Certification Practice Statement
Of
PHOENIX CONTACT
Device PKI

Document status: Valid

CS-IT-000002 -01- 2021-09

Last Modified: September 2021

Document History

Version	Date	Description
01	13.09.2021	Initial version

Content

1. Introduction

1.1. Overview

This document is the Certification Practice Statement (CPS) for the services provided by PHOENIX CONTACT GmbH & Co. KG related to public key certificates for Initial Device Identification (IDevID) and code signing of firmware and secure boot software for members of the PHOENIX CONTACT group. In addition, a Time Stamp Service is also offered by PHOENIX CONTACT GmbH & Co. KG to members of the PHOENIX CONTACT group that is used in Code signing signatures.

Service Provider

The Trust Service Provider (TSP) – also in a legal sense - is

PHOENIX CONTACT GmbH & Co. KG

Flachsmarktstraße 8

D-32825 Blomberg

The outsourcing of services or parts of services under this CPS to third parties, partners or external providers, is not intended.

The TSP PHOENIX CONTACT GmbH & Co. KG (hereinafter referred to as PHOENIX CONTACT), represented by the management or their representatives, remains responsible for compliance with the procedures in the sense of this document or any legal or certification requirements for the TSP.

PHOENIX CONTACT also issues certificates for internal purposes only (e.g. TLS communication certificates). The management of these certificates is conducted by means of a purely internal Public Key Infrastructure (PKI) and is not subject to the present CPS.

Phoenix Contact group companies are such companies that are affiliated with PHOENIX CONTACT within the meaning of §§ 15 et seq. AktG (German Stock Corporation Act).

About this document

This CPS defines processes and procedures throughout the lifecycle of certificates issued for Certification Authorities (CA) and certificates issued for end-entities. Minimum measures are defined that must be fulfilled by all participants in the PKI.

This CPS refers to the Certificate Policy (CP) of PHOENIX CONTACT (cf. [CP]) for the issuing and management of Initial Device ID certificates and certificates for code signing of firmware and secure boot software with the Object Identifier 1.3.6.1.4.1.4346.2.2.2.1. It describes the realization or implementation of the requirements defined in the CP.

The processes and procedures described in this document allow certificate users and relying parties to trust the components of this PKI and PKI participants and to make decisions whether the level of trust and security granted by the PKI is suitable for applications.

The structure of the document follows the Internet standard RFC 3647 “Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practice Framework” [RFC 3647].

Properties of the PKI

The services offered by PHOENIX CONTACT are based on a multi-tiered PKI. Figure 1 shows the hierarchy of the PKI. It consists of a Root Certification Authority (Root-CA) followed by several Subordinated Certification Authorities (Sub-CA) or Intermediate CAs. The last Sub-CA in this chain is the so-called “issuing CA” that issues certificates for end entities. There is only one level of Sub-CAs.

Currently, there are three Sub-CAs for issuing end-entity certificates.

- Sub-CA for Initial Device Identities (CA-IDevID)
- Sub-CA for Code Signing (CA-CS)
- Sub-CA for Time Stamping (CA-TSA)

Due to a possible flexibilization, there can also be several Sub-CAs of the types CA-IDevID and CA-CS. However, these are organized on the same level.

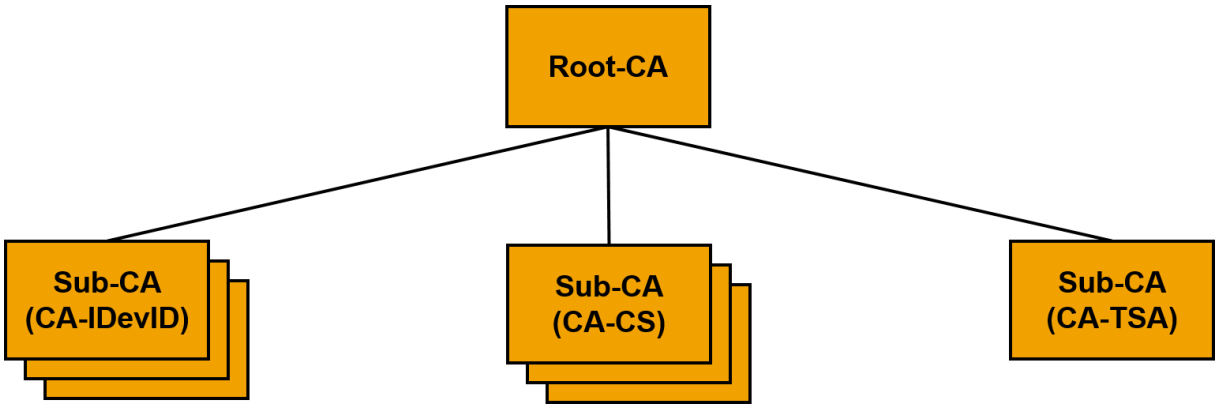

Figure 1: PHOENIX CONTACT multi-tiered PKI

It is intended to support different “cipher suites” in the PKI for the issuing and management of certificates. For this, RSA and ECDSA based on NIST curves as well as ECDSA on brainpool curves will be supported. However, a mixture of algorithms is not intended. Starting with the RSA, three separate multi-tiered PKI as shown in Figure 1 are thus to be operated in parallel in the future (see Figure 2).

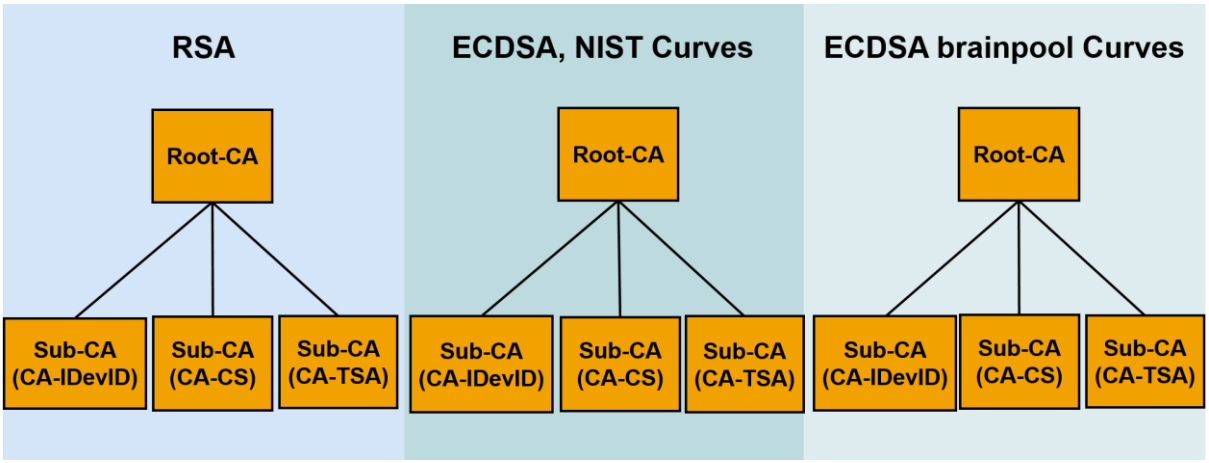

Figure 2: PHOENIX CONTACT multi-tiered PKI

1.2. Document name and identification

Name of document:	Certificate Practice Statement of PHOENIX CONTACT Device PKI
Object Identifier:	1.3.6.1.4.1.4346.2.2.2.1
Version:	01

1.3. PKI participants

Certification Authorities

Certification authorities that issue certificates and certificate revocation lists (CRL) are operated by PHOENIX CONTACT. The following types of certificates are possible:

- Certificates for Initial Device Identities (IDevID)
- Certificates for Code Signing Firmware (CS-FW)
- Certificates for Code Signing Secure Boot (CS-SB)
- Certification Authorities as Subordinated CAs and
- Root Certification Authorities.

Root Certification Authorities issue certificates only for Sub-CAs, i.e. all certificates issued by a Root-CA contain the `basicConstraint` extension with cA = TRUE. Sub-CAs issue certificates for end-entities (Issuing CA) or for further Sub-CAs. There is only a multi-tiered PKI with two CA levels, i.e. no Sub-CA issues certificates for an additional Sub-CA.

All Certification Authorities are identified by a Distinguished Name (cf. [X.501]) in the field issuer of the issued certificate or CRL. There is one exception, the issuing of CRLs by the Root-CA. For this, a dedicated Root-CA CRL signer (RCACRL) is established that is derived from a further Sub-CA (CA-RCACRL) for the issuing of CRL signer certificates for the Root-CA. So Figure 1 has to be adjusted as follows.

