Protect. Renew. Empower.

Certificate Policy

For CharIN V2G PKI by Irdeto
Compliant to ISO 15118-2

Document Summary

The document is the Certificate Policy for the CharIN Vehicle-to-Grid first-generation Public Key Infrastructure delivered by Irdeto [hereafter, CharIN V2G PKI]. This first-generation PKI complies with ISO 15118-2, [5]. (For ISO 15118-20 compliance please refer to the following document [7]).

Document Number	986557
Revision	1.1
Author(s)	Irdeto
Classification	Unrestricted
Date Issued	April 15, 2024

Table of Contents

List of Figures

List of Tables

Structure

This Certificate Policy (CP) conforms to the structure of Certificate Policies and Certification Practice Statements specified in RFC 3647 [1], with the following comments:

- To retain the outline structure specified by RFC 3647, some sections of this CP contain the statement "Not applicable" or "No stipulation."
- To prevent sections from becoming too long, or to clearly indicate which requirements are applicable for which PKI participants, sections are sometimes divided into multiple subsections.
- Finally, a few sections have been added that do not appear in RFC 3647, to discuss topics that are not clearly identified in the RFC.

Intended audience

This document is public. However, it is intended primarily for CharIN V2G PKI participants, as described in section 1.3. Readers of this document are supposed to be familiar with ISO 15118-2, [5] and VDE-AR-E 2802-100-1, [8].

Key words

Within this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL", if written in capitals, are to be interpreted as described in RFC 2119, [3].

Change History

Rev.	Date	Author	Description
1.0	Nov 23, 2023	CharIN PnC Europe Governance Board	First public version
1.1	Jan 22, 2024	Irdeto CrossCharge Governance Board	Updated by Irdeto, the new V2G PKI owner

Terms, Acronyms and Abbreviations

Term	Definition
API	Application Programming Interface
CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPO	Charging Point Operator
CPS	Certificate Provisioning Service
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DER	Distinguished Encoding Rules
DN	Distinguished Name
ECC	Elliptic Curve Cryptography

Term	Definition
EV	Electric Vehicle
EVCC	Electric Vehicle Communication Controller
EVSE	Electric Vehicle Supply Equipment
HSM	Hardware Secure Module
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
ISMS	Information Security Management System
MO	Mobility Operator
MSO	Mobility Service Operator
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OID	Object Identifier
OTP	One-Time Password
PKI	Public Key Infrastructure
RA	Registration Authority
SE	Secure Element (in a SECC or an EVCC)
SECC	Supply Equipment Communication Controller
TLS	Transport Layer Security
V2G	Vehicle to Grid

Notes, Tips, and Warnings

Notes provide additional important information that should be read, such as a brief explanation, a reinforcing comment, or offset information used to alert the reader of important information.

Tips provide additional information for advanced users, such as an alternate operation method or a keyboard shortcut.

Warnings alert the reader to possible serious consequences, such as service interruption or system failure.

1 Introduction

1.1 Overview

About Irdeto

For over 50 years, Irdeto has been a trusted partner in securing the products and businesses of many of the world's leading software application providers, connected device manufacturers, pay-media operators, and content creators. Irdeto is the world leader in digital platform security, with software security technology and cyber security services currently protecting over six billion devices and/or applications for some of the world's best-known brands. Irdeto has more than 400 customers in 75+ countries, including EV OEMs, CP OEMs, Tier 1s, CPOs, and MSOs.

With our vast experience in stopping hackers and hacking tools and technologies, we are ideally and uniquely suited to provide value to automotive, mobility, and similar companies whose businesses are based on the security of software and devices deployed in untrusted environments and within reach of hackers. We know, from our customer implementations, that background security knowledge and experience are critical to successful and secure deployments of technology into the market.

For our electromobility customers, we offer a complete set of managed services for Plug and Charge from regional V2G Roots to Certificate Pools following the ISO 15118 standard and VDE guidelines. Our services are underpinned by our in-house technology that manages over 350 million devices and 1 billion certificates for our customers today. To enable ISO 15118 adoption, Irdeto operates V2G Roots in the European and North American markets (hereinafter "V2G Roots").

About CharIN V2G PKI by Irdeto

This document is the Certificate Policy (CP) for certificate services used within the CharIN Vehicle-to-Grid (V2G) first-generation Public Key Infrastructure (PKI) by Irdeto. The aim of this PKI is to secure the information transfer between an electric vehicle (EV) and an electric vehicle supply equipment (EVSE). This first-generation V2G PKI is compliant with ISO 15118-2 [5]. For many of the options left open in that standard, this document makes specific choices. Please refer to section 1.3.2.3 for an overview.

Irdeto has also established a second-generation V2G PKI, which is compliant with ISO 15118-20 [5]. The Certificate Policy for the second-generation V2G PKI can be found in [7]. In the remainder of the current document, the term '(CharIN V2G) PKI' indicates the first-generation PKI.

This CP sets forth the business, legal, and technical requirements for approving, issuing, managing, using, revoking, and renewing public key certificates by all Certification Authorities within the CharIN V2G PKI. This CP additionally contains requirements for other participants in the PKI, in particular for the subscribers requesting end entity certificates from Tier-2 CAs. These include Charging Point Operators (CPO), Certificate Provisioning Services (CPS), Mobility Operators (MO) and OEMs of electric vehicles. This CP also contains requirements for the relying parties that need to trust a certificate issued by a CA in the CharIN V2G PKI. These requirements protect the security and integrity of the CharIN V2G PKI and comprise a single set of rules that apply PKI-wide consistently, thereby providing assurances of uniform trust throughout the PKI.

This CP does not govern any systems or services outside the CharIN V2G PKI. This CP is not a legal agreement between participants of the CharIN V2G PKI.

1.2 Document name and identification

This CP is identified by the following information:

- Name: Certificate Policy for CharIN V2G PKI, Compliant to ISO 15118-2, version 1.1.
- OID: 1.3.6.1.4.1. 59034.1.2

Notes on the OID:

- 1.3.6.1.4.1. 59034 is the arc for CharIN e.V.; see https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers.
- The first digit 1 identifies this document, i.e., the Certificate Policy for CharIN V2G PKI, Compliant to ISO 15118-2
- The second digit 2 identifies the current version of this document, i.e., v1.1.

This CP SHALL become effective the day when it is published on the Irdeto website on the following URL: www.irdeto.com/connected-transport/electric-vehicle-ev-charging/pki. It SHALL remain valid until Irdeto replaces it by a new version. For the process of updating this CP (and its OID), please refer to section 9.12.

1.3 PKI Participants

1.3.1 Disclaimer

This section is for informational purposes only. If there are statements in this section that conflict with requirements in ISO 15118-2, then ISO 15118-2 takes precedence, unless explicitly stated otherwise.

1.3.2 PKI overview

1.3.2.1 PKI structure

Figure 1 gives an overview of the Certification Authorities and their subscribers in the CharIN V2G Public Key Infrastructure.

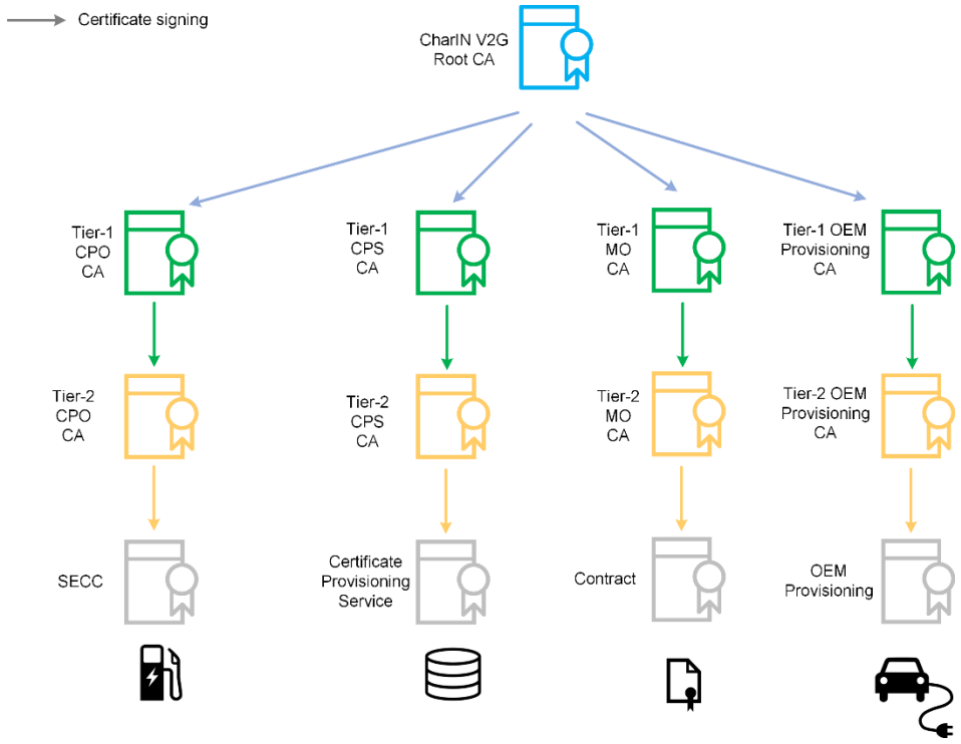

Figure 1: Overview of the CharIN V2G PKI for ISO 15118-2

As shown in the figure, the PKI consists of four levels: a root CA, Tier-1 CAs, Tier-2 CAs and end entities. The Tier-1 CAs are subordinate CAs of the V2G Root CA, meaning that their certificates are

signed by the Root CA. Similarly, the Tier-2 CA certificates are signed by the Tier-1 CAs. The Tier-2 CAs sign the end entity[1] certificates.

There SHALL be only one V2G Root CA in the V2G PKI, which SHALL be appointed by the Irdeto CrossCharge Governance Board (see section 1.5). However, there MAY be multiple instances of the Tier-1 and Tier-2 CAs in each of the branches within the V2G PKI. As an example, each Charging Point Operator may operate its own Tier-2 CPO CA, and there may be a Tier-1 CPO CA in each country to sign the certificates of the Tier-2 CPO CAs.

Figure 1also shows that there are five different branches present in the CharIN V2G PKI. These are:

- The Charging Point Operator (CPO) branch,
- The Certificate Provisioning Service (CPS) branch,
- The Mobility Operator (MO) branch,
- The OEM Provisioning (OEM Prov) branch[2].

The purpose of each branch is briefly described in section 1.3.2.2.

1.3.2.2 Branches within the PKI

1.3.2.2.1 Charging Point Operator (CPO) branch

The end entities in the CPO branch are the supply equipment communication controllers (SECC) in electric vehicle supply equipment (EVSE, also known as charging stations). A SECC obtains a SECC certificate from a Tier-2 CPO CA and uses it for authenticating itself to the EVCC of an EV at the start of a charging session. The SECC always acts as the TLS Server.

1.3.2.2.2 Certificate Provisioning Service (CPS) branch

The end entities in the CPS branch are parties acting as a Certificate Provisioning Service (CPS). A CPS obtains a Certificate Provisioning Service certificate from a Tier-2 CPS CA, and uses the private key associated with that certificate to sign messages containing Contract certificates and associated private keys. These messages will be sent to an EVCC in case the EV needs a Contract certificate. This can be done either via a SECC, during a charging session, or via an OEM backend. The first option is described in the next section; the second option is not further discussed in this document.

1.3.2.2.3 Mobility Operator (MO) branch

The end entities in the MO branch are electric vehicles having a contract with a Mobility Operator for delivering energy via a charging station (EVSE). Such a contract is represented by a Contract certificate stored in the EVCC of the EV. During a charging session, the EVSE will verify this Contract certificate[3].

After establishing a contract with an EV owner, a Mobility Operator creates a Contract key pair consisting of a private and a public key, and requests a Contract certificate from a Tier-2 MO CA. After receiving the new Contract certificate, the MO obtains the OEM Provisioning certificate of the EVCC, for example from an OEM Provisioning certificate pool (see section 1.3.8.2). It uses the public key in that certificate in a Diffie-Helman key agreement process to derive a session key, which it then uses to encrypt the new Contract certificate and associated private key[4].

---

[1] ISO 15118-2 calls these the 'leaf certificates'.

[2] ISO 15118-2 distinguishes two types of 'provisioning' certificates – Certificate Provisioning Service certificates and OEM Provisioning certificates, each with their associated Tier-2 and Tier-1 CAs. Unfortunately, the naming conventions is ISO 15118-2 are not fully consistent. This document uses the names shown in Figure 1.

[3] Note that even if the certificate is valid, the EVSE will contact the MO to get approval for starting the charging process.

[4] Clause 7.9.2.5 of 15118-2 specifies that the MO must use the existing Contract public key to derive the session key in case there already is a valid Contract certificate for the EVCC ('certificate update'). In case there is no valid Contract certificate, the MO must use the OEM Provisioning certificate of the EVCC. However, this

Then, the encrypted Contract certificate and the associated private key SHALL be sent to the EVCC[5]. One possible method is to do this during a charging session, using a SECC, as follows:

- The MO forwards the encrypted Contract certificate and private key to the Certificate Provisioning Service, see section 1.3.2.2.2.
- The Certificate Provisioning Service signs the credentials to ensure their integrity and authenticity.
- The Certificate Provisioning Service makes the signed and encrypted Contract credentials available to the SECC, for example by storing them in a Contract certificate pool, see section 1.3.8.1.
- During a charging session, if the SECC determines the EVCC needs a new Contract certificate, it searches the Directory Service (see section 1.3.8.1) to see if a new Contract certificate is available in a Contract certificate pool. If so, the SECC requests the signed and encrypted Contract credentials from the pool, compiles a message containing these credentials and transmits that to the EVCC.
- The EVCC verifies the signature over the credentials, decrypts the credentials, securely stores the Contract private key in its secure memory, and also stores the Contract certificate.

1.3.2.2.4 OEM Provisioning (OEM Prov) branch

The end entities in the OEM Prov branch are EVCCs in electric vehicles. During the manufacturing of the EV, the OEM creates an OEM Provisioning key pair, and stores the associated private key in the EVCC. The OEM then requests an OEM Provisioning certificate from the Tier-2 OEM Prov CA, and makes it available to Mobility Operators, for example using an OEM Provisioning certificate pool, as explained in section 1.3.8.2. Mobility Operators will use the public key in this certificate to encrypt Contract certificates and private keys for this EV, as described in the previous section.

1.3.2.3 Compliance with ISO 15118-2

The CharIN V2G PKI described above complies with the certificate structure defined in ISO 15118-2. With respect to the options allowed in ISO 15118-2, this document makes the following choices:

- There SHALL be no MO Root CA; instead, the Tier-1 MO CAs SHALL be sub-CAs of the V2G Root CA and SHALL thus be part of the public CharIN V2G PKI.
- There SHALL be no OEM Root CA; instead, the Tier-1 OEM Prov CAs SHALL be sub-CAs of the V2G Root CA and SHALL thus be part of the public CharIN V2G PKI[6].

CP stipulates that the MO SHALL always use the latter certificate. This change was made for following reasons:
-There seems to be no good reason for not always using the same public key, i.e. the one from the OEM Provisioning certificate of the EVCC. Doing so is simpler conceptually and in practice.
-Using the existing Contract certificate may lead to operational problems if the existing contract is with a different MO. It is not clear how the new MO then obtain the existing Contract certificate.
-Using the existing Contract certificate would also force the new MO to trust the existing Contract certificate, even in case it is issued by another MO.
Finally, in 15118-20, the difference between certificate installation and certificate update does not exist. It is undesirable to have different approaches in the two PKIs.

[5] A more standard approach would be to let the EVCC itself create the Contract key pair, and then let the EVCC send the public key to the MO to be certified. This would avoid having to send the sensitive private key over a remote connection. However, it would also mean that the entire process described in this section (possibly including the process of concluding the contract between the MO and the EV owner) needs to take place during a charging session, and before the actual charging can begin. The current process allows pre-calculation of the signed and encrypted Contract credentials.

