HUBJECT

Onboarding Guidelines for Root CAs

ISO 15118 V2G PKI
Hubject Plug&Charge

Version 1.1 – June 2020

Hubject GmbH

Hubject Plug&Charge

Onboarding guidelines for Root CAs

to the Hubject ISO 15118 V2G PKI

Hubject GmbH

Version 1.1

June 2020

EUREF Campus 22

10289 Berlin

http://www.hubject.com/pki

support.iso15118@hubject.com

Tel: 0049 30 78 89 32 00

Status Document: **Final**

Documentation Classification: **Public**

1. Introduction

This document serves as a checklist for MO and OEM Root CAs to be authorized to the Hubject ISO 15118 V2G Root Certificate Pool. As the Hubject Certificate Policy (CP) stipulates, MO and OEM Root Certificates are operated by these organisations them self. The Root CA certificate of such an independent MO or OEM can be added to the Hubject Root Certificate Pool. The respective Root CA operator must enter a contractual relationship with Hubject GmbH to abide by all the requirements stipulated by [V2G-CP-17]. Within this document, the key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” are to be interpreted as described in [RFC 2119].

The audit part in Section **Error! Reference source not found.** of the document is structured as follows:

- Every item starts with a requirement statement call the **Control step**
- In **Checks** it is described how the “Auditor”, either Hubject or a contracted Auditor, verifies the requirement in the audit
- The **Source references** is referring to the specific section of the Hubject Certificate Policy or ISO 15118-2 standard section to which the requirement is related. When applicable, the specific stipulation of the Hubject Certificate Policy is copied for clarification

2. Definition of the Hubject PKI

The Hubject V2G Public Key Infrastructure, hereafter abbreviated as “PKI”, summarizes all authorities whose trust anchors can be traced back to the original V2G Root CA using digital signatures and certificates. Furthermore, such authorities should also be regarded as part of the PKI, which fulfil all the requirements of the V2G Root CAs Certificate Policy and, based on this conformity, are granted participation in the infrastructure.

- The OEM Root CA and the Mobility Operator Root CA are never considered part of the PKI but provide the trust anchors of their subordinated CAs. These subordinated CAs can be considered part of the PKI as long as they conform to the CP and can be subordinated to the V2G Root CA through cross certification.
- The Leaf certificates are by definition not part of the PKI.
- All certificate pools are considered part of the PKI and must be protected as such.

The set of roles, policies, hardware, so ware and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption at all these CAs are considered as part of the PKI.

3. Definition of Root CA role

In the Hubject PKI and Plug&Charge Ecosystem, the use of root certificates other than the V2G Root are allowed. The ISO 15118-2 and the VDE Application Guide describe the function of these root CAs and their responsibilities more in detail.

For OEMs, the OEM root CA certificate is used for signing an OEM sub-CA certificate, which, in turn, signs either an additional OEM sub-CA 2 certificate or, directly, an OEM provisioning certificate.

For MOs this type of certificate is used to issue and sign the end user's contract certificates installed in the vehicle via a chain of one or, at most, two sub-CAs.

4. Processes

The following describe how Root CAs of OEMs and MOs are audited regarding the compliance to [V2G-CP-17] and being authentically added to the Root Certificate Pool (RCP). The test results must be documented and archived at Hubject. A notification channel will be offered which shows changes in the content of the root certificate pool and which other subscribers can subscribe to (e.g. email newsletter). Random quality checks will be performed on all Root CAs added to the Root Certificate Pool.

5. Onboarding checklist

5.1. Certificate validation

Prior to all following checks, the validity of the investigated certificate is to be checked.

Control Step 1

The Auditor shall review that the Root CAs certificate to be added is a valid x.509 certificate.

Checks:

1. Sight the digital certificate can be parsed by the OpenSSL library without any errors;

Source Reference n/a

5.2. Authentication of organization identity

Before adding the new Root CAs certificate to the Root Certificate Pool, the following authentication check is to be fulfilled.

