Annex 1 Porthos PKI CP/CPS

This is the combined Certificate Policy (CP) and Certification Practice Statement (CPS) of the Porthos PKI defining the framework conditions for issuing digital certificates in accordance with the ITU-T recommendation X.509. The content of this CP/CPS document follows the template published by the [RFC 3647] internet standard.

Revision

Date	Version	Signature	Changes
23/02/2021	1.0	LEGIC	First official Version

Table of Contents

Table of Contents 2

1. Introduction 6

1.1 Overview 6

1.2 Document name and identification 6

1.3 PKI participants 6

1.3.1 Certification authorities 7

1.3.2 Registration authorities 7

1.3.3 Trusted third party 7

1.3.4 Trusted agent 7

1.3.5 Subscribers 8

1.3.6 Relying parties 8

1.4 Certificate usage 8

1.5 Policy administration 8

1.5.1 Organization administering the document 8

1.5.2 Contact information 8

1.5.3 Approval procedures 9

1.6 Definitions and Acronyms 9

2. Publication and repository responsibilities 10

2.1 Repositories 10

2.2 Publication of certification information 10

2.3 Time or frequency of publication 10

2.4 Access controls on repositories 10

3. Identification and authentication (I&A) 11

3.1 Naming 11

3.2 Initial identity validation 11

3.2.1 Method to prove possession of private key 11

3.2.2 Authentication of organization identity 11

3.2.3 Authentication of individual identity 11

3.2.4 Non-verified subscriber information 12

3.3 Identification and authentication for re-key requests 13

3.3.1 Identification and authentication for routine re-key 13

3.3.2 Identification and authentication for re-key after revocation 13

3.4 Identification and authentication for revocation requests 13

4. Certificate life-cycle operational requirements 14

4.1 Certificate application 14

4.1.1 Who can submit a certificate application 14

4.1.2 Enrollment process and responsibilities 14

4.2 Certificate application processing 14

4.2.1 Performing identification and authentication functions 14

4.2.2 Approval or rejection of certificate applications 14

4.2.3 Time to process certificate applications 15

4.3 Certificate issuance 15

4.3.1 CA actions during certificate issuance 15

4.3.2 Notification to subscriber by the CA of issuance of certificate 15

4.4 Certificate acceptance 15
4.5 Key pair and certificate usage 15
4.5.1 Subscriber private key and certificate usage 15
4.5.2 Relying party public key and certificate usage 15
4.6 Certificate renewal 15
4.7 Certificate re-key 16
4.7.1 Circumstance for certificate re-key 16
4.7.2 Who may request certification of a new public key 16
4.7.3 Processing certificate re-keying requests 16
4.7.4 Notification of new certificate issuance to subscriber 17
4.7.5 Conduct constituting acceptance of a re-keyed certificate 17
4.7.6 Publication of the re-keyed certificate by the CA 17
4.7.7 Notification of certificate issuance by the CA to other entities 17
4.8 Certificate modification 17
4.9 Certificate revocation and suspension 17
4.9.1 Circumstances for revocation 17
4.9.2 Who can request revocation 18
4.9.3 Procedure for revocation request 18
4.9.4 Revocation request grace period 18
4.9.5 Time within which CA must process the revocation request 18
4.9.6 Revocation checking requirements for relying parties 18
4.9.7 CRL issuance frequency 18
4.9.8 Maximum latency for CRLs 19
4.9.9 Online revocation/status checking availability 19
4.10 End of subscription 19
4.11 Key escrow and recovery 19
5. Facility, Management, and Operations Controls 20
5.1 Physical controls 20
5.1.1 Hosting provider, Site location and construction 20
5.1.2 Physical access 20
5.1.3 Power and air conditioning 20
5.1.4 Water exposures 20
5.1.5 Fire prevention and protection 21
5.1.6 Media storage 21
5.1.7 Waste disposal 21
5.1.8 Off-site backup 21
5.2 Procedural controls 21
5.2.1 Trusted roles 21
5.2.2 Number of persons required per task 22
5.2.3 Identification and authentication for each role 22
5.2.4 Roles requiring separation of duties 22
5.3 Personnel controls 22
5.3.1 Qualifications, experience, and clearance requirements 22
5.3.2 Background check procedures 22
5.3.3 Training requirements 22
5.3.4 Retraining frequency and requirements 22
5.3.5 Job rotation frequency and sequence 23
5.3.6 Sanctions for unauthorized actions 23
5.3.7 Independent contractor requirements 23
5.3.8 Documentation supplied to personnel 23

5.4 Audit logging procedures 23
5.4.1 Types of events recorded 23
5.4.2 Frequency of processing log 23
5.4.3 Retention period for audit log 23
5.4.4 Protection of audit log 23
5.4.5 Audit log backup procedures 24
5.4.6 Audit collection system (internal vs. external) 24
5.4.7 Notification to event-causing subject 24
5.4.8 Vulnerability assessments 24
5.5 Records archival 24
5.6 Key changeover 24
5.7 Compromise and disaster recovery 25
5.8 CA or RA termination 26
6. Technical security controls 27
6.1 Key pair generation and installation 27
6.1.1 Key pair generation 27
6.1.2 Private key delivery to subscriber 27
6.1.3 Public key delivery to certificate issuer 27
6.1.4 CA public key delivery to relying parties 27
6.1.5 Key sizes 27
6.1.6 Public key parameters generation and quality checking 27
6.1.7 Key usage purposes (as per X.509 v3 key usage field) 28
6.2 Private key protection and cryptographic module engineering controls 28
6.2.1 Cryptographic module standards and controls 28
6.2.2 Private key (n out of m) multi-person control 28
6.2.3 Private key escrow 28
6.2.4 Private key backup 28
6.2.5 Private key archival 28
6.2.6 Private key transfer into or from a cryptographic module 28
6.2.7 Private key storage on cryptographic module 28
6.2.8 Method of activating private key 29
6.2.9 Method of deactivating private key 29
6.2.10 Method of destroying private key 29
6.2.11 Cryptographic module rating 29
6.3 Other aspects of key pair management 29
6.3.1 Public key archival 29
6.3.2 Certificate operational periods and key pair usage periods 29
6.4 Activation data 29
6.5 Computer Security Controls 29
6.5.1 Specific computer security technical requirements 29
6.5.2 Computer security rating 30
6.6 Life cycle technical controls 30
6.6.1 System development controls 30
6.6.2 Security management controls 30
6.6.3 Life cycle security controls 30
6.7 Network Security Controls 30
6.8 Timestamping 30
7. Certificate, CRL, and OCSP profiles 31

7.1 Certificate profile 31
7.1.1 Porthos root CA certificate profiles 31
7.1.2 Porthos issuing CA certificate profiles 32
7.1.3 Porthos subscriber certificate profiles 34
7.1.4 AWS CA Verification Certificate profiles 36
7.2 CRL Profile 38
7.2.1 CRL of Porthos Root CA 38
7.2.2 CRL of Porthos Issuing CAs 38
7.3 OCSP Profile 39
8. Compliance audit and other assessment 40
8.1 Frequency or circumstances of assessment 40
8.2 Identity/qualifications of assessor 40
8.3 Assessor's relationship to assessed entity 40
8.4 Topics covered by assessment 40
8.5 Actions taken as a result of deficiency 40
8.6 Communication of results 40
9. Other business and legal matters 41
Appendix A Definitions 42
Appendix B Acronyms 44
Appendix C References 45

1. Introduction

LEGIC Identsystems AG is a subsidiary of the dormakaba Group. With its sound expertise in security and trusted software services acquired over the last 25 years, LEGIC was entrusted with the establishment and operation of the Porthos Public Key Infrastructure, a private PKI as a service for dormakaba and their products and customers.

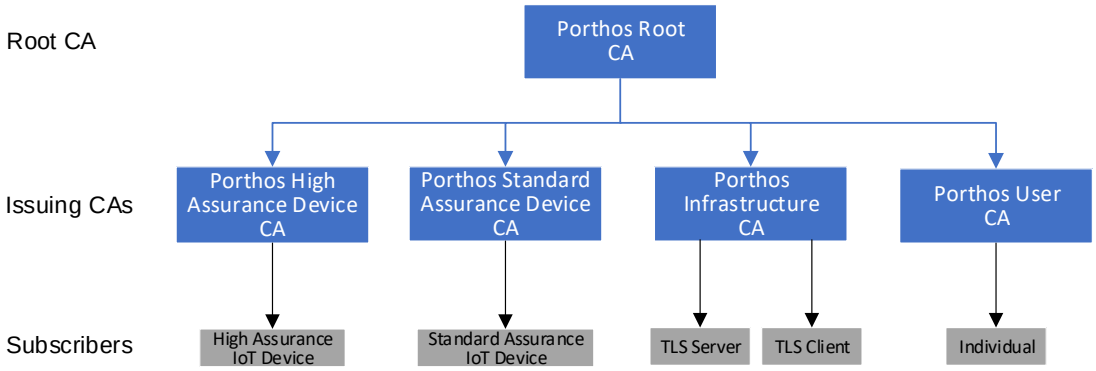
This CP/CPS document states the certificate policies of the Porthos PKI and describes the practices for issuing and managing public key certificates. It shall apply as a binding content to all PKI participants to aim judging the trust level and reliability of the Porthos PKI.

