Telekom Security PKI – Certificate Practice Statement

Certificate Practice Statement of 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	Content
Issuer	Deutsche Telekom Security GmbH Trust Center & ID-Solutions Untere Industriestraße 20, 57250 Netphen, Germany
Filename	Telekom-Security-PKI-CPS-EN-v12.00-20200605.docx
Valid since	01.07.2020
Title	Telekom Security PKI – Certificate Practice Statement- Certificate Practice Statement of 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 for DT Security PKI

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	Update BR changes 1.5.7 to 1.6.6 Update EV changes 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	Release of new version
11.01	05.06.2020	T-Systems	Changing T-System 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	Freigabe

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 DT Security Trust Center Public Key Infrastructure (PKI) is operated in the DT Security Trust Center by the Deutsche Telekom Security GmbH 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 certification practice statement (CPS) for all certification authorities operated within the DT Security PKI. The main target of the given document is the Root CA. The document 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 DT Security PKI meet and comply with all requirements and regulations of the current published version of the [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	Date	Object Identifier
Telekom Security PKI – Certificate Practice Statement	12.00	01.07.2020	1.3.6.1.4.1.7879.13.39

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.

In addition to operating certification authorities for proprietary internal products and services, the Trust Center issues CA certificates for certification authorities of other operators, which are operated under the following root certification authorities (root CAs):

Deutsche Telekom Root CA 2

Key: RSA 2048, SHA-1

Serial#: 26

Thumbprint: 85:a4:08:c0:9c:19:3e:5d:51:58:7d:cd:d6:13:30:fd:8c:de:37:bf

Valid until: 10. July 2019

T-TeleSec GlobalRoot Class 2

Key: RSA 2048, SHA-256

Serial#: 01

Thumbprint: 59:0d:2d:7d:88:4f:40:2e:61:7e:a5:62:32:17:65:cf:17:d8:94:e9

Valid until: 2. October 2033

T-TeleSec GlobalRoot Class 3

Key: RSA 2048, SHA-1

Serial#: 01

Thumbprint: 55:a6:72:3e:cb:f2:ec:cd:c3:23:74:70:19:9d:2a:be:11:e3:81:d1

Valid until: 2. October 2033

TeleSec GlobalRoot Class 1 G3

Key: ECDSA_P384, sha384ECDSA

Serial#: 1a:f8:94:c5:45:27:c2:c5:68:25:b8:a9:31:5c:bf:da

Thumbprint: 52 7f 0d 83 1b 02 bd 85 a6 8b f6 db 23 f6 e7 0d e2 f8 a0 20

Valid until: 10. April 2044

TeleSec GlobalRoot Class 2 G3

Key: ECDSA_P384, sha384ECDSA

Serial#: 08:22:70:67:e1:16:f6:90:56:ef:0b:fe:fb:bd:d9:91

Thumbprint: 63 2e 29 d7 8a 73 ab 29 5f 50 84 35 a5 f0 6a 7e f6 55 d9 81

Valid until: 10. April 2044

TeleSec GlobalRoot Class 3 G3

Key: ECDSA_P384, sha384ECDSA

Serial#: 2b:d4:0e:3e:f9:1f:9a:c5:f9:19:af:04:24:6c:7e:fb

Thumbprint: 46 3c 28 b0 b9 41 91 a6 23 38 aa dc db 79 b4 46 ca 97 a9 e9

Valid until: 10. April 2044

The root CA certificates are self-signed by the Trust Center and are published by DT Security. The publication makes it possible to fully check the validity of all certificates issued in this hierarchy. Only certificates from directly subordinate certification authorities (sub-CAs) are issued. End entity certificates (subscriber certificates) are not issued. Regulations regarding subscriber certificates are described in separate CPS of additional DT Security certificate solutions.

1.3.2 Registration authorities (RA)

Registrations and all related activities for the root CAs listed in this CPS are processed by a central internal registration authority of DT Security. No further external or internal registration authorities (RA) are consulted.

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

Relying parties are legal entities or organizational units that trust in the integrity and quality of an issued subscriber certificate.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

See CP, section 1.4.1

1.4.2 Prohibited certificate uses

See CP, section 1.4.2

1.5 Policy administration

1.5.1 Organization administering the document

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

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 notification of abuse, compromise of certificates and keys of the DT Security Trust Center can be reported at the URL https://www.telesec.de/en/kontakt-en 24/7. The prioritization takes place via selection "Report suspicion of certificate abuse" in the field "Subject" on the form. The most accurate and comprehensive presentation should be in the "Text" field, so that an evaluation by DT Security can be done early enough and adequate measures can be initiated. As a rule, DT Security will respond within 24 hours with a first assessment of the specified communication channels. If necessary, DT Security will involve law enforcement agencies and regulators. The entry of the report is considered as an agreement that in such cases data can be passed on to authorities without further consent.

1.5.3 Person determining CPS suitability for the policy

This document (CPS) 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 must be in compliance with the associated Certificate Policy (CP).

1.5.4 CPS approval procedures

The publisher named in Section 1.5.1 is responsible for this document (CPS). 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 CPS. This shall also apply even if no changes are made to contents.

1.6 Definitions and acronyms

1.6.1 Definitions

Table 4 - Glossary

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.
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 Safe Browsing list or names that the CA identifies based on its own risk-minimization criteria.
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 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.
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.
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 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.
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).
Certificate	An electronic document that uses a digital signature to bind a public key to an identity (e.g., person, device).

Term	Explanation
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.
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).
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.
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 certification authority (CA) follows for issuing, managing, revoking, and renewing 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.
Change Advisory Board	A board within DT 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).
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.

Term	Explanation
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 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.

Term	Explanation
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.
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 maintained using several queries). LDAP is used in particular to query digital certificates and revocation lists within public key infrastructures.
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.
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.

Term	Explanation
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.
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).
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).
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.

Term	Explanation
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.
Registered domain name	A domain name that is registered with a domain name registration authority (registrar).
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.
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.

Term	Explanation
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 connection with 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.
Transport layer security (TLS)	Crypto protocol for ensuring end-to-end connections on the Internet.
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.
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

Term	Explanation
	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
CARL	Certification Authority Revocation List (same as ARL)
CMP	Certificate Management Protocol
CP	Certificate Policy
CPS	Certification Practice Statement
CN	Common Name
CRL	Certificate Revocation List
DN	Distinguished Name
EDP	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

Abbreviation	Definition
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*)
SK	Single Key
SLA	Service Level Agreement
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

2.1 Repositories

A distinction is made between the following information services within the PKI:

- OCSP
- ARL or CARL
- CP and CPS
- Other

2.2 Publication of certification information

DT Security makes ARL and OCSP information available 24/7.

OCSP

The status of a certificate can be queried via the Online Certificate Status Protocol (OCSP). For this purpose, the certificate status is made publicly accessible via a defined interface.

CRL

The Trust Center provides the PKI certificate users on the Internet with a publicly available CRL.

CP and CPS

The Trust Center's website can be reached at http://www.telesec.de/pki/index.html. The CP and the CPS are published at https://www.telesec.de/de/trust-center

Other information

The Trust Center also provides the certificate users of the PKI with the following information on the website:

- Root CA certificate and its fingerprint (SHA1 and/or SHA256)
- Information about the change of a Root-CA or Sub-CA certificate
- Information on a compromise, a suspected compromise, or the revocation of a root CA or sub-CA certificate

2.3 Time or frequency of publication

In case of a revocation the revocation information of root-CA and sub-CA certificates are updated (CRL, OCSP responder). CP, CPS and other informationen material are published at https://www.telesec.de.