[6] In principle, participants in the CharIN V2G PKI MAY accept Contract certificates, OEM Provisioning certificates or Vehicle certificates that have been issued under a separate MO Root CA or OEM Root CA, provided that these root CA certificates have been cross-certified by the CharIN V2G Root CA. Cross-certification is specified in ISO 15118-20. However, cross-certification is out of scope of this document.

Note that section 7.1 of this document also makes specific choices for many of the options indicated for the certificate profiles in Annex F of ISO 15118-2. That section also corrects a few mistakes in these profiles.

1.3.3 Certification Authorities

The responsibilities of any CA within the CharIN V2G PKI SHALL include:

- Generating signing key pairs as needed, in accordance with the requirements in ISO 15118-2 and in this CP.
- Obtaining a certificate for each key pair from the appropriate superordinate CA, if applicable[7].
- Receiving certificates to-be-signed from the associated Registration Authority; see section 1.3.5.
- Signing the requested certificate, using the private signing key indicated in the request.
- Keeping traceable records of all signed certificates.
- Revoking an issued certificate when necessary, keeping traceable records of revocations, and maintaining and publishing a Certificate Revocation List as specified in section 4.9.

ISO 15118-2 (optionally) tasks a Tier-2 MO CA with signing Sales Tariffs, when requested by a Mobility Operator. This function SHALL not be used within the CharIN V2G PKI.

Moreover, each CA or PKI Operator within the CharIN V2G PKI SHALL

- Create and maintain a Certification Practice Statement explaining how the CA complies with all applicable requirements in this CP.
- Establish an information security management system (ISMS), based on a risk assessment for all the operations involved. The ISMS SHALL cover all information and processes related to key management and issuing certificates. The implementation of the ISMS SHALL be certified according to ISO 27001 [9].

A PKI Operator (see next section) MAY use a single Certification Practice Statement covering all CAs included. However, in that case the Certification Practice Statement SHALL, where needed, clearly distinguish between the (systems of the) different CAs. Similarly, a PKI Operator MAY establish a single ISMS, but this ISMS SHALL make clear distinctions between information and processes related to the different CAs.

1.3.4 PKI Operator

A single organization MAY operate both the V2G Root CA as well as an instance of each Tier-1 and Tier-2 CA within the CharIN V2G PKI. Such an organization is called the PKI Operator. The presence of a PKI Operator SHALL not preclude the existence of other Tier-1 or Tier-2 CAs, operated by other organizations. The V2G Root CA run by the PKI Operator SHALL not discriminate against such 'external' CAs (if present) in favor of the CAs operated by the PKI Operator itself.

- Since there can be only one V2G Root CA, there can be one PKI Operator at most.
- The PKI Operator SHALL be appointed by Irdeto.
- The V2G Root CA is not a PKI Operator if it does not operate a Tier-1 CA and a Tier-2 CA for each of the CPO, CPS, MO, and OEM Prov branches as well.

[7] The V2G Root CA does not have a superordinate CA. The V2G Root CA is the trust anchor of the CharIN V2G PKI; the relevant information consists of a public key, a public key signature algorithm identifier, and a name. For convenience, the trust anchor information is distributed in the form of a self-signed certificate.

1.3.5 Registration Authorities

Each CA within the CharIN V2G PKI SHALL operate its own Registration Authority (RA). The registration process for issuing certificates is in the sole responsibility of the issuing CA. The registration process SHALL ensure that only authenticated requests will result in issued certificates.

The RA responsibilities SHALL include:

- Receiving certificate applications.
- Identifying and authenticating the certificate applicant, as specified in section 4.2.1.
- Validating the certificate application, as specified in section 4.2.2.
- Formally accepting or rejecting certificate applications.
- Generating and forwarding the to-be-signed certificate to the associated CA.
- Receiving and reviewing the resulting issued certificate from the CA.
- Sending an issued certificate to the applicant, and to a certificate pool if applicable, see sections 1.3.8.1 and 1.3.8.2.

1.3.6 Subscribers

As described in RFC 3647, the subscriber for the certification services of a particular CA is the person or organization that has a contract with that CA and is authorized to request the CA to sign certificates. In the CharIN V2G PKI, subscribers are always organizational entities. Thus,

- The subscribers for the V2G Root CA are the Tier-1 CPO, CPS, MO, and OEM Prov CAs.
- The subscribers for a Tier-1 CA are the Tier-2 CAs in the respective branch.
- The subscribers for a Tier-2 CPO CA are Charge Point Operators.
- The subscribers for a Tier-2 CPS CA are Certificate Provisioning Services. As described in ISO 15118-2, this role MAY be fulfilled by a Mobility Operator, an EVSE operator, or a dedicated CPS operator.
- The subscribers for a Tier-2 MO CA are Mobility Operators.
- The subscribers for a Tier-2 OEM Prov CA are OEMs of electric vehicles.

Subscribers SHALL be responsible for:

- Indicating registered contact points (section 3.2.2) and authorized administrators (section 3.2.3.2).
- Timely sending certificate applications to the respective RA,
- Ensuring the accuracy of the information in any certificate application sent,
- Accepting or rejecting any issued certificate according to section 4.4.1.
- Using any certificate according to all applicable requirements in section 4.5.1.
- Notifying the respective CA without delay in case
  - the data in the certificate is, or becomes, inaccurate.
  - a compromise of the private key associated with a certificate is proven or suspected.
  - the subscriber has lost control over the private key associated with a certificate. In case the private key is located in an EVCC or SECC, this includes cases of theft, malfunctioning, or destruction.

For the V2G Root CA and the Tier-1 CAs, the Subject of the issued certificate will indicate the subscriber requesting and receiving that certificate. But for most Tier-2 CAs, this is not the case, as they issue end entity certificates for EVCCs and SECCs. Thus, the certificate's Subject field will contain an identifier for an EVCC, a SECC or a Contract, instead of an identifier for the subscriber. Certificate Provisioning Service certificates (signed by a Tier-2 CPS CA) are the exception among the Tier-2 CAs. For these certificates, the subject is in fact the same party as the subscriber requesting and receiving the certificate.

1.3.7 Relying parties

In general, relying parties of the CharIN V2G PKI are:

- EV owners and MOs, for being able to buy and sell electricity at any charging station (EVSE) using Plug-and-Charge,
- OEMs and CPOs, for being able to manufacture vehicles and operate charging stations that support the Plug-and-Charge service.
- For any CA, the relying parties are all organizations, individuals, or devices that use certificates issued by that CA for any purpose and rely on the authenticity of such a certificate to achieve that purpose.

In more detail,

- For the V2G Root CA, the relying parties are:
  - For the (self-signed) Root CA certificates: all participants in the CharIN V2G PKI, as described in this section 1.3, since all trust in this PKI is ultimately based on trust in the authenticity of these root certificates.
  - For the Tier-1 CA certificates issued by the V2G Root CA: the parties using those Tier-1 certificates to validate the associated Tier-2 certificates.
- For the Tier-1 CAs the relying parties are the same ones as for the respective Tier-2 CAs, see bullets below.
- For a Tier-2 CPO CA, the relying parties are the EVCCs. These rely on these certificates for authenticating a charge station (EVSE) during charging sessions.
- For a Tier-2 CPS CA, the relying parties are also the EVCCs. These rely on these certificates for authenticating the Contract certificate and private key they receive from a MO.
- For a Tier-2 MO CA, the relying parties are the SECCs, which validate the signature over a Contract certificate in order to approve charging.
- For a Tier-2 OEM Prov CA, the relying parties are the Mobility Operators, which validate the OEM Prov certificate of an EV in order to
  - trust the authenticity of a CertificateInstallationRequest message relayed by a SECC from an EVCC that does not currently possess a valid Contract certificate to start the charging process;
  - be able to trust the authenticity of the public key they use for encrypting the Contract certificate and private key.
- For a Tier-2 Vehicle CA, the relying parties are the SECCs. These rely on these certificates for authenticating an EV (EVCC) during charging sessions.

1.3.8 Other participants

1.3.8.1 Contract certificate pool operators and Directory Service

Section 1.3.2.2.3 described that a Mobility Operator needs to create a Contract certificate and an associated Contract key pair for every EV for which it has contractually agreed to deliver electricity using the CharIN ecosystem. During a charging session, the EVSE needs to verify if it needs to transfer a new Contract certificate and associated private key to the EV. To do so, it needs to be able to check quickly if there is any Mobility Operator that has created a Contract certificate for this EV that still needs to be transferred to the EV.

ISO 15118-2 does not specify how an EVSE can do this. However, VDE-AR-E 2802-100-1, [8], section 5.6, explains one possibility, which is to use a Contract certificate pool. A Contract certificate pool contains Contract certificates and private keys that must still be transferred to an EVSE. These are signed by the Certificate Provisioning Service (see section 1.3.2.2.2) and encrypted as described in section 1.3.2.2.4.

VDE-AR-E 2802-100-1 also introduces the concept of a Directory Service that refers to multiple Contract certificate pools and allows an EVSE to quickly find the pool containing the Contract credentials for a specific EV.

Contract certificate pool operators and Directory Services within the CharIN V2G PKI SHALL comply with all relevant requirements in VDE-AR-E 2802-100-1, [8].

VDE-AR-E 2802-100-1 does not specify the necessary APIs for a Directory Service provider and for a Certificate contract pool operator.

1.3.8.2 OEM Provisioning certificate pool operators

Section 1.3.2.2.3 also described that a Mobility Operator needs to encrypt the new Contract certificate and private key with the OEM Provisioning public key of the relevant EV. This ensures that only the EVCC of that EV will be able to decrypt the Contract private key and use the associate contract to charge its battery.

However, this means that the Mobility Operator needs a way to search for and obtain the OEM Provisioning certificate of the vehicle it is creating a Contract certificate for. VDE-AR-E 2802-100-1, [8], section 5.7, explains one possibility for doing so, which is to use the services of an OEM Provisioning certificate pool operator.

OEM Provisioning certificate pool operators within the CharIN V2G PKI SHALL comply with all relevant requirements in VDE-AR-E 2802-100-1, [8].

VDE-AR-E 2802-100-1 does not specify the necessary APIs for an OEM Provisioning certificate pool operator.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

A certificate issued by any CA within the CharIN V2G PKI SHALL only be used by participants in the CharIN V2G PKI, as described in section 1.3 of this CP. Moreover, each certificate SHALL be used only for its respective purpose(s), as described in section 1.3 and in ISO 15118-2 [5].

1.4.2 Prohibited certificate uses

A certificate issued by any CA within the CharIN V2G PKI SHALL NOT be used for any purpose not explicitly allowed in section 1.4.1.

1.5 Policy administration

1.5.1 Organization administering the document

This document is administered by the Irdeto CrossCharge Governance Board, which can be contacted as stated in section 1.5.2.

1.5.2 Contact person

Questions regarding this CP SHOULD be addressed to the Irdeto CrossCharge Governance Board, which can be reached using one of the following channels:

Address: Irdeto CrossCharge Governance Board
Irdeto Security B. V.
Taurusavenue 105
2132 LS Hoofddorp
The Netherlands

E-mail: pki.ma@irdeto.com
Phone: +31 23 556 2000
Fax: +31 23 556 2240
website : www.irdeto.com/connected-transport/electric-vehicle-ev-charging/pki

1.5.3 Determination of Certification Practice Statement suitability for the policy

The CharIN V2G PKI Management Authority is responsible for determining the suitability of this CP for achieving Irdeto business objectives. This CP SHALL be approved by the Irdeto CrossCharge Governance Board before being published.

The CharIN V2G PKI Management Authority is also responsible for determining whether the Certification Practice Statement of the CharIN V2G Root CA conforms to this CP. The Certification Practice Statement SHALL be approved by the Irdeto CrossCharge Governance Board before the V2G Root CA is allowed to start operating.

If a Tier-1 or Tier-2 CA is run by the same organization as the CharIN V2G Root CA (meaning it is part of the PKI Operator, see section 1.3.4), then the CharIN V2G Root PKI Management Authority SHALL be responsible for determining whether the CA's Certification Practice Statement complies to this CP.

If a Tier-1 or Tier-2 CA is run by an organization other than the V2G Root CA, then the approving organization identified in section 3.2.6 SHALL be responsible for determining whether the CA's Certification Practice Statement complies to this CP.

The Certification Practice Statement of a Tier-1 or Tier-2 CA SHALL be approved before the CA is allowed to start operating.

1.5.4 Certification Practice Statement approval procedures

See section 3.2.6.

2 Publications and repository responsibilities

2.1 Repositories

An OEM that receives an OEM Provisioning certificate for an EV from a Tier-2 OEM Prov CA in the CharIN V2G PKI SHALL make this certificate available to all Mobility Operators in the CharIN V2G ecosystem, under terms and conditions that are fair, reasonable, and non-discriminatory. To do so, the OEM MAY publish that certificate in an OEM Provisioning certificate pool as described in section 1.3.8.2 and specified in more detail in [8]. The OEM SHALL remove the certificate from its OEM Provisioning certificate pool when it expires or is revoked.

When a MO has created a new Contract private key and associated Contract certificate for an EV, and has made sure these are properly signed and encrypted, the MO SHALL make this certificate available to all CPOs and OEMs in the CharIN V2G ecosystem, under terms and conditions that are fair, reasonable, and non-discriminatory. To do so, the MO MAY publish these credentials in a Contract certificate pool, as described in section 1.3.8.1 and specified in more detail in [8]. The MO SHALL remove the signed and encrypted Contract credentials from its Contract certificate pool immediately after they have been successfully transmitted to the respective EVCC, or when the Contract certificate expires or is revoked.

2.2 Publication of certification information

Each CA in the CharIN V2G PKI SHALL publish the following information:

- This Certificate Policy, or a link to it,
- Information on how to request revocation of a certificate issued by the CA.

Each CA MAY additionally publish

- its valid (Root) CA certificates, identified at least by a fingerprint,
- its Certification Practices Statement,
- A statement from the approving organization (see section 3.2.6) regarding the compliance of the CA's Certification Practice Statement to this CP, and the outcome of audit(s) done for the operations of the CA.

All information SHALL be published on a public website. Read-only access to this information SHALL be available without restrictions.

Upon request of a participant in the CharIN V2G PKI, the V2G Root CA SHALL additionally make available the following information:

- Name and contact information of all parties that have been admitted to the CharIN V2G PKI as a Tier-1 or Tier-2 CA.
- Name and contact information of all parties that have been admitted to the CharIN V2G PKI as a Charging Point Operator, Mobility Operator, Certificate Provisioning Service, or OEM.
- URLs of all Contract certificate pools, for each of the Mobility Operators in the CharIN ecosystem,
- URLs of all OEM Provisioning certificate pools, for each of the OEMs in the CharIN ecosystem.

2.3 Time or frequency of publication

Each CA in the CharIN V2G PKI SHALL publish any update to the information listed in 2.2 within 7 days from the relevant change.

Information relating to changes in this policy SHALL be published according to the schedule defined in the amendment procedures laid down in section 9.12 of this document.

2.4 Access control on repositories

All information mentioned in sections 2.1 and 2.2 SHALL have read-only access. Each party mentioned in these sections SHALL designate staff having write or modify access to the information under its control. Access controls, including both logical and physical security measures, SHALL be

implemented to prevent unauthorized persons from adding, deleting, or modifying published information.

Websites and repositories used for publishing this information SHALL be protected using Transport Layer Security (TLS), v1.2 or later.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

Within the CharIN V2G PKI, a consistent hierarchy for naming SHALL be used. Each CA SHALL identify each of its subscribers through a unique distinguished name (DN) according to RFC 5280 [4]. The following attributes MAY be used in a distinguished name:

- CountryName (C),
- Organisation (O),
- Organisational Unit (OU),
- Common Name (CN),
- DomainComponent (DC).

Other attributes SHALL not be present. Only the *organisationalUnit* attribute MAY be added more than once.

Attributes SHALL be encoded following the same order provided above. In other words, if present, a *countryName* SHALL always be encoded first. A *domainComponent* SHALL always be encoded last.

Detailed requirements regarding the presence of attributes in the DNs can be found in the certificate profiles in section 7.1.