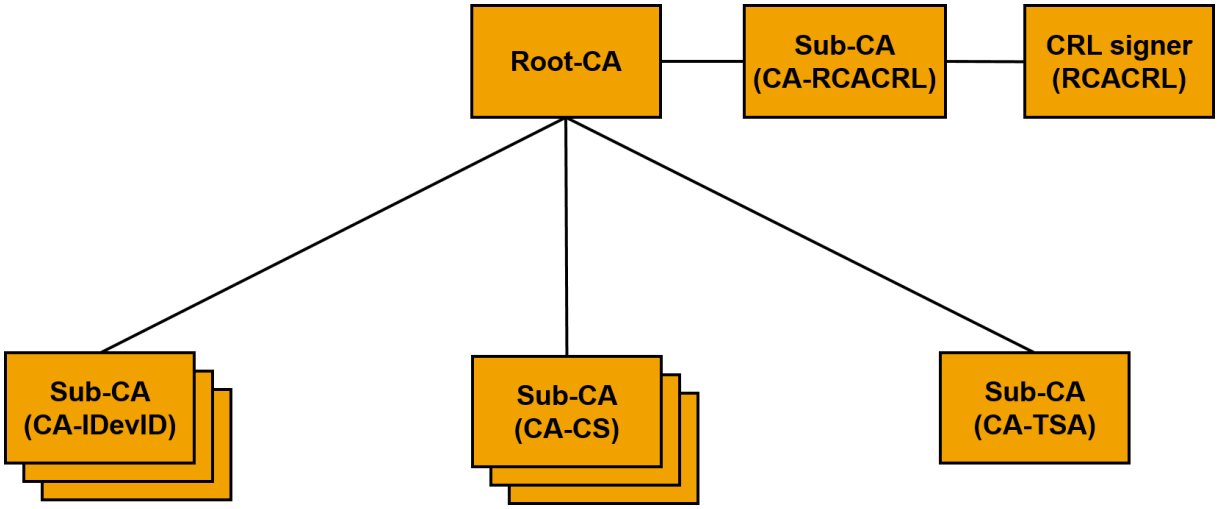

Figure 3: PHOENIX CONTACT multi-tiered PKI with Root-CA CRL signer

Registration Authorities

Local Registration Authorities for the issuance of IDevID certificates operate in an automated manner within the framework of the present CPS. For the issuance of code signing certificates as well as certificates for time stamp units, a manual process is established. Key pairs are generated by the end-entity which is a device for initial device identity or a signing server in case of code signing certificates or time stamp units. The end-entity in combination with the related application environment generates the certificate signing request that is submitted to the responsible CA. The responsible CA issues the certificate that is transferred back to the end-entity.

Subscribers

Subscriber of the certificates is PHOENIX CONTACT or a member of the PHOENIX CONTACT group.

Subject in initial device identity certificates is a device that is identified with a Distinguished Name (DN) that uniquely identifies the device. For this, the device serial number is part of the subject's DN.

Subject in code signing certificates is PHOENIX CONTACT or a member of the PHOENIX CONTACT group. A distinction is made between certificate subjects for signing firmware and secure boot software. In addition, the subject's name is a pseudonym instead of a name of a natural person. This holds also for subjects in certificates assigned to Time Stamp Units.

Relying Parties

Relying Parties are natural or legal persons or technical devices that uses the certificates issued by the PKI. For the initial device identity certificates relying parties are the customers of PHOENIX CONTACT group members who are able to verify the authenticity of PHOENIX CONTACT group devices.

In case of code signing certificates the relying party is the device that verifies the authenticity of the firmware loaded into the device or of the software in the boot process. This holds also for time stamps and their related certificates that are included in long term signature formats used for the signing of firmware and secure boot software.

Other Participants

There are no other participants in the PKI.

1.4. Certificate usage

The trust model used in the PKI based on this CPS is the chain model. Thus, all digital signatures and certificates have to be verified based on this model and for the verification the time of signature generation must be used.

For this, signature formats on firmware and secure boot software are used that contain a time stamp (CAdES, LT level at least) issued by a time stamp unit. It must be verified whether the time of signature generation lies within the validity period of the signer's certificate.

For certificates it must be verified that value `notBefore` of the certificate to be verified lies within the validity period of the related issuer certificate.

Appropriate certificate uses

Certification Authority certificates are used exclusively and in accordance with their extensions (e.g. `basicConstraints`) for the issuance of subordinate certificates and revocation lists.

The certificates of end-entities may be used for the application that are in accordance with the types of use specified in the certificate.

Initial Device Identity Certificates are used by PHOENIX CONTACT group's customers to verify the authenticity of devices. Afterwards, the customer stores its own Local Device Identity certificate into the device. By this, the device is "taken over" and integrated into the customers PKI.

Code signing certificates are used to verify the authenticity of firmware during the update of software or of secure boot software during the boot process of the device. For this, the firmware and software is signed by a signing server during the final production process. The related certificates are separated, i.e. certificates for code signing can only be used for the verification of signatures on firmware or secure boot software and not for both uses. This is stored in the certificate attributes (e.g. naming) and must be evaluated by the Relying Party.

Certificates of Time Stamp Units may only be used for the verification of time stamps.

In addition, the rules of PHOENIX CONTACT's certificate policy apply.

Prohibited certificate uses

Other uses than those specified in the certificate are not permitted.

In addition, the rules of PHOENIX CONTACT's certificate policy apply.

1.5. Policy administration

Organization administering the document

This Certification Practice Statement is maintained and updated by PHOENIX CONTACT. The security officer, authorized by the management of PHOENIX CONTACT, is responsible for the acceptance of the document.

Contact person

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
D-32825 Blomberg

Corporate Product & Solution Security Officer
E-Mail: device-pki@phoenixcontact.com

Person determining CPS suitability for the policy

The security officer, authorized by the management of PHOENIX CONTACT, is responsible for determining whether the CPS is suitable for the Certificate Policy of PHOENIX CONTACT.

CPS approval procedures

This Certification Practice Statement is reviewed yearly by PHOENIX CONTACT and adjusted if necessary. A change is indicated by a new version number of the document.

1.6. Definitions and acronyms

Term / acronym	Description
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CS	Code signing

Term / acronym	Description
CSR	Certificate Signing Request
DN	Distinguished Name
DWH	Data Warehouse
FW	Firmware
HSM	Hardware Security Module
IDevID	Initial Device Identity
OCSP	Online Certificate Status Protocol
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for comments
SB	Secure Boot
Sub-CA	Subordinated Certification Authority
TSA	Time Stamp Authority
TSU	Time Stamp Unit
TSP	Trust Service Provider
USV	Uninterruptible Power Supply (in German unterbrechungsfreie Stromversorgung)
VA	Validation Authority

1.7. References

[CP] PHOENIX CONTACT, Certificate Policy of PHOENIX CONTACT, latest version.

[DIR IT-Oper] PHOENIX CONTACT, Directive on secure IT operation

[IEEE 802.1] IEEE Standard for Local and Metropolitan Area Networks, Secure Device Identity, IEEE Std 802.1 AR™ – 2018

[IEC 62443-4-1] Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements, 2018

[IEC 62443-4-2] Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components, 2019

[RFC 2986] PKCS #10: Certification Request Syntax Specification, Version 1.7, November 2000

[RFC 3161] Internet X.509 Public Key Infrastructure, Time-Stamp Protocol (TSP), August 2001
[RFC 3647] Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, November 2003.
[RFC 5272] Certificate Management over CMS (CMC), June 2008
[RFC 5280] Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile, May 2008.
[RFC 7030] Enrollment over Secure Transport, October 2013
[X.501] ITU-T Recommendation X.501, Information Technology – Open Systems Interconnection – The Directory: Models, Version October 2019.
[X.509] ITU-T Recommendation X.509 (1997 E), Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, October 2019.

2. Publication and Repository Responsibility

2.1. Repositories

Information related to the Public Key Infrastructure is published on PHOENIX CONTACT websites in an area under the domain “phoenixcontact.com”. A repository in a kind of a Directory Service is not offered by PHOENIX CONTACT.

2.2. Publication of certificate information

The following information are available on the above mentioned website:

- CA certificates
- Certificate Revocation Lists
- Certificate Policy of PHOENIX CONTACT
- Certification Practice Statement of PHOENIX CONTACT

2.3. Time or frequency of publication

CA certificates are published immediately after they are generated and retained for at least 10 years after the expiry of the validity of the CA.

CRLs are issued regularly and can be accessed at least until the end of the validity of the issuer certificate. Revocation lists are generated immediately after the revocation of certificates and published after 60 minutes at the latest. Even if no revocation of certificates takes place, it is warranted that a new revocation list is issued at least every 24 hours.

This CPS shall be published and shall remain available for at least as long as certificates issued on the basis of this CPS are valid. Invalid CPS versions are available under a dedicated website area.

PHOENIX CONTACT's websites can be accessed publicly and free of charge 24x7.

2.4. Access controls on repositories

PHOENIX CONTACT's websites can be accessed publicly and free of charge 24x7. There are no access restrictions for read access. Changes to the directory or web content can only be made by authorized persons. This is controlled by the appropriate assigned access rights.

3. Identification and Authentication

3.1. Naming

Type of Names

Certificates always contain information about the issuer and the subject. For initial device identity certificates, a unique ID is assigned in the subject. For firmware and secure boot certificates, a product specific name is used. These names are assigned as Distinguished Names. For Root-, Sub- and Timestamp CAs names are also assigned as Distinguished Name and contain a reference to the algorithm used and to the service they are assigned to.

For initial device identity certificates, alternative names can be registered and included in the `subjectAltName` extension of the certificate. The `serialNumber` attribute as part of the Distinguished Name is used according to the standard [RFC 5280] to include the serial number of the device.

Necessity for meaningful or unique names

The assigned Distinguished Name and `serialNumber` are unique within this PKI. Every IDevID (initial device ID) certificate is unique among certificates issued by this CA.

