Certificate Policy
Of
PHOENIX CONTACT
Device PKI

Document status: Valid

CS-IT-000001 -02- 2022-02

Last Modified: February 2022

Document History

Version	Date	Description
01	13.09.2021	Initial version
02	25.02.2022	Adjustment for the issuing of Root CA CRLs; Addition of a new Root CA (IDevID); Adjustments in sections 2.3, 6.5

Content

1. **Introduction** 5
   - 1.1. **Overview** 5
   - 1.2. **Document name and identification** 6
   - 1.3. **PKI participants** 6
   - 1.4. **Certificate usage** 6
   - 1.5. **Policy administration** 7
   - 1.6. **Definitions and acronyms** 7
   - 1.7. **References** 8
2. **Publication and Repository Responsibility** 9
   - 2.1. **Repositories** 9
   - 2.2. **Publication of certificate information** 9
   - 2.3. **Time or frequency of publication** 9
   - 2.4. **Access controls on repositories** 10
3. **Identification and Authentication** 10
   - 3.1. **Naming** 10
   - 3.2. **Initial identity validation** 11
   - 3.3. **Identification and authentication for re-key requests** 11
   - 3.4. **Identification and authentication for revocation requests** 11
4. **Certificate Life-Cycle Operational Requirements** 11
   - 4.1. **Certificate Application** 11
   - 4.2. **Certificate application processing** 11
   - 4.3. **Certificate issuance** 12
   - 4.4. **Certificate acceptance** 12
   - 4.5. **Key pair and certificate usage** 12
   - 4.6. **Certificate renewal** 12
   - 4.7. **Certificate re-key** 12
   - 4.8. **Certificate modification** 12
   - 4.9. **Certificate revocation and suspension** 13
   - 4.10. **Certificate status service** 13
   - 4.11. **End of subscription** 13
   - 4.12. **Key escrow and recovery** 13
5. **Facility, Management, and operational Controls** 13
   - 5.1. **Physical controls** 13
   - 5.2. **Procedural controls** 13
   - 5.3. **Personnel controls** 14
   - 5.4. **Audit logging procedures** 14
   - 5.5. **Records archival** 15

5.6. Key changeover 15
5.7. Compromise and disaster recovery 15
5.8. CA or RA termination 15
6. Technical Security Controls 16
6.1. Key pair generation and installation 16
6.2. Private key protection and cryptographic module engineering controls 17
6.3. Other aspects of key pair management 18
6.4. Activation data 18
6.5. Computer security controls 18
6.6. Life cycle technical controls 18
6.7. Network security controls 19
6.8. Time-stamping 19
7. Certificate, CRL and OCSP Profiles 19
7.1. Certificate profile 19
7.2. CRL profile 19
7.3. OCSP profile 20
8. Compliance Audit and other Assessments 20
9. Other Business and Legal Matters 20
9.1. Fees 20
9.2. Financial responsibility 20
9.3. Confidentiality of business information 21
9.4. Privacy and personal information 21
9.5. Intellectual property rights 22
9.6. Representation and warranties 22
9.7. Disclaimers of warranties 22
9.8. Limitations of liability 23
9.9. Indemnities 23
9.10. Term and termination 23
9.11. Individual notices and communications with participants 23
9.12. Amendments 23
9.13. Dispute resolution provisions 23
9.14. Governing law 24
9.15. Compliance with applicable law 24
9.16. Miscellaneous provisions 24
9.17. Other provisions 25

1. Introduction

1.1. Overview

This document describes the Certificate Policy (hereinafter referred to as CP) of the PKI operated by PHOENIX CONTACT GmbH & Co. KG. The policy is valid for the services provided by PHOENIX CONTACT GmbH & Co. KG to members of the PHOENIX CONTACT Group related to public key certificates for Initial Device Identification (IDevID) and code signing of firmware and secure boot software. In addition, a time stamp service is also offered by PHOENIX CONTACT GmbH & Co. KG for members of the PHOENIX CONTACT Group in code signing signatures and for future applications with IDevID.

It is intended to implement and operate the PKI in such a way that conformity with the PKI related requirements according to IEC 62443 (cf. [IEC 62443-4-1], [IEC 62443-4-2]) can be achieved or at least no contradictory specifications are made.

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 CP 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 CP.