1.1 Overview

A Certificate Authority (CA) is a collection of hardware, software, personnel, and operating procedures that issue and manage public key certificates, also known as digital certificates. The public key certificate binds a public key to a named subject. This allows relying parties to trust signatures with the private key that corresponds to the public key contained in the certificate.

Porthos PKI certificates shall be the basis for several security services including authentication, confidentiality, integrity, and non-repudiation for IoT devices, infrastructure components and users or individuals.

The figure below shows an overview of the CAs and the subscribers which are part of the Porthos PKI. The PKI is operated as a productive and non-productive environment. With minor exceptions, both are identical in terms of security and operation.



1.2 Document name and identification

Document name and version is indicated in the footer of this document.

1.3 PKI participants

This clause describes the different roles that are relevant to the administration and operation of the Porthos PKI under this policy.

1.3.1 Certification authorities

As outlined in 1.1, the Porthos PKI consists of 5 certification authorities, an offline root CA and four online issuing CAs.

The **Porthos Root CA** is the root of the Porthos PKI. Its public key is published in a self-signed certificate. This allows all participants of the PKI to verify the authenticity and validity of subordinate certificates. The Porthos Root CA solely issues certificates and the Certificate Revocation List (CRL) for its subordinate issuing CAs.

The **Porthos High Assurance Device CA** issues certificates to high assurance IoT devices. Such devices must contain a secure element (SE) to store their keys and a pre-provisioned Device Manufacturer Certificate (DMC) to prove their identity to the Porthos CA. Porthos CA must be aware of the manufacturer's root and issuing certificates as well as the DNs that are acceptable.

The **Porthos Standard Assurance Device CA** issues certificates to IoT devices which do not contain an SE and cannot prove their identity with a DMC.

The **Porthos Infrastructure CA** issues certificates to server and client infrastructure components.

The **Porthos User CA** issues certificates to users or individuals.

Common responsibilities of all issuing CAs include:

- Approving the issuance of subscriber certificates
- Storing of subscriber certificates in a certificate repository
- Revocation of subscriber certificates and publication of CRLs
- Generation and destruction of CA signing keys

Beside the certificates issued to the subscribers listed above, both Device Issuing CAs of the Porthos PKI may issue AWS CA Verification Certificates which are solely needed to register the Issuing CA certificate with AWS IoT service used by the IoT device subscribers. Except for their certificate profiles defined in 7.1.4, these special-purpose certificates are not further mentioned in this CP/CPS.

1.3.2 Registration authorities

The registration authority (RA) collects and verifies each subscriber's identity and information that is to be entered into the subscriber's public key certificate. There is no RA for the offline Porthos Root CA. Each issuing CA possesses an RA which is accessible through a web interface or optionally through an application programming interface (API) for automatic subscriber registration or re-keying. The methods of the RA to verify the subscriber's identity may differ and are described in clause 3.

RA operator: RA operators are the individuals holding trusted roles that operate and manage RA components.

1.3.3 Trusted third party

The trusted third party (TTP) is an entity which facilitates interactions between two parties which both trust the third party.

1.3.4 Trusted agent

The trusted agent is a person or computer who performs identity proofing as a proxy for the RA.

1.3.5 Subscribers

A subscriber is the entity whose name appears as the subject in a subscriber certificate, agrees to use its key and certificate in accordance with this certificate policy, and does not itself issue certificates.

In the context of the Porthos PKI, subscribers are IoT devices, infrastructure components (servers or client computers) or individuals.

1.3.6 Relying parties

A relying party is an entity that relies on the validity of the binding of the subscriber's name to a public key. The relying party uses a subscriber's certificate to verify or establish the identity of the subscriber. A relying party is responsible for deciding whether or how to check the validity of the certificate. A relying party may use information in the certificate to determine the suitability of the certificate for a particular use.

1.4 Certificate usage

In general, certificates of the Porthos PKI shall only be used within the Porthos realm and for the purpose defined in the certificate's key usage attributes (see also 7.1)

1.5 Policy administration

1.5.1 Organization administering the document

This document is administered and issued by LEGIC Identsystems AG.

The currently valid CP/CPS document is published at https://www.legic.com/porthos_pki/cpcps/ and is only available to dormakaba as the only customer of the Porthos PKI.

1.5.2 Contact information

LEGIC Identsystems AG
Binzackerstrasse 41
8620 Wetzikon
Switzerland
Phone +41 44 933 64 64
E-Mail: pki@legic.com

1.5.3 Approval procedures

This document remains valid until the Porthos PKI operation is terminated in accordance with this contract.

LEGIC Identsystems AG has the right to change or adapt this CP/CPS document at any time. This may be necessary due to technical or operational changes of the Porthos PKI or due to changed security requirements.

The version of the document (exposed in all the pages of the document) is controlled with two numbers separated by a period. The first number (major version) is incremented if the new version could affect the acceptance of the certificates by the users. The second number (minor version) is incremented if the amendment is not considered to affect the certificate acceptance criteria.

Updates of this document must be approved by the Security Officer of LEGIC Identsystems AG and be issued under a new version which replaces its predecessor. The PKI customer shall be notified promptly if a new CP/CPS document version is available.

1.6 Definitions and Acronyms

See Appendix A and Appendix B

2. Publication and repository responsibilities

2.1 Repositories

The Porthos Root CA shall post any issued certificate in a repository that is publicly accessible through the Uniform Resource Identifier (URI) referenced by the Authority Information Access (AIA) field in valid certificates issued by that CA.

All CAs under this policy shall post any issued CRL in a repository that is publicly accessible through the Uniform Resource Identifier (URI) referenced by the Certification Distribution Point (CDP) field in valid certificates issued by that CA.

The repositories of the CA certificates and CLRs are reachable at the following internet URLs:

Published Resource	Porthos Prod PKI	Porthos Non-Prod PKI
CRLs	http://crl.pki.porthos.services	http://crl.pki.porthos.io
CA certificates	http://crt.pki.porthos.services	http://crt.pki.porthos.io

2.2 Publication of certification information

See 2.1 for the publication of CA certificates and CRLs.

Subscriber certificates will not be publicly available. However, each CA stores its issued subscriber certificates in a repository which may be accessed by an RA operator using the web interface of the respective CA.

2.3 Time or frequency of publication

CA certificates will be published as soon as possible after they were generated. For CRL issuance frequency, see clause 4.9.7.

2.4 Access controls on repositories

CA certificates and CRLs published in the repositories are for public information and read access is freely available. However, the Porthos PKI has logical access control measures in place to prevent unauthorized modification or deletion of information in these repositories.

3. Identification and authentication (I&A)

3.1 Naming

Each CA assigns an X.501 Distinguished Name (DN) to each PKI entity. This DN appears in the certificate's subject field and must represent an unambiguous identifier. Names shall be meaningful enough for a human to identify the named entity, irrespective of whether the entity is a person, machine, or IoT device.

Each CA of the Porthos PKI ensures that each of its subscribers is identifiable by a unique name.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

Key pairs will typically be generated by the subscriber of the Porthos PKI so the private key must not leave their environment. To prove possession of the private key, the subscriber signs its corresponding public key in the certificate signing request (CSR) which will then be verified by the responsible CA.

Key generation may also be performed under the CA or RA's direct control. In such cases, proof of possession is not required.

3.2.2 Authentication of organization identity

The Porthos PKI does not issue certificates to organizational identities.

3.2.3 Authentication of individual identity

The issuing CAs of the Porthos PKI support authentication of the following individual identities:

Individual identity	Responsible RA/CA
High assurance IoT device	Porthos High Assurance Device CA
Standard assurance IoT device	Porthos Standard Assurance Device CA
Applications or services	Porthos Infrastructure CA
Human subscribers	Porthos User CA

The following subclauses define the initial authentication and registration process for each of the above identity types.

3.2.3.1 Authentication of high assurance IoT devices

A high assurance IoT device uses its SE to generate a new key pair and create a certificate signing request. The CN part of the DN in the CSR must identify the device in a unique manner. The CSR is then signed with the Device Manufacturer Certificate (DMC) and transferred to the RA of the Porthos High Assurance Device CA.

After signature and signer certificate have been cryptographically verified, the Chip-ID of the SE is read from the signer certificate and checked against the list of Chip-IDs which have been assigned to devices of the Porthos realm. This is required as SEs are not exclusively used by the Porthos realm and other devices, likely operated by untrusted parties, are technically able to successfully prove the possession of an SE.

The device is successfully authenticated if the given Chip-ID belongs to an authorized device.

3.2.3.2 Authentication of standard assurance IoT devices

Devices without an SE can only be provisioned with the assistance of a trusted third party (e.g. an authenticated user) and a trusted agent. It is assumed that the third party and the device can communicate via an authenticated and integrity protected channel.