OCSP

Before using the certificates, the information is available for OCSP requests.

ARL/CARL update

See Section 4.9.7

CP and CPS

This document and the associated CP are reviewed at least once a year.

If there are relevant changes regarding requirements, explanations, measures or procedures, the CP/CPS will be updated in a timely manner.

2.4 Access controls on repositories

The repositories are publicly available for read-only access. There are no further restrictions.

Write access to all information listed in Section 2.2 is only used by authorized employees or systems of the Trust Center.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

A distinguished name (DN) is a unique, global name for directory objects in accordance with the X.500 standard. Distinguished names allow people and systems to be clearly distinguished worldwide. The DN ensures that a digital certificate is never issued with the same name for different people.

3.1.1 Types of names

The naming conventions for the "SubjectDistinguishedName" (subject DN) and "IssuerDistinguishedName" (issuer DN) are defined in accordance with the X.501 standard and include fields with the following attributes:

- Country (C)
- Organization (O)
- Organizational Unit (OU)
- State or Province (S)
- Locality (L)
- Common Name (CN)
- E-mail Address (E)
- Subject Alternative Name (SAN)

3.1.2 Need for names to be meaningful

The name in the "SubjectDistinguishedName" (CN) and "SubjectAlternativeName" (SAN) clearly identifies the subscriber. Permissible abbreviations of the name entered in the commercial register, for example, are also used.

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 requirements of the corresponding chapter in the CP are fulfilled.

3.1.6 Recognition, authentication, and role of trademarks

The requirements of the corresponding chapter in the CP are fulfilled.

3.2 Initial Identity validation

No stipulation.

3.2.1 Method to Prove Possession of Private Key

No stipulation.

3.2.2 Authentication of Organization and Domain Identity

The requirements of the corresponding chapter in the CP are fulfilled.

3.2.2.1 Identity

See CP, Section 3.2.2

3.2.2.2 DBA/ Trade name

See CP, Section 3.2.2

3.2.2.3 Verification of Country

See CP, Section 3.2.2

3.2.2.4 Validation of Domain Authorization or Control

No stipulation.

3.2.2.4.1 Validating the Applicant as a Domain Contact

No stipulation.

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

No stipulation.

3.2.2.4.3 Phone Contact with Domain Contact

No stipulation.

3.2.2.4.4 Constructed Email to Domain Contact

No stipulation.

3.2.2.4.5 Domain Authorization Document

No stipulation.

3.2.2.4.6 Agreed-upon Change to Website

No stipulation.

3.2.2.4.7 DNS Change

No stipulation.

3.2.2.4.8 IP Address

No stipulation.

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

No stipulation.

3.2.2.4.12 Validating Applicant as a Domain Contact

No stipulation.

3.2.2.4.13 Email to DNS CAA Contact

No stipulation.

3.2.2.4.14 Email to DNS TXT Contact

No stipulation.

3.2.2.4.15 Phone Contact with Domain Contact

No stipulation.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

No stipulation.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

No stipulation.

3.2.2.5 Authentication for an IP Address

No stipulation.

3.2.2.5.1 Agreed-upon Change to Website

No stipulation.

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

No stipulation.

3.2.2.5.3 Reverse Address Lookup

No stipulation.

3.2.2.5.4 Any Other Method

No stipulation.

3.2.2.5.5 Phone Contact with IP Address Contact

No stipulation.

3.2.2.5.6 ACME “http-01” method for IP Addresses

No stipulation.

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

No stipulation.

3.2.2.6 Wildcard Domain Validation

No stipulation.

3.2.2.7 Data Source Accuracy

See CP, section 3.2.2

3.2.2.8 CAA Records

No stipulation.

3.2.3 Authentication of Individual Identity

The requirements of the corresponding chapter in the CP are fulfilled.

3.2.4 Non-verified Subscriber Information

None of the root and sub CA certificates issued by Deutsche Telekom Security GmbH contain non-verified subject information.

3.2.5 Validation of Authority

The requirements of the corresponding chapter in the CP are fulfilled.

3.2.6 Criteria for Interoperation or Certification

The requirements of the corresponding chapter in the CP are fulfilled.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

No stipulation.

3.3.2 Identification and Authentication for Re-key after Revocation

No stipulation.

3.4 Identification and Authentication for Revocation Request

The Trust Center offers subscribers a central revocation service so that the internal certificate can be revoked in the event of loss or suspicion of misuse. A revocation is authenticated by entering the basic data (name, company, call-back number, e-mail address). The revocation request is authorized by providing the revocation password.

Persons and institutions authorized for revocation may request a certificate to be revoked by e-mail or telephone. In case of revocation, the certificate is added to a revocation list and is reported as revoked for OCSP requests.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a Certificate Application?

Applications may only be submitted by an authorized representative of the respective applicant organization. The certificates are issued exclusively to legal persons.

4.1.2 Enrollment Process and Responsibilities

The application procedure is as follows, depending on the certificate:

Root-CA

- Management request
- Involvement of the ETSI inspection and certification authority
- Review of the request by the operator
- Release for certification by the operator
- Check of hardware
- Key pair generation
- Self-signed certificate generation
- Approval of the ETSI inspection and certification authority
- Storage and subsequent archiving of the documentation

Sub-CA/cross

- Conclusion of contract with third parties or request from management
- Creation of the certificate application
- Creation of the keys and attachment of the request incl. public key
- Review of the request by the operator
- Monitoring of key delivery
- Release for certification by the operator
- Issue and delivery of the certificate
- Storage and subsequent archiving of the documentation

Service certificates

- Creation of the certificate application
- Creation of the keys and attachment of the request incl. public key
- Review of the request by the operator
- Check of key delivery
- Release for certification by the operator
- Issue and delivery of certificates
- Storage and subsequent archiving of the documentation

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Identification and authentication is part of the registration process and include at least the following steps:

- Signed contract is in place when a certificate is applied for by a third party
- Completed, current order form, digital or in paper format. The application form must be signed electronically or in writing by an authorized representative of the customer
- Check of the certificate application for authorization of the signatory. Also check of completeness and verification of signature
- For a Sub-CA the service specific CPS must be available
- If necessary, submission of further documents, e.g., documents of the inspection and certification authority on successful certification in accordance with the required standards or partial confirmation and subsequent delivery of the certificate
- Check and release of the service specific CPS
- Proof of ownership of the private key in accordance with Section 3.2.1 and review of the request

All process steps are documented and signed by the processor.

4.2.2 Approval or Rejection of Certificate Applications

A certificate application is authorized and prepared for processing only if the review was successful.

If the application is rejected, the subscriber will be notified in an appropriate manner, stating reasons, and measures will be agreed with the customer to remedy the defects and continue the process.

4.2.3 Time to Process Certificate Applications

Processing of the certificate application starts within a suitable period following receipt of the application. There are no provisions for the processing time of an application if no processing time has been specified in an individual agreement.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

An approval step is the precondition to produce certificates by the Root-CA. A CAA check is not performed for certificates of the Root-CA. The operator responsible documents the process steps and loads the request onto a mobile data storage. Production takes place exclusively in line with the dual-control principle, which means that two role owners are then able to produce the desired certificate.