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

Currently, there is no complex document hierarchy for the existing PKI. The requirements are described in this CP and the associated CPS [CPS] contains the details for implementing the policy.

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 rules are described in the certification practice statement that belongs to this policy. Under this policy PHOENIX CONTACT issues certificates for initial device identities, code signing certificates and certificates for time stamp units. In all these certificates the related CPS can be found in the “`cPSUri`” field of the extension `certificatePolicies`.

The specified OID in the certificate defines that the certificate belongs to this policy:

> The following OID is assigned for certificates issued under this policy:
> OID: 1.3.6.1.4.1.4346.2.2.1

1.2. Document name and identification

Document name:	Certificate Policy of PHOENIX CONTACT
Identifier (OID):	This document has the OID: 1.3.6.1.4.1.4346.2.2.1
Version:	02

1.3. PKI participants

The PKI participants and the CA hierarchy used in the PKI are described in the CPS [CPS] that belongs to this policy.

1.4. Certificate usage

The trust model used in the PKI based on this CP 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. The following types of end-entity certificates are issued under this policy by PHOENIX CONTACT.

- Initial Device Identity Certificate (IDevID)
- Code Signing Firmware (CS-FW)
- Code Signing Secure Boot (CS-SB)
- Time Stamp Units (TSU)

Prohibited certificate uses

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

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

1.5. Policy administration

Organization administering the document

This Certificate Policy 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

CP approval procedures

This Certificate Policy 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

Term / acronym	Description
CRL	Certificate Revocation List
CS	Code signing
CSR	Certificate Signing Request
DN	Distinguished Name
DWH	Data Warehouse
FW	Firmware
HSM	Hardware Security Module
IDevID	Initial Device Identification
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

[CPS] PHOENIX CONTACT, Certification Practice Statement 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.

Complete links to CA certificates and CRLs can be found in the certificates. For this, the extensions `cRLDistributionPoints` and `authorityInfoAccess` are used.

The repository also contains test certificates for all kind of certificates issued 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 PHOENIC CONTACT
- Certification Practice Statement of PHOENIC CONTACT

2.3. Time or frequency of publication

CA certificates are published immediately after they are generated and have to be retained for at least 10 years after the expiry of the validity of the CA. Certificates of Root-CAs are published immediately after they are generated and always available as long as the service is offered.

CRLs are issued regularly and have to be accessible 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 has to be warranted that a new revocation list of a Subordinated CA that issues certificates for end-entities is issued at least every 24 hours. The issuing of Root-CA CRLs is a manual procedure and conducted if an issued certificate has to be revoked or at the latest when their expiry date is reached.

This CP shall be published and shall remain available for at least as long as certificates issued on the basis of this CP are valid. Invalid CP 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

Identification and authentication of PHOENIX CONTACT certificates have to be carried out according to product specific requirements. So the identification and authentication depends on whether the certificate is issued for an initial device identity, a code signing system or a time stamp unit.

For initial device identity certificates identification and authentication is an automatic process. Related system components, e.g. production system and Local Registration Authority, are involved in this process. The CSR generated by the production site is transferred to the CA that verifies the CSR and issues the requested certificate. The communication between production system and Local Registration Authority must be protected by cryptographic means (e.g. TLS).

For firmware certificates, a responsible administrator generates the key pair and an appropriate CSR and transmits it via a designated interface to the CA. This applies also to certificates for time stamp units.

These rules are described in the respective CPS [CPS] that belongs to this policy.

3.1. Naming

All CA and end-entity certificates contain unique issuer and subject names as Distinguished Names.

CA names contain information related to PHOENIX CONTACT as a legal person. In addition, CA names include information about the intended kind of service and the used cryptographic algorithm.

Names for initial device identities contain information related to the manufacturer, the type of product, the serial number of the product and optionally the Hardware-ID, e.g. of the installed

flash module. In the extension `subjectAltName` a `ProductInstanceUri` must be included.

Names for code signing contain information related to the manufacturer and the type of code signing, i.e. firmware or secure boot. These certificates are not issued for natural persons but for code signing systems. For this, the subject may be anonymized (e.g. code signer 1, developer 2).

This applies also to certificates issued for time stamp units.

The specific naming rules are described in the CPS [CPS] that belongs to this policy.

3.2. Initial identity validation

The specific naming rules are described in the CPS [CPS] that belongs to this policy.