Control Step 2

The Auditor shall authenticate that the requesting organization exists and that the certificate application was authorized and that the person submitting the certificate application on behalf of the certificate applicant is authorized to do so,

Checks:

1. Sight the excerpt of a trusted third-party identity proofing service.
2. Sight that the certificates CN field contents matches the organization name.
3. Sight that a confirmatory postal mail that authorizes the certificate application exists.
4. Sight that a proof exists that that the person submitting the certificate application on behalf of the certificate applicant is authorized to do so,

Source Reference [V2G-CP-17] 3.2.2

ISO 27000 Certification

The company operating the Root CA needs to hold an ISO 27001 or comparable certificate on over all IT security processes in connection with the CA.

Control Step 3

The Auditor shall review that a valid IT Security Certificate on exists and its scope is covering all parts in relation with the Root CA operation.

Checks:

1. Sight the existence of an IT Security Certification;
2. Sight that the scope of the certificate is fully covering the CA operation.

Source Reference n/a

5.3. Certificate Profile Validation

The Root CA certificate to be added must implement the certificate profiles as defined in [ISO 15118-2:2014].

Control Step 4

The Auditor shall review that the certificate of the Root CA to be added confirms to the certificate profile regarding the assigned role in all elements.

Checks:

1. Sight that each of the given properties of the certificate complies with the profile definition;
2. Sight that no restricted extensions are present in the certificate;
3. Sight that all required fields are present and populated in compliance with the profile;
4. Sight that all required extensions are present;

Source Reference [V2G-CP-17] 2.1

5.4. Certificate Policy Validation

The requirements in the CP of the Root CA to be added must guarantee security comparable to the CP of the Hubject ISO 15118 V2G PKI.

Control Step 5

The Auditor shall review that a released, productive and published CP of the Root CA to be added is available.

Checks:

1. Sight the existence of the publication location;
2. Sight that the status of the published document is released;
3. Inquire the CA if the received CP document is the productive version and sight the confirmation;

Source Reference [V2G-CP-17] 2.1

Control Step 6

The Auditor shall review that the requirements in that CP guarantee security comparable to the CP of the Hubject ISO 15118 V2G PKI.

Checks:

1. Observe the CP document that has security requirements comparable to the V2G CP.

Source Reference [V2G-CP-17] 2.1

5.5. Certificate Practice Statement Validation

It must be formally confirmed that the compliance of all requirements has been regulated by a Certificate Practice Statement.

There are two options to choose from to confirm that compliance:

- External independent auditor (trusted third party)
- Internal audit by Hubject

Control Step 7

The Auditor shall review that all requirements of the CP of the Root CA to be added are regulated by a Certificate Practice Statement.

Checks:

1. Sight evidence that a Certificate Practice Statement regulates all requirements of the CP.

Source Reference [V2G-CP-17] 2.1

5.6. Certificate Checks

The certificate checks defined in the Certificate Policy must be carried out.

Control Step 8

The Auditor shall review that the fingerprint of the certificate has been authentically obtained via second channel from the corresponding Root CA and that it corresponds to the fingerprint of the certificate,

Checks:

1. Inquire the CA for the certificate fingerprint through a second channel;
2. Sight the correctness of the certificates fingerprint;

Source Reference [V2G-CP-17] 2.1

Control Step 9

The Auditor shall review that the validity field of the Root CAs certificate is 40 years or longer.

Checks:

1. Sight the validity period of the certificate;

Source Reference [V2G-CP-17] 2.1

Control Step 10

The Auditor shall review that the certificate to be added is not revoked.

Checks:

1. Inquire owner of the root certificate company for the revocation status;
2. Sight the confirmation on that the certificate has not been revoked;

Source Reference [V2G-CP-17] 2.1

Control Step 11

The Auditor shall review that the algorithms used comply with the ISO 15118 specification.

Checks:

1. Sight the certificate signature algorithm to conform to [V2G2-006];

Source Reference [V2G-CP-17] 2.1

6. References

Document	Identifier	Version	Date
Certificate Policy (CP) for the Hubject ISO 15118 V2G PKI	[V2GCP-17]	1.7	June 2020
ISO 15118-2:2014 Road vehicles – Vehicle-to-Grid Communication Interface – Part 2: Network and application protocol requirements 2014	[ISO 15118-2:2014]	ISO 15118-2:2014	2014