The names in the certificate are meaningful in the way that for firmware, secure boot and initial device identity certificate the name references the relevant product type. For Root and Sub CAs the names contain information regarding the algorithm used and the services they are assigned to.

Anonymity or pseudonyms for subscribers

Pseudonyms for subscribers are used only in Distinguished Names of Initial Device IDs to stipulate Hardware-ID (e.g. of the installed flash module).

Rules for the interpretation of various name forms

Root-CA / Sub-CA

DN component	Interpretation
`G (GivenName)`	Field is not used
`SN (Surname)`	Field is not used

DN component	Interpretation
CN (commonName)	Depending on the algorithm and the corresponding service: RSA / ECDSA-NIST / ECDSA-brainpool Phoenix Contact Root-CA RSA / ECDSA-NIST / ECDSA-brainpool Phoenix Contact Initial DeviceID Sub-CA<Nr.> RSA / ECDSA-NIST / ECDSA-brainpool Phoenix Contact Firmwaresigning Sub-CA<Nr.> RSA / ECDSA-NIST / ECDSA-brainpool Phoenix Contact Secure Boot Sub-CA<Nr.> RSA / ECDSA-NIST / ECDSA-brainpool Phoenix Contact Timestamping Sub-CA<Nr.>
PN (Pseudonym)	Field is not used
Serial Number (serialNumber)	Field is not used
O (organizationName)	Phoenix Contact GmbH & Co. KG
OU (organizationalUnit)	Type of CA (e.g. code signing)
OrgID (organizationIdentifier)	Field is not used
C (countryName)	DE
Street (streetAddress)	Field is not used
L (localityName)	Blomberg
S (stateOrProvinceName)	Nordrhein-Westfalen
PostalCode (postalCode)	Field is not used

Device Certificate

DN component	Interpretation
G (GivenName)	Field is not used
SN (Surname)	Field is not used
CN (commonName)	Device Type

DN component	Interpretation
PN (Pseudonym)	Hardware-ID, e.g. of the installed flash module
Serial Number (serialNumber)	Serial number of device
O (organizationName)	Phoenix Contact GmbH & Co. KG
OU (organizationalUnit)	Field is not used
OrgID (organizationIdentifier)	Field is not used
C (countryName)	DE
Street (streetAddress)	Field is not used
L (localityName)	Blomberg
S (stateOrProvinceName)	Nordrhein-Westfalen
PostalCode (postalCode)	Field is not used

SAN component	Interpretation
ProductInstanceUri	Device specific URL address

Firmware Certificate

DN component	Interpretation
G (GivenName)	Field is not used
SN (Surname)	Field is not used
CN (commonName)	Product group specific Firmware Signing Certificate
PN (Pseudonym)	Field is not used
Serial Number (serialNumber)	Field is not used
O (organizationName)	Phoenix Contact GmbH & Co. KG
OU (organizationalUnit)	Firmware Signing
OrgID (organizationIdentifier)	Field is not used

DN component	Interpretation
C (countryName)	DE
Street (streetAddress)	Field is not used
L (localityName)	Blomberg
S (stateOrProvinceName)	Nordrhein-Westfalen
PostalCode (postalCode)	Field is not used

Secure Boot Certificate

DN component	Interpretation
G (GivenName)	Field is not used
SN (Surname)	Field is not used
CN (commonName)	Product specific Secure Boot Certificate
PN (Pseudonym)	Field is not used
Serial Number (serialNumber)	Field is not used
O (organizationName)	Phoenix Contact GmbH & Co. KG
OU (organizationalUnit)	Secure Boot
OrgID (organizationIdentifier)	Field is not used
C (countryName)	DE
Street (streetAddress)	Field is not used
L (localityName)	Blomberg
S (stateOrProvinceName)	Nordrhein-Westfalen
PostalCode (postalCode)	Field is not used

Timestamp Certificate

DN component	Interpretation
G (GivenName)	Field is not used
SN (Surname)	Field is not used
CN (commonName)	Phoenix Contact GmbH & Co. KG TSA {Nummer}
PN (Pseudonym)	Field is not used
Serial Number (serialNumber)	Field is not used
O (organizationName)	Phoenix Contact GmbH & Co. KG
OU (organizationalUnit)	Field is not used
OrgID (organizationIdentifier)	Field is not used
C (countryName)	DE
Street (streetAddress)	Field is not used
L (localityName)	Blomberg
S (stateOrProvinceName)	Nordrhein-Westfalen
PostalCode (postalCode)	Field is not used

Recognition, authentication, and the role of trademarks

With regard to the corresponding regulations, reference is made to chapter 9 in the CP [CP] as well as the General Terms and Conditions of the respective PHOENIX CONTACT group member.

3.2. Initial identity validation

For device certificates, the key pair is generated and stored inside the device's secure element (e.g. TPM). The CSR is generated in the production environment and is signed by the device's private key (proof of possession). The CSR is transmitted via a designated interface (Local Registration Authority) to the CA.

For firmware certificates, a responsible administrator generates the key pair and an appropriate CSR and transmits it via a designated interface for certificate issuing purpose to the CA.

The interfaces to the CA are TLS encrypted. TLS certificates are issued through an internal PKI.

3.3. Identification and authentication for re-key requests

No specifications are made as re-key requests are not provided.

3.4. Identification and authentication for revocation requests

A process for externally triggered revocation requests is not provided. Revocation requests are only issued and processed in a manual, internal process in which the relevant personnel has to identify and authenticate themselves at the CA appliance.

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

The certification generation process for device certificates is automated.

The CA expects a valid certificate signing request (CSR) on the basis of which the certificate generation process is started. The CSR from the device is forwarded through a Local Registration Authority and must be addressed to a defined interface of the Certification Authority. Only CSRs from authenticated systems are accepted for further processing which are signed by the devices private key.

For firmware certificates, the responsible administrators of build servers have to authenticate themselves at the appropriate build servers to manually issue a CSR. This applies also for signing servers, i.e. responsible administrators of signing servers initiate manually the generation of a CSR. The evaluation of these CSRs by the CA and the issuing of the related certificates must be invoked manually by responsible CA administrators. Unlike the issuance of certificates for IDevIDs, this process is not automated.

No provisions regarding the enrollment process used by subjects and responsibilities are made.

4.2. Certificate application processing

Certificates for IDevIDs are issued in an automated process and the issuance of certificates for code signing as well as for time stamp units must be invoked manually. The CA receives a CSR through designated interfaces, i.e. via a TSL protected network interface (IDevID) or functions of the CA’s administrator user interface (code signing, time stamp unit), and verifies the quality of the public key.

The CA checks the consistency between the CSR and the certificate profile. The CSR is declined in case of inconsistency, if the private key does not match the CSR or if the CSR is not received from an authorized interface.

No provisions for a time line for the certificate application process are made.

4.3. Certificate issuance

Certificates are generated inside the CA application and signed with CA's private key stored in the CA's HSM and distributed via the designated interfaces.

No provisions are made to notify the subscriber of the issuance of the certificates as processes are automated or manual.

4.4. Certificate acceptance

Certificates are created and distributed via the designated interfaces. No provisions are made for the conduct of an applicant regarding the acceptance of the certificate as processes are automated for IDevID certificates. For code signing certificates as well as certificates for time stamp units a manual process takes place.

No provisions are made regarding the publication of the certificate by the CA as the certificates are not published. The CA certificates are published on PHOENIX CONTACT's website.

No provisions are made regarding the notification of certificate issuance by the CA to other entities as other entities are not informed of the certificate issuance.

4.5. Key pair and certificate usage

The private keys are to be used exclusively for the intended applications in accordance with the types of use specified in the certificate.

The certificates can be used by all certificate users. However, they can only be trusted if

- the certificates are used in accordance with the types of use noted therein (key usage, extended key usage, possibly restrictive extents),
- the verification of the certificate chain up to a trusted root certificate can be carried out successfully, and
- all further precautions specified in agreements or elsewhere and any restrictions in the certificate and any application-specific precautions on the part of the certificate user have been taken into account and recognized as compatible.

4.6. Certificate renewal

No provisions are made as certificate renewals are not provided.

4.7. Certificate re-key

No provisions are made as re-key requests are not provided.

4.8. Certificate modification

No provisions are made as certificate modifications are not provided.

4.9. Certificate revocation and suspension

A process for externally triggered revocation requests is not provided. Revocation requests are only issued and processed in a manual, internal process.

No provisions are made for the suspension of certificates as this process is not provided.

Key pairs used for code signing and time stamp units will be deactivated by authorized personnel of PHOENIX CONTACT.

4.10. Certificate status service

Certificate revocation lists are published in order to verify whether a certificate has been revoked. OSCP services are not provided.

4.11. End of subscription

The validity of a certificate ends with the date noted in the certificate. Device certificates are issued with a long life time. After a certificate is expired, a new certificate has to be requested.

4.12. Key escrow and recovery

Key escrow and recovery for the private keys of devices and firmware are not offered.
For the Root CA and the HSM a back-up of the keys exists which is secured with master back up keys, so that recovery of the root CA is possible in the event of a disaster.

