Deutsche Telekom Security GmbH
CPS TeleSec ServerPass

Public

Version: 18.00

Valid from: Nov. 29, 2021

Status: release

Last review: Nov. 18, 2021

Publication details

Table 1: Publication details

Details	Characteristic
Published by	Deutsche Telekom Security GmbH Trust Center & ID-Solutions, Chapter Trust Center Products Untere Industriestrasse 20, 57250 Netphen, Germany
File name	CPS_TeleSec_ServerPass_EN_V18.00.final.docx
Valid from	Nov. 29, 2021
Title	CPS TeleSec ServerPass
Version	18.00
Last review	Nov. 18, 2021
Status	release
Author	Telekom Security
Contents reviewed by	Telekom Security
Approved by	Telekom Security
Organizational unit involved	Telekom Security Trust Center & ID Solutions
Point of contact	Telekom Security Head of Trust Center Operations
Brief description	Certification practice statement (CPS)

Change history

Version	Last revised	Editor	Changes/comments
1.0	Nov. 28, 2000	DB	Initial version
2.0	Sep. 1, 2001	LE	Inclusion of new items
3.0	Nov. 11, 2003	LE	Certificate hierarchy update, content revision, layout changes
3.4	May 4, 2007	LE	Layout adaptation, update of Section 14
Products TeleSec ServerPass Standard and TeleSec ServerPass EV (Extended Validation) merged, thereby combining them in a new CP/CPS document.			
1.0	Apr. 14, 2010	LEI, SK, UV	Replaces CPS_ServerPass_V3.4 and CPS_ServerPass_EV_V1.0 Structure in line with RFC3647, all sections revised and contents updated accordingly, layout adaptation.
2.0	Jul. 1, 2013	UV; MG, LE	The entire document has been revised and extended, and further details have been added
3.0	Mar. 25, 2015	UV, LE, MB, ME	The entire document has been revised, updated and extended, and further details have been added QA and release
4.0	Apr. 14, 2016	LE, MB, LR ME, AT	Revised and updated as part of a document review. QA and release
5.0	Apr. 19, 2017	LR, MB, LEI ME. AT	Extensions for eIDAS added, Section 6.1.5 updated, Section 4.2.3 added. Section 5.7.1 added, Sections 6.5.1 and 6.5.1.1 added, Section 6.1.1 and Section 5.4.8 added, Section 1.3.1 added, EV added to EV SAN, Section 4.11 added. QA and release
6.0	Mar. 28, 2018	AR	QA for release After release by ME
7.0	Apr. 13, 2018	LE	After release by ME
8.0	Aug. 2, 2018	GK	After release by ME
9.0	Oct. 11, 2018	DD	Release
10.00	Oct. 16, 2018	ME	Release
11.00	Jul. 17, 2019	ME	Release
12.00	Feb. 27, 2020	HH	Release
13.00	Jun. 4, 2020	HH	Release
14.00	Sep. 16, 2020	Telekom Security	Release
15.00	Feb. 12, 2021	Telekom Security	Release
15.01	Feb. 17, 2021	Telekom Security	Sections 3.2, 3.2.2.4.6, 3.2.2.4.18, 3.2.2.5.1, 3.2.5, 4.3.1, 4.6.3, 4.7.3, 4.7.11, 4.7.12, 9.6.3, and 9.6.4 updated.

15.02	Mar. 10, 2021	Telekom Security	Section 5.2.1 updated
15.03	Mar. 11, 2021	Telekom Security	Structural revision of the document. Changes to Sections 1.2, 5, 5.1, 5.1.1 to 5.1.7, 5.2.2 to 5.2.4, 5.5.1, 6.7, 7.1.6.3, 7.2.0, 7.2.2.3, 7.2.2.4, and 12
15.04	Apr. 8, 2021	Telekom Security	Changes to Sections 4.2.2, 4.9.1.2, and 6.6.2
15.05	Apr. 23, 2021	Telekom Security	Changes to Sections 1.5.2, 4.9.7, 4.9.12, 4.10.2, 6.1.5, 6.1.6, 7.1.3, 7.1.3.1, and 7.1.3.2. Publication details amended. Tables revised.
15.06	Apr. 28, 2021	Telekom Security	Changes to Sections 3.2.2.4.18, 4.9.5, 9.2.1, and 12
15.07	May 11, 2021	Telekom Security	CPS translated from German to English.
16.00	May 11, 2021	Telekom Security	Release
16.01	September 6, 2021	Telekom Security	Changes to Sections 3.2.2.4.18, 4.4.2, 4.4.4
16.02	September 21, 2021	Telekom Security	Changes to Section 4.3.1
16.03	September 22, 2021	Telekom Security	Changes to Section 7.1.4.2.1., 7.1.4.2.2
16.04	September 22, 2021	Telekom Security	Last formal revision before approval
17.00	September 24, 2021	Telekom Security	Release
17.01	Nov. 17, 2021	Telekom Security	Changes to section 1.1.5, 3.2.2.4.18, 4.2.2, 5.5.2, 6.3.2 (table 3)
17.02	Nov. 18, 2021	Telekom Security	Changes to the description of table 8 to 12
18.00	Nov. 24,2021	Telekom Security	Release

Note: Refer to the preceding version to fully track changes.

Contents

List of figures

List of tables

1 INTRODUCTION

Deutsche Telekom AG has been operating a Trust Center (Telekom Trust Center) since 1994, which – in 1998 – became the first Trust Center in Germany to obtain approval for issuing certificates for digital signatures in accordance with the German Digital Signature Act (*Signaturgesetz* – *SigG*) at the time.

The Telekom Trust Center was operated by the Group unit T-Systems International GmbH and has been certified in accordance with ISO 9002 and ISO 9001:2000 since 1996 and January 2001, respectively.

Operations were transferred to Deutsche Telekom Security GmbH (hereinafter "DT Security GmbH") as part of a demerger as of July 1, 2020.

In addition to the precisely specified and certified operational processes, the Trust Center is characterized by a very high standard of security. The trustworthiness of the Trust Center personnel has been checked by the public authorities. All services are subject to regular quality controls. The technology used is state-of-the-art and is continuously monitored by trained administrators.

The Trust Center operates a series of different certification authorities under different roots for different electronic certificates. The certification authorities of the certificate services differ with regard to application contexts for certificates, specific designs of the technical interfaces, registration procedures, certificate profiles, processes in the event of revocations, as well as the publication of information.

1.1 Overview

TeleSec ServerPass is a PKI service operated in the Trust Center for issuing various X.509v3 server certificates. The unit specified in Section 1.5.1 is responsible for ensuring that the described workflows, activities, systems, roles, and security measures are also implemented if they are outsourced.

TeleSec ServerPass (SSL/TLS certificate) makes an internet/intranet server identifiable and links the organization's identity to it.

TeleSec ServerPass is composed of the verified information from the subscriber, the public key of the web server, data on the certificate issuer, and the signature of the Trust Center certification authority. The encryption option (SSL/TLS) ensures additional security of communication. The strength of encryption is based on the options of the server and the end user software (browser).

TeleSec ServerPass is offered in various product variants.

ServerPass certificates primarily serve the following purposes:

- Identifying the legal person (organization) that has a website under its control
- Encrypted communication with a website

1.1.1 TeleSec ServerPass Standard

The standard server certificate offers the features outlined above and contains precisely one FQDN, host name or an IP address, which can be resolved by a public DNS.

1.1.2 TeleSec ServerPass SAN/UCC

ServerPass SAN/UCC also fulfills the features outlined above and compared to ServerPass Standard offers the possibility to also fill additional SAN fields. It consists of:

- Basic package (6-pack): one (1) public FQDN (full domain name) or one (1) public IP address and up to 5 subdomains of the public domain or 5 multi-level subdomains of the public domain
- Additional public FQDN or other public IP addresses
- Additional subdomains of the public domains

1.1.3 TeleSec ServerPass EV

The TeleSec ServerPass EV (Extended Validation) product variant fulfills the above-mentioned general performance features and contains precisely one FQDN (host name), which can be resolved by a public DNS. Moreover, it offers additional security thanks to stricter issuance guidelines under [CABF-BREV] for example (see Section 10.2) and an enhanced registration process.

1.1.4 TeleSec ServerPass EV SAN

ServerPass EV SAN fulfills the general features outlined above and, compared to ServerPass EV, it offers the possibility to also fill additional SAN fields. It consists of:

- Basic package (5-pack): one (1) public FQDN (full domain name) and up to 4 subdomains of the public domain or 4 multi-level subdomains of the public domain
- Additional public FQDN
- Additional subdomains of the public domains

Other purposes of ServerPass EV are:

- Making phishing and fraudulent activities more difficult in connection with TLS/SSL certificates.
- Helping organizations to give their websites/web servers a clear identity.
- Supporting law enforcement agencies in their investigations into phishing and other online fraud cases, including contacting, investigating, or taking legal action against the subject, where appropriate.

1.1.5 eIDAS

All EV certificates with the flag "Qualified Website Certificate" meet the eIDAS requirements for EU-qualified certificates and the ETSI EN 319 411-2 policy for QCP-w. All these ServerPass EV certificates meet the requirements for qualified trust service providers (TSPs) or qualified trust services for website authentication in accordance with eIDAS Regulation (EU) No. 910/2014.

Websites that use Extended Validation certificates may be highlighted in color in some browsers. Depending on the web browser used, this can be done by means of a green address bar, a green font in the address field or such like. Additional information can be displayed concerning the validation.

When registering all ServerPass EV variants, the following facts are expressly **not** checked:

- That the organization named in the certificate is engaged in an active business activity.
- That the organization named in the certificate is conducting its business activity in conformity with the law.

- That the organization named in the certificate is conducting its business activity in a trustworthy, honest, or serious manner.
- That it is safe or not dangerous to conduct business with the organization named in the certificate.

It supplements the TeleSec ServerPass General Terms and Conditions [GT&C] by describing the issuance and management procedures for TeleSec ServerPass as part of the certification-based public key infrastructure (PKI).

The CPS allows the quality of the service to be assessed based on the existing descriptions.

This document is based on the international standard for certificate policies and certificate practice statements, the "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" [RFC3647] of the Internet Society (ISOC).

Some sections refer to the guidelines of the CA/Browser Forum set out in the EV SSL Certificate Guidelines [CABF-BREV].

Moreover, the ServerPass EV certificates correspond to the ETSI standard for web certificates [ETSI WEB].

1.1.6 Compliance with the baseline requirements of the CA/Browser Forum

The Trust Center ensures that sub-CAs used for TeleSec ServerPass comply with and fulfill the requirements and regulations of the published [CABF-BR] https://cabforum.org/baseline-requirements/ and [CABF-BREV] https://cabforum.org/extended-validation/ as amended. In the event that this document and the [CABF-BR] contradict one another, the regulations in the [CABF-BR] have priority.

1.1.7 Compliance with the comprehensive certification guideline of the Trust Center

The Trust Center assures that the requirements of the comprehensive certification guideline of the Telekom Security Trust Center ("Telekom Security CP" with the OID 1.3.6.1.4.1.7879.13.42) have been implemented or are being complied with for TeleSec ServerPass. The Telekom Security CP is published online at https://www.telesec.de/de/service/downloads/pki-repository/.

1.2 Document name and identification

This document is named "CPS TeleSec ServerPass."

The binding information on version, validity date, and status are listed on the cover sheet.

1.3 PKI participants

The following subsections will explicitly discuss the parties of the TeleSec ServerPass service involved in PKIs.

1.3.1 Certification authorities

The certification authority (CA) is the part of a public key infrastructure that issues and distributes certificates and provides checking options. Depending on the product variant or requirement, different root certification authorities (root-CAs) are available for TeleSec ServerPass. Requirements for the root CAs as well as the sub-CA certificates issued by the root CA can be referenced in the CP of the respective root CA.

Sub-CAs that no longer productively issue end-user certificates are still used for signing revocation lists and/or OCSP responses, insofar as this is required.

The certification authority provides root CA(s) for each product variant. The root CA and/or sub-CA may vary depending on the product variant. New trust anchors and sub-CAs may be offered or existing ones may be withdrawn from the market. This is due to changing national and/or international requirements, new security procedures, compromise of existing security procedures, or other reasons. Any resulting expenses that may arise on the customer side are not borne by the certification authority.

The root certificates currently in use offer great market penetration, compatibility, and flexibility. Security notices can be avoided by installing the subordinate certification authority certificate, so that the end entity is not irritated by any security notices requiring interpretation during the connection setup. An overview of all certification authorities used is provided in Section 7.1.2.9.

All components have been continually subject to the annual certifications required for issuance of certificates since 2008.

All TeleSec ServerPass sub-CAs issue end-entity certificates only and are used for signing revocation lists and/or OCSP responses. In particular, no sub-CA certificates are issued. Both the root certification authorities (root-CAs) and the subordinate certification authorities (sub-CAs) can vary owing to changing technical or other requirements. The validation model is based on the shell model, that is, each certificate is valid at the maximum for as long as the issuing certificate above it.

With TeleSec ServerPass, DT Security GmbH offers a PKI solution with an infrastructure that is installed in a Trust Center and operated by qualified personnel. All security-relevant actions are performed via an encrypted connection (HTTPS).

Various root certification authorities (root-CAs) are available for TeleSec ServerPass. These can be selected during the request process. An overview of the certification authorities is provided in the figures below. The scope of this document includes the sub-CAs contained in the red dashed areas and certificates from these figures.

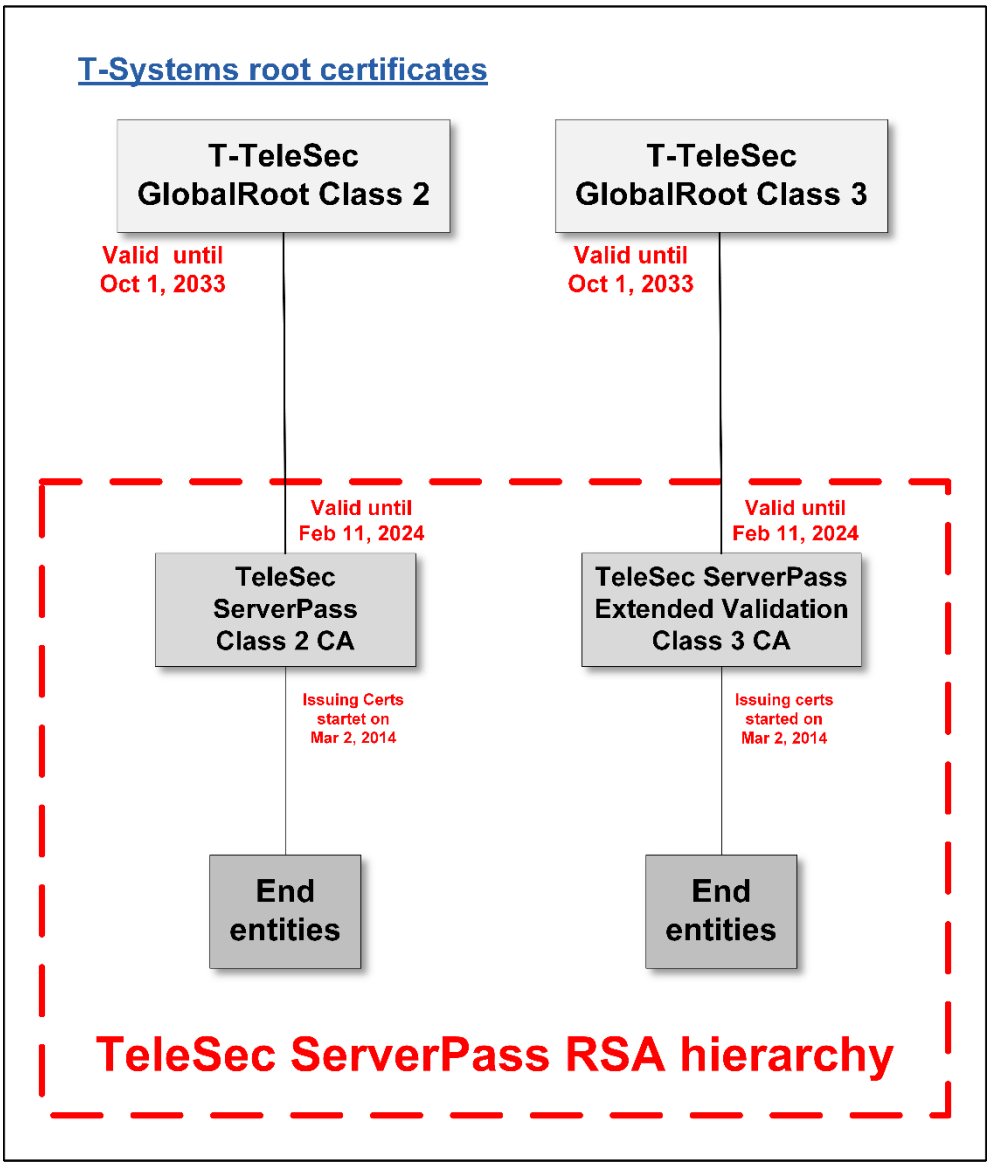

Figure 1: Overview of RSA certificate hierarchies for TeleSec ServerPass

Both the root certification authority (class 3 root-CA) and its subordinate certification authority (sub-CA) are operated in compliance with the currently applicable guidelines for the issuance and management of Extended Validation certificates ("Guidelines"), which are published at http://www.cabforum.org. If there is a discrepancy between this document and the Guidelines, the Guidelines shall prevail.

1.3.2 Registration authorities

A registration authority (RA) is an authority that carries out the identification and authentication of customers, processes certificate requests (approves, rejects, resubmits) or processes or forwards revocation requests.

In principle, a registration authority must ensure that no unauthorized person or machine gains possession of a certificate.

The Trust Center registration authority performs the following tasks, in particular:

- Accepting requests and checking identification documents
- Checking documents for authenticity and completeness
- Identifying the legal person (see Section 3.2)

  - Organization check
  - Identity check
  - Domain check
  - Authorization check
- Approving certificate issuance
- Revoking certificates if reasons for revocation exist (see Section 4.9)

No third-party registration authorities (external RAs) are permitted to register TeleSec ServerPass certificates.

TeleSec ServerPass EV/EV SAN:

For the product variant TeleSec ServerPass EV/EV SAN, the registration authority acts strictly in accordance with the EV Guidelines of the CA/Browser Forum [CABF-BREV] when carrying out the above tasks.

1.3.3 End entity

End entities are understood to be all certificate users to whom a certificate can be issued.

Certificates are only issued to legal persons (e.g., foundations under civil law, corporations under private law such as stock corporations, registered associations, limited liability companies, or registered cooperatives).

