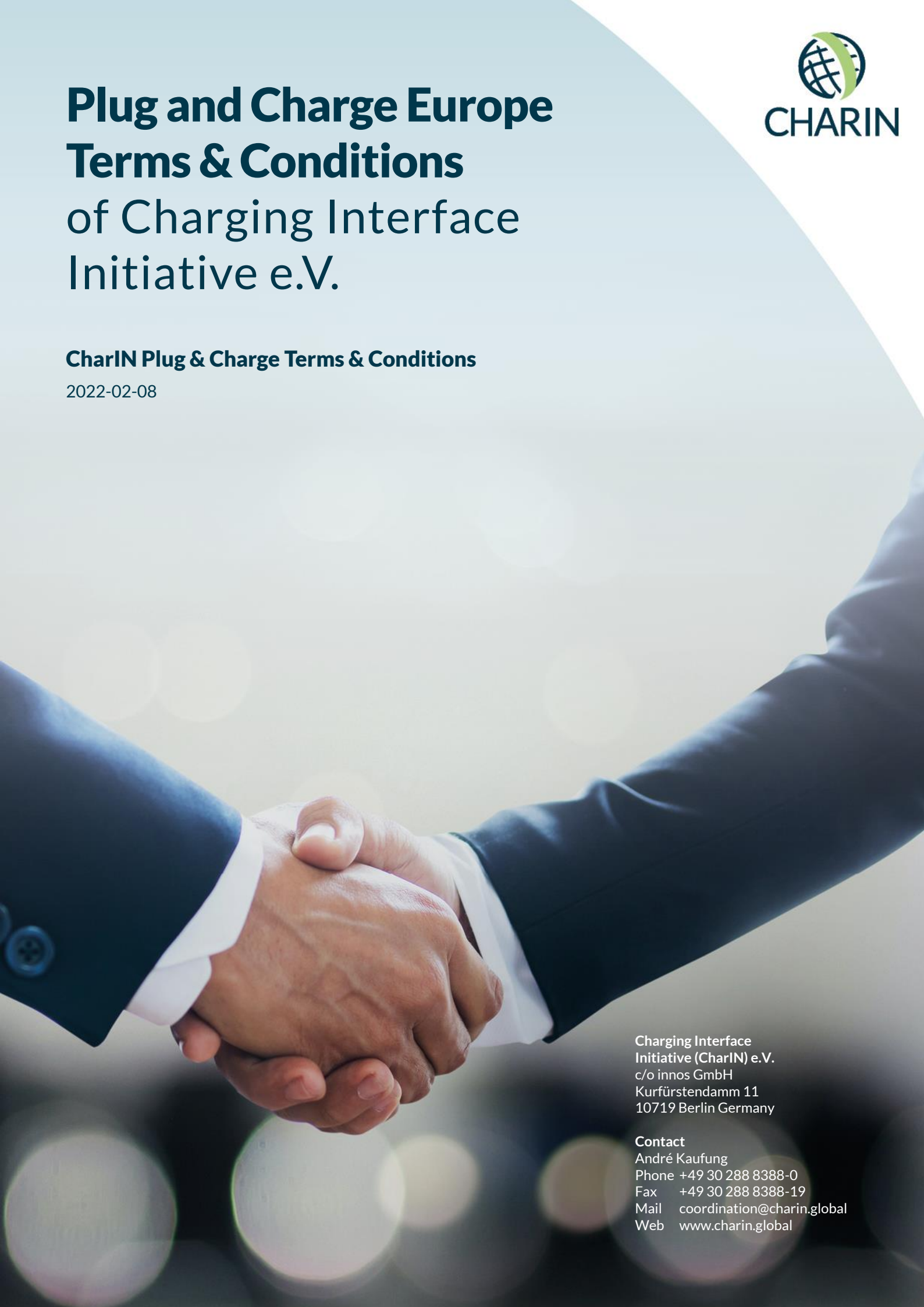
Plug and Charge Europe Terms & Conditions of Charging Interface Initiative e.V.