5. Facility, Management, and operational Controls

5.1. Physical controls

PHOENIX CONTACT operates two data warehouses (DWH) in hot-hot modus. The DWH with identical setups are located in Blomberg, Germany, structurally separated and in different fire zones of the site. Both DWH are equipped with fire detection systems, fire extinction systems, air conditioning and separate USV-systems. Electricity supply is continuously monitored. Proper function of fire detection, fire extinction and alarm system are regularly checked.

5.2. Procedural controls

Part of the documentation is a role concept in which employees are assigned to one or more roles by the management of PHOENIX CONTACT and receive corresponding authorizations through a controlled process. The authorizations of the individual roles are limited to those who need them to fulfill their tasks.

Roles with security responsibility for the operation PHOENIX CONTACT, called "Trusted Roles", are defined in the authorization concepts of PHOENIX CONTACT. These are Security Officer, System Administrator, System Operator and Auditor. In addition, the role concept includes a data protection officer.

Employees who work in the field of certification act independently and free from commercial and financial constraints that could influence their decisions and actions.

The role concept provides for various role exclusions in order to prevent conflicts of interest. It is implemented through technical and organizational measures, such as access authorizations and querying knowledge. Before gaining access to security-critical applications, the person carrying it out must successfully authenticate. The person performing the action can subsequently be assigned to an action via event logs.

Security-critical systems for issuing certificates are additionally protected by multi-factor authentication.

5.3. Personnel controls

Qualifications, experience, and clearance requirements

PHOENIX CONTACT warrants, that personnel working in the certificate service have the knowledge, experience and skills necessary for this activity.

The identity, reliability and specialist knowledge of the staff is checked before the start of the work. Initial and event-related training warrants competence in the areas of activity as well as general information security. Training courses and proof of performance are documented.

Training requirements

PHOENIX CONTACT trains personnel working in the certificate service. This covers information security awareness trainings as well as PKI specific aspects.

Retraining frequency and requirements

PHOENIX CONTACT trains personnel working in the certification service at the beginning of their assignment and when necessary.

Sanctions for unauthorized actions

PHOENIX CONTACT excludes unreliable employees from the activities in the certification service.

Violations by employees against the processes of PHOENIX CONTACT’s operation are analyzed and evaluated. If the relationship of trust cannot be warranted, these employees are excluded from security-related activities.

Documentation supplied to personnel

Comprehensive procedural instructions define the responsible employee roles and rights as well as corresponding manual and machine tests for all production steps. All required documents (such as procedural instructions, training materials) are made available to employees.

5.4. Audit logging procedures

Only personnel authorized in accordance with the role concept are allowed to administer computers, networks and other components. Both, the HSM and PrimeKey appliance, have an internal event logging. There is a regular evaluation of log files for rule transfers, attack attempts and other incidents. Monitoring measures begin with the commissioning of a device and end with its disposal.

5.5. Records archival

Types of records archived

A distinction is made between records in electronic form and paper-based records.

Documents on procedural guidelines (certificate policy, certification practice statement), certificates (e.g. Root-CA, Sub-CAs), revocation documentation, electronic files and logs or log data on the certificate life cycle are archived. If applicable, this also includes the corresponding system protocols that arise within the framework of the aforementioned results. This also includes the recording of security-related events.

Records in Logfiles contain a time stamp of the local system time that is synchronized with a central time source.

Retention period for archive

Archived data is kept for at least 30 years.

Protection of archive

Archiving takes place exclusively internally at PHOENIX CONTACT and in secured premises. PHOENIX CONTACT warrants that only trusted individuals have access to the archives. All data is secured against unauthorized read, change and delete access.

Archive backup procedures

The archive is located in secure premises. These are subject to the role concept and access regulations of PHOENIX CONTACT.

Requirements of time-stamping of records

Records in Logfiles contain a time stamp of the local system time that is synchronized with a central time source.

Archive collection system

Data from the backup is transferred to the archive through internal IT measures.

Procedure to obtain and verify archive information

The collection and verification of archived data is carried out by PHOENIX CONTACT's IT operations.

5.6. Key changeover

A reasonable time before a CA expires, new CA keys are generated, and new CA instances are set up and published on the PHOENIX CONTACT's website. Reasons for changeover can result from key compromise, expiration of the certificate, change of algorithm, key length or certificate contents. Key ceremonies for a key changeover will be documented according to the stipulations given in section 6.1. For the root CA PHOENIX CONTACT uses a cross certification period while the renewal of sub CAs are only time-shifted.

Cross certificates for Root-CAs are issued in both directions, i.e. the old key is used to issue a certificate for the new key and the new key is used to issue a certificate for the old key.

The envisaged time frame for the validity period of certificates for Root-CAs, Sub-CAs, signing servers and TSU's is stipulated in section 6.3. For the IDevID certificates the value `notAfter` is set to the `GeneralizedTime` value "99991231235959Z" (cf. [IEEE 802.1], section 8.5) to indicate that devices are expected to operate indefinitely. The following values are used by PHOENIX CONTACT as validity periods.

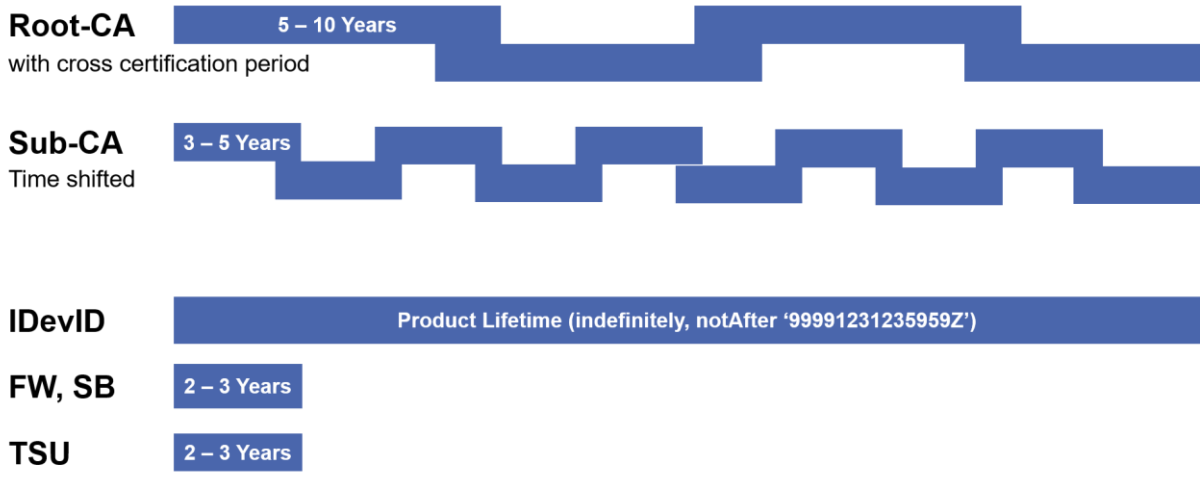

Figure 4: Key Changeover

5.7. Compromise and disaster recovery

PHOENIX CONTACT has a disaster recovery plan that is known to the roles involved and that is implemented by them if necessary. The personnel responsible and the corresponding "trusted roles" are declared in the authorization concept and known to the respective employees, should a system recovery be necessary. See also 5.2.

The disaster recovery plan describes the implementation of recovery procedures to restore the operability of PHOENIX CONTACT. There is a daily backup and a backup after changes. Backups are kept in a different fire compartment. The restoration of critical CA systems are tested regularly.
In addition, PHOENIX CONTACT has different algorithms in use and in the event of a key compromise the algorithm can be switched.

This disaster recovery plan is reviewed annually by PHOENIX CONTACT and adjusted if necessary. A change is indicated by a new version number of the document.

5.8. CA or RA termination

No stipulations.

6. Technical Security Controls

6.1. Key pair generation and installation

Key pair generation

CA keys are generated in a Hardware Security Module (HSM) which has a “FIPS 140-2 Level 3” certification. The CAs and its HSMs are operated in secure data centers. The key ceremony is carried out according to established procedures. The key ceremony is performed by designated Trusted Roles (System Operator) in the presence of the Security Officer. If necessary, the key ceremony can take place under the supervision of an independent third party. The application of a dual control principle is enforced during key generation.

The key ceremony is documented.

Optionally, an independent auditor can be present during the generation of CA keys or the auditor can convince himself of the proper procedure of the key generation after the key generation by means of records and documentation.

Keys of end-entities are not generated by CAs.

Private key delivery to subscriber

No stipulations because keys of end-entities are not generated by CAs.

Public key delivery to certificate issuer

End-entities' public keys are transmitted to the CA by means of certificate signing requests (e.g., PKCS #10, cf. [RFC 2986]). For this, appropriate enrolment processes are used, for example Certificate Management over CMS (CMC) defined in [RFC 5272], enrolment over Secure Transport (EST) protocol, in [RFC 7030] or manual enrolment realized by trained personal.

CA public key delivery to relying parties

A dedicated delivery process of CA public keys to relying parties is not offered by PHOENIX CONTACT. Initial device identities are stored in the device and contain all certificates needed to verify the IDevID certificate and its related certificate chain. In code signing signatures the signature format contains also all necessary CA certificate for the verification of the signature and related information.

In addition CA certificates are available via website repository.