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.

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

4. Certificate Life-Cycle Operational Requirements

4.1. Certificate Application

PHOENIX CONTACT issues certificates for initial device identities, code signing and time stamp units. All subjects are PKI participants that are under control of PHOENIX CONTACT or the PHOENIX CONTACT group. Public keys of external subjects are not certified by PHOENIX CONTACT.

For certificate application a valid certificate signing request must be submitted to the responsible subordinated CA that issues these kind of certificates. For this, the CSR must be submitted via a dedicated interface of the related CA system. Name forms to be used are part of the CPS [CPS] belonging to this policy.

4.2. Certificate application processing

Certificates are issued by a subordinated CA in an automated process. The CA receives CSR through designated interfaces and has to verify the quality of the public key.

The CA must check the consistency between the CSR and the certificate profile. The CSR has to be 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.

4.3. Certificate issuance

Certificates are generated inside the CA application and signed with CA's private key. For the generation and usage of the CA's private key a HSM must be used. The generated certificate is distributed via the designated interfaces.

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.

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. Restrictions on key usages may be defined in the extensions `keyUsage` and `extendedKeyUsage`.

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 extensions),
- 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 stipulation – a certificate renewal process is not intended. A new certificate application and issuance is necessary.

4.7. Certificate re-key

No stipulation – a certificate re-key process is not intended. A new certificate application and issuance is necessary.

4.8. Certificate modification

No stipulation – a certificate modification process is not intended. A new certificate application and issuance is necessary.

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.

4.10. Certificate status service

Certificate revocation lists have to be published in order to verify whether a certificate has been revoked. The issuing of CRLs is mandatory for this policy. 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.

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

4.12. Key escrow and recovery

Key escrow and recovery for the private keys of devices are not offered.

For Root CAs and CAs and all other components, which use the HSM provided by the CA product manufacturer for the generation and usage of their private keys, a back-up of the keys exists. The keys have to be secured with master back up keys, so that recovery of these keys is possible in the event of a disaster.

5. Facility, Management, and operational Controls

PHOENIX CONTACT sets up facility, management, and operational controls.

5.1. Physical controls

PHOENIX CONTACT has to make provisions to warrant the failsafe of the PKI infrastructure. This includes the set-up of redundant data warehouses (either in hot-cold or hot-hot modus) with a sufficient level of assurance that external influences do not jeopardize the redundancy. Each warehouse has to be protected against external influences such as fire or power outage.

5.2. Procedural controls

PHOENIX CONTACT has to implement and document procedural controls and a role concept in which employees are assigned to one or more security relevant roles (“Trusted Roles”) by the management of PHOENIX CONTACT and receive corresponding authorization through a

controlled process. The authorizations of these individual roles have to be limited to those who need them to fulfill their tasks.

At least the following trusted roles have to be assigned: Security Officer, System Administrator, System Operator and Auditor. In addition, the role concept should include a data protection officer.

It has to be warranted that 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 has to provide for various role exclusions in order to prevent conflicts of interest. Role exclusions have to be 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 must additionally be protected by multi-factor authentication.

5.3. Personnel controls

PHOENIX CONTACT has to warrant, 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 has to be confirmed before the start of the work. Initial and event-related training has to be offered to warrant competence in the areas of activity as well as general information security. Training courses and proof of performance have to be documented.

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

PHOENIX CONTACT must exclude unreliable employees from the activities in the certification service. Provisions must be made to sanction violations by employees against the processes of the TSP operation. If the relationship of trust cannot be warranted, these employees must be excluded from security-related activities.

All relevant documents (e.g. procedural instructions, training materials) must be made available to employees.

5.4. Audit logging procedures

Only personnel authorized in accordance with the role concept must be allowed to administer computers, networks and other components. Event logs must be generated for at least the HSM and the PKI appliance and a regular evaluation of log files for rule transfers, attack attempts and other incidents must be conducted. Monitoring measures for devices must cover their entire life cycle form commissioning to disposal.

5.5. Records archival

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

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

Archived data must be kept for at least 30 years. Archiving must take place exclusively internally at PHOENIX CONTACT and in secure premises. These must be subject to the role concept and access regulations of PHOENIX CONTACT.

The data from the backup must be transferred to the archive through internal IT measures.