The inspection or certification or control authority is involved as a witness when new root certificates are produced. A customer representative can also participate as guest.

4.3.2 Notification (to subscriber) of Certificate Issuance

The subscriber is informed after production and receives the certificate for verification.

4.4 Certificate Acceptance

A produced certificate is sent to the subscriber before publication, to proof the correctness of the content and coding.

4.4.1 Conduct constituting certificate acceptance

The applicant must send an acceptance confirmation to the Trust Center within 7 days.

4.4.2 Publication of the certificate by the CA

The Root-CA and Sub-CA certificates are published on the Trust Center website http://www.telesec.de after acceptance.

4.4.3 Notification of certificate issuance by the CA to other entities

There is no explicit notification of further instances. After the production of a new Sub-CA certificate, the certificate is added to the CCADB certificate database https://www.ccadb.org

4.5 Key pair and certificate usage

The Root-CA only issues certificates for itself, for subordinate CAs, and service certificates.

4.5.1 Subscriber private key and certificate usage

The certificates issued according to this CPS are only issued for the application in certification authorities.

4.5.2 Relying party public key and certificate usage

Relying parties may only use certificates of the Root-CA if

- compatible software is used for the standards and validity models deployed
- before using a certificate, its validity is checked in accordance with the applied validity model
- the certificate is used exclusively for authorized and legal purposes

4.6 Certificate renewal

The renewal of Root-CA/Sub-CA certificates or service certificates is not supported. Therefore this section contains no stipulations.

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

No stipulation.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate Re-key

The generation of Root-CA/Sub-CA certificates or service certificates is not subject to re-keying. Therefore this section contains no stipulations.

4.7.1 Circumstance for certificate re-key

No stipulation.

4.7.2 Who may request certification of a new public key

No stipulation.

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

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

A certificate modification is not part of the certificate lifecycle of the certificates pertaining to this CPS. If the certificate has to be modified, this is documented and a new certificate request/order will be generated. Therefore, this section contains no stipulations.

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 re-key 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 created by the Root-CA is particularly critical and must usually be carried out with the participation of the accredited certification authority.

4.9.1 Circumstances for Revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

No stipulation.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

The 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 central certificate information have changed.
6. 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;

7. The Issuing CA determines that any of the information appearing in the certificate is inaccurate or misleading;
8. 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
9. The Issuing CA's or Subordinate CA's right to issue certificates under these requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
10. The Issuing CA has got the suspicion that its own private key has been compromised.
11. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.

The issuing CA SHOULD revoke a certificate after evaluation or a time limit if one or more of the following occurs:

12. There are legal regulations or adjudications or instructions of a supervisory authority.

4.9.2 Who can request Revocation?

If the CA or the certificate subscriber learns of information which are a mandatory cause for revocation, a request for revocation needs to be generated. The revocation must be executed by the CA itself, after consultation with the certificate subscriber, or due to a request of the certificate subscriber.

A revocation which has no origin in the mandatory reasons for revocation, has to be initiated by the certificate subscriber or other authorized persons. Since the subscriber is usually a legal person, proof of the power of attorney must be provided.

4.9.3 Procedure for Revocation Request

Persons authorized for revocation may request a certificate 7x24h to be revoked by signed e-mail or in writing. Due to the criticality, contact should be made by telephone beforehand. The process to report a misuse is described in section 1.5.2, contact information are available also online at www.telesec.de

If the conditions for the revocation are met, the revocation is carried out and the revoked certificate is included in the revocation information. The revocation information is provided in a format that complies with the standard (ARL).

The person or institution authorized will be notified that the revocation has been carried out.

4.9.4 Revocation Request Grace Period

The CA or the certificate holder needs to initiate a revocation request immediately after detecting a reason for revocation.

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 for the issued certificates of the Root-CA is provided in a standard form (ARL) in the DER format and can therefore be checked using applications that comply with the standard. In addition, the revocation status may be checked via an OCSP request.

4.9.7 CRL Issuance Frequency

The revocation information of the Root-CA is updated every six months in a standardized form (ARL) and provided. Any revocation of a certificate that is relevant for the list within these six months triggers a new ARL to be created at that time.

Due to the application of cross certificates, an ARL is being issued at least every 31 days.

An entry will not be removed from the CRL until it is listed in a regular planned CRL issued after the regular validity time of the revoked certificate has expired.

4.9.8 Maximum Latency for CRLs

The revocation lists are made available in the directory device within an economically reasonable period after they have been generated. The latency of the ARL is maximum five (5) days.

4.9.9 On-line Revocation/Status Checking Availability

DT Security runs an OCSP-responder to verify the validity of issued Root-CA and Sub-CA certificates. OCSP responses are valid for five (5) days. The OCSP database will be updated after a certificate revocation during a max. timeframe of five (5) days.

Both the revocations lists and OSCP service are provided on a 24/7 basis. Online information (OCSP) about the certificate status are available at http://ocsp.telesec.de/ocspr

The OCSP responses are conform to the requirements of RFC 6960.

4.9.10 On-line Revocation Checking Requirements

Trusting third parties must be able to check the revocation status of a certificate to gather enough information about the trustworthiness and validity of a certificate. The OCSP service (OCSP Responder) is available for requesting up-to-date status information (see Section 4.9.9).

The OCSP service operates conform to RFC 6960 and/or RFC 5019.

The Root CA updates the OCSP database at least every twelve (12) months or within 24 hours after a new certificate revocation.

The OCSP information for subscriber certificates issued by Sub-CAs will be updated at least every four (4) days. OCSP responses have a maximum expiration time of ten (10) days.

The OCSP responder offers replies about a certificate status, but does not answer with “good” if a certificate serial number has the state “unused”. Instead the OSCP responder gives the answer “unknown”.

The OCSPs are being monitored.

4.9.11 Other Forms of Revocation Advertisements Available

No other forms of communication are used at present.

4.9.12 Special Requirements Related to Key Compromise

If a private key is compromised, the relevant certificate must be revoked as promptly as possible. There are no further regulations.

4.9.13 Circumstances for Suspension

A suspension (revocation reason „on-hold“) for a certification authority are not being offered.

4.9.14 Who can request Suspension

Suspension is not supported.

4.9.15 Procedure for Suspension Request

Suspension is not supported.

4.9.16 Limits on Suspension Period

Suspension is not supported.

4.10Certificate status services

An online status information service is available (see Section 4.9.9).

4.10.1 Operational Characteristics

No additional characteristics (see Section 4.9)

4.10.2 Service Availability

The status information service is available on a 24/7 basis.

4.10.3 Optional Features

No optional features are available.

4.11End of subscription

If a contractual relationship is terminated by the subscriber, the certificate is revoked.

4.12Key escrow and recovery

For certification authorities run by the Trust Center, encrypted key pairs are stored on an approved hardware security module (HSM) in a secure environment. Key escrow at third parties is not implemented.

4.12.1 Key escrow and recovery policy and practices

No stipulation. Key escrow and recovery are not supported.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation. Key escrow and recovery are not supported.

5 FACILITY, MANAGEMENT, AND PHYSICAL CONTROLS

The Root-CAs considered in this CPS are housed within the Trust Center in a specially protected area and are operated by trusted and expert personnel. All processes for requesting and generating certificates are defined in detail. All security measures are documented in a security plan (not publicly available).