Key sizes

Root-CA certificates and CA-certificates, that are used for verification of end-entity certificates issued under this CPS, use RSA keys with a key length of 4096 Bit or ECDSA keys with a key length of at least 256 bits with domain parameters of NIST or brainpool curves.

CA	Subject Key	Min. Key Length in Bit	Certificate Signature	Min. Key Length in Bit
Root-CA	RSA	4096	RSA	4096
Root-CA	ECDSA, NIST	256	ECDSA, NIST	256
Root-CA	ECDSA, brainpool	256	ECDSA, brainpool	256
Sub-CA	RSA	4096	RSA	4096
Sub-CA	ECDSA, NIST	256	ECDSA, NIST	256
Sub-CA	ECDSA, brainpool	256	ECDSA, brainpool	256

Certificates for end-entities use RSA keys with a key length of at least 2048 Bit or ECDSA keys with a key length of at least 256 bits with domain parameters of NIST or brainpool curves. In case of RSA keys a key length of 2048 Bit is used only in devices with secure elements (e.g. TPMs) that support a key generation up to 2048 Bit. In all other cases end-entities use RSA keys with key length of 4096 Bit.

CA	Subject Key	Min. Key Length in Bit	Certificate Signature	Min. Key Length in Bit
IDevID	RSA	2048	RSA	4096
IDevID	ECDSA, NIST	256	ECDSA, NIST	256
IDevID	ECDSA, brainpool	256	ECDSA, brainpool	256
Codesigning	RSA	4096	RSA	4096
Codesigning	ECDSA, NIST	256	ECDSA, NIST	256
Codesigning	ECDSA, brainpool	256	ECDSA, brainpool	256
TSU	RSA	4096	RSA	4096
TSU	ECDSA, NIST	256	ECDSA, NIST	256
TSU	ECDSA, brainpool	256	ECDSA, brainpool	256

Public key parameters and quality checking

CA keys are generated in a Hardware Security Module (HSM) which has a “FIPS 140-2 Level 3” certification. This also applies for code signing keys as well as for keys for the generation of time stamps. IDevID keys are generated in the device’s secure element (e.g. TPM).

Key usage purposes

Private Root-CA keys are used only for the signing of Sub-CA certificates. All other private CA keys are used for the signing of Sub-CA certificates, end-entity certificates and CRLs. The CRL of the Root-CA is signed by a dedicated CRL signer that is derived from a specific Sub-CA for the issuing of CRL signer certificates.

End-entity certificates may be used only for use cases defined in the certificate. Key usage types are defined in the extensions `keyUsage` and `extKeyUsage`.

6.2. Private key protection and Cryptographic Module Engineering Controls

Cryptographic module standards and controls

The cryptographic modules, hardware security modules, used by PHOENIX CONTACT for certification authorities are “FIPS 140-2 Level 3” certified. This applies also to the cryptographic modules used for the code signing (signing server) and the time stamp units.

The cryptographic modules used for initial device identities are the device’s secure element (e.g. TPM).

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

The hardware security module used by PHOENIX CONTACT for the generation and usage of CA keys have a master key for secure key storage and reloading of keys. For this, the keys are encrypted and integrity protected. The master key is generated at initialization of the hardware security module and securely stored on smart cards with a 2 out of 3 or 3 out of 5 multi-person control.

Private key escrow

All private keys generated and used in the hardware security modules of CAs, signing servers and TSUs are stored in a protected manner under the module's master key. This enables the secure reload of private keys in the event of a disaster. For this, at first the master key of the hardware security module must be reloaded under the established multi-person control. Afterwards the private keys protected with this master key can be loaded into the module.

For private keys of initial device identities key escrow is not established.

Private key backup

All private keys generated and used in the hardware security modules of CAs, signing servers and TSUs are stored in a protected manner under the module's master key. This allows these keys to be backed up and restored if necessary.

Private keys of initial device identities are not subject to any backup.

Private key archival

All private keys generated and used in HSMs are part of the HSM backup that is part of the appliance backup. These backup data are transferred to the archive.

Private key transfer into or from a cryptographic module

Private keys of CAs, signing servers and TSUs are only transferred for backup and recovery purposes. For the export and import of private keys between two hardware security modules the keys are protected by encryption and integrity check values. For this, the module's master key is used. A key transfer between two modules is only possible if the modules have the same master key.

Private key storage on cryptographic module

Private keys of CAs, signing servers and TSUs are generated and used in hardware security modules that are "FIPS 140-2 Level 3" certified.

The private keys of initial device identities are generated and used in the device's secure element (e.g. TPM).

Method of activating private key

Private keys of the Root-CA may only be used under dual control. Private keys of Sub-CAs have to be activated once after their generation. Afterwards, Sub-CAs for the issuing of IDevID certificates running in an automatic mode and certificate signing requests must be submitted via a TLS protected interface assigned to this Sub-CA. The issuance of certificates by Sub-CAs for code signing and time stamp units are manual processes.

For private keys of initial device identities an activation is not necessary.

Method of deactivating private key

The private keys of CAs, signing servers and TSU's are deactivated by termination of the connection between HSM and application or by the end of validity of the associated certificate.

For private keys of initial device identities there is no deactivation process. The private key and its certificate lose their validity when the device is finally taken out of service and disposed of in accordance with the product-specific specifications.

Method of destroying private key

The private keys of CAs, signing servers and TSU's are destroyed at the end of their life cycle. This is done by deleting these keys in the hardware security module.

Cryptographic Module Rating

Private keys of CAs, signing servers and TSUs are generated and used in hardware security modules that are "FIPS 140-2 Level 3" certified.

The private keys of initial device identities are generated and used in the device's secure element (e.g. TPM).

6.3. Other aspects of key pair management

Public key archival

Public keys of certification authorities, signing servers and TSU's are logged with their certificates during certificate generation. These log files are part of backup files that are taken over into the archival records.

Certificate operational periods and key pair usage periods

The validity period of certificates for CAs, signing servers and TSU's is variable and can be taken from the certificate. The following values are used by PHOENIX CONTACT as validity periods.

Component	Validity period
Root-CA	5 – 10 Years
Sub-CA	3 – 5 Years
Code signing (Firmware, Secure Boot)	2 – 3 Years
TSU	2 – 3 Years
IDevID	Product's lifetime, indefinitely (notAfter "99991231235959Z")

6.4. Activation data

Activation data generation and installation

See section 6.2, Method of activating private key.

Activation data protection

Private keys of the Root-CA may only be used under dual control. The activation data must be kept securely by authorized persons or protected by physical measures (e.g. smart cards, hardware security modules or similar).

Other aspects of activation data

No stipulations.

6.5. Computer security controls

PHOENIX CONTACT and PHOENIX CONTACT group members operate an information security management system (ISMS). Part of the ISMS is a secure IT operation policy [DIR IT-Oper].

The computers, networks and other components used by PHOENIX CONTACT and PHOENIX CONTACT group members warrant in the configuration used that only actions can be carried out which do not contradict the CPS. It is warranted that security-relevant software updates are installed on the relevant systems in a reasonable time.

Certificate holders and certificate users must use trustworthy computers and software.

The relevant systems are continuously monitored to warrant availability. Critical reports are handled as part of the incident management process.

The Root-CA is entirely offline without a network connection, i.e. the Root-CA does not have interfaces for communication with other technical components of the PKI. The Root-CA only has a web user interface for its operation.

6.6. Life cycle technical controls

System development controls

During the development of all system development projects carried out by PHOENIX CONTACT or on behalf PHOENIX CONTACT, security requirements are analyzed in the design stage. The results obtained are defined as requirements during the development and security measures are implemented accordingly.

Security management controls

Only personnel authorized in accordance with the role concept are allowed to administer computers, networks and other components. There is a regular evaluation of log files for rule violations, attack attempts and other incidents. Monitoring measures begin with the commissioning of a device and end with its disposal.

Life cycle security controls

The devices used are operated in accordance with the manufacturer's instructions. Before devices are put into operation, they are thoroughly checked and are only used if there is no doubt that they have not been tampered with. Replaced devices or obsolete data carriers are decommissioned and disposed of in such a way that functionality or data misuse is excluded.

Electronic data or paper-based logs document all relevant events that influence the life cycle of the CA as well as the issued certificates and generated keys. These are saved in an audit-proof manner on durable media. The company's media are reliably protected against damage, theft, loss or compromise according to their classification within the framework of the PHOENIX CONTACT's documentation guideline.

6.7. Network security controls

A network concept is implemented in the operation of the CAs, which warrants that the relevant CA systems are operated in specially secured network zones.

To protect the processes of PHOENIX CONTACT, for example firewall and intrusion detection / prevention mechanisms are used which only allow connections that are explicitly permitted. PHOENIX CONTACT operates network segments with different protection requirements and carefully separates employee and Internet-related networks from server networks.

The availability of the internet connection is warranted by redundancy. There are two permanent connections to the provider on two different routes. If the provider's access point fails, the system automatically switches to the second connection.

The physical security of the networks operated and used by PHOENIX CONTACT is warranted and is adapted to the structural conditions and their changes.

6.8. Time-stamping

PHOENIX CONTACT offers for its public key infrastructure and especially for code signing service a time stamp service. The time stamp service has its own subordinated certification authority and time stamp units that are certified by it. The certification authority as well as the time stamp units generate and use their private keys in hardware security modules that are “FIPS 140-2 Level 3” certified. The time stamp units are processed on a signing server.