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

5.6. Key changeover

A reasonable time before a CA expires, new CA keys have to be generated, and new CA instances have to be set up and published. Reasons for changeover can result from key compromise, expiration of the certificate, change of algorithm, key length or certificate contents. For the root CAs PHOENIX CONTACT uses two different practices. For Root-CAs with limited certificate validity a cross certification period is used while the renewal of sub CAs are only time-shifted, otherwise the validity period of Root-CA and Sub-CA certificates are based on the life cycle of the products. This is only the case for the issuing of Initial Device Identities.

More details can be found in the CPS of PHOENIX CONTACT [CPS].

5.7. Compromise and disaster recovery

PHOENIX CONTACT must have a disaster recovery plan that is known to the roles involved and implemented by them when necessary.

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

More details can be found in the CPS of PHOENIX CONTACT [CPS].

5.8. CA or RA termination

No stipulations are made.

6. Technical Security Controls

6.1. Key pair generation and installation

CA keys must be generated in a Hardware Security Module (HSM) which has a “FIPS 140-2 Level 3” certification. Alternatively, HSMs can be used that have a Common Criteria evaluation and, if applicable, a certificate based on the evaluation. For example, an HSM can also be used for which a successful Common Criteria evaluation based on the CEN EN 419 221-5 Protection Profile is available. The CAs and its HSMs must operate in a secure data center. The key ceremony has to be carried out according to established procedures. The key ceremony must be performed by designated Trusted Roles 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 must be enforced during key generation.

The key ceremony has to be 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.

Hereby procedural and technical controls are in place to protect private keys from unauthorized access or modification and to warrant that they are not stolen or modified (cf. [IEC 62443-4-1], SM8 Controls for private keys).

Keys of end-entities are not generated by CAs.

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

Certificates use RSA keys with a key length of 4096 Bit for Root-CA and CA-certificates and at least 2048 Bit for end-entities. A key length of 2048 Bit may only be used 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. Alternatively, ECDSA keys with a key length of at least 256 Bit with domain parameters of NIST or brainpool curves are used. Details regarding the key sizes can be found in PHOENIX CONTACT’s CPS [CPS].

CA keys must be generated in a Hardware Security Module (HSM) which has a “FIPS 140-2 Level 3” certification. Alternatively, HSMs can be used that have a Common Criteria evaluation and, if applicable, a certificate based on the evaluation. 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).

Private Root-CA keys are used only for the signing of Sub-CA certificates and CRLs. All other private CA keys are used for the signing of Sub-CA certificates, end-entity certificates and CRLs.

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

The cryptographic modules, hardware security modules, used by PHOENIX CONTACT for certification authorities must be “FIPS 140-2 Level 3” certified. This applies also for the cryptographic modules used for the code signing (signing server) and the time stamp units. Alternatively, HSMs can be used that have a Common Criteria evaluation and, if applicable, a certificate based on the evaluation. The cryptographic modules used for initial device identities are the device’s secure element (e.g. TPM). Hereby, technical controls are in place to protect private keys from unauthorized access or modification and to warrant that they are not stolen or modified (cf. [IEC 62443-4-1], CR 1.9 – Strength of public key-based authentication).

The hardware security modules used by PHOENIX CONTACT should support a backup process for generated private keys. For this, the keys must be secured by encryption and integrity protection and the key used for securing the private key must have at least the same security level as the private key. This applies for all private keys generated and used in the hardware security modules of CAs, signing servers and TSUs.

For private keys of initial device identities key escrow does not need to be supported.

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 must be protected by encryption and integrity check values.

Method of activating private key

Private keys of Root-CAs may only be used under dual control. Private keys of Sub-CAs have to be activated only once after their generation or after booting of the Sub-CA.

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 must be 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 a deactivation process need not be supported.

Method of destroying private key

The private keys of CAs, signing servers and TSU’s must be inactivated at the end of their life cycle.

The private keys of initial device identities and its certificates lose their validity when the device is finally taken out of service and disposed of in accordance with the product-specific specifications.

6.3. Other aspects of key pair management

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.

The validity period of certificates for CAs, signing servers and TSU's is variable and can be taken from the certificate. More details can be found in the CPS of PHOENIX CONTACT [CPS].

6.4. Activation data

Private keys of Root-CAs may only be used under dual control. Private keys of Sub-CAs have to be activated at least once after their generation and after each booting of the system.