CharIN Plug & Charge Terms & Conditions

2022-02-08



Charging Interface Initiative (CharIN) e.V.
c/o innos GmbH
Kurfürstendamm 11
10719 Berlin Germany

Contact
André Kaufung
Phone +49 30 288 8388-0
Fax +49 30 288 8388-19
Mail coordination@charin.global
Web www.charin.global

Contents

List of abbreviations

CA	Certificate Authority
CCP	Contract Certificate Pool
CCS	Combined Charging System
CM	Certificate Manager
CP	Certificate Policy
CPO	Charge Point Operator
CPS	Certificate Practice Statement (in PKI context)
CPS	Certificate Provisioning Service (in VDE Application Rule context)
CRL	Certificate Revocation List
CSO	Charging Station Operator
eMSP	e-Mobility Service Provider
EV	Electric Vehicle
MO	Mobility Operator
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer (in EV context)
OTA	Over-the-Air (in telematics context)
PCP	Provisioning Certificate Pool
PKI	Public Key Infrastructure
RCP	Root Certificate Pool

List of figures

List of related documents

- VDE-AR-E 2802-100-1 Anwendungsregel:2019-12
  Handling of certificates for electric vehicles, charging infrastructure and backend systems within the framework of ISO 15118
- DIN EN ISO 15118-2:2014:
  Road vehicles - Vehicle-to-Grid Communication Interface - Part 2: Network and application protocol requirements (ISO 15118-2:2014)
- CharIN implementation guide to Plug and Charge in the context of ISO 15118
- CharIN e.V. Plug and Charge Europe Governance Guidelines
- CharIN e.V. Plug and Charge Europe Certificate Policy
- CharIN e.V. Plug and Charge Europe Certificate Practice Statement
- CharIN Task Force PKI Interoperability Guideline

1. Introduction

The Combined Charging System (CCS) is currently the world's only international standardized charging system covering standard and fast charging scenarios by one integrated system approach. The maturity of CCS has been confirmed by its interoperability and availability all over Europe, North America, and other nations globally. For the empowerment of CCS, the Charging Interface Initiative association (CharIN e.V.) was founded in May 2015 in Berlin. CharIN currently consists of more than 200 members (numbers still growing), covering all value chain areas. To give the best support and input to all regions of the world, CharIN has set up six international offices (India, Asia, Korea, Japan, China, and North America) in addition to the headquarter in Berlin, Germany. Furthermore, by organizing several regional and international events with up to 500 participants, CharIN enables its members to network and exchange the latest developments on CCS and create new cooperation.

Concentrating on international and industry sector comprehensive expertise, interests, and ideas, CharIN aims at also defining future levels of charging. The structure and the work content of its focus groups allow the continuous integration of future-oriented topics according to upcoming requirements to reach the next level of requirements definition for interoperable and global standards.

To enhance the customer charging experience for seamless charging, the feature Plug and Charge offers additional value. ISO, the International Organization for Standardization, has defined the necessary interfaces in ISO standard 15118.

For enabling the functionalities of the ISO 15118, CharIN operates a V2G Root for all stakeholders in the European market.

1.1. Objectives

The overall purpose of this document is to provide binding Terms & Conditions to participate in an open and fair PKI ecosystem for ISO 15118 operated and governed by CharIN e.V., ensuring freedom of choice for consumers as well as a level playing field for its participants.

Commercial and technical applicability

It should be noted that these Terms & Conditions promote the interoperability of ISO 15118, where every party (i.e., service provider) can work with another to ensure customers' freedom of choice. However, interoperability requires bilateral commercial agreements between the business partners on a business level, where every party is free in choosing business partners.

The defined rules apply in the agreement between two parties, which should be interpreted as guidelines to support CharIN's goal of interoperability.

On a business level, CSOs and eMSPs make separate roaming agreements. However, these agreements are independent from the certificate handling in the EVSEs or backend systems.

As indicated before, the purpose of this document is not to limit any commercial relationships or prescribe any business models. The terms "open" and "openness" should rather be understood as a promotion of unrestricted access for every market participant to guarantee fairness in the market, provided that relevant security requirements which are defined in the CP and CPS documents are met.

For reasons of better readability, the CP and CPS documents are implicitly referred to from here on when security requirements are addressed.

Applicability on PnC ecosystem

CharIN is aware that parts of the PnC ecosystem (e.g., pool services, CTL services, other PKIs) do not need to be commercially or technically connected to the CharIN PKI. However, a certain degree of openness and fairness in the ecosystem needs to be ensured as well, as the PKI and the ecosystem can only function in tandem. Therefore, this document also defines binding Terms & Conditions for ecosystem service providers as well as other PKI operators which want to be part of and/ or connected to the CharIN PnC Environment. Find a schematic overview of the CharIN PnC Environment in Figure 1.