1.3.4 Relying parties

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

Relying parties also include software manufacturers who integrate TeleSec ServerPass root and sub-CA certificates into the certificate store, for example.

1.3.5 Other participants

For TeleSec Server pass, no functions and/or tasks are outsourced to external authorities (delegated third party) that relate to the operation of the CA infrastructure as well as the verification, approval, processing. or management of certificates or certificate requests.

1.4 Certificate usage

1.4.1 Permitted certificate uses

TeleSec ServerPass certificates must only be used within the permitted and legally valid framework. This applies particularly to the relevant country-specific import and export provisions.

The certification authority only issues certificates for legal persons.

Purpose of TLS/SSL certificates

Table 2: Use of certificates for legal persons

	Encryption	Authentication	Secure online communication	Test level
TeleSec ServerPass Standard	Yes	Yes	Yes	Medium
TeleSec ServerPass SAN/UCC	Yes	Yes	Yes	Medium
TeleSec ServerPass EV/EV SAN (Extended Validation)	Yes	Yes	Yes	High

1.4.2 Prohibited certificate uses

TeleSec ServerPass and TeleSec ServerPass EV certificates are not intended for use or transmission, designed, or authorized for

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

End-entity certificates may only be used for the permitted purpose and not as a subordinate certification authority (sub-CA) or root certification authority (root-CA).

1.5 Administration of the document

1.5.1 Responsibility for the document

This document is published by

Deutsche Telekom Security GmbH
Trust Center & ID Solutions, Chapter Trust Center Products
Untere Industriestrasse 20
57250 Netphen
Germany

1.5.2 Contact information

Deutsche Telekom Security GmbH
Trust Center & ID Solutions, Chapter Trust Center Products
Untere Industriestrasse 20
57250 Netphen
Germany

Phone:+49 1805 268 204 (landlines EUR 0.14 per minute, mobile networks max. EUR 0.42 per minute))
Email: telesec_support@t-systems.com
Internet: https://www.telesec.de

For general inquiries, please use the following input channel:

https://www.telesec.de/de/service/kontakt/anfragemitteilung/.

Certificate misuse, key compromises, faulty or non-compliant certificates, other security-related certificate problems, or suspicion of such incidents can be reported at

https://www.telesec.de/de/service/kontakt/zertifikatsmissbrauch-melden/

or via FMB_Trust_Center_Rootprogram@t-systems.com

to Telekom Security. This should contain as much information as possible that helps to verify the problem. In the event of a compromise, this should include, for example, a CSR with commonName "Compromised Key" that is signed with the private key.

If necessary, Telekom Security will involve law enforcement and supervisory authorities. The entry of the report is deemed agreement that data can be passed on to authorities without further consent in such a case.

1.5.3 Department that decides whether this policy is compatible with the CP

Section 1.5.1 names the organization that is responsible for ensuring that this CPS or documents that supplement or are subordinate to this document are compatible with the Certificate Policy (CP).

1.5.4 CPS approval procedures

It is approved via a formal document release process.

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

1.6 Acronyms and definitions

Acronyms and term definitions are provided in Section 12.

2 RESPONSIBILITIES FOR PUBLICATIONS AND REPOSITORIES

2.1 Repositories

The Trust Center operates a directory service and a central data repository for the TeleSec ServerPass service and is responsible for the contents.

Extracts of these databases in prepared form provide the basis for publishing certificate information and certificate revocation lists (CRL) on the directory service or for providing the validation service (OCSP responder) with status information.

In addition, documents that are relevant to the public are made available in the form of a central data repository. This includes, in particular, the relevant CP/CPS documents of the certification authorities (root CAs and sub-CAs) involved. This directory is available around the clock. The downtime is a maximum of 1.5 days on a monthly average.

The Trust Center uses appropriate mechanisms to protect the central data repository against unauthorized manipulation attempts (add, delete, change).

2.2 Publication of certification information

The certification authority publishes certificate revocation lists (CRLs) at regular intervals. The certificate revocation lists contains certificates that were issued by a TeleSec ServerPass CA and then revoked before reaching the expiration date. Only certificates that are valid at the time of revocation are revoked.

Furthermore, the validation service (OCSP responder) is available, which can be accessed via the "Online Certificate Status Protocol" (OCSP) internet protocol and returns the status of X.509 certificates.

The latest ServerPass documents are published here:

https://www.telesec.de/de/service/downloads/pki-repository/

Explanation of the menu structure:

- The ServerPass CPS is located in the "Certificate Practice Statement (CPS) -> ServerPass" menu.
- The ServerPass PDS is located in the "PKI Disclosure Statement (PDS)" menu.
- The root CA certificates are located in the "Root CA Certificates" menu
- The ServerPass sub-CA certificates are located in the "Sub-CA Certificates -> ServerPass" menu.

Server certificates that contain a CT log entry (Section 4.4.2) are published via third-party log servers (e.g., Google).

In addition, test sites are run (e.g., for software developers) that display information about the status (valid, revoked, and expired) of a web server certificate depending on the root certification authority (root CA).

The following test sites are operated:

https://root-class2.test.telesec.de

https://root-class2-revoked.test.telesec.de

https://root-class2-expired.test.telesec.de

https://root-class3.test.telesec.de

https://root-class3-revoked.test.telesec.de

https://root-class3-expired.test.telesec.de

The above information is published on the website https://www.telesec.de/, tab "Root Programm > Informationen zu CA-Zertifikaten > Root-CA-Zertifikate" [Root Program > CA certificate information > Root CA certificates]. In addition, in the event of security-critical incidents, the subscribers are notified in writing, on the internet, or by email.

Changes to the information security policy are communicated to the assessment authorities/auditors (Section 8 et seq.) and/or the supervisory authority.

The certification authority offers a reverse search via the following link: https://www.telesec.de/de/root-programm/support/pki-service-ermitteln/. After uploading an end-entity certificate (binary or base64 encoded), the following information is displayed:

- Issuer (Issuer DN)
- Subject (Subject DN)
- Certificate serial number
- Valid-from date
- Valid-to date
- Length of the public key (bit)
- Signature algorithm
- Link to Certification Practice Statement (CPS)
- Link to the ServerPass Services and Terms of Use
- Link to the TeleSec-Server Pass General Terms and Conditions [GT&C]
- Link to Terms of Use
- Link to the PKI Disclosure Statement
- Link to the CA certificates

Note: The reverse search is currently only supported by the following browsers (full versions): Microsoft Edge, Mozilla Firefox, and Google Chrome.

2.3 Updating the information (point in time, frequency)

Updates to the CPS are published as described in Section 9.12.

This CPS undergoes an annual review, 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 is noted in the change history of the CPS. This also applies in the event that no changes are made to contents. Current developments, amendments, and changed requirements (for example by CABF-BR) are tracked and considered in the release planning.

The revocation list and the OCSP responses are published as described in Section 4.9.7.

2.4 Access to the repositories and information services

Access to the revocation lists (CRL, ARL) and the OCSP service is not subject to any access control for end entities (Section 1.3.3) or relying parties (Section 1.3.4). Read access to this information is not restricted.

The integrity and authenticity of revocation lists and OCSP information are ensured by digitally signing with trusted signatories (Section 4.10.1).

Subscribers and users also have unrestricted read access to information from the CA and root-CA (see Section 2.2) via the relevant websites. The same applies to the directory of the published CPS.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming conventions

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.

Within a certificate, a distinction should be made between the following:

- IssuerDistinguishedName (Issuer DN)
- SubjectDistinguishedName (Subject DN)

All subject information must be entered in one language throughout – either in German or in the English translation.

3.1.1 Name forms

The certificate subscriber's identity is checked for all SSL/TLS certificates to be issued. The relevant information is transferred to the certificate.

At least the following mandatory fields must be completed:

- organizationName O (organization)
- localityName L (locality/city)
- countryName C (country)
- stateOrProvinceName ST (federal state/region/province) (EV/EV SAN only)

The above fields go through a database-supported consistency check. Discrepancies are clearly indicated. To enable correction of these discrepancies without generating a new request, these fields can be changed manually by the customer. However, the certificate issued with these changed fields then no longer corresponds to the data of the original request. There may be applications and constellations (e.g., Microsoft IIS) where problems occur during the installation (import) of the certificate. It is therefore recommended to use a new certificate request for this order instead of the correction.

No domain validated certificates (DV) are issued.

With the exception of the subject:organizationalUnitName (OU) field, only information that has been checked for correctness (accuracy and completeness) is entered in a subject field.

It is not permitted to use "meta characters" such as "-" or "." or " " (space) to signal that a field is not populated with subscriber information or is not relevant (n/a).

3.1.1.1 TeleSec ServerPass Standard and SAN/UCC: conventions for name components

The English terms used below are also commonly used in Germany today.

3.1.1.1.1 SubjectAlternativeName (mandatory field)

The SubjectAlternativeName extension must contain at least one entry. If the certificate request does not contain the SubjectAlternativeName extension, the CommonName of the certification authority is entered in the first SAN field. This is the SubjectCommonName in the case of TeleSec ServerPass. The entry is usually either a DNS name in the form of the FQDN (Fully Qualified Domain Name) or a public IP address.

As of June 1, 2013, the certification authority will no longer issue a certificate that contains an IP address/top-level domain from a reserved address space or an internal server/host name in the SubjectAlternativeName or SubjectCommonName field.

SAN fields may only contain the following characters: A-Z, a-z, 0-9, . (period), * (asterisk), - (hyphen).

TeleSec ServerPass Standard, -SAN/UCC: entries containing the placeholder "*" (asterisk) as a wildcard are permitted. Certain combinations of wildcard characters and characters and/or letters (e.g., h*l.example.com) as well as more than one wildcard character (e.g., *.*.example.com) per FQDN are not accepted.

The following conventions are defined for the subject DN.

3.1.1.1.2 OrganizationName (O) (mandatory field)

This field contains the organization name (e.g., company, institution, authority) of the subscriber. The organization name in the certificate should have the official spelling of the organization, i.e., it should be identical to the respective entry in the register (commercial register or similar). The official abbreviation/acronym may also be used. In addition, the official spelling of the legal form may be deviated from if a common abbreviation is used. It is not mandatory to indicate the legal form. Example: O=Sample limited liability company, O=Sample GmbH, or O=Sample company. The attribute "O" may be specified only once.

The certification authority verifies this information during the registration process based on the extract from the commercial register or equivalent, reliable directories/documents. Minor deviations in the spelling of the organization name can be accepted as long as the organization name is still unique (O=Alpha-Company AG or O=Alpha Company AG).

The certification authority will ask the subject to make a correction or document the accepted deviation from the official company name.

3.1.1.1.3 OrganizationalUnitName (OU) (optional)

This field is **optional** and contains an organization, unit (department, area) or a division/subdivision or group, team. If OU fields are used, it must be ensured that a link to the organization (O) can be established. The attribute "OU" may be specified several times.

Example: OU1=Procurement, OU2=Sample city branch

If information is provided in this field, it will be verified in the course of the registration process. Confusing, misleading, or ambiguous information is not permitted. The certification authority will refuse to issue the certificate if a check is not possible or can only be carried out with great difficulty.

3.1.1.1.4 CommonName (CN) mandatory input (optional)

If this field exists, it has to contain an individual FQDN (Fully Qualified Domain Name), in other words the complete name of a publicly resolvable domain or an individual public IP address of a subjectAltName extension field.

The use of an IP address/top-level domain from a reserved address space or an internal server/host name or an IP address from a reserved address space in the extensions:subjectAltName extension or in the subject:commonName field is not permitted.

Example: CN=www.example.de

The common name may contain the following characters: A-Z, a-z, 0-9, . (period), * (asterisk), - (hyphen).

The wildcard character (* asterisk) is only accepted on the far left in the FQDN. Certain combinations of wildcard characters and characters and/or letters (e.g., h*l.example.com) as well as more than one wildcard character (e.g., *.*.example.com) per FQDN are not accepted.

3.1.1.1.5 LocalityName (L) (mandatory field)

This field contains the name of the city in which the organization (e.g., company, institution, authority) is based. The full, official place name must be used.

If the place name exists several times in one country, uniqueness must be additionally ensured by:

- the zip code = postalCode,

- and/or the federal state = StateOrProvinceName (ST)

Example: L=Frankfurt am Main, L=Frankfurt (Oder)

The certification authority checks these details as part of the address in the course of the registration process on the basis of the commercial register excerpt "HR Auszug" or equivalent, reliable directories/documents. Verifiable evidence of a location different from the above document is also acceptable.

3.1.1.1.6 StateOrProvinceName (ST) (optional)

This field contains the federal state or province where the organization (e.g., company, institution, authority) is based. The spelling of the federal states in accordance with ISO 3166-2 (with and without country code) is accepted.

For the federal states of North Rhine-Westphalia (NRW) and Rhineland-Palatinate (RLP), the common abbreviation given in brackets may also be used. For the federal states of Bavaria, Saxony, and Thuringia, the designation "Freistaat " may be prefixed.

Example: ST=NRW or ST=Freistaat Bayern (Free State of Bavaria)

In the course of the registration process, this information is checked as part of the address on the basis of the commercial register excerpt "HR excerpt" or equivalent, reliable directories/documents. Verifiable evidence of a location different from the above document is also acceptable.

3.1.1.1.7 Country Name (C) (mandatory field)

This mandatory attribute contains the international country code. This is a code made up of two capital letters, which is specified in ISO 3166-1, Alpha-2 (International Organization for Standardization). This field specifies the country where the subscriber is located.

Example: C=DE

For more information please see:

http://www.unece.org/cefact/locode/subdivisions.html

http://www.nationsonline.org/oneworld/country_code_list.htm

In the course of the registration process, this information is checked as part of the address on the basis of the commercial register excerpt "HR excerpt" or equivalent, reliable directories/documents. Verifiable evidence of a location different from the above document is also acceptable.

3.1.1.1.8 StreetAddress (optional)

This field contains the name of the street where the organization (e.g., company, institution, authority) is based.

Example: streetaddress=Hauptstrasse 17 [17 High Street]

In the course of the registration process, this information is checked as part of the address on the basis of the commercial register excerpt "HR excerpt" or equivalent, reliable directories/documents. Verifiable evidence of a location different from the above document is also acceptable.

3.1.1.1.9 PostalCode (optional)

This field contains the postal code/zip code of the city in which the organization (e.g., company, institution, authority) is based.

Example: postalcode=12345

The certification authority checks these details as part of the address in the course of the registration process on the basis of the commercial register excerpt "HR Auszug" or equivalent, reliable directories/documents. Verifiable evidence of a location different from the above document is also acceptable.

3.1.1.1.10 EmailAddress (E) (optional)

Data from the EmailAddress field is ignored and not included in the certificate.

3.1.1.2 TeleSec ServerPass EV/EV SAN: conventions for name components

3.1.1.2.1 SubjectAlternativeName (mandatory field)

The SubjectAlternativeName extension must contain at least one entry. If the certificate request does not contain the SubjectAlternativeName extension, the CommonName is entered in the first SAN field. This is the SubjectCommonName in the case of TeleSec ServerPass. The entry is usually a DNS name in the form of the FQDN (Fully Qualified Domain Name).

SAN fields may only contain the following characters: A-Z, a-z, 0-9, . (period), - (hyphen). Entries containing the placeholder "*" (asterisk) as a wildcard are not permitted.

3.1.1.2.2 OrganizationName (O) (mandatory field)

This field contains the organization name (e.g., company, institution, authority) of the subscriber. The organization name in the certificate should have the official spelling of the organization, i.e., it should be identical to the respective entry in the register (commercial register or similar). The official abbreviation/acronym may also be used. In addition, the official spelling of the legal form may be deviated from if a common abbreviation is used. It is not mandatory to indicate the legal form. Example: O=Sample limited liability company, O=Sample GmbH, or O=Sample company. The attribute "O" may be specified only once.

The certification authority verifies this information during the registration process based on the extract from the commercial register or equivalent, reliable directories/documents. Minor

deviations in the spelling of the organization name can be accepted as long as the organization name is still unique (O=Alpha-Company AG, O=Alpha Company AG).

The certification authority will ask the subject to make a correction or document the accepted deviation from the official company name.

3.1.1.2.3 OrganizationalUnitName (OU) (optional)

This field contains an organization, unit (department, area) or division/subdivision or group, team. If OU fields are used, it must be ensured that a link to the organization (O) can be established. Confusing or ambiguous information is not permitted.

Example: OU1=Procurement

If information is provided in this field, the registration authority will check and verify it in the course of the registration process. The certification authority will refuse to issue the EV/EV SAN certificate if a check is not possible or can only be carried out with great difficulty.

3.1.1.2.4 CommonName (CN) (optional)

If this field exists, it has to contain an individual FQDN (Fully Qualified Domain Name), in other words the complete name of a publicly resolvable domain of a subjectAltName extension field.

The use of internal server names or IP addresses in the extensions:subjectAltName extension or in the subject:commonName field is not permitted for EV/EV SAN certificates.

Example: CN=www.sampledomain.de

Entries containing the placeholder "*" (asterisk) as a wildcard are not permitted.

The certification authority will check this information as well as the ownership relationships in the course of the registration process, using publicly accessible directories.

3.1.1.2.5 LocalityName (L) (mandatory field)

This field contains the name of the city where the organization has its registered place of business. The full, official place name must be used. Abbreviations, as well as other spellings or additions are not allowed.

Example: L=Frankfurt am Main, L=Frankfurt (Oder)

The certification authority checks these details as part of the address in the course of the registration process on the basis of the commercial register excerpt "HR Auszug" or equivalent, reliable directories/documents. Verifiable evidence of a location different from the above document is also acceptable.

3.1.1.2.6 StateOrProvinceName (ST) (mandatory field)

This is field and contains the state or province where the organization has its registered place of business. The spelling of the federal states in accordance with ISO 3166-2 (with and without country code) is accepted.

For the federal states of North Rhine-Westphalia (NRW) and Rhineland-Palatinate (RLP), the common abbreviation given in brackets may also be used. For the federal states of Bavaria, Saxony, and Thuringia, the designation "Freistaat " may be prefixed.

Example: ST=North Rhine-Westphalia

The certification authority checks these details as part of the address in the course of the registration process on the basis of the commercial register excerpt "HR Auszug" or equivalent, reliable directories/documents. Verifiable evidence of a location different from the above document is also acceptable.

3.1.1.2.7 CountryName (C) (mandatory field)

This field contains the name of the country in which the subscriber has its registered place of business. This is a code made up of two capital letters, which is specified in ISO 3166-1, Alpha-2 (International Organization for Standardization).