Wildcards (e.g., *.cpoprovider.de) SHALL NOT be used in DNs.

3.1.2 Need for names to be meaningful

Distinguished names used in certificates within the CharIN V2G PKI SHALL use commonly understood semantics permitting the determination of the real-world identity of the organization that is the subject or issuer (as applicable) of the certificate.

3.1.3 Anonymity or pseudonymity of subscribers

Anonymity or pseudonymity of subscribers is not allowed within the CharIN V2G PKI. Refer to the naming requirements in section 3.1.5.

3.1.4 Rules for interpreting various name forms

Distinguished names in certificates issued by a CA in the CharIN V2G PKI SHALL be interpreted using the X.500 standards, the ASN.1 syntax and RFC 2253 (LDAP v3).

When a DN has to be represented as a string, the protocol described in RFC 4514 SHALL be used (i.e., reversed - attributes denoting the top of the naming hierarchy are shown last).

3.1.5 Uniqueness of names

3.1.5.1 Tier-1 CAs and Tier-2 CAs

Each CA SHALL declare a unique Subject distinguished name (DN) during the approval procedure described in section 3.2.6.1. The DN SHALL contain a *domainComponent* attribute, which SHALL have value “CPO”, “CPS”, “MO”, or “OEM”[8]. The Subject DN SHALL also contain a *commonName*

[8] These values are specified in ISO 15118-2, Annex F, with the exception of the values “MO” for a Tier-1 or Tier-2 MO CA and “OEM” for a Tier-1 or Tier-2 OEM Prov CA. This document adds these values.

and an *organizationName* attribute. The DN MAY contain a *countryName* and/or one or more *organizationalUnitName* attributes. The DN SHALL NOT contain any other attributes.

The approving organization SHALL verify that this DN is unique within the CharIN V2G PKI, is meaningful according to section 3.1.2, and matches the real-world identity of the CA, including the appropriate value for the *domainComponent* attribute. If so, the approving organization SHALL register the DN. The Tier-1 or Tier-2 CA SHALL use the registered Subject DN in all certificate applications it subsequently sends to the respective CA.

If the distinguished name of a CA changes, the CA SHALL notify the approving organization. The approving organization SHALL apply the verifications listed above to the new distinguished name, and SHALL register the new DN. Afterwards, the CA SHALL use the new DN in all certificate applications.

The requirements for the Subject DN of a V2G Root CA certificate are specified in section 7.1.3.

3.1.5.2 Subscribers to Tier-2 CAs

A subscriber to a Tier-2 CA SHALL declare a unique Subject distinguished name (DN) during the approval procedure described in section 3.2.6.2. The DN SHALL contain a *domainComponent* attribute, which SHALL have value "CPO", "CPS", "MO", or "OEM"[9]. The DN SHALL contain an *organizationName* attribute. The DN MAY contain a *countryName* and/or one of more *organizationalUnitName* attributes. A subscriber to the Tier-2 CPS CA SHALL also declare a value for the *commonName* attribute. The DN SHALL NOT contain any other attributes.

The Tier-2 CA SHALL verify that the combination of Subject DN attributes is unique across all the CA's subscribers, is meaningful according to section 3.1.2, and matches the real-world identity of the subscriber, including the appropriate value for the *domainComponent* attribute. If so, the Tier-2 CA SHALL register the DN attributes. The subscriber SHALL use the registered DN attributes in all certificate applications it subsequently sends to the respective CA.

Except for a Tier-2 CPS CA (see note in section 1.3.6), the *commonName* attribute of the DN will be different for all end entity certificates issued by a Tier-2 CA, unless the certificate results from a re-key request, see section 4.7. For that reason, other Tier-2 CAs SHALL not register a *commonName* attribute value.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The certificate applicant for a Tier-1 or Tier-2 CA certificate or an end entity certificate SHALL demonstrate that they hold the private key corresponding to the public key to be listed in the certificate.

The method to prove possession of a private key SHALL be the submission of a Certificate Signing Request (CSR), for instance a CSR complying with PKCS#10 (RFC 2986, [10]). This CSR SHALL be signed using the private key corresponding to the public key in the certificate. By verifying the signature using this public key, the CA can verify that the certificate applicant is indeed in possession of the corresponding private key.

[9] These values are specified in ISO 15118-2, Annex F, except for the values "MO" for a Contract certificate and "OEM" for an OEM Provisioning certificate. This document adds these values.

In case the key generation is performed under the CA's direct control (i.e., if both the CA and the certificate applicant are part of the PKI Operator), proof of private key possession is not required.

3.2.2 Authentication of organization identity

During the approval process of a subscriber for any of the CAs in the CharIN V2G PKI, as detailed in section 3.2.6, the party responsible for the approval SHALL

- validate that the subscriber exists, by using a third-party identity proofing service or trademark registration organization. If available, an official registry that is provided at national or international level SHALL be consulted.
- register the name and contact details (e-mail address, physical address and phone number(s)) of one or more contact person(s) at the subscriber. The approver SHALL validate the correctness of these contact details, for example by calling the registered phone number and/or sending an e-mail to the registered e-mail address.

When the new subscriber is approved, the party responsible for approval SHALL inform the CharIN V2G PKI Management Authority of this approval and SHALL provide the contact person(s) and associated contact details of the new subscriber. The CharIN V2G PKI Management Authority SHALL keep a registry of approved participants in the CharIN V2G PKI, registering at least their

- role in the PKI, for example Tier-2 CPO CA or Mobility Operator,
- superordinate CA,
- subscribers (only in case the participant is a CA),
- contact person(s) and contact detail(s).

3.2.3 Authentication of individual identity

3.2.3.1 Identification of authorized certificate applicants

When a CA within the CharIN V2G PKI is informed that a new subscriber to its services is approved, the CA SHALL contact the registered contact person (see section 3.2.2) at the new subscriber to obtain the name(s), identity document number(s) and contact details (e-mail address, physical address and phone number(s)) of the administrator(s) authorized by the subscriber to send certificate applications to the CA.

3.2.3.2 Authentication of authorized certificate applicants

For each of the authorized administrators of the subscriber, the CA SHALL set up a secure remote (i.e., online) communication channel, which SHALL identify the administrator and SHALL be protected by two-factor authentication and/or out-of-band authentication. For the CharIN V2G Root CA, a Tier-1 CA, and a Tier-2 CPS CA the authorized administrator SHALL use this channel to send certificate applications to the CA and to receive the response, as specified in chapter 4. For a Tier-2 CPO CA, a Tier-2 MO CA or a Tier-2 OEM Prov CA, authorized administrators MAY use this channel, but MAY also send certificate applications using the automated channel described in section 3.2.3.3.

When deciding which authenticator types to support for two-factor authentication, the CA SHOULD consider the 'Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2'[10]. However, the CA SHALL NOT support One-Time Passwords (OTP) sent via SMS as a (second) authentication factor for authenticating administrators.

3.2.3.3 Authentication of automated certificate applicants

In addition to the authorized communication channel for administrators, a Tier-2 CPO CA, a Tier-2 MO CA, or a Tier-2 OEM Prov CA SHALL set up a mutually authenticated communication channel or API, allowing a fully automated process for requesting and receiving certificates. This channel

[10] Available at https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf?retry=1

SHALL be protected using TLS v1.2 (RFC 5246) or later. The channel SHALL use TLS Server authentication based on digital certificates. The channel SHOULD use TLS Client authentication based on digital certificates. The associated digital public key certificate(s) SHALL be issued via a PKI separate from the CharIN V2G PKI.

If TLS Client authentication based on digital certificates is used, the Tier-2 CA SHALL bind the necessary private cryptographic key(s) and associated public key certificate(s) to a physical cryptographic secure token, such as a smart card. The physical secure token SHOULD have been certified according to Common Criteria, using a suitable Protection Profile such as BSI-CC-PP-0084-2014. The cryptographic keys on each secure token SHALL be unique. To activate and use the keys on the physical secure token, unique activation data such as a PIN or password SHALL be necessary. The Tier-2 CA SHALL validate that the token is in physical possession of the authorized administrator before accepting certificate applications with proof-of-possession of the cryptographic key(s) on that token. The Tier-2 CA SHALL collect evidence that the authorized administrator implements sufficient controls to prevent and detect unauthorized access to the token and its activation data, and also implements measures to replace the token reactively and proactively on a regular basis.

The Tier-2 CA MAY authenticate TLS Clients by means of strong credentials other than digital certificates, such as bearer access tokens. The Tier-2 CA SHALL generate strong bearer tokens with an appropriate Random Number Generator (RNG), and it SHALL securely distribute these to the relevant authorized administrator. The Tier-2 CA SHALL collect evidence that the administrator implements sufficient controls to prevent and detect unauthorized access to the bearer token, and measures to replace the token reactively and proactively on a regular basis. Client authentication based on bearer access tokens MAY be forbidden in future versions of this Certificate Policy.

The Tier-2 CA SHALL not authenticate clients by means of passwords.

In its Certification Practice Statement, each Tier-2 CA SHALL fully specify all details necessary for a subscriber to set up an automated communication channel and use it to send certificate applications to the CA and receive the signed certificates (or error messages, see section 4.2) in return. The CA SHALL communicate this specification to all of its approved subscribers.

3.2.3.4 Authentication of subscribers within a PKI Operator

If the V2G Root CA or a Tier-1 CA is part of the PKI Operator (see section 1.3.4), set-up of the secure and authorized remote communication channel(s) for subscribers, as described in section 3.2.3.2, is not mandatory. This is provided that the certificate applications are received from an adequately protected internal network domain of the PKI Operator.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

No stipulation.

3.2.6 Criteria for interoperation

3.2.6.1 Approval of Tier-1 or Tier-2 CAs

A Tier-1 or Tier-2 CA SHALL be approved before it is allowed to join the CharIN V2G PKI and to start operations. The V2G Root CA SHALL be responsible for approving a Tier-1 CA. The superordinate Tier-1 CA SHALL be responsible for approving a Tier-2 CA.

The V2G Root CA SHALL have documented processes for approving a Tier-1 CA that applies to become a subscriber to the Root CA. These processes SHALL guarantee the impartiality of any decision to approve or reject the Tier-1 CA, meaning that the criteria applied SHALL be equal for all Tier-1 CAs, whether or not they are part of the same organization as the Root CA.

A Tier-1 CA SHALL have documented processes for approving a Tier-2 CA that applies to become a subscriber to the Tier-1 CA. These processes SHALL guarantee the impartiality of any decision to approve or reject the Tier-2 CA. The criteria applied SHALL be equal for all Tier-2 CAs, whether or

not they are part of the same organization as the Tier-1 CA. The approval process of a Tier-1 CA for Tier-2 CAs SHALL be considered during the approval of the Tier-1 CA itself.

The approval process SHALL include:

- A confirmation by the Tier-1 or Tier-2 CA that they accept the latest version of CharIN V2G PKI Terms and Conditions, [11].
- A confirmation by the superordinate CA that the format of the Certificate Signing Requests generated by the Tier-1 or Tier-2 CA complies with all applicable requirements.
- A review of the Certification Practice Statement of the CA by a qualified person, to determine whether or not the contents of the Certification Practice Statement comply with the respective requirements in this CP.
- An audit by an independent assessor according to chapter 8 of this CP, to determine whether or not the CA is operating in accordance with the practices documented in its Certification Practice Statement and in any documents referenced therein.

The Tier-1 or Tier-2 CA SHALL be approved if the outcome of all of these steps is positive. This approval SHALL be valid indefinitely, provided that

- Any change in the Certification Practice Statement of the CA is approved by the party that approved the original Certification Practice Statement. This approval SHALL take place before the CA starts operating in accordance with the changed Certification Practice Statement.
- The outcome of repeat audits according to chapter 8 is positive.

Each approval decision SHALL be confirmed by the CharIN V2G PKI Management Authority and notification sent to the Irdeto CrossCharge Governance Board.

3.2.6.2 Approval of subscribers to Tier-2 CAs

As described in section 1.3.6, subscribers to Tier-2 CAs within the CharIN V2G PKI include Charging Point Operators, Certificate Provisioning Services, Mobility Operators, and OEMs of electric vehicles. Each of the subscribers SHALL write and maintain a Security Policy which describes the security practices of the subscriber with regard to cryptographic keys and certificates in the CharIN V2G PKI throughout their lifecycle.

Each subscriber to a Tier-2 CA SHALL be approved before being allowed to request the issuance of end entity certificates. The superordinate Tier-2 CA SHALL be responsible for approving a subscriber.

A Tier-2 CA SHALL have documented processes for approving a party that applies to become a subscriber to the Tier-2 CA. These processes SHALL guarantee the impartiality of any decision to approve or reject the subscriber. The criteria applied SHALL be equal for all subscribers, whether or not they are part of the same organization as the Tier-2 CA. The subscriber approval process of a Tier-2 CA SHALL be considered during the approval of the Tier-2 CA itself.

The approval process SHALL include:

- A confirmation by the subscriber that they accept the latest version of CharIN V2G PKI Terms and Conditions, [11].
- A confirmation by the Tier-2 CA that integration testing between their systems and the subscriber's systems, including a verification of the format of the CSRs created by the subscriber's systems, has been carried out successfully.
- A review of the Security Policy of the subscriber by a qualified person, to determine whether or not the security practices documented in that policy comply with the applicable requirements in this CP and in the latest version of the Security Requirements for Subscribers to the CharIN V2G PKI, [2].
- An audit by an independent assessor according to chapter 8 of this CP, to determine whether or not the subscriber is operating in accordance with the practices documented in its Security Policy and in any documents referenced therein.

The subscriber SHALL be approved if the outcome of all of these steps is positive. This approval SHALL be valid indefinitely, provided that

- Any change in the Security Policy of the subscriber is approved by the approving organization. This approval SHALL take place before the subscriber starts operating in accordance with the changed Security Policy.
- The outcome of repeat audits according to chapter 8 is positive.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

No stipulation. Once a secure and authenticated communication channel is set up according to section 3.2.3, it is not necessary to differentiate between initial and re-key requests.

3.3.2 Identification and authentication for re-key after revocation

No stipulation; see section 3.3.1.

3.4 Identification and authentication for revocation request

Revocation of a certificate issued by a CA within the CharIN V2G PKI MAY be requested by the parties identified in section 4.9.2.

If the subscriber that requested and received a particular certificate wants to revoke it, one of the subscriber's authorized administrators SHALL send a revocation request to the CA that issued the certificate. The administrator SHALL send the request using an authenticated communication channel set up according to section 3.2.3.

For Contract certificates specifically, the Tier-2 MO CA SHALL enable its subscribers (i.e., MOs) to send a revocation request using the automated interface described in section 3.2.3.3[11]. Other Tier-2 CAs SHOULD similarly enable automated certificate revocation requesting for their subscribers.

If another party in the CharIN V2G PKI wants to request a CA to revoke a particular certificate, it SHALL follow the process for revocation published by the CA (see section 2.2). The CA SHALL then contact that party's official contact person, registered according to section 3.2.2, to validate that the request is authentic. The CA SHALL NOT use any contact details contained in the revocation request itself.

If the CA does not know the official contact person and registered contact details of the relevant party, it MAY ask these from the CharIN V2G PKI Management Authority; see section 3.2.2. The CharIN V2G PKI Management Authority SHALL honor a request for these details if the request originates from a registered contact person of an approved participant in the CharIN V2G PKI.

[11] The reason for this requirement is the following: VDE-AR-E 2802-100-1, [8], section 12.1, requires MOs to provide a B2C interface for consumers to change or cancel their subscription, which will lead to the revocation of their Contract certificate. The MO CA must then be able to handle that revocation request in an automated fashion. The MO may also wish to revoke a Contract certificate automatically in case its validity period extends beyond the subscription period. A drawback of using revocation in these cases is that the CRL may become large. Therefore, MOs within the CharIN V2G PKI are free to deal with these business risks in any manner, and are not obliged to revoke Contract certificates under these circumstances. Another solution could be to use Contract certificates with a short duration. This will reduce the need for revocations, but increase the number of necessary certificate re-keys. It is up to each MO, in consultation with their Tier-2 MO CA, to design a solution that fits their business needs best.