For private keys of initial device identities an activation process needs to not be supported.

6.5. Computer security controls

PHOENIX CONTACT and the 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 warrant in the configuration used that only actions can be carried out which do not stand in contradiction to the company's CPS [CPS].

6.6. Life cycle technical controls

During the development, security measures should be in place. Security requirements should already be analyzed in the design phase and the results obtained should be defined as a requirement during development and implemented accordingly.

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

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

6.7. Network security controls

A network concept must be 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 PHOENIX CONTACT, for example firewall and intrusion detection / prevention mechanisms have to be 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 have to be warranted and 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. Alternatively, HSMs can be used that have a Common Criteria evaluation and, if applicable, a certificate based on the evaluation. The time stamp units are processed on a signing server.

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

All certificates issued in the public key infrastructure conformant to the CP at hand are X.509 public key certificates, version 3 (cf. [X.509]). The recommendations of RFC 5280 [RFC 5280] as well as IEEE Std. 802.1 ARTM-2018 [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.

The certificate profiles are described in the certification practice statement issued by PHOENIX CONTACT.

7.2. CRL profile

All certificate revocation lists (CRL) issued in the public key infrastructure conformant to the CP at hand are X.509 certificate revocation lists, version 2 (cf. [X.509]). The recommendation of RFC 5280 [RFC 5280] as well as IEEE Std. 802.1 AR^{TM}-2018 [IEEE 802.1] are taken into

consideration for the definition of the CRL profiles. In all CRLs only standardized CRL extensions or CRL entry extensions are used. Private extensions are not defined by PHOENIX CONTACT.

The certificate revocation list profiles are described in the certification practice statement issued by PHOENIX CONTACT.

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

9.1. Fees

Certificates are only issued to internal certificate subjects and based on the application of internal subjects and subscribers. No fees are charged for the relevant services. Any expenses incurred will be charged internally, if applicable.

Information about certificates will be provided without additional charges to external parties.

9.2. Financial responsibility

Insurance coverage

PHOENIX CONTACT has the necessary resources and financial stability to operate the public key infrastructure in accordance with this CP and the associated CPS.

Other Assets

No stipulations.

Insurance or warranty coverage for end-entities

No stipulations.

9.3. Confidentiality of business information

PHOENIX CONTACT issues certificates for initial device identities, code signing and time stamp units. All subjects are PKI participants that are under control of PHOENIX CONTACT or the PHOENIX CONTACT group. Public keys of external subjects are not certified by PHOENIX CONTACT. The issuance and management of end-user certificates does not require the processing of personal or confidential data.

Notwithstanding the above, the following rules shall apply in principle.

Scope of confidential information

Unless otherwise agreed or required by law, confidential shall be all information, facts, documents, data and/or knowledge, in particular technical and/or economic information, design documents, specifications, drawings, samples, prototypes, test results, source codes, object codes, as well as data of customers of PHOENIX CONTACT and/or secret know-how and trade secrets of PHOENIX CONTACT, i.e., identifiable knowledge which is accessible to a limited circle of persons only, e.g., in the form of information not publicly known about production processes or audit results which the recipient receives from PHOENIX CONTACT, whether in writing, in text form, electronically, orally, visually, or in any other form. Confidential information shall also include all copies made thereof, self-produced materials, and summaries.

Information not in the scope of confidential information

Unless otherwise agreed or required by law, information is not confidential, which (a) was already in the public domain at the time of its disclosure or which, after its disclosure, has come into the public domain without breach of a Non-Disclosure-Agreement; or (b) was already known to the recipient at the time of its disclosure; or (c) was made available to the recipient by a third party after its disclosure in a lawful manner and without restriction with regard to confidentiality or use; or (d) was developed independently by the recipient itself and without recourse, either directly or indirectly, to confidential information or in accordance with the exceptions provided for in this section under (a)–(c).

All information in issued and published certificates as well as the data mentioned in section 2.2 are considered public.

Responsibility to protect confidential information

PHOENIX CONTACT protects confidential information and takes the appropriate and necessary measures for this purpose. In particular, PHOENIX CONTACT has an internal know-how protection policy that protects both its own confidential information and third-party confidential information.