5.1 Physical security controls

This section describes the infrastructural measures.

5.1.1 Site location and construction

The Root-CAs are operated at a site location of the Trust Center for which security requirements are mandatory. At the location several operation and administration employees of the Trust Center are stationed, which allows short chains of command for the operation and maintenance of the infrastructure. Inside the building there are especially secured rooms where e.g. container and cable channels are secured with additional technical and organizational measures.

The technical measures are supplemented by organizational elements that include the handling of security-relevant techniques and regulations regarding access to security zones for employees and third parties (visitors, external staff and cleaning staff), delivery of materials (hardware, accessories, resources) and tidiness at the work station as well as in computer rooms.

5.1.2 Physical access

Access to the building:

The location is monitored by a janitor during the main business hours from 06 am to 06 pm. Outside of this time frame the exit doors are secured via an alarm system and the building is monitored with the help of video installation.

DT Security manages smart cards, keys and the access control system to the administration area internally. If there are external guests, a DT Security employee meets the guests at the reception area and guides them to their meeting location.

Access to the administration area:

The administration area houses IT components for the operation of the CA. The administration area is located on the first upper floor in a secured area of the administration personnel. Not only the administrators' offices but also the IT inside the administration area are access restricted. The access control system has been installed in addition to the access control system and monitoring of the building. Therefore, to garner access to the administration area, two access control systems must be passed:

- The organizational access control guidelines are implemented and monitored via the technical access control system
- There is a regular inspection of the granted access rights
- Each access right and access to the area is being protocolled

- The chief of Trust Center operation defines and authorizes the access rights for the personnel. Smart cards and keys are being issued to the employees based on these access rights guidelines. They are monitored with the help of lists.
- The keys are reserved for emergency situations and only handed out to a restricted number of employees. The access control system also monitors the usage of a key in an emergency.
- A named administrator manages the access control system. Insight or access to the protocols of the access control system is only possible based on a 4 eyes principle process.

The server is in a secured and locked server rack which is again operated based on a 4 eyes principle process. There is an additional security level to access the Hardware Security Module (HSM). The HSMs are operated inside a safe which is located in the administration area. The key to the safe is stored inside another safe whose access is restricted to specific administrators. The second safe is located in a different section of the administration area.

Alarm system:

- The walls and windows of the administration area are monitored and protected against intruders.
- The halls are equipped with a motion sensor system
- The doors for the emergency exit are alarm protected
- The security area has its own intruder alarm system. The alarms are forwarded to the alarm system of the location. The system is activated outside the business hours.

5.1.3 Power and air conditioning

The power supply of the location provides a separate network (green outlet) for an uninterruptible power supply. The administration area is equipped with an air conditioning system. The outer walls are built in massive construction. One of the walls contains the in- and out-ventilation of the air conditioning system. The ventilation is secured from the inside and can not be removed from the outside. The maintenance area of the air conditioning system is separated via an additional door. The door is only opened during maintenance work under supervision.

5.1.4 Water exposures

The administration area is located on the first floor to prevent danger of flooding.

5.1.5 Fire prevention and protection

The applicable fire regulations (e.g. local fire department, regulations regarding fire resistance, VDE-compliant electrical installation) are complied with. All fire-resistant doors to and inside the administration area include automatic closing mechanisms. As agreed with the fire department, water will only be used to put out fires in extreme emergencies.

The location is separated in different fire sections. The administration area and necessary additional rooms are designed as a separate section with the help of the installed doors and the quality of the walls.

The entire building is equipped with an early fire detection system. The fire alarm system located in the reception area forwards alarms to the fire department of the city Siegen.

5.1.6 Media storage

Data media containing production software and data, audit, archive, or backup information, are stored in rooms with appropriate physical and logical access controls which offer protection against accident damage (e.g., water, fire, and electromagnetic damage).

5.1.7 Waste disposal

Confidential documents and materials are physically destroyed before being disposed of. Prior to their disposal, data media containing confidential information must be treated in such a way that this data cannot be extracted or restored. Prior to their disposal, cryptographic devices are physically destroyed according to the manufacturer's guidelines. Other waste is disposed of in accordance with DT Security’s regular disposal guidelines.

5.1.8 Off-site backup

DT Security regularly runs backups of critical system data, audit log data or other confidential information. The backup copies are kept in a different room from the original data.

5.2 Procedural controls

5.2.1 Trusted roles

All persons working for the Root-CAs are listed as trusted roles. These are operators, system administrators, internal auditors, and responsible persons for the operation service. The high requirements for this role transfer apply to all persons.

5.2.2 Number of Individuals Required per Task

The operational maintenance of the certification authority and the directory service (administration, backup, restoration) is carried out by knowledgeable and trusted staff.

Work on highly sensitive components (e.g., key generation system, HSM) is governed by special internal control procedures and carried out by at least two members of staff in trusted roles in a secure environment and in accordance with the dual-control principle.

5.2.3 Identification and Authentication for Trusted Roles

DT Security employees who are classed as trustworthy and who carry out trustworthy activities are subject to a DT Security internal security check (see Section 5.3.2).

DT Security ensures that employees have achieved a trusted status and the department has given its approval before these employees:

- receive access tokens and access to facilities,
- Receive authorization to access IT systems
- Are permitted to carry out certain tasks in connection with these systems

5.2.4 Roles Requiring Separation of Duties

The following roles require a separation of duties and are therefore assumed by different employees:

- Backup and recovery of databases and HSMs,
- Key life-cycle management of Sub-CA and Root-CA certificates.

5.3 Personnel controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Employees wishing to work as trusted persons are required by DT Security to prove that they have the qualifications and experience necessary to fulfill their prospective work obligations in a competent and satisfactory manner, see also Section 5.3.2.

5.3.2 Background Check Procedures

Before an employee starts work in a trusted role, DT Security runs a security check which includes the following:

- Checking and confirming the previous work relationships
- Checking employment references
- Confirming the highest or most relevant educational/vocational qualification
- Certificate of good conduct in accordance with § 30 of the German Federal Central Criminal Register Act (Bundeszentralregistergesetz – BZRG)

Sofern die in diesem Abschnitt festgelegten Anforderungen nicht erfüllt werden können, macht DT Security ersatzweise Gebrauch von einer gesetzlich zulässigen Ermittlungsmethode, die im Wesentlichen die gleichen Informationen liefert.

Results of a security check which could lead to a candidate for a trusted person being rejected can include

- false statements by the candidate or the trusted person
- particularly negative or unreliable employment references
- certain previous convictions.

Reports containing such information are evaluated by HR employees or security personnel. They are determining the next steps. Further proceedings may involve measures that can even lead to candidates for trusted positions having their employment offer withdrawn or to trusted persons being dismissed.

The application of information gathered during a background check for executing aforementioned measures underlies legal regulations.

DT Security must be provided with a certificate of good conduct at regular intervals, but no later than after three (3) years, or a new check will be performed.

5.3.3 Training Requirements and Procedures

The staff at DT Security undergo the training measures required to fulfill their work obligations in a competent and satisfactory manner. DT Security stores records about training measures.