4 Certificate life-cycle operational requirements

4.1 Certificate application

4.1.1 Who can submit a certificate application

Only the authorized administrators of an approved subscriber SHALL be entitled to submit a certificate application to an RA within the CharIN V2G PKI.

Since each CA in this PKI issues only one type of certificate, there is no need to register the type(s) of certificate each subscriber is allowed to request.

4.1.2 Enrolment process and responsibilities

Please refer to section 3.2.6 for the approval process of subscribers, and to section 3.2.3 for the registration of authorized administrators.

An RA SHOULD additionally require that the certificate applicant enter into a service agreement with the CA regarding the signing of certificates, and MAY require that payment for the requested certificate has been received or is guaranteed.

A certificate applicant SHALL only submit certificate applications that comply with the requirements in section 4.2.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

When receiving a certificate application, an RA within the CharIN V2G PKI SHALL verify that it was communicated over a secure channel set up according to section 3.2.3:

- In case of a request by an authorized administrator, the RA SHALL verify that the administrator is properly authenticated using two-factor and/or out-of-band authentication.
- In case of an automated request, the (Tier-2) RA SHALL perform TLS Client authentication as described in section 3.2.3.3.

4.2.2 Approval or rejection of certificate applications

The RA SHALL reject the certificate application if the conditions in section 4.2.1 are not fulfilled. In such a case, the RA MAY contact the applicant for clarification.

The RA SHALL verify that the algorithm and the domain parameters of the public key in the certificate application are consistent with the relevant certificate profile in section 7.1. The RA SHALL verify that the public key is consistent with the domain parameters.

The RA SHALL verify the proof-of-possession of the private key by the applicant using the method described in section 3.2.1.

The RA SHALL verify the correctness of the entire certificate application and the legitimacy of the information elements provided by the applicant for inclusion in the certificate (for example, via a Certificate Signing Request (CSR) compliant to PKCS#10 [10]), considering the role of the CA within the CharIN V2G PKI and the agreement between the CA and the subscriber.

The RA SHALL set the value and format of all fields in the to-be-signed certificate fields in accordance with the appropriate certificate profile in section 7.1. The RA MAY complete the to-be-signed certificate with information elements based on the agreement between the CA and the subscriber.

The RA SHALL set the Subject Distinguished Name (DN) of the to-be-signed certificate correctly:

- for the V2G Root RA and a Tier-1 RA: the Subject DN in the to-be-signed certificate SHALL be set identical to the Subject DN registered for the subscriber per section 3.1.5.1.
- for a Tier-2 RA: the fixed attributes in the Subject DN in the to-be-signed certificate SHALL be identical to the attributes registered for the subscriber per section 3.1.5.2. For a Tier-2 CPS CA,

this include the CommonName attribute. Any other Tier-2 RA SHALL copy the value of the CommonName attribute used by the certificate applicant in the application to the CommonName attribute in the to-be-signed certificate.

- If both the RA and the subscriber are part of the PKI Operator (see section 1.3.4), the CommonName attribute in the Subject DN in the to-be-signed certificate SHALL be set as follows[12]:
- For the V2G Root RA: "CharIN T1V1 CPO CA" , "CharIN T1V1 CPS CA", "CharIN T1V1 MO CA", or "CharIN T1V1 OEM Prov CA", as applicable given the role of the subscriber.
- For the Tier-1 CPO RA: "CharIN T2V1 CPO CA".
- For the Tier-1 CPS RA: "CharIN T2V1 CPS CA".
- For the Tier-1 MO RA: "CharIN T2V1 MO CA".
- For the Tier-1 OEM Prov RA: "CharIN T2V1 OEM Prov CA".

If the outcome of all validations is positive, the RA SHALL approve the certificate application and SHALL notify the associated CA of the approval. The RA SHALL make the to-be-signed certificate available to the associated CA.

If the outcome of any of the validations is negative or inconclusive, the RA SHALL reject the certificate application and SHALL communicate the reason(s) for the rejection to the certificate applicant.

4.2.3 Time to process certificate applications

Certification service levels guaranteed by the CA, such as availability, planned downtime, response times, maximum failure rates, maximum downtime after a failure, and business continuity, SHOULD be defined by appropriate Key Performance Indicators in the service agreement between the CA and the subscriber.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

After receiving to-be-signed certificate from the associated RA, a CA SHALL generate the requested certificate.

The following information SHALL be recorded in a database kept by the RA and/or the CA for each certificate application received:

- the complete certificate application, as sent by the certificate applicant,
- the certification decision (approval or rejection), and in case of rejection, the reasons for this,
- the complete resulting certificate, if any,
- timestamps of the reception of the certificate application, the generation of the certificate (if any) and the notification to the certificate applicant.

4.3.2 Notification to subscriber by the CA of issuance of certificates

If an authorized administrator (section 3.2.3.3) requested a certificate, the RA SHALL notify them once the certificate has been issued, and SHALL make the certificate available to them.

[12] T1" or "T2" in these CommonNames is short for 'Tier-1' or 'Tier-2', respectively. V1 indicates a certificate compliant with this CP. V2 indicates that the certificate is compliant with [7]; other versions are not supported.

If the certificate was requested in a fully automated fashion (section 3.2.3.3), notification of the subscriber is not required.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Upon receiving a certificate, the authorized administrator SHOULD validate the contents of the certificate with respect to the information provided in the certificate application. The subscriber SHOULD also verify the certificate as described in section 4.5.2 and SHOULD validate that the certificate format complies with the appropriate certificate profile in section 7.1.

If any of these verifications fail, the subscriber SHALL NOT install or use the certificate, but SHALL contact the CA. The CA SHALL investigate the issue and, if necessary, SHALL revoke the certificate according to section 4.9.

Installation and/or use of a certificate SHALL constitute the subscriber's acceptance of the certificate.

4.4.2 Publication of the certificate by the CA

Each CA in the CharIN V2G PKI SHALL publish all certificates it issues in a repository, except the self-signed Root CA certificates generated by the Root CA[13]. The repository containing the issued certificates SHALL be made available with restricted access.

4.4.3 Notification of certificate issuance by the CA to other entities

Notifying other entities is optional.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

A private key associated with a public key in a certificate issued by the Root CA or a Tier-1 CA within the CharIN V2G PKI SHALL only be used by the subscriber.

A private key associated with a public key in a certificate issued by a Tier-2 CA within the CharIN V2G PKI SHALL only be used by the end entity (see section 1.3.2.2) for which it is intended. In particular, a MO that generated a key pair for a Contract certificate SHALL NOT use the private key of this key pair for any purpose, but SHALL only send it to an EVCC, as specified in ISO 15118-2 and summarized in section 1.3.2.2.3.

There is one exception: In some cases, end-entity key pairs are generated by subscribers rather than the end-entities themselves. In such cases, the subscriber will use the private key for performing proof-of-possession to the Tier-2 CA during certificate application.

Moreover,

- The subscriber or end entity SHALL use the private key only for its respective purpose(s), as described in ISO 15118-2 [5].
- A CA private key SHALL NOT sign any certificates, possibly except OCSP Responder certificates, after its key usage period (specified in section 6.3.2) is over.
- An end entity private key SHALL NOT be used for any purpose after its key usage period is over.

4.5.2 Relying party public key and certificate usage

Before using or trusting a certificate, a relying party SHALL

[13]These are trust anchors rather than proper certificates.

- Verify the certificate validity using the basic path validation process described in Section 6.1 of RFC 5280.
- Check the revocation status of the certificate as specified in section 4.9.6.

The basic path validation process requires as input:

- One or more trust anchors, in the form of CharIN V2G Root CA certificates.
- A chain of intermediate CA certificates linking the target certificate to a trust anchor. The relying party SHALL validate each intermediate CA certificate as defined in this section.
- An appropriate estimate of the current date and time.

The relying party SHALL not use an expired CharIN V2G Root CA certificate (for which the *notAfter* date and time is in the past) as a trust anchor.

A relying party SHALL also verify that the *domainComponent* attribute is present in the *Subject* of all CA and end entity certificates and that it matches the relevant branch:

- "CPO" if the end entity certificate is a SECC certificate.
- "CPS" if the end entity certificate is a Certificate Provisioning Service certificate.
- "OEM" if the end entity certificate is an OEM Provisioning certificate.
- "MO" if the end entity certificate is a Contract certificate.

A relying party SHALL use any certificate issued by a CA in the CharIN V2G PKI in accordance with the requirements in section 1.4 of this policy.

If a relying party validated a certificate during a charging session, it SHALL continue to trust that certificate until the end of the session[14].

4.6 Certificate renewal

RFC 3647 [1] defines certificate renewal as the issuance of a new certificate to the subscriber without changing the public key or any other information, except the validity period, in the certificate.

Certificate renewal SHALL NOT be used for any certificate issued by a CA in the CharIN V2G PKI.

4.7 Certificate re-key

RFC 3647 [1] defines certificate re-key as the process in which the subscriber generates a new key pair and applies for the issuance of a new certificate that certifies the new public key. In a re-key request, the Subject DN is identical to the DN in a certificate previously signed by the CA.

There are three circumstances for certificate re-key:

- a currently valid certificate is about to expire,
- the usage period of the private key associated to a currently valid certificate is about to expire,
- a currently valid certificate was revoked; see section 4.9.

When the key usage period of a V2G Root CA private key (specified in section 6.3.2) is about to end, the V2G Root CA SHALL generate a new key root key pair and SHALL issue a new V2G Root CA certificate with the same Subject DN but an incremented generation value, as per section 7.1.3. This implies that the V2G Root CA MAY have multiple valid root certificates concurrently, whose validity periods overlap. In its Certification Practice Statement, the V2G Root CA SHALL specify precisely at which moments new root certificates will be generated.

As specified in section 6.3.2, the usage period of all other private keys used in the CharIN V2G PKI is equal to the validity period of the corresponding certificate. Prior to the expiration of a certificate, the subscriber that requested that certificate SHALL request a re-key of the certificate, to maintain operational continuity.

In addition, Tier-1 and Tier-2 CA's MAY, for operational reasons, use multiple private keys concurrently, with overlapping validity periods of the corresponding certificates. In its Certification

[14] In other words: if a certificate was valid at the beginning of the session, it remains trusted during the entire session, even if it expires during that session.

Practice Statement, each Tier-1 or Tier-2 CA SHALL specify how many CA certificates it will hold concurrently, and at which moments these certificates will be re-keyed.

A CA in the CharIN V2G PKI SHALL process a certificate re-key request in exactly the same manner as a certificate application (sections 4.1 - 4.3). However, if a subscriber sends a re-key request for a certificate that is expired, the CA SHOULD implement additional controls to verify the authenticity of the request and the reason(s) for which the subscriber allowed the original certificate to expire without timely sending a re-key request. Similarly, if a subscriber sends a re-key request for a certificate that has been revoked, the CA SHOULD implement additional controls to verify that the issues that necessitated the revocation of the original certificate have been resolved.

For CA certificates, these additional verifications SHALL take place before the CA issues the requested certificate. For end entity certificates, the CA MAY issue the certificate prior to doing these verifications.

4.8 Certificate modification

Certificate modification SHALL not be used in the CharIN V2G PKI.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A CA in the CharIN V2G PKI SHALL revoke a certificate it issued[15] if at least one of the following conditions is true:

- The subscriber rejected the certificate upon receiving it (see section 4.4.1).
- The CA receives an authenticated and legitimate request (see section 3.4) from a party authorized to order revocation of the certificate (see section 4.9.2).
- The CA determined that it issued the certificate in a manner not in accordance with the stipulations in this CP or in its own Certification Practice Statement.
- The CA determined that the private key associated with the certificate was compromised, or that valid reasons exist to suspect a compromise of the private key.
- The CA determined that the subscriber has lost control over the private key associated with a certificate. In case the private key is located in an EVCC or SECC, this includes cases of theft, malfunctioning, or destruction.

Revocation of a certificate SHALL be irreversible, even if the certificate was revoked for invalid reasons.

4.9.2 Who may request revocation

4.9.2.1 Revocation of Tier-1 or Tier-2 CA certificates

The following parties SHALL be authorized to order the revocation of a Tier-1 or Tier-2 CA certificate:

- The CharIN V2G Root CA,
- The CA that issued the certificate,
- The subscriber that requested and received the certificate.

Any other participant in the CharIN V2G PKI MAY request revocation of a Tier-1 or Tier-2 CA certificate, but the CA SHALL confirm that one of the circumstances listed in section 4.9.1 exists before revoking the certificate.

4.9.2.2 Revocation of end-entity certificates

The following parties SHALL be authorized to order the revocation of an end-entity certificate:

[15] A Root CA certificate cannot be revoked, since it is a trust anchor. Neither a CRL nor an OCSP Responder can be used to distrust a Root CA certificate, since the security of these mechanisms ultimately depends on the trust anchor itself.

- The CharIN V2G Root CA,
- The CA that issued the certificate,
- The subscriber that requested and received the certificate.

Any other participant in the CharIN V2G PKI MAY request revocation of an end entity certificate, but the CA SHALL confirm that one of the circumstances listed in section 4.9.1 exists before revoking the certificate.

4.9.3 Procedure for revocation request

Prior to the revocation of a certificate, a CA in the CharIN V2G PKI SHALL verify all the applicable conditions for authentication of the requestor listed in section 3.4 are fulfilled, and that that one of the circumstances listed in section 4.9.1 exists. Each CA SHALL describe a procedure for receiving, handling, and deciding upon revocation requests in its Certification Practice Statement.

4.9.4 Revocation request grace period

Once a (perceived) circumstance for revocation of a certificate arises, subscribers and other PKI participants SHALL submit a revocation request to the issuing CA as promptly as possible within a commercially reasonable time. Each CA in the CharIN V2G PKI SHALL specify a grace period in its Certification Practice Statement.

4.9.5 Time within which CA SHALL process the revocation request

After receipt of a revocation request, a CA withing CharIN V2G PKI SHALL process the request as promptly as possible within a commercially reasonable time. Each CA in the CharIN V2G PKI SHALL specify the maximum time for processing a request in its Certification Practice Statement. Additional requirements MAY be specified in the service agreement between a CA and the subscriber.

4.9.6 Revocation checking requirements for relying parties

A relying party SHALL verify the revocation status of any currently valid certificate issued by a CA within the CharIN V2G PKI.

In order of preference, the relying party SHALL assess:

- (Only for EVCCs): An OCSP response collected from the SECC during the TLS handshake, requested as specified in section 4.9.11.
- An OCSP response that has been locally cached for no longer than 1 week.
- (Only if the certificate has an Authority Information Access extension with access method id-ad-ocsp, and only if the relying party has connectivity): An OCSP response collected from the OCSP Responder. The relying party SHALL use the HTTP GET method.
- (Only if the certificate has a CRLDistributionPoints extension): A CRL that has been locally cached. The relying party SHOULD first update the CRL by collecting it from the CRL distribution point if it has connectivity.

The relying party SHALL ignore OCSP responses and CRLs outside of their validity periods.

The relying party SHALL accept the currently valid certificate if the collected OCSP response has the *certStatus* field set to '*good*'. For any other OCSP response, the relying party SHALL deem the certificate as revoked.

The relying party SHALL verify that the OCSP Responder certificate carried in the OCSP Response is valid and that the *ExtendedKeyUsage* extension asserts *OCSPSigning*, but it SHALL NOT check its revocation status, as the certificate uses the *id-pkix-ocsp-nocheck* extension; see section 7.1.

With reference to the VDE Implementation Guide [8] section 7.2, the requirements in this section imply that the 'shell model' is used for certificate validation within the CharIN V2G PKI, not the 'chain model'.

4.9.7 Revocation checking requirements for other PKI participants

A Contract certificate pool operator (see section 1.3.8.1) within the CharIN V2G PKI SHALL comply with all relevant requirements in VDE-AR-E 2802-100-1, [8], chapter 12, regarding checking of the revocation status of all certificates that are involved in the provisioning of a new Contract certificate. This includes the certificates in the MO, OEM Prov, and CPS branches.