Example: C=DE

For more information please see:

http://www.unece.org/cefact/locode/subdivisions.html

http://www.nationsonline.org/oneworld/country_code_list.htm

The certification authority checks these details as part of the address in the course of the registration process on the basis of the commercial register excerpt "HR Auszug" or equivalent, reliable directories/documents. Verifiable evidence of a location different from the above document is also acceptable.

3.1.1.2.8 StreetAddress (street) (optional)

This field is **optional** and contains the name of the street where the organization has its registered place of business.

Example: streetaddress=Hauptstrasse 17 [17 High Street]

The certification authority checks these details as part of the address in the course of the registration process on the basis of the commercial register excerpt "HR Auszug" or equivalent, reliable directories/documents. Verifiable evidence of a location different from the above document is also acceptable.

3.1.1.2.9 PostalCode (optional)

This field is **optional** and contains the postal/zip code of the city where the organization has its registered place of business.

Example: postalcode=12345

The certification authority checks these details as part of the address in the course of the registration process on the basis of the commercial register excerpt "HR Auszug" or equivalent, reliable directories/documents. Verifiable evidence of a location different from the above document is also acceptable.

3.1.1.2.10 Business Category (mandatory field)

This **EV/EV SAN-specific** field provides information on the business category. The correct value of this field is set by the certification authority based on the specified business category.

Example: businessCategory=Private organization

The business category is checked by the certification authority in the course of the registration process.

3.1.1.2.11 Jurisdiction of Incorporation or Registration (mandatory fields)

These **EV/EV SAN-specific** fields (according to the classifications stated below) provide information on the address of the competent district court or register court. Specifically, this is:

- jurisdictionOfIncorporationLocalityName
- jurisdictionOfIncorporationStateOrProvinceName
- jurisdictionOfIncorporationCountryName

These fields only contain information at the level of the registering authority.

For example, the place of jurisdiction for a registering authority at national level contains information about the country, but not the federal state/province and city. The place of jurisdiction for a registering authority on a federal state/province level contains information about the country, but not the federal state/province and city. A register court at city/district level would contain all three pieces of information. In the simplest case (register court at national level), it is imperative to give the country name.

The country name is given as a code made up of two letters, which is specified in ISO 3166-1, Alpha-2 (International Organization for Standardization).

Examples:

- jurisdictionOfIncorporationLocalityName=Sample locality
- jurisdictionOfIncorporationStateOrProvinceName=Sample province
- jurisdictionOfIncorporationCountryName=SC (Sample country)

3.1.1.2.12 Registration Number (mandatory field)

This **EV/EV SAN-specific** field contains the unique registration number. In the event that no registration number is/was issued, this field must contain the date of registration in the format as specified in ISO 8601: YYYY-MM-DD. The details in the Registration Number field are stored in the certificate subject in the SERIALNUMBER field.

Examples: SERIALNUMBER=HRB 3244

SERIALNUMBER=2005-10-23

3.1.1.2.13 EmailAddress (E) (optional)

Data from the EmailAddress field is ignored and not included in the certificate.

3.1.2 Need for names to be meaningful

End entity and CA certificates must contain names in the subject of the certificate with a conventional meaning, based on which the organization's identity can be established.

The name must identify the end entity or organization in a clear and verifiable way.

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation. No certificates with pseudonyms or anonymous certificates are issued.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

The certification authority ensures that certificates for different customers but with the same subjectDN are differentiated by assigning a serial number in the subjectDN (see Section 7.1.10).

A customer can own several certificates with the same unique subjectDN. These differ in their certificate serial number.

3.1.6 Recognition, authentication, and role of brand names

It is the responsibility of the end entity to ensure that the choice of name does not infringe any trademarks, brand names, trademark rights, etc., or intellectual property rights. The certification authority TeleSec ServerPass is not obligated to check such rights. Any resulting claims for damages are at the expense of the end customer.

3.2 Identity checks for new requests

The new request can only be made after successful registration in the <myServerPass> service portal.

Only the proofs necessary for verifying the identity are required.

3.2.1 Method to prove possession of private key

When making a request, the customer must prove to the certification authority in a suitable manner that it owns the private key that is mapped to the public key to be certified. Proof of ownership is provided by the PKCS#10 method.

3.2.2 Authentication of the organization and domain identity

All request information must be verified by at least one of the following checks. A list of information on the registration authorities used to meet EV verification requirements is published in the online repository (https://www.telesec.de/de/service/downloads/pki-repository/) under "Validation Resources."

For EV certificate requests with QC statement (QWAC, QCP-w) the following applies: by signing, the customer's representative confirms the connection to the FQDN(s) specified in the request.

3.2.2.1 Identity

Subject identity information is verified by at least one of the following methods:

1. A public authority in the territory of the lawful establishment, existence, or recognition of the customer (e.g., https://www.handelsregister.de or https://handelsregister.ch)

2. A third-party database that is regularly updated and considered a reliable data source (Bisnode Deutschland GmbH: D&B Credit - https://credit.dnb.com/login)

3. A site visit by the CA or a third party acting as agent for the CA

4. A letter of confirmation

3.2.2.2 Company name/trade name

If the subject identity information includes a company name or trade name, the CA verifies the customer's right to use the name/trade name applying at least one of the following methods:

1. Documentation submitted by a public authority in the territory of the lawful establishment, existence, or recognition of the customer or documented by communication with such an authority (e.g., https://www.handelsregister.de or https://handelsregister.ch)

2. A reliable data source (Bisnode Deutschland GmbH: D&B Credit - https://credit.dnb.com/login),

3. Communication with a government agency responsible for managing such companies or trade names

4. A letter of confirmation accompanied by supporting documents

5. A utility bill, bank statement, credit card statement, tax document issued by the state, or any other form of identification that the CA determines to be reliable

3.2.2.3 Verifying the country code

The country associated with the subject in the subject:countryName field will be verified by the CA using one of the following methods:
1. The allocation of the IP address space by the country to (i) the IP address of the website, as specified by the DNS entry for the website, or (ii) the IP address of the customer
2. The ccTLD of the requested domain name
3. Information provided by the domain name registrar
4. A method identified in Section 3.2.2.1

3.2.2.4 Checking the authorization or control of the domain

For each fully qualified domain name (FQDN), the certification authority confirms that the customer (or the customer's parent company, subsidiary, or affiliate, collectively referred to in this section as "customer") is either the domain name registrant or has control over the FQDN on the date that the certificate is issued.

At least one of the following methods is used to check the domain control over all domain names contained in the certificate request.

3.2.2.4.1 Checking whether the customer is the domain contact

No stipulation.

3.2.2.4.2 Contacting the domain contact by email, fax, SMS, or letter post

The domain contact is contacted by email, fax, text message, or letter with a unique, one-time, random value that the domain contact must confirm by email, fax, SMS, or letter. The domain name registrar requests the required contact data. (Procedure in accordance with Section 3.2.2.4.2 of the [CABF-BR]). The following rules apply:

- An email, fax, SMS, or mail item can confirm the authorization for several authorization domain names.
- The email, fax, SMS, or mail item created can be sent to several recipients provided that the registrar of the domain name has listed these recipients as representatives of the registrar of the domain name for the FQDN to be validated.
- The random value sent my email, fax, SMS, or mail item is for one-time use.

- An email, fax, SMS, or mail item can be resent, including reuse of the random value. This requires that the entire content and the recipients remain unchanged.
- The random value remains valid for use in a confirmation response for a maximum of 30 days following creation.

As soon as the FQDN is validated using these methods, certificates can also be created for other FQDNs that end with all labels from the validated FQDN.

This method is also used for validating wild card domain names.

3.2.2.4.3 Contacting the domain contact by phone

No stipulation.

3.2.2.4.4 Constructed email to domain contact

To confirm that the customer has control over the domain, an email is sent to one or more addresses using the prefix 'admin', 'administrator,' 'webmaster,' 'hostmaster,' or 'postmaster,' followed by the "at" symbol ("@"), followed by the domain name of the FQDN to be checked. The response email must include the random value. (Procedure in accordance with Section 3.2.2.4.4 of the [CABF-BR]). The following rules apply:

- Every email can confirm the authorization for several FQDNs provided the authorization domain name used in the email is an authorization domain name for every FQDN that is confirmed.
- The random value is unique in every email.
- The email may only be resent in its entirety, including re-use of the random value, provided the entire content and the recipients remain unchanged.
- The random value remains valid for use in a confirmation response for a maximum of 30 days following creation.

As soon as the FQDN is validated using these methods, certificates can also be created for other FQDNs that end with all labels from the validated FQDN.

This method is also used for validating wild card domain names.

3.2.2.4.5 Domain proxy

No stipulation.

3.2.2.4.6 Agreed change on the website

No stipulation.

3.2.2.4.7 Change in DNS

With this validation procedure, domain control is demonstrated by the targeted insertion of unique information in the DNS:

- A unique, constructed random value is used.
- The random value is valid for a maximum of 30 days after it has been created.
- The recipient inserts the random value in the DNS of the FQDN to be checked.

As soon as the FQDN is validated using these methods, certificates can also be created for other FQDNs that end with all labels from the validated FQDN.

This method is also used for validating wild card domain names. (Procedure in accordance with Section 3.2.2.4.7 of the [CABF-BR]).

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 Validation of the subject as the domain contact

Validation of the subject verifies that the subject is the domain contact for the requested FQDN. This method can only be used if the certification authority is also the domain name registrar or an affiliate of the registrar of the main domain name.

Note: once the fully qualified domain name has been validated using this method, the CA can also issue certificates for other fully qualified domain names that end with all the identifiers of the validated fully qualified domain name. This method is suitable for validating wildcard domain names.

A contract with Deutsche Telekom AG's domain management (registrar) contains a list of specified domains owned by the Telekom Group that may be used by defined Group units. The requested FQDN of an internal customer is checked against this list.

In the case of internal requests from other Group units, the employee of the registrar arranges for Domain Management to confirm the customer as an authorized domain contact.

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 Telephone contact with domain contact

No stipulation.

3.2.2.4.16 Telephone contact with DNS-TXT telephone contact

No stipulation.

3.2.2.4.17 Telephone contact with DNS-CAA telephone contact

No stipulation.

3.2.2.4.18 Agreed change on the website – v2

Control over the FQDN is proven by checking whether the customer has placed a request token in the content of a file on the website. This is done by means of an HTTP request. The request token does not appear in this request.

The response is accepted if the HTTP response contains the status code 2xx.

The file that contains the request token

- is retrieved via the domain name used to authorize the FQDN and
- is read from the path "/.well-known/pki-validation/serverpassdv.txt," and
- is retrieved using either the "HTTPS" or "HTTP" scheme and port 443 or 80.

Redirects are tracked when

- they are initiated at the HTTP protocol level, and
- the HTTP response contains the status code 301, 302, 307 or 308, and
- the redirects lead to resource URLs that can be retrieved using the "HTTPS" or "HTTP" scheme and port 443 or 80.

The request token contains a timestamp, a unique random value and, if applicable, a reference number. The request token is valid for a maximum of 30 days after it has been created.

Certificates for other FQDNs that end with all the labels of the validated FQDN are not issued unless the CA performs a separate HTTP or HTTPS validation for each FQDN.

This method is not suitable for validating wildcard domain names.

3.2.2.4.19 Agreed change on the website – ACME

No stipulation.

3.2.2.4.20 TLS using ALPN (Application-Layer Protocol Negotiation)

No stipulation.

3.2.2.5 Checking the authorization or control of an IP address

This section describes the permitted processes and procedures for determining that the customer (or the customer's parent, subsidiary, or affiliate, collectively referred to as the "customer" for purposes of this section) owns or controls an IP address included in the certificate. Before a certificate is issued, a confirmation is sent to confirm that each included IP address has been verified using at least one of the following procedures.

It is verified that the customer owns or has control of each IP address listed in a certificate at the time the certificate is issued.

3.2.2.5.1 Agreed change on the website

It is verified whether the customer can prove practical control of the requested IP address by making an agreed change on the website. (Procedure in accordance with Section 3.2.2.5.1 of the [CABF-BR]).

For the verification, a certain unique text file must be placed under a specified path on the server (/.well-known/pki-validation/serverpassdv.txt).

- The certification authority must be able to access it via HTTP/HTTPS.
- A unique, constructed random value is used.
- The random value is valid for a maximum of 30 days after it has been created.
- The recipient inserts the random value at the defined position.

3.2.2.5.2 Email, fax, SMS, or letter to the IP address contact

The IP address contact is contacted by email, fax, text message, or letter with a unique, one-time, random value that the IP address contact must confirm by email, fax, SMS, or letter. The domain name registrar requests the required contact data. (Procedure in accordance with Section 3.2.2.5.2 of the [CABF-BR]).

The following rules apply:

- An email, fax, SMS, or mail item can confirm the authorization for several IP addresses.
- The email, fax, SMS, or mail item created can be sent to several recipients provided that the registration authority has listed this recipient for the IP address to be validated.
- The random value sent my email, fax, SMS, or mail item is for one-time use.
- An email, fax, SMS, or mail item can be resent, including reuse of the random value. This requires that the entire content and the recipients remain unchanged.
- The random value remains valid for use in a confirmation response for a maximum of 30 days following creation.

3.2.2.5.3 Reverse search for the IP address

Control over the IP address is confirmed by first finding an associated domain name using the reverse search and then verifying the search result using the permitted procedures from Section 3.2.2.4 (procedure in accordance with Section 3.2.2.5.3 of the [CABF-BR]).

3.2.2.5.4 Other methods

No stipulation.

3.2.2.5.5 Telephone contact with the IP address contact

During the phone call, the CA has the IP address contact confirm the certificate request for each IP address (procedure in accordance with Section 3.2.2.5.5 of the [CABF-BR]).

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 Verification of a wildcard domain

The wildcard character (* asterisk) is only accepted on the far left in the FQDN. Certain combinations of wildcard characters and characters and/or letters (e.g., h*l.example.com) as well as more than one wildcard character (e.g., *.*.example.com) per FQDN are not accepted.

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

3.2.2.7 Reliability of the data source

Only third-party data sources and databases that have been deemed sufficiently reliable are considered. No exclusively self-maintained data sources or data sources maintained by affiliated companies are used.

3.2.2.8 CAA records

See Sections 3.2.5.2 and 4.2.2.

3.2.3 Authenticating the identity of end entities

3.2.3.1 Organization review

3.2.3.1.1 TeleSec ServerPass Standard and SAN/UCC:

In order to confirm the legal person named in the subject Distinguished Name (subjectDN) of the certificate under Organization (O), the following document is required according to the type of legal person upon the initial request:

Legal person:

The request form signed by a signatory or by an authorized representative of the organization.

Authority:

The request form signed by an authorized representative of the authority and stamped with the official seal.

Association:

The certified copy (no more than 30 days old) of the register of associations excerpt must be submitted together with the signed request form.

Trader(s):

The certified copy (no more than 30 days old) of a current trade license and the personal ID of the trader must be submitted together with the signed request form.

The following is checked for all business categories:

- The information on the request form is identical to the information in the Certificate Signing Request (CSR) of the online request.
- The company name of the organization/company in the field O = OrganizationName matches the information on the organization and the entry in the electronic commercial register (for German organizations) or comparable directories (e.g., according to foreign jurisdiction, register of associations). Additional current organization documents may be needed (no more than 30 days old), which are issued by a competent authority and confirm the organization's existence (e.g., register of associations or comparable document, official stamp).
- The address of the organization specified in the certificate request is checked on the basis of the electronic commercial register or equivalent directories. The customer must operate a branch, business office, or such like at the specified location.
- The authorization of the responsible contact at the organization named in the request (legal person).
- If a third party carries out the certificate request/management on behalf of the organization, it must have a corresponding written authorization concerning the transfer of rights.

To verify the existence or address of the organization, other methods may be used as an alternative/in addition to the commercial register or equivalent directories. If required, a Dun & Bradstreet report can be used as a trusted, reliable, and independent source of data.

Another method permitted for verification is the submission of a legal statement issued by someone with the relevant qualification. Also, an employee of the registration authority or someone acting on its behalf may personally visit and confirm the specified location.

Additional checks are carried out as required.

3.2.3.1.2 TeleSec ServerPass EV/EV SAN:

The required checks are carried out in accordance with [CABF-BREV].

3.2.3.2 Identity check on a natural person

The customer for TeleSec ServerPass must be a legal person, i.e., no certificate is issued for a natural person.

3.2.4 Unverified entity information

The TeleSec ServerPass certificate does not contain any unverified information.

3.2.5 Authorization check

If the subject is not the certificate subscriber, the full name and authorization of the subject to act on behalf of the certificate subscriber is verified.

To avoid conflicts of interest, the TSP and the subject must be different entities. The only exception is the TSP itself if it orders TLS certificates for its own servers.

3.2.5.1 Ensuring the authenticity of the certificate request

3.2.5.1.1 TeleSec ServerPass Standard and SAN/UCC:

Every ServerPass customer enters into a contract for the relevant service with Deutsche Telekom Security GmbH. The customer representative who signs the contract is known by name to the Trust Center.

3.2.5.1.2 TeleSec ServerPass EV/EV SAN:

To verify the authenticity of the initial certificate request, a call is made to the customer's central telephone number, which is stored in the commercial register or an equivalent directory. The executing RA employee is put in contact with the customer representative named above. The customer representative confirms the authenticity of the certificate request, i.e., confirms that the requesting party is an authorized representative of the subject.

The authorization is checked in accordance with the EV Guidelines [ETSI EV].

3.2.5.1.3 TeleSec ServerPass EV/EV SAN with Q note (QWAC, QCP-w)

In addition to the checks described above, personal identification via POSTIDENT of a representative of the legal person is mandatory for issuing a qualified website certificate (QWAC, QCP-w).

3.2.5.2 Checking CAA entries in the DNS

As part of the authorization check, all FQDN records are checked against CAA records in the DNS immediately before the certificate is issued (Certification Authority Authorization; CAA Records for Fully Qualified Domain Names).

If one or more CAA resource records are found whose issue property or issuewild property does not contain "telesec.de", then the certificate request is rejected. If the issuewild property contains a semicolon (";"), then a wildcard certificate request is always rejected.

If no CAA resource record has been stored or its issue property or issuewild property contains "telesec.de," then the verification process continues.

8 CNAME chain records are processed and the length of the chain is limited to a maximum of 10 as recommended.

3.2.6 Criteria for interoperability

No stipulation.

3.3 Identity check and authentication in the event of re-certification

3.3.1 TeleSec ServerPass Standard and SAN/UCC:

Re-certification takes place exclusively in the service portal and can only be ordered by the authorized customer. The identity and authenticity are confirmed by means of the correct access data and the service password required for renewal.

