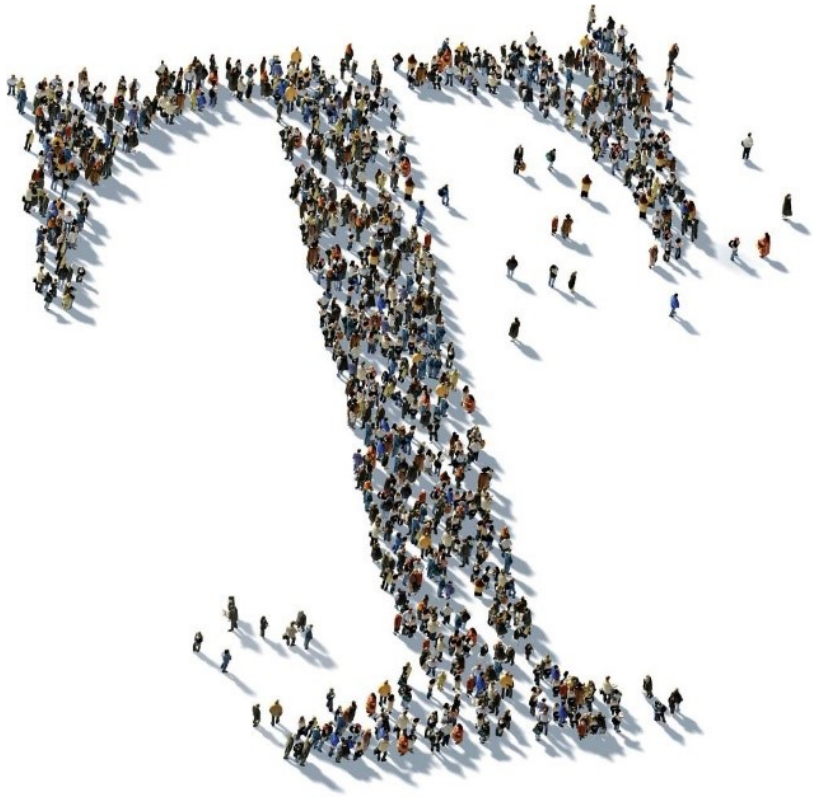
Telekom Security PKI Certificate Policy

Certificate Policy of the Telekom Security Trust Center Public Key Infrastructure



Deutsche Telekom Security GmbH

Public

Version: 12.00

Valid: 01.07.2020

Status: release

Last review: 05.06.2020

IMPRINT

Table 1 – Document properties

Property	Value
Issuer	Deutsche Telekom Security Trust Center & ID-Solutions Untere Industriestraße 20, 57250 Netphen, Germany
Filename	Telekom-Security-PKI-CP-EN-v12.00-20200605.docx
Valid since	01.07.2020
Title	Telekom Security PKI Certificate Policy Certificate Policy of the Telekom Security Trust Center Public Key Infrastructure
Version	12.00
Last review	05.06.2020
Status	release
Contact	Telekom Security Leiter Trust Center Betrieb
Abstract	Certificate Policy (CP) for Telekom Security PKI

Copyright © 2020 by Deutsche Telekom Security GmbH, Bonn

All rights reserved, including those relating to partial reprinting, photomechanical reproduction (including microcopy) and analysis using databases or other equipment.

VERSION HISTORY

Table 2 – Version history

Version	Date	Author	Changes
8.0	15.05.2018	T-Systems	Initial version after splitting CP & CPS document and changing the document structure conform to RFC 3647. A new version history has been started as older document versions base on a different document structure.
9.0	12.10.2018	T-Systems	Changes in sections 1.5.2, 4.9 and 5
10.0	10.10.2019	T-Systems	Changes according to BR 1.5.7-1.6.6 Changes according to EV 1.6.9-1.7.0
10.1 10.2	03.03.2020	T-Systems	Changes towards an accessible document template Changes according to Mozilla 2.7 requirements Changes according to BR 1.6.7 Changes according to EV 1.7.1
10.3	03.03.2020	T-Systems	Quality check
11.00	13.03.2020	T-Systems	Approval and release of new version
11.01	05.06.2020	T-Systems	Changing T-Systems International GmbH to Deutsche Telekom Security GmbH
11.02	05.06.2020	T-Systems	Review
11.03	05.06.2020	T-Systems	QS
12.00	08.06.2020	T-Systems	Release

TABLE OF CONTENT

LIST OF TABLES

LIST OF FIGURES

There are no figures in the current version of the document.

1 INTRODUCTION

1.1 Overview

The Telekom Security Trust Center Public Key Infrastructure (Telekom Security PKI) is operated in the Telekom Security Trust Center by the Deutsche Telekom Security GmbH Group unit within Deutsche Telekom AG. The Trust Center maintains a number of different certification authorities under different root certification authorities (root CAs).

This document is the certificate policy (CP) for all certification authorities operated within the Telekom Security PKI, focusing the Root-CA level. It is based on the international standard for certificate policies (RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework) of the Internet Engineering Task Force (IETF).

The Trust Center additionally guarantees that all certification authorities within the Telekom Security PKI meet and comply with the requirements and regulations of the current published version of the "CA/Browser-Forum Baseline Requirements" [CAB-BR] (http://www.cabforum.org/documents.html). In the event that this document and the [CAB-BR] contradict one another, the regulations in the [CAB-BR] have priority.

1.2 Document name and identification

Table 3 – Document properties

Name	Version	Datum	Objektbezeichnung (Object Identifier)
Telekom Security PKI Certificate Policy	12.00	01.07.2020	1.3.6.1.4.1.7879.13.38

1.2.1 Revisions

The revisions of the document are integrated in the version history at the beginning of the document.

1.2.2 Relevant Dates

The relevant dates are integrated in the version history at the beginning of the document.

1.3 PKI participants

1.3.1 Certification authorities (CA)

In addition to operating certification authorities for proprietary internal products and services, the Trust Center issues CA certificates for certification authorities of other operators.

1.3.2 Registration authorities (RA)

One or more registration authorities are mapped to each certification authority. There are no restrictions about the number of registration authorities that are mapped. A registration authority reports to the mapped certification authority and operates as an interface to the subscribers of the PKI. The registration authorities are therefore also governed by this CP.

For the majority of the certification authorities, a new hierarchy is created within the mapped registration authorities into one or more higher level and one or more subordinate registration authorities. Every subordinate registration authority is mapped to exactly one higher-level registration authority.

Tasks of higher-level registration authorities include:

- Approving and revoking subordinate registration authorities
- Mapping the relevant area of responsibility of a subordinate registration authority (for which subset of subscriber orders is the registration authority responsible?)
- Revoking and suspending subscriber certificates across all areas of responsibility
- Tasks of subordinate registration authorities include:
- Registering subscribers within the defined area of responsibility
- Reviewing subscriber orders within the defined area of responsibility in accordance with the policies of the respective certification authorities (with the help of certified or officially sealed identification documents, where necessary)
- Approving subscriber orders following a successful review or rejecting them
- Sending the order to the certification authority following the approval of a subscriber order so that the subscriber certificate can be issued and delivered
- Within the defined area of responsibility, accepting and reviewing orders for certificates that may have to be revoked or suspended (if a suspension is planned in the context of the relevant certification authority)
- Sending a request to the certification authority to revoke or suspend the subscriber certificate once a revocation or suspension request has been approved

If the registration authorities are not placed into a hierarchy, the registration authorities carry out the same tasks as the subordinate registration authorities without there being a division into areas of responsibility.

The registration authorities are equipped with the necessary technology. The employees of the registration authenticate securely to the respective certification authority.

1.3.3 Subscribers

Root CA subscribers are exclusively directly subordinate certification authorities. No end-entity certificates are issued.

The subscriber

- applies for the certificate (represented by an authorized natural person)
- is authenticated by the responsible CA as part of the registration process
- is identified by the certificate, i.e., it is confirmed that the public key contained in the certificate belongs to the subscriber
- owns the private key that belongs to the public key in the certificate

1.3.4 Relying parties

A relying party is a natural person or subject who/that relies on the trustworthiness of the certificate issued by Telekom Security and/or the digital signature.

1.3.5 Other participants

No functions and/or tasks are outsourced to external authorities (delegated third party), which relate to operation of the CA infrastructure, as well as verification, approval, or processing of certificates or certificate applications.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates are used for authentication purposes, the digital signature, as well as encryption as part of various applications depending on the assignment of the attributes on key usage and the CPS definitions of the relevant certification authority.

The subscriber is responsible for using certificates in such a way that their use complies with the applicable legal provisions. This applies in particular to compliance with the applicable export or import regulations.

1.4.2 Prohibited certificate uses

Certificates are not intended, designed, or permitted for use or forwarding for:

- management and control facilities in dangerous environments
- environments in which fail-safe operation is required (e.g., operation of nuclear facilities, aircraft navigation or communication systems, air traffic control systems, or weapon control systems) and where failure could lead to damage (e.g., personal injury, death, medium and serious environmental damage, or other disasters)

Furthermore, it is not permitted to use an issued certificate for a MITM scenario or if its use is prohibited by law.

1.5 Policy administration

1.5.1 Organization administering the document

This document (CP) is published by Deutsche Telekom Security GmbH, Trust Center & ID-Solutions.

1.5.2 Contact person

Address:

Deutsche Telekom Security GmbH

Trust Center & ID Solutions

Leiter Trust Center Betrieb

Untere Industriestraße 20

57250 Netphen, Germany

Phone:

+49 0 1805 268 204 (from Germany: landlines EUR 0.14/minute, mobile networks max. EUR 0.42/minute)

WWW: https://www.telesec.de

E-Mail: telesec_support@t-systems.com

The report of abuse, compromise of certificates and keys of Trust Center must be able to be reported under a URL 24/7 for everyone. The website must contain a process description/instruction for the user and must also be present in chapter 1.5.2 of the CPS.

1.5.3 Person determining CPS suitability for the policy

This document (CP) remains valid as long as it is not revoked by the publisher (see Section 1.5.1). It is updated when required (but at least once a year) and is then assigned a new ascending version number (see also Sections 9.12.1 and 9.12.2).

The CPS has to be created in conformance to the given CP.

1.5.4 CP approval procedures

The publisher named in Section 1.5.1 is responsible for this document (CP). The approval is given by the Change Advisory Board.

This CP undergoes an annual review process, regardless of any other amendments. The department named in Section 1.5.1 is responsible for carrying out or coordinating the review.

The annual review must be noted in the change history of the CP. This shall also apply even if no changes are made to contents.

1.6 Definitions and acronyms

1.6.1 Definitions

Table 4 – Definitions

Term	Explanation
Affiliate	For example, a company, partnership, joint venture, corporation, (capital) company, association, foundation, or other organization (legal person) that supervises, is supervised by, or is controlled together with another organization (legal person), facility, department, governmental unit, or unit that is directly subordinate to a governmental authority.
Applicant	The natural or legal person who applies for a certificate (or requests its renewal). Once the certificate has been issued, the applicant is referred to as the subscriber. In the case of certificates issued for devices, the applicant is the organization that controls or operates the device listed on the certificate, even if the device sends the actual certification application.
Applicant's representative	If different from the applicant, a natural person or payer, an employee of the applicant, or an authorized representative who has the express authority to represent the applicant: (i) who signs, submits, or approves an application for a certificate in the name of the applicant and/or (ii) signs and submits a subscriber agreement in the name of the applicant and/or (iii) acknowledges and agrees to the certificate's terms of use in the name of the applicant if the applicant is an affiliated company (affiliate) of the certification authority (CA).
Application for a certificate with increased risk	An application for which the CA provides an additional check with regards to internal criteria and databases that the CA runs. This can concern names that are subject to a high risk about phishing or other fraudulent use, names that are contained in previously rejected certificate applications or revoked certificates, names that are on the MillerSmiles phishing list, or the Google

Term	Explanation
	Safe Browsing list or names that the CA identifies based on its own risk-minimization criteria.
Application software provider	A provider of Internet browser software or other application software on the relying side that displays or uses certificates and contains root certificates.
Authentication	Checking an identity based on claimed characteristics.
Authority revocation list (ARL)	List showing digital certificates that have been revoked by certification authorities (except root CA). Before a digital certificate of a certification authority is used, the ARL should be used to check whether the certificate may still be used.
Authorization document	The documentation that proves an applicant is authorized to apply for one or more certificates for a certain natural person, group of persons or functions, legal person, or device. This may also be a document from the certification authority regarding communication with the person or organization in question.
Bulk	Function of a CA with which the sub-registration authority can generate soft PSEs in bulk.
Central registration model	Following successful registration, the sub-registration authority requests the certificate on the sub-registration authority website (using a web form or in bulk) and directly receives this certificate or the key material for the end entity (except in the case of a registration authority certificate).
Central repository	An online database that contains public PKI documents (e.g., certificate policy, certificate practice statement, CA certificates), as well as additional information, either in the form of a CRL or an OCSP response.
Certificate	An electronic document that uses a digital signature to bind a public key to an identity (e.g., person, device).
Certificate administration process	Processes, practices, and procedures relating to the use of keys, software, and hardware that the certification authority (CA) uses to check certificate data, issue certificates, maintain a central data repository, and revoke certificates.
Certificate application	A request made in electronic or written form that contains data regarding an applicant.
Certificate data	Certificate applications and associated data (obtained from the applicant or elsewhere) that is in the possession of the certification authority (CA), is subject to monitoring by the CA or that the CA has access to.
Certificate Management Protocol (CMP)	The Certificate Management Protocol is a protocol developed by the IETF to manage X.509 certificates within a public key infrastructure (PKI).
Certificate policy (CP)	Defines the guidelines for generating and managing certificates of a certain type. A set of rules that specifies the options for using a named certificate in a certain community (parties involved in PKIs) and/or a PKI implementation with common security requirements.
Certificate problem report	Complaints due to suspicion that the key is at risk, certificate misuse, or with regard to other types of fraudulent behavior, risk, misuse, or incorrect behavior in connection with certificates.
Certificate revocation list (CRL)	A regularly updated, time-stamped list of revoked certificates that is generated and signed digitally by the issuing certification authority (CA). The authority revocation list (ARL) is a special certificate revocation list (CRL), as it contains only sub-CA certificates.
Certificate signing request (CSR) [TC]	A certificate request that is created electronically by a device (e.g., server) and signed using the private key, which contains the public key and the certificate data in coded form. The syntax is described by the standard PKCS#11.
Certification authority (CA)	An organization that is responsible for generating, issuing, revoking and managing certificates. This term is used for both root certification authorities (root CA) and subordinate certification authorities (sub-CA).
Certification practice statement (CPS)	Explanations for operating a certification authority. In particular, the CPS implements the provisions and policies of the CP of a certification authority. One of several documents that provide general and specific framework conditions. This contains, in particular, a description of the procedure the