An OEM Provisioning certificate pool operator (see section 1.3.8.2) SHALL regularly perform revocation checking of OEM Provisioning certificates it contains, and SHALL remove certificates that are revoked.

4.9.8 CRL issuance frequency

A CA within the CharIN V2G PKI SHALL regularly generate a new CRL as per its Certification Practice Statement, even if there are no changes made.

The CA SHALL ensure an adequate overlap period between each two consecutively generated CRLs, to avoid outages during the transition:

- The V2G Root CA SHALL generate a new CRL at least every 6 months with a minimum overlap period of 1 month.
- Tier-1 and Tier-2 CAs SHALL generate a new CRL at least every 4 weeks with a minimum overlap period of 2 weeks.
- Further, after the first year of operation, a Tier-2 CA SHALL generate a new CRL at least every 2 days, with a minimum overlap period of 5 days.

A CA SHALL generate a new CRL as soon as reasonably possible upon a revocation.

A CA SHALL not include in a CRL certificates that are expired at the moment of the generation.

Each CA in the CharIN V2G PKI SHALL mention the URI(s) at which it publishes its Certificate Revocation List for issued certificates in each issued certificate. The CRL SHALL be available to any party, without restrictions.

4.9.9 Maximum latency for CRLs

A CA SHALL publish a new CRL as soon as reasonably possible after its generation. The maximum time for processing and communication of a new CRL SHALL be defined in the Certification Practice Statement of each CA in the CharIN V2G PKI.

4.9.10 On-line revocation/status checking availability

The Tier-2 MO CA and the Tier-2 CPO CA within the PKI Operator (see section 1.3.4) SHALL operate an OCSP Responder, allowing relying parties to validate the revocation status of a Contract certificate or SECC certificate issued by the PKI Operator.

The V2G Root CA, the Tier-1 MO CA and Tier-1 CPO CA within the PKI Operator SHALL also operate an OCSP Responder. Other CAs in the CharIN V2G PKI MAY operate an OCSP Responder at their discretion[16].

If a CA operates an OCSP Responder, the CA SHALL mention the URI at which it maintains its OCSP Responder in each issued certificate. The OCSP Responder SHALL be available to any party, without restrictions.

4.9.11 On-line revocation checking requirements

See section 4.9.6.

[16] These requirements differ from the requirements regarding OCSP in ISO 15118-2:
-The certificate profiles in Annex F of ISO 15118-2 optionally allow any CA to have an OCSP Responder.
-However, at the same time there are requirements in the standard, such as [V2G2-070] and the note below it, that imply that the V2G Root CA and each Tier-1 CPO CA must operate an OCSP Responder, while a Tier-2 CPO CA must not operate an OCSP Responder.
-The standard does not contain any specific requirements regarding OCSP for other CAs.
Within the CharIN V2G PKI, the requirements regarding OCSP in ISO 15118-2 are replaced by the requirements in this section.

If one or more of the CAs within the CPO branch of the CharIN V2G PKI (see section 1.3.2.2) operates an OCSP Responder, a SECC SHALL provide all available OCSP responses during the TLS handshake, in response to a 'status_request' extension, in accordance with RFC 6066 (for TLS v1.2) or RFC 8446 (for TLS v1.3)[17]. The SECC SHOULD update and cache the OCSP responses at least once a week.

4.9.12 Other forms of revocation advertisements available

No stipulation.

4.9.13 Special requirements regarding key compromise

No stipulation. Revocation of a certificate because of a private key compromise SHALL not be handled differently than revocation for any other reason.

4.9.14 Circumstances for suspension

Certificate suspension is the temporary withdrawal from service of a certificate. Suspension SHALL not be supported for any certificate issued by a CA in the CharIN V2G PKI.

4.9.15 Who can request suspension

Not applicable, see above.

4.9.16 Procedure for suspension request

Not applicable, see above.

4.9.17 Limits on suspension period

Not applicable, see above.

4.10 Certificate status service

4.10.1 Operational characteristics

No stipulation.

4.10.2 Service availability

No stipulation.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

Subscription for the certification services of a CA within the CharIN V2G MAY end for multiple reasons, such as ending without renewal of the service agreement between the CA and the subscriber.

Certificates issued by a CA to a subscriber whose subscription is ended SHOULD NOT be revoked for this reason alone.

4.12 Key escrow and recovery

Key escrow and recovery SHALL NOT be used within the CharIN V2G PKI.

4.12.1 Key escrow and recovery policy and practices

Not applicable, see above.

[17] If a later TLS version is used, the respective RFC SHALL be used.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable, see above.

5 Physical, procedural and personnel security controls

5.1 Physical controls

5.1.1 Site location and construction

The location and construction of the facilities housing the CAs and RAs of the CharIN V2G PKI, as well as any site housing remote workstations used to administer the CAs and RAs, SHALL be appropriate for protecting high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high-security locks, and intrusion sensors, SHALL provide robust protection against unauthorized access to the CA and RA equipment and records.

The hardware security modules (HSMs) holding the CA private keys of each CA SHALL be housed in a dedicated secure area within these facilities, protected by a clearly defined security perimeter, with appropriate security barriers and entry controls to prevent unauthorized access, damage, and interference.

5.1.2 Physical access

All CAs and RAs within the CharIN V2G PKI SHALL provide continuous monitoring and alarm facilities to detect and register any unauthorized or irregular attempts to access its resources, and to react upon them in a timely manner.

Physical access to the dedicated secure area housing the CA equipment and the HSMs holding CA private keys SHALL be limited to personnel in trusted roles (see section 5.2.1). The CA SHALL ensure that either none or at least two trusted persons simultaneously are present in the secure area. Other individuals (including authorized security auditors and maintenance personnel) SHALL be escorted by two persons in a trusted role. All trusted persons and all organizations represented by the other individuals SHALL be recorded in the access log.

RA equipment SHALL be protected from unauthorized access during operation, while the HSM is activated. RAs SHALL implement physical access controls to reduce the risk of equipment tampering even when the HSM is not activated. These security mechanisms SHALL be commensurate with the level of threat in the RA equipment environment.

5.1.3 Power and air conditioning

Each CA or RA within the CharIN V2G PKI SHALL investigate the possible consequences of an interruption of electric power and air conditioning to its critical services. If necessary, the CA or RA SHALL install electrical power and air condition backup systems to mitigate any unacceptable consequences.

5.1.4 Water exposures

Each CA or RA within the CharIN V2G PKI SHALL take measures to minimize the risk of exposure to water of their critical systems, especially key management and certificate generation systems.

5.1.5 Fire prevention and protection

Each CA or RA within the CharIN V2G PKI SHALL take measures to minimize the risk of fire in the facilities housing their systems.

5.1.6 Media storage

Each CA or RA within the CharIN V2G PKI SHALL take measures to protect any storage media used to store confidential information, such as hard disks, smart cards and HSMs. Such storage media SHALL be protected against unauthorized or unintended use, access, disclosure, or damage, and against other threats such as fire and water.

Confidential information is defined in section 9.3.

Confidential information SHALL be protected to safeguard its confidentiality, integrity and availability when stored, when in use and when exchanged over networks. Confidential information that is deleted SHALL be permanently destroyed.

5.1.7 Waste disposal

Each CA or RA within the CharIN V2G PKI SHALL control waste disposal in such a way that the risk of compromise of confidential information is minimized. Information stored on digital media to be disposed SHALL be permanently destroyed.

5.1.8 Off-site backup

Each of the CAs within the CharIN V2G PKI SHALL use an off-site backup of all critical data, especially CA private keys, in order to ensure disaster recovery. In case of a complete loss of critical data at the regular production facilities, the critical data SHALL be fully recovered from the backup data. See also section 5.7.

Off-site backup locations SHALL offer at least the same level of security as the regular location. Only persons in trusted roles SHALL be able to access the backup data or restore this data to the regular production facilities, in accordance with the authorizations assigned to their role.

5.1.9 Internet access

Each CA or RA within the CharIN V2G PKI SHALL investigate the possible consequences of an interruption of internet access to their critical services. If necessary, they SHALL install internet access backup systems to mitigate any unacceptable consequences.

5.2 Procedural controls

5.2.1 Trusted roles

The Certification Practice Statement of each CA within the CharIN V2G PKI SHALL identify the trusted roles on which the security of its operations is dependent, as well as the responsibilities of each trusted role. These trusted roles SHALL be used in secure operating procedures. The trusted roles and their associated responsibilities and authorizations SHALL be defined from the viewpoints of separation of duties and least privilege and SHALL be documented in job descriptions.

People in trusted roles SHALL include all employees, contractors, and consultants that have access to, or control authentication or cryptographic operations that may affect:

- the validation of information in certificate applications,
- the acceptance, rejection, or other processing of certificate applications, revocation requests, or re-key requests,
- the issuance or revocation of certificates, including personnel having access to restricted portions of its repository or the handling of subscriber information or requests.

People having such access or privileges SHALL have been formally appointed to a trusted role by senior management of the respective organization prior to commencing their duties.

5.2.2 Number of persons required per task

Each CA within the CharIN V2G PKI SHALL identify in its Certification Practice Statement which tasks are considered critical and consequently need multiple-person control. For each critical task, the Certification Practice Statement SHALL list the trusted roles, and the number of persons in each trusted role, that are needed to carry out that task.

Critical tasks SHALL include at least:

- the generation or destruction of a private CA key,
- the issuing or revocation of a CA certificate.

5.2.3 Identification and authentication for each role

The systems of each CA and RA within the CharIN V2G PKI SHALL ensure effective user administration and access management. Access to critical systems SHALL be limited to individuals who are properly authenticated and authorized. Access to information and applications SHALL be

restricted, only allowing access to resources as necessary for carrying out the trusted role allocated to a user.

Two-factor authentication SHALL be used for the authentication of all users in trusted roles. When deciding which authenticator types to support for two-factor authentication, the CA SHOULD consider the 'Opinion of the European Banking Authority on the elements of strong customer authentication under PSD2'[18]. However, the CA SHALL NOT support One-Time Passwords (OTP) sent via SMS as a (second) authentication factor for authenticating administrators.

5.2.4 Roles requiring separation of duties

No single person SHALL be allowed to simultaneously assume more than one of the trusted roles identified according to section 5.2.1.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Each CA and RA within the CharIN V2G PKI SHALL properly train all personnel involved with the CharIN V2G PKI operations, and SHALL ensure they possess the knowledge, experience, and qualifications necessary for the services offered and appropriate to the job function.

Each CA and RA SHALL, for all personnel in trusted roles, have appropriate background screening with positive results. Detailed clearance requirements for personnel in trusted roles SHALL be provided in the Certification Practice Statement of the CA.

5.3.2 Background check procedures

Each CA and RA within the CharIN V2G PKI SHALL manage personnel appointment to trusted roles in accordance with a background screening process established in the Certification Practice Statement of the CA. Personnel in trusted roles SHALL have no conflicts of interest that might prejudice the impartiality of the CharIN V2G PKI operations.

5.3.3 Training requirements

Each CA and RA within the CharIN V2G PKI SHALL manage the training of personnel in trusted roles according to a training plan described in the Certification Practice Statement of the CA. Evidence of training attendance and training result SHALL be recorded and retained for each person in a trusted role.

5.3.4 Retraining frequency and requirements

Retraining of CA or RA personnel in trusted roles SHALL take place at regular intervals, documented in the Certification Practice Statement of the CA. Retraining SHALL take place at least in case of changes to documented policies, procedures, or operations. Evidence of training attendance and training result SHALL be recorded and retained for each person in a trusted role.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

CA and RA personnel in trusted roles SHALL be held accountable for their activities, which SHALL be logged in event logs as described in section 5.4. Possible consequences of unauthorized actions SHOULD be defined in personnel employment contracts.

[18] Available at https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/4bf4e536-69a5-44a5-a685-de42e292ef78/EBA%20Opinion%20on%20SCA%20elements%20under%20PSD2%20.pdf?retry=1

5.3.7 Independent contractor requirements

CAs and RAs within the CharIN V2G PKI MAY outsource tasks to a subcontractor, or personnel from independent contractors MAY be hired to carry out the responsibilities of the CA or RA. However, in such cases the personnel controls defined in this section 5.3 and in the Certification Practice Statement of the CA SHALL be maintained.

Each CA and RA SHALL retain responsibility for all aspects of the provisioning of its services as described in this policy, even if some functions are outsourced to subcontractors. Responsibilities of any subcontractors SHALL be clearly defined by the respective CA or RA, and appropriate arrangements SHALL be made to ensure that subcontractors are bound to implement any controls specified in this document.

5.3.8 Documentation supplied to personnel

CAs and RAs within the CharIN V2G PKI SHALL provide their personnel with up-to-date versions of the documentation necessary for carrying out their role. In its Certification Practice Statement, each CA or RA SHALL identify the documentation to be provided to each role.

5.4 Audit logging procedures

5.4.1 Types of events recorded

Each CA and RA within the CharIN V2G PKI SHALL automatically record and timestamp all significant security events in their CA and RA software in system log files.

In its Certification Practice Statement, each CA or RA SHALL identify the type of events to be recorded. This SHALL include at least the following events (where applicable):

- Successful and failed attempts to create, update, remove or retrieve status information about accounts of personnel, or to set or revoke the privileges of an account.
- Successful and failed attempts to set or change an authentication method (for instance a password, a biometric, or a cryptographic certificate) associated to a personal account.
- Successful and failed attempts to log-in and log-out on an account.
- Successful and failed attempts to change the software configuration.
- Software starts and stops.
- Software updates.
- System start-up and orderly shut-down.
- Successful and failed interactions with the database(s) containing data on critical processes, including connection attempts and read, write and update or removal operations.

In addition, the RA software SHALL log the following events (where applicable):

- Reception of a certificate application from a subscriber.
- Sending a to-be-signed certificate to the associated CA.
- Sending an issued certificate to a subscriber.

In addition, the CA software SHALL log the following events (where applicable):

- Reception of a to-be-signed certificate from the associated RA.
- Successful and failed attempts to process a to-be-signed certificate and sign a certificate. In case of failure, information on the error(s) or cause(s) of the failure.
- Successful and failed attempts to connect to or disconnect from an HSM.
- Successful and failed attempts to authenticate a user to an HSM.
- Successful and failed attempts to generate or destroy a key pair inside an HSM.
- Successful and failed attempts to import or export a private key to or from an HSM;
- Successful and failed attempts to change the life cycle state of a key pair;
- Successful and failed attempts to use a private key inside an HSM for any purpose.

In order to be able to investigate security incidents, where possible the system log SHALL include information allowing the identification of the person or account that initiated the events.

5.4.2 Frequency of processing log

5.4.2.1 Root CA, Tier-1 CAs, and RAs

Each Root CA and RA and Tier-1 CA and RA within the CharIN V2G PKI SHALL process audit event logs at least following an alarm or anomalous event, in order to establish its probable cause.

In addition, each CA and RA SHALL periodically process audit logs. These inspections SHALL take place within one month after the related activity occurred.

Audit log processing SHALL consist of a review of the audit logs, including a verification that the logs have not been tampered with, an inspection of all log entries, and an investigation of any alerts or irregularities in the audit logs. The CA or RA SHALL document any unexpected events in an audit log summary, and then SHALL investigate the reason for such unexpected events. The audit log summary SHALL be approved by the personnel involved.

The requirements in this section also apply to a Tier-2 RA or CA that does not use a fully automated process for receiving certificate applications and generating certificates (see section 3.2.3.3).

5.4.2.2 Tier-2 CAs

Each Tier-2 RA or CA within the CharIN V2G PKI that uses a fully automated process for receiving certificate applications and generating certificates (see section 3.2.3.3) SHALL automatically process audit events logs in real-time. Any alert or irregularity in the audit logs SHALL be notified immediately to the relevant personnel.

In addition, each Tier-2 CA and RA SHALL periodically process audit logs. These inspections SHALL take place within three months after the related activity occurred.