The checks to be carried out (identity, address, authorization) correspond in principle to the initial request procedure (see Section 3.2.2). Existing documents and information can be drawn on here. It is not necessary for re-certification to either sign the renewal request or to send the request to the Trust Center. The request is simply printed to complete the customer's documentation.

3.3.2 TeleSec ServerPass EV/EV SAN:

Re-certification does not take place with ServerPass EV/EV SAN. Instead a new request is made in accordance with Section 3.2.2.

To validate a renewal request, the certification authority only uses documents, documentation, or other information not older than 13 months at the time the certificate is issued.

3.3.3 Identification and authentication for routine re-key

3.3.3.1 TeleSec ServerPass Standard and SAN/UCC:

The customer is responsible for routine generation of the key. The key can be renewed in the framework of renewing the certificate in the service portal and may only be requested by the authorized customer. The identity and authenticity are checked by means of the correct access data as well as the service password required for renewal.

3.3.3.2 TeleSec ServerPass EV/EV SAN:

There is no routine key renewal.

3.3.4 Identity check in the event of re-key following certificate revocation

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

3.4 Identification and authentication for revocation requests

Authorized end entities can revoke their certificates themselves via the <myServerPass> service portal.

After the certificate to be revoked has been selected, the revocation request must be confirmed and the revocation performed by entering the certificate service password.

In addition to an end entity generating a revocation request, the certification authority reserves the right to carry out certificate revocations in the event of misuse or suspected misuse (see also Sections 4.9.1.1, 4.9.2, and 4.9.3 et seq.).

The justified and intentional revocation of a certificate is final.

3.4.1 Revocation request on discovery of misuse

If the misuse of a Trust Center certificate is suspected, this can be reported to the service desk by giving the issuer CA and serial number of the certificate and by describing the nature of the misuse. These cases are forwarded to the Trust Center. Appropriate investigative measures are initiated. If the justified misuse of a certificate is confirmed, the certification authority can revoke this certificate.

The following input channels must be used for establishing contact to report certificate misuse:

Internet: https://www.telesec.de/de/service/kontakt/zertifikatsmissbrauch-melden/

Email: telesec_support@t-systems.com

4 OPERATIONAL REQUIREMENTS IN THE LIFECYCLE OF CERTIFICATES

4.1 Certificate request

4.1.1 Authorized customers

TeleSec ServerPass issues certificates only for legal persons (customers):

- Companies
- Public authorities
- Private organizations
- Non-business enterprises

These are, for example, foundations under civil law, corporations under private law such as stock corporations, registered associations, limited liability companies, registered cooperatives.

The customer must appoint the following roles:

- Contact in charge
  The contact in charge is authorized to act on behalf of the customer. Telekom Security is obliged to verify the contact in charge on the basis of the commercial register excerpt (HRA), or equivalent directories. If the contact in charge is not listed in the HRA, a corresponding power of attorney is required, which in turn must be signed by a person listed in the HRA.
- Technical contact
  This person is the point of contact for Telekom Security. They are authorized to order the certificate, download the issued certificate, and manage the certificate and the customer data. The technical contact can also be employed by an ISP or a hosting company. The authorization to represent the company must then be in the form of a power of attorney.
- Commercial contact
  This person is the addressee for billing and will be contacted if there are any billing-related problems.
- Agent (deputy of the technical contact):
  Agents can be created by the technical contact to assist them. Agents have the same permissions as the technical contact, except for the management of agents.
- Administrative contact (only for EV certificates)
  This person is authorized to act as the certificate approver. The certificate approver approves certificate requests created by the technical contact. The certificate approver can also take on the role of the technical contact or assign others to assume the role of technical contact. As part of the authentication process, Telekom Security will contact the certificate approver to verify the details of the certificate request and the authorization to represent the company. The authorization to represent the company must be in the form of a power of attorney.
- Authorized signatory contact (only for EV certificates)
  The authorized signatory contact corresponds to the contact in charge of EV certificates.

The customer may entrust one person with several of the listed roles.

4.1.2 Request process and responsibilities

4.1.2.1 End entity

The end entity (customer) must accept the Data Privacy Notes, the TeleSec ServerPass General Terms and Conditions [GT&C], the ServerPass Services and Terms of Use, the TeleSec ServerPass CPS, and the Service Specifications and Prices before submitting the request.

Furthermore, the end entity warrants

- that the statements made in the certificate request are true and correct;
- to generate a key pair or order its generation;
- to transmit its public key with its certificate data to the certification authority in PKCS#10 format for certificate generation.

Through this certificate request, the ServerPass customer (customer) enters into a contract with Deutsche Telekom Security GmbH for an end entity certificate. The agreements of the contract or the consent to the terms of use are repeated for each new request, renewal, or re-issue.

4.2 Processing of certificate requests

The following process description also applies to the TSP itself if it orders TLS certificates for its own servers.

4.2.1 Initial and one-time preparations

Every ServerPass customer initially enters into a contract for the relevant service with Deutsche Telekom Security GmbH.

4.2.1.1 Conditions

If the certificate subscriber and the issuing CA belong to a common legal person (affiliate), the subject's representative must accept the terms of use before a certificate is issued. If the certificate subscriber is not a Group company (commissioned third party or non-affiliate), the subject must consent to the TeleSec ServerPass General Terms and Conditions [GT&C] and the ServerPass Terms of Use in a legally enforceable form.

Both the Terms of Use and the TeleSec ServerPass General Terms and Conditions [GT&C] are managed in a corresponding electronic form in the ServerPass service portal.

The agreement of the subscription contract or the consent to the Terms of Use will be repeated for each new request, renewal, or re-issue.

4.2.1.2 Performing identification and authentication functions

To validate a request, the certification authority only uses documents, records, or other information not older than 13 months at the time a certificate is issued.

Denied List (blacklist)

The Trust Center maintains an internal database containing certificates that have been revoked in connection with phishing, misuse, or fraud attempts. This information is used to be able to identify future suspicious certificate requests.

High-risk list

The Trust Center maintains a database containing organizations as well as domain names or IP addresses that may become a target of phishing, misuse, or fraud attacks due to their attractiveness. These certificate requests are identified automatically to notify the registration employees to take particular care. This is to generate additional vigilance and attentiveness when checking request data. In individual cases, the verification process can have the effect that a requested certificate is not issued.

4.2.1.2.1 TeleSec ServerPass Standard and SAN/UCC:

The identification and authentication of the required end-entity information is performed by the certification authority in accordance with Section 3.2.

4.2.1.2.2 TeleSec ServerPass EV/EV SAN:

The identification and authentication of the required end entity information is performed by the certification authority.

4.2.2 Approval or rejection of certificate requests

If all the required checks from Section 3 are successfully completed, the certificate request is approved and the certificate is issued.

All FQDN entries are checked against CAA records in the DNS immediately before a certificate is issued. If no CAA resource record is stored or its issue property or issuewild property contains "telesec.de," the certificate is issued. "iodef" records are evaluated, but are not tracked further. Further entries of the CAA record are not supported.

A reference number is issued during the certificate request to provide a clear assignment of an issued certificate to the relevant request documents and additional documents (e.g., powers of attorney).

A certificate request must be rejected if:

- The request does not contain at least one fully qualified domain name or IP address that will be included in the SAN extension.
- The request contains an IP address/top-level domain from a reserved address space or an internal server/host name.
- The public key falls short of the RSA minimum length of 2,048 bits.
- The result of checking for Debian weakness is positive.
- A public key, which is already used for another ServerPass certificate, is to be used for a new request.
- A CAA resource record is found whose issue property or issuewild property does not contain "telesec.de."
- Not all required tests are successfully passed.

The Trust Center checks regularly (no more than every 30 days) on the ICANN website (https://newgtlds.icann.org) whether new gTLDs have been released or canceled. In the event of changes, the Trust Center checks to see whether certificates have been issued for this gTLD and stops further certificate issuance until control over the domain name or the customer's exclusive right to use the domain name has been proven.

If the request is delayed or rejected, the subscriber's authorized representative (technical contact) will be notified by email giving reasons.

4.2.3 Processing period for certificate requests

The certificate request is processed within a suitable period following receipt of the request.

4.3 Issue of certificates

4.3.1 CA activities during certificate issuance

The TSP ensures that integrity and authenticity are guaranteed when the certificates are issued. Technical, organizational, and personnel measures ensure the protection of data against forgery until the certificates are issued.

A reference number is issued during the certificate request to provide a clear assignment of an issued certificate to the relevant request documents and additional documents (e.g., powers of attorney).

By verifying the signature of a key that has been handed over by means of a signed PKCS#10 request, the TSP ensures that the customer is in possession of the keys or has control over them.

The end entity certificates are published as "pre-certificates" in a sufficiently large number of CT log servers (Certificate Transparency according to RFC 6962) before issuance. The time-stamped confirmations returned in this process is included in the certificates as an extension with the OID 1.3.6.1.4.1.11129.2.4.2.

TeleSec ServerPass uses Certificate Transparency for all certificates issued.

This ensures the security and transparency of the certificate issuing process. Details are available at https://www.certificate-transparency.org.

4.3.2 Notification of the end entity about the issuance of a certificate

The technical contact is notified about the issuance of the certificate by email. The issued certificate is listed in the <myServerPass> service portal under 'My certificates' and made available for download.

4.4 Certificate acceptance

4.4.1 Acceptance by the certificate subscriber

After the request data has been successfully checked, the certificate is generated. The request confirmation, with which the contract comes into force, is sent at the same time.

The end entity must check that the information contained in the certificate is correct before using it.

4.4.2 Publication of the certificate by the CA

No stipulation.

All certificates issued by the CA are published in several public Certificate Transparency (CT) log servers.

4.4.3 Notification of certificate issuance by the CA to other entities

The notification of other entities is not envisaged.

4.5 Key and certificate use

4.5.1 Use of the key pair and the certificate by the end entity

The certificate and the associated private key may only be used in accordance with the General Terms and Conditions TeleSec-ServerPass [GT&C], Services and Terms of Use, and the requirements of this CPS.

End entities must protect their private key against unauthorized access and may no longer use the private key once the validity period has run out or the certificate is revoked. The certificate may be used for authorized and legal purposes only, in accordance with this document.

4.5.2 Use of public keys and certificates by relying parties

Every relying party who uses a certificate issued by a TeleSec ServerPass sub-CA, should

- check that the certificate is valid before using it, by validating the entire certificate chain as far as the root certificate (certificate hierarchy) and checking the validity period and revocation information (CRL, OCSP) of the certificate, amongst other things,
- check the technical purpose of use, which is established via the "key usage" and "extended key usage" attributes shown in the certificate.

Relying parties must use appropriate software (e.g., current browser) to check certificates (validation) and the associated cryptographic procedures.

4.6 Renewal of certificates (re-certification)

4.6.1 TeleSec ServerPass Standard and SAN/UCC:

In order to ensure authentic and secure electronic communication at all times, a certificate must be renewed before it expires, meaning that only valid certificates can be renewed. Re-certification is based on the existing certificate data; it is not necessary to register again. In the event of re-certification, a new certificate is generated based on the same subjectDN (Section 3.1.1.1), with a new validity period and a new serial number. The customer can decide for itself whether a new public key of a newly generated key pair or the old key should continue to be used for the re-certification.

A prerequisite for continuing to use the old key pair is that the unique mapping of the certificate holder and the key is assured, the key is not compromised, and the cryptographic parameters (e.g., key length) are still sufficient for the period of validity of the new certificate.

4.6.2 Circumstance for re-certification

4.6.2.1 TeleSec ServerPass Standard and SAN/UCC:

Re-certification is possible at any time whilst the current certificate remains valid. Expired certificates cannot be renewed. The certificate that is no longer required must be revoked immediately.

4.6.2.2 TeleSec ServerPass EV/EV SAN:

Re-certification is not currently offered. Instead, a new request can be initiated in the <myServerPass> service portal as easily as a re-certification.

4.6.3 Circumstance for re-certification

See Section 4.1.1.

4.6.4 Processing of re-certification requests

The request for re-certification is checked and approved automatically following successful verification of all relevant data. The underlying documents and data must not be older than 13 months. In the course of this request, the customer must agree to the prevailing contractual terms and conditions (e.g., GT&C, service specifications, terms of use, etc.).

If the automated check is not successful, there will be no automated approval and manual processing will be carried out by the TSP.

4.6.5 Notification of new certificate issuance to certificate subscriber

See Section 4.3.2.

4.6.6 Acceptance of a re-certification

See Section 4.4.1.

4.6.7 Publication of the re-certification by the CA

See Section 4.4.2.

4.6.8 Notification of re-certification by the CA to other entities

See Section 4.4.3.

4.7 Re-certification with new key (re-keying)

TeleSec ServerPass Standard and SAN/UCC:

A new public key is used in the re-key process with the certificate request. The basic requirement for this is to generate a new key pair. The certificate content and identification data remain unchanged.

Whether a re-key for the application in use is possible or whether the "old" key pair and thus the "old" public key has to be reused, depends on the technical requirements of the application (e.g., web server) and is the responsibility of the customer.

A re-key can be requested when the certificate is being renewed (Section 4.6) and in case of a re-issue (Section 4.7.8).

4.7.1 Circumstance for certificate re-key

4.7.1.1 TeleSec ServerPass Standard and SAN/UCC:

Re-certification with re-key can be carried out at any time during the current certificate's period of validity and only by the authorized customer. The current certificate must not be revoked and not be invalid/expired.

4.7.1.2 TeleSec ServerPass EV/EV SAN:

A re-key is not currently offered.

4.7.2 Eligible subjects for re-issue

See Section 4.1.1.

4.7.3 Processing certificate re-keying requests

4.7.3.1 TeleSec ServerPass Standard and SAN/UCC:

When the authorized end customer has sent the re-key in the framework of the re-certificate or the certificate re-issue after entering the service password, the certificate is issued after successfully checking all relevant details. In the course of this request, the customer must agree to the prevailing contractual terms and conditions (e.g., GT&C, service specifications, terms of use, etc.).

If the automated check is not successful, there will be no automated approval and manual processing will be carried out by the TSP.

4.7.4 Notification of the end entity about the issuance of a renewed certificate

The regulations laid out in Section 4.3.2 apply.

4.7.5 Acceptance of a certificate re-issue with new key material

See Section 4.4.1.

4.7.6 Publication of re-issued certificates by the certification authority

The regulations laid out in Section 4.4.2 apply.

4.7.7 Notification of third parties about the issue of new certificates by the certification authority

The regulations laid out in Section 4.4.3 apply.

4.7.8 Re-issuing a certificate

4.7.8.1 TeleSec ServerPass Standard and SAN/UCC:

In order to support consistently authentic and secure electronic communication, the option is offered under certain circumstances to re-issue a certificate for the remaining term of the existing certificate.

Such a situation occurs, for example, if the private key is damaged, becomes unusable, has been inadvertently deleted, or no longer corresponds with the public key as a result of a defect on the web server or a work error. Cryptographic functions (signature, encryption) cannot be performed without the private key. This means that the certificate is also unusable.

A certificate re-issue can be requested under such circumstances based on the current identification data and with the same certificate content. A new certificate is generated based on the same subjectDN (Section 3.1.1.1), which has a new serial number and a new issue date but the expiration date of the preceding certificate. It is recommended to generate a new

key pair and use the new public key. The customer must revoke the certificate that is no longer in use immediately following activation of the new certificate.

A prerequisite for using the same key pair is that the unique mapping of the certificate subscriber and the key is assured, the key is not compromised, and the cryptographic procedures (e.g., key length) are still sufficient for the period of validity of the new certificate.

Whether a certificate re-issue for the application in use is possible and whether a new key pair and thus the "new" public key can be used, depends on the technical requirements of the application (e.g., web server) and is the responsibility of the customer.

4.7.8.2 TeleSec ServerPass EV/EV SAN:

The re-issue process is the same as for ServerPass Standard and SAN/UCC. The only exception is that a new key pair must always be used.

4.7.9 Conditions for re-issue

A certificate re-issue is possible at any time during the term of the current certificate. A certificate re-issue of a revoked, invalid, or expired certificate is not possible. The original certificate that has been issued by means of a re-issue cannot use the re-issue option again. The certificate that is no longer required must be revoked immediately by the customer.

The system monitors whether the certificate is revoked by the customer. After 30 days, a forced revocation is performed.

4.7.10 Who may request a re-issue?

The certificate re-issue is only ordered by registered and authorized persons. The authorized person has the required login details as well as the certificate service password.

4.7.11 Processing re-issues

The request for a re-issue is checked electronically and can be approved following successful verification of all relevant data. In the course of this request, the customer must agree to the prevailing contractual terms and conditions (e.g., GT&C, service specifications, terms of use, etc.).

4.7.12 Notification of the subscriber about the issuance of a re-issue certificate

The regulations in Section 4.3.2 apply.

4.7.13 Acceptance of the re-issue

4.7.13.1 TeleSec ServerPass Standard and SAN/UCC:

The regulations in Section 4.4.1 apply.

4.7.13.2 TeleSec ServerPass EV/EV SAN:

Re-issue is not currently offered.

4.7.14 Publication of the re-issue by the CA

The regulations in Section 4.4.2 apply.

4.7.15 Notification of other authorities about a re-issue by the CA

The regulations in Section 4.4.3 apply.

4.8 Amendment of certificate data

If certificate data in the existing certificate changes, the certificate must be requested again.

4.8.1 Conditions for a certificate change

It is absolutely necessary for a new certificate to be issued if the contents of the certificate (except for public keys) change or have changed.

4.8.2 Who may request a certificate change?

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.No stipulation.

4.8.5 Acceptance of a modified certificate

No stipulation.No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.No stipulation.

4.8.7 Notification of other authorities by the CA about a certificate issuance

No stipulation.No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for revoking an end-entity certificate

The following reasons require certificate revocation by the subscriber:

- The private key has been compromised, lost, stolen, or disclosed or there is strong suspicion that this has happened.
- The details in the certificate (except for unverified end-entity information) are no longer up to date, are invalid, incorrect, or do not correspond to the provisions of the naming convention (also refer to Section 3.1 et seq.). This also applies to domain names (e.g., generic top-level domains (gTLD) that are no longer owned by the domain owner or that have been withdrawn by authorized bodies (e.g., ICANN).
- The formerly internal top-level domain becomes a public top-level domain (collision of domain names).
- The certified key (public key) or the cryptographic algorithms used with it no longer meet current requirements.

- A case of misuse by the persons authorized to use the key has occurred or is suspected to have occurred.
- Legal requirements or court judgments
- The certificate is no longer required or the subscriber expressly requests the revocation of the certificate.