Term	Explanation
	certification authority (CA) follows for issuing, managing, revoking, and renewing certificates.
Change Advisory Board	A board within Telekom Security that decides on PKI functions.
Chip card	Plastic card with an integrated computer chip. Telephone cards are an example of these. If the computer chip is able to perform calculations, it is also called a smartcard. Smartcards can also be used for cryptographic applications.
Compromise	A private key is compromised if it is made known to unauthorized persons or can be used by them. A compromise could occur through a criminal attack, for example.
Country	Either a member of the United Nations or a geographical region that at least two member states of the UNO recognize as a sovereign state.
Cryptography	Science dealing with the encryption of data and related issues (such as digital signatures).
Delegated third party	A natural or legal person who is not identical to the certification authority (CA) but is authorized by this authority to support the certificate management process by performing tasks to fulfill one or more requirements. This may be an external registration authority or an internal enterprise registration authority.
Device	Component such as a router, server, gateway, or application that supports certificate-based functions but cannot request certificates itself or can do so only to a limited extent. Frequently, certificates are requested via an authorized person (e.g., administrator) and installed on the component.
Device certificate	X.509 V3 certificate that contains either a host name, an IP address, or an e-mail address in the commonName field (CN) of the subscriber's distinguishedName (subject) and/or in at least one subjectAltName extension.
Digital signature	A checksum created with a special mathematical procedure. Guarantees the authenticity of the signatory and the integrity of the data.
Directory service	Data repository for calling up certificates and certificate validation information (revocation list).
Distinguished name	Format with which distinguished names can be specified in accordance with the X.500 standard. A digital certificate must contain a DN.
Domain authorization document	The documentation that the domain name registrar, a registered domain owner (domain name registrant), or the person or organization that is listed as the registered domain owner in WHOIS (including all private, anonymous, or proxy registration services) provides and that proves the applicant's authorization to request a certificate for a particular domain name space. This may also be a document from the certification authority regarding communication with the person or organization in question.
Domain name	The name that is given to a node in the Domain Name System (DNS).
Dual key certificate	Variant in which separate key pairs are used for encryption and signing. This means the user has two corresponding certificates.
End entity	Also see Subscriber. The term end entity is largely used in the X.509 environment.
End-entity certificate	A certificate that does not use the "certification authority" basic constraint and therefore cannot sign certificates itself.
ETSI certification	Check and confirmation for certification authorities by an independent expert to ensure that the PKI is operated in accordance with the "ETSI TS 102 042" ETSI criteria. The aim of ETSI audits is to strengthen demand-side trust in electronic business transactions.
External registration authority	An employee (staff member) or representative of a company that is not affiliated with the certification authority (CA) (non-affiliate) that approves certificates for third parties. These roles (trusted roles) are performed, for

Term	Explanation
	example, by the tenant's master and sub-registration authority or authorized representative.
Fully qualified domain name (FQDN)	Correct and complete domain name, i.e., a chain of all labels for a path in the domain name space (for further information see RFC 2181).
Hardware security module (HSM)	Hardware to generate and store private keys securely.
Hash value	In this context, a fixed length cryptographic checksum (the correct name is cryptographic hash value). It should be as unlikely as possible to calculate the entry from the hash value or to find several possible inputs for the same hash value (hash value is used as a synonym for fingerprint). In most cases a hash value is signed instead of a complete digital document.
Identification	The process of providing the identity of a subject or object (e.g., user, device) to a system. The identification is part of the validation.
Interface	An interface is part of a system that is used for communication (input and output).
Internal registration authority	An employee (staff member) or representative of a CA who checks the "domain" specified by the PKI tenant and provides it for the certificate application. This role (trusted role) is performed, for example, by the Trust Center operator.
Internal server name	A server name (which may or may not contain a registered domain name) that cannot be dissolved with the public Domain Name System (DNS).
Issuer distinguished name (issuer DN)	Format with which distinguished names can be specified in accordance with the X.500 and LDAP standards. The issuer DN describes the CA issuing the certificate in a unique way.
Issuing certification authority (CA)	The certification authority (CA) that issued a specific certificate. This could be a root certification authority (root CA) or a subordinate certification authority (sub-CA).
Key backup	Mechanism for backing up keys. In order to be able to restore encrypted e-mails in the event of key loss, we recommend backing up the key material of the encryption key. Key backup is also used as a synonym for key archiving.
Key compromise	A private key is considered to be compromised if its value is shared with an unauthorized person, an unauthorized person has access to it, or there is a practical method that an unauthorized person could use to find out its value.
Key owner	A natural person authorized by the delegated third party who is responsible for the proper use (distribution, use and, if necessary, revocation) of the key pair and certificate that was issued for a group of persons or functions, legal person, or device.
Key pair	The private key and its corresponding public key.
Key recovery	Mechanism for recovering keys. This can be necessary if users lose their key (such as through a damaged file).
Latency period	Period of time between an action and the occurrence of a delayed reaction (delay period). With latency periods, the action occurs unnoticed and is only discovered through the reaction.
LDAP server	Server that saves information that can be called up via LDAP.
Legal person	A company, group, partnership, sole trader, trust, government authority, or legal entity with legal standing within the legal system of a country.
Lightweight Directory Access Protocol (LDAP)	Protocol for querying directories. This has displaced the significantly more complicated Directory Access Protocol (DAP) in many areas. LDAP offers more options than HTTP and FTP (such as setting up a context that can be

Term	Explanation
	maintained using several queries). LDAP is used in particular to query digital certificates and revocation lists within public key infrastructures.
Local registration model	The user requests the certificate via the user website or by sending an e-mail request, or the device uses its SCEP interface to request the certificate. This request is processed by the sub-registrar (approval, rejection, or postponement (resubmission)).
Mail security	Security functions such as digital signature and encryption that support standard mail applications.
Management system for information security (ISMS)	The management system for information security (ISMS) represents a set of procedures and rules within a company that serve to define, manage, monitor, maintain, and continually improve information security over the long term. The term is used in the ISO/IEC 27002 standard; ISO/IEC 27001 defines an ISMS.
Master domain	Independent administrative area that has a distinguished name and is set up exclusively for a delegated third party. The delegated third party can approve and manage certificates within the tenant. The tenant is managed using the master registration authority certificate. Further information is available under: Tenant.
Master registration authority	Natural person (trusted role) who manages the master domain.
Multitenancy	In information technology (IT), multitenancy refers to the property of software or a server to map multiple, fully separated tenants on one installation. The respective tenants (e.g., legal units or companies) are unable to view the data, user administration, or similar of the other parties/tenants.
Object identifier (OID)	A unique, alphanumeric, or numeric identifier that is registered for a specific object or object class of the International Standards Organization (ISO) under the appropriate standard.
OCSP responder	An online server that is subordinate to the certification authority (CA) and is connected to its central repository to process certificate applications. Also see Online Certificate Status Protocol (OCSP).
Online Certificate Status Protocol (OCSP) [BR]	A protocol for online certificate validation with the help of which the application software on the relying side can determine the status of an identified certificate. Also see OCSP responder.
Period of validity	The period from the issue date (not before) until the expiry date (not after).
Permitted Internet domains	A domain name that consists of the top-level domain and further sub-domains and is added to the tenant's PKI configuration (master domain) as a "permitted Internet domain" following a successful check by the internal registration authority.
Permitted public data source	An authentication document or a data source (e.g., identity database, commercial register) that is used to check subject identity data, that is generally recognized by commercial companies and authorities (public administration) as reliable and that a third party created for a different purpose other than the issuing of certificates by the applicant.
Person authorized to revoke	A person who is authorized by the subscriber or key owner to revoke a certificate for a group of persons or functions, legal person, or device. Authorization is via the certificate revocation password.
Personal Identification Number (PIN)	Secret code used at cash machines, for example.
Personal security environment (PSE)	All security-relevant information such as the private key is saved in the personal security environment. The PSE can be available as an encrypted file or on a smartcard and is protected by a password or a PIN.
Policy	Guidelines or explanations that determine the security level for creating and using certificates. There is a difference between certificate policy (CP) and certification practice statement (CPS).

Term	Explanation
Power of attorney	Power of attorney is understood to be a power of representation founded on a legal transaction. The power of attorney is established through unilateral declarations of intent that the principal must communicate to the agent of the power of attorney.
Private key	They key from a key pair that the key owner keeps secret and uses to create digital signatures and/or decrypt electronic data and files that were encrypted using the corresponding public key.
Public device certificate	A device certificate that a sub-CA issues in the CA hierarchy below a root certificate.
Public key	The key from a key pair that the owner of the corresponding private key is permitted to make publicly available and that the relying side uses to verify digital signatures that were created using the owner's private key and/or to encrypt messages that can only be decrypted using the owner's corresponding private key.
Public key infrastructure	Hardware, software, persons, procedures, rules, guidelines, and obligations that enable certificates and keys to be generated, issued, managed, and used reliably based on the public key cryptography.
Public Key Infrastructure X.509 (PKIX)	IETF standard that standardizes all relevant parts of a PKI.
Public Key Service (PKS)	Service of the Trust Center for issuing and administrating certificates that comply with the German Digital Signature Act.
Qualified auditor	A natural or legal person who meets the specified criteria.
Registered domain name	A domain name that is registered with a domain name registration authority (registrar).
Registration authority (RA)	A legal person who is responsible for identifying and authenticating certificate subjects. However, this is not a CA and therefore does not sign or issue certificates. An RA can provide support when requesting or denying a certificate or in both cases. When "RA" is used as an adjective to describe a role or function, this does not necessarily refer to an independent authority. It can, however, be part of the CA.
Registration authority of a company (enterprise RA)	An employee (staff member) or representative of an organization who is not affiliated with the certification authority (CA) (non-affiliate) that approves certificates for third parties. These roles (trusted roles) can be performed, for example, by the tenant's master and sub-registration authority or authorized representative.
Registration model	A distinction is made between the central registration model (see there) and the local registration model (see there).
Relying parties	A natural or legal person who relies on a valid certificate. A provider of software is not a relying party if the software this provider sells merely contains information on a certificate.
Revocation authority	An employee (staff member) or representative of an organization who performs certificate revocations.
Rivest Shamir Adleman (RSA)	Procedure for encryption, for digital signature and for the secure transmission of keys that is named after the three cryptographers Rivest, Shamir, and Adleman.
Root CA	See Root certification authority.

Term	Explanation
Root certification authority (root CA)	The highest-level certification authority whose root certificate is distributed by application software providers and who issues the subordinate CA certificates (sub-certificates).
Root certification authority certificate (root certificate)	The self-signed certificate that the root certification authority (root CA) issues for self-identification. In addition, this certificate helps with the validation of issued sub-certificates.
Secure Multipurpose Internet Mail Extension (S/MIME)	Secure Multipurpose Internet Mail Extension. Extension of the MIME e-mail format, which describes additions for cryptographic services that guarantee the authenticity, integrity, and confidentiality of messages.
Secure Socket Layer (SSL)	Crypto protocol for ensuring end-to-end connections on the Internet. This has now been superseded by the newer TLS process. Can be used instead of the more complex IPSec in many cases.
Service desk	The service desk is an organizational unit within a company that serves as the tenant or delegated third party's central contact point for all service and support requests and that conveys these within the company in accordance with the agreed business processes.
Simple Certificate Enrollment Protocol (SCEP)	Simple Certificate Enrollment Protocol. Protocol for ordering and loading certificates in IPSec devices.
Simple Object Access Protocol (SOAP)	Simple Object Access Protocol: SOAP provides a simple mechanism for exchanging structured information between applications in a decentralized, distributed environment.
Single key certificate	Variant in which the same key pair is used for encryption and signing. This means the user has one certificate.
Smartcard	A special plastic card with an integrated computer chip that can also be used for cryptographic applications.
Software PSE (soft PSE)	An encrypted file for saving the certificate and the corresponding private and public keys.
Sub-domain	Hierarchically subordinated sub-section of the master domain that is managed by a sub-registration authority.
Subject	The natural person, device, system, unit, or legal person that is named as the subject in a certificate. The subject is either the subscriber or a device that is under the subscriber's control or is operated by this person.
Subject Alternative Name	Additional fields in a certificate. The fields can be used to enter additional names of the subscriber and are a standard extension of the X509 standard.
Subject distinguished name (subject DN)	Format with which distinguished names can be specified in accordance with the X.500 and LDAP standards. The subject DN uniquely specifies a person or device.
Subject identity data	Data that identifies the subject of the certificate. Subject identity data does not contain a domain name that is listed in the subjectAltName extension or the subject commonName field.
Subordinate certification authority (sub-CA)	A certification authority whose certificate is signed by a root certification authority (root CA) or another subordinate certification authority (sub-CA).
Sub-registration authority	Natural person (trusted role) who manages the sub-domain.
Subscriber agreement	An agreement between the certification authority (CA) and the applicant/subscriber that specifies the rights and obligations of the parties.
Suspension	In relation to the PKI, suspension means a provisional or temporary revocation. The certificate initially appears in the certificate revocation list, but can be re-activated by the sub-registration authority.