The training programs at DT Security are tailored towards the individual work areas and include, for example:

- Advanced PKI knowledge including key management:
- Procedures in accordance with ITIL
- Data protection,
- Security and operational guidelines and processes of DT Security,
- Use and operation of the hardware and software in use
- Reporting and handling of faults and compromises
- Procedures for disaster recovery and business continuity

- Requirements of the CA Browser Forum
- Requirements of the browser manufacturers, e.g., Mozilla Root Program

5.3.4 Retraining Frequency and Requirements

DT Security personnel receive refresher and training courses to the required extent and at the required intervals. In particular, training is provided in further development of the root programs of the browser manufacturers and the CA/Browser Forum.

5.3.5 Job Rotation Frequency and Sequence

If there are employee changes, care is taken to ensure that no risks arise from the change.

5.3.6 Sanctions for Unauthorized Actions

DT Security reserves the right to punish unauthorized activities or other violations of this CPS and the procedural and work instructions resulting therefrom and to take appropriate disciplinary measures. The disciplinary measures may include measures up to a dismissal based on the number and severity of unauthorized activities.

5.3.7 Independent Contractor Controls

DT Security reserves the right to name / apply independent contractors or consultants for trustworthy positions. These persons underly the same functional or security criteria as DT Security employees.

The above group of people who have not yet concluded or successfully completed the security screening described in Section 5.3.2 will only be granted access to DT Security's secure facilities provided they are always accompanied by trusted persons and are closely supervised.

5.3.8 Documentation Supplied to Personnel

To enable employees to properly fulfill their work obligations, DT Security provides its employees with all the aids and documents they need for this (training documents, procedural instructions).

5.4 Audit logging procedures

5.4.1 Types of Events Recorded

Generally, all log data entries 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

For the life-cycle management of CA key pairs or CA systems, the Trust Center logs at least the following events for:

a) generation, destruction, 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

CA certificates

For the life-cycle management of CA certificates, the Trust Center logs at least the following events for:

- 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, the Trust Center logs all security-relevant events for operation of the infrastructure. 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

5.4.2 Frequency of Processing and Archiving Audit Logs

The audit logs/logging files are continuously examined for important events relevant to security and operations. Furthermore, DT Security checks its audit logs/logging files for suspicious and unusual activities resulting from irregularities and faults.

Measures taken in response to the analysis of audit logs/logging files are also being logged.

5.4.3 Retention Period for Audit Log

Audit logs/logging files are archived after processing for seven (7) years.

5.4.4 Protection of Audit Log

Audit logs/logging files are protected against unauthorized access.

5.4.5 Audit Log Backup Procedures

An audit log backup is done if needed.

5.4.6 Audit Log Accumulation System (internal vs. external)

Applications create and log audit data. Manually generated audit data is recorded by DT Security employees.

5.4.7 Notification to Event-Causing Subject

Events recorded by the audit monitoring system are assessed and passed on to the Trust Center staff responsible. High priority events are immediately passed on to the Trust Center staff, including outside of regular working hours.

5.4.8 Vulnerability Assessments

The Trust Center administrators are regularly informed about weaknesses found in software products. After analyzing the information, the vulnerability is assessed and counter-measures are determined which are then immediately implemented.

5.5 Records archival

5.5.1 Types of Records Archived

DT Security archives the following data:

- Hard copy of application documents
- All audit/event logging files recorded

5.5.2 Retention Period for Archive

The following records and storage periods are stipulated:

- Order documents, in particular information regarding certificate applications, their validation, and the certificates resulting from this and revocations executed are retained for a minimum of seven (7) years after the certificate expires
- Audit- and event log data are stored for seven (7) years

5.5.3 Protection of Archive

DT Security ensures that only authorized and trusted persons are given access to archives. Archive data is protected against unauthorized read access, changes, deletions, or other forms of tampering.

5.5.4 Archive Backup Procedures

An incremental backup of the electronic archives is carried out on a daily basis.

5.5.5 Requirements for Time-stamping of Records

Data such as certificates, certificate revocation lists, OSCP responses, and logging files are given information on the date and time. The time source is the receive signal of the DCF 77, from which the UTC is derived.

5.5.6 Archive Collection System (internal or external)

DT Security only uses internal archiving systems.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized and trusted personnel receive access to archives and archive data. When archive data is restored, its authenticity is verified.

5.6 Key changeover

Within the period of validity, a key change or certificate change may be required if the

- key material is compromised
- cryptographic algorithm needs to be changed

- key size needs to be changed
- certificate content is changed

The generation of new keys and certificates is documented and monitored in accordance with the rules of the key generation ceremony. New certificates and their fingerprints are published (see Section 2.3).

Certificates can only be renewed within the period of validity of the Root-CA higher up in the hierarchy. Expired or revoked certificates remain available for validation on a website.

In case of a key changeover of Root-CA or Sub-CA the generation of new keys and certificates has to be documented and to be monitored according to the requirements of the security concept. Sub-CA New certificates and their fingerprints must be published (see Section 2.2).

5.7 Compromise and disaster recovery

If private keys of a Root-CA or Sub-CA are compromised, this must be communicated without delay (see Section 2.2). Sub-CA certificates must then be revoked without delay and the corresponding ARL must be published immediately. The generation of new keys and certificates must be documented and monitored according to the stipulations of the related security plan. New certificates and their fingerprints must be published (see Section 2.2).

5.7.1 Incident and Compromise Handling Procedures

Incidents are submitted via the contacts defined in Section 1.5.2 and processed in the context of service management.

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 is immediately investigated and reported to the DT Security security department. The event entails a corresponding escalation, incident investigation, incident response, and finally incident resolution. Disaster recovery is carried out depending on the incident classification.

5.7.3 Recovery Procedures After Key Compromise

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

End entities are informed that the relevant websites may be compromised (see Section 2.3). If necessary, the certificate(s) must be immediately revoked and the corresponding certification authority revocation list (ARL) must be generated and published.

5.7.4 Business Continuity Capabilities after a Disaster

DT Security has developed, implemented, and tested an emergency plan for data center operation in order to alleviate the effects of catastrophes of all kinds (natural catastrophes or catastrophes of human origin) and to restore the availability of critical business processes as quickly as possible. This also includes all Trust Center processes, components, systems, and services. This plan is reviewed at least once a year, tested, and updated accordingly, so as to be able to respond in a targeted and structured manner in the case of a disaster.

The emergency plan contains 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

As part of a compliance audit (see Section 8), the auditor is authorized to view the details of the emergency plan.

5.8 CR or RA termination

Termination of operations may only be invoked by the DT Security Board of Management.

If one or all DT Security Root-CAs (see Section 1.3.1) have to cease operating, a cessation plan will be developed. Economically reasonable efforts (or efforts promised in the individual agreements) will be made to notify in advance any subordinate authorities affected by these terminations of operations.

A termination plan may include the following regulations:

- Continuity of revocation service
- Revocation of issued CA certificates
- Any transition regulations required for a successor CA
- Reimbursement of costs depending on the content of existing individual agreements
- Retention of the documentation and archives of the CA

If operations (the revocation service, in particular) are not taken over by another certification authority, all certificates issued will be revoked.

6 TECHNICAL SECURITY CONTROLS

The Trust Center is housed in a specially protected building and operated by expert staff. All processes for requesting and generating certificates of the certification authorities operated there are defined in detail. All technical security measures are documented in a security plan (not publicly available).