The certification authority revokes a certificate within 24 hours if at least one of the following conditions is met:

- The certificate subscriber or authorized representative submits the request for revocation in writing.
- The certificate subscriber or authorized representative notifies the certification authority that the underlying certificate request was not authorized and that the authorization will not be given retroactively.
- The certification authority has evidence that the certificate subscriber's private key has been compromised.
- The certification authority becomes aware that evidence of domain control for an FQDN or IP address cannot be trusted.
- The certification authority becomes aware that there is a method to easily calculate the private key that corresponds to a public key (comparable to the Debian weak key, http://wiki.debian.org).

An end entity certificate will be revoked, if possible within 24 hours but at the latest within five days, if one of the following reasons for revocation applies.

- The certificate no longer meets the requirements of Sections 6.1.5 and 6.1.6.
- The certification authority has evidence that the certificate has been misused.
- The certification authority becomes aware of one or more serious breaches of contract by the certificate holder.
- The certification authority becomes aware that the right to use an FQDN or an IP address has expired (e.g., a court forbids its use, a power of attorney expires, etc.).
- The certification authority becomes aware that a wildcard certificate is being used to authenticate a misleading subordinate FQDN that is being used fraudulently.
- The certification authority becomes aware of a relevant change in the certificate entries.
- The certification authority is informed that the certificate has not been issued in accordance with the rules as described in the requirements of the CA Browser Forum or the applicable CP or CPS.
- The certification authority determines that information in the certificate is incorrect or misleading.
- The certification authority ceases operations and has not made any arrangements for the revocation support to be continued by another CA in the event of cessation of operations.
- Proof of the CA's conformity with the CA Browser Forum has lost its validity. The need for revocation does not apply if the certification authority has taken precautions to ensure that the CRL and the OCSP service continue to be maintained and made available.
- The root TSP provides for revocation.
- From a technical point of view, the content or format of the certificate represents an unacceptable risk for application software manufacturers or relying parties, e.g., if the CA Browser Forum indicates such a risk and the certificate should therefore be revoked and replaced.
- There are statutory provisions, court judgments, or instructions from a supervisory authority.

4.9.1.1.1 TeleSec ServerPass EV/EV SAN:

In addition to these reasons, there are a number of specific reasons named in [CABF-BREV] which the certification authority records and logs accordingly:

- The EV/EV SAN certificate is not authorized. This means that, for example, it is later discovered that the EV/EV SAN certificate was issued under false pretenses.
- The terms of use were not complied with.
- The certificate violates the provisions and conditions with regard to the issuing of EV certificates.

4.9.1.2 Reasons for revocation of a sub-CA certificate

The certification authority initiates the revocation of a sub-CA certificate if

- the original certificate request was not authorized and cannot or should not be authorized retroactively;
- the private key of the sub-CA has been compromised or disclosed to an unauthorized person or an organization that is not associated with the sub-CA or no longer meets the requirements (see Sections 6.1.5 and 6.1.6);
- the certificate has been misused;
- the sub-CA certificate was not issued in conformity with the Trust Center CP or the TSP does not operate in conformity with the Trust Center CP;
- information in the certificate is incorrect or misleading;
- the operation of the sub-CA is discontinued and no arrangements have been made for the continuation of the revocation service;
- the sub-CA's right to issue certificates in accordance with the requirements of the trust center CP expires or is revoked or terminated and no arrangements have been made for the continued operation of the revocation services.

In addition, the certification authority may request the revocation of a sub-CA certificate without giving reasons.

4.9.2 Who can request a certificate to be revoked?

The following persons and institutions are authorized to initiate the revocation of a certificate:

- Authorized persons representing legal persons.
- Registration staff from the Trust Center.

The regulations in Section 3.4.1 apply in particular.

4.9.3 Revocation procedure

4.9.3.1 Revocation of end-entity certificates

A certificate is normally revoked by the end entity 7x24h in the <myServerPass> service portal via the <Revoke> action button. The revocation is authorized by the service password and is definitive. The subscriber is automatically informed by email about the revocation status.

The Trust Center reserves the right to revoke certificates at any time (24/7) if at least one of the reasons for revocation listed in Section 4.9.1.1 applies.

The Trust Center enables users, software manufacturers, or other third parties an option to report suspicions of compromised keys, certificate misuse, or other (attempted) fraud in relation to certificates.

The Trust Center begins investigating within 24 hours of receiving notification of suspected misuse in order to determine whether further measures are to be taken (such as revocation). Within these 24 hours, a first report of the facts and the results of the analysis will be prepared and given as feedback to the certificate subscriber and the person who reported the problem. Having inspected the facts and environmental parameters, the certification authority will discuss the analysis results with the certificate subscriber/authorized representative or the reporting person and decide to what extent a certificate revocation will be necessary In this context, the revocation date is determined.

The period between receipt of the certificate problem report or revocation request and the published revocation must not exceed the time limits for revocation required in Section 4.9.

The further procedure is determined based on the following criteria:

- The cause or nature of the problem (context, severity, impact, risk, or damage)
- The impact of a revocation (direct or shared impact on certificate subscribers and relying parties)
- The number of notifications about this certificate problem or from this certificate subscriber
- The entity that has entered the report (e.g., a report by a law enforcement agency is given higher priority)
- The relevant legislation

Through extremely precise problem reporting, the Trust Center is able to respond internally at any time and can decide whether it is necessary to involve a law enforcement agency or to revoke a certificate that is the subject of such a report.

4.9.4 Deadlines for a revocation request

As soon as there is a reason for revocation according to Section 4.9.1.1, the revocation request must be made as soon as possible within an economically suitable period.

4.9.5 Periods for processing of a revocation request by the CA

The revocation option is available to the end entity 24/7 and is passed on to the linked systems immediately after the revocation process in the <myServerPass> service portal. The OCSP service that uses these systems therefore also has access to the current certificate status.

The period between receipt of the revocation request and the published revocation must not exceed the time limits for revocation required in Section 4.9.

4.9.6 Checking methods for relying parties

Relying parties must be given the opportunity to check the status of certificates that they wish to rely on.

The OCSP service, which shows the current status of a server certificate, can be used for this purpose. Another method with which a relying party can check whether a certificate has been revoked is to check the current certificate revocation list (CRL) published in the directory service.

The revocation lists also include expired certificates (ExpiredCertsOnCRL).

4.9.7 Frequency of the publication of revocation information

The certificate revocation list (CRL) is published via the directory service, as described in Section 2.3.

The certificate revocation list (CRL), which contains the revoked certificates of end entities, is updated at least once a day or as required and published by the directory service. Regularly scheduled CRLs are issued before the time stored in the nextUpdate field of the previously issued CRL.

Before a sub-CA is decommissioned, a final CRL is created with a nextUpdate value that is after the time of the notAfter value of the associated CA certificate. This CRL is provided until the day following the expiration of the issuing CA certificate.

4.9.8 Maximum latency period of revocation lists

The latency period of the certificate revocation list (CRL) following automatic generation is a few minutes. The latency period for the certification authority revocation list (CARL/ARL) following manual publication is a few minutes.

4.9.9 Online availability of revocation/status information

In addition to the revocation information via the CRL and CARL/ARL, the certification authority provides online information regarding the certificate status via OCSP. OCSP responses for end-entity certificates issued by ServerPass correspond to the requirements from RFC 6960.

The URL of the OCSP responder is listed in the certificate under the "Authority Information Access" extension (see Section 7.1.2.9).

4.9.10 Requirements for an online checking process

Relying third parties must check the status of a certificate to find out whether a certificate that they wish to rely on is trustworthy. The OCSP service (OCSP responder) is available for requesting up-to-date status information.

The OCSP responses output for end entity certificates meet the specifications of RFC 6960.

The OCSP responder responds to requests for certificate serial numbers not issued by the TeleSec ServerPass service with "unknown." Furthermore, the OCSP responder monitors requests for "unused" certificate serial numbers.

The OSCP responder supports the HTTP GET method. The OCSP data source (repository) is synchronized every 10 minutes. The OCSP responses are valid for 5 days. Another way of checking the status is via the current certificate revocation list (CRL).

4.9.11 Other available forms of communicating revocation information

The technical contact is informed by email of the revocation of the certificate (revoke notification) in which the relevant certificate information is included.

4.9.12 Special requirements regarding private key compromise

If a private key is compromised, the relevant certificate must be revoked immediately.

Third parties wishing to report a key compromise are requested to use the contact options described in Section 1.5.2. Sufficient information or references to information proving the existence of a key compromise must be provided, e.g., a CSR with commonName "Compromised Key" signed with the compromised private key. The affected certificate itself should also be referenced.

4.9.13 Suspension of certificates

The suspension (temporary revocation) of certificates is not envisaged.

4.9.14 Who can request a certificate to be suspended?

No stipulation.No stipulation.

4.9.15 Procedure for suspension

No stipulation.No stipulation.

4.9.16 Limitation of the suspension period

No stipulation.No stipulation.

4.10 Status information services for certificates

The status of end entity certificates can be indicated via the OCSP service. Revoked certificates can also be identified via the certificate revocation list (CRL).

4.10.1 Operating characteristics

OCSP responses are signed by an OCSP responder, whose certificate is in turn signed by the ServerPass sub-CA that issued the end-entity certificate in question.

The OCSP responder's certificate contains the extension described in Section 7.3.1.

The OCSP response contains one of the following statuses:

- good means:
  - it is an issuer of the service and
  - the certificate is valid (within the certificate validity period) and
  - the certificate is not revoked.
- revoked means:
  - it is an issuer of the service and
  - the certificate is valid (within the certificate validity period) and
  - the certificate was revoked.
- unknown means:
  - the certificate is invalid (outside the certificate validity period) or
  - the certificate is valid but was not issued by the requested issuer of the service or
  - the certificate is valid but was not issued by the issuer of the service.

The certification authority has implemented mechanisms to protect the revocation status service (CRL, ARL, OCSP) against unauthorized attempts to prevent manipulation of revocation status information (add, delete, change).

OCSP stapling is not offered.

4.10.2 Availability of the service

The certificate status service is available 24/7. Under normal operating conditions, the response time of the OCSP responder is less than 3 seconds.

Measures have been taken to ensure that OCSP responders can generally operate without downtime (multiple redundancies, caching). In emergency scenarios, downtimes of up to one day are possible.

The revocation information for end-entity certificates is provided until the day following the expiration of the issuing CA certificate.

4.10.3 Additional features

No stipulation.

4.11 Ending the use of a certificate

If the use of a certificate is ended before the expiry date, the certificate must be revoked by the end entity.

4.12 Key storage and restoration

4.12.1 Guidelines and practices for key deposit and recovery

For the certification authority TeleSec ServerPass operated at the Trust Center, the key pair is stored on a security-checked hardware security module (HSM) and filed in a secure environment. The key material is only stored on further HSMs for back-up purposes, so that qualified staff (trusted role) at the Trust Center can restore and maintain the service. Key storage at third parties (e.g., trustee, notary) is not implemented.

4.12.2 Guidelines and practices for protecting and restoring session keys

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The Trust Center of Deutsche Telekom Security GmbH is within the scope of a security policy approved by management and an associated information security management system (ISMS), which is certified in accordance with ISO 27001.

The ISMS itself as well as other security policies, security concepts, and other documents ensure compliance with the requirements specified in the Telekom Security CP (Section 5). In particular, risk management comprises a risk analysis including probabilities of occurrence and extent of damage as well as appropriate risk treatment including final (residual) risk acceptance. The risk management processes are carried out at least annually and also as required.

5.1 Physical measures

Trust Center facilities, media, and information are protected against loss, theft, damage, or compromise by physical measures in accordance with their criticality. These measures are recorded in internal security policies and other documents.

5.1.1 Location and construction

The Trust Center's infrastructure is located in two geo-redundant data centers (a "twin-core data center") within Germany. The choice of locations, based on an appropriate risk analysis, took into account environmental conditions such as vulnerability to natural disasters and other sources of danger. The building's construction and infrastructure are designed for the secure operation of critical systems and meet the requirements for a high-security zone.

The areas relevant to the operation of the Trust Center are separated from all other areas by additional enclosures and are audited and certified in accordance with "Trusted Site Infrastructure TSI V3.2 Dual Site".

5.1.2 Physical access

The data centers have extensive physical security measures, including security personnel, secured entrances, intrusion detection systems, and multi-level access systems. In particular, the Trust Center premises are accessible only to authorized persons in trusted roles and visitors are permitted only when accompanied by such a person. Access rights are reviewed and adjusted as necessary on a regular basis and as needed.

5.1.3 Power supply and air conditioning

The data centers are equipped with redundant power supplies and air conditioning systems. The systems are protected against voltage fluctuations and are backed up by uninterruptible power supplies (short- and long-term bypasses) with cross-cabling.

5.1.4 Water exposure

The data centers are located outside the danger zone of floods or other sources of danger. In addition, the premises themselves are protected against water ingress or water damage by further measures.

5.1.5 Fire prevention and protection

The data centers are protected against fire damage with structural measures in accordance with the critical protection requirements and in accordance with applicable fire protection regulations.

5.1.6 Storage of media

Media is stored exclusively in the Trust Center's operating rooms, protected from fire and water exposure and unauthorized access. No media will be used for permanent or long-term storage or archiving.

5.1.7 Waste disposal

Confidential documents and storage media are disposed of securely and exclusively by certified disposal companies. In addition, all storage media are erased using certified processes before they are disposed of.

5.1.8 External backup

No provisions.

5.2 Organizational measures

The relevant requirements from [ETSI EN 319 401] Section 7.4 b, c, d, e are implemented.

5.2.1 Trusted roles

The TSP is organized based on the following trusted roles:

- Head of TSP: bears overall responsibility for the Trust Center services provided
- Information Security Officer: plans and supervises the implementation of security measures, is responsible for vulnerability scans and penetration tests, manages the ISMS
- ISMS team member: supports the information security officer in their tasks
- Administrator: configures and maintains the IT infrastructure (networks, databases, servers, and technically sets up access rights for RA staff, etc.)
- CA operator: generates CA keys and imports the CA certificates created
- Internal auditor: audits certificates, processes, and documentation on a regular basis and in the event of discrepancies, and assesses the conformity of key and root ceremonies
- Root program/compliance team (PKI): coordinates the implementation of requirements, monitors requirement sources (mailing lists, root store policies, ETSI), handles external communication with root store operators and "Bugzilla", advises on incidents and changes, is responsible for CP, and processes applications for CA issuances
- Order processor (RAOP): processing of certificate orders
- Crypto officer: expert for cryptographic topics
- Product manager: responsibility for lifecycle management of the TSP
- Technical product manager: requirements management and product testing

The above trusted individuals must meet the requirements specified in this CPS (see Section 5.3.1).

5.2.2 Number of persons required for a task

At least one representative is appointed for all roles listed in Section 5.2.1.

Technical and organizational measures have been established whereby security-relevant or security-critical activities are only performed by persons in trusted roles and only in accordance with the dual control principle. The number of employees performing such security-relevant or security-critical activities is kept to a minimum, taking into account substitution rules and work-related circumstances.

TeleSec ServerPass EV/EV SAN:

The dual control principle stipulated in the EV guidelines [CABF-BREV] for approval process of an EV/EV SAN certificate is implemented by the certification authority in line with the requirements. Technical means are in place to prevent circumvention of the dual control principle.

Furthermore, the SubjectDN information is checked for each request in accordance with the dual control principle.

5.2.3 Identification and authentication for each role

The identification of suitable persons to fill roles, the transfer of roles (authentication), as well as their withdrawal are carried out in accordance with a documented process, which includes, among other things, the clarification of the need or exclusion of conflicts of interest, the willingness of the person to take on the activities, management approval, and the documentation of evidence for this.

Prior to the transfer of a trusted role (or at the time of hiring an employee), the relevant person is personally identified by presenting official identification and acceptance is obtained from this person as well as from the Trust Center management concerning the transfer of the role, the associated responsibility, and the resulting duties to ensure security.

Roles are only transferred to individuals if this does not give rise to any conflicts of interest (see also Sections 5.2.1 and 5.2.4) and independence is maintained, i.e.,

- the areas of the Trust Center responsible for generating and revoking certificates are independent of other organizations in their decisions regarding the establishment, provision, maintenance, and suspension of services in accordance with the applicable certificate policies,
- all employees entrusted with the generation and revocation of certificates are free from financial or other pressures in the performance of their duties that could affect confidence in the services provided by the Trust Center. This applies to all employees in trusted roles as well as to senior managers and executives.

This structure, which ensures the impartiality of operations, is documented in the Trust Center's ISMS manual, among other documents.

Role owners are officially appointed to the trusted role by Trust Center management.

Role owners are advised that they may only act in the assigned role when performing tasks assigned to the role.

The assignment of required privileges is based on the "least privilege" principle, i.e., all privileges are limited to the minimum required.

After termination of employment of an employee in a trusted role, their access permissions are revoked within 24 hours.

5.2.4 Roles requiring separation of duties

The following roles are separated from each other:

- Management of the TSP
- IT security officer and/or internal auditor
- RAOP
- Administrator and/or CA operator.

To avoid conflicts of interest, the TSP and the subject must be different entities. The only exception is the TSP itself if it orders TLS certificates for its own servers.

5.3 Personnel-related measures

The Trust Center implements a comprehensive range of personnel-related security measures that ensure a high level of protection for their facilities and certification services. Only qualified and trained personnel may be deployed in the Trust Center, with security measures for personnel being defined in the security concept.

5.3.1 Required qualifications, experience, and security checks

Employees who are to assume a trusted role are required by the Trust Center to prove that they have the qualifications and experience necessary to fulfill their prospective work obligations in a competent and satisfactory manner.

A new police clearance certificate must be submitted to the personnel supervisor at regular intervals.

5.3.2 Security check

Before employment is taken up in a trusted role, the Trust Center carries out security checks that involve the following:

- Checking and confirming the previous work relationships
- Checking employment references
- Confirming the highest or most relevant educational/vocational qualification
- Police clearance certificate

If the requirements set out in this section cannot be fulfilled, the Trust Center will use another legally permitted method of ascertaining essentially the same information.

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 assessed by employees of the HR department and security personnel, who decide the appropriate subsequent course of action. The measures involved in the course of action can even lead to candidates for trusted positions having their employment offer withdrawn or to trusted persons being dismissed.

The use of information obtained in a security check in order to take such measures is governed by the applicable law.

5.3.3 Education and training requirements

The staff at the Trust Center undergo the training measures required to fulfill their work obligations in a competent and satisfactory manner. The Trust Center keeps records of these training measures.