Term	Explanation
Tenant	The tenant is a separate, logically self-contained unit with its own legal, organization, and data management within the system. The tenant thus structures the use of the system. The master domains are known as tenants. Within the master domains, there are further subdivisions in the form of areas of responsibility (also known as sub-domains).
Terms of use	Provisions regarding safekeeping and permitted usage of an issued certificate in accordance with the specified requirements if the applicant/subscriber is an affiliated company of the certification authority (CA), for example.
Transport layer security (TLS)	Crypto protocol for ensuring end-to-end connections on the Internet.
Triple key certificate	Variant in which separate key pairs are used for encryption and signing and Microsoft smartcard logon. This means the user has three corresponding certificates.
Trusted certificate	A certificate that is trusted due to the fact that its corresponding root certificate represents a trust anchor in widely distributed application software.
Unregistered domain name	A domain name that is not a registered domain name.
Valid certificate	A certificate that passes the validation procedure described in RFC 5280.
Validation	Evidence of the reproducibility of a result from a described procedure under defined conditions. The more precisely a procedure is described and the fewer unknown influencing factors there are, the more certain it is that corresponding results will be produced. A description of the goal and method is required for a validation. In this context, valid means that the method leads to the result in a repeatable manner. In the context of a PKI, there is a validation process in the following places: notification and verification of an identity (e.g., natural person, device) against the certificate application. Algorithm to check a certificate for its validity period, issuing certification authorities, and certificate status (valid, revoked).
Validation specialist	Someone who performs the data validation tasks in accordance with the requirements in question. In the context of the Trust Centers these are the following role owners: Trust Center operator, master registrar, sub-registrar
WHOIS	Information that is (a) directly retrieved from the Domain Name Registrar or registry operator via RFC 3912 protocol, (b) the Registry Data Access Protocol (RFC 7482), or (c) an HTTPS website.
Wildcard certificate	A certificate that has an asterisk (*) in the left-most position of a fully qualified domain name of the subject contained in the certificate.
X.509	Standard, whose most important element is a format for digital certificates. Certificates of version X.509v3 are supported in all common public key infrastructures.

1.6.2 List of acronyms

Table 5 – List of acronyms

Abbreviation	Definition
ARL	Authority Revocation List
BR	Baseline Requirements
DK	Dual Key
CA	Certification Authority
CMP	Certificate Management Protocol
CP	Certificate Policy
CPS	Certification Practice Statement

Abbreviation	Definition
CN	Common Name
CRL	Certificate Revocation List
DN	Distinguished Name
EDV	Electronic Data Processing
eIDAS	Electronic Identification and Signature
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
FQDN	Fully Qualified Domain Name
GRP	Identifies a group, function, or role certificate
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IPS	Intrusion-Prevention-System
IPSec	Internet Protocol Security
ISMS	Information Security Management System
ISO	International Organization for Standardization
IV	Individual Validation
LB	Service Description
LDAP	Lightweight Directory Access Protocol
n.a.	not available
NCP	"Normalized" Certificate Policy
NIC	Network information center
OCSP	Online Certificate Status Protocol
OID	Object Identifier
opt.	optional
OV	Organization Validated
OVCP	"Organizational Validation" Certificate Policy
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PN	Stands for pseudonym
PSE	Personal Security Environment
PTC	Publicly trusted certificate
RA	Registration Authority
RFC	Request for Comments
SCEP	Simple Certificate Enrollment Protocol
SK	Single Key
SLA	Service Level Agreement
RSA	Rivest Shamir Adleman
S/MIME	Secure Multipurpose Internet Mail Extension
SigG	German Digital Signature Act (*Signaturgesetz*)
SigV	German Digital Signature Regulation (*Signaturverordnung*)
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
TK	Triple Key
UPN	User Principal Name
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
XML	Extensible Markup Language

1.6.3 References

Table 6 - References

Shortcut	Reference
[BDSG]	Datenschutzgesetz, Bundesgesetzblatt I 2003 S.66 (Data Protection Act, Federal Law Gazette I 2003 p.66)
[CAB-BR]	Version of the “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” document published by CA/Browser Forum at http://www.cabforum.org/documents.html valid at the time
[EU-RL]	Directive of the European Parliament and of the Council on a Community framework for electronic signatures, 1999/93/EC, EU, 1999
[Moz-2-7]	Mozilla Root Store Policy, Version 2.7, Stand 01.01.2020, https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy
[PKCS]	RSA Security Inc., RSA Laboratories "Public Key Cryptography Standards," http://www.rsasecurity.com/rsalabs
[PKIX]	RFCs and specifications by the Public Key Infrastructure (X.509) IETF working group.
[RFC3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003
[RFC5280]	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008
[RFC6960]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.
[RFC6962]	Certificate Transparency. B. Laurie, A. Langley, E. Kasper. June 2013.
[SigG]	Law on general conditions for digital signatures and for the amendment of additional provisions (Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung von weiteren Vorschriften), Federal Law Gazette (Bundesgesetzblatt) I 2001, p. 876
[SigV]	Digital signature regulation (Verordnung zur elektronischen Signatur), BGBl (German Civil Code). I p. 3074, November 21, 2001
[X.509]	Information technology - Open Systems Interconnection - The Directory:authentication framework, Version 3, ITU, 1997

1.6.4 Conventions

No stipulation.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

The included CAs must develop, implement, enforce, and annually adapt a CPS and/or CP. The CPS must describe in detail how the respective valid requirements, in particular those of the Baseline Requirements and the Mozilla Root Program, are implemented.

2.1 Repositories

Each included CA must provide at least access to the revocation data through the directory service.

The included CAs can also make the subscriber certificates available in the directory service. If personal data is published that is subject to data protection, consent of the data subjects must have been obtained.

2.2 Publication of certification information

The included CAs must provide the following information to PKI participants:

Status information

In addition to the root and cross certificates, the PKI participants (see 1.3) must be provided with ARL, CRL, and OCSP information online on a 24/7 basis.

CP/CPS

Furthermore, the associated certificate policy/certification practice statement must be made easily accessible to all PKI participants with 24/7 availability.

Test websites

For web server certificates, the sub-CAs must provide test websites with participant certificates that are concatenated up to a public root. Websites with a valid, an expired, and a revoked certificate must be provided.

2.3 Time or frequency of publication

Root CA and sub-CA certificates must be made publicly available after production. Revocation information for root CA and sub-CA certificates must be updated in the event of a revocation. The ARL for the root CA and sub-CA certificates must be updated at least every six months. If cross-certificates are used, the ARL must be updated every 31 days.

CP/CPS documents must be reviewed at least once a year. The document must be updated if relevant changes are made to the explanations, measures, or procedures described in the CPS.

2.4 Access controls on repositories

The repositories under 2.2 must be publicly available without access restrictions. The repositories must be protected against unauthorized modification. Access from the public area may only take place in the form of read-only access.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

No stipulation.

3.1.1 Types of names

No stipulation.

3.1.2 Need for names to be meaningful

No stipulation.

3.1.3 Anonymity or pseudonymity of subscribers

No anonymized or pseudonymized certificate data may be used.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

The CN in Root-CA certificates must be unique.

3.1.6 Recognition, authentication, and role of trademarks

It is the sole responsibility of the subscriber that the choice of name does not infringe any trademarks, brand rights, etc. The certification authority is not obliged to verify such rights.

Only the subscriber is responsible for such checks. If a certification authority is notified of a violation of such rights, the certificate will be revoked.

3.2 Initial Identity Validation

The requested validation level must be ensured at every point of the trust chain. The validation level may become stronger in the trust hierarchy but must not become weaker at any level.

3.2.1 Method to Prove Possession of Private Key

In the event of a new order, the subscriber must prove to the certification authority in a suitable manner that he owns the private key that is mapped to the public key to be certified. Proof of ownership is provided by the PKCS#10 method. This requirement does not apply where the key is generated at the certification authority.

3.2.2 Authentication of Organization and Domain Identity

Certificate signing requests for certificates that contain only information in the "countryName" field are not permitted. All order information must be verified by the following checks.

3.2.2.1 Identity

If the subject identity information is to include the name or address of an organization, the CA MUST verify and check the identity and address of the organization. For this purpose, checks must be carried out to establish whether the address is the existing or valid address of the customer. The CA MUST verify the identity and address of the customer using the documentation provided by or procured through communication with at least one of the following bodies:

1. A public authority in the territory of the lawful establishment, existence, or recognition of the customer
2. A third-party database that is regularly updated and considered a reliable data source
3. A site visit by the CA or a third party acting as agent for the CA
4. A letter of confirmation

The CA MAY use the same documentation or communication described in 1 to 4 above to verify the identity and address of the customer.

Alternatively, the CA MAY verify the customer's address (but not the customer's identity) by using a utility bill, bank statement, credit card statement, tax document issued by the state, or any other form of identification that the CA determines to be reliable.

3.2.2.2 DBA/ Tradename

If the subject identity information is to include a company name or trade name, the CA MUST verify the customer's right to use the name/trade name by at least one of the following methods:

1. Documentation submitted by a public authority in the territory of the lawful establishment, existence, or recognition of the customer or documented by communication with such an authority
2. A reliable data source
3. Communication with a government agency responsible for managing such companies or trade names
4. A letter of confirmation accompanied by supporting documents
5. A utility bill, bank statement, credit card statement, tax document issued by the state, or any other form of identification that the CA determines to be reliable

3.2.2.3 Verification of Country

If the "subject:countryName" field exists, the CA MUST verify the subject's country using one of the following methods:

a. The allocation of the IP address range by the country to (i) the IP address of the website, as specified by
b. the DNS entry for the website, or (ii) the IP address of the customer
c. The ccTLD of the requested domain name
d. Information provided by the domain name registrar
e. A method identified in Section 3.2.2.1

The CA SHOULD implement a procedure to check proxy servers to prevent recourse to IP addresses assigned in countries other than the country in which the customer actually resides.

3.2.2.4 Validation of Domain Authorization or Control

For each fully qualified domain name (FQDN) listed in a certificate, the CA or a delegated third party MUST confirm that the customer (or the customer's parent company, subsidiary, or affiliate, collectively referred to in this section as "customer") is either the domain name registrant or has control over the FQDN on the date that the certificate is issued by performing at least one of the following checks:

3.2.2.4.1 Validating the Applicant as a Domain Contact

This method has expired on July 31st, 2018 and is no longer valid.

Validations which have been executed based on this method MUST NOT be used for issuing new certificates.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

The CA sends a random value to the domain contact by e-mail, fax, SMS (text message), or letter, which MUST be confirmed by the domain contact by e-mail, fax, SMS (text message), or letter. The contact data must be requested by the domain name registrar.

Each random value may only be used once and may not be older than 30 days.

3.2.2.4.3 Phone Contact with Domain Contact

The CA MUST use the phone number of the domain name registrant submitted to the domain name registrar for telephone contact. During the phone call, the CA must have the domain name registrant confirm the certificate application for each FQDN.

This method shall not be applied after May 31, 2019. Completed validations using this method shall continue to be valid for subsequent issuance per the applicable certificate data reuse periods.

3.2.2.4.4 Constructed Email to Domain Contact

By communicating with the domain administrator using an e-mail address, the CA MUST confirm that the customer has control over the domain. The e-mail address must be preceded by "admin," "administrator," "webmaster," "hostmaster," or "postmaster," followed by the "at" sign ("@"), then the domain name. The email message MUST contain a unique random value that MUST be included in the administrator's reply mail.

Each random value may only be used once and may not be older than 30 days.

3.2.2.4.5 Domain Authorization Document

This method has expired on July 31st, 2018 and is no longer valid.

Validations which have been executed based on this method MUST NOT be used for issuing new certificates.

3.2.2.4.6 Agreed-upon Change to Website

For each FQDN listed in the certificate, the customer MUST demonstrate practical control by making an agreed change on a website.

3.2.2.4.7 DNS Change

The CA must confirm the applicant's control over the FQDN. The control is verified by the presence of a unique random value issued by the CA during the order or a unique request token in the DNS CNAME, TXT, or CAA record.

3.2.2.4.8 IP Address

The CA must confirm the applicant's control over the FQDN. This can be verified by the applicant by controlling an IP address returned by a DNS search for A or AAAA records for the FQDN in accordance with Section 3.2.2.5.

3.2.2.4.9 Test certificate

No stipulation.

3.2.2.4.10 TLS using a random number

No stipulation.

3.2.2.4.11 Any other method

This method is no longer valid and MUST NOT be used.

3.2.2.4.12 Validating Applicant as a Domain Contact

The CA must confirm the applicant’s control over the FQDN. This may be verified by validating that the applicant is the domain contact. This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

The CA may issue other FQDNs that end with all the labels of the previous validated FQDN using this method. This method is also suitable for validating Wildcard Domain Names.

3.2.2.4.13 Email to DNS CAA Contact

The CA must confirm the applicant’s control over the FQDN. This may be done via sending a random value via email and then receiving a confirming response utilizing the random value. The random value must be sent to a DNS CAA email contact. The relevant CAA resource record set must be found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 (Appendix A).

Each email may confirm control of multiple FQDNs. Precondition is that each email address is a DNS CAA email contact for each authorization domain name being validated. The same email may be sent to multiple recipients. These recipients must be all DNS CAA email contacts for each authorization domain name being validated.