The registration and authentication process are split into three steps:

1. The third party authenticates itself against the trusted agent so it becomes a “trusted third party (TTP)” for this registration process.
2. The device generates (eventually in cooperation with the TTP) a new key pair and creates a certificate signing request. The CN part of the DN in the CSR must identify the device in a unique manner. The TTP sends the CSR over the authenticated channel via the trusted agent to the RA where a transaction-ID is calculated and sent back to the TTP. The TTP may share the received transaction-ID with the device.
3. The device or TTP sends the CSR and the transaction-ID to the RA of the Porthos Standard Assurance Device CA. Depending on the connectivity type of the device this can be done either via a direct connection to the RA or with the assistance of the connected TTP. After the transaction-ID was verified by the CA, the certificate is issued.

3.2.3.3 Authentication of application or service

Certificates for applications or services will be requested and issued to an Authorized Organizational Representative (AOR). The AOR is responsible for providing registration information which shall include:

- Fully qualified hostname (FQDN) and optional software application or service name
- Software application or service CSR

The responsible RA operator verifies the information provided by the AOR and validates whether the AOR is authorized to request a certificate for the application or service. If the request is compliant to the internal CA policies, the certificate is issued immediately to the RA operator who passes it on to the AOR.

3.2.3.4 Authentication of humans

Humans or users and their certificates are managed by a trusted agent of the Porthos User CA and includes the following steps:

1. The user with the help of his device or the trusted agent generates a new key pair and the corresponding CSR. The CN part of the DN in the CSR should identify the user.
2. The trusted agent authenticates the user and passes the CSR over an authenticated channel to the Porthos User CA
3. The CA verifies the CSR and issues and returns the certificate.

3.2.4 Non-verified subscriber information

Information that is not verified will not be included in certificates.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

There is no routine re-key of CA certificates under this policy. Instead, the complete CA hierarchy will be replaced by a new generation every 5 years (see 5.6).

For re-key of any subscriber certificate issued under this certificate policy, identity shall be established using the current signature key. Where this is not possible, identity shall be established following the same procedures as the initial registration process defined in 3.2.

3.3.2 Identification and authentication for re-key after revocation

In the event of certificate revocation, issuance of a new certificate shall always require that the party go through the initial registration process defined in 3.2.

3.4 Identification and authentication for revocation requests

Revocation requests must be authenticated and executed by a member of the RA staff of the pertinent CA which approved the certificate application. The RA staff must ensure that the person requesting revocation is in fact the subscriber. In all cases, the RA staff shall record the reason for the revocation.

4. Certificate life-cycle operational requirements

4.1 Certificate application

The online issuing CAs of the Porthos PKI support a manual and/or an automatic certificate application process as defined in the table below.

Issuing CA	Manual application	Automatic application
Porthos High Assurance Device CA	-	X
Porthos Standard Assurance Device CA	-	X
Porthos Infrastructure CA	X	-
Porthos User CA	X	X

In either case, the certificate application process must provide enough information to:

- Establish the applicant's authorization to obtain a certificate (per clause 3.2.3)
- Establish and record identity of the applicant (per clause 3.2.3)
- Obtain the applicant's public key and verify the applicant's possession of the private key for each certificate required. (per clause 3.2.3)
- Verify any role or authorization information requested for inclusion in the certificate

These steps may be performed in any order that is convenient for the CA and applicants that does not compromise security, but all must be completed before certificate issuance.

4.1.1 Who can submit a certificate application

Automatic certificate applications shall be submitted to the CA by the subscriber using the API. Manual certificate applications shall be submitted to the CA by the subscriber or an AOR.

4.1.2 Enrollment process and responsibilities

All communications among PKI participants supporting the certificate application and issuance process shall be authenticated and protected from modification. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair shall be used. Out-of-band communications shall protect the confidentiality and integrity of the data.

Subscribers are responsible for providing accurate information on their certificate applications. See clause 3.2.3 for initial identity validation for subscribers of the Porthos PKI.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

The identification and authentication of the subscriber will be executed either by the responsible RA or the trusted agent as defined in 3.2 or the responsible RA as defined in 3.3.

4.2.2 Approval or rejection of certificate applications

Any certificate application that is received by one of the issuing CAs, and for which the identity and authorization of the applicant has been validated, will be duly processed. However, the CA shall reject any application for which such validation cannot be completed.

4.2.3 Time to process certificate applications

Automatic certificate applications will be processed typically within several seconds. Manual certificate applications will be processed typically within 10 working days after identity verification.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Upon receiving the request, the respective CA/RA shall:

- Verify the identity of the requester as specified in clause 3.2.
- Verify the authority of the requester and the integrity of the information in the certificate request as specified in clause 4.1.
- Build and sign a certificate if all certificate requirements have been met.
- Make the certificate available to the subscriber.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Any CA operating under this policy informs the subscriber about the issuance of a certificate by sending it back to the subscriber using the same authenticated communication channel and protocol over which the request was received. When a new subscriber certificate is issued it appears in the web interface of the issuing CA.

4.4 Certificate acceptance

After reception of a certificate, the subscriber shall verify its content (e.g. the subject name) before it can use it. If the subscriber cannot accept the certificate, it must immediately request its revocation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The intended scope of usage for a private key will be specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2 Relying party public key and certificate usage

Certificates issued by the Porthos PKI specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. All CAs operating under this policy shall issue CRLs containing a list of all unexpired revoked certificates. It is recommended that relying parties process and comply with this information whenever using certificates in a transaction.

4.6 Certificate renewal

The Porthos PKI does not offer certificate renewal. Instead a certificate re-keying shall be applied as defined in 4.7. Therefore, the remaining subclauses of this clause referring to certificate renewal are not applicable.

4.7 Certificate re-key

Re-keying of a certificate consists of creating new certificates based on a different public/private key pair while retaining the contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, specify a different CRL distribution point, and/or be signed with a different key.

4.7.1 Circumstance for certificate re-key

The longer and more often a key is used, the more susceptible it is to loss or discovery. Therefore, it is important that a subscriber periodically obtains new keys. The following table summarizes usage periods for private keys of CAs and subscribers.

Entity	Key lifetime
Porthos Root CA	10 years
Porthos Issuing CAs	7 years
Subscribers	13 months

Circumstances requiring certificate re-key include expiration, loss or compromise. Re-keying of CA certificates is not supported in case of expiration. Instead, such CA certificates will be replaced with a certificate of a new CA generation which is based on a different certificate subject.

4.7.2 Who may request certification of a new public key

Requests for certification of a new public key may be done by subscribers or by RAs on behalf of a subscriber or an AOR.

4.7.3 Processing certificate re-keying requests

The online issuing CAs of the Porthos PKI support a manual and/or an automatic certificate re-key process as defined in the table that follows.

Issuing CA	Manual re-key	Automatic re-key
Porthos High Assurance Device CA	-	A, B
Porthos Standard Assurance Device CA	-	A, B
Porthos Infrastructure CA	B	-
Porthos User CA	B	B

Re-key requests according to **A** require identity authentication based on the current signature key as per 3.3. The CA verifies the signature and issues the new certificate to the subscriber. However, the CA refuses the re-key request if

- it is received 6 months before the subscriber's certificate expires (renewal window)
- the validity of the subscriber's current certificate is not anymore valid for more than 5 years (grace period)

Processing re-key requests according to **B** do not allow identity authentication based on the current signature key. Instead, these subscribers must use the same procedure as for the initial registration process defined in 3.2.

4.7.4 Notification of new certificate issuance to subscriber

The CA shall inform the subscriber of the re-key of his or her certificate and the contents of the certificate as per 4.3.2.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

As per section 4.4.

4.7.6 Publication of the re-keyed certificate by the CA

Re-keyed subscriber certificates must be published as specified in clause 2.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.8 Certificate modification

The Porthos PKI does not offer certificate modification. Instead the old certificate shall be revoked, and a new certificate shall be issued as its replacement.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

A subscriber or CA certificate of the Porthos PKI may be revoked if there has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key associated with the certificate.

Any subscriber certificate of the Porthos PKI may be revoked under the following circumstances:

- Either the Porthos PKI or the subscriber may choose to end the relationship expressed in the certificate
- There has been a modification of the information pertaining to the subscriber that is contained within the certificate
- The certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities
- A certificate re-key is requested before the CA's renewal window starts as per 4.7.3

4.9.2 Who can request revocation

- Within the Porthos PKI, a CA may revoke certificates within its domain. A written notice and brief explanation for the revocation may subsequently be provided to the subscriber where applicable.
- The RA can request the revocation of a subscriber's certificate on behalf of any authorized party.
- A subscriber may request that its own certificate be revoked.
- The AOR of the organization that owns or controls a device can request the revocation of the device's certificate.
- Other parties may report suspected private key compromise, certificate misuse, or other types of fraud, compromise, inappropriate conduct, or any other matter related to certificates by the email given in 1.5.2.

4.9.3 Procedure for revocation request

A request to revoke a certificate shall identify the certificate to be revoked and allow the request to be authenticated (e.g., digitally or manually signed). The CA may request information sufficient to explain the reason for revocation.