The training programs are tailored toward the individual work areas and include, for example:

- Advanced PKI knowledge
- Procedures in accordance with ITIL
- Data privacy
- Data and telecommunications secrecy
- Information protection
- Access control
- Anti-corruption
- Security and operational policies and procedures of the DTAG Group
- Use and operation of the hardware and software deployed
- Reporting and handling of faults and compromises
- Procedures for disaster recovery and business continuity

Employees who are involved with validating certificate requests receive additional training in the following areas:

- Guidelines, procedures, and current developments regarding validation methods
- Contents and particularly relevant amendments to this CPS and the corresponding CP
- Relevant requirements and specifications from the certification standards

General threat and attack scenarios regarding the validation methods (e.g., social engineering)

5.3.4 Follow-up training intervals and requirements

Trust Center personnel receive refresher training and in-service training to the extent required but no later than after 12 months. The requirements are reviewed annually and incorporated into the training program.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions in the event of unauthorized activities

The certification authority reserves the right to punish unauthorized activities or other violations of this CPS and the procedures resulting therefrom and to take appropriate disciplinary measures. These disciplinary measures can extend to dismissal of the employee and are based on the frequency and severity of the unauthorized activities.

5.3.7 Requirements for independent contractors

The Trust Center reserves the right to use independent contractors or consultants to fill trusted positions. These persons are subject to the same functional and security criteria as employees of the Trust Center in comparable positions.

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

5.3.8 Documentation for the staff

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

5.4 Log events

What data and events are recorded by whom and at what intervals is defined in the logging concept as well as the installation manual. In addition, rules are laid down that govern how long the log data is stored (currently for six weeks) and how it is protected against loss and unauthorized access. The requirements under [ETSI EN TSP] Section 7.10 are implemented for this.

5.4.1 Type of events recorded

Generally, all log 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.

5.4.1.1 CA key pairs and CA systems

For the lifecycle management of CA key pairs or CA systems, the Trust Center logs at least the following events for TeleSec ServerPass:

a) Generation, destruction, storing, backup, and restoration as well as archiving of the key pair or parts of the key pair
b) Events in the lifecycle management of cryptographic devices (e.g., HSM) as well as the CA software in use

5.4.1.2 EE and CA certificates

For the lifecycle management of EE as well as CA certificates, the Trust Center logs at least the following events for TeleSec ServerPass:

a) Initial request and revocation of certificates
b) Request for renewal with and without a change of key (renewal and re-key)
c) All activities relating to the verification of information
d) 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
e) Acceptance or rejection of certificate requests
f) Issuance of a certificate
g) Generation of revocation lists and OCSP entries

5.4.1.3 Other security-related events

In addition, the Trust Center logs all security-related events for operation of the TeleSec ServerPass infrastructure. This includes at least the following events:

a) Successful and unsuccessful attempts to access the PKI systems
b) Actions performed on and by PKI systems and other systems that are relevant for security
c) Changes to the security profile
d) System crashes, hardware failures, and other anomalies
e) Firewall and router activities
f) Entering and exiting of Trust Center facilities
g) Results of network checks (vulnerability scans)
h) Start and termination of the logging process

5.4.2 Processing interval for logs

The audit logs/logging files are continuously examined for important events relevant to security and operations. Furthermore, the Trust Center checks the audit logs/logging files for suspicious and unusual activities resulting from irregularities and faults in the TeleSec ServerPass service.

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

5.4.3 Retention period for audit logs

Audit logs/history data/logging files are archived after processing in accordance with Section 5.5.2.

5.4.4 Protection of audit logs

Audit logs/history data/logging files are protected against unauthorized access.

5.4.5 Backup procedures for audit logs

An incremental backup of audit logs/history data/logging files is carried out on a daily basis.

5.4.6 Audit recording system (internal vs. external)

Audit data/history data/logging files at an application, network, and operating system level are automatically generated and recorded. Manually generated audit data is recorded by Trust Center employees.

5.4.7 Notification of the event-triggering 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

An automatic vulnerability scan is performed once a week, though at least once per calendar quarter, following every significant change in the system or network or as requested by the CA/Browser Forum. Potential vulnerabilities are analyzed, assessed, and registered. Based on the assessment, measures are determined and implemented in a defined plan. The vulnerability scans, their results, and actions (resolutions, replacement) are documented.

Critical vulnerabilities are handled via the ISMS process. Critical vulnerabilities reported to the TSP are evaluated by the ISMS team within 48 hours and a solution scenario is presented. In the event that immediate and complete elimination of the vulnerability is not possible, a treatment plan is drawn up with the aim of reducing the critical vulnerabilities.

5.5 Data archiving

5.5.1 Types of archived data records

The following data is collected:

- All registration information including
  - documents and contact information submitted by the subject as part of the request for issuance, revocation, or renewal

    - the identification data of identification documents
    - the method for validating identification documents if available
    - the POSTIDENT documentation if applicable
    - the identity of the RA employee who checked, approved, or denied the request
- All major certificate lifecycle events (request, review, approval, rejection, issuance, revocation, renewal)
- All published CPS
- Certification documents and audit reports
- Any other information required to ensure continuity of services
- Any other information that has been issued and received and may be required as evidence in legal proceedings
- All audit/event logging files recorded in accordance with Section 5.4

Additional data is archived (such as emails, documents sent electronically), taking into account the relevant data protection aspects.

5.5.2 Retention period for archived data

The following records and storage periods are stipulated:

- Order documents, in particular information regarding certificate requests, their validation, the certificates resulting from this, and revocations executed are retained for seven years after the certificate validity expires.
- In the case of ServerPass EV until the end of operation, but at least seven years after the certificate expires.
- Audit and event logging data is archived in accordance with the current legal provisions.

5.5.3 Protection of archives

The Trust Center ensures that only authorized and trusted persons are given access to storage media archives. Archive data is protected against unauthorized read access, changes, deletions, or other forms of manipulation.

5.5.4 Backup procedures for archives

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

5.5.5 Requirements for time-stamping of records

Datasets such as certificates, certificate revocation lists, OSCP responses, and logging files are given information on the date and time. The time source is an NTP appliance (with GPS and DCF77 antenna) from which the UTC time is derived. The individual systems synchronize the system time with the time source several times a day.

5.5.6 Archive recording system (internal or external)

The Trust Center uses internal archive systems only.

5.5.7 Procedures for obtaining and verifying archive information

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

5.6 Key change

Within the period of validity, a key change or certificate change may be required in the following cases:

- If the key material is compromised
- If the cryptographic algorithm needs to be changed
- If the key length needs to be changed
- If the 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.

5.7 Compromise and emergency restoration

5.7.1 Procedures for reporting and handling incidents and compromises

The Trust Center's emergency documentation takes into account the requirements of the Telekom Security CP.

The Trust Center employees have several options (technical interface, direct contact to the ISMS, employee portal) for reporting (information security) incidents and are obligated to report incidents. Reports or alarms are followed up by qualified personnel within a reasonable period of time in accordance with the criticality.

5.7.2 Damage to IT equipment, software, and/or data

If the IT components, software, and/or data are damaged, the incident is immediately investigated and reported to the Trust Center security department (the information security officer). The event initiates a corresponding escalation, incident investigation, incident response, and finally incident resolution. Disaster recovery is carried out depending on the incident classification. All hardware and software that is required for provision of the TeleSec ServerPass service is managed as an asset and application in DT Security GmbH's configuration management.

5.7.3 Certification authority private key compromise procedures

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 after an emergency

The Trust Center has developed, implemented, and tested an emergency plan for data center operation in order to alleviate the effects of catastrophes of all kinds (natural disasters or disasters 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 the ServerPass 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 ServerPass 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 Termination of operation of a certification or registration authority

5.8.1 Cessation of the certification authority

Only DT Security GmbH can announce the cessation of operations at the certification authority or the registration authority.

Economically suitable efforts (or efforts promised in the individual agreements) will be made to notify in advance any subordinate authorities (end entities, registration authorities) affected by these cessations of operations.

If the certification service ceases operations, the certification authority proceeds in accordance with the requirements in [ETSI EN TSP] Section 7.12 and has drawn up a termination plan for this that describes the following measures:

- Notification of end entities and relying parties about the planned cessation of the service
- Continuation of revocation functions, including the regular generation of revocation lists, retrieval of certificate status information and service desk functions
- Revocation of sub-CA certificates involved
- Any transitional 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 certification authority (CA)

All possible measures will be taken prior to cessation of the service in order to minimize the potential damage for all parties involved and to ensure that all those concerned are informed as early as possible.

All rights are withdrawn from the employees of the certification authority and the registration authorities and the private keys of the CA are destroyed. All certificates that are still valid are revoked.

All electronically recorded data is deleted with the exception of the certificates and revocation lists. The certificates, revocation lists, and hard copy documents are archived so that they can, if necessary, be accessed for evidential purposes in case of litigation.

6 TECHNICAL SECURITY CONTROLS

The technical security measures applied are defined in a security concept, with their effectiveness being demonstrated on the basis of a threat analysis. The requirements under [ETSI EN TSP] Section 7.5 are implemented.

6.1 Generation and installation of key pairs

6.1.1 Generation of key pairs

All keys satisfy the algorithms, key lengths, and quality requirements listed in Sections 6.1.5 and 6.1.6. The technical and organizational specifications for generating the various keys are listed below.

6.1.1.1 Generation of root CA key pairs

No stipulation.

6.1.1.2 Generation of sub-CA key pairs

Sub-CA key pairs are generated in a crypto module in accordance with Section 6.2.1 in the secure environment of the sub-CA that wants to use these keys.

The roles involved as well as their tasks and responsibilities before, during, and after the key ceremony are defined and documented.

The individual steps of the key ceremony follow a defined generation protocol and are documented in it.

The generation is performed by at least two trusted employees of the TSP. Each of the two employees has knowledge of part of the activation data required for key generation but no knowledge of the complete activation data.

To prove authenticity and integrity, the hash value of the generated public key or of the certificate request containing the public key is recorded in the generation log and transferred when the certificate is requested (see Section 4.1).

6.1.1.3 Generation of RA key pairs

The TSPs generate RA key pairs in cryptographic modules in accordance with Section 6.2.1.

6.1.1.4 Generation of end entity key pairs

No stipulation.

Keys pairs are not generated for end entities. The end entity generates the key pair of its own accord using tools provided by the server application.

6.1.2 Assignment of private keys to end entities

The end entity's private key always remains with the end entity. Private keys are not assigned to end entities. No private keys are generated on behalf of the customer.

6.1.3 Assignment of public keys to certification authorities (CA)

Following successful authentication, all end entities submit the public key to be certified to the certification authority in electronic form (PKCS#10 request) via a connection secured by TLS/SSL.

6.1.4 Assignment of public CA keys to relying parties

The root CA certificate that is needed to form the trust chain (certificate validation) is made available to all end entities and relying parties by being embedded in the certificate store of the operating systems and applications (e.g., web browsers). Furthermore, the certificates are delivered for end entities with all CA certificates (except root CA) of the trust chain. The required root CA and CA certificates are also available on the websites of the TSP.

6.1.5 Key lengths

In order to determine private keys without the help of cryptographic analysis, the key lengths must be long enough within the defined usage period.

For sub-CA and end-entity certificates, the key length and algorithm requirements of the baseline requirements [CABF-BR] and [SOGIS] are fulfilled.

6.1.6 Generation and quality check of public key parameters

The certificate request (PKCS#10) submitted during the commissioning is checked for the following quality parameters:

- The public key is not a Debian weak key.
- RSA: The key length divisible by 8 is 2,048 bits, 3,072 bits, or 4,096 bits.
- RSA: The value of the exponent is an odd number greater than or equal to 3 and is in the range of 2^{16} and 2^{256}-1.
- RSA: The modulus value is an odd number that is not the power of a prime number and has no factors less than 752.
- ECC: The public key is from one of the following curves:
    - prime256v1 [NIST P-256, Windows display ECDH_P256]
    - secp384r1 [NIST P-384, Windows display ECDH_P384]
- ECC: The public key can be successfully checked with the ECC routine for full validation.
- All linter checks were performed successfully.
- The public key is unique for the certification authority.
- At least SHA-256 is used as the signature hash algorithm in the certificate request. (SHA-1 is currently still allowed. However, a warning is displayed that switching to SHA-256 or higher is recommended).

If any of the checks fail, the certificate request is rejected. Compliance with the quality parameters for CA keys of the TSP is ensured by the technical checks of the cryptographic modules used as described in Section 6.2.

6.1.7 Key usage (in accordance with the "key usage" X.509v3 expansion)

See Section 7.1.2.5.

6.2 Protection of private keys and technical checks of cryptographic modules

The Trust Center has implemented physical, organizational, and procedural mechanisms to ensure the security of CA keys.

End entities are obliged to take all necessary precautions to prevent the loss, disclosure, or unauthorized use of private keys.

6.2.1 Standards and checks for cryptographic modules

The private keys of the CAs are stored on an FIPS 140-2/level 3-evaluated hardware security module (HSM). The keys are backed up using high-quality multi-person backup techniques (see also Section 6.2.2)

To protect cryptographic devices during operation, transport, and storage, the manufacturer-specific mechanisms tested during FIPS and CC certifications are used. The devices are stored separately from the PED keys required for operation and use so that the compromise of a single location is not sufficient to misuse the devices.

Integrity and function tests are conducted and documented before commissioning and decommissioning.

6.2.2 Multi-person controls (m out of n) for private keys

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

6.2.3 Storage of private keys

Private keys are not put into escrow with trustees outside the Trust Center.

6.2.4 Backup of private keys

The Trust Center retains backup copies of the key material for every CA certificate for restoration and emergency purposes. These keys are stored in encrypted form within the cryptographic hardware module (HSM) and associated key storage devices.

In addition, backups of the private CA keys for the ServerPass sub-CAs are stored in a secure environment. Access to these keys is permitted only for trusted individuals at the Trust Center (trusted roles).

The private key in question is saved in encrypted form on special security tokens.

Restoring a private key for a CA, i.e., loading the key in the CA software, also requires multiple trusted individuals at the Trust Center (trusted roles). A restoration may only be performed within the high security zone of the Trust Center.

The Trust Center provides no backup of the private key for ServerPass at the request of the end entity.

6.2.5 Archiving of private keys

Sub-CA or OCSP keys are destroyed when they reach the end of their validity periods. They are not archived.

The Trust Center provides no archiving of the private key at the request of the end entity.

6.2.6 Private key transfer into or from a cryptographic module

Sub-CA keys are generated on the cryptographic hardware modules (HSM) in online operation.

The key material for a certificate of an intermediate certification authority (sub-CA) is generated on a cryptographic hardware security module (HSM) in online operation. The public key to be certified, with the data of the Subject DN, is transferred securely in electronic form (PKCS#10-Request) to the offline CA, which generates the sub-CA certificate. The sub-CA certificate is then securely transferred to the HSM of the online CA and assigned to the private key.

6.2.7 Private key storage on cryptographic module

The Trust Center saves CA keys in a secure manner on cryptographic hardware security modules (HSM) that are evaluated in accordance with FIPS 140-2/level 3.

6.2.8 Method for activating private keys

All end entities, registrars, administrators, and operators must protect the activation data (e.g., PIN, import password) for their private key against loss, theft, change, disclosure, and unauthorized usage in accordance with the present CPS.

The private key belonging to the sub-CA certificate remains active until the certificate loses its validity or there is a reason for revocation.

6.2.8.1 Private keys of end entities

The end entity is entitled to take economically suitable measures to physically protect the hardware/software used, to prevent the space/components and the respective private key being used without the end entity's authorization.

6.2.8.2 Private keys of administrators

The administrator or operator must comply with the following provisions to protect the private key:

- Setting of a password or a PIN (in accordance with Section 6.4.1) or integration of an equivalent security measure in order to authenticate the administrator or operator prior to activation of the private key. This can, for example, also contain a password for operating the private key, a Windows login or screensaver password or a login password for the network.
- Appropriate measures must be taken to physically protect the administrator or operator workplace against unauthorized access.

6.2.8.3 Private keys of sub-CA and root-CA certificates

Key material for CA and root CA certificates is activated accordingly by the authorized persons and stored on cryptographic hardware modules (HSM) (Sections 6.2.2 and 6.4.1).

The private key belonging to the CA certificate remains active until the certificate loses its validity or there is a reason for revocation.

The private key belonging to the root CA certificate is activated only to generate further CA certificates. Once the root CA certificate expires, the private key is no longer used.

6.2.9 Method for deactivating private keys

The deactivation of private keys belonging to administrators and operators is event-based and the responsibility of the Trust Center staff.

The end entity is responsible for the deactivation of private end-entity keys.

Private keys that belong to ServerPass CA certificates are destroyed in principle (see 6.2.10) and not disabled under any circumstances.

6.2.10 Method for destroying private keys

The destruction of CA keys requires the participation of several trusted persons (trusted roles) from the Trust Center. After the key has been destroyed, it needs to be ensured that there are no residual fragments which could lead to the key being reconstructed. The Trust Center uses an integrated deletion function of the HSM for secure destruction of keys.

End entities are responsible for destroying their own private keys.

6.2.11 Evaluation of cryptographic modules

See Section 6.2.1.

6.3 Other aspects of managing key pairs

6.3.1 Archiving of public keys

The Trust Center backs up and archives the certificates (CA, root CA, and end entity certificates) as part of regular backup measures.

6.3.2 Validity periods of certificates and key pairs

The validity period of a certificate begins when the certificate is generated. The certificate's validity period ends when it expires or is revoked. The validity period of key pairs is the same as the validity period for the corresponding certificate.

The validity periods of CA certificates are described in the following table.

The Trust Center ensures that the CA certificates are changed before they expire, in order to guarantee the relevant certificate validity of end-entity certificates.

Table 3: Validity of certificates

Type of certificate:	Period of validity:
TeleSec ServerPass Standard and SAN/UCC	
TeleSec ServerPass Class 2 CA	10 years
T-TeleSec GlobalRoot Class 2	25 years
End entity certificates	1 year. The period of grace is up to 5 days.
TeleSec ServerPass EV/EV SAN, QWAC	
TeleSec ServerPass Extended Validation Class 3 CA	10 years
T-TeleSec GlobalRoot Class 3	25 years
End entity certificates	1 year. The period of grace is up to 5 days.
Other certificates	
OCSP-Signer <root CA>	3 months
OCSP-Signer <sub-CA>	1 month

6.4 Activation data

6.4.1 Generation and installation of activation data

In order to protect the private keys of the CA certificates stored on the HSM, activation data (secret shares) is generated according to the requirements described in Section 6.2.2 of this CPS and the "Key Ceremony" document. The generation and distribution of secret shares is logged.

6.4.2 Protection of activation data

The Trust Center administrators or persons authorized by the Trust Center undertake to protect the secret shares for activating the private keys of root-CA, CA, and OCSP certificates.