The generated random value must be unique in each email. The email may be re-sent provided that its entire content and recipients remain unchanged. The random value must remain valid for a maximum of 30 days. The CPS may specify a shorter validity time for random values. In that case the regulations of the CPS apply.

The CA may issue other FQDNs that end with all the labels of the previous validated FQDN using this method. This method is also suitable for validating Wildcard Domain Names.

3.2.2.4.14 Email to DNS TXT Contact

The CA must confirm the applicant's control over the FQDN. This may be verified by sending a random value via email and then receiving a confirming response utilizing the random value. The email is sent to the DNT TXT record email contract for the authorization domain name selected to validate the FQDN.

Each email may confirm the control over multiple FQDNs. Precondition is that each email address is a DNS TXT record email contact for each authorization domain name being validated. The same email may be sent to multiple recipients. These recipients must be all DNS TXT record email contacts for each authorization domain name being validated.

The generated random value must be unique in each email. The email may be re-sent provided that its entire content and recipients remain unchanged. The random value must remain valid for a maximum of 30 days. The CPS may specify a shorter validity time for random values. In that case the regulations of the CPS apply.

The CA may issue other FQDNs that end with all the labels of the previous validated FQDN using this method. This method is also suitable for validating Wildcard Domain Names.

3.2.2.4.15 Phone Contact with Domain Contact

The CA must confirm the applicant's control over the FQDN. This may be verified by calling the domain contact's phone number to obtain a confirming response to validate the authorization domain name (ADN). Each phone call may confirm control of multiple ADNs provided that the same domain contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

If someone else than a domain contact answers the call, the CA may request to be transferred to the domain contact. If the CA reaches voicemail she may leave a message with the random value and the ADN(s) being validated. The random value must be returned to the CA to approve the request.

The random value must remain valid for a maximum of 30 days. The CPS may specify a shorter validity time for random values. In that case the regulations of the CPS apply.

The CA may issue other FQDNs that end with all the labels of the previous validated FQDN using this method. This method is also suitable for validating Wildcard Domain Names.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

The CA must confirm the applicant's control over the FQDN. This may be verified by calling the DNS TXT record phone contact's phone number and obtain a confirming response to validate the authorized domain name (ADN). Each phone call may confirm control of multiple ADNs provided that the same DNS TXT record phone contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

The CA may not knowingly be transferred or request to be transferred as this phone number has been specifically listed for the purposes of domain validation.

In the event of reaching voicemail, the CA may leave the random value and the ADN(s) being validated. The random value MUST be returned to the CA to approve the request.

The random value must remain valid for a maximum of 30 days. The CPS may specify a shorter validity time for random values. In that case the regulations of the CPS apply.

The CA may issue other FQDNs that end with all the labels of the previous validated FQDN using this method. This method is also suitable for validating Wildcard Domain Names.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

The CA MUST confirm the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone and obtain a confirming response to validate the Authorization Domain Name (ADN). In each phone CALL multiple ADNs MAY be confirmed, provided that the same DNS CAA Phone Contact is being responsible and listed for each ADN being verified. A confirming response must be provided for each ADN.

For the confirmation the relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 6844, Section 4. The amendment of Errata 5065 has to be considered.

The responsibility for the CA MUST NOT be transferred to another phone number, as the one listed as a contact, has been listed specifically for the purpose of domain validation.

If the call is forwarded to voicemail, the CA MAY leave a random value as well as the ADNs which SHALL be validated. The random value MUST be named in the reply of the phone contact to the CA to approve the request.

The random value must remain valid for a maximum of 30 days. The CPS may specify a shorter validity time for random values. In that case the regulations of the CPS apply.

The CA may issue other FQDNs that end with all the labels of the previous validated FQDN using this method. This method is also suitable for validating Wildcard Domain Names.

3.2.2.5 Authentication for an IP Address

For each IP address listed in a certificate, the CA must confirm that the applicant has control over the IP address on the date the certificate is issued. Therefore, the CA must execute a validation process based on at least one of the methods mentioned in the following sub sections.

After a successful validation of an applicant's authority it may be used for the issuance of multiple certificates. This does not apply endlessly. The validation must have been initiated within the time period specified in the relevant requirement (see also 4.2.1) prior to a certificate issuance.

Starting the 01st of August 2019 the CA must record a table for documenting which method for IP address validation has been used for a request to validate each IP address as well as the matching baseline requirements version number.

It may be considered that IP addresses verified in accordance with this section may be listed in subscriber certificates as defined in section 7.1.4.2 or in subordinate CA certificates via IPAddress in permittedSubtrees within the name constraints extension. CAs are not required to verify IP addresses listed in subordinate CA certificates via IPAddress in excludedSubtrees in the Name Constraints extension prior to inclusion in the Subordinate CA certificate.

3.2.2.5.1 Agreed-upon Change to Website

One method for validating the authority over an IP address is the execution of an agreed-upon change to a corresponding website.

The CA confirms the applicants control over the requested IP address by confirming a request token or random value contained in the content of a file or webpage. This token or value needs

to be integrated in the form of a meta tag under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of validating control of IP addresses, on the IP address that is accessible by the CA via HTTP/HTTPS over an authorized port.

During this process the request token or random value must not appear in the request.

For the random value the CA must implement a process for guaranteeing that the random value is not used multiple times for different purposes. The CA must also provide a random value unique to the certificate request. This random value has a maximum lifetime of 30 days or may no longer be used if the applicant already submitted the certificate request. In case of the already submitted certificate request the timeframe permitted for reuse of validated information relevant to the certificate (see also 4.2.1) must be considered.

3.2.2.5.2 Email, Fax, SMS, or Postal Mail to IP Address Contact

A second option for validating the authority over an IP address is the exchange of a random value via email, fax, SMS or postal mail between CA and applicant. The CA must send the random value to an email address, fax/SMS number, or postal mail address identified as the IP address contact. This may be more than one recipient as long as the IP address registration authority identifies them as an IP address contact for every requested IP address. The applicant sends the response utilizing the random value. Each email, fax, SMS, or postal mail may confirm control of multiple IP Addresses. The random value must be unique in each email, fax, SMS, or postal mail.

The CA may resend the email, fax, SMS, or postal mail in its entirety, including the random value, in case the entire content and recipients are unchanged.

The random value must remain valid for a maximum of 30 days. The CPS may specify a shorter validity time for random values. In that case the regulations of the CPS apply.

3.2.2.5.3 Reverse Address Lookup

In the third option for validating the IP address authority, the CA uses a reverse address lookup procedure. The applicants control over the IP address must be confirmed by obtaining a domain name associated with the IP address through a reverse-IP lookup. The next step is the verification of the control over the FQDN using an additional method permitted in 3.2.2.4.

3.2.2.5.4 Any Other Method

The CA may use other methods, variations or combinations of the methods proposed in this section 3.2.2.5, provided that the CA maintains documented evidence that the method of confirmation establishes that the applicant has control over the IP Address to at least the same level of assurance as the methods previously described in older version of this CP.

This method will be invalid after July 31st, 2019. Completed validations using this method are not be re-used for a new certificate issuance after this date. Any certificates created before or on the 31st have a regular lifetime until they expire.

3.2.2.5.5 Phone Contact with IP Address Contact

In the fifth option for validating the IP address authority, the CA incorporates the phone contact with the IP address contact. The applicant's control over the IP address must be confirmed by calling the IP address contact's phone number to obtain a response confirming the applicant's request for validation of the IP address. The specific phone contact must be obtained from the IP address registration authority. This way each phone call must be made to one single number. If the CA does not reach the IP address contact, the CA may request a transfer to the

correct IP address contact. If the CA just reaches voicemail, it may leave a message containing a random value and the IP addresses being validated. In case there is a call back, the random value must be named to the CA.

The random value must remain valid for a maximum of 30 days. The CPS may specify a shorter validity time for random values. In that case the regulations of the CPS apply.

3.2.2.5.6 ACME “http-01” method for IP Addresses

A sixth method for confirming the applicant's control over the IP address may the procedure documented for an “http-01” challenge in draft 04 of “ACME IP Identifier Validation Extension,” available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4.

3.2.2.5.7 ACME “tls-alpn-01” method for IP Addresses

A seventh method of confirming the applicant's control over the IP address may use the procedure documented for a “tls-alpn-01” challenge in draft 04 of “ACME IP Identifier Validation Extension,” available at https://tools.ietf.org/html/draft-ietf-acme-ip-04#section-4.

3.2.2.6 Wildcard Domain Validation

The wildcard character (*, asterisk) is only accepted in the left label of the CN or "subjectAltName." More than one wildcard character (e.g. *.*.example.com) per CN or "subjectAltName" is not accepted.

If a wildcard character appears in a label immediately to the left of a "registry-controlled" or "public suffix", the issuance MUST be rejected (e.g., "*.co.uk" or "*.de"), unless the customer can prove that he has legal control over the entire domain namespace.

The use of wildcard characters is not permitted for EV certificates.

3.2.2.7 Data Source Accuracy

Before using a data source as a permitted data source, the source MUST be assessed for its reliability, accuracy, and protection against tampering or forgery. The following must be taken into account:

1. The age of the information provided
2. The frequency of updates to the information source
3. The data provider and the purpose of data collection
4. The availability of data
5. The integrity of the data

Databases maintained by the CA, its owner, or its affiliates are not considered a reliable data source if the primary purpose of the database is to collect information to meet the validation requirements under this Section 3.2.

3.2.2.8 CAA Records

When issuing certificates, the certification authority must check the CAA records for each dNS name in the subjectAltName field as described in RFC 6844 (Errata 5065). This includes the processing of issue, issuewild, and iodef property tags as specified in RFC 6844 (if applicable).

The CA must respect a critical flag and must not issue a certificate in case an unknown property is set with this flag. CAs may treat a non-empty CAA resource record set that does not contain any issue property tags (or issuewild property tags in case of Wildcard Domain Name) as

permission to issue, provided that no records in the CAA resource record set otherwise prohibit issuance.

The CAA records check can be omitted for certificates

- for which a certificate transparency (CT) pre-certificate has already been issued, which is stored in at least two CT log servers
- issued by a technically limited sub-CA in accordance with Section 7.1.5
- requested by an affiliate of the issuing CA

CAs must document potential issuances that were prevented by a CAA record in sufficient detail in case of reporting.

3.2.3 Authentication of Individual Identity

When certificates are issued to natural persons, appropriate procedures must be used to verify their identity, e.g.:

- German ID card
- Passport with official certificate of residence

3.2.3.1 Low Validation Level

No stipulation.

3.2.3.2 Medium Validation Level

The following validation procedures must be carried out to identify a natural person who requests services with a medium validation level:

- Ascertaining that the natural person exists based on identification features that can be verified

In order to verify such identification features, the CA or RA MAY access an identity verification service recognized by Telekom Security, an identity verification database, or the passport documents issued by a public body or authority.

3.2.3.3 High Validation Level

The following validation procedures must be carried out to identify a natural person who requests services with a high validation level:

- The requirements for the medium validation level must be met
- Personal appointment at a CA or RA with an officially issued passport document with photo

3.2.4 Non-verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

The authorization of a natural person as being entitled to act on behalf of an organization, or a natural person must take place in accordance with an adequate procedure.

3.2.6 Criteria for Interoperation or Certification

All cross-certificates that were issued by a CA must be published.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

To renew a certificate from a subordinate certification authority (sub-CA), the "Initial identity validation" (see Section 3.2) must be carried out.

3.3.2 Identification and Authentication for Re-key after Revocation

It is not possible to renew the key of a revoked certificate.

3.4 Identification and Authentication for Revocation Request

The revocation of a certificate can only be requested by persons and institutions authorized to revoke certificates.

The revocation must be authenticated in a suitable way. We recommend using a revocation password that is defined as part of the certificate application or delivery and is securely transmitted to the subscriber.

The telephone numbers, fax numbers, websites, or addresses to be used for the revocation must be published.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

This section deals with operational requirements in the life cycle of certificates.

4.1 Certificate Application

The subsections define requirements for the certificate application process. The certificate application process usually takes place in the registration authority.

4.1.1 Who can submit a Certificate Application

The root CAs or the CAs to be included must describe their request process including key generation, request processing in the RA, and forwarding to the CA in the CPS. Furthermore, the customer must be obliged to provide up-to-date and correct information in the application process.

A sub-CA must operate an internal database that contains all previous revoked certificates or certificate application operations that have been rejected for security reasons. This database is to be used in the application process to prevent misuse.

4.1.2 Enrollment Process and Responsibilities

Before a certificate can be generated, the following activities must be completed in the registration process as a minimum:

- Conclusion of the contract or CA-internal agreement
- Submission of the certificate application using the mechanisms prescribed by the certification authority (e.g., signed online order in the PKCS#10 format) and its syntactic/semantic audit
- Possibly presentation of additional authorization and identification documents by the customer in accordance with the validation level for organizations or natural persons
- Evidence of ownership of the private key in accordance with Section 3.2.1
- Fully positive verification of the order data by the processor, usually the registration authority
- Archiving of the order data
- Authorization by the management

The certificate application must receive confirmation that the data in the certificate application is true. This confirmation must be issued by the customer himself or by an authorized representative.

The root CA must receive a certificate application and the consent to the contractual agreements or instructions for use, or equivalent contractual documents, from the applicant before a certificate can be generated.

4.2 Certificate Application Processing

This section deals with the requirements for processing a certificate application.

4.2.1 Performing Identification and Authentication Functions

The applicant must provide all information required for certificate creation and/or required in this CP. If not all the information is included, the root CA must request this information from the applicant or obtain and use the data from a trusted and independent data source following confirmation by the applicant.