4.9.4 Revocation request grace period

In general, there is no revocation grace period under this policy. Revocation requests should be submitted as promptly as possible within a reasonable time of becoming aware of a revocation circumstance listed in 4.9.1.

However, the issuing CAs may use a grace period for certificate revocations due to a re-keying which is requested before the renewal window starts as per 4.7.3. This allows the subscriber to still use the old and still valid certificate until the new one is in place.

4.9.5 Time within which CA must process the revocation request

Revocations will be processed as promptly as possible after receipt and validation of the request.

4.9.6 Revocation checking requirements for relying parties

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the relying party.

4.9.7 CRL issuance frequency

The CRL of the offline root CA has a validity of 2 years and is updated about once every year or after a revocation was processed.

The CRLs of the online issuing CAs have a validity of 28 days and are updated every 14 days or after a revocation request was processed.

4.9.8 Maximum latency for CRLs

The Porthos PKI does not employ a maximum latency for CRLs, but they will be published typically within one hour of generation in the repository defined in 2.1. However, CRLs shall be published no later than the time specified in the nextUpdate field of the previously issued CRL.

4.9.9 Online revocation/status checking availability

Online revocation/status checking using OSCP responder is not supported by the Porthos PKI.

4.10 End of subscription

Subscription is synonymous with the certificate validity period. The subscription ends when the certificate is revoked or expired.

4.11 Key escrow and recovery

Key escrow and recovery are not supported by the Porthos PKI.

5. Facility, Management, and Operations Controls

The Porthos PKI runs as an AWS cloud service. Therefore, most subclauses in this clause refer to statements defined in the Amazon Web Webservices: Overview of Security Processes document.

5.1 Physical controls

5.1.1 Hosting provider, Site location and construction

The online issuing CAs of the Porthos PKI are currently operated in an ISO 27001 certified data center from AWS, located in Frankfurt, Germany. Private keys of the CAs are stored in a hardware security module (HSM) from AWS located at the same site. LEGIC shall have the right, without Client's consent, to move to any hosting provider and location within the EU or Switzerland; however, LEGIC shall provide at least thirty (30) days' advance written notice (email sufficient) to Client of any such relocation. Such relocation does not entitle Client to terminate the Contract for cause.

5.1.2 Physical access

AWS data centers are state of the art, utilizing innovative architectural and engineering approaches. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in facilities that are not branded as AWS facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors are required to present identification and are signed in and continually escorted by authorized staff.

AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical access to data centers by AWS employees is logged and audited routinely.

5.1.3 Power and air conditioning

The AWS data center electrical power systems are designed to be fully redundant and maintainable without impact to operations, 24 hours a day, and seven days a week. Uninterruptible Power Supply (UPS) units provide back-up power in the event of an electrical failure for critical and essential loads in the facility. Data centers use generators to provide back-up power for the entire facility

5.1.4 Water exposures

Not stipulated.

5.1.5 Fire prevention and protection

Automatic fire detection and suppression equipment has been installed to reduce risk. The fire detection system utilizes smoke detection sensors in all data center environments, mechanical and electrical infrastructure spaces, chiller rooms and generator equipment rooms. These areas are protected by either wet-pipe, double-interlocked pre-action, or gaseous sprinkler systems.

5.1.6 Media storage

Media will be stored to protect it from accidental damage (water, fire, electromagnetic) and unauthorized physical access. Storage protection of private key material will be consistent with stipulations in clause 5.1.2.

5.1.7 Waste disposal

Media and paper used to collect or transmit privacy information will be destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8 Off-site backup

The Porthos PKI service does not perform off-site backups. Instead, data protection is achieved through geographical redundancy and continuous online backups of critical system data to minimize data loss in the event of a disaster.

5.2 Procedural controls

5.2.1 Trusted roles

The following subclauses identify the trusted roles of the Porthos PKI. Except for the RA Operator role, all roles are occupied by dedicated personnel of LEGIC Identsystems as the operator of this PKI.

5.2.1.1 Auditor

The Auditor is responsible for internal auditing of the Porthos PKI to ensure that it is operated in accordance with this CP/CPS.

5.2.1.2 HSM Security Officer

The HSM Security Officer role has the following responsibilities:

- Operation of the offline Porthos Root CA
- Generation of all CA keys within the HSM
- Issuance of the root and issuing CA certificates
- Issuance of the root CA’s CRL
- Control the access and usage of the root CA’s private key

These tasks will effectively be executed by a PKI Administrator but will be enabled and supervised by two HSM Security Officers applying multi-party control.

5.2.1.3 PKI Administrator

The role of the PKI Administrator includes:

- Tasks supervised by two HSM Security Officers as per 5.2.1.2
- Installation, configuration, maintenance and operation of the online issuing CAs
- Establishing and maintaining AWS system accounts
- Backup and restore of Porthos PKI data and system components

5.2.1.4 RA Operator

The RA Operator has web interface access to the online issuing CAs and is responsible for:

- Processing of manual certificate applications according to 4.1
- Registering new subscribers and requesting the issuance of certificates
- Requesting, approving and executing the revocation of certificates

5.2.2 Number of persons required per task

Roles which are relevant to assure seamless and continuous PKI operation will be occupied by two persons. Security-critical tasks require multi-party control by two HSM Security Officers.

5.2.3 Identification and authentication for each role

Trusted roles must identify themselves with username and password to be authenticated by the Porthos PKI system component and perform any actions set forth above for that role.

5.2.4 Roles requiring separation of duties

All trusted roles defined in 5.2.1 are held by different individuals. All roles except for RA Operator have one identity for accessing Porthos PKI system components.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

The Porthos PKI will be operated by qualified and trustworthy personnel.

5.3.2 Background check procedures

All Porthos PKI staff undergo normal employment reference checks.

5.3.3 Training requirements

Training for staff assigned to a trusted role is primarily via mentoring.

5.3.4 Retraining frequency and requirements

Not stipulated.

5.3.5 Job rotation frequency and sequence

Not stipulated.

5.3.6 Sanctions for unauthorized actions

Not stipulated

5.3.7 Independent contractor requirements

Independent contractors shall be permitted access to the CA's secure facilities only to the extent they are escorted and directly supervised by personnel holding trusted roles.

5.3.8 Documentation supplied to personnel

Personnel is provided with sufficient documentation to define duties and procedures for each role shall.

5.4 Audit logging procedures

For audit purposes, logs will be generated for events relating to the security and lifecycle of the Porthos PKI. Where possible, the audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, will be retained and made available during compliance audits.

5.4.1 Types of events recorded

At least, the following types of events shall be recorded:

- CA certificate lifecycle management, including certificate issuance and revocation
- CA rollover, including generation of new CA keys
- Subscriber certificate lifecycle management, including successful and unsuccessful certificate applications, certificate issuances and certificate re-keying
- Subscriber certificate revocation requests, including revocation reason
- Creation and publishing of CRLs
- Software updates of issuing CAs
- Unplanned system failure or downtime

5.4.2 Frequency of processing log

No regular log reviewing will be applied. Logs may be reviewed during the Porthos PKI audit or on in case of unexpected behavior. Some automatically logged events such as system failure may generate an alarm to the PKI Administrators.

5.4.3 Retention period for audit log

Audit logs will be retained onsite for at least 12 months.

5.4.4 Protection of audit log

Only PKI Administrators have the system level access required to modify or delete logs.

5.4.5 Audit log backup procedures

Audit logs will be regularly backed up.

5.4.6 Audit collection system (internal vs. external)

Not stipulated.

5.4.7 Notification to event-causing subject

Not stipulated.

