HUBJECT

Onboarding Guidelines for PKI Subscribers

ISO 15118 V2G PKI
Hubject Plug&Charge

Version 1.1 – June 2020

Hubject GmbH

Hubject Plug&Charge

Onboarding guidelines for Subscribers

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 CPOs, MOs and OEMs which are to be authorized to act as a Subscriber to the Hubject ISO 15118 V2G PKI. As defined in the Hubject Certificate Policy (CP) [V2G-CP-17] stipulates, the Subscriber bears ultimate responsibility for the use of the credentials. Therefore, Hubject GmbH requires an on-boarding audit of Subscribers to certify the compliance to the stipulated security standards.

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 5 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 the Subscriber role

“Subscriber” is the entity which contracts with Hubject GmbH for the issuance of credentials. The Subscriber holds the organizational and technical responsibilities.

The Subscriber bears ul mate responsibility for the use of the credential, but the Subject is the entity which is authenticated when the credential is presented.

See [V2G-CP-17] sec on 1.3.3.

4. Process

The following describe how Subscribers are audited regarding the compliance to [V2G-CP-17] and being authentically added to the Hubject PKI. 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 PKI.

5. Onboarding checklist

5.1. Certificate uses

The private keys of end-entity certificates issued within the PKI must be used in accordance with [ISO 15118-2:2014], which is the primary source of information on permitted CA and end-entity types and certificate usages. Other uses of end-entity keys and certificates are not permitted.

Control Step 1

The Auditor shall review that the audited Subscriber takes precautions that the private key corresponding to a certificate issued by the PKI is used in compliance with the key usage indicated in the certificate.

Checks:

1. For role CPO only: Sight that the hardware on-boarding guidelines of the CPO contains control steps for conforming key usage;
2. Sight that the Subscriber's system architecture foresees key usage scenarios conforming to [ISO 15118-2:2014];
3. Sight that the subscription contract includes obligation to adhere to the key usage.

Source Reference [V2G-CP-17] 1.4.1, 1.4.2

5.2. Subject Naming of organization identity

The V2G Certificate Policy [V2G-CP-17] specifies a consistent hierarchy for naming:

Source Reference [V2G-CP-17] 3.1.6

> Each issuing Sub1-CA declares a unique subject namespace towards the superordinate V2G Root CA. Each issuing Sub2-CA declares a unique subject namespace towards the superordinate Sub1-CA. The issuing Sub1- or Sub2-CAs must not use subject DNs outside the stipulated namespace. The uniqueness of subject DNs is in the sole responsibility of the issuing CA. The subject DNs has a limit of 64 characters.

The issuing CA will therefore enforce these naming conventions towards the end-entity certificates of the Subscriber.

Control Step 2

The Auditor shall review that the Subscriber confirms to the naming convention in the Certificate Signing Requests.

Checks:

1. Sight that the Subscriber has a naming scheme in place which conforms to the naming rules;
2. Sight that the Subscriber's systems generate CSRs with attributes within the declared namespace;

Source Reference [V2G-CP-17] 3.1.1

The V2G Certificate Policy [V2G-CP-17] specifies the following naming conventions:

> End-entity Subscriber certificates shall include meaningful names in the following sense: end-entity Subscriber certificates shall contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the subject of the certificate.
>
> Contract Certificates and SECC certificates shall include Subject names which meet the requirements for the name forms specified in Annex H of [ISO 15118-2]. Wildcard and SAN certificates (e.g. *.cpoprovider.de) must not be used. End-entity Subscribers are not permitted to use pseudonyms within the PKI.

Control Step 3

The Auditor shall review that the Subscriber requests certificates for unique names only.

Checks:

1. For role CPO only: Sight that the Subscribers systems generate CSRs with the charging stations unique SECCID in the common name field;
2. For role MO only: Sight that the Subscribers systems generate CSRs with a unique EMAID as defined in [ISO 15118-2:2014] Annex H;
3. Sight that the Subscriber uses Provider IDs and Operator IDs which were assigned by a central issuing authority;

Source Reference [V2G-CP-17] 3.1.2, 3.1.3

Certificate applicants shall not use names in their certificate applications that infringe upon the Intellectual Property Rights of others.