Only data created up to 825 days before the certificate is issued may be used for the validation of applications. No previous applications are used for order processing.

4.2.2 Approval or Rejection of Certificate Applications

A certificate application must be rejected if not all the requirements of the previous sections have been met. The applicant must be informed of the reasons for rejection.

CAs MUST NOT issue certificates that contain internal names, see section 7.1.4.2

4.2.3 Time to Process Certificate Applications

The CPS should make a statement about the expected processing time if no processing time is specified in the contract.

4.3 Certificate Issuance

If this is successful, the certificate will be generated.

4.3.1 CA Actions during Certificate Issuance

All activities during the issuance of root and sub-CA certificates must be subject to pre-defined procedures (key ceremony) and logged. For root CA certificates, witnesses (e.g., external auditor) must observe the ceremony.

4.3.2 Notification (to subscriber) of Certificate Issuance

The CA must inform the applicant after the certificate has been issued.

4.4 Certificate Acceptance

The applicant accepts the generated certificate. In the case of certificates of a root CA or sub-CA an explicit declaration of acceptance should be made.

4.4.1 Conduct constituting certificate acceptance

The CA should request confirmation of acceptance from the applicant within a specified period. The type of acceptance must be set out in the CPS.

4.4.2 Publication of the certificate by the CA

The certificates generated by the root CA must be published. This must be done via publicly accessible media, e.g., website.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

Certificates issued as part of this CP are issued for certification authorities only.

4.5.1 Subscriber private key and certificate usage

The CA must define regulations for the storage and use of the private key and the certificate by the subscriber. Certificates may only be used in a certification authority. The subscriber must be informed in particular of any consequences of misconduct (e.g., immediate revocation).

4.5.2 Relying party public key and certificate usage

The CA must create regulations and notes on the use of certificates and public keys for potential users (e.g., software manufacturers) and make them publicly accessible.

4.6 Certificate renewal

Certificates certified by the root CA should not be renewed.

4.6.1 Circumstance for certificate renewal

The regulations and deadlines for the initial application must be observed; this applies in particular to the topicality of the available validations. Furthermore, the regulations of the version of this CP valid at the time of processing must be taken into account.

Certificates must not be renewed for compromised keys.

4.6.2 Who may request renewal

It must be ensured that the certificate renewal can only be requested by an authorized person.

4.6.3 Processing certificate renewal requests

The certificate renewal MUST take place within a specific period; this must be specified in the CPS.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

The regulations in Section 4.4 apply.

4.6.6 Publication of the renewal certificate by the CA

The regulations in Section 4.4.2 apply.

4.6.7 Notification of certificate issuance by the CA to other entities

The regulations in Section 4.4.3 apply.

4.7 Certificate Re-key

With a re-key, a new key pair is used for an existing certificate. All requirements must be met and the respective regulations described in the CPS.

4.7.1 Circumstance for certificate re-key

The regulations and deadlines for the initial application must be observed, this applies in particular to the topicality of the available validations. Furthermore, the regulations of the version of this CP valid at the time of processing must be taken into account.

4.7.2 Who may request certification of a new public key

It must be ensured that the re-key can only be requested by an authorized person.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Section 4.4 applies.

4.7.6 Publication of the re-keyed certificate by the CA

The regulations in Section 4.4.2 apply.

4.7.7 Notification of certificate issuance by the CA to other entities

The regulations in Section 4.4.3 apply.

4.8 Certificate modification

If certificate data changes during the certificate validation period, checks must be carried out to establish whether the certificate still meets the requirements or whether the applicant still holds all authorizations and usage rights. If not, the certificate must be revoked.

In this case, a new certificate application must be submitted with updated data.

When adjusting data, the same rules apply as to certificate renewal.

4.8.1 Circumstance for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

The revocation of certificates, which have been issued on Root CA level, are especially critical and the revocation process MUST include the accredited certification authority.

The rules for revoking certificates must be described in the CPS. Root CA and Sub-CA certificates may not be suspended.

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

A CA MUST revoke a Subscriber Certificate within 24 hours if at least one of the following reasons exists:

1. The Subscriber/authorized representative requests in writing that the Sub-CA SHALL revoke the certificate.
2. The Subscriber/authorized representative notifies the Sub-CA that the original certificate request was not authorized and does not retroactively grant authorization.
3. The Sub-CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise.
4. The Sub-CA obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name (FQDN) or IP address in the Certificate should not be relied upon.

A CA MUST revoke a certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6 of the baseline requirements.
2. The Sub-CA has evidence that the certificate has been misused.
3. The Sub-CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use.
4. The Sub-CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the certificate is no longer legally permitted.
5. The Sub-CA is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;

6. The Sub-CA is made aware of a material change in the information contained in the certificate.
7. The Sub-CA is made aware that the certificate was not issued in accordance with the requirements of the CA-Browserforum or the CA's CP or CPS.
8. The Sub-CA determines or is made aware that any of the information appearing in the certificate is inaccurate or misleading.
9. The Sub-CA's right to issue certificates conform to the baseline requirements ceases operations or is being cancelled for any reason, unless the CA has made arrangements to continue maintaining the CRL/OCSP repository;
10. Revocation is required by the Sub-CA's Certificate Policy and/or Certification Practice Statement
11. The Sub-CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the certificates or the CA is made aware that there is a method by which the private key corresponding to a public key can be easily calculated.

A CA MUST revoke S/MIME certificates, if one or more of the following occurs:

1. The certificate owner notifies the Sub-CA that the original certificate request was not authorized and does not retroactively grant authorization.
2. The Sub-CA receives notification that the private key of the certificate owner has been compromised.
3. The Sub-CA receives the confirmation that the certificate has been misused.
4. The Sub-CA receives information that the certificate owner violated one or more essential stipulations of the contract.
5. The Sub-CA receives information that the e-mail address used in the certificate may no longer be used legally.
6. The Sub-CA receives information that central information inside the certificate have been changed.
7. The Sub-CA is made aware that the certificate was not issued in accordance with the requirements of the CA's CP or CPS.
8. The Sub-CA detects or is informed that central information contained inside the certificate are no longer correct.
9. The Sub-CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate
10. The Sub-CA has suspicions that the own private key has been compromised
11. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.
12. The certificate has not been issued conform to the Mozilla Root Store Policy which has been valid at the time of issuance.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

An Issuing CA SHALL revoke a Subordinate CA certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;

3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6,
4. The Issuing CA obtains evidence that the certificate was misused;
5. The Issuing CA is made aware that the certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. The Issuing CA determines that any of the information appearing in the certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate
8. The Issuing CA's or Subordinate CA's right to issue certificates under the requirements of the CA-Browserforum expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. The Issuing CA has the suspicion that its own private key has been compromised
10. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.
11. There are legal regulations or adjudications or instructions of a supervisory authority.

4.9.2 Who can request Revocation

The following persons and institutions MUST be able to initiate a revocation:

- The subscriber or another authorized person
- The certification authority for the reasons set out in the previous section

If a third party reports a defect or deviation from the above standards, the root CA must initiate a revocation after checking the facts of the case.

4.9.3 Procedure for Revocation Request

The root CAs must arrange for revocation for the persons named in 4.9.2 via common communication channels. To be able to issue a revocation request, the root CAs must be provided with at least one communication channel that is available on a 24/7 basis.

The necessary information must be online available, and the revocation process must be described in detail in the CPS. CAs must provide understandable instructions on how to identify certificate misuse, key compromise, fraud, or similar issues and must describe the process for the target group in section 1.5.2 of the CPS.

4.9.4 Revocation Request Grace Period

No stipulation.

4.9.5 Time within which CA Must Process the Revocation Request

Within 24 hours after receiving a Certificate Problem Report, the CA SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, the CA SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related

notice to published revocation MUST NOT exceed the time frame set forth in Section 4.9.1. The date selected by the CA SHOULD consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
5. Relevant legislation.

In case of a revocation executed by an Intermediate CA, an incident report must be generated and provided for the Root-CA. The Root-CA checks this report.

4.9.6 Revocation Checking Requirement for Relying Parties

Revocation information must be provided in a standardized form, such as AR or OCSP, so that checks can be performed with standard-compliant applications.

The mechanisms used must be described in the CPS.

4.9.7 CRL Issuance Frequency

The revocation information of the root CA MUST be updated after a revocation or at least every 6 months and made publicly available. Cross-certificates must be updated every 31 days.

A CRL entry MUST not be removed until it is part of a regular planned CRL, which has been issued after the regular certificate validity time of the revoked certificate.

4.9.8 Maximum Latency for CRLs

The ARL revocation list must be published before the "next update" entry.

4.9.9 On-line Revocation/Status Checking Availability

Revocation information must be provided online for the certificate users based on a procedure that complies with the standard. All CA certificates revoked by this certification authority must be included.

Both the revocations lists and OSCP must be provided on a 24/7 basis.

OCSP responses MUST be conform to the RFC 6960 requirements.

4.9.10 On-line Revocation Checking Requirements

The root CA must support the OCSP request with the GET method as detailed in RFC 6960 and/or RFC 5019. The root CA MUST update the OCSP database at least every twelve (12) months or within twenty-four (24) hours of a revocation.

When issuing Subscriber certificates, the CA MUST update OCSP information at least every four (4) days. OCSP responses MUST have a maximum expiration time of ten (10) days.

The OCSP responder should not return a "good" status for a certificate that has not been issued by the CA or which has a certificate number in status "unused". The OCSP responder should be monitored for such requests.

The OCSP-responder MAY answer to requests about certificate serial numbers with a state “reserved”, similar as if there was a corresponding certificate for a pre-certificate. The certificate states of “assigned”, “reserved” and “unused” must be used according to the requirements of [RFC 6962].

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

If a private key is compromised, the corresponding certificate MUST be revoked within 24 hours after this becomes known and the key may no longer be used.

4.9.13 Circumstances for Suspension

A CA certificate may NOT be suspended.

4.9.14 Who can request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate status services

An OCSP service MAY be provided for CA certificates. An ARL revocation list must be provided.

4.10.1 Operational Characteristics

Entries in the ARL may only be removed once the certificate has exceeded its expiry date and is part of a revocation list which has been issued after the expiry date of the certificate.

4.10.2 Service Availability

The status information service must be provided on a 24/7 basis. Sufficient capacities must be provided so that the response time does not exceed 10 seconds under normal operating conditions.

4.10.3 Optional Features

No stipulation.

4.11 End of subscription

In the event of termination of the contract or termination of the internal agreement by the customer, the certificate must be revoked.

4.12Key escrow and recovery

Key escrow and recovery may only be carried out with the express permission of the subscriber.

4.12.1 Key escrow and recovery policy and practices

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

The included CAs must each develop, implement, and maintain a comprehensive security plan that meets the following requirements:

- Protection of the confidentiality, integrity, and availability of certificate data and the certificate management process
- Protection against potential threats and risks to the confidentiality, integrity, and availability of certificate data and the certificate management process.
- Protection against unauthorized or unjustified access, use, publication, replacement, or destruction of certificate data or the certificate management process
- Protection against accidental loss or destruction of, or damage to certificate data or the certificate management process.
- Maintaining compliance with statutory security requirements (e.g., Trust Services Act (Vertrauensdienstegesetz))

The security plan must contain administrative, organizational, technical, and infrastructural measures that are appropriate for the sensitivity of the certificate data and the certificate management process. The security plan must take into account the current state of technology, the costs of certain measures, and an appropriate level of security for the damage that could occur, and the protection needs of the data that is to be protected.

The security plan must include an annual risk analysis that identifies the foreseeable internal and external threats that could lead to unauthorized access, publication, misuse, replacement, or destruction of certificate data or the certificate management process. The risk analysis must examine the probabilities and potential damage of these threats. Furthermore, the sensitivity of the certificate data and the certificate management process must be considered.

The security plan should consider tools and products that support the achievement of an appropriate level of security.

The certificate management process must consider the security plan and contain the following subjects:

- Physical security and environmental measures
- System integrity measures, configuration management, maintaining the integrity of trusted code, malware detection, and preventive measures
- Network security and firewall management that includes port restrictions and IP address filtering.
- User management, own assignment of trusted roles, training, raising awareness, and further training
- Logical access control, activity logging, and inactivity time-outs to enable personal accountability.

5.1 Physical security controls

The included CAs must describe the infrastructural measures that are implemented by the CA.

5.1.1 Site location and construction

The included CAs must describe the locations and the technical and structural measures, in particular for high-security zones of the CA operation.

5.1.2 Physical access

The physical access control of the CA is to be described. The following requirements SHOULD be considered:

- Only physical access authorizations that are operationally necessary should be granted
- This authorization should be limited in time and checked on a regular basis
- Physical access for guests should only be granted in exceptional cases and after the need for such access has been checked.
- Authorization may not be granted by one employee alone.
- The allocation of authorizations and any physical access must be logged.

5.1.3 Power and air conditioning

The power supply and air conditioning measures, which ensure a state-of-the-art provision in accordance with the required availability, must be described.

5.1.4 Water exposures

The measures taken to protect against water damage must be described. If the property is situated close to any body of water or in low-lying areas, the flood risk MUST be assessed, and measures taken if necessary.

5.1.5 Fire prevention and protection

It MUST be described how the CA systems are protected against fire hazards, i.e., what fire protection measures are implemented to maintain high availability.

Early fire detection systems (suction systems) must be installed in all system and system operator rooms, archives, UPS rooms, and other selected rooms. The supply and exhaust air of the air conditioning units in the individual rooms is monitored. Fire alarms must be installed in the other rooms.

5.1.6 Media storage

Data carriers with critical operating data must be stored securely and protected from environmental influences. The measures must be described.