The following statements describe technical measures and apply to the root CA certificates operated by the Trust Center.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

All key pairs for root CA certificates are generated in a protected environment and created and stored on a security-checked hardware component (FIPS 140-2/ level 3 evaluated). This process will be executed in form of a key ceremony.

Implementation of the dual-control principle is enforced when generating the key. 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

No stipulation.

6.1.2 Private Key Delivery to Subscriber

No stipulation.

It is not planned to deliver private keys to subscribers.

6.1.3 Private Key Delivery to Certificate Issuer

Public keys of a sub-CA to be certified are transmitted to the Trust Center (certificate issuer) for certificate generation in the form of a signed PKCS#10 request.

6.1.4 CA Public Key Delivery to Relying Parties

The public keys of the DT Security root CAs can be obtained both from the "ldap.telesec.de" LDAP server and from the Trust Center websites (the corresponding fingerprints are also published there) (see also Section 2).

6.1.5 Algorithm type and Key sizes

6.1.5.1 Root CA Certificates

The key size of the DT Security Root CA certificates is at least 2048 bits when using an RSA key and 384 bits when using an ECC key.

Applied hash algorithms are SHA-1[1], SHA-256 and SHA384ECDSA bits, see also section 7.1.3 and CP.

6.1.5.2 Subordinate CA Certificates

The key size of sub-CA certificates is at least 2048 bits for RSA keys and 256 bits for ECC keys.

Applied hash algorithm is at least SHA-256 bits.

6.1.5.3 Subscriber Certificates (EE)

No stipulation. This CPS does not cover the issuance of subscriber certificates.

6.1.6 Public Key Parameter Generation and Quality Checking

Public keys are generated in accordance with the stipulations of [CAB-BR].

The keys included in requests for sub CAs are checked in accordance with the relevant section of the stipulations of [CAB-BR].

6.1.7 Key Usage Purposes

Private root CA keys are used exclusively to sign sub-CA certificates, OCSP certificates, and revocation lists.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

DT Security has implemented physical, organizational, and procedural mechanisms to ensure the security of CA keys.

In the case of root CA and sub-CA certificates, the private keys are generated and stored on a hardware security module that has been security-checked. Keys can be backed up using high-quality multi-person backup techniques. The security plan regulates the details.

6.2.1 Cryptographic Module Standards and Controls

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

Throughout the entire life-cycle, the modules are protected against unauthorized tampering by technical and organizational measures.

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

DT Security has implemented technical, organizational, and procedural mechanisms that require the participation of several trusted and trained persons of the Trust Center to be able to carry out confidential cryptographic CA operations. The usage of the private key is protected by a divided authentication process. Every person involved in the process has secrets that only enable certain activities in their entirety.

[1] SHA-1 is restricted to not be used for issuing new Root CA certificates. It is only applicable for the still running Root CAs. Further information see CP, section 7.1.3.

6.2.3 Private Key Escrow

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

6.2.4 Private Key Backup

DT Security creates backup copies of the key material of the root CA certificates for restoration and disaster recovery purposes. These keys are stored in encrypted form within cryptographic hardware modules (HSM) and associated key storage devices.

The recovery of private keys is protected by a divided authentication process (trusted path authentication with key). Every person involved in the process has secrets that only enable activities in their entirety.

6.2.5 Private Key Archival

Root CA keys are destroyed when they reach the end of their validity periods. Keys are not archived.

The provisions of the deletion plan are implemented.

6.2.6 Private Key Transfer into or from a Cryptographic Module

DT Security generates root CA keys on cryptographic hardware modules (HSM). Copies of these keys are made for recovery and emergency purposes (see Sections 6.2.4 and 6.2.5). In this case the transfer between both modules takes place in encrypted form.

All work steps can only be performed and documented by authorized individuals and in accordance with the dual-control principle.

6.2.7 Private Key Storage on Cryptographic Module

DT Security stores root CA keys in secure form on approved and FIPS 140-2 level 3 evaluated cryptographic hardware security modules (HSM).

6.2.8 Activating Private Keys

Private Root CA Key Activation on Cryptographic Modules

The root CA keys are activated in a log by multiple persons (one person of roles TC-PV and RFK each).

TC-PV and RFK protect the activation data against loss, theft, modification, disclosure, and unauthorized use.

Private Sub-CA Key Activation on Cryptographic Modules

Private keys of sub-CA certificates are only available to the respective service.

End entity Key Activation on Cryptographic Modules

Private keys of end entities are not available.

6.2.9 Deactivating Private Keys

The private CA keys are deactivated by terminating the connection between HSM and the application. The deactivation is logged after actions (generation of keys, signing of revocation lists) have been completed.

6.2.10 Destroying Private Keys

Root CA keys are destroyed by deletion in the HSM and all backup tokens. The deletion is carried out and documented by multiple persons (two persons with different roles). Further use of the private key is therefore no longer possible.

6.2.11 Cryptographic Module Capabilites

The rating is based on the specified methods. FIPS 140-2/level 3 evaluated components are monitored for validity in accordance with NIST.

6.3 Other aspects of Key Pair Management

6.3.1 Public Key Archival

Public keys are archived in the form of the certificates generated.

Certificates are backed up and archived as part of the regular DT Security backup measures. Other procedures are defined in the individual agreements.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

OCSP certificates are valid for a maximum period of one (1) year.

6.4 Activation data

6.4.1 Activation data generation and installation

During generation and installation, the specifications of the CP were adhered to.

The activation data of the root CA keys is requested by the HSM. When assigning passwords, the dual-control principle is enforced by dividing the password into two halves. Each half is set by a person with the TC-PV and RFK role, respectively. In addition, activation requires the use of two different PED keys that are accessed separately by persons with the TC-PV and RFK roles.

6.4.2 Activation data protection

The persons involved (trusted roles) store their activation data protected from view in safes provided for this purpose.

6.4.3 Other aspects of activation data

Transfer of activation data

Activation data is transferred personally.

Destruction of activation data

As soon as the activation data is no longer required, it is securely deleted, shredded, or destroyed in specially marked containers for secure file disposal.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

DT Security ensures that the required systems are backed up in accordance with the security plan, depending on the protection requirements.

The root CA is operated offline, i.e., with no network connection.

6.5.2 Computer Security Rating

As part of the security plan, different threat analyses are carried out to test the effectiveness of all measures implemented.

The rating will be reviewed after each incident, but not later than once a year.

6.6 Life cycle Technical Controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

DT Security has implemented mechanisms and/or guidelines to be able to control and monitor the configuration of its CA systems. The integrity is manually verified prior to installation.

6.6.3 Life cycle security controls

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

By sealing the hardware and carrying out software checks, any tampering or attempted tampering can be detected with every action or audit.

6.7 Network Security Controls

The following network security measures are implemented:

- Directory services and OCSP responder
    - The directory services and OCSP responders accessible from the Internet are separated from the internal networks by firewalls.
    - Vulnerability scans are performed at regular intervals. Further details are described in Section 5.4.8.
- Security-critical components
    - The security-critical components and systems (e.g., CA, DB, Signer, HSM) are only wired directly in the rack and completely isolated from the network.

6.8 Time-stamping

The time source is manually synchronized on the offline system.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

The root CA 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.

Certificate profiles for CA and subscriber certificates are defined in detail in the CPS of the respective certification authority.

The serial numbers are generated using a cryptographically secure random number generator. They are greater than zero and have at least 64 bit entropy.