The clock of the time stamp units is synchronized with UTC with an accuracy of +/- 500 ms or better. In the case the clock drifts out of accuracy, no time stamp will be issued until synchronization of the clock.

The time stamp service includes standard compliant RFC 3161, Internet Public Key Infrastructure – Time-Stamp protocol, time stamps (cf. [RFC 3161]).

7. Certificate, CRL and OCSP Profiles

7.1. Certificate profile

Version numbers

All certificates issued in the public key infrastructure conformant to the CPS at hand are X.509 public key certificates, version 3 (cf. [X.509]). The recommendation of RFC 5280 (cf. [RFC 5280]) as well as IEEE Std. 802.1 AR™-2018 (cf. [IEEE 802.1]) are taken into consideration for the definition of the certificate profiles. In all certificates only standard extensions or private internet extensions defined in RFC 5280 are used. Private extensions are not defined by PHOENIX CONTACT.

Certificate Extensions

The following types of certificate profiles for certificates are defined:

- Root Certification Authority (Root-CA)
- Subordinate Certification Authority for Initial Device Identities (CA-IDevID)
- Subordinate Certification Authority for Code Signing (CA-CS)
- Subordinate Certification Authority for Time Stamping (CA-TSA)
- Initial Device Identity Certificate (IDevID)
- Code Signing Firmware (CS-FW)
- Code Signing Secure Boot (CS-SB)
- Time Stamp Units (TSU)

The certificate profiles for Subordinate Certification Authorities (CA-IDevID, CA-CS, CA-TSA) are described in the same tables. This holds also for the certificate profiles used for code signing (CS-FW, CS-SB). Where specific differentiations are required, reference is made to them in the appropriate fields.

It is intended to support different cryptographic algorithms in the public key infrastructure. For this purpose, the three “cipher suites” RSA, ECDSA based on NIST curves and ECDSA based

on brainpool curves for the signing of certificates and CRLs as well as for signing of application data will be used. However, a mixture of different algorithms is not intended.

For the issuing of CRLs by the Root-CA a dedicated subordinated certification authority (CA-RCACRL) is established that certifies public keys of end entities authorized for the signing of Root-CA CRLs (RCACRL).

Root Certification Authority (Root-CA)

Field Name	Description	Value
`version`	X.509 Version of the certificate	3
`serialNumber`	Serial number	Positive Integer, minimum 16 Octects, up to 20 Octects
`signature`	`AlgorithmIdentifier` of the signature algorithm used by the Root-CA to sign the certificate	Object Identifier (OID) of the signature algorithm
`issuer`	Name of Root-CA	Distinguished Name of Root-CA

`validity`	Validity period	`notBefore`
		`notAfter`
		
		UTCTime or Generalized Time according to RFC 5280

`subject`	Name of Root-CA	Distinguished Name of Root-CA
`subjectPublic-KeyInfo`	Public key of Root-CA	Subject Public Key: RSA ECDSA NIST curve ECDSA Brainpool curve
`extensions`	Certificate extensions	See table “Root Certification Authority (Root-CA) - extensions”
`Signature-Algorithm`	`AlgorithmIdentifier` of the signature algorithm used by the Root-CA to sign the certificate	Object Identifier (OID) of the signature algorithm
`signatureValue`	Signature of the certificate generated by the issuing Root-CA	Value of the signature

Root Certification Authority (Root-CA) - extensions

Field Name	OID	Critical	Description	Value
`Basic-Constraints`	2.5.29.19	Yes	Statement whether the subject of the certificate is a CA or not.	`cA` = True
`keyUsage`	2.5.29.15	Yes	Restriction of key usage	`keyCertSign`
`CRLDistributionPoints`	2.5.29.31	No	Distribution Point(s) of CRLs	`CRLDistributionPoints`
`subjectKeyIdentifier`	2.5.29.14	No	Key Identifier of the certified key. This identifier matches the `authorityKey-Identifier` of the certificates issued by the Root-CA identified in subject.	`keyIdentifier` of the Root-CA key 160-bit SHA-1 hash of subjectPublicKey

Subordinate Certification Authority (CA-RCACRL)

Field Name	Description	Value
`version`	X.509 Version of the certificate	3
`serialNumber`	Serial number	Positive Integer, minimum 16 Octects, up to 20 Octects
`signature`	`AlgorithmIdentifier` of the signature algorithm used by the CA to sign the certificate	Object Identifier (OID) of the signature algorithm
`issuer`	Name of issuing CA	Distinguished Name of Root-CA

`validity`	Validity period	`notBefore`
		`notAfter`
		
		UTCTime or Generalized Time according to RFC 5280

`subject`	Name of CA	Distinguished Name of subordinate CA-RCACRL
`subjectPublic-KeyInfo`	Public key of the subordinate CA	Subject Public Key: RSA ECDSA NIST curve ECDSA Brainpool curve

Field Name	Description	Value
extensions	Certificate extensions	See table “Subordinate Certification Authority (CA-RCACRL) - extensions”
Signature-Algorithm	AlgorithmIdentifier of the signature algorithm used by the CA to sign the certificate	Object Identifier (OID) of the signature algorithm
signatureValue	Signature of the certificate generated by the issuing CA	Value of the signature

Subordinate Certification Authority (CA-RCACRL) - extensions

Field Name	OID	Critical	Description	Value
basicConstraints	2.5.29.19	Yes	Statement whether the subject of the certificate is a CA or not.	cA = True pathLenContraint = 0
keyUsage	2.5.29.15	Yes	Restriction of key usage	keyCertSign
authorityKey-Identifier	2.5.29.35	No	Key Identifier of the CA key used to sign the certificate. This identifier matches the subjectKeyIdentifier of the issuer’s certificate.	keyIdentifier of Root-CA key 160-bit SHA-1 hash of subjectPublicKey of the issuer’s certificate
certifcatePolicies	2.5.29.32	No	Identification of the certificate policy valid for the issued certificate	OID of the certificate policy and Link to the related CPS (CPSUri)
subjectKeyIdentifier	2.5.29.14	No	Key Identifier of the certified key. This identifier matches the authorityKey-Identifier of the certificates issued by the CA identified in subject.	keyIdentifier of the CA key 160-bit SHA-1 hash of subjectPublicKey

Root-CA CRL signer (RCACRL)

Field Name	Description	Value
version	X.509 Version of the certificate	3

Field Name	Description	Value
serialNumber	Serial number	Positive Integer, minimum 16 Octects, up to 20 Octects
signature	AlgorithmIdentifier of the signature algorithm used by the CA to sign the certificate	Object Identifier (OID) of the signature algorithm
issuer	Name of issuing CA	Distinguished Name of Sub-CA (CA-RCACRL)
validity	Validity period	notBefore notAfter UTCTime or Generalized Time according to RFC 5280
subject	Name of Production System	Distinguished Name of CRL signer
subjectPublic-KeyInfo	Public key of Production System	Subject Public Key: RSA ECDSA NIST curve ECDSA Brainpool curve
extensions	Certificate extensions	See table “Root-CA CRL signer (RCACRL) - extensions”
Signature-Algorithm	AlgorithmIdentifier of the signature algorithm used by the CA to sign the certificate	Object Identifier (OID) of the signature algorithm
signatureValue	Signature of the certificate generated by the issuing CA	Value of the signature

Root-CA CRL signer (RCACRL) - extensions

Field Name	OID	Critical	Description	Value
basicConstraints	2.5.29.19	Yes	Statement whether the subject of the certificate is a CA or not.	cA = False
keyUsage	2.5.29.15	Yes	Restriction of key usage	cRLSign

Field Name	OID	Critical	Description	Value
authorityKey-Identifier	2.5.29.35	No	Key Identifier of the CA key used to sign the certificate. This identifier matches the subjectKeyIdentifier of the issuer's certificate.	keyIdentifier
certifcatePolicies	2.5.29.32	No	Identification of the certificate policy valid for the issued certificate	OID of the certificate policy and Link to the related CPS (CPSUri)

Subordinate Certification Authorities (CA-IDevID, CA-CS, CA-TSA)

Field Name	Description	Value
version	X.509 Version of the certificate	3
serialNumber	Serial number	Positive Integer, minimum 16 Octects, up to 20 Octects
signature	AlgorithmIdentifier of the signature algorithm used by the CA to sign the certificate	Object Identifier (OID) of the signature algorithm
issuer	Name of issuing CA	Distinguished Name of Root-CA
validity	Validity period	notBefore notAfter UTCTime or Generalized Time according to RFC 5280
subject	Name of CA	Distinguished Name of subordinate CA; different DNs for CA-IDevID, CA-CS and CA-TSA
subjectPublic-KeyInfo	Public key of the subordinate CA	Subject Public Key: RSA ECDSA NIST curve ECDSA Brainpool curve
extensions	Certificate extensions	See table "Subordinate Certification Authorities (CA-IDevID, CA-CS, CA-TSA) - extensions"

Field Name	Description	Value
Signature-Algorithm	AlgorithmIdentifier of the signature algorithm used by the CA to sign the certificate	Object Identifier (OID) of the signature algorithm
signatureValue	Signature of the certificate generated by the issuing CA	Value of the signature