5.1.7 Waste disposal

Documents and data carriers must be disposed of in such a way that the relevant confidentiality level of the data is guaranteed at all times. Disposal has to be protocolled.

5.1.8 Off-site backup

Backup copies of critical data must be made and stored in a different location than the original data or in a different fire protection zone.

5.2 Procedural controls

5.2.1 Trusted roles

All roles that can perform critical functions within the CA and restrict the trustworthiness of the CA are called trusted roles. These are primarily the following groups of system administrators, RA-employees, CA operators or internal auditors.

These roles must be mapped in the CPS. These roles may only be filled by suitable and trusted persons. The appointment may only be made with the approval of the senior management and must be reviewed regularly at least every three (3) years.

5.2.2 Number of Individuals Required per Task

Critical tasks, in particular working with the private key of the CA, must be performed by persons in a trusted role and in accordance with the dual control principle.

5.2.3 Identification and Authentication for Trusted Roles

Employees who assume trusted roles must be identified and security-cleared in accordance with 5.3.2.

Each role owner of a trusted role must authenticate himself before his activity. It must be ensured that the role owner can be identified reliably.

5.2.4 Roles Requiring Separation of Duties

A separation of tasks MUST be guaranteed for the following role groups: RA officer, CA operator, CA administrator, and internal auditor. A person may only take over tasks within these areas.

5.3 Personnel controls

5.3.1 Qualifications, Experience, and Clearance Requirements

All persons in the certificate administration must be trustworthy and have the necessary expertise and experience. These criteria must be checked. This check must have been completed with a positive result before activities are performed in a trusted role. If the check is not completed, an activity may take place while monitoring by another employee in a trusted role in exceptional cases.

5.3.2 Background Check Procedures

Persons who are to assume a trusted role must hold a certificate of good conduct in accordance with § 30 of the German Federal Central Criminal Register Act (Bundeszentralregistergesetz – BZRG) or similar. If entries prevent the assumption of the role, the assumption of the role must be refused. The CA may carry out further checks. The certificate of good conduct or similar should be re-verified every three years.

5.3.3 Training Requirements and Procedures

Personnel must be trained before taking on such activities. This training must at least cover the following topics: basic knowledge of public key infrastructures, PKI requirements, e.g., CAB forum, certificate policy, and/or certification practice statement. Additional topics are common

options for tampering with documents and the verification process and threats from phishing and social engineering.

5.3.4 Retraining Frequency and Requirements

Personnel must be retrained regularly; individuals with trusted roles, in particular, must be kept up to date as regards the relevant level of knowledge that is currently defined for them. In the event of changes, follow-up training should be carried out within 3 months.

5.3.5 Job Rotation Frequency and Sequence

It must be ensured that due to a job change no role exclusion can be bypassed (see Section 5.2.4). This has to be considered in the security plan.

5.3.6 Sanctions for Unauthorized Actions

Unauthorized actions must be logged and sanctioned and, depending on the severity of the action, the person must be excluded from the CA operation.

5.3.7 Independent Contractor Controls

The same requirements as those described for employees must apply to and be implemented for external personnel. This also applies to the regulations for the storage period of documents and the requirements for event logging.

5.3.8 Documentation Supplied to Personnel

The role owners must be provided with sufficient documentation to carry out their activities.

5.4 Audit logging procedures

5.4.1 Types of Events Recorded

All log entries must contain at least the date and time of the entry, a reference to the person or system that generated the entry, and a description of the event.

CA key pairs and CA systems

At least the following events must be logged for life-cycle management for CA key pairs or CA systems:

a. Generation, deletion, storage, backup, recovery, and archiving of the key pair or parts of the key pair
b. Events in the life-cycle management of cryptographic devices (e.g., HSM) and the CA software used

EE and CA certificates

At least the following events must be logged for life-cycle management for EE and CA certificates:

- Initial request and revocation of certificates
- Request for renewal with and without a change of key (renewal and re-key)
- All activities relating to the verification of information
- The event, as well as the date/time and phone number of phone calls relating to the verification and the name of the contact person

- Acceptance or rejection of certificate applications
- Issue of a certificate
- Generation of revocation lists and OCSP entries

Other security-related events

In addition, all security-relevant events for operation of the infrastructure must be logged. This includes at least the following events:

- Successful and unsuccessful attempts to access the PKI systems
- Actions performed on and by PKI systems and other systems that are relevant for security
- Changes to the security profile
- System crashes, hardware failures, and other anomalies
- Firewall and router activities
- Entering and exiting of Trust Center facilities

This documentation duty MUST also be observed for the processing of certificate applications by third parties for the third party.

All log data must be made available to the authorized internal and external auditors on request in order to be able to check compliance with the requirements mentioned.

5.4.2 Frequency of Processing and Archiving Audit Logs

The log data must be analyzed and archived regularly, at least every six months.

5.4.3 Retention Period for Audit Log

The log data must be kept for at least seven years. The log data must be made available to an internal or external auditor on request.

5.4.4 Protection of Audit Log

Audit log data must be stored, and their integrity has to be protected. The CA has to secure that audit log data is not being deleted.

5.4.5 Audit Log Backup Procedures

A backup of audit logs and logging data MUST be prepared daily and stored on a different site.

5.4.6 Audit Log Accumulation System (internal vs. external)

If automatic audit logging is used, the CA MUST ensure integrity at all times. In the event of system malfunctions, operation should be suspended until the issue has been resolved.

5.4.7 Notification to Event-Causing Subject

If a person triggers an audit event, the person MAY be informed about the triggering, depending on the type.

5.4.8 Vulnerability Assessments

The CA MUST regularly and at least quarterly check its systems for current vulnerabilities.

The security plan MUST include an annual risk analysis that identifies the foreseeable internal and external threats that could lead to unauthorized access, publication, misuse, replacement,

or destruction of certificate data or the certificate management process. The risk analysis must examine the probabilities and potential damage of these threats. Furthermore, the sensitivity of the certificate data and the certificate management process must be considered.

The risk analysis must verify that policies, procedures, information processing systems, technology, and other compilations used by the CA are sufficient to effectively address the threats.

5.5 Records archival

5.5.1 Types of Records Archived

The CA must archive the following data as a minimum:

- CPS, CP, GT&C, and contractual documents
- Certification documents and audit reports
- System configurations
- Application documents including validations.
- Issued certificates
- Revocation requests
- Security plan
- Security incidents
- Audit and event log data

5.5.2 Retention Period for Archive

All records mentioned in 5.5.1 must be available for seven (7) years. The retention period must adhere to stipulations made by law or legal regulations.

5.5.3 Protection of Archive

The CA MUST ensure that only authorized and trusted persons are given access to archives.

5.5.4 Archive Backup Procedures

Archive data must be protected against unauthorized read access, changes, deletions, or other forms of manipulation. The durability of the media and the data formats used MUST be ensured.

5.5.5 Requirements for Time-stamping of Records

All events that are recorded (mentioned in 5.5.1) must contain date and time.

5.5.6 Archive Collection System (internal or external)

Telekom Security only uses internal archiving systems or third-party archiving services which are certified for this task.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized and trusted personnel receive access to archives and archive data. The integrity of archive data must be protected and will be checked during access. This will be recorded in a log.

5.6 Key changeover

The CAs must explain how the CA key is changed and the new key reaches the user.

5.7 Compromise and disaster recovery

The included CAs must have comprehensive regulations for the continuation of business in the event of a breakdown or failure of the service. The plan must be reviewed and tested annually.

5.7.1 Incident and Compromise Handling Procedures

The business continuity plan must cover the following aspects:

1. The conditions for initiating the measures described
2. The emergency processes
3. The fallback processes
4. Recovery plans
5. Review information for planning
6. Sensitization and knowledge requirements
7. Personal responsibilities of the parties involved
8. Specifications for recover times
9. Regular testing of possible scenarios
10. A schedule for restoring or resuming business after a fault or failure
11. A requirement for storing critical cryptographic material (e.g., HSM) at a different location
12. Determination of acceptable times for system failure and recovery.
13. Determination of backup cycles for essential business information and software
14. The removal of recovery locations and the CA's main location
15. Planning documents for safeguarding business premises during a disaster and for recovery at that site or at another site

The CA must test, review, and – if necessary – revise these processes annually.

The CA does not necessarily need to disclose the business continuation measures; this information only needs to be provided to the authorized auditors on request.

5.7.2 Recovery Procedures if Computing Resources, Software, and/or Data Are Corrupted

If the IT components, software, and/or data are damaged, the incident MUST be immediately investigated and reported.

5.7.3 Recovery Procedures After Key Compromise

If it becomes known that the private key of a CA is compromised, the incident MUST be immediately investigated and assessed, and the necessary steps taken.

Subscriber MUST be informed if compromise occurred via public Websites.

If necessary, the affected certificate(s) must be immediately revoked and the corresponding certification authority must generate and publish revocation lists (ARL, CRL).

5.7.4 Business Continuity Capabilities after a Disaster

The CA must develop, implement, and test an emergency plan for data center operation in order to alleviate the effects of disasters of all kinds (natural disasters or disasters of human origin) and restore the availability of critical business processes as quickly as possible. This MUST cover all CA processes, components, systems, and services. This plan MUST be reviewed, tested, and updated accordingly on a regular basis and at least once a year so as to be able to respond in a targeted and structured manner in the event of a disaster.

The emergency plan MUST contain at least the following information:

- The necessary criteria for activating the plan
- Possible emergency measures (depending on the situation)
- Fallback procedures
- Restart procedure
- Procedure for regular maintenance, updating, and further development
- Awareness-raising measures
- Training requirements for the affected personnel
- The responsibilities of the individuals (role description and assignment)
- Recovery time objective (RTO)
- Regular execution of the emergency plans for test purposes
- A procedure for maintenance or timely restoration of business activities following an interruption or failure of critical business processes
- An obligation to back up or keep critical cryptographic devices and information at a different location
- Specification of the maximum tolerable downtime (MTD) and corresponding restoration times
- Frequency at which backups are created of critical business information and the software used including its configuration
- Physical distance between the backup locations or facilities and the main office or the Trust Center data center
- Procedure for securing the business premises and facilities as well as possible following a disaster (emergency operation) until secured normal operation in line with the requirements is restored

The internal and external auditor must be able to inspect the emergency plan on request.

5.8 CR or RA termination

The included CAs must describe appropriate measures upon termination of operation, i.e., discontinuation of the service. This includes in particular the notification of the cessation of operations and the safekeeping of the corresponding documents of the CA and the repository.

6 TECHNICAL SECURITY CONTROLS

Certification authorities that are in the hierarchy of the included root CA certificates must implement regulations like the ones described below in an adequate manner and describe them in their CPS.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Root CA key pairs should be generated in accordance with a generation script, and this process should be accompanied by a qualified auditor. The process MUST follow a key generation ceremony.

CA keys must be generated in a hardware security module that complies with "FIPS 140-2 level 3" or "Common Criteria EAL 4." During key generation, the implementation of the role concept and thus the dual-control principle are enforced. The generation of CA keys is documented in accordance with [EN 319 411].

6.1.1.2 RA Key Pair Generation

No stipulation.

6.1.1.3 Subscriber Key Pair Generation

When generating EE keys, the subscriber is obliged to generate them in a cryptographically secure manner in accordance with the specifications in [EN 319 411-1].

6.1.2 Private Key Delivery to Subscriber

The generated keys are to be handed over securely to the customer via CD, integrity-protected data container, or signed and encrypted e-mail.

Private keys may only be archived by the subscriber.

If the CA becomes aware that the subscriber's private key has been transferred to an unauthorized person or non-affiliated organization, the CA revokes all certificates that contain the public key that corresponds to the transferred private key.

6.1.3 Private Key Delivery to Certificate Issuer

The delivery of the public key to the certification authority must be described in the CPS of the respective certification authority. The public key is usually to be delivered securely in the form of a signed certificate request.

6.1.4 CA Public Key Delivery to Relying Parties

Delivery can be made as an attachment to the certificate. It can be made available by publishing it on a web page or in an LDAP directory.

The specific delivery/provision of the public key to the issuing certification authority must be described in the CPS of the respective certification authority.

6.1.5 Algorithm type and key sizes

6.1.5.1 Root CA Certificates

The key size of the root CA certificates MUST be at least 2048 bits when using an RSA key and 256 bits when using an ECC key. Allowed are ECC curves with NIST P-256, P-384 or P-521.

The used hash-algorithm MUST be either SHA-256, SHA-384 or SHA-512.

When using DSA the min. DSA modulus and divisor sizes MUST be L=2048 and N=224 or L=2048 and N=256 bits.

6.1.5.2 Subordinate CA Certificates

The key size of sub-CA certificates MUST be at least 2048 bits for RSA keys and 256 bits for ECC keys. The Hash algorithm MUST be at least SHA-256 bits.

When using DSA, L=2048 and N=224 MUST at least be applied, see also FIPS 186-4.

6.1.5.3 Subscriber Certificates

The key size for EE certificates MUST be at least 2048 bits for RSA keys and 256 bits for ECC keys. The Hash algorithm MUST be at least SHA-256 bits.

When using DSA, L=2048 and N=224 MUST at least be applied, see also FIPS 186-4.

6.1.6 Public Key Parameters Generation and Quality Checking

The parameters of the public keys of root CA, sub-CA, and EE certificates and any quality controls to be applied are defined in the CPS documents of the certification authorities.

The provisions of the relevant section of [CAB-BR] must be complied with.

6.1.7 Key Usage Purposes

Private root CA keys may only be used to sign sub-CA certificates, OCSP certificates, and revocation lists.

The private sub-CA keys may be used to sign sub CA certificates, OCSP certificates, EE certificates, and revocation lists.