7.1.1 Version Number(s)

Root CA certificates are issued in accordance with the international X.509 standard (version 3).

7.1.2 Certificate Content and Extensions; Application of RFC 5280

7.1.2.1 Root CA Certificate

The certificate extensions of the Root CA and Sub-CA certificates comply with the CP requirements.

7.1.2.2 Subordinate CA Certificafe

The certificate extensions of the Root CA and Sub-CA certificates comply with the CP requirements.

7.1.2.3 Subscriber Certificate

No stipulation.

7.1.2.4 All Certificates

All additional fields are being realized in accordance to [RFC 5280].

7.1.2.5 Application of RFC 5280

All additional fields are being realized in accordance to [RFC 5280].

7.1.3 Algorithm Object Identifiers

The following signature algorithms are used in root CA certificates:

- SHA256 RSA (OID 1.2.840.113549.1.1.11)
- SHA384 ECDSA (OID 1.2.840.10045.4.3.3)

SHA-1 hash algorithm is no longer used for new Root-CA certificates. Currently valid Root-CA certificates may use them until their validity time expires, see also [CA-BR, v.1.6.7]

7.1.4 Name Forms

The name forms of Root-CA are compliant with the CP.

7.1.4.1 Issuer Information

No stipulation.

7.1.4.2 Subject Information – Subscriber Certificates

No stipulation.

7.1.4.2.1 Subject Alternative Name Extension

No stipulation.

7.1.4.2.2 Subject Distinguished Name Fields

No stipulation.

7.1.4.3 Subject Information – Root Certificates and Subordinate CA Certificates

7.1.4.3.1 Subject Distinguished Name Fields

For the Root-CA the name forms are compliant to the certificate policy.

7.1.5 Name Constraints

The name constraints of Root CA are compliant with the CP.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifiers

The included Root CA certificates do not contain certificate policies.

See CP, section 7.1.6.1

7.1.6.2 Root CA Certificates

The certificate policies for underlying Sub-CA certificates are defined in the CPS or the respective services.

7.1.6.3 Subordinate CA Certificates

No stipulation.

7.1.6.4 Subscriber Certificates

No stipulation.

7.1.7 Usage of Policy Constraints extension

The policy constraints extension is not being used for Root CA certificates.

7.1.8 Policy Qualifiers Syntax and Semantics

Policy Qualifiers are not being used for Root CA certificates.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The certificate policies extension is not being used for Root CA certificates.

7.2 CRL Profile

7.2.1 Version number(s)

The revocation lists issued by DT Security 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)

7.2.2 CRL and CRL entry extensions

7.2.2.1 "Authority Key Identifier" (AuthorityKeyIdentifier) extension

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

7.2.2.2 "Revocation list number" extension

The revocation lists contain the "revocation list number" 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 is used in accordance with [RFC 6960]

7.3.2 OCSP extensions

No OCSP extensions are used.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The root CAs are certified conform to the policies ETSI TS 102 042 (since June 2018 ETSI EN 319 411-1). This is reviewed on an annual basis. The compliance audit of the root CAs is scheduled in context of the sub-CAs certification process. The assignment is indicated on the http://www.telesec.de/de/trust-center website under the published certificates.

Since no tasks of the root CA are performed by third parties, no regulations and checks at third parties are necessary.

8.1 Frequency or circumstances of assessment

In accordance with the requirements, a certification audit and an internal audit take place at least once a year.

8.2 Identity / qualification of assessor

For the determination of ETSI compliance, an accredited inspection authority is commissioned for the audit and an accredited certification authority for certification. Internal audits are carried out by the trusted role of "internal auditor," who is appropriately qualified (CISA and/or Lead Auditor ISO 27001).

8.3 Assessor's relationship to assessed entity

The ETSI compliance audit is carried out in accordance with ISO/IEC 17021 and meets the requirements for the auditor's relationship with the inspecting authority stated therein. With regards to the internal auditor, a role exclusion applies to all other roles of the unit to be audited.

8.4 Topics covered by assessment

The audit covers the complete scope of the ETSI EN 319 411-1 standard. According to ETSI EN 319 411-1 Section 4.4, this includes the complete CA operation including the components registration service, certificate generation service, dissemination service, revocation management service, revocation status service, and subject device provision service.

8.5 Actions taken as a result of deficiency

If defects or faults are detected during an audit by the accredited inspection authority, these are evaluated and, depending on the evaluation, immediate measures must be initiated or within certain deadlines. The Head of Trust Center decides relevant measures in cooperation with the inspection authority. The Head of the Trust Center, represented by the IT security officer, is responsible for updating and implementing the action plan.

8.6 Communication of results

The certification documents will be communicated by the accredited inspection authority to the management of the DT Security CAs and will be published on the website of the Trust Center: https://www.telesec.de/de/trust-center

The audit reports of the inspection authority on which the certification is based are not published. The requirements and the result of the audit are published in an annex to the certification document.

8.7 Self-Audits

Trust Center executes internal self-audits in regular intervals to check the conformity of the CP/CPS against formal requirements such as e.g. [CA-BR].

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

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

9.1.1 Certificate issuance or renewal fees

DT Security is entitled to charge for issuing, renewing, and managing certificates. Prices are governed by the certification authority's General Terms and Conditions (AGB) applicable to the relevant service or by individual agreement.

9.1.2 Certificate access fees

DT Security does not charge for access to certificates in the directory service.

9.1.3 Revocation or status information access fees

DT Security does not charge for access to revocation or status information for the relevant parts that fall under the scope of this document.

9.1.4 Fees for other services

DT Security does not charge for access to this document and the associated simple viewing.

Any other usage, e.g., reproduction, amendment, or production of a derived document is subject to prior written consent of the authority (Sections 1.5.1, 9.5) that holds the copyright.

The use of this document is also free of charge if it serves as a further applicable contractual document for the contractual relationship between the customer and DT Security.

9.1.5 Refund policy

DT Security reimburses charges in accordance with the legal regulations under German law. Detailed provisions can be found in the General Terms and Conditions (AGB).

9.2 Financial responsibility

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

9.2.1 Insurance coverage

DT Security has business liability insurance and D&O liability insurance cover. It is guaranteed that the requirements regarding insurance cover are fulfilled.

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

Data of legal persons and organizations as subscribers is recorded and verified to an extent as is required for issuing the sub-CA certificates and to guarantee that these certificates can be trusted.

Personal information is protected in accordance with the German Federal Data Protection Act (Bundesdatenschutzgesetz). Personal data is only made available to third parties if this becomes necessary as a result of legal requirements.

9.3.1 Scope of confidential information

Confidential information is any information from parties involved in PKIs (see Sections 1.3.2 and 1.3.3), which is not covered by Section 9.3.2.

9.3.2 Information not within the scope of confidential information

Non-confidential information is any implicit and explicit information that is included in issued certificates, revocation lists, and status information or can be derived from these.

9.3.3 Responsibility to protect confidential information

DT Security, as PKI service provider, is responsible for the protection of confidential information and compliance with data protection provisions.

9.4 Privacy of personal information

Personal data of certificate holders is recorded and verified to an extent as is required for issuing the subscriber certificates and to guarantee that these certificates can be trusted.

As part of the data review, only the identity of the subscriber is determined but not his trustworthiness, credit rating, or credit worthiness.