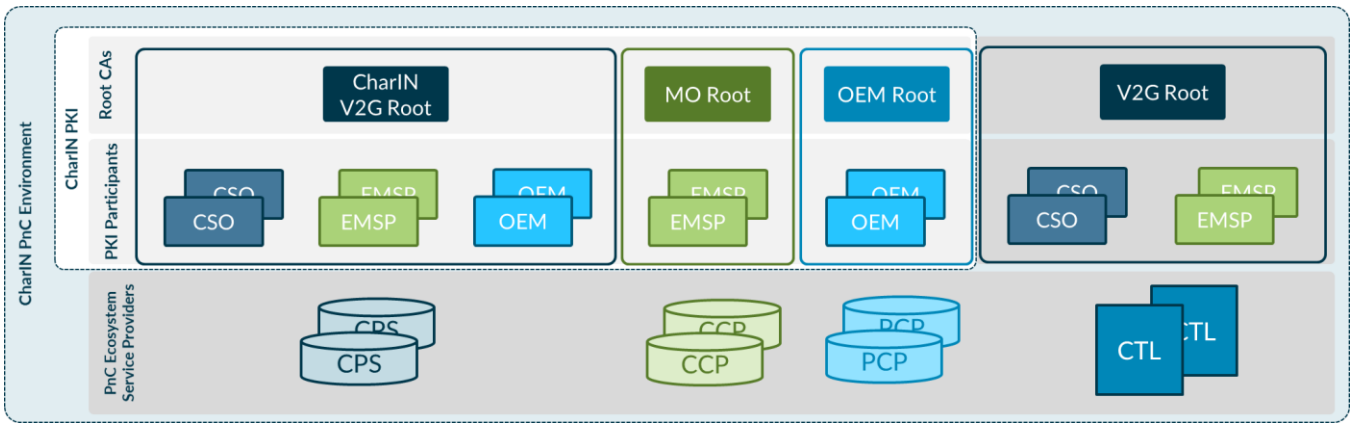


Figure 1: Schematic illustration of CharIN PnC Environment

In the further sections of this document, following stakeholders are referred to as CharIN PKI Participants due to their involvement in the CharIN PKI:

- CSOs
- eMSPs
- EV OEMs (from here on only referred to as OEMs)

and following stakeholders are referred to as CharIN PnC Participants due to their involvement in the CharIN PnC Ecosystem:

- CPS operators
- CCP operators
- PCP operators
- CTL operators
- Other PKI operators

A list of trusted ecosystem service providers that comply with these Terms & Conditions can be found on the CharIN website [LINK].

1.2. Governance

The governance of this document, i.e., additions, changes, and removals of any sections within the CharIN PnC Terms & Conditions, is under the responsibility of the CharIN PnC Governance Body and elaborated in the CharIN PnC Governance Guidelines document.

These Terms & Conditions are binding for any company that wants to participate in the CharIN PnC Environment. Any violation will be reviewed and examined individually by the CharIN PnC Governance Body, potentially leading to an exclusion from the CharIN PKI.

1.3. Applicability of ISO 15118-20

Due to the pending publication of ISO 15118-20, the present Terms & Conditions are mainly focused on the ISO 15118-2. As soon as the ISO 15118-20 is published, the CharIN PnC Terms & Conditions will be reviewed and, if necessary, adapted to the ISO 15118-20 content (e.g., handling of OEM Root CAs).

2. General Terms & Conditions

2.1. CharIN V2G Root CA and PKI Participants

1. CharIN offers open access to its V2G Root CA service to all entities that wish to join the CharIN V2G Root CA as long as these Terms & Conditions are respected.

2. In addition to these Terms & Conditions, the CharIN V2G Root CA only requires Sub CA applicants to meet the security requirements.

3. An independent auditor ensures compliance of the Sub CA applicant with the security requirements.

4. The CharIN PKI Participants must provide certificate status information with the OCSP responder or Certificate Revocation List to all other CharIN PKI Participants without any restriction.

2.2. Interoperability between V2G Root CAs

5. The CharIN V2G Root CA and the CharIN PKI Participants must support interoperability mechanisms, if multiple V2G Root CAs emerge in the European market, e.g.,

   i. by joining one PKI and installing all accompanying Cross Certificates of the V2G Root CA,

   ii. or by being compliant with CTL.

6. With respect to PKI interoperability, CTL operators and 3rd party V2G Root CAs must prove/ support same or equivalent security requirements and Terms & Conditions to the one's defined by CharIN.