6.4.3 Other aspects of activation data

6.4.3.1 Transfer of activation data

If activation data for private keys is transferred, regardless of the transfer medium, the Trust Center administrators must strictly protect the transfer with the help of methods for protecting against loss, theft, changes, unauthorized disclosure, or use of these private keys.

6.4.3.2 Destruction of activation data

After the private keys have been deleted (Section 6.2.4), the activation data is no longer worth protecting.

6.5 Computer security controls

The Trust Center carries out all PKI functions with the help of trusted and appropriate systems.

The functionality and capacity of the systems are continuously checked by monitoring systems so that resources can be extended promptly if necessary. The security regulations for computers of the certification authority (e.g., network security, access control, monitoring etc.) are described in the security concept. The requirements under [ETSI EN 319 401] Section 7.4 are implemented.

The systems for development, testing (TU) and production (PU) are completely separate from one another. They run on different hardware in different network segments, which means that mutual influence is excluded.

6.5.1 Specific technical requirements for computer security

The Trust Center uses only trusted systems that guarantee the technical security and reliability of the processes supported by the systems. All certificate management systems and the status and directory services are taken into account in the Trust Center's risk management and protected in accordance with their criticality or damage potential.

The required separation of trusted roles (see Section 5.2.4) is technically supported by all necessary systems. In particular, the accounts of the trusted roles (see Section 5.2.1) required for the operation of the critical systems are managed in such a way that access to the systems and data is restricted to the persons identified and authenticated for these roles (see Section 5.2.3) with the minimum required permissions. All accounts are reviewed on a regular basis, at least every 3 months, and modified or deleted as needed within a reasonable period of time.

The administration systems for implementing the security policies are used exclusively for this and no other purposes.

The CA, certificate management, security, and front-end systems and, if applicable, other internal systems to support operations are hardened by default in accordance with Group-wide specifications or best practices, i.e., accounts, services, protocols, and ports not required for the operation of the CAs are deactivated.

Telekom Security systems are provided with integrity protection to guard against viruses, malicious code, and the import of unauthorized software, and are monitored in terms of capacity utilization and available resources to ensure uninterrupted operation. These and other security measures for Trust Center systems are described in the security concept.

The data recorded for the generation and, if necessary, revocation of certificates, including the log data in accordance with Section 5.4.1, is backed up in such a way that its integrity, confidentiality, and availability is ensured over the entire retention period.

The development, test, and production environments of the Trust Center are operated on different hardware in different network segments and are therefore completely separate from one another.

6.5.2 Assessment of computer security

Following every significant change in the system or network, an automatic vulnerability scan is performed within a week, but at least once per calendar quarter. Potential vulnerabilities are analyzed, assessed, and registered. Based on the assessment, measures are determined and implemented in a defined plan. The vulnerability scans, their results, and actions (resolutions, replacement) are documented.

Critical vulnerabilities are handled via the ISMS process. Critical vulnerabilities are evaluated by the ISMS team within 48 hours and a solution scenario is presented. If immediate and

complete elimination of the vulnerability is not possible, a treatment plan is drawn up with the aim of reducing the critical vulnerabilities.

In addition, "penetration tests" are implemented once a year. In this case, corresponding measures are derived and implemented too, if necessary. The penetration tests and vulnerability scans are performed by personnel trained for this purpose. The tools used correspond to the current state of the art.

6.6 Lifecycle technical controls

6.6.1 System development controls

The Trust Center has implemented mechanisms and controls to monitor and protect purchased, developed, or modified software for damaging elements or malicious code (e.g., Trojans, viruses). The integrity is manually verified prior to installation.

New software versions (planned updates) or fault resolutions (short-term bug fixes) are initially provided and tested on the manufacturer's/developer's development system.

After a check, the software is installed on a test system. The software is installed on the live system only following exhaustive and successful tests.

The PKI systems (CA, HSM, web server, etc.) are administered by the system administrators via a separate network that is exclusively available to these role owners. Administration of other IT systems (not PKI systems) via this network is not permitted.

DT Security GmbH's established change management is used.

6.6.2 Security management measures

All releases, patches, and short-term bug fixes, as well as changes to the configuration that affect the security guidelines, are handled and documented via regulated change management processes.

All changes that affect the defined security level are approved in advance by the Trust Center management.

The Trust Center's vulnerability management is regulated to ensure that

- security patches are applied within a reasonable period of time, but within 6 months at the latest;
- security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefit of the patch;
- the reasons for not applying security patches are documented.

The systems log, as far as possible, all security-relevant events. This includes monitoring the systems for the following activities (including appropriate alerting functions):

- Security-relevant system events, which include:
    - Successful and unsuccessful attempts to access the certificate systems
    - Activities performed on the certificate and security systems
    - Startup and shutdown of logging functions
- Availability and use of required services

- Changes to the security profiles
- Installation, update, and removal of software on a certificate system
- System crashes, hardware failures, and other anomalies
- Firewall and router activities
- Physical access and exit to and from the operating rooms of the certificate management systems

The integrity of the systems, including their relevant (configuration) settings, is continuously monitored for changes. In the event of changes that were not made on the basis of an authorized change, the resulting alarm messages are followed up by qualified personnel.

Telekom Security monitors the capacity requirements of the systems to ensure that adequate processing power and storage capacity are permanently available.

Data backups are tested regularly to ensure that they meet the requirements of the contingency plan. The data backup and restore functions are performed by the designated trusted roles.

6.6.3 Lifecycle security controls

The Trust Center has implemented mechanisms and controls to ensure that security patches are installed within a reasonable time after they are available. The integrity of the security patch is manually verified prior to installation.

A security patch is not installed if additional security gaps or instabilities arise that outweigh the advantages of using the security patch. The reason for not applying security patches is documented.

6.7 Network security controls

The requirements under [ETSI EN 319 401] Section 7.8 are implemented.

The internal networks and systems are protected against unauthorized access and attacks with the help of multi-level firewalls, IDS, IPS, zoning, and other protective measures. All network components are configured in such a way that only the minimum required protocols, services, and accesses are available.

The segmentation of the network is based on a risk assessment taking into account the functional, logical, and physical (including location) relationships between trusted systems and services.

All systems critical to CA operations are placed in secure or high-security zones. Communication between systems within the security zones is protected by appropriately implemented and configured security procedures.

The networks for administering the systems are separated from the operational networks.

Within a zone, the same minimum security requirements apply to all systems.

Firewalls are implemented between the zones, protecting systems and communications within the secure zones as well as communications with systems outside the zones. The connections are restricted so that only those required for operation are possible; connections that are not required are explicitly prohibited or deactivated.

The configurations of the systems are checked for compliance with these rules at regular intervals and as required.

All network components (e.g., routers) are installed in physically and logically secure environments. Their configurations are regularly checked for compliance with the requirements defined by the TSP.

As a rule, communication between all trusted as well as other systems is encrypted on several layers and is implemented for almost all systems, but at least for the trusted systems, via trusted channels that are logically different from other communication channels and ensure secure identification of their endpoints.

All external network connections are set up redundantly.

After each significant system or network change, an automated vulnerability check is usually performed within one week, but at least once per calendar quarter, on public and private IP addresses identified by the Trust Center. Vulnerability testing is conducted by individuals or organizations with the skills, tools, abilities, ethics, and independence necessary to conduct reliable testing and documentation. The performance of a vulnerability assessment, indicating the qualifications of the person or organization conducting the assessment, is controlled by the ISMS and documented along with the results.

Penetration tests are performed on the systems during commissioning or significant changes to the infrastructure or applications, but at least once a year. Penetration testing is conducted by individuals or organizations with the skills, tools, abilities, ethics, and independence necessary to conduct reliable testing and documentation. The performance of a penetration test, indicating the qualifications of the person or organization conducting the assessment, is controlled by the ISMS and documented along with the results.

Once a critical vulnerability has been identified, it is usually remediated within 4 days unless there are good reasons not to remediate the vulnerability. If remediation is not possible within 4 days, a mitigation plan for the vulnerability, including prioritization of activities, is created and processed within the timeframe specified therein. If it is decided not to remediate a vulnerability, the justified decision is documented in the ISMS.

6.8 Timestamp

Certificates, revocation lists, online status checks, and other important information contain date and time information derived from a reliable time source (see Section 5.5.5).

7 CERTIFICATE LISTS, REVOCATION LISTS, AND OCSP PROFILES

7.1 Certificate profile

The certificates issued by the certification authority meet the following requirements:

- [RFC 5280]
- [X.509]
- [CABF-BR]
- [CABF-BREV]
- ETSI guidelines [ETSI WEB], [ETSI POL], [ETSI QC]

X.509v3 certificates must include at least the contents listed in Table 4.

Table 4: Certificate attributes in accordance with X.509.v3

Field:	**Value or value limitation:**
Version:	Certificate version
Serial number:	Unique value to identify the certificate
Signature algorithm:	RSA - SHA-256 SHA384 ECDSA SHA-256 ECDSA (dependent on the issuing sub-CA)
Issuer:	See Section 7.1.4
Valid from:	Time basis Coordinated Universal Time (UTC). Coded in accordance with RFC 5280.
Valid until:	Time basis Coordinated Universal Time (UTC). Coded in accordance with RFC 5280.
Subject:	Distinguished name (see Section 7.1.4)
Public key:	Coded in accordance with RFC 5280.
Extensions:	
Key usage:	Section 7.1.2.5
Certificate guidelines:	Section 7.1.2.1
Alternative subject name:	Section 7.1.2.6
Basic constraints:	Section 7.1.2.3
Enhanced key usage:	Section 7.1.2.4
Revocation list distribution point:	Section 7.1.2.2
Authority key identifier:	Section 7.1.2.7
Subject key identifier:	Section 7.1.2.8
Access to authority information	Section 7.1.2.9
QC statement	Section 7.1.2.10

The certificate serial numbers are assigned by ServerPass in non-sequential numbering and contain a 126-bit long random value (entropy).

Additional extensions and properties (in particular also for extended validation certificates) are explained in more detail in the following sections.

7.1.1 Version number(s)

The X.509 certificates issued for end entities are the latest version (currently version 3). Additional extensions and properties are described in more detail in the sections that follow.

The root CA and sub-CA certificates are also of the X.509v3 type.

7.1.2 Certificate extensions

In order to fulfill the X.509v3 standard and the guidelines for EV/EV SAN certificates [CABF-BREV], the certification authority supplements the certificate profile with corresponding extensions. These are described in the following sections.

7.1.2.1 "Certificate policies" extension (certificatePolicies)

The "Certificate policies" extension consists of an object identifier (OID; see also Section 7.1.6) and a link, via which this certification policy can be accessed:

certificatePolicies:policyIdentifier = 2.23.140.1.2.2 (OV) or

certificatePolicies:policyIdentifier = 2.23.140.1.2.1 (DV) or

certificatePolicies:policyIdentifier = 2.23.140.1.1 (EV)

certificatePolicies:policyIdentifier = 0.4.0.2042.1.4 (EVCP only EV/EV SAN)

certificatePolicies:policyIdentifier = 0.4.0.194112.1.4 (QCP-w only EV/EV SAN)

certificatePolicies:policyQualifiers:policyQualifierId = id-qt 1.

certificatePolicies:policyQualifiers:qualifier = URL to this document

The risk value of this extension is set to "not critical."

7.1.2.2 "Revocation list distribution point" extension (cRLDistributionPoint)

All end-entity certificates contain a certificate revocation list distribution point (cRLDistributionPoint), to the associated certificate revocation list (CRL). Relying parties need this URL for certificate validation. The criticality of this extension is set to "not critical."

The CA certificate also has a revocation list distribution point, through whose URI (HTTP and LDAP) the current revocation list for certification authorities (ARL) can be accessed on the directory service. Relying parties need this URI for certificate validation. The criticality of this extension is set to "not critical."

7.1.2.3 "Basic constraints" extension (BasicConstraints)

The "Basic constraints" extension defines the certificate type (end entity, CA) and the certification path length constraint (pathLenConstraint).

For end-entity certificates, the user type "end unit" is set (cA = false) and the path length is not set. The criticality of this extension is set to "critical."

The sub-CA certificates are given the user type "certification authority" with the path length "0." The criticality of this extension is set to "critical."

7.1.2.4 "Extended key usage" extension (ExtendedKeyUsage)

The end-entity certificates contain the extended key usage client authentication (id-kp-clientAuth,1.3.6.1.5.5.7.3.2) and TLS web server authentication (id-kp-serverAuth,1.3.6.1.5.5.7.3.1). The criticality is set to "not critical."

7.1.2.5 "Key usage" extension (keyUsage)

The key usage is based on the rules of RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" and is described therein.

The key uses are assigned in table form to the different certificate profiles in Table 5 and Table 6.

Table 5: Assignment of the "Key usage" extension

		TeleSec ServerPass Standard and SAN/UCC		
		EE certificates	Sub-CA certificates	Root CA certificates
	Risk value (criticality)	Critical	Critical	Critical
Bit	Designation			
0	digitalSignature	Yes	No	No
1	nonRepudation	No	No	No
2	keyEncipherment	(Yes) (only RSA key)	No	No
3	dataEncipherment	No	No	No
4	keyAgreement	(Yes) (only ECC key)	No	No
5	keyCertSign	No	Yes	Yes
6	CRLSign	No	Yes	Yes
7	encipherOnly	No	No	No
8	decipherOnly	No	No	No

Table 6: Assignment of the "Key usage EV/EV SAN" extension

		TeleSec ServerPass EV/EV SAN		
		EE certificate	Sub-CA certificates	Root CA certificates
	Risk value (criticality)	Critical	Critical	Critical
Bit	Designation			
0	digitalSignature	Yes	No	No
1	nonRepudation	No	No	No
2	keyEncipherment	(Yes) (only RSA key)	No	No
3	dataEncipherment	No	No	No
4	keyAgreement	(Yes) (only ECC key)	No	No
5	keyCertSign	No	Yes	Yes
6	CRLSign	No	Yes	Yes
7	encipherOnly	No	No	No
8	decipherOnly	No	No	No

In the event that the key usage is declared "not critical", there is an extended key usage labeled as "critical."

7.1.2.6 "Alternative subject name" extension (subjectAltName)

The common name of the distinguished name is entered as alternative subject name (subjectAltName). The criticality of this extension is set to "not critical."

7.1.2.7 "Authority key identifier" extension (authorityKeyIdentifier, AKI)

The "Authority key identifier" extension in the "Key identifier" field contains a fixed 160-bit SHA-1 hash value, which mathematically corresponds to the value of the "CA certificate subject key identifier" (see Section 7.1.2.8). This value is formed of the hash value of the public key of the issuing certification authority.

The criticality of this extension is set to "not critical."

7.1.2.8 "Subject key identifier" extension (subjectKeyIdentifier)

The "Subject key identifier" extension is a 160-bit SHA-1 hash value which is individually composed of the relevant public key of the current certificate. The hash value of the "Subject key identifier" extension mathematically corresponds to the value of the "Authority key identifier" extension (see Section 7.1.2.7) of the certificate below it in the hierarchy.

The criticality of this extension is set to "not critical."

7.1.2.9 "Authority Information Access" extension

In end-entity (EE) certificates the "Authority information access" extension is given the object ID (OID) 1.3.6.1.5.5.7.48.1 for the OCSP service, as well as the HTTP address of the OCSP responder.

End-entity certificate issued by:

- TeleSec ServerPass Class 2 CA: http://ocsp.serverpass.telesec.de/ocspr
- TeleSec ServerPass Extended Validation Class 3 CA: http://ocsp.serverpass.telesec.de/ocspr

In certification authorities (sub-CA), the "Authority information access" extension contains the object ID (OID) 1.3.6.1.5.5.7.48.1 for the OCSP service, as well as the HTTP URL of the OCSP responder in question:

CA certificates

- TeleSec ServerPass Class 2 CA: http://ocsp.telesec.de/ocspr
- TeleSec ServerPass Extended Validation Class 3 CA: http://ocsp.telesec.de/ocspr

The criticality of this extension is set to "not critical."

7.1.2.10 "Instructions for a qualified certificate" extension (qcStatements)

The "Instructions for a qualified certificate" extension (qcStatements) consists of the object identifier (OID) in accordance with:

- 0.4.0.1862.1.1 = qcStatement - QcCompliance [ETSI QC]
- 0.4.0.1862.1.5 = qcStatement - QcPDS [ETSI QC]
- 0.4.0.1862.1.6 = qcStatement - QcType [ETSI QC]
- 0.4.0.1862.1.6.3 = QcType - id-etsi-qct-web [ETSI QC]

7.1.3 Algorithm object identifier (OID)

7.1.3.1 SubjectPublicKeyInfo

7.1.3.1.1 RSA

The SubjectPublicKeyInfo field for an RSA key contains the rsaEncryption identifier (OID: 1.2.840.113549.1.1.1).

The parameters are available and have the value NULL.

The AlgorithmIdentifier is coded as follows: 300d06092a864886f70d0101010500.

7.1.3.1.2 ECDSA

The SubjectPublicKeyInfo field for an ECDSA key contains the id-ecPublicKey identifier (OID: 1.2.840.10045.2.1).

The parameters use the namedCurve encoding. The namedCurve for P-256 keys is secp256r1 (OID: 1.2.840.10045.3.1.7) and for P-384 keys it is secp384r1 (OID: 1.3.132.0.34).

The AlgorithmIdentifier for secp256r1 is encoded as follows:

301306072a8648ce3d020106082a8648ce3d030107.

The AlgorithmIdentifier for secp384r1 is encoded as follows:

301006072a8648ce3d020106052b81040022.

7.1.3.2 Signature AlgorithmIdentifier

7.1.3.2.1 RSA

The Signature AlgorithmIdentifier field for RSA contains the sha256WithRSAEncryption identifier (OID: 1.2.840.113549.1.1.11).

The parameters are available and have the value NULL.

The AlgorithmIdentifier is coded as follows: 300d06092a864886f70d01010b0500.

7.1.3.2.2 ECDSA

No stipulation.

7.1.4 Name forms

Test certificates are not issued in the live system. Instead, we offer certificates with 30-day validity under a non-public test CA.

7.1.4.1 Information about the issuer

CA certificates used by TeleSec ServerPass contain a unique issuer name (Issuer DN) as described in Section 3.1.1.

Issued end-entity certificates contain a unique issuer name (Issuer DN) of the respective certification authority.

The issuer name in a certificate ("Issuer DN") corresponds to the "Subject DN" of the issuing certificate "byte-by-byte."

7.1.4.2 Subject information of the end-entity certificates

The contents of the subject DN (subject) of end entity certificates are optionally composed of the fields as described in Section 3.1.1. The fields contain mandatory and optional information.

7.1.4.2.1 Subject Alternative Name extension

Fully-Qualified Domain Names MUST consist solely of P-Labels and Non-Reserved LDH Labels (letters, digits, hyphen).