Personal information is protected in accordance with the Federal Data Protection Act and § 14 of the German Digital Signature Act (Signaturgesetz). Personal data is only made available to third parties if this becomes necessary as a result of legal requirements.

9.4.1 Privacy plan

DT Security adheres to the requirements of the privacy plan for DT Security PKI. Excerpts from the privacy plan can be provided upon request.

9.4.2 Information treated as private

The same regulations as in Section 9.3.1 apply to personal data.

9.4.3 Information not deemed private

The same regulations as in Section 9.3.2 apply to personal data.

9.4.4 Responsibility to protect private information

The same regulations as in Section 9.3.3 apply to personal data.

9.4.5 Notice and consent to use private information

The certificate applicant consents to the use of personal data by a CA or RA insofar as it is necessary for service provision purposes. Furthermore, all data may be published that is not treated as confidential in accordance with Section 9.4.3.

9.4.6 Disclosure pursuant to judicial or administrative process

The obligation not to disclose confidential information or personal data does not apply if disclosure of such information/data has been ordered by force of law or by a court ruling or an administrative authority or serves to implement legal judgments. As soon as there is reason to institute legal or official proceedings, which could lead to confidential or private information being disclosed, the contracting party involved in the proceedings will inform the other contracting party about this, taking into account the legal provisions.

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 DT Security. Intellectual property rights to the certificates and the ARL remain with DT 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

DT Security commits to the following:

- That certificates do not include any false statements that are known to or originate from the registration authorities that approve the certificate application or issue the certificate
- That the certificates do not contain any errors made by the staff of the registration authorities that approve the certificate application or issue the certificate and which can be attributed to improper or careless certificate issuance and management
- That all certificates comply with the requirements of this document
- That the revocation functions and the use of the CA database (directory service, OCSP responder) fulfill all the essential requirements of the applicable CP/CPS

Furthermore, the Trust Center guarantees that, at the time a SSL/TLS certificate is issued:

1. A defined procedure is in place to ensure that the applicant has the right to use the domains and/or IP addresses named in the certificate. Alternatively, that he has a relevant power of attorney that was issued by a person or an organization that has the right to this use
2. The procedure described under 1) is followed and
3. The procedure described under 1) is specified in detail in this CP/CPS
4. A defined procedure is followed to ensure that the subscriber (subject) named in the certificate has approved the issuing of the certificate and that the applicant's representative is authorized to make the request
5. The procedure described under 4) is followed and

6. The procedure described under 4) is specified in detail in this CP/CPS
7. A defined procedure is followed to check that, except for the OU field, all the information contained in the certificate is correct in the subject DN
8. The procedure described under 7) is followed and
9. The procedure described under 7) is specified in detail in this CP/CPS
10. A defined procedure is followed to minimize the probability that the OU field of the subject DN contains misleading information
11. The procedure described under 10) is followed and
12. The procedure described under 10) is specified in detail in this CP/CPS

In addition, the Trust Center guarantees that, in the event that the SSL/TLS certificate to be issued contains information regarding the subscriber's identity:

13. A defined procedure to check the provided identity is followed, which meets the requirements of the version of the [BR], Sections 9.2.4 and 11.2, valid at the time the certificate is issued
14. The procedure described under 13) is followed and
15. The procedure described under 13) is specified in detail in this CP/CPS

The Trust Center additionally guarantees that:

16. If the subscriber is a group company (affiliate), the applicant's representative must accept the "General Terms of Use" before issuing a certificate
17. If the subscriber is not a group company (affiliate), the applicant agrees the "General Terms and Conditions" with DT Security in a legally enforceable form
18. It operates a publicly accessible directory that contains status information regarding all certificates that have not expired (valid or revoked). This directory is available around the clock, 365 days a year
19. The issued certificates will be revoked in the event of all reasons listed in the [CAB-BR]

9.6.2 RA Representations and Warranties

All registration authorities commit to the following:

- Not to include any essentially false statements in certificates that are known to or originate from the registration authorities that approve the certificate application or issue the certificate
- That the certificates do not contain any errors made by the staff of the registration authorities that approve the certificate application or issue the certificate and which can be attributed to improper or careless certificate issuance and management
- To bear the legal consequences arising from the non-fulfillment of the obligations described.
- That all certificates fulfill the essential requirements of this document

9.6.3 Subscriber Representations and Warranties

No stipulation.

9.6.4 Relying Party Representations and Warranties

Relying parties must have sufficient information and knowledge to be able to evaluate the handling of certificates and their validation. The relying party is responsible for its own decisions regarding whether the information provided is reliable and trustworthy.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of warranties

The disclaimer of warranties is regulated in the applicable General Terms and Conditions (AGB).

9.8 Limitations of liability

The certification authority will have unlimited liability for damage arising out of injury to life, limb, or health, and damage resulting from willful breaches of obligations. Apart from that, liability for damage resulting from a breach of obligations due to negligence will be governed by the General Terms and Conditions (AGB) or by individual agreement.

9.9 Indemnities

Compensation is regulated in the applicable General Terms and Conditions (AGB).

9.9.1 Indemnification by CAs

Compensation is regulated in the applicable General Terms and Conditions (AGB).

9.9.2 Indemnification by Subscribers

Compensation is regulated in the applicable General Terms and Conditions (AGB).

9.9.3 Indemnification by Relying Parties

Compensation is regulated in the applicable General Terms and Conditions (AGB).

9.10Term and termination

9.10.1 Term

This document becomes effective upon publication on the DT 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.

9.11Individual notices and communications with participants

Unless otherwise contractually agreed, the up-to-date contact details (address, e-mail, etc.) for individual messages will be given to the certification authority.

9.12Amendments

In order to respond to changing market requirements, security requirements and legislation, etc., DT Security reserves the right to amend or adjust this document.

9.12.1 Procedure for amendment

Amendments to the CP/CPS can only be made by the Change Advisory Board. With every official change, this document receives a new ascending version number and publication date.

Amendments enter into force immediately upon publication (see also Section 2.3).

Updated versions result in the previous document versions becoming invalid. In the event of contradictory provisions, the Change Advisory Board will decide on how to proceed.

9.12.2 Notification mechanisms and period

Subordinate certification authorities will be notified of amendments and are given the opportunity to object within six weeks. If no objections are made, the new document version enters into force after the end of this period. Any claims beyond this for individual end users to be notified are explicitly excluded.

If the Change Advisory Board believes that significant (e.g., security-relevant) amendments are required immediately, the new CP/CPS will enter into force immediately upon its release (see Section 9.12.1).

9.12.3 Circumstances under which OID must be changed

There are no separate regulations.

9.13Dispute resolution provisions

In the event of disputes, the parties shall come to an agreement considering any applicable laws, regulations, and agreements made.

9.14Governing law

The law of the Federal Republic of Germany shall apply.

9.15Compliance with applicable law

The present document is subject to the applicable German laws, regulations, guidelines, ordinances, acts, and orders, in particular the import and export provisions for security components described therein (software, hardware, or technical information). Applicable mandatory laws, regulations, guidelines, ordinances, acts, and orders result in the corresponding provisions of the present document becoming invalid.

9.16Miscellaneous provisions

9.16.1 Entire agreement

Not applicable.

9.16.2 Assignment

Not applicable.

9.16.3 Severability

Should any provision of this CPS 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.

9.17Other provisions

No stipulation.