7. The CharIN PnC Governance Body determines and implements the optimal interoperability solution for the CharIN PKI in alignment with the European V2G Root market.

3. OEM commitments

8. OEMs must enable the installation of an eMSP contract that was chosen freely by the consumer.

9. The technical and commercial terms defined by OEMs for installing an eMSP contract in the vehicle must be equal for all eMSPs.

10. EVs shall only be sold or delivered with a pre-selected eMSP contract with the consumer's explicit consent.

11. In case of multiple eMSP contracts installed in the EV, the consumer must have the freedom to switch to the contract of choice.

12. OEMs must provide a simple and secure way for the consumer to access the PCID of the EV. Additionally, OEMs must offer a consumer-friendly way for the replacement in case of loss or change of the PCID.

13. OEMs must inform consumers of the PCID changes of their EVs. Alternatively, OEMs can transfer the responsibility for informing of PCID changes to a third party.

14. OEMs must provide an automated way to the consumer's eMSP for contract certificate installation and update with the EV owner's explicit consent, e.g., via EVSE or OEM telematics route. Consumer consent is not required if the contract certificate update is performed due to expired validity of the certificate.

15. OEMs must ensure that the consumers' EVs always have valid OEM provisioning certificates in case of an existing telematics route. If the OEM does not offer telematics services, the certificate must be updated at the next workshop visit at an OEM service partner before the expiration of the installed certificate.

16. OEMs must ensure a way for eMSPs to have access to the EV's OEM provisioning certificates (e.g., indicating the location of OEM provisioning certificates directly or via a third party or OEM pushes OEM provisioning certificates at eMSP request).

17. OEMs must publish all relevant EV information as defined in the List of related documents for the eMSPs to ensure the functionality of the Plug and Charge contract in the EV.

4. eMSP commitments

18. eMSPs that operate their own MO Root CAs must publish their MO Root CA certificates.

19. eMSPs must ensure that their eMSP contracts always have valid contract certificates.

20. eMSPs must indicate the contract certificates' location to the OEMs and CSOs.

21. eMSPs must make contract certificates accessible to the customer's EV OEM to install contract certificates in EVs via the OTA/ vehicle telematics interface and OEM backend. Alternatively, eMSPs transfer the responsibility for enabling access to a third party, e.g., Contract Certificate Pool Operator.

22. eMSP contract certificate bundles must be signed by a CPS certificate chain derived from the CharIN V2G Root CA.

5. CSO commitments

23. CSOs must ensure that the EVSEs always have valid EVSE leaf certificates.

24. CSOs, which support contract certificate installation/ update, must offer connection to Contract Certificate Pools either via direct connection or via Pool Interoperability.

6. Certificate Pool Operator commitments

6.1. Certificate Provisioning Service – CPS

25. The Certificate Provisioning Service Operator must provide access for all eMSPs.

26. The Certificate Provisioning Service Operator must ensure that the CPS always has valid provisioning certificates for the contract signing.

6.2. OEM Provisioning Certificate Pool – PCP

27. In case only one OEM Provisioning Certificate Pool is available in the CharIN PnC Environment, all OEMs and eMSPs must have equal access to it.

28. In case multiple OEM Provisioning Certificate Pools are available in the CharIN PnC Environment, all OEM Provisioning Certificate Pool Operators must enable all eMSPs to access their OEM Provisioning Certificate Pools.

29. All eMSPs must have access to all available repositories for OEM Provisioning Certificate Pools.

6.3. Contract Certificate Pool – CCP

30. In case only one Contract Certificate Pool is available in the CharIN PnC Environment, all OEMs, CSOs and eMSPs must have equal access to it.

31. In case multiple Contract Certificate Pools are available in the CharIN PnC Environment, all Contract Certificate Pool Operators must enable all CSOs and OEMs to retrieve the contract certificates from their Contract Certificate Pools.

32. All OEMs and CSOs must have access to all available repositories for eMSP Contract Certificate Pools.

6.4. Pool Interoperability

33. PKI Pool Operators must ensure Pool Interoperability with all other PKI Pool Operators.

7. Reference

This document was created by the "Plug and Charge Europe" project team of the CharIN association.

The project committed to set up a Public Key Infrastructure (PKI), a technology needed to enable secure authentication and authorization via Plug and Charge in accordance with ISO 15118, with CharIN as operator and provider of required services. CharIN, as neutral and international authority, shall ensure fairness as well as openness and guarantees a level playing field for operating the PKI across all stakeholders.