Audit log processing SHALL consist of a review of the audit logs, including a verification that the logs have not been tampered with, an inspection of all log entries, and an investigation of any alerts or irregularities in the audit logs. The CA or RA SHALL document any unexpected events in an audit log summary, and the SHALL investigate the reason for such unexpected events. The audit log summary SHALL be approved by the personnel involved.

5.4.3 Retention period for audit log

Each CA and RA in the CharIN V2G PKI SHALL store audit logs for at least five years.

In case applicable legal regulations require a longer or a shorter period of archival, the CA or RA SHALL comply with such regulations. In its Certification Practice Statement, each CA SHALL define the applicable requirements.

5.4.4 Protection of audit log

Each CA and RA within the CharIN V2G PKI SHALL maintain the integrity of system event logs during storage.

The Certification Practice Statement of the CA SHALL specify who (which role) is authorized to inspect, modify, or delete log files, and under what circumstances. Logs SHALL be protected from unauthorized inspection, modification, deletion, or destruction.

5.4.5 Audit log backup procedures

Each CA and RA within the CharIN V2G PKI SHALL back up and store its audit logs. Applicable procedures SHALL be described in the Certification Practice Statement.

5.4.6 Audit collection system (internal or external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessment

Each CA and RA within the CharIN V2G PKI SHALL perform vulnerability assessments of any software it uses on a regular basis, the frequency of which SHALL be specified in the Certification Practice Statement of the CA. Each CA or RA SHALL make a best effort to get informed of relevant known vulnerabilities, through vendor notifications, automated scanning, and audit activities.

The CA or RA SHALL assess each vulnerability that it is made aware of. The CA or RA SHALL determine and implement appropriate countermeasures in a timely manner, based on the level of risk arising from the vulnerability. The CA SHALL document possible risk levels and associated timelines in its Certification Practice Statement.

5.5 Records archival

5.5.1 Types of records archived

CAs and RAs SHALL archive at least:

- Contractual agreements within the CharIN V2G PKI context,
- Documents supporting the CA's approval and admission to the CharIN V2G PKI,
- Key ceremony reports (see section 6.1.1)
- Software and hardware configuration with relevant change logs,
- Their own CA certificates
- All CA certificates issued,
- All CA certificates revoked,
- All requests for revocation,
- Audit log summaries according to section 5.4.2,
- Audit reports according to chapter 8.

5.5.2 Retention period for archive

Each CA or RA SHALL retain all archived information until at least five years after it is terminated as a participant of the CharIN V2G PKI (see section 5.8). The CA or RA SHALL take measures to ensure that the record archive is stored in such a way that loss is reasonably excluded.

5.5.3 Protection of archive

Each CA and RA SHALL put in place measures and procedures to ensure that:

- Only persons in trusted roles can view the archive, in accordance with the authorizations assigned to their role.
- The availability, integrity, and confidentiality of archived records is protected.
- The archive is protected against storage media deterioration and (future) obsolescence of hardware, operating systems, and software.

5.5.4 Archive backup procedures

No stipulation. Each CA and RA SHALL document appropriate back-up and recovery procedures for all relevant data in its Certification Practices Statement.

5.5.5 Requirements for timestamping of records

Archived records SHALL be timestamped as necessary to ensure the usefulness of the archive.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

Each CA and RA SHALL document procedures to retrieve information from the archive and verify the correctness of such data.

5.6 Key changeover

Requirements regarding certificate re-key are specified in section 4.7. Each CA within the CharIN V2G PKI SHALL distribute the new certificate (containing the new public key) to its subscribers in the same way as the existing certificate; see sections 2.2 and 4.4.2.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling

Each CA and RA within the CharIN V2G PKI SHALL define procedures for handling security incidents and compromises in a Security Incident Response Plan.

If a security incident is suspected to have happened within the operations of a CA or RA, certificate issuance by that CA SHALL be stopped immediately and an investigation SHALL be performed in order to determine the nature and the degree of damage. The scope of potential damage SHALL be assessed in order to determine appropriate remediation procedures. If a CA private signing key is suspected of compromise, the procedures outlined in section 5.7.3 SHALL be followed.

The V2G Root CA SHALL notify the Irdeto CrossCharge Governance Board, and a Tier-1 or Tier-2 CA SHALL notify its superordinate CA, if any of the following has occurred:

- Suspected or detected compromise of any CA system,
- Physical or electronic penetration of any CA system,
- Successful denial of service attacks on any CA system.
- Notification SHALL occur within 24 hours after the incident.

5.7.2 Computing resources, software and/or data are corrupted

In its Certification Practice Statement, each CA within the CharIN V2G PKI SHALL outline the procedures for recovering a secure environment after computing resources are corrupted. As a last resort, this MAY include the invocation of the disaster recovery plan, according to section 5.7.4.

5.7.3 Entity private key compromise procedures

In its Certification Practice Statement, each CA SHALL specify recovery procedures to be used if a CA private key is compromised. In case of a confirmed compromise, the CA SHALL notify all of its subscribers within 24 hours, so that they can remove the CA certificate from their trust stores.

If the cause of the compromise can be adequately addressed, and it is determined that the CA system can be securely re-established, the CA SHALL

- request revocation of the CA certificate from its superordinate CA within 24 hours, if applicable.
- generate a new CA key pair,
- create a new CA certificate,
- solicit certificate applications from all of its subscribers,
- issue new certificates to replace all valid certificates signed with the compromised key, and
- distribute the new CA certificate.

5.7.4 Business continuity capabilities after a disaster

Each CA within the CharIN V2G PKI SHALL develop, test, and maintain a Business Continuity Plan, detailing how it will maintain its services in the event of a disaster. A disaster is any incident involving people, premises, hardware, software, information, or external services that would make it impossible to continue normal operations. In the Business Continuity Plan, the CA SHALL describe adequate measures it takes to

- if possible, avoid a disaster, for example by means of providing redundancy in staff, premises, hardware, information storage, or external services provisioning.
- if a disaster happens, limit its consequences.

In the Business Continuity Plan or in a separate Disaster Recovery Plan, the CA SHALL also describe its capabilities to ensure business continuity if a natural disaster would make it impossible to continue operations at the regular production facilities.

The Business Continuity Plan and/or the Disaster Recovery Plan SHALL specify values for the Recovery Time Objective and Recovery Point Objective for each of the critical services of the CA, in case a disaster happens.

The CA SHALL regularly test and, if necessary, update the Business Continuity Plan and the Disaster Recovery Plan.

5.8 Termination

5.8.1 Root CA or RA termination

In the event of termination of the current provider of the CharIN V2G Root CA or RA services, and if continuation of the CharIN V2G PKI is intended, any active subscriber or any consortia of active subscribers of the CharIN V2G PKI has a pre-emptive right to purchase the Root CA from Irdeto. If Irdeto intends to sell the Root CA, the Irdeto CrossCharge Governance Board shall be informed.

Upon the transfer of relevant assets to a new owner, Irdeto and the new owner SHALL collectively ensure that their availability, confidentiality, and integrity are maintained. The purchase agreement between Irdeto and the new owner SHALL specify which assets will be transferred, and how the transfer will take place.

5.8.2 Tier-1 or Tier-2 CA or RA termination

If continuation of the CharIN V2G PKI is intended, the Irdeto CrossCharge Governance Board SHALL ensure that at least one Tier-1 CA and RA and one Tier-2 CA and RA remains present for each of the CPO, CPS, MO, and OEM Prov branches in the CharIN V2G PKI.

In case there is only one provider of Tier-1 or Tier-2 CA or RA services within a particular branch and this service provider is terminated, the Irdeto CrossCharge Governance Board SHALL appoint a new service provider in its place. The service provider being terminated SHALL transfer all relevant assets to the new service provider or to the Irdeto CrossCharge Governance Board, while ensuring that their availability, confidentiality, and integrity are maintained. The service agreement between the Irdeto CrossCharge Governance Board and the provider of the Tier-1 or Tier-2 CA or RA services SHALL specify which assets will be transferred in case of termination, and how transfer will take place. The Tier-1 or Tier-2 CA or RA service provider being terminated SHALL ensure that potential disruptions to subscribers and relying parties due to the termination are minimized. In particular, certificates issued by the Tier-1 or Tier-2 CA SHOULD NOT be revoked because of the termination alone.

In case there are multiple Tier-1 or Tier-2 CA or RA service providers within a particular branch and one of these providers is terminated, it is up to the service provider being terminated whether or not to transfer its assets to a new provider. However, the service provider SHALL ensure that potential disruptions to subscribers and relying parties due to the termination are minimized.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

A CA within the CharIN V2G PKI SHALL generate its CA key pairs during an audited Key Generation Ceremony. The Key Generation Ceremony SHALL be documented, and a report of the ceremony SHALL be approved by attendants and archived according to section 5.5.

Key pair generation for CA keys SHALL take place in a hardware security module (HSM) complying with the requirements in section 6.2.1. The HSM SHALL be located in a physically secured environment complying with the requirements in section 5.1. The CA SHALL use publicly specified and appropriate cryptographic algorithms for key pair generation.

6.1.2 Private key delivery to subscriber

Key pairs SHALL be generated by the subscriber requesting certification of a public key from a CA within the CharIN V2G PKI. Consequently, there is no need for CAs to distribute private keys to subscribers.

6.1.3 Public key delivery to certificate issuer

The public key SHALL be delivered securely to the RA (e.g., using TLS with appropriate algorithms and key lengths). The channel shall bind the certificate applicant's identity (as described in section 4.2.2), the certificate application, and the public key.

6.1.4 CA public key delivery to relying parties

As specified in section 2.2, the CharIN V2G Root CA MAY publish its valid CA public keys in Root CA certificates on its website. A party relying on one of these public keys SHALL access the Irdeto website over TLS with a recognized browser relying on a WebTrust trust store[19], such that the authenticity of the website is ensured. In addition, the relying party MAY request a hash value or fingerprint of the root certificate from the Root CA using a second channel, such as an e-mail to the e-mail address registered in section 1.5.2.

Tier-1 and Tier-2 CAs SHALL distribute the CA certificates containing their public keys to their subscribers directly. In addition, Tier-1 and Tier-2 CAs MAY publish their CA certificates on their website, as specified in section 2.2. A party relying on any of these certificates SHALL verify the certificate using the certification path validation process in RFC 5280, using one of the (verified) V2G Root CA public keys as the trust anchor.

6.1.5 Key sizes

The ECC domain parameters of all keys generated or certified within the CharIN V2G PKI SHALL comply with the requirements in the appropriate certificate profile in section 7.1.

6.1.6 Public key parameters generation and quality checking

A subscriber to a CA within the CharIN PKI SHALL NOT generate any public key parameters when generating a key pair.

CAs SHALL perform public key parameter quality checking by verifying that the correct standardized ECC domain parameters are used in each certificate application, as per section 6.1.5.

6.1.7 Key usage purposes

A CA within the CharIN V2G PKI SHALL use the private key(s) corresponding to its certified CA public keys exclusively for signing certificates for its subscribers.

[19] See https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services

A subscriber to a Tier-2 CA SHALL use the private key(s) corresponding to its certified end entity public keys exclusive for the respective purpose(s) described in ISO 15118-2 [5].

These purposes are also reflected in the *KeyUsage* extension in the certificate profiles in section 7.1.

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

HSMs used in the CharIN V2G PKI SHALL

- be certified to EAL 4 or higher in accordance with ISO/IEC 15408 [11] (better known as Common Criteria) using a suitable Protection Profile; or
- meet the requirements in ISO/IEC 19790 [13] level 3; or
- meet the requirements in NIST FIPS PUB 140-2 [14] level 3; or
- meet the requirements in NIST FIPS PUB 140-3 [15] level 3; or
- offer a level of security deemed equivalent to the above by the CharIN PnC Europe Governance Board, possibly based on nationally or internationally recognized evaluation criteria for IT security.

CAs within the CharIN V2G PKI SHALL NOT perform any operations involving private keys, or secret keys derived or agreed upon using these keys, outside an HSM.

6.2.2 Private key escrow

Key escrow SHALL not be used for any private key in the CharIN V2G PKI.

6.2.3 Private key backup

In its Certification Practice Statement, each CA in the CharIN V2G PKI SHALL describe backup and restore procedures for its CA private keys. These secure operating procedures SHALL be appropriate to minimise the chance of loss of these keys, including as a result of a disaster.

Key backups SHALL be regularly verified to make sure that private keys can still be restored from them.

Any (unencrypted) copies of a CA private key in another HSM SHALL be subject to the same level of security controls as the key in use.

6.2.4 Private key archival

CA private keys in the CharIN V2G PKI SHALL NOT be archived.

6.2.5 Private key transfer into or from a cryptographic module

CA private keys within the CharIN V2G PKI SHALL be transferred between HSMs only for purposes of redundancy (e.g., high-availability clusters, fallback systems) or backup as described in section 6.2.3. When being transferred, a private key SHALL be wrapped (encrypted) prior to leaving the source HSM and SHALL be unwrapped only inside the destination HSM(s). Transport keys used for wrapping CA private keys SHALL be protected under multi-person control. A private key SHALL never exist in plaintext form outside the cryptographic module boundary.

6.2.6 Private key storage on cryptographic module

The HSM SHALL comply with the relevant requirements in the applicable standard for cryptographic modules (see section 6.2.1).

6.2.7 Method of activating private key

A CA private key SHALL be activated within an HSM before it can be used. Activation SHALL require the authentication of personnel in a trusted role (see section 5.2.1) towards the HSM.

Authentication SHALL use activation data. Activation data SHALL be protected from disclosure and SHOULD be protected by means of a smart card or other secure cryptographic hardware token.

6.2.8 Method of deactivating private key

After use, a CA private key SHALL be deactivated within an HSM, for instance via a secure wipe, manual logout or reset procedure or automatically after a period of inactivity, as defined in the Certification Practice Statement or Security Policy (as applicable). HSMs SHALL be removed and stored in a secure container when not in use.

6.2.9 Method of destroying private key

At the end of the certificate validity period of a private CA key (as specified in section 6.3.2), the CA SHALL destroy the private key. The CA SHALL also destroy any (backup) copies of the private key at that moment, if technically possible. If destruction of data in backups is not possible, the CA SHALL make sure that the private key is destroyed if and when the backup is restored to production.

6.2.10 Cryptographic module rating

See section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Each CA within the CharIN V2G PKI SHALL archive its own CA certificates and hence its public keys, in accordance with section 5.5. The Root CA and each Tier-1 CA SHALL also archive the CA certificates they have issued.

6.3.2 Certificate operational periods and key pair usage periods

Table 1 below show the validity periods for all certificate types in the CharIN V2G PKI.

Certificate type	Validity period
V2G Root CA	40 years Private key usage period: 10 years
Tier-1 CPO CA Tier-2 CPO CA SECC	20 years 10 years 90 days
Tier-1 MO CA Tier-2 MO CA Contract	20 years 10 years up to 2 years
Tier-1 CPS CA Tier-2 CPS CA Certificate Provisioning Service	20 years 10 years 5 years
Tier-1 OEM Prov CA Tier-2 OEM Prov CA OEM Provisioning	20 years 10 years 5 years
OCSP Responder	To be determined by the relevant CA based on a risk analysis; at most 1 year.

Table 1: Certificate validity periods and private key usage periods

A CA within the CharIN V2G PKI SHALL respect these validity periods when issuing certificates. Relying parties within the CharIN V2G PKI SHALL NOT use any certificate, or trust the public key in a certificate, after the certificate is expired. This SHALL include the V2G Root CA certificates; the public key in such a certificate SHALL NOT be used as a trust anchor after it is expired.