Control Step 4

The Auditor shall review that Hubject is not required to determine whether the Subscriber has Intellectual Property Rights in the name appearing in a certificate application.

Checks:

1. Sight that the subscription contract includes obligation to adhere to the IPR regulations of the certificate policy

Source Reference [V2G-CP-17] 3.1.6

Whenever a certificate contains an organization name, the identity of the organization and other enrolment information provided by the certificate applicant must be validated.

At a minimum, the CA shall: determine that the organization exists by using at least one third-party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or recognized authority that confirms the existence of the organization, confirm by telephone, confirmatory postal mail, or comparable procedure that the organization has authorized the certificate application, and that the person submitting the certificate application on behalf of the certificate applicant is authorized to do so.

Control Step 5
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 Sub-CAs validation record for CN field contents matches the organization name;
3. Sight that a confirmatory postal mail that authorizes the Subscriber application exists;
4. Sight that a proof exists that that the person submitting the Subscriber application behalf of the subscribing company is authorized to do so;

Source Reference [V2G-CP-17] 3.2.2

5.3. Key handling

Prior to the expiration of an existing certificate, it is necessary for the Subscriber to obtain a new certificate to maintain seamless operation. The (Subscriber) must generate a new key pair to replace the expiring key pair (technically defined as “re-keying”).

Certificate renewal is not allowed in the PKI.

Control Step 6
The Auditor shall review that the Subscriber takes precautions to only request new certificates after re-keying.

Checks:
1. For the CPO role only: Sight that the hardware on-boarding guidelines of the CPO contains control steps for enforcing re-keying on hardware level;
2. 2. Sight that the Subscriber’s system architecture foresees re-keying for new certificate requests.

Source Reference [V2G-CP-17] 3.3.1, 4.6, 4.7.1

The V2G certificate policy specifies the key pair generation:

End-entity keys should preferably be generated in the subject device (i.e. the car control unit, charge point control unit, as described in Section 6.2.2), or in an HSM, which is located either in the production site of the control unit or the end product (i.e. car, charging equipment).

If the keys are generated outside the subjected device, then: the secrecy of the private key during delivery to and storage at the end-entity, must be provided by the infrastructure of the Subscriber OEM (manufacturer) of that device and must be reporting this to the issuing CA OEM protect production line, to ensure that the key pair cannot duplicated to other entities/subjects.

Information about that situation will be stored on public CA statement site (include description how that can be detected that information in certificate – i.e. as information stored within the Common Name.)

Re-use of key material is prohibited. If an end-user private key is generated in an HSM, it shall be destroyed after generation and read-out using the key removal function of the HSM.

Control Step 7

The Auditor shall review that the Subscriber implements a secure key generation method.

Checks:

1. For the CPO role only: Sight that the hardware on-boarding guidelines of the CPO contain control steps for verifying the key genera on security measures;
2. For the CPO role only: Sight that the hardware on-boarding guidelines of the CPO contain control steps to report the OEM of new devices to the CA;
3. For the CPO role only: Sight that information about the key generation situation has been stored on the public CA statement site;
4. For the CPO role only: Sight that the hardware on-boarding guidelines of the CPO contain control steps to require hardware supporting curve secp256r1 (NIST p256) and private/public key lengths of 256 bits for the key generation.
5. For the role MO only: Sight that the Subscribers system architecture implements curve secp256r1 (NIST p256) and private/public key lengths of 256 bits for the Contract Certificates key generation.

Source Reference [V2G-CP-17] 6.1.1, 6.1.5, 6.2.5, 6.2.10

5.4. Trusted Root Store

The public key and the certificate of the V2G Root CA must be stored by every end-entity of the PKI. The Subscriber shall use a second communication channel for validating the V2G Root CA Certificate fingerprint, before installing it at the end-entities.

Control Step 08

The Auditor shall review that the Subscriber will store the public key and the certificate of the V2G Root CA on every end-entity.

Checks:

- For the CPO role only: Sight that the Subscribers system architecture implements methods to authentically store the V2G Root Certificate on every SECC;

Source Reference [V2G-CP-17] 6.1.4

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