The EE keys may only be used for the usage types specified in the certificate.

Only the key usages (keyUsage) from Section 7 are to be used.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The private keys of the root CAs must be stored on a security-checked hardware security module (FIPS 140-2/level 3 evaluated).

Technical or other controls relating to the cryptographic modules in accordance with [CAB-BR] and [ETSI] must be observed.

6.2.2 Private key (n out of m) Multi-person Control

The control of private root keys must be defined in detail in the CPS of the respective certification authority. The execution of actions and access must be restricted in such a way that at least two persons with different authorizations are required.

6.2.3 Private Key Escrow

The storage of private keys with trustees outside Telekom Security is not permitted.

6.2.4 Private Key Backup

The backup of public keys and associated security controls must be described in the CPS of the respective certification authority.

The private keys may only be backed up, stored, and restored by persons with trusted roles. The backup may only be performed on cryptographic keystore devices.

6.2.5 Private Key Archival

Once the root CA keys have expired, the requirements of the deletion plan must be implemented.

Sub-CA keys may only be archived by the subscriber.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private keys must be transferred in appropriate security tokens. Private keys must not be available in unencrypted form at any time. The dual-control principle (in accordance with Section 6.2.2) must be documented.

6.2.7 Private Key Storage on Cryptographic Module

Only hardware that fulfills the requirements in accordance with the NIST list and [ETSI] may be used.

The storage of private keys on cryptographic modules must be described, if applicable, in the CPS of the respective certification authority.

6.2.8 Activating Private Keys

Private Root CA Key Activation on Cryptographic Modules

The activation of private keys on cryptographic modules must be described in the CPS of the respective certification authority.

The root CA keys must be activated in a log by multiple persons (two persons with different roles). This requires approved cryptogr. hardware (HSM), the dual-control principle, and the use of shared secrets.

Private Sub-CA Key Activation on Cryptographic Modules

The activation of private keys on cryptographic modules must be described in the CPS of the respective certification authority.

End entity Key Activation on Cryptographic Modules

The keys must be protected in an economically reasonable way by at least one of the following measures:

- Password protection
- protection by suitable hardware
- encryption
- suitable storage

6.2.9 Deactivating Private Keys

Private root CA keys must be deactivated immediately after the end of the actions performed by multiple persons (two persons with different roles). The private root CA keys are deactivated by terminating the connection between HSM and the application. The deactivation must be logged.

6.2.10 Destroying Private Keys

The destruction of root CA keys must be performed and documented by multiple persons (2 persons with different roles). It must be ensured that no fragments or backups of the key remain after destruction which could lead to a reconstruction of the key.

6.2.11 Cryptographic Module Capabilities

Cryptographic modules must be rated based on the Common Criteria Level EAL 4 or FIPS 140-2 level 3.

6.3 Other aspects of Key Pair Management

6.3.1 Public Key Archival

The activation of root CA keys must be performed and documented by multiple persons (2 persons with different roles).

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Root CA keys and root CA certificates are valid for a maximum of 25 years.

Sub-CA keys and sub-CA certificates are valid for a maximum of 25 years.

SSL/TLS certificates are valid for a maximum of 825 days.

User certificates are valid for a maximum of 60 month.

The validity of certificates must not be longer than the validity of the issuing CA certificate.

6.4 Activation data

6.4.1 Activation data generation and installation

The generation of activation data must be performed and documented by multiple persons (2 persons with different roles).

If an EE key pair is generated by the subscriber, the activation secret must also be produced in this process and is therefore available to the subscriber.

6.4.2 Activation data protection

The activation data (secret shares) must be protected in a suitable manner against unauthorized access and inspection:

Storage in appropriate safes, smart cards, or by splitting passwords among several authorized persons.

6.4.3 Other aspects of activation data

Transfer of activation data

Activation data may only be transferred through personal handover.

Destruction of activation data

Activation data must be destroyed when it is no longer required. The destruction must be carried out by suitable measures such as secure deletion, rendering it unidentifiable by shredding, or in specially marked containers for secure disposal of files.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

It must be ensured that the management of CA systems is protected against unauthorized third-party access.

It is mandatory to use protection mechanisms (e.g., firewalls, access protection, two-factor authentication, personalized chipcards, or dual control principle) to protect the CA functions, directory services, and OCSP responder against internal and external intruders.

6.5.2 Computer Security Rating

A computer security assessment must be conducted for each computer security incident, but at least once a year.

6.6 Life cycle Technical Controls

6.6.1 System development controls

All aspects of secure system development must be considered (such as secure development environment or configuration management)

6.6.2 Security management controls

The security management controls must be described in the CPS.

6.6.3 Life cycle security controls

The equipment used must be operated in accordance with the manufacturer's instructions. Before the start of operation, it must be thoroughly checked and may only be used if there is no doubt that it has not been tampered with.

The hardware (for root CAs) must be sealed and the software checked so that any tampering and attempted tampering can be detected.

6.7 Network Security Controls

All necessary network security measures must be taken.

The following network security measures must be implemented:

The networks of the subordinate certification services must be cut off from the Internet by state-of-the-art firewalls. Data traffic must be limited to what is necessary for the functions.

Security-critical components and systems that are accessible from the Internet (e.g., directory service, OCSP responder) must be separated from the Internet and the internal networks by firewalls. All other security-critical components and systems (e.g., CA, DB, Signer) must be operated in a separate network.

6.8 Time-stamping

Date and time information in certificates, revocation lists, online status checks, and other important information must be derived from a reliable time source (see Section 5.5.5).

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

The certificates are structured in accordance with the X.509 standard. The name attributes for both subscribers and issuers are documented in the X.501 standard.

The serial number must be generated using a cryptographically secure random number generator. It must be greater than zero and have at least 64 bit entropy. It must be unique for each issuer.

The certificate profiles must be defined in detail in the CPS of the respective certification authority.

7.1.1 Version Number(s)

Certificates must be issued in accordance with version 3 of the international X.509 standard (X.509v3).

7.1.2 Certificate Content and Extensions; Application of RFC 5280

Telekom Security PKI uses certificate extensions to meet X509v3 requirements. Depending on the type of certificate, mandatory and optional extensions are defined.

For each extension, specifications are given with regard to the parameters to be used and requirements for the criticality of the parameters.

7.1.2.1 Root CA Certificate

Root CA certificates must not contain a "certificatePolicies" extension.

Root CA certificates must contain the following extensions ("mandatory field"):

Table 7 – Certificate extensions for root-CA certificates (1)

Extension (mandatory fields)	OID	Parameters	Criticality of the extension
KeyUsage	2.5.29.15	keyCertSign, cRLSign, digitalSignature (optional)	critical
BasicConstraints	2.5.29.19	CA=TRUE, (no pathLenConstraint)	critical
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 hash of the subject public key	non-critical

Root CA certificates may contain the following optional extensions:

Table 8 – Certificate extensions for root-CA extensions (2)

Extension (optional)	OID	Parameters	Criticality of the extension
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 hash of the issuer key	non-critical

7.1.2.2 Subordinate CA Certificate

Sub-CA certificates must contain the following extensions ("mandatory field"):

Table 9 – Certificate extensions for sub-CA certificates (1)

Extension	OID	Parameters	Criticality
KeyUsage	2.5.29.15	keyCertSign, cRLSign, digitalSignature (optional)	critical
BasicConstraints	2.5.29.19	CA=TRUE, pathLenConstraint	critical
certificatePolicies	2.5.29.32	OIDs of the supported CPs	non-critical
cRLDistributionPoints	2.5.29.31	Address(es) of the CRL issuing authority	non-critical
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation {…} accessMethod=caIssuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}	non-critical

Sub-CA certificates may contain the following optional extensions:

Table 10 - Certificate extensions for sub-CA certificates (2)

Extension	OID	Parameters	Criticality
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 hash of the issuer key	non-critical
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 hash of the subject public key	non-critical
nameConstraints			In accordance with [CAB-BR]
ExtKeyUsage	2.5.29.37	In accordance with [RFC 5280]	non-critical

Other extensions are allowed but must be set to non-critical.

7.1.2.3 Subscriber Certificate

EE (end entity) certificates must contain the following extensions:

Table 11 – Certificate extensions for EE-certificates (1)

Extension	OID	Parameters	Criticality
certificatePolicies	2.5.29.32	OIDs of the supported CPs cpsURI	non-critical
AuthorityInfoAccess	1.3.6.1.5.5.7.1.1	accessMethod=OCSP {1.3.6.1.5.5.7.48.1}, accessLocation {…} accessMethod=caIssuer {1.3.6.1.5.5.7.48.2}, accessLocation {…}	non-critical
ExtKeyUsage	2.5.29.37	In accordance with [RFC 5280]	non-critical
SubjectAltName	2.5.29.17	Alternative subscriber name	non-critical

EE certificates may contain the following optional extensions:

Table 12 – Certificate extensions for EE-certificates (2)

Extension	OID	Parameters	Criticality
AuthorityKeyIdentifier	2.5.29.35	160-bit SHA-1 hash of the issuer key	non-critical
SubjectKeyIdentifier	2.5.29.14	160-bit SHA-1 hash of the subject public key	non-critical
CRLDistributionPoints	2.5.29.31	Address(es) of the CRL issuing authority	non-critical
KeyUsage	2.5.29.15	keyCertSign and cRLSign must NOT be set The following are possible: digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement, encipherOnly, decipherOnly and combinations thereof	critical
BasicConstraints	2.5.29.19	The value CA=TRUE must NOT be set	critical
QCStatements (only QCP-w)	1.3.6.1.5.5.7.1.3	esi4-qcStatement-1 {0 4 01862 1 1}; esi4-qcStatement-5 {0 4 01862 1 5}; esi4-qcStatement-5; qc-type-web {0 4 0 1862 1 6 3};	non-critical

7.1.2.4 All Certificates

All additional fields MUST be in conformance to [RFC 5280].

7.1.2.5 Application of RFC 5280

All additional fields MUST be in conformance to [RFC 5280].

7.1.3 Algorithm Object Identifiers

Only a limited number of algorithms may be used to sign certificates.

The following signature algorithms may be used for new certificates:

- SHA256 RSA (OID 1.2.840.113549.1.1.11)
- SHA384 RSA (OID 1.2.840.113549.1.1.12)
- SHA512 RSA (OID 1.2.840.113549.1.1.13)
- SHA256 ECDSA (OID 1.2.840.10045.4.3.2)
- SHA384 ECDSA (OID 1.2.840.10045.4.3.3)
- SHA512 ECDSA (OID 1.2.840.10045.4.3.4)

Sub-CA and EE certificates may only be issued with the SHA-256 hash algorithm or higher.

CAs MUST NOT use the SHA-1 algorithm for issuing subordinate or end entity certificates anymore. Sub-CA or EE certificates MUST be issued with hash algorithm SHA-256 bits or higher. EE certificates SHOULD NOT chain up to a SHA-1 Sub-CA.

CAs MAY issue Root CA certificates or Sub-CA certificates with SHA-1 algorithm if those are cross certificates.

Furthermore, CAs MAY continue using their already existing SHA-1 root certificates.

7.1.4 Name Forms

For the name forms of root CA, sub CA, and EE certificates, the specifications in the corresponding section of the [CAB-BR] must be observed.

7.1.4.1 Issuer Information

The content of the “Issuer Distinguished Name” field MUST be in accordance to the Subject DN of the Issuing CA. The content MUST be consistent to the requirements of RFC 5280, section 4.1.2.4.

7.1.4.2 Subject Information – Subscriber Certificates

7.1.4.2.1 Subject Alternative Name Extension

CAs SHALL NOT issue certificates which contain a reserved IP-address or internal name in the Subject Alternative Name Extension or in the Subject CommonName fields. Entries in the dNSName field MUST follow the name syntax of RFC 5280 and MUST NOT contain underscores “_”.

7.1.4.2.2 Subject Distinguished Name Fields

The end entity certificates of the subordinate certification authorities (sub-CA) must contain a distinguished issuer name (issuer DN) and a distinguished subject name (subject DN) for this service, as described in Section 3.1.

If the Policy-OID 2.23.140.1.2.1 (DV) is used in a certificate, the following subject DN fields MUST NOT be populated:

- organizationName
- streetAddress
- localityName
- stateOrProvinceName
- postalCode

If the policy OID 2.23.140.1.2.2 (OV) is used in a certificate, the following subject DN fields MUST be populated:

- organizationName
- localityName
- stateOrProvinceName (if a meaningful value exists, e.g., federal state)
- countryName

If the policy OIDs 2.23.140.1.1 (EV) and 0.4.0.194112.1.4 (qcp-web) are used in a certificate, the following subject DN fields MUST be populated:

- organizationName
- AltName
- businessCategory
- jurisdictionLocalityName (exception permitted in accordance with CAB-BR)
- jurisdictionStateOrProvinceName (exception permitted in accordance with CAB-BR)
- jurisdictionCountryName (exception permitted in accordance with CAB-BR)
- serialNumber
- streetAddress
- localityName
- stateOrProvinceName (if a meaningful value exists, e.g., federal state)

- countryName
- postalCode

7.1.4.3 Subject Information – Root Certificates and Subordinate CA Certificates

7.1.4.3.1 Subject Distinguished Name Fields

The following fields must be populated for root CA and sub-CA certificates:

- commonName
- organizationName
- countryName

Subject attributes must not contain only metadata such as ".", "-" and " ". Furthermore, the value must not be absent, incomplete, or not applicable. If there are other attributes present in the Subject field, they must contain information and the CA must verify them.

7.1.5 Name Constraints

Root CA certificates MUST NOT be subject to name constraints.

Name constraints for sub-CA certificates are optional. They are used to technically restrict a sub-CA.