Private key usage periods within the CharIN V2G PKI SHALL be determined as follows:

- The private key usage period SHALL start when the validity period of the corresponding certificate starts.
- As shown in Table 1, the usage period of a V2G Root CA private key SHALL be 10 years.
- A Tier-1 or Tier-2 CA within the CharIN V2G PKI SHALL NOT use a CA private key to sign a certificate whose validity period extends beyond the validity period of the corresponding CA certificate. Consequently,
  - The usage period of a Tier-1 CA private key SHALL be maximum 10 years.
  - The usage period of a Tier-2 CPO CA private key SHALL be maximum 10 years minus 90 days.
  - The usage period of a Tier-2 MO CA private key SHALL be maximum 8 years[20].
  - The usage period of a Tier-2 CPS CA private key SHALL be maximum 5 years.
  - The usage period of a Tier-2 OEM Prov CA private key SHALL be maximum 5 years.
  - The usage period of a Tier-2 Vehicle CA private key SHALL be maximum 5 years.
- The key usage period of an end entity private key SHALL be equal to the validity period of the corresponding certificate.
- The key usage period of an OCSP Responder private key SHALL be equal to the validity period of the corresponding certificate.
- The key usage period of any private key SHALL end immediately when the corresponding certificate is revoked.

As pointed out in section 4.9.6, and referring to the VDE Implementation Guide [8] section 7.2, the requirements in this section imply that the 'shell model' is used for determining key usage periods and certificate validity periods within the CharIN V2G PKI, not the 'chain model'.

6.4 Activation data

6.4.1 Activation data generation and installation

Each CA within the CharIN V2G PKI SHALL describe in its Certification Practice Statement all credentials, such as passwords, PINs, authentication smart cards or other tokens, that are necessary to bring the HSM(s) containing the CA private key(s) in an operational state or to activate a private key for use.

The CA SHALL also document requirements regarding the length and complexity of these credentials, as well as regarding the trusted role responsible for generating them and the circumstances and frequency under which they must be changed. The CA SHALL document the secure operating procedures to be followed to set each of the credentials to their initial value and to change them.

All knowledge-based credentials SHALL be changed periodically, and at least whenever a person that is in possession of or has knowledge of that credential leaves their function or is assigned to another trusted role.

[20] In theory, a Tier-2 MO CA could be used after 8 years, provided the validity period of the Contract certificate it signs is shorter than 2 years and does not extend beyond the validity period of the CA certificate. However, this would require a case-by-case decision, which may lead to mistakes.

6.4.2 Activation data protection

Each CA in the CharIN V2G PKI SHALL describe the measures taken to protect the availability, confidentiality, and integrity of all activation data.

6.4.3 Other aspects of activation data

No stipulation

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

All CAs and RAs within the CharIN V2G PKI SHALL implement computer security controls to ensure secure operations, protect all sensitive information they store or process from unauthorized access or modification, and ensure system and data integrity. Each CA SHALL describe the specific technical security measures taken to harden their systems in its Certification Practice Statement. A proven system security checklist appropriate for the relevant operating system SHOULD be applied.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

Each CA and RA within the CharIN V2G PKI SHALL describe the practices and controls used during the development or sourcing of its systems. A risk analysis SHALL be carried out during the design and requirements specification of any systems development project, to ensure that an adequate level of security is built into the developed systems.

The functionality and security of hardware and software SHALL be tested properly before being taken into production.

6.6.2 Security management controls

Each CA and RA within the CharIN V2G PKI SHALL implement security management controls which include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures SHALL include checking the integrity of the security software, firmware, and hardware to ensure their correct operation. Each CA SHALL specify in its Certification Practice Statement the tools and procedures used for integrity checking, as well as the scope and frequency of such checks.

Each CA and RA SHALL implement mechanisms and policies for controlling and monitoring the integrity of their systems.

6.6.3 Life cycle security controls

Each CA and RA within the CharIN V2G PKI SHALL describe its policy regarding updates of hardware, operating systems, and software. Change control procedures SHALL be documented and used for releases, modifications and (emergency) software fixes for any operational software. Change procedures and security management procedures SHALL guarantee that the required security level is maintained in the Production systems.

In particular, a separation between Acceptance (or Pre-Production) and Production systems SHALL be maintained. Acceptance systems SHALL be technically equivalent to Production systems to the maximum intent possible, with the possible exception of capacity. Acceptance systems MAY be used to carry out testing, including acceptance testing and integration testing with the systems of issuing CAs and (potential) subscribers.

6.7 Network security controls

Each CA and RA within the CharIN V2G PKI SHALL document its network architecture, including the use of firewalls and IDS/IPS, if any. Each CA and RA SHALL design and implement its network architecture in such a way that access from the internet to their internal network domain, and from the internal network domain to the systems used to generate, manage and store cryptographic keys (including the HSMs), can be effectively controlled.

6.8 Time stamping

Each CA and RA within the CharIN V2G PKI SHALL use time information from a reliable source. Each CA SHALL describe in its Certification Practice Statement the source of time information, how often it is synchronized, and the verification of time used by the CA and the associated RA in case of unexpected changes.

7 Certificate, CRL, and OCSP profiles

7.1 Certificate profiles

7.1.1 Legend

The legend is identical to the legend within Annex F of ISO/IEC 15118-2. Most tables are laid out as in Annex F of ISO/IEC 15118-2, although field names and ASN.1 types are used according to RFC 5280.

Symbol	Meaning
X	Required value, specified according to RFC 5280.
(X)	Optional value, specified according to RFC 5280.
-	SHALL NOT be present
C	Critical. Unrecognized critical fields during certificate / trust path validation will result in a validation failure.
NC	Non-Critical. Unrecognized non-critical fields during certificate / trust path validation will **not** result in a validation failure.

7.1.2 Guidance

The following applies:

1. The *serialNumber* within any certificate SHALL consist of a non-negative number, encoded in no more than 20 octets, non-sequential, containing at least 64 bits of output from a CSPRNG.
2. The *signatureValue* SHALL be an ASN.1 BIT STRING. This is as specified in RFC 5280, but is different from ISO 15118-2, which erroneously specifies it as an Octet-String (where OCTET STRING is meant).
3. No CRL distribution point or OCSP Responder is made available to validate the V2G Root CA certificate.
4. The *authorityInformationAccess* extension contains information on the OCSP Responder. This extension is shown as optional in all (non-Root CA) certificate profiles. However, the requirements in section 4.9.10 apply. The *authorityInformationAccess* – if present – SHALL contain a single *accessDescription* entry which indicates the OCSP protocol in the *accessMethod* and contains the URL in the *accessLocation*.
5. The *digitalSignature* bit in the *KeyUsage* extension of the OCSP certificate profile has been set, to make sure that the certificate can be used to sign OCSP responses. This is a change from the ISO 15118-2 standard.
6. The *authorityKeyIdentifier* extension does not include the optional *authorityCertIssuer* and *authorityCertSerialNumber* fields.
7. The *domainComponent* values "CPO", "CPS", "MO" or "OEM" are used not just for end entity certificates, but also for the issuing CA certificates, both in the Issuer and in the Subject fields. This deviates from ISO 15118-2, as in that standard the Issuer and Subject fields may differ regarding the presence or absence of the *domainComponent*, which by definition would mean that the trust path cannot be constructed, and certificate validation would fail.
8. It is expected that the actual key usage may be a subset of the key usages specified within the certificate profiles as defined in ISO 15118-2 – for instance *keyEncipherment* may go unused.
9. The *cRLDistributionPoints* – if present – SHALL contain one *distributionPointName* element which in turns contains a *fullName* with the URL to the distribution end point;
10. If there is a choice of string type for a field, the string type *UTF8String* SHALL be used.

11. The *publicKey* field in subjectPublicKeyInfo SHALL be an ASN.1 BIT STRING containing the uncompressed encoding of the public key. Uncompressed encoding means[21] that the value starts with a byte 0x04 indicating that uncompressed encoding is used, followed by the x and y coordinates of the public point.
12. The value of the *keyIdentifier* (within the *keyIdentifier* and *authorityKeyIdentifier* fields) SHALL be the 160-bit SHA-1 hash of the value of the BIT STRING *subjectPublicKey*, excluding the tag, length, and number of unused bits, but including the encoding indicator byte 0x04.
13. Requirement [V2G2-010] in ISO 15118-2 stipulates that the size of a certificate in DER encoded form shall not be bigger than 1600 bytes. This requirement is not mandated for certificates in the CharIN V2G PKI.
14. The Validity fields SHALL be encoded as a *UTCTime* or *GeneralizedTime* type, according to the rules in section 4.1.2.5 of RFC 5280.
15. The *basicConstraints* extension field in end entity certificates is optional. It should be noted that ISO 15118-2 mandates that the *basicConstraints* field is present. However, according to RFC 5280, the absence of this field is equivalent to having CA=false set within the extension. If the extension is present in end entity certificates, then it SHALL be marked as critical and it SHALL have CA=false.

7.1.3 V2G Root CA certificate profile

Branch	**V2G Root**	
Name	**V2G Root**	
Type	**Root certificate**	
Field	**Sub-field**	**Value**
tbsCertificate	version	2
	serialNumber	see section 7.1.2.
issuer	countryName	-
	organizationName	"CharIN e. V."
	organizationalUnitName	-
	commonName	"CharIN V2G Root CA G#V1" (see note below this table)
	domainComponent	"V2G" (see note below this table)
validity	notBefore/notAfter	see section 6.3.2
subject	see issuer	
subjectPublicKeyInfo	algorithm	1.2.840.10045.2.1 (id-ecPublicKey)
	parameters	1.2.840.10045.3.1.7 (secp256r1)
	publicKey	see section 7.1.2.
extensions	authorityKeyIdentifier	X, NC
	subjectKeyIdentifier	X, NC
	keyUsage	keyCertSign, cRLSign, C

[21] It is specified, among others, in BSI TR 03111.

	extendedKeyUsage	-
	certificatePolicies	(X), NC
	basicConstraints	X, C
	cA	true
	pathLen	-
	cRLDistributionPoints	-
	authorityInformationAccess	-
signatureAlgorithm	algorithm	1.2.840.10045.4.3.2 (ecdsa-with-SHA256)
signatureValue		BIT STRING with a DER encoded X9.62 representation of the r and s values

Notes on Issuer and Subject values:

- The *commonName* specified above contains a #, which indicates the certificate generation and SHALL be replaced by a consecutive number indicating the generation of the Root CA certificate. "V1" in the *commonName* indicates that the certificate complies with this CP; see also section 4.2.2.
- For instance, the *commonName* used in the first Root CA certificate issued by CharIN will be "CharIN V2G Root CA G1V1". The second Root CA certificate will have *commonName* "CharIN V2G Root CA G2V1", etc.
- The *domainComponent* is put as the last RDN in the Issuer and Subject. Although slightly odd given standard conventions, this is in accordance with ISO 15118-2.

7.1.4 CPO certificate profiles

7.1.4.1 Tier-1 CPO CA certificate profile

Branch	**CPO**	
Name	**CPO Sub 1**	
Type	**Sub CA**	
Field	**Sub-field**	**Value**
tbsCertificate	version	2
	serialNumber	see section 7.1.2.
issuer		subject of V2G Root CA, see section 7.1.3
validity	notBefore/notAfter	see section 6.3.2
subject		see section 3.1.5.1
subjectPublicKeyInfo	algorithm	1.2.840.10045.2.1 (id-ecPublicKey)
	parameters	1.2.840.10045.3.1.7 (secp256r1)
	publicKey	see section 7.1.2

extensions	authorityKeyIdentifier	X, NC
	subjectKeyIdentifier	X, NC
	keyUsage	keyCertSign, cRLSign, C
	extendedKeyUsage	-
	certificatePolicies	(X), NC
	basicConstraints	X, C
	cA	true
	pathLen	1
	cRLDistributionPoints	X, NC
	authorityInformationAccess (OCSP)	(X), NC
signatureAlgorithm	algorithm	1.2.840.10045.4.3.2 (ecdsa-with-SHA256)
signatureValue		BIT STRING with a DER encoded X9.62 representation of the r and s values

7.1.4.2 Tier-2 CPO CA certificate profile

Branch	**CPO**	
Name	**CPO Sub 2**	
Type	**Sub CA**	
Field	**Sub-field**	**Value**
tbsCertificate	version	2
	serialNumber	see section 7.1.2.
issuer		subject of issuing CA certificate
validity	notBefore/notAfter	see section 6.3.2
subject		see section 3.1.5.1
subjectPublicKeyInfo	algorithm	1.2.840.10045.2.1 (id-ecPublicKey)
	parameters	1.2.840.10045.3.1.7 (secp256r1)
	publicKey	see section 7.1.2.
extensions	authorityKeyIdentifier	X, NC
	subjectKeyIdentifier	X, NC
	keyUsage	keyCertSign, cRLSign, C
	extendedKeyUsage	-
	certificatePolicies	(X), NC
	basicConstraints	X, C
	cA	true
	pathLen	0
	cRLDistributionPoints	X, NC

	authorityInformationAccess (OCSP)	(X), NC
signatureAlgorithm	algorithm	1.2.840.10045.4.3.2 (ecdsa-with-SHA256)
signatureValue		BIT STRING with a DER encoded X9.62 representation of the r and s values

7.1.4.3 SECC certificate profile

Branch	**CPO**	
Name	**SECC**	
Type	**End Entity**	
Field	**Sub-field**	**Value**
tbsCertificate	version	2
	serialNumber	see section 7.1.2
issuer		subject of issuing CA certificate
validity	notBefore/notAfter	see section 6.3.2
subject		see section 3.1.5.2
subjectPublicKeyInfo	algorithm	1.2.840.10045.2.1 (id-ecPublicKey)
	parameters	1.2.840.10045.3.1.7 (secp256r1)
	publicKey	see section 7.1.2
extensions	authorityKeyIdentifier	X, NC
	subjectKeyIdentifier	X, NC
	keyUsage	digitalSignature, C
	extendedKeyUsage	-
	certificatePolicies	(X), NC
	basicConstraints	(X), C
	cA	false
	pathLen	-
	cRLDistributionPoints	X, NC
	authorityInformationAccess (OCSP)	(X), NC
signatureAlgorithm	algorithm	1.2.840.10045.4.3.2 (ecdsa-with-SHA256)
signatureValue		BIT STRING with a DER encoded X9.62 representation of the r and s values

7.1.5 CPS certificate profiles

7.1.5.1 Introduction

This section specifies the CPS certificate profiles[22] by marking the differences with the profiles specified for the CPO certificates in section 7.1.4.

7.1.5.2 Tier-1 CPS CA certificate profile

This certificate profile is identical to the Tier-1 CPO CA certificate profile specified in section 7.1.4.1.

7.1.5.3 Tier-2 CPS CA certificate profile

This certificate profile is identical to the Tier-2 CPO CA certificate profile specified in section 7.1.4.2.

7.1.5.4 Certificate Provisioning Service certificate profile

This certificate profile is identical to the SECC certificate profile specified in section 7.1.4.3.

7.1.6 MO certificate profiles

7.1.6.1 Introduction

This section specifies the MO certificate profiles by marking the differences with the profiles specified for the CPO certificates in section 7.1.4.

7.1.6.2 Tier-1 MO CA certificate profile

This certificate profile is identical to the Tier-1 CPO CA certificate profile specified in section 7.1.4.1.

7.1.6.3 Tier-2 MO CA certificate profile

This certificate profile is identical to the Tier-2 CPO CA certificate profile specified in section 7.1.4.2, with the following differences:

- the *nonRepudiation* bit, the *keyCertSign* and the *cRLSign* SHALL be set for *KeyUsage*, in addition to the *digitalSignature* bit[23].

Note that the ISO/IEC 15118-2 standard indicates that this could be either a sub-CA or an end entity certificate; in the CharIN V2G PKI it is a CA certificate, since a Tier-2 MO CA does not sign Sales Tariffs, see section 1.3.3.

7.1.6.4 Contract certificate profile

This certificate is identical to the SECC certificate specified in section 7.1.4.3, except for the following:

- The nonRepudiation, keyEncipherment and keyAgreement bits are set for KeyUsage, in addition to the digitalSignature bit[24].
- *KeyUsage* remains a critical extension.