Subordinate Certification Authorities (CA-IDevID, CA-CS, CA-TSA) - extensions

Field Name	OID	Critical	Description	Value
basicConstraints	2.5.29.19	Yes	Statement whether the subject of the certificate is a CA or not.	cA = True pathLenContraint = 0
keyUsage	2.5.29.15	Yes	Restriction of key usage	keyCertSign cRLSign
authorityKey-Identifier	2.5.29.35	No	Key Identifier of the CA key used to sign the certificate. This identifier matches the subjectKeyIdentifier of the issuer's certificate.	keyIdentifier of Root-CA key 160-bit SHA-1 hash of subjectPublicKey of the issuer's certificate
certifcatePolicies	2.5.29.32	No	Identification of the certificate policy valid for the issued certificate	OID of the certificate policy and Link to the related CPS (CPSUri)
CRLDistributionPoints	2.5.29.31	No	Distribution Point(s) of CRLs	CRLDistributionPoints
subjectKeyIdentifier	2.5.29.14	No	Key Identifier of the certified key. This identifier matches the authorityKey-Identifier of the certificates issued by the CA identified in subject.	keyIdentifier of the CA key 160-bit SHA-1 hash of subjectPublicKey
AuthorityInfo-Access	1.3.6.1.5.5.7.1.1	No	The information lists certificates that were issued to the CA that issued the certificate containing this extension.	id-ad-caIssuers access Method = caIssuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}

Initial Device Identity Certificate (IDevID)

Field Name	Description	Value
`version`	X.509 Version of the certificate	3
`serialNumber`	Serial number	Positive Integer, minimum 16 Octects, up to 20 Octects
`signature`	`AlgorithmIdentifier` of the signature algorithm used by the CA to sign the certificate	Object Identifier (OID) of the signature algorithm
`issuer`	Name of issuing CA	Distinguished Name of Sub-CA (CA-IDevID)

`validity`	Validity period	`notBefore`
		`notAfter`
		
		notAfter = 99991231235959Z
		
		UTCTime or Generalized Time according IEEE Std. 802.1 AR™-2018

`subject`	Name of device	Distinguished Name of the device
`subjectPublic-KeyInfo`	IDevID's public key	Subject Public Key: RSA ECDSA NIST curve ECDSA Brainpool curve
`extensions`	Certificate extensions	See table "Device Identity Certificate (DevID) - extensions"
`Signature-Algorithm`	`AlgorithmIdentifier` of the signature algorithm used by the CA to sign the certificate	Object Identifier (OID) of the signature algorithm
`signatureValue`	Signature of the certificate generated by the issuing CA	Value of the signature

Initial Device Identity Certificate (IDevID) - extensions

Field Name	OID	Critical	Description	Value
basicConstraints	2.5.29.19	Yes	Statement whether the subject of the certificate is a CA or not.	cA = False
authorityKey-Identifier	2.5.29.35	No	Key Identifier of the CA key used to sign the certificate. This identifier matches the subjectKeyIdentifier of the issuer's certificate.	keyIdentifier 160-bit SHA-1 hash of subjectPublicKey of the issuer's certificate
certifcatePolicies	2.5.29.32	No	Identification of the certificate policy valid for the issued certificate	OID of the certificate policy and Link to the related CPS (CPSUri)
CRLDistributionPoints	2.5.29.31	No	Distribution Point(s) of CRLs	CRLDistributionPoints
subjectAltName	2.5.29.17	No	Alternative Name of the device.	ProductInstanceUri
AuthorityInfo-Access	1.3.6.1.5.5.7.1.1	No	The information lists certificates that were issued to the CA that issued the certificate containing this extension.	id-ad-caIssuers access Method = calssuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}

Code Signing Firmware (CS-FW, CS-SB)

Field Name	Description	Value
version	X.509 Version of the certificate	3
serialNumber	Serial number	Positive Integer, minimum 16 Octects, up to 20 Octects
signature	AlgorithmIdentifier of the signature algorithm used by the CA to sign the certificate	Object Identifier (OID) of the signature algorithm
issuer	Name of issuing CA	Distinguished Name of Sub-CA (CA-CS)

Field Name	Description	Value
validity	Validity period	notBefore notAfter UTCTime or Generalized Time according to RFC 5280
subject	Name of code signer	Distinguished Name of code signer; Identification of CS-FW or CS-SB in DN
subjectPublic-KeyInfo	Public key of Code Signer	Subject Public Key: RSA ECDSA NIST curve ECDSA Brainpool curve
extensions	Certificate extensions	See table “Code Signing Firmware (CS-FW, CS-SB) - extensions”
Signature-Algorithm	AlgorithmIdentifier of the signature algorithm used by the CA to sign the certificate	Object Identifier (OID) of the signature algorithm
signatureValue	Signature of the certificate generated by the issuing CA	Value of the signature

Code Signing Firmware (CS-FW, CS-SB) - extensions

Field Name	OID	Critical	Description	Value
basicConstraints	2.5.29.19	Yes	Statement whether the subject of the certificate is a CA or not.	cA = False
keyUsage	2.5.29.15	Yes	Restriction of key usage	digitalSignature
authorityKey-Identifier	2.5.29.35	No	Key Identifier of the CA key used to sign the certificate. This identifier matches the subjectKeyIdentifier of the issuer’s certificate.	keyIdentifier 160-bit SHA-1 hash of subjectPublicKey of the issuer’s certificate
certifcatePolicies	2.5.29.32	No	Identification of the certificate policy valid for the issued certificate	OID of the certificate policy and Link to the related CPS (CPSUri)

Field Name	OID	Critical	Description	Value
CRLDistribution-Points	2.5.29.31	No	Distribution Point(s) of CRLs	CRLDistributionPoints
extendedKeyUsage	2.5.29.37	No	This extension indicates one or more purposes for which the certified public key may be used. The indented key usage is code signing.	id-kp-codeSigning according to RFC 5280
AuthorityInfo-Access	1.3.6.1.5.5.7.1.1	No	The information lists certificates that were issued to the CA that issued the certificate containing this extension.	id-ad-caIssuers access Method = calssuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}

Time Stamp Unit (TSU)

Field Name	Description	Value
version	X.509 Version of the certificate	3
serialNumber	Serial number	Positive Integer, minimum 16 Octects, up to 20 Octects
signature	AlgorithmIdentifier of the signature algorithm used by the CA to sign the certificate	Object Identifier (OID) of the signature algorithm
issuer	Name of issuing CA	Distinguished Name of Sub-CA (CA-TSA)
validity	Validity period	notBefore notAfter UTCTime or Generalized Time according to RFC 5280
subject	Name of Production System	Distinguished Name of TSU
subjectPublic-KeyInfo	Public key of Production System	Subject Public Key: RSA ECDSA NIST curve ECDSA Brainpool curve

Field Name	Description	Value
extensions	Certificate extensions	See table “Time Stamp Unit (TSU) - extensions”
Signature-Algorithm	AlgorithmIdentifier of the signature algorithm used by the CA to sign the certificate	Object Identifier (OID) of the signature algorithm
signatureValue	Signature of the certificate generated by the issuing CA	Value of the signature

Time Stamp Unit (TSU) - extensions

Field Name	OID	Critical	Description	Value
basicConstraints	2.5.29.19	Yes	Statement whether the subject of the certificate is a CA or not.	cA = False
keyUsage	2.5.29.15	Yes	Restriction of key usage	digitalSignature
authorityKey-Identifier	2.5.29.35	No	Key Identifier of the CA key used to sign the certificate. This identifier matches the subjectKeyIdentifier of the issuer’s certificate.	keyIdentifier
certifcatePolicies	2.5.29.32	No	Identification of the certificate policy valid for the issued certificate	OID of the certificate policy and Link to the related CPS (CPSUri)
CRLDistribution-Points	2.5.29.31	No	Distribution Point(s) of CRLs	CRLDistributionPoints
extendedKeyUsage	2.5.29.37	No	This extension indicates one or more purposes for which the certified public key may be used. The indented key usage is TLS WWW server authentication and TLS WWW client authentication.	id-kp-timeStamping according to RFC 5280

Field Name	OID	Critical	Description	Value
AuthorityInfo-Access	1.3.6.1.5.5.7.1.1	No	The information lists certificates that were issued to the CA that issued the certificate containing this extension.	id-ad-caIssuers access Method = caIssuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}

Algorithm Object Identifiers

The following Object Identifiers (OID) are used for the identification of cryptographic algorithms in CA and end entity certificates.

Algorithm	Object Identifier
PKCS #1 RSASSA-PSS	1.2.840.113549.1.1.10
sha256WithRSAEncryption	1.2.840.113549.1.1.11
sha384WithRSAEncryption	1.2.840.113549.1.1.12
sha512WithRSAEncryption	1.2.840.113549.1.1.13
ANSI X9.62 ECDSA with SHA 256	1.2.840.10045.4.3.2
ANSI X9.62 ECDSA with SHA 384	1.2.840.10045.4.3.3
ANSI X9.62 ECDSA with SHA 512	1.2.840.10045.4.3.4

In the case of RSASSA-PSS, the following hash functions as well as the following mask generation function are used.