5.4.8 Vulnerability assessments

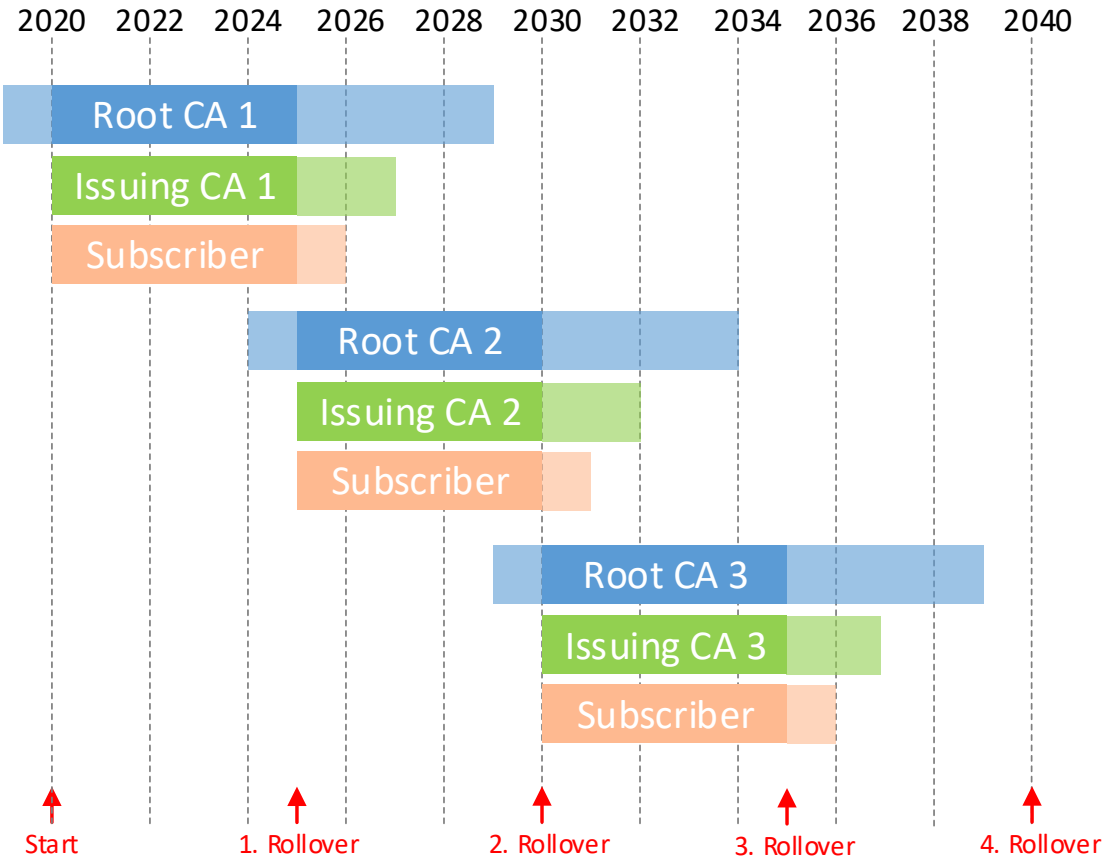
Not stipulated.

5.5 Records archival

Omitted.

5.6 Key changeover

To minimize risk from compromise of a CA's private signing key, all CAs of the Porthos PKI will be replaced by a new generation after 5 years of active operation. From that time on, only the new key will be used to sign CA and subscriber certificates. Since the old private key is used to sign CRLs that cover certificates signed with that key, the old key will be retained and protected. The CA rollover is visualized in the following graphics.



To provide a fallback when the CA rollover cannot be completed in time, the Issuing CA has a validity of 7 years. The Root CA certificate has a lifetime of 10 years and will be distributed 1 year in advance to update all subscribers prior to the rollover. The Root CA provides an operational reserve of 2 years at the end of an Issuing CA certificates lifetime.

5.7 Compromise and disaster recovery

All incidents (including compromises), both suspected and actual, are reported to the Security Officer of LEGIC Identsystems for investigation and will be handled by LEGIC's Business Continuity Management (BCM) process.

5.8 CA or RA termination

In case of termination of the Porthos PKI operations according to this contract, the following measures will be instigated:

- Revocation of all subscriber certificates which are still unrevoked or unexpired at the end of the termination notice period
- Generation and publication of each CA's CRL with the *nextUpdate* field set to a time after the expiration of all issued subscriber certificates. This CRL will be at least available for download until the *nextUpdate* date.
- Destruction of all private keys held by each CA or export of the keys to a successor.

6. Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

Cryptographic key pairs for the root and issuing CAs of the Porthos PKI are generated directly by and within a FIPS 140-2 level 3 validated Hardware Security Module (HSM) using a dedicated command line tool. The CA keys are always protected by the HSM.

CA keys will be generated in a key generation ceremony using multi-person control as per section 6.2.2. CA key generation in the HSM shall be documented in a verifiable audit trail.

Subscribers' cryptographic key pairs shall be generated by the subscribers themselves on systems that the subscribers can access.

6.1.2 Private key delivery to subscriber

The Porthos PKI does not generate key pairs for subscribers and thus makes no provisions for delivery of private keys.

6.1.3 Public key delivery to certificate issuer

The certificate application including the CSR formatted as a self-signed PKCS#10 structure shall be submitted to the issuing CA using a secure communication channel (e.g. TLS).

6.1.4 CA public key delivery to relying parties

All relying parties may download the root and any issuing CA's public key from the repository defined in 2.1.

The public key of the root CA shall be provided to the relying parties in a secure manner so that the trust anchor is not vulnerable to modification or substitutions. Acceptable methods for delivery of a trust anchor include but are not limited to:

- In case of IoT devices as the relying party: Downloading by firmware update via secure out-of-band mechanism
- Loading a trust anchor onto tokens delivered to relying parties via secure mechanisms
- Comparison of certificate hash (fingerprint) against the trust anchor hash made available via authenticated out-of-band sources
- Use of a link certificate which contains the public key of the trust anchor signed by a currently valid trust anchor

6.1.5 Key sizes

The first CA generation of the Porthos PKI (see 5.6) uses the NIST-P256 elliptic curve algorithm (with SHA-256 checksums) for digital signatures. Security strength of the algorithms will be re-evaluated based on the NIST recommendations prior to a CA rollover and adapted if appropriate.

6.1.6 Public key parameters generation and quality checking

Not applicable.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Key usage purposes and restrictions on the same are stipulated in the appropriate X.509 v3 key usage field (see 7.1).

6.2 Private key protection and cryptographic module engineering controls

6.2.1 Cryptographic module standards and controls

The HSMs used to generate and store CA keys are certified and operated according to the FIPS 140-2 Level 3 standard.

The private key of a Porthos high assurance IoT device shall be generated and stored in an SE having at least EAL5 compliancy.

Other subscriber's private key may be generated and/or stored in a software or hardware token, e.g. in a file or on a cryptographic smartcard.

6.2.2 Private key (n out of m) multi-person control

Creation and deletion of all CA private keys require control by two HSM Security Officers.

Activation, usage and deactivation of the private key for the offline root CA requires control by two HSM Security Officers. The root CA private key will only be activated for a short period to sign CA certificates and the CRL of the root CA.

Activation of the private key for the online issuing CAs do not require two-party control. Once activated, online issuing CAs can use their private key to generate certificate signatures.

6.2.3 Private key escrow

Not stipulated.

6.2.4 Private key backup

Private keys of the CAs stored in the HSM are backed up with mechanisms provided by the HSM. The resulting encrypted HSM backup files are stored in on-site repositories.

6.2.5 Private key archival

Not stipulated.

6.2.6 Private key transfer into or from a cryptographic module

The CA private keys never leave the HSM in normal operation. If the HSM equipment provider needs to be changed for whatever reason, the CA private keys may be transferred in encrypted form into the new HSM using multi-person control.

6.2.7 Private key storage on cryptographic module

See 6.2.1.

6.2.8 Method of activating private key

See 6.2.2

6.2.9 Method of deactivating private key

See 6.2.2.

6.2.10 Method of destroying private key

See 6.2.2.

6.2.11 Cryptographic module rating

See 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys are archived as part of the certificate archival.

6.3.2 Certificate operational periods and key pair usage periods

The period of use for a key pair will correspond to the term of validity of the certificate based on that key pair. See 4.7.1 for key pair lifetimes.

6.4 Activation data

Activation data are pass-phrases that protect private keys and are entered and/or used to unlock and activate these for the purposes of certification, signature and decryption.

The password to access the root CA keys has a length of 32 characters and is divided into two halves generated and shared by two HSM Security Officers. Each half is stored in the HSM Security Officer's personal password manager tool and protected by his individual master password.

The password of each issuing CA key has a minimum length of 20 characters and is stored in a data vault of the CA operating system and as a backup in a data vault accessible by the PKI Administrators.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

The online issuing CA applications of the Porthos PKI run on cloud-based services from AWS which meet the requirements of the most security-sensitive organizations.
Software components and operating systems will be maintained and updated on a regular basis to minimize the risk of security breaches. Administration access to these systems is only granted to persons acting in trusted roles.

6.5.2 Computer security rating

Not stipulated.

6.6 Life cycle technical controls

6.6.1 System development controls

Third-party software is only deployed after passing internal tests.

6.6.2 Security management controls

Not stipulated.

6.6.3 Life cycle security controls

Not stipulated.

6.7 Network Security Controls

The online issuing CAs of the Porthos PKI run within Virtual Private Clouds (VPC) of AWS. Public access to these CAs is protected by firewalls to filter unwanted protocols.

6.8 Timestamping

The Porthos PKI does not make use of time stamping. Date/times set in CRLs and certificates are based on the time of the underlying operating system.

7. Certificate, CRL, and OCSP profiles

7.1 Certificate profile

Certificates issued by the Porthos PKI are compliant with the X.509 version 3 certificate format as defined in [RFC 5280]. This clause contains the certificate profiles issued by the first CA generation of the Porthos PKI. Profiles of future CA generations may be listed here once they become valid.