[22] Table F.3 in ISO 15118-2 calls these 'Certificate Installation Service Certificates (Provisioning)' profiles
[23] Within the CharIN V2G PKI, a Tier-2 MO CA certificate is not used for non-repudiation, but ISO 15118-2 requires setting this bit.
[24] Within the CharIN V2G PKI, a Contract certificate is not used for non-repudiation, key encipherment or key agreement. In particular, as specified in section 1.3.2.2.3, an (existing) Contract certificate SHALL NOT be used for key agreement to encrypt a (new) Contract certificate during transport between an MO and an EVCC. However, ISO 15118-2 requires setting these bits.

7.1.7 OEM Provisioning certificate profiles

7.1.7.1 Introduction

This section specifies the OEM Provisioning certificate profiles by marking the differences with the profiles specified for the CPO certificates in section 7.1.4.

7.1.7.2 Tier-1 OEM Prov CA certificate profile

This certificate profile is identical to the Tier-1 CPO CA certificate profile specified in section 7.1.4.1.

7.1.7.3 Tier-2 OEM Prov CA certificate profile

This certificate profile is identical to the Tier-2 CPO CA certificate profile specified in section 7.1.4.2.

7.1.7.4 OEM Provisioning certificate profile

This certificate is identical in structure with the SECC certificate profile specified in section 7.1.4.3, with the following differences:

- The *keyAgreement* and *keyEncipherment* bits are set for Key Usage, in addition to the *digitalSignature* bit.

7.2 CRL profiles

7.2.1 Body and tbsCertList

CertificateList		
Field	**Sub-field**	**Value**
version		1 (v2)
signature	algorithm	ecdsa-with-SHA256
	parameters	secp256r1
issuer		subject of issuing CA certificate
thisUpdate		X, see section 4.9.8
nextUpdate		
revokedCertificates	see section 7.2.2	
crlExtensions	see section 7.2.3	
signatureAlgorithm	algorithm	ecdsa-with-SHA256
	parameters	secp256r1
signatureValue		BIT STRING with a DER encoded X9.62 representation of the r and s values

7.2.2 RevokedCertificates

revokedCertificates is an ASN.1 SEQUENCE containing the fields in the table below.

RevokedCertificates		
Field	**Sub-field**	**Value**
userCertificate		serial number

revocationDate		X
cRLEntryExtensions	reasonCode	(X)
	invalidityDate	(X)
	certificateIssuer	-

7.2.3 CRL Extensions

crlExtensions is an ASN.1 SEQUENCE containing the fields in the table below.

Extensions		
Field	**Sub-field**	**Value**
authorityKeyIdentifier		X
	keyIdentifier	X
	authorityCertIssuer	-
	authorityCertSerialNumber	-
IssuerAlternativeName		-
cRLNumber		sequential number
deltaCRLIndicator		-
issuingDistributionPoint	distributionPoint	(X), C
	onlyContainsUserCerts	-
	onlyContainsCACerts	-
	onlySomeReasons	-
	indirectCRL	-
	onlyContainsAttributeCerts	-
freshestCRL		-
authorityInformationAccess		-

7.3 OCSP Responder certificate profile

The OCSP Responder certificate profile is specified in the ISO/IEC 15118-2 standard. An OCSP Responder certificate is required to be based on the same secp256r1 Elliptic Curve parameters. An OCSP Responder certificate is used during the revocation status check of certificates issued by the CA that operates the OCSP Responder. It SHALL be signed by the key pair of that CA.

Branch	**Any**	
Name	**OCSP Responder**	
Type	**End entity OCSP Responder**	
Field	**Sub-field**	**Value**
tbsCertificate	version	2
	serialNumber	see section 7.1.2
issuer		subject of issuing CA certificate
validity	notBefore/notAfter	see section 6.3.2

subject		CommonName SHALL be present and SHALL make clear that this is an OCSP Responder certificate. OrganizationName SHALL be present and SHALL clearly identify the real-world identity of the OCSP Responder CountryName, DomainComponent and organizationalUnitName MAY be present.
subjectPublicKeyInfo	algorithm	see section 7.1.2
	parameters	see section 7.1.2
	publicKey	Uncompressed point representation public key
extensions	authorityKeyIdentifier	
	subjectKeyIdentifier	
	keyUsage	
	extendedKeyUsage	1.3.6.1.5.5.7.3.9 (OCSPSigning), C
	certificatePolicies	(X), NC
	basicConstraints	X, C
	cA	false
	pathLen	-
	cRLDistributionPoints	-
	authorityInformationAccess	-
	id-pkix-ocsp-nocheck	NULL, NC
signatureAlgorithm	algorithm	see section 7.1.2
	parameters	see section 7.1.2
signatureValue		BIT STRING with a DER encoded X9.62 representation of the r and s values

The non-critical extension *id-pkix-ocsp-nocheck* is required for OCSP Responder certificates.

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

8.1.1 CAs and RAs within the Irdeto CharIN V2G PKI

All CAs and RAs operating under this CharIN V2G PKI certificate policy SHALL be audited for conformance with this Certificate Policy regularly. The first full and formal audit SHOULD be performed before a CA starts issuing certificates. The Irdeto CrossCharge Governance Board reserves the right to allow a CA to start issuing certificates if the CA commits to achieve, within the first year of operation, the required level of compliance (see section 1.3.3). Subsequently, an audit SHALL take place at least once every 36 months. If an audit finds evidence of nonconformity, the next audit SHALL be performed within 12 months.

An audit SHALL verify the CA's and RA's compliance with the applicable requirements in this policy, as well as with their own Certification Practice Statement and other internal documentation.

The CA or RA that will be audited SHALL plan and (let) conduct the audit, in consultation with the approving organization (see section 3.2.6).

8.1.2 Subscribers to Tier-2 CAs

All subscribers to Tier-2 CAs SHALL be audited regularly for conformance with this Certificate Policy and with the latest version of the Security Requirements for Subscribers to the CharIN V2G PKI, [2]. The first full and formal audit SHALL be performed before the subscriber is allowed to send certificate applications to its superordinate Tier-2 CA. Subsequently, an audit SHALL take place at least once every 36 months. If an audit finds evidence of nonconformity, the next audit SHALL be performed within 12 months.

The audit SHALL verify the subscriber's compliance with the applicable requirements in the abovementioned documents, as well as with their own Security Policy and other internal documentation.

The Tier-2 CA subscriber that will be audited SHALL plan and (let) conduct the audit, in consultation with the approving organization (see section 3.2.6).

8.2 Identity/qualifications of assessor

Auditors SHALL comply with the following requirements:

- Ethical behavior - trustworthiness, uniformity, confidentiality regarding their relationship to the organization to be audited and when handling its information and data.
- Fair presentation - findings, conclusions and reports from the audit are true and precisely describe all the activities carried out during the audit.
- Professional approach - has a high level of expertise and professional competency and makes effective use of its experience gained through good and deep-rooted practice in information technologies, PKI and the related technical norms and standards.

The auditor SHALL possess significant knowledge and expertise of, and preferably be accredited for:

- Performance of information system security audits.
- PKI and cryptographic technologies.
- The CharIN V2G PKI, the ecosystem in which it operates, and the role of the audited party within the PKI and the ecosystem.

8.3 Assessor's relationship to assessed entity

The auditor SHALL be independent of and not connected to the organization being the subject of the audit.

8.4 Topics covered by assessment

8.4.1 CAs and RAs

Each CA and RA audit SHALL cover compliance to this Certificate Policy, the CA's Certification Practice Statement and the associated procedures and techniques documented by the CA.

The scope of the compliance audit SHALL be the implementation of the technical, procedural and personnel practices described in these documents. Some areas of focus for the audits SHALL be:

- Identification and authentication operations (chapter 3).
- Operational functions/services (chapter 4).
- Physical, procedural and personnel security controls (chapter 5).
- Technical security controls (chapter 6).

During the audit, the auditor SHALL assess the audit logs (see section 5.4) to determine whether weaknesses are present in the security of the systems of the organization to be audited. Determined (possible) weaknesses SHALL be mitigated. The assessment and possible weaknesses SHALL be recorded.

8.4.2 Subscribers to Tier-2 CAs

Each audit for a subscriber to a Tier-2 CA SHALL cover compliance to this Certificate Policy, the latest version of the Security Requirements for Subscribers to the CharIN V2G PKI, [2], the subscriber's Security Policy and the associated procedures and techniques documented by the subscriber. The scope of the compliance audit SHALL be the implementation of the technical, procedural and personnel practices described in these documents.

During the audit, the auditor SHALL assess the audit logs (see section 5.4) to determine whether weaknesses are present in the security of the systems of the organization to be audited. Determined (possible) weaknesses SHALL be mitigated. The assessment and possible weaknesses SHALL be recorded.

8.5 Actions taken as a result of deficiency

The auditor SHALL deliver an audit report for each audit to the approving organization (see section 3.2.6). If irregularities are found in an audit, the audit report SHALL define corrective actions, including an implementation schedule. The audited organization SHALL carry out these corrective actions according to this schedule.

Upon the receipt of an audit report, the approving organization SHALL take appropriate action, depending on the severity of the findings. Actions MAY include termination of the audited organization, if the irregularities are severe and the audited organization does not succeed in solving these issues. Termination is described in section 5.8. Termination for this reason SHALL be confirmed by the Irdeto CrossCharge Governance Board.

8.6 Communication of results

The approving organization SHALL provide a summary of the audit report, in English, to the Irdeto CrossCharge Governance Board. This summary SHALL include at least the number of deviations found and the nature of each deviation.

9 Other business and legal matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees

Governed in separate mutual agreements.

9.1.2 Certificate access fees

Governed in separate mutual agreements.

9.1.3 Revocation or status information access fees

Governed in separate mutual agreements.

9.1.4 Fees for other services

Governed in separate mutual agreements.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

9.2.1 Insurance coverage

Each CA in the CharIN V2G PKI SHALL have adequate arrangements to cover liabilities arising from their operations and/or activities.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Confidential information SHALL include at least:

- private keys,
- audit logs (see section 5.4),
- passwords, PINs, activation data (see section 6.4), etc.
- detailed secure operating procedures and other documents regarding system management and security controls.
- any other information not explicitly deemed public (see section 9.3.2)

9.3.2 Information not within the scope of confidential information

The following information is public:

- information included in public key certificates,
- CRLs and OCSP responses,
- this Certificate Policy.

9.3.3 Responsibility to protect confidential information

Confidential information SHALL NOT be released by any PKI participant, unless a legal obligation exists to do so.

9.4 Privacy of personal information

9.4.1 Privacy plan

Each CA in the CharIN V2G PKI SHALL treat all personal information according to the applicable regional regulatory statutory requirements. Appropriate technical and organizational measures SHALL be taken to prevent unauthorized or unlawful processing of personal data and to prevent accidental loss or destruction of, or damage to, personal data.

9.4.2 Information treated as private

Personally identifiable information, contact information, and authorizations of CA staff are private.

Personally identifiable or corporate information and contact information of subscribers that does not appear in a certificate issued by the CA, is private.

9.4.3 Information not deemed private

The following personal information is not deemed private:

- information included in public key certificates issued by the MSCA.

9.4.4 Responsibility to protect private information

See section 9.4.1.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

No stipulation.

9.6 Representations and warranties

No stipulation.

9.6.1 CA representations and warranties

No stipulation.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

No stipulation.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

This Certificate Policy is valid from the moment it is published by the Irdeto CrossCharge Governance Board on the website indicated in section 1.5.2.

9.10.2 Termination

This Certificate Policy is valid until it is replaced by the Irdeto CrossCharge Governance Board.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedures for amendment

This Certificate Policy is issued under responsibility of the Irdeto CrossCharge Governance Board. The Governance Board may revise this document if it deems this necessary. It is allowed to make editorial or typographical corrections to this policy without notification to the PKI participants, and without an increase in version number. It is allowed to change the contact information in section 1.5 with notification to the PKI participants, but without change to the document version number.

For all other changes of this document, the procedure for change proposals and approvals SHALL be as follows:

1. Any PKI participant MAY, at any time, submit proposals for change to this Certificate Policy to the Irdeto CrossCharge Governance Board.
2. The Governance Board SHALL distribute any proposal to change the Certificate Policy to all PKI participants.
3. PKI participants MAY comment on the proposed changes within 15 days of change proposal notice.
4. The Governance Board SHALL consider the comments and SHALL decide which, if any, of the notified changes to implement.
5. The Governance Board SHALL notify the PKI participants about its decision.
6. The Governance Board SHALL publish a new version of this Certificate Policy, including all implemented changes, accompanied by an increase in the version number of the document.
7. The Governance Board SHALL set an appropriate period for the changes to be implemented. Any item in this policy MAY be changed with 90 days' notice. Changes to items that, in the judgment of the Irdeto CrossCharge Governance Board, will not materially impact a substantial majority of the users or relying parties using this policy MAY be changed with 30 days' notice.
8. Each PKI participant SHALL determine the changes that must be made to its documentation, systems, and processes as a result of the changed Certificate Policy, and SHALL implement these changes within the implementation period set.

9.12.2 Notification mechanism and period

See the previous section.

9.12.3 Circumstances under which OID must be changed

The OID for this CP is specified in section 1.2. The value of the last digit ('arc') SHALL be increased by 1 for every new version (with increased version number) that is published by Irdeto.

For instance, if Irdeto publishes version 1.1 of this CP, the corresponding OID will be 1.3.6.1.4.1.59034.1.2. A subsequent version 2.0 will have OID 1.3.6.1.4.1.59034.1.3.

9.13 Dispute resolution provisions

Each CA in the CharIN V2G PKI SHALL have documented policies and procedures for the resolution of complaints and disputes received from subscribers or other parties about the provisioning of their services.

Any dispute related to key and certificate management between the PKI participants SHALL be resolved using an appropriate dispute settlement mechanism. The dispute SHALL be resolved by negotiation if possible. A dispute not settled by negotiation SHOULD be resolved through arbitration by the Irdeto CrossCharge Governance Board.

9.14 Governing law

No stipulation.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

If a CA within the CharIN V2G PKI is part of a larger organization, it SHALL

- be independent of this organization for its decisions relating to the establishing, provisioning, maintaining, or suspending of services in conformance with this Certificate Policy. In particular, its senior executives, senior staff and staff in trusted roles SHALL be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.
- have a documented organizational structure which safeguards impartiality of operations under this Certificate Policy.

10 References

[1] RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, S. Chokani et. al., November 2003

[2] Security Requirements for Subscribers to the Irdeto CrossCharge V2G PKI

[3] RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, S. Bradner, March 1997

[4] RFC 5280, Internet X.509 Public Key Infrastructure - Certificate and CRL Profile, D. Cooper et al., May 2008

[5] ISO 15118-2:2014, Road vehicles – Vehicle to Grid communication Interface – Part 2: Network and application protocol requirements

[6] ISO 15118-20:2022, Road vehicles – Vehicle-to-Grid Communication Interface – Part 20: 2nd generation network layer and application layer requirements

[7] Certificate Policy for CharIN V2G PKI by Irdeto Compliant to ISO 15118-20, Irdeto CrossCharge Governance Board, Irdeto Security B. V.

[8] VDE-AR-E 2802-100-1:2017-10 Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118 (English translation of VDE-AR-E 2802-100-1:2017-10)

[9] ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements

[10] RFC 2986, PKCS #10: Certification Request Syntax Specification Version 1.7, M. Nystrom et al., November 2000

[11] Irdeto Terms & Conditions

[12] ISO/IEC 15408-1, -2 and -3, Information technology – Security techniques – Evaluation criteria for IT security, Parts 1, 2 and 3. Third edition, 2008-2014

[13] ISO/IEC 19790, Information technology – Security techniques – Security requirements for cryptographic modules. Second edition, 2012-08-15

[14] National Institute of Standards and Technology (NIST), FIPS PUB 140-2, Security requirements for cryptographic modules, December 3, 2002

[15] National Institute of Standards and Technology (NIST), FIPS PUB 140-3, Security requirements for cryptographic modules, March 22, 2019

Irdeto CrossCharge V2G PKI Governance Board
Irdeto USA, Inc.
Email: pki.ma@irdeto.com
Web: www.irdeto.com/connected-transport/electric-vehicle-ev-charging/pki