For a sub-CA certificate to be technically restricted, the certificate MUST contain an Extended Key Usage (EKU) extension that specifies all authorized key uses. The sub-CA may only issue certificates for these uses.

If the "id-kp-serverAuth" EKU is set, the sub-CA certificate must contain the Name Constraints X.509v3 extension with restrictions for dNSName, iPAddress, and/or DirectoryName.

The "anyExtendedKeyUsage" value must NOT be set within this extension.

When setting restrictions, the detailed specifications in the corresponding section of the [CAB-BR] must be observed.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers

The reserved object identifiers in the corresponding section in the [CAB-BR] must be observed and may only be set for the intended purposes.

7.1.6.2 Root CA Certificates

Root CA certificates must not contain certificate policies.

7.1.6.3 Subordinate CA Certificates

External Sub-CA certificates (non-affiliate) contain a policy OID that represents a dedicated assurance that the sub-CA meets the requirements in the corresponding chapter of the [CAB-BR] during its life cycle.

In external sub-CA certificates (non-affiliate) the anyPolicy-OID (2.5.29.32.0) is not allowed. This OID may be used for internal sub-CA certificates (affiliate).

In all cases it must be ensured that at least one of the policy OIDs used is present in both the corresponding public device certificate(s) and the corresponding sub-CA certificate(s).

The regulations in this section apply to all hierarchical levels below the root CAs, that is, also to the concatenation of sub-CA certificates.

7.1.6.4 Subscriber Certificates

End entity certificates issued by a sub-CA in the scope of this document MUST contain a certificate policy extension and policy OID that is dedicated to ensuring that the certificate meets the requirements of the [CAB-BR] during its life cycle. This MUST be documented in the certificate policy or CPS.

This policy OID must be defined and described in the CPS of the respective sub-CA.

7.1.7 Usage of Policy Constraints extension

No requirements for using the Policy Constraints extension

7.1.8 Policy Qualifiers Syntax and Semantics

See Section 1.2

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

In sub-CA and EE certificates, the CertificatePolicies extension is NOT critical. It is up to the subscribers and certificate users to evaluate this extension.

7.2 CRL Profile

The revocation lists issued must meet the following requirements:

- [RFC 5280] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- [X.509] Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, Recommendation X.509 (08/05), Recommendation X.509 (2005) Corrigendum 1 (01/07)

7.2.1 Version number(s)

Certificate revocation lists must be issued in X.509 version 2 format, which meets the requirements of RFC 5280.

7.2.2 CRL and CRL entry extensions

7.2.2.1 "Authority Key Identifier" (AuthorityKeyIdentifier) extension

The revocation lists must contain the "Authority Key Identifier" (AuthorityKeyIdentifier) extension. The criticality of this extension is set to "non-critical."

7.2.2.2 "Revocation list number" extension

The revocation lists must contain the "revocation list number" (cRLNumber) extension as a sequential serial number of the revocation list. The criticality of this extension is set to "non-critical."

7.3 OCSP profile

7.3.1 Version number(s)

OCSP V1 MUST be used in accordance with [RFC 6960].

7.3.2 OCSP extensions

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The rule within a hierarchy is that the included CAs must be certified in accordance with ETSI EN 319 411-1 or similar.

If parts of the PKI are operated by third parties, they must undertake to enable and support audits by Deutsche Telekom Security GmbH or an authorized representative as well as audits by external inspection authorities within the scope of certification.

8.1 Frequency or circumstance of assessment

The included CAs must be subjected to regular internal audits. The audit must cover the requirements for operation and personnel, compliance with this CP, and the requirements of the standard applied under 8.4.

If tasks have been outsourced to third parties, these parties must be regularly audited.

In accordance with the requirements, certification is reviewed at least once a year by an accredited assessment authority, which must be commissioned by the included CAs in such a way that sufficient time is given for the inspection so that there are no periods without certification.

Furthermore, event-driven audits must be conducted if this is necessary due to security incidents, for example.

Web server certificates require quarterly internal audits. A sample of at least 3 percent of all certificates generated during the period under observation is used and the fulfillment of the requirements are reviewed.

8.2 Identity/qualifications of assessor

For internal audits, expert assessors (internal auditors) must be employed who are trained in the performance of audits and have many years of expertise in PKI technology.

Compliance with the above standards must be audited by an accredited assessment authority. The certification must be carried out by an accredited certification authority.

8.3 Assessor's relationship to assessed entity

The assessor must be an employee or an authorized representative of an assessment authority. The assessment must be conducted in accordance with the ISO/IEC 17021 rules.

For internal audits, expert assessors (internal auditors) should be employed who otherwise do not perform any function within the CA to be audited.

8.4 Topics covered by assessment

The scope of the assessment is determined by the standard selected. Internal audits must cover compliance with the requirements of the CA/Browser Forum, the Mozilla Foundation root program, security management, and the standard selected.

The CA shall undergo either an audit in accordance with

(1) WebTrust for CAs v2.0 or newer and WebTrust for SSL Baseline with Network Security v2.2 or newer or
(2) ETSI EN 319 411-1, including references to ETSI EN 319 401 or
(3) ETSI EN 319 411-2 incl. normative references about ETSI 319 401 or
(4) in case of a Government CA and internal audit scheme encompassing all requirements of one of the above schemes or comparable criteria.

The audit or assessment must be carried out in regular intervals.

The execution of the audit must be done by a qualified auditor.

8.5 Actions taken as a result of deficiency

The included CAs must have standard procedures for the elimination of defects and deficits. An individual risk analysis must be prepared and documented. Remediation measures must be defined and documented so that minimization is achieved depending on the possible risk. The measures and their implementation will be monitored by the security management.

8.6 Communication of results

The compliance of the audit object with the requirements of the standard must be confirmed by an accredited certification authority in the form of a certificate. The underlying audit report does not have to be published if the result is referenced in the certificate.

The relevant certificate reports must be available on the Trust Center website at:

https://www.telesec.de/de/trust-center

In the case of legal requirements, the results must also be communicated to the specified authorities. The certificates must be published no later than 3 months after completion of the audit.

8.7 Self-Audits

There must be an internal self-audit process to monitor adherence to the CP / CPS stipulations.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees must be determined in the relevant General Terms and Conditions (AGB) of the certification authorities.

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

Financial responsibilities must be determined in the relevant General Terms and Conditions (AGB) of the certification authorities or in individual agreements.

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

The treatment of confidential business information must be specified in the policies of the certification authorities. The relevant legal provisions and, if applicable, further regulations on data protection must be observed.

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of personal information

The treatment of personal data must be specified in the policies of the certification authorities in a privacy plan.

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

No stipulation.

9.4.3 Information not deemed private

No stipulation.

9.4.4 Responsibility to protect private information

No stipulation.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

This document is protected by copyright. It is not permitted to use the texts or diagrams or extracts thereof without the written consent of Telekom Security. Intellectual property rights to the certificates and the ARL remain with Telekom Security. The rights of use to the certificates issued are set out in individual agreements with the corresponding certification authorities.

9.6 Representations and warranties

9.6.1 CA Representations and Warranties

By issuing a certificate, the CA assumes the certificate warranties listed here for the following authorized certificate holders:

1. The subscriber who is a party to the subscriber agreement or the terms of use agreement for the certificate
2. All suppliers of application software with whom the root CA has entered into an agreement to include their root certificate in the software distributed by that supplier of application software
3. All relying parties who reasonably rely on a valid certificate. The CA assures the authorized certificate holders and ensures that the CA complies with these requirements and its certificate policy and/or certification practice statement during the period of validity of the certificate when issuing and managing the certificate.

The certificate warranties include, but are not limited to, the following:

1. Right to use the domain name or IP address: at the time of issue, the CA (i) implemented a procedure to verify that the applicant had either the right to use or control the domain name(s) and IP address(es) listed in the "subject" field and in the "subjectAltName" extension of the certificate (or, only in the case of domain names, has been granted such right or control by a person with the right to use or control), (ii) followed the procedure for issuing the certificate, and (iii) accurately described the procedure in the CA's certificate policy and/or certification practice statement.
2. Authorization for the certificate: at the time of issue, the CA has (i) implemented a procedure to verify that the subject has approved the issuance of the certificate and that the applicant's proxy is authorized to apply for the certificate on behalf of the subject, (ii) followed the procedure for issuing the certificate, and (iii) accurately described the procedure in the CA's certificate policy and/or certification practice statement.
3. Accuracy of information: at the time of issue, the CA has (i) implemented a procedure to verify the accuracy of all information contained in the certificate (except for the "subject:organizationalUnitName" attribute), (ii) followed the procedure for issuing the certificate, and (iii) accurately described the procedure in the CA's certificate policy and/or certification practice statement.
4. No misleading information: at the time of issue, the CA has (i) implemented a procedure to reduce the likelihood that the information in the attribute "subject:organizationalUnitName" is misleading, (ii) followed the procedure for issuing the certificate, and (iii) accurately described the procedure in the CA's certificate policy and/or certification practice statement.
5. Identity of the applicant: if the certificate contains subject identity information, at the time of issue the CA has (i) implemented a procedure to verify the applicant's identity in accordance with Sections 3.2 and 11.2, (ii) followed the procedure for issuing the certificate, and (iii) accurately described the procedure in the CA's certificate policy and/or certification practice statement.
6. Subscriber agreement: if the CA and the subscriber are not affiliated companies, the subscriber and the CA are parties to a valid and enforceable subscriber agreement that meets these requirements, or if the CA and the subscriber are affiliated companies, the applicant's proxy has confirmed and accepted the terms of use.
7. 24/7 service: the CA maintains a 24/7 publicly accessible repository with current information about the status (valid or revoked) of all certificates that have not expired. - and -
8. Revocation: the CA will revoke the certificate for one of the reasons stated in these requirements. The root CA WILL be liable under these requirements for the performance and warranties of the sub-CA, for compliance with these requirements by the sub-CA, and for all liabilities and indemnities of the sub-CA, as if the root CA were the sub-CA issuing the certificates.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

The CA WILL, under the subscriber agreement or the terms of use agreement, require the subscriber to assume the representations and warranties in this section in favor of the CA and the certificate holders. Before issuing a certificate, the CA WILL act in favor of the CA or the holders and obtain either

1. the applicant's consent to the subscriber agreement with the CA or
2. the applicant's consent to the terms of use agreement.

The CA WILL implement a procedure to ensure that any subscriber agreement or terms of use agreement is legally enforceable against the applicant. In any case, the agreement MUST apply to the certificate issued in accordance with the certification application. The CA MAY use an electronic or click-through agreement if the CA has determined that such agreements are legally enforceable. A separate agreement MAY be used for each certification application, or a single agreement MAY be used to cover multiple future certification applications and the resulting certificates, as long as each certificate that the CA issues to the applicant clearly falls under that subscriber agreement or terms of use agreement.

The subscriber agreement or terms of use agreement MUST contain provisions that impose the following obligations and warranties on the applicant (or are assumed by the applicant on behalf of his customer or agent under a subcontractor agreement or hosting services agreement):

1. Accuracy of information: a commitment and warranty to provide accurate and complete information to the CA at all times, both in the certification application and as requested by the CA in connection with the issuance of the certificate(s) to be provided by the CA.
2. Private key protection: a commitment and warranty by the applicant to take all reasonable measures to maintain the exclusive control of the private key, which corresponds to the public key to be included in the requested certificate(s) (and any associated activation data or devices, e.g., passwords or tokens), its secrecy, and its proper protection at all times.
3. Certificate acceptance: an obligation and warranty that the subscriber checks and verifies the content of the certificate for accuracy.
4. Use of the certificate: a commitment and warranty to install the certificate only on servers accessible under the "subjectAltName(s)" listed in the certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use.
5. Reporting and revocation: an obligation and warranty to immediately cease using a certificate and the associated private key and to promptly request the CA to revoke the certificate if any of the following circumstances occur: (a) information in the certificate is or becomes inapplicable or inaccurate, or (b) there is an actual or suspected misuse or threat to the subscriber's private key that is associated with the public key included in the certificate.
6. Termination of use of the certificate: an obligation and warranty to immediately surrender any use of the private key associated with the public key included in the certificate after revocation of that certificate due to key compromise.
7. Responsiveness: an obligation to respond to the CA's instructions regarding a key compromise or certificate misuse within the specified time period.

8. Confirmation and acceptance: a confirmation and acceptance that the CA is entitled to immediately revoke the certificate if the applicant has violated the terms of the subscriber agreement or the terms of use agreement, or if the CA determines that the Certificate is being used to enable criminal activities, such as phishing, attacks, fraud, or the distribution of malware.

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

The certification authorities may limit their liability toward third parties. These limitations of liability must be described in the CP/CPS of the certification authority.

9.9 Indemnities

No stipulation.

9.9.1 Indemnification by CAs

No stipulation.

9.9.2 Indemnification by Subscribers

No stipulation.

9.9.3 Indemnification by Relying Parties

No stipulation.

9.10 Term and termination

9.10.1 Term

This document becomes effective upon publication on the Telekom Security website. Changes also take effect when they are published on public websites (see Section 2.3).

9.10.2 Termination

This document remains in effect in the latest version until it is replaced by a new version.

9.10.3 Effect of termination and survival

When the Telekom PKI service ends, all users remain bound by the regulations contained in the CP/CPS until the last certificate issued expires or is revoked.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

No stipulation.

9.12.1 Procedure for amendment

No stipulation.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

No stipulation.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should any provision of this document be or become invalid or unenforceable, this shall not affect the validity of the remainder of this statement. Instead of the invalid and unenforceable provision, a provision is deemed to have been agreed which comes closest to the economic purpose of this document in a legally effective manner. The same applies to additions made in order to close contractual lacunas.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.