7.1.1 Porthos root CA certificate profiles

7.1.1.1 Porthos Root CA

Certificate field	Value (Porthos Prod. PKI)	Value (Porthos Non-Prod PKI)
Version	V3 (0x2)	V3 (0x2)
Serial number	b8ec04ef98cdfebc	e2d3d4a3294ec782
Issuer	CN=Porthos Root CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos Root CA 1 O=dormakaba C=CH
Not before	Aug 19 07:00:00 2019 GMT	Aug 19 07:00:00 2019 GMT
Not after	Aug 19 07:00:00 2029 GMT	Aug 19 07:00:00 2029 GMT
Subject	CN=Porthos Root CA 1 O=dormakaba C=CH	CN=Porthos Root CA 1 O=dormakaba C=CH
Public key algorithm	prime256v1 (OID: 1.2.840.10045.3.1.7)	prime256v1 (OID: 1.2.840.10045.3.1.7)
Public key	EC 256 bit	EC 256 bit
Authority key identifier	6a84e371168997e8595553c71d49c12e5b51d31d	942d1526121ffa4a9dd501d041ffe52b81611ceb
Subject key identifier	6a84e371168997e8595553c71d49c12e5b51d31d	942d1526121ffa4a9dd501d041ffe52b81611ceb
Key usage	critical, certSign, crlSign	critical, certSign, crlSign
Basic constraints	critical, CA:true, pathlength:not set	critical, CA:true, pathlength:not set
Signature algorithm	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)

7.1.1.2 Porthos Link Root CA

A Link Root CA Certificate will be issued when the first CA rollover is executed (see 5.6).

7.1.2 Porthos issuing CA certificate profiles

7.1.2.1 Porthos High Assurance Device CA

Certificate field	Value (Porthos Prod. PKI)	Value (Porthos Non-Prod PKI)
Version	V3 (0x2)	V3 (0x2)
Serial number	1	01
Issuer	CN=Porthos Root CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos Root CA 1 O=dormakaba C=CH
Not before	Aug 19 07:00:00 2020 GMT	Aug 19 07:00:00 2020 GMT
Not after	Aug 19 07:00:00 2027 GMT	Aug 19 07:00:00 2027 GMT
Subject	CN=Porthos High Assurance Device CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos High Assurance Device CA 1 O=dormakaba C=CH
Public key algorithm	prime256v1 (OID: 1.2.840.10045.3.1.7)	prime256v1 (OID: 1.2.840.10045.3.1.7)
Public key	EC 256 bit	EC 256 bit
Authority key identifier	6a84e371168997e8595553c71d49c12e5b51d31d	942d1526121ffa4a9dd501d041ffe52b81611ceb
Subject key identifier	e9a59215678b89bec09b999b8442e5b7cabf0548	b22c491931331c95f7aa7697f8b50ac072f04702
CDP	http://crl.pki.porthos.services/root-ca-1.crl	http://crl.pki.porthos.io/root-ca-1.crl
AIA	http://crt.pki.porthos.services/root-ca-1.crt	http://crt.pki.porthos.io/root-ca-1.crt
Key usage	critical, certSign, crlSign	critical, certSign, crlSign
Basic constraints	critical, CA:true, pathlength:0	critical, CA:true, pathlength:0
Signature algorithm	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)

7.1.2.2 Porthos Standard Assurance Device CA

Certificate field	Value (Porthos Prod. PKI)	Value (Porthos Non-Prod PKI)
Version	V3 (0x2)	V3 (0x2)
Serial number	2	02
Issuer	CN=Porthos Root CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos Root CA 1 O=dormakaba C=CH
Not before	Aug 19 07:00:00 2020 GMT	Aug 19 07:00:00 2020 GMT
Not after	Aug 19 07:00:00 2027 GMT	Aug 19 07:00:00 2027 GMT
Subject	CN=Porthos Standard Assurance Device CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos Standard Assurance Device CA 1 O=dormakaba C=CH
Public key algorithm	prime256v1 (OID: 1.2.840.10045.3.1.7)	prime256v1 (OID: 1.2.840.10045.3.1.7)
Public key	EC 256 bit	EC 256 bit
Authority key identifier	6a84e371168997e8595553c71d49c12e5b51d31d	942d1526121ffa4a9dd501d041ffe52b81611ceb
Subject key identifier	ed2b269376d85656393dec2c9e09cf478232b0c2	686faa51d6d4c3a8d7a925ae7fb67d87fa3340e8
CDP	http://crl.pki.porthos.services/root-ca-1.crl	http://crl.pki.porthos.io/root-ca-1.crl
AIA	http://crt.pki.porthos.services/root-ca-1.crt	http://crt.pki.porthos.io/root-ca-1.crt
Key usage	critical, certSign, crlSign	critical, certSign, crlSign
Basic constraints	critical, CA:true, pathlength:0	critical, CA:true, pathlength:0
Signature algorithm	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)

7.1.2.3 Porthos Infrastructure CA

Certificate field	Value (Porthos Prod. PKI)	Value (Porthos Non-Prod PKI)
Version	V3 (0x2)	V3 (0x2)
Serial number	3	03
Issuer	CN=Porthos Root CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos Root CA 1 O=dormakaba C=CH
Not before	Aug 19 07:00:00 2020 GMT	Aug 19 07:00:00 2020 GMT
Not after	Aug 19 07:00:00 2027 GMT	Aug 19 07:00:00 2027 GMT
Subject	CN=Porthos Infrastructure CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos Infrastructure CA 1 O=dormakaba C=CH
Public key algorithm	prime256v1 (OID: 1.2.840.10045.3.1.7)	prime256v1 (OID: 1.2.840.10045.3.1.7)
Public key	EC 256 bit	EC 256 bit
Authority key identifier	6a84e371168997e8595553c71d49c12e5b51d31d	942d1526121ffa4a9dd501d041ffe52b81611ceb
Subject key identifier	a47b102814a25a9038b0af61cd6a99b0d1f4bc4d	a8daef52d730940058c7d0ad663806722d3cc521
CDP	http://crl.pki.porthos.services/root-ca-1.crl	http://crl.pki.porthos.io/root-ca-1.crl
AIA	http://crt.pki.porthos.services/root-ca-1.crt	http://crt.pki.porthos.io/root-ca-1.crt
Key usage	critical, certSign, crlSign	critical, certSign, crlSign
Basic constraints	critical, CA:true, pathlength:0	critical, CA:true, pathlength:0
Signature algorithm	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)

7.1.2.4 Porthos User CA

Certificate field	Value (Porthos Prod. PKI)	Value (Porthos Non-Prod PKI)
Version	V3 (0x2)	V3 (0x2)
Serial number	4	04
Issuer	CN=Porthos Root CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos Root CA 1 O=dormakaba C=CH
Not before	Aug 19 07:00:00 2020 GMT	Aug 19 07:00:00 2020 GMT
Not after	Aug 19 07:00:00 2027 GMT	Aug 19 07:00:00 2027 GMT
Subject	CN=Porthos User CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos User CA 1 O=dormakaba C=CH
Public key algorithm	prime256v1 (OID: 1.2.840.10045.3.1.7)	prime256v1 (OID: 1.2.840.10045.3.1.7)
Public key	EC 256 bit	EC 256 bit
Authority key identifier	6a84e371168997e8595553c71d49c12e5b51d31d	942d1526121ffa4a9dd501d041ffe52b81611ceb
Subject key identifier	817ef4fa4d2bf45e61336d805104550612c8a987	0fdbd20c662089c1f59fb886db36ca7792ccaa18
CDP	http://crl.pki.porthos.services/root-ca-1.crl	http://crl.pki.porthos.io/root-ca-1.crl
AIA	http://crt.pki.porthos.services/root-ca-1.crt	http://crt.pki.porthos.io/root-ca-1.crt
Key usage	critical, certSign, crlSign	critical, certSign, crlSign
Basic constraints	critical, CA:true, pathlength:0	critical, CA:true, pathlength:0
Signature algorithm	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)

7.1.3 Porthos subscriber certificate profiles

7.1.3.1 Porthos High Assurance IoT Device

Certificate field	Value (Porthos Prod. PKI)	Value (Porthos Non-Prod PKI)
Version	V3 (0x2)	V3 (0x2)
Serial number	*<Unique serial number within issuing CA>*	*<Unique serial number within issuing CA>*
Issuer	CN=Porthos High Assurance Device CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos High Assurance Device CA 1 O=dormakaba C=CH
Not before	*<now>*	*<now>*
Not after	*<now + 13 months>*	*<now + 13 months>*
Subject	CN=*<CN from CSR (UUID)>* OU=Porthos HA Device O=dormakaba	CN=*<CN from CSR (UUID)>* OU=Porthos HA Device O=dormakaba
Public key algorithm	prime256v1 (OID: 1.2.840.10045.3.1.7)	prime256v1 (OID: 1.2.840.10045.3.1.7)
Public key	EC 256 bit	EC 256 bit
Authority key identifier	e9a59215678b89bec09b999b8442e5b7cabf0548	b22c491931331c95f7aa7697f8b50ac072f04702
Subject key identifier	*<Key ID>*	*<Key ID>*
CDP	http://crl.pki.porthos.services/ha-device-ca-1.crl	http://crl.pki.porthos.io/ha-device-ca-1.crl
AIA	http://crt.pki.porthos.services/ha-device-ca-1.crt	http://crt.pki.porthos.io/ha-device-ca-1.crt
Key usage	critical, digitalSignature, keyAgreement	critical, digitalSignature, keyAgreement
Extended key usage	TLS Web Client Authentication (OID: 1.3.6.1.5.5.7.3.2)	TLS Web Client Authentication (OID: 1.3.6.1.5.5.7.3.2)
Basic constraints	critical, CA:false	critical, CA:false
Signature algorithm	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)