Algorithm	Object Identifier
SHA 256	2.16.840.1.101.3.4.2.1
SHA 384	2.16.840.1.101.3.4.2.2
SHA 512	2.16.840.1.101.3.4.2.3
SHA3 - 256	2.16.840.1.101.3.4.2.8
SHA3 – 384	2.16.840.1.101.3.4.2.9
SHA3 - 512	2.16.840.1.101.3.4.2.10
MGF 1	1.2.840.113549.1.1.8

For ECDSA signatures the following curves are used.

Algorithm	Object Identifier
NIST P-256	1.2.840.10045.3.1.7
Secp384r1 / NIST P-384	1.3.132.0.34
Secp521r1 / NIST P-521	1.3.132.0.35
brainpoolP256r1	1.3.36.3.3.2.8.1.1.7
brainpoolP256t1	1.3.36.3.3.2.8.1.1.8
brainpoolP384r1	1.3.36.3.3.2.8.1.1.11
brainpoolP384t1	1.3.36.3.3.2.8.1.1.12
brainpoolP512r1	1.3.36.3.3.2.8.1.1.13
brainpoolP512t1	1.3.36.3.3.2.8.1.1.14

Name forms

In the certificate fields *issuer* (name of the certificate issuer) and *subject* (name of the end entity), names are stated as Distinguished Names (cf. [X.501]). The encoding of the attributes is done as UTF-8 string or PrintableString for the attribute country (C).

The extension *SubjectAlternativeName* of IDevID certificates contains a *ProductInstanceUri*. The extension *IssuerAlternativeName* is not used in any certificate.

Name constraints

The extension *NameConstraints* is not used in any certificate.

Certificate Policy Object Identifier

The Certificate Policy Object Identifier contains the Object Identifier that identifies the related Certificate Policy of PHOENIX CONTACT.

Usage of Policy Constraints Extension

The extension *PolicyConstraints* is not used in any certificate.

Policy qualifiers syntax and semantics

The extension *CertificatePolicies* contains only the Policy Qualifier *cPSUri* (id-qt-cps) with Object Identifier 1.3.6.1.5.5.7.2.1 according to RFC 5280 (cf. [RFC 5280]), section 4.2.1.4.

Processing semantics for the critical Certificate Policies Extension

In all CA and end entity certificates the extension *CertificatePolicies* is not marked as critical. It is at the discretion of the certificate subjects, certificate subscribers and relying parties to evaluate this extension.

7.2. CRL profile

Version number(s)

All certificate revocation lists (CRL) issued in the public key infrastructure conformant to the CPS at hand are X.509 certificate revocation lists, version 2. The recommendation of RFC 5280 (cf. [RFC 5280]) as well as IEEE Std. 802.1 AR™-2018 (cf. [IEEE 802.1]) are taken into consideration for the definition of the certificate profiles. In all certificates, only standardized CRL extensions or CRL entry extensions are used. Private extensions are not defined by PHOENIX CONTACT.

CRL and CRL entry extensions

The following types of CRL profiles for certificate revocation lists are defined:

- CRLs issued by Root Certification Authority (CRL-RootCA)
- CRLs issued by Subordinate Certification Authorities (CRL-SubCA)

For the issuing of CRLs by the Root-CA a dedicated subordinated certification authority (CA-RCACRL) is established that certifies public keys of end entities authorized for the signing of Root-CA CRLs (RCACRL). Therefore, a distinction is made between two different profiles.

CRLs issued by Root Certification Authority (CRL-RootCA)

Field Name	Description	Value
`version`	X.509 Version of the certificate	2
`signature`	`AlgorithmIdentifier` of the signature algorithm used by the Root-CA to sign the certificate	Object Identifier (OID) of the signature algorithm
`issuer`	Name of CRL signer	Distinguished Name of CRL signer
`thisUpdate`	Ausgabedatum	UTCTime or Generalized Time according to RFC 5280

Field Name	Description	Value
nextUpdate	Zeitpunkt der nächsten Ausgabe	UTCTime or Generalized Time according to RFC 5280
Revoked-Certificates	List of revoked certificates; In case of an empty list this field is omitted; For each revoked certificate:	
	serialNumber of the revoked certificate	serialNumber
	Time of revocation	UTCTime or Generalized Time according to RFC 5280
	cRLEntryExtensions	See table “CRLs issued by Root Certification Authority (CRL-RootCA) – CRL Entry extensions”
cRLextensions	Certificate extensions	See table “CRLs issued by Root Certification Authority (CRL-RootCA) – CRL extensions”
Signature-Algorithm	AlgorithmIdentifier of the signature algorithm used to sign the certificate	Object Identifier (OID) of the signature algorithm
signatureValue	Signature of the CRL generated by the CRL signer	Value of the signature

CRLs issued by Root Certification Authority (CRL-RootCA) – CRL entry extensions

Field Name	OID	Critical	Description	Value
certificateIssuer	2.5.29.29	Yes	Certificate issuer identifies the certificate issuer associated with an entry in an indirect CRL.	Distinguished Name of Root-CA
reasonCode	2.5.29.21	No	The reason code identifies the reason for the certificate revocation.	reasonCode according to RFC 5280

CRLs issued by Root Certification Authority (CRL-RootCA) – CRL extensions

Field Name	OID	Critical	Description	Value
issuingDistributionPoint	2.5.29.28	Yes	The issuing distribution point identifies the CRL distribution point and scope for a particular CRL, and it indicates whether the CRL covers revocation for CA certificates only. The indirectCRL value is set to TRUE because the scope of the CRL includes certificates issued by the Root-CA that is not the CRL issuer or CRL signer.	distributionPoint of the CRL onlyContainsUserCerts = FALSE onlyContainsCACerts = TRUE indirectCRL = TRUE onlyContainsAttributeCerts = FALSE
authorityKeyIdentifier	2.5.29.35	No	Key Identifier of the CRL signer key. This identifier matches the subjectKey-Identifier of the certificate issued to the CRL signer.	keyIdentifier of the CRL signer key 160-bit SHA-1 hash of subjectPublicKey of CRL signer
cRLNumber	2.5.29.20	No	Conveys a monotonically increasing sequence number for the CRL issuer.	Positive Integer up to 20 Octects

CRLs issued by Subordinated Certification Authorities (CRL-SubCA)

Field Name	Description	Value
version	X.509 Version of the certificate	2
signature	AlgorithmIdentifier of the signature algorithm used by the Root-CA to sign the certificate	Object Identifier (OID) of the signature algorithm
issuer	Name of Sub-CA	Distinguished Name of Sub-CA (CA-IDevID, CA-CS, CA-TSA)
thisUpdate	Ausgabedatum	UTCTime or Generalized Time according to RFC 5280
nextUpdate	Zeitpunkt der nächsten Ausgabe	UTCTime or Generalized Time according to RFC 5280

Field Name	Description	Value
`Revoked-Certificates`	List of revoked certificates; In case of an empty list this field is omitted; For each revoked certificate:	
	serialNumber of the revoked certificate	serialNumber
	Time of revocation	UTCTime or Generalized Time according to RFC 5280
	cRLEntryExtensions	See table “CRLs issued by Subordinated Certification Authorities (CRL-SubCA) – CRL Entry extensions”
`cRLextensions`	Certificate extensions	See table “CRLs issued by Subordinated Certification Authorities (CRL-SubCA) – CRL extensions”
`Signature-Algorithm`	`AlgorithmIdentifier` of the signature algorithm used to sign the certificate	Object Identifier (OID) of the signature algorithm
`signatureValue`	Signature of the CRL generated by the CRL signer	Value of the signature

CRLs issued by Subordinated Certification Authorities (CRL-SubCA) – CRL entry extensions

Field Name	OID	Critical	Description	Value
`reasonCode`	2.5.29.21	No	The reason code identifies the reason for the certificate revocation.	`reasonCode` according to RFC 5280

CRLs issued by Subordinated Certification Authorities (CRL-SubCA) – CRL extensions

Field Name	OID	Critical	Description	Value
`authorityKeyIdentifier`	2.5.29.35	No	Key Identifier of the Sub-CA key. This identifier matches the `subjectKey-Identifier` of the certificate issued to the Sub-CA.	`keyIdentifier` of the Sub-CA's public key 160-bit SHA-1 hash of subjectPublicKey of Sub-CA's certificate
`cRLNumber`	2.5.29.20	No	Conveys a monotonically increasing sequence number for the CRL issuer.	Positive Integer up to 20 Octects

7.3. OCSP profile

A status information service based on an online certificate status protocol (OCSP) is not offered.

8. Compliance Audit and other Assessments

Internal audits, audit objects and processes are described in detail in the documentation of PHOENIX CONTACT. The role concept documents the qualification and the position of the auditor. Internal audits take place on a regular basis.

The conformity of PHOENIX CONTACT regarding IEC 62443 is regularly checked by an independent conformity assessment body. This includes a review of the documentation. If there is justified interest, the relevant parts of these documents can be inspected. A security level of SL-3 according to IEC 62443 is pursued. Fully comprehensive audits are carried out in the certified areas every three years. Additionally, interim audits are carried out annually. Internal Audits are also conducted every year.

9. Other Business and Legal Matters

With regard to the corresponding regulations, reference is made to chapter 9 in the CP [CP] as well as the General Terms and Conditions of the respective PHOENIX CONTACT group member.