeronautical equipment communication and authentication at airports worldwide.
- ICAO e-Passport - The International Civil Aviation Organization (ICAO) Public Key Directory (PKD)[2], a PKI trust model used for e-Passports. This PKI authenticates the identity of the passport holder. Current participants include 65 out of the 100 state and non-state entities that currently issue e-Passports.
- DNSSEC[3] - The Domain Name System Security Extensions (DNSSEC) is a global scale[4] PKI designed to authenticate the origin of DNS responses and verify the integrity of the data. It could be said that DNSSEC is the largest single PKI in the history of the Internet considering the number of people using it on Internet Protocol networks.

These deployed PKIs benefit from the collaboration of major stakeholders who convened governing bodies or coalitions to craft the PKI governance, architecture, and operational requirements that best serve their industries. The EV charging community has not yet created a governing body to develop a PKI suitable for the entire EV industry. Without such collaboration, including input and oversight from stakeholders across the industry, it is difficult to assure interoperability across EVs, EVSE, charging network platforms, and other service providers and parties in the ecosystem.

[2] https://www.icao.int/Security/FAL/PKD/Pages/ePassportBasics.aspx
[3] https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en
[4] https://www.internetsociety.org/deploy360/dnssec/maps/

Conclusion and Next Steps

After performing a 360ºPKI maturity assessment on the ISO 15118 PKI, it is clear that the proposed ISO 15118 (First edition) V2G PKI is not ready for a scalable, production implementation in light of critical governance, technology and operations issues which negatively impact the proposed goals of the standard and EV charging industry stakeholders. The proposed V2G PKI is too complex, leaves too much room for different interpretation by implementers, and conflicts with best practices that exist today in successfully deployed global PKIs.

In fact, our assessment shows that the current ISO 15118 standard fails to meet the established criteria in 85% of the categories assessed. There is no current development of PKI best practices for existing EV charging infrastructure; the proposed ISO 15118 PKI is not sufficiently agile or flexible enough to handle the projected use cases (including Plug and Charge). If the shortcomings outlined in this assessment are not addressed then the EV industry risks deploying EVs and EVSEs that will not work outside of their designated home region or with other manufacturer's equipment. This opens the ecosystem up to attacks that can be launched from bad actors which can harm the network through, for example, Man-in-the-Middle attacks or DDOS attacks. Furthermore, any updates that need to be made can be slow and cumbersome to implement due to the complexity of provisioning EVs in the field and can result in high cost and loss of revenue for stakeholders.

A PKI's success depends on how it's designed, deployed, and maintained throughout all levels of governance, technology, and operations, and as such, continual updates and ecosystem collaboration must be part of the ISO I5118 PKI Standard development to achieve success as a global PKI that is able to serve all participants and stakeholders within the EV ecosystem. Thus, it is strongly advised that the issues found in this assessment be addressed by the stakeholders within the ISO 15118 community quickly before any product is launched. Stakeholders would benefit in establishing a coalition with a diverse set of skills and experiences to address the recommendations of this paper, to provide overall governance and to continue developing a standards-based solution that is not only secure, scalable, and interoperable but also reduces implementation complexity and integration costs of the PKI within the ecosystem.

About Eonti

Eonti provides consulting, strategy, governance, technology, and lifecycle operations for Trust Management and Public Key Infrastructure (PKI). The team is led by Eonti Founder and CEO Oscar Marcia, a former 15-year VP of Security for CableLabs. Oscar has built a team with extensive first-hand expertise in working with the organizations that lead Homeland Security's critical infrastructure sectors, including transportation (aviation and automotive), communications (cable, satellite, and wireless), healthcare, and IoT industries. Eonti partners with DigiCert to bring IoT security to all critical infrastructure deployments.

About DigiCert

DigiCert is the world's leading provider of scalable TLS/SSL, PKI solutions for identity and encryption. The most innovative companies, including 89 percent of Fortune 500 companies and 97 out of the 100 top global banks, choose DigiCert for its expertise in identity and encryption for web servers and Internet of Things devices. DigiCert supports TLS/SSL and other digital certificates for PKI deployments at any scale through its certificate lifecycle management platform, CertCentral®. The company is recognized for its enterprise-grade certificate management platform, fast and knowledgeable customer support, and market-leading security solutions. For the latest DigiCert news and updates, visit digicert.com or follow @digicert.

About ChargePoint

ChargePoint is the leading electric vehicle (EV) charging network in the world, with charging solutions in every category EV drivers charge, at home, work, around town and on the road. With more than 65,000 public and semi-public commercial charging spots and thousands of customers (businesses, cities, agencies and service providers), ChargePoint is the only charging technology company on the market that designs, develops and manufactures hardware and software solutions across every use case. Leading fleet managers, EV hardware makers and other partners rely on the ChargePoint network to make charging station details available in mobile apps, energy management solutions, online and in navigation systems for popular EVs. ChargePoint drivers have completed more than 55 million charging sessions, saving upwards of 60 million gallons of gasoline and driving more than a billion gas-free miles on dispensed energy. For more information, visit www.chargepoint.com.