7.1.3.2 Porthos Standard Assurance IoT Device

Certificate field	Value (Porthos Prod. PKI)	Value (Porthos Non-Prod PKI)
Version	V3 (0x2)	V3 (0x2)
Serial number	*<Unique serial number within issuing CA>*	*<Unique serial number within issuing CA>*
Issuer	CN=Porthos Standard Assurance Device CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos Standard Assurance Device CA 1 O=dormakaba C=CH
Not before	*<now>*	*<now>*
Not after	*<now + 13 months>*	*<now + 13 months>*
Subject	CN=*<CN from CSR (UUID)>* OU=Porthos SA Device O=dormakaba	CN=*<CN from CSR (UUID)>* OU=Porthos SA Device O=dormakaba
Public key algorithm	prime256v1 (OID: 1.2.840.10045.3.1.7)	prime256v1 (OID: 1.2.840.10045.3.1.7)
Public key	EC 256 bit	EC 256 bit
Authority key identifier	ed2b269376d85656393dec2c9e09cf478232b0c2	686faa51d6d4c3a8d7a925ae7fb67d87fa3340e8
Subject key identifier	*<Key ID>*	*<Key ID>*
CDP	http://crl.pki.porthos.services/sa-device-ca-1.crl	http://crl.pki.porthos.io/sa-device-ca-1.crl
AIA	http://crt.pki.porthos.services/sa-device-ca-1.crt	http://crt.pki.porthos.io/sa-device-ca-1.crt
Key usage	critical, digitalSignature, keyAgreement	critical, digitalSignature, keyAgreement
Extended key usage	TLS Web Client Authentication (OID: 1.3.6.1.5.5.7.3.2)	TLS Web Client Authentication (OID: 1.3.6.1.5.5.7.3.2)
Basic constraints	critical, CA:false	critical, CA:false
Signature algorithm	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)

7.1.3.3 Porthos TLS Client

Certificate field	Value (Porthos Prod. PKI)	Value (Porthos Non-Prod PKI)
Version	V3 (0x2)	V3 (0x2)
Serial number	*<Unique serial number within issuing CA>*	*<Unique serial number within issuing CA>*
Issuer	CN=Porthos Infrastructure CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos Infrastructure CA 1 O=dormakaba C=CH
Not before	*<now>*	*<now>*
Not after	*<now + 13 months>*	*<now + 13 months>*
Subject	CN=*<CN from CSR (FQDN of host:application)>* OU=Porthos client O=dormakaba	CN=*<CN from CSR (FQDN of host:application)>* OU= Porthos client O=dormakaba
Public key algorithm	prime256v1 (OID: 1.2.840.10045.3.1.7)	prime256v1 (OID: 1.2.840.10045.3.1.7)
Public key	EC 256 bit	EC 256 bit
Authority key identifier	a47b102814a25a9038b0af61cd6a99b0d1f4bc4d	a8daef52d730940058c7d0ad663806722d3cc521
Subject key identifier	*<Key ID>*	*<Key ID>*
CDP	http://crl.pki.porthos.services/infrastructure-ca-1.crl	http://crl.pki.porthos.io/infrastructure-ca-1.crl
AIA	http://crt.pki.porthos.services/infrastructure-ca-1.crt	http://crt.pki.porthos.io/infrastructure-ca-1.crt
Key usage	critical, digitalSignature, keyAgreement	critical, digitalSignature, keyAgreement
Extended key usage	TLS Web Client Authentication (OID: 1.3.6.1.5.5.7.3.2)	TLS Web Client Authentication (OID: 1.3.6.1.5.5.7.3.2)
Basic constraints	critical, CA:false	critical, CA:false
Signature algorithm	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)

7.1.3.4 Porthos TLS Server

Certificate field	Value (Porthos Prod. PKI)	Value (Porthos Non-Prod PKI)
Version	V3 (0x2)	V3 (0x2)
Serial number	*<Unique serial number within issuing CA>*	*<Unique serial number within issuing CA>*
Issuer	CN=Porthos Infrastructure CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos Infrastructure CA 1 O=dormakaba C=CH
Not before	*<now>*	*<now>*
Not after	*<now + 13 months>*	*<now + 13 months>*
Subject	CN=*<CN from CSR (FQDN of host)>* OU=Porthos service O=dormakaba	CN=*<CN from CSR (FQDN of host)>* OU= Porthos service O=dormakaba
Public key algorithm	prime256v1 (OID: 1.2.840.10045.3.1.7)	prime256v1 (OID: 1.2.840.10045.3.1.7)
Public key	EC 256 bit	EC 256 bit
Authority key identifier	a47b102814a25a9038b0af61cd6a99b0d1f4bc4d	a8daef52d730940058c7d0ad663806722d3cc521
Subject key identifier	*<Key ID>*	*<Key ID>*
CDP	http://crl.pki.porthos.services/infrastructure-ca-1.crl	http://crl.pki.porthos.io/infrastructure-ca-1.crl
AIA	http://crt.pki.porthos.services/infrastructure-ca-1.crt	http://crt.pki.porthos.io/infrastructure-ca-1.crt
Key usage	critical, digitalSignature, keyAgreement, keyEncipherment	critical, digitalSignature, keyAgreement, keyEncipherment
Extended key usage	TLS Web Server Authentication (OID: 1.3.6.1.5.5.7.3.1)	TLS Web Server Authentication (OID: 1.3.6.1.5.5.7.3.1)
Basic constraints	critical, CA:false	critical, CA:false
Signature algorithm	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)

7.1.3.5 Porthos User

Certificate field	Value (Porthos Prod. PKI)	Value (Porthos Non-Prod PKI)
Version	V3 (0x2)	V3 (0x2)
Serial number	*<Unique serial number within issuing CA>*	*<Unique serial number within issuing CA>*
Issuer	CN=Porthos User CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos User CA 1 O=dormakaba C=CH
Not before	*<now>*	*<now>*
Not after	*<now + 13 months>*	*<now + 13 months>*
Subject	CN=*<CN from CSR (user name)>* OU=Porthos user O=dormakaba	CN=*<CN from CSR (user name)>* OU= Porthos user O=dormakaba
Public key algorithm	prime256v1 (OID: 1.2.840.10045.3.1.7)	prime256v1 (OID: 1.2.840.10045.3.1.7)
Public key	EC 256 bit	EC 256 bit
Authority key identifier	817ef4fa4d2bf45e61336d805104550612c8a987	0fdbd20c662089c1f59fb886db36ca7792ccaa18
Subject key identifier	*<Key ID>*	*<Key ID>*
CDP	http://crl.pki.porthos.services/user-ca-1.crl	http://crl.pki.porthos.io/user-ca-1.crl
AIA	http://crt.pki.porthos.services/user-ca-1.crt	http://crt.pki.porthos.io/user-ca-1.crt
Key usage	critical, digitalSignature, keyAgreement	critical, digitalSignature, keyAgreement
Extended key usage	TLS Web Client Authentication (OID: 1.3.6.1.5.5.7.3.2)	TLS Web Client Authentication (OID: 1.3.6.1.5.5.7.3.2)
Basic constraints	critical, CA:false	critical, CA:false
Signature algorithm	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)

7.1.4 AWS CA Verification Certificate profiles

7.1.4.1 Porthos High Assurance Device CA

Certificate field	Value (Porthos Prod. PKI)	Value (Porthos Non-Prod PKI)
Version	V3 (0x2)	V3 (0x2)
Serial number	*<Unique serial number within issuing CA>*	*<Unique serial number within issuing CA>*
Issuer	CN=Porthos High Assurance Device CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos High Assurance Device CA 1 O=dormakaba C=CH
Not before	*<now>*	*<now>*
Not after	*<now + 5 days>*	*<now + 5 days>*
Subject	CN=*<AWS registration code>*	CN=*<AWS registration code>*
Public key algorithm	rsaEncrypt (OID: 1.2.840.113549.1.1.1)	rsaEncrypt (OID: 1.2.840.113549.1.1.1)
Public key	RSA 2048 bit	RSA 2048 bit
Authority key identifier	e9a59215678b89bec09b999b8442e5b7cabf0548	b22c491931331c95f7aa7697f8b50ac072f04702
Subject key identifier	*<Key ID>*	*<Key ID>*
CDP	http://crl.pki.porthos.services/ha-device-ca-1.crl	http://crl.pki.porthos.io/ha-device-ca-1.crl
AIA	http://crt.pki.porthos.services/ha-device-ca-1.crt	http://crt.pki.porthos.io/ha-device-ca-1.crt
Key usage	critical, digitalSignature	critical, digitalSignature
Basic constraints	critical, CA:false	critical, CA:false
Signature algorithm	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)