9.4. Privacy and personal information

Privacy Plan

PHOENIX CONTACT processes personal data in accordance with the relevant applicable law. Nonetheless, the issuance and management of end-user certificates does not require the processing of personal or confidential data.

Information treated as private

The issuance and management of end-user certificates does not require the processing of personal or confidential data.

Information not deemed as private

All information and data contained in or derivable from the certificates issued by PHOENIX CONTACT and in the documents referred to in section 2 shall be treated as non-confidential data.

Responsibility to protect private information

The issuance and management of end-user certificates does not require the processing of personal or confidential data.

Disclosure pursuant to judicial or administrative process

PHOENIX CONTACT is subject to the laws of the Federal Republic of Germany. Information on certificate-related data will be released to the investigating authorities if a court order exists or other legal provisions require release.

Other information disclosure circumstances

Information other than that described in "Disclosure pursuant to judicial or administrative process" will not be provided.

9.5. Intellectual property rights

The existence, content and rights of use of and to industrial property rights and copyrights shall be governed by the statutory provisions and/or contractual agreements.

9.6. Representation and warranties

Unless certain conditions are expressly designated as representation or guarantee, PHOENIX CONTACT does not provide any representations or guarantees. In all other respects, the respective contractual agreements and the General Terms and Conditions of the respective PHOENIX CONTACT group member shall apply.

PHOENIX CONTACT confirms that the procedures described in the CP and the CPS are adhered to.

9.7. Disclaimers of warranties

The contractual agreements shall apply and, otherwise the General Terms and Conditions of the respective PHOENIX CONTACT group member shall apply if no contractual agreement has been made.

9.8. Limitations of liability

The contractual agreements shall apply and, otherwise the General Terms and Conditions of the respective PHOENIX CONTACT group member shall apply if no contractual agreement has been made.

9.9. Indemnities

The contractual agreements shall apply and, otherwise the General Terms and Conditions of the respective PHOENIX CONTACT group member shall apply if no contractual agreement has been made.

9.10. Term and termination

Term, termination, and effect of termination and survival

This CP shall apply from the date of publication and shall remain effective until the expiry of the last certificate issued under this CP. The version of the CP published at the time of application shall apply in each case.

9.11. Individual notices and communications with participants

Certificate subjects and / or subscribers shall be notified via internally available means of communications, if necessary.

9.12. Amendments

Procedure for amendment

Changes and amendments to this CP will be incorporated in this document and published under the same OID. Editorial changes are marked. The version number of the document will be updated.

Notification mechanism and period

No stipulations.

Circumstances under which OID must be changed

No stipulations.

9.13. Dispute resolution provisions

Complaints can be submitted to PHOENIX CONTACT in writing or by e-mail (see section 1.5 for contact information).

9.14. Governing law

The CP shall exclusively be governed by German law. The provisions of the Vienna UN Convention of 11 April 1980 on Contracts for the International Sale of Goods (CISG) shall be excluded.

Place of Jurisdiction:
Exclusive place of jurisdiction for all disputes concerning the CP shall be Cologne, Germany.

9.15. Compliance with applicable law

The respective certificate holder is responsible for ensuring that the certificates issued by PHOENIX CONTACT are used in accordance with the statutory provisions.

9.16. Miscellaneous provisions

Entire Agreement

The following documents are the subject matter of the applicable agreements involving the PKI participants and apply in the event of contradictions or regulatory gaps in the following order of precedence:

- application documentation (Certificate Signing Request),
- CP valid at the time of application as well as the valid CPS, and
- General Terms and Conditions valid at the time of application or the effectively withdrawn version thereof, if applicable.

Assignment

No stipulations.

Severability

Should individual provisions of this CP be ineffective or non-feasible or contain any regulatory gaps this will not affect the validity of the other provisions of this CP. Instead of the ineffective or non-feasible provision, the effective and feasible provision will be considered as agreed that comes closest to the meaning and purpose of the ineffective or non-feasible provision.

Enforcement (attorneys' fees and waiver of rights) and Force Majeure

The contractual agreements shall apply and, otherwise the General Terms and Conditions of the respective PHOENIX CONTACT group member shall apply if no contractual agreement has been made.

9.17. Other provisions

Compliance with export laws and regulations

The contractual agreements shall apply and, otherwise the General Terms and Conditions of the respective PHOENIX CONTACT group member shall apply if no contractual agreement has been made.