7.1.4.2 Porthos Standard Assurance Device CA

Certificate field	Value (Porthos Prod. PKI)	Value (Porthos Non-Prod PKI)
Version	V3 (0x2)	V3 (0x2)
Serial number	*<Unique serial number within issuing CA>*	*<Unique serial number within issuing CA>*
Issuer	CN=Porthos Standard Assurance Device CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos Standard Assurance Device CA 1 O=dormakaba C=CH
Not before	*<now>*	*<now>*
Not after	*<now + 5 days>*	*<now + 5 days>*
Subject	CN=*<AWS registration code>*	CN=*<AWS registration code>*
Public key algorithm	rsaEncrypt (OID: 1.2.840.113549.1.1.1)	rsaEncrypt (OID: 1.2.840.113549.1.1.1)
Public key	RSA 2048 bit	RSA 2048 bit
Authority key identifier	ed2b269376d85656393dec2c9e09cf478232b0c2	686faa51d6d4c3a8d7a925ae7fb67d87fa3340e8
Subject key identifier	*<Key ID>*	*<Key ID>*
CDP	http://crl.pki.porthos.services/sa-device-ca-1.crl	http://crl.pki.porthos.io/sa-device-ca-1.crl
AIA	http://crt.pki.porthos.services/sa-device-ca-1.crt	http://crt.pki.porthos.io/sa-device-ca-1.crt
Key usage	critical, digitalSignature	critical, digitalSignature
Basic constraints	critical, CA:false	critical, CA:false
Signature algorithm	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)

7.2 CRL Profile

CLRs issued by the Porthos PKI are compliant with X.509 version 2 CRL profile as described in [RFC 5280].

7.2.1 CRL of Porthos Root CA

Certificate field	Value (Porthos Prod. PKI)	Value (Porthos Non-Prod PKI)
Version	V2 (0x1)	V2 (0x1)
Signature	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)
Issuer	CN=Porthos Root CA 1 O=dormakaba C=CH	CN=Non-Prod Porthos Root CA 1 O=dormakaba C=CH
This Update	*<time of issuance>*	*<time of issuance >*
Next Update	*<time of issuance + 2 years>*	*<time of issuance + 2 years>*
Revocations list		
Serial number	*<serial number of revoked certificate>*	*<serial number of revoked certificate>*
Date	*<date of revocation>*	*<date of revocation>*
Reason	*<reason code defined by [RFC 5280]>*	*<reason code defined by [RFC 5280]>*
CRL extensions		
Authority key identifier	6a84e371168997e8595553c71d49c12e5b51d31d	942d1526121ffa4a9dd501d041ffe52b81611ceb
CRL number	*<Incremental number of CRL>*	*<Incremental number of CRL>*
Signature		
Signature algorithm	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)
Signature	*<signature>*	*< signature >*

7.2.2 CRL of Porthos Issuing CAs

Certificate field	Value (Porthos Prod. and Non-Prod PKI)
Version	V2 (0x1)
Signature	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)
Issuer	CN=*<CN of issuing CA>* O=dormakaba C=CH
This Update	*<time of issuance>*
Next Update	*<time of issuance + 28 days>*
Revocations list	
Serial number	*<serial number of revoked certificate>*
Date	*<date of revocation>*
Reason	*<reason code defined by [RFC 5280]>*
CRL extensions	
Authority key identifier	*<Key ID of issuing CA>*
CRL number	*<Incremental number of CRL>*
Signature	
Signature algorithm	ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)
Signature	*<signature>*

7.3 OCSP Profile

Not applicable.

8. Compliance audit and other assessment

8.1 Frequency or circumstances of assessment

Compliance with this CP/CPS shall be ensured by a regular internal or external audit. Unscheduled audits may be executed if special security-related events occur.

8.2 Identity/qualifications of assessor

Internal audits will be executed by the Auditor role. The assigned person shall have the necessary knowledge and skills about PKI, IT security and auditing.

8.3 Assessor's relationship to assessed entity

The assigned Auditor shall not take over other roles for the operation of the Porthos PKI.

8.4 Topics covered by assessment

The audit shall ensure that all procedures and processes applied to operate the Porthos PKI are carried out in compliance with the provisions of this CP/CPS. Topics to be audited will be defined by the auditor.

8.5 Actions taken as a result of deficiency

The results of the audit will be documented in an audit report. If deficiencies are found, the auditor defines the necessary measures and the time to solve them. In case of a severe security-related deficiency, the auditor must report it to the LEGIC management which decides about the measures and period to solve it.

8.6 Communication of results

Internal audits will not be publicly available. LEGIC will disclose to Client upon request a security report generated by internal or external bodies. Such reports are disclosed only at the premises of LEGIC. This right may not be assigned in full or in part to any third party, without prior written consent of LEGIC.

9. Other business and legal matters

Fees and other business and legal matters are regulated in the contractual agreement between the concerned parties. Therefore, this section is not stipulated.

Appendix A Definitions

Authorized Organizational Representative (AOR): A person within an organization who is authorized to vouch for non-person identities. Any AOR is not permanently linked to any non-person identity; the CA must only ascertain that the AOR is legitimately associated with the organization, and that the AOR is identified as having authority for the identity in question

AWS CA Verification Certificate: Special type of certificate which is required to register a CA certificate with AWS IoT service in order to verify IoT device certificates signed by that CA.

Basic Constraints: Means an extension that specifies whether the subject of the Certificate may act as a CA or only as an end-entity

Certificate: An electronic document that uses a digital signature to bind a Public Key and an entity

Certificate Authority (CA): Component of the PKI that holds the private key of the issuing certificate and signs a Subscriber's certificate after its CSR was approved by the RA.

Certificate Signing Request (CSR): A message sent from a Subscriber to the RA of the PKI in order to apply for a digital certificate. The CSR usually contains the Public Key for which the Certificate should be issued, identifying information (such as a domain name) and a digital signature

Certificate Policy: Means a statement of the issuer that corresponds to the prescribed usage of a digital Certificate within an issuance context

Certificate Revocation List (CRL): List of certificates that have been declared invalid. This list is issued by the CA at regular intervals

Device Manufacturer Certificate (DMC): A certificate and its corresponding private key, which is stored in a hardened hardware module, i.e. an SE. The DMC proofs the hardware identity and manufacturer and serves as an initial root of trust to other relying parties

Distinguished Name (DN): The Distinguished Name uniquely identifies either the subject or issuer in an X.509 certificate. A DN consists of the mandatory Common Name (CN) attribute, which may be followed by optional attributes, such as Organization (O), Organizational Unit (OU), Country Name (C), etc.

Fully Qualified Domain Name (FQDN): A domain name that specifies all domain levels, including the top-level domain. An FQDN is distinguished by its lack of ambiguity and can be interpreted only in one way.

Link Root CA Certificate: A CA certificate that is used to establish a trust relationship between two Root CAs.

Online Certificate Status Protocol (OCSP): An Internet protocol used for obtaining the revocation status of an X.509 digital certificate

PKI-Customer: An organization that has entered a business relationship with LEGIC for the hosting and operation of its PKI. The PKI-Customer may operate some PKI components such as the RA service

Private Key: The key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key

Public Key: The key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key

Registration Authority (RA): An individual or application that verifies the identity of Subscribers requesting their digital certificates and tells the Certificate Authority (CA) to issue it.

Relying Party: An entity that relies upon the information contained within the Certificate

Revocation: Invalidation of a certificate. Every CA regularly issues a list of revoked certificates called CRL. This list should be verified by all Relying Parties using certificates from that CA before trusting a certificate.

Rollover: To rollover a certificate means that a new certificate is issued while the old one is still valid and usable. The CA rollover is used to issue a new CA certificate while keeping the old one valid along with all the certificates issued with it.

Secure Element (SE): A tamper-resistant hardware platform, capable of securely hosting applications and storing confidential and cryptographic data

Subject: Field in the certificate that identifies the owner of it. Also referred to as distinguished name (DN).

Subscriber: An entity that has been issued a Certificate

Transport Layer Security (TLS): A protocol that enables secure transactions via the Internet.

Trusted Third Party (TTP): An entity which facilitates interactions between two parties who both trust the third party.

Universally Unique Identifier (UUID): A randomly generated 128-bit number used to identify information in computer systems. UUID objects are defined in [RFC 4122]

Appendix B Acronyms

AIA	Authority Information Access
API	Application Programming Interface
AWS	Amazon Web Services
CA	Certification Authority
CDP	Certification Distribution Point
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
DMC	Device Manufacturer Certificate
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
OSCP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RA	Registration Authority
RPC	Remote Procedure Call
SE	Secure Element
TLS	Transport Layer Security
TTP	Trusted Third Party
URI	Uniform Resource Identifier
UUID	Universal Unique Identifier
VPC	Virtual Private Cloud

Appendix C References

[RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. D. Cooper etal, May 2008
https://www.ietf.org/rfc/rfc5280.txt

[RFC 3647] Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003
https://www.ietf.org/rfc/rfc3647.txt

[RFC 4122] A Universally Unique IDentifier (UUID) URN Namespace, Paul J. Leach, Michael Mealling, and Rich Salz, July 2005.
https://www.ietf.org/rfc/rfc4122.txt