See Sections 3.1.1.1 and 3.1.1.2.

7.1.4.2.2 Subject Distinguished Name fields

Fully-Qualified Domain Names MUST consist solely of P-Labels and Non-Reserved LDH Labels (letters, digits, hyphen).

See Sections 3.1.1.1 and 3.1.1.2.

7.1.4.3 Subject information of the CA certificates

The contents of the subject DN (subject) of CA certificates are optionally composed of the fields as described in Section 3.1.1. The fields contain mandatory and, if necessary, optional generated information.

The following fields contain mandatory information:

- Country Name (C):

- Organization Name (O)
- Organizational Unit Name (OU)
- Common Name (CN)

The following fields are optional:

- StateOrProvinceName (ST)
- Locality (L)
- PostalCode
- StreetAddress (Street)

7.1.5 Name constraints

TeleSec ServerPass does not operate sub-CAs with name restrictions.

7.1.6 Object IDs (OIDs) of certificate policies

7.1.6.1 Reserved Certificate Policy Identifier

See Sections 1.2, 7.1.2.1 and 7.1.6.3.

7.1.6.2 Object identifiers in root CA certificates

The root CA certificates do not contain a certificatePolicies extension.

7.1.6.3 Sub-CA certificates

TeleSec ServerPass Class 2 CA

The TSP uses the "anyPolicy" policy OIDs (2.5.29.32.0) in the "TeleSec ServerPass Class 2 CA" sub-CA certificate, which was issued under a public root.

TeleSec ServerPass Extended Validation Class 3 CA

The TSP uses the "anyPolicy" policy OIDs (2.5.29.32.0) in the "TeleSec ServerPass Extended Validation Class 3 CA" sub-CA certificate, which was issued under a public root.

7.1.6.4 Object identifiers in end-entity certificates

A certificate issued to an end-entity contains one of the following certificatePolicies extensions:

Policy OID 2.23.140.1.1

If the policy OID **2.23.140.1.1** EV (extended validation certificate) is used in a certificate, the following fields of the subjectDN must be filled: organizationName, localityName, stateOrProvinceName (if a meaningful value exists, such as federal state in Germany), commonName, and countryName.

Policy OID 2.23.140.1.2.1

If the policy OID **2.23.140.1.2.1** DV (domain validated certificate) is used in a certificate, it is mandatory that the following field of the Subject DN is filled in: commonName.

The following fields are not used: organizationName, localityName, stateOrProvinceName, postalCode, StreetAddress, and countryName.

Policy OID 2.23.140.1.2.2

If the policy OID 2.23.140.1.2.2 OV (Organization Validated certificate) is used in a certificate, the following fields of the subjectDN must be filled: organizationName, localityName, stateOrProvinceName (if a meaningful value exists, such as federal state in Germany), commonName, and countryName.

The policy OID **2.23.140.1.2.3** is not used, as no IV (Individual Validated) certificates are issued.

Public device certificates use the policy OID 2.23.140.1.2.2 in order to ensure that the public device certificate and its management fulfill the requirements of [CABF-BR] during its lifetime.

7.1.7 Using the policy constraints extension

No stipulation.

7.1.8 Syntax and semantics of policy identifiers

The end-entity certificates contain a URL to the location where the CPS is stored. Older versions are stored in the corresponding repository.

7.1.9 Processing semantics for the "Critical certificate policies" extension

No stipulation.

7.1.10 Subject DN Serial Number (SN)

Certificates with the same subjectDN are issued exclusively for a customer. New certificates of other customers with a subjectDN that is already used have a unique and distinctive serial number (SN) added in the subjectDN.

7.2 Revocation list profile

The revocation lists issued by the certification authority meet the following requirements:

- [RFC 5280]
- [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)

Certificate revocation lists must include at least the contents described in Table 7.

Table 7: Revocation list attributes in accordance with X509.v2

Field	Value or value constraints
Version:	Revocation list version (see Section 7.2.1)
Issuer:	(see Section 7.1.4)
Valid from:	Time basis Coordinated Universal Time (UTC). Coded in accordance with RFC 5280.
Next update (NextUpdate):	Date and time of the next planned publication.
Signature algorithm:	1.2.840.113549.1.1.11 / sha256WithRSAEncryption(11)
Revoked certificates:	List of revoked certificates including serial number with revocation date and time of the revoked certificate.
Extensions	
Authority key identifier (AuthorityKeyIdentifier):	Section 7.2.2.1 applies accordingly
Revocation list number (cRLNumber):	Serial number of the certificate revocation list (Section 7.2.2.2).
Reason for revocation:	(optional) coding of the reason for revocation in accordance with RFC 5280; see Section 7.2.2.3
CRL contains expired certificates (ExpiredCertsOnCRL)	Section 7.2.2.4 applies accordingly

7.2.1 Version number(s)

The certification authority supports certificate revocation lists in the X.509 Version 2 format, which fulfill the requirements in accordance with RFC 5280.

7.2.2 Revocation list and revocation list entry extensions

7.2.2.1 "Authority key identifier" (authorityKeyIdentifier) extension

The revocation lists contain the "Authority Key Identifier" extension as described in Section 7.1.2.6.

The criticality of this extension is set to "not critical."

7.2.2.2 "Revocation list number" extension (cRLNumber)

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 "not critical."

7.2.2.3 "Reason for revocation" extension

When revoking certificates, it is essential to state a reason for revocation. The following reason codes are implemented in accordance with Table 8:

Table 8: Reason for revocation

Input value on website:	Reasons for revocation in accordance with RFC 5280:	Value:
Not specified; incorrect certificate use ("certificate misuse")	unspecified	
Key compromised	keyCompromise	1
CA compromised	cACompromise	2
Information in the certificate is out of date or incorrect	affiliationChanged	3
Certificate is no longer required	superseded	4
Cessation of operation	cessationOfOperation	5
Rights have been withdrawn (right to use the domain name expired)	privilegeWithdrawn	9

The criticality of this extension is set to "not critical."

7.2.2.4 CRL contains expired certificates (ExpiredCertsOnCRL)

The revocation lists also include expired certificates (ExpiredCertsOnCRL).

The criticality of this extension is set to "not critical."

7.3 OCSP profile

OCSP (Online Certificate Status Protocol) provides a validation service on a protocol of the same name, with the help of which the relying party is sent timely information on the revocation status of end entity certificates.

The OCSP service used fulfills the requirements of RFC 6960.

7.3.1 OCSP extensions

The OCSP certificate issued by the certification authority contains the “extended key usage” attribute with the OID "1.3.6.1.5.5.7.3.9" (OCSP noCheck, id-pkix-ocsp-nocheck); i.e., the OCSP certificate is not validated.

The ArchiveCutOff extension is not used.

8 COMPLIANCE AUDITS AND OTHER CHECKS

Those authorities that are subject to an audit, check, or investigation must support the Trust Center and/or a delegated third party.

Furthermore, the Trust Center is entitled to commission third parties to perform these audits, checks, and investigations on its behalf (Section 8.2).

TeleSec ServerPass Standard and SAN/UCC:

The Trust Center processes are subject to a regular annual check (ETSI EN 319 411 -1, policy OVCP) by an independent third party. In addition, the Trust Center carries out internal audits at regular intervals (see also Section 8.1).

TeleSec ServerPass EV/EV SAN:

The Trust Center processes are subject to regular annual audits (ETSI EN 319 411-1, EVCP, ETSI EN 319 411-2 QCP-w) by independent third parties. In addition, the Trust Center carries out internal audits at regular intervals (see also Section 8.1).

The subject of certification is all processes used to apply for, issue, reissue, revoke, and renew end-entity certificates.

8.1 Frequency and circumstances of audits

Compliance audits take place at least annually and additionally as required (Section 8) and are carried out at the expense of the audited authority. Notice of the start of a compliance audit must be given in writing at least one week in advance. Audits are conducted during an uninterrupted sequence of audit periods that do not exceed one year.

Quality assessment self-audits that ensure the service quality are performed on a regular basis, at least four times per year. At least 3 (three) percent of the certificates issued in this time period, but always at least 1, are examined. The selection is random. The period starting from the previous self-assessment is always used for the selection.

8.2 Identity/qualifications of the auditor

The Trust Center-specific compliance audits are carried out by qualified employees of DT Security GmbH or a third party (e.g., qualified company such as TÜV IT) who can demonstrate experience in the areas of public key infrastructure technology, security auditing, as well as procedures and aids for information security.

Special requirements apply to auditors who perform an audit in the Trust Center at the request of one or more application software providers. The Trust Center commissions an auditor of a certification authority accredited for IT security for ServerPass. This ensures that the special requirements of the auditor (e.g., qualification, independence) are met.

8.3 Relationship of the auditor to the authority to be audited

The auditor for the ETSI certification is an independent, qualified auditor (e.g., financial auditor, expert).

Self-audits (quality assessments) are carried out by qualified internal auditors of DT Security GmbH.

8.4 Topics covered by audit

The aim of the audit is to implement this document. All processes associated with the lifecycle management of certificates are to be checked:

- Identity verification of end entities
- Certificate request procedures
- Processing of certificate requests
- Certificate renewal/re-certification (only TeleSec ServerPass standard, SAN/UCC)
- Certificate revocations
- Access control
- Authorization and role concept
- Anti-break-in measures
- Human resources

In each case, the audit is performed in line with the currently valid version of the following audit criteria:

ETSI EN 319 411-1, policy OVCP.

TeleSec ServerPass EV/EV SAN:

The audits also cover the points named in ETSI EN 319 411-1 policy EVCP that require particular attention for the issuance of extended validation certificates.

There is also an annual full audit under ETSI EN 319 411-2, policy QCP-w for issuing eIDAS-compliant qualified certificates for website authentication.

8.4.1 Risk assessment and security plan

The Trust Center performs an annual risk assessment that includes the ServerPass product.

The assessment covers at least the following items:

1) Identification of foreseeable external and internal risks (i.e., in particular the underlying vulnerabilities) that may lead to:
    1. Unauthorized access to relevant data or systems
    2. Handover or misuse of relevant data
    3. Modification or destruction of relevant data
    4. Impairment, interruption, or failure of parts of or the entire certificate management process

2) Assessment of the likelihood of occurrence and the resulting potential damage (i.e., extent of damage) due to exploitation of a vulnerability. Here, the special security requirements of certificate data and the certificate management process must be taken into account.
3) Assessment of the effectiveness and suitability of the countermeasures taken (e.g., policies, procedures, security systems used, technologies, insurance policies) in order to remove the danger or minimize the risk.

Based on the risk assessment, the Trust Center has developed a security plan that is regularly checked and, if necessary, modified. This security plan consists of procedures, measures, and products used to aid the evaluation and management of risks that are identified during the risk assessment. The security plan contains administrative, organizational, technical, and physical security measures according to the sensitivity of the data and the certificate management process.

8.5 Measures for rectifying any defects or deficits

If an auditor finds major deficits or errors during a compliance audit at the certification authority's operator, the appropriate corrective measures will be decided on. The Head of the Trust Center decides together with the auditor which suitable measures should be implemented in an economically suitable timeframe. In the event of serious security-critical deficits, a correction plan must be devised within 10 days and the deviation rectified. In the event of less serious deficits, the Head of the Trust Center will decide on the rectification timeframe.

8.6 Communication of results

The results of the audit will be documented in a report prepared by the auditor and passed on to the Trust Center.

The Trust Center reserves the right to publish results or partial results if misuse occurred or the reputation of DT Security GmbH was damaged.

Audit reports filed at the request of one or more application software vendors embedding a root certification body certificate of the Trust Center must be published no later than three months after the end of the respective audit period.

The required audits are filed for ServerPass. The associated reports are published on the website https://www.telesec.de/de/service/downloads/pki-repository/ in the menu "Audit Attestations and Certifications -> Certifications -> ETSI-Zertifikate TeleSec ServerPass" [ETSI Certificates TeleSec ServerPass] and "Audit Attestations and Certifications -> Certifications -> eIDAS – Konformitätsbewertungen für Vertrauensdiensteanbieter" [eIDAS - Conformity Assessments for Trust Service Providers].

8.7 Self-audits

Self-audits are conducted as described in Section 8.1.

9 OTHER BUSINESS AND LEGAL PROVISIONS

9.1 Charges

9.1.1 Charges for issuing or renewing certificates

The certification authority is entitled to charge for issuing, renewing, and managing end entity certificates. The fees are regulated in the applicable "TeleSec ServerPass Service Specifications and Charges."

9.1.2 Charges for access to certificates

The Trust Center does not charge for access to certificates in the directory service of TeleSec ServerPass. The Trust Center allows third parties, who themselves market products and services, to access and retrieve certificates only with prior express written permission.

Third parties require prior express permission in writing before marketing the certificates and status information that the Trust Center provides publicly or providing them for marketing.

9.1.3 Charges for access to revocation or status information

The Trust Center does not charge for access to revocation or status information for the relevant parts that fall under the scope of this document. The Trust Center allows third parties, who themselves market products and services, to access and retrieve revocation and status information only with prior express written permission.

Third parties require prior express permission in writing before marketing the certificates and status information that the Trust Center provides publicly or providing them for marketing.

9.1.4 Charges for other services

The Trust Center 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 the written consent of the authority (Section 1.5.1, 9.5.2) that owns the copyright.

9.1.5 Reimbursement of charges

DT Security GmbH reimburses charges in accordance with the legal regulations under German law. Detailed provisions can be found in the document "TeleSec-ServerPass General Terms and Conditions" [GT&C].

9.2 Financial responsibilities

Financial responsibilities are determined in the "TeleSec-ServerPass General Terms and Conditions."

9.2.1 Insurance coverage

DT Security GmbH is integrated into the DTAG liability Group insurance program. The liability insurance coverage goes far beyond the level of insurance coverage requested in the requirements.

There is additional insurance over the coverage required under eIDAS (2.5 million per incident of damage).

9.2.2 Other financial resources

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

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) of the TSP, which is not covered by Section 9.3.2.

9.3.2 Scope of non-confidential information

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

9.3.3 Responsibility regarding the protection of confidential information

The Trust Center, as the PKI service provider, is responsible for protecting confidential information and ensuring compliance with data protection regulations.

9.4 Protection of personal data (data privacy)

The points of data privacy and data security are described in the TeleSec-ServerPass General Terms and Conditions [GT&C].

9.4.1 Data privacy concept

Within the TSP, personal data is stored and processed electronically in order to provide services. A data protection concept has been drawn up for the TSP in accordance with the Group provisions. This data privacy concept summarizes the aspects of the PKI service that are relevant to data protection.

Excerpts from the data privacy concept can be provided upon request.

9.4.2 Data to be treated as confidential

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

9.4.3 Data not to be treated as confidential

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

9.4.4 Responsibility for the protection of confidential data

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

9.4.5 Notification and consent for the use of confidential data

The certificate customer consents to the use of personal data by a CA or RA insofar as it is necessary for service provision purposes.

Furthermore, all information may be published that is not treated as confidential in accordance with Section 9.4.3.

9.4.6 Disclosure in accordance with legal or administrative processes

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 (Copyright)

The following Sections 9.5.1 to 9.5.4 apply for intellectual property rights of end entities and relying parties.

9.5.1 Property rights to certificates and revocation information

The certification authority reserves all intellectual property rights to certificates, revocation or status information, publicly accessible directory services, and databases with the information contained therein, which the TeleSec ServerPass CA issues or manages.

If certificates and their contents state the origin of this certificate hierarchy in full and without changes, the certification authority gives its consent for certificates to be reproduced and published on a non-exclusive basis and free of charge.

The certification authority gives its consent for revocation lists and status information to be reproduced and published, especially to relying parties, on a non-exclusive basis and free of charge, provided that the use of revocation or status information and their contents and the origin of this certificate hierarchy are stated in full and not changed.

9.5.2 Property rights of this CPS

This document is copyright protected; all intellectual property rights belong to DT Security GmbH. Any other use (e.g., duplication, use of texts and images, changes, or creation of a comparable or derived document, transmission to persons who are not interested in the service described in this document), including as excerpts, is subject to the express prior written consent of the publisher of this document (see Section 1.5.1).

9.5.3 Property rights to names

The end entity reserves all rights, where applicable, to names or trademarks contained in the certificate, provided that the certificate has a unique name.

9.5.4 Property rights to keys and key material

The intellectual property rights of the CA's key material remain with DT Security GmbH, regardless of the medium on which they are stored. Copies of CA certificates may be duplicated in order to integrate them in trusted hardware and software components.

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

9.6 Assurances and guarantees

9.6.1 Assurances and guarantees of the certification authority

The TSP is responsible for all aspects of providing the certification service as well as for activities that are outsourced to subcontractors. The TSP has clearly regulated the responsibilities and made suitable provisions to allow the certification instance to perform checks at third parties.

The certification authority ensures that the security of the information is maintained even if the tasks of the certification authority are outsourced to other organizations.

The certification instance has a documented agreement and current contractual relationship that supports the provision of the PKI service with regard to delivery, outsourcing of operating functions, or other agreements with third parties.

The relevant "delegation of activities" rules from the [CABF-BR] also apply.

The TSP undertakes to ensure that

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

Furthermore, it is assured that at the time of issuance of an SSL/TLS certificate:

1) A defined procedure is in place to ensure that the subject has the right to use the domains and/or IP addresses named in the certificate. Alternatively, that the subject 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
3) The procedure described under 1) is specified in detail in this CPS
4) A defined procedure is followed to ensure that the certificate subscriber (subject) named in the certificate has approved the issuing of the certificate and that the subject's representative is authorized to make the request
5) The procedure described under 4) is followed
6) The procedure described under 4) is specified in detail in this CPS
7) A defined procedure is followed to check that, with the exception of the OU field, all the information contained in the certificate is correct in the subject DN
8) The procedure described under 7) is followed
9) The procedure described under 7) is specified in detail in this 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
12) The procedure described under 10) is specified in detail in this 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 in place and followed, which meets the requirements of the version of the [CABF-BR], Sections 9.2.4 and 11.2, valid at the time the certificate is issued.
14) The procedure described under 13) is specified in detail in this CPS
The TSP further assures that

15) If the subscriber is a Group company (affiliate), the subject's representative must accept the "General Terms of Use" before issuing a certificate.
16) If the certificate holder is not a Group company (affiliate), the subject agrees the "TeleSec-ServerPass General Terms and Conditions" and the ServerPass Services and Terms of Use with DT Security GmbH in a legally enforceable form.
17) A publicly accessible directory is operated which contains status information on certificates. This directory is available 24/7.
18) The issued certificates will be revoked in the event of all reasons listed in the [CABF-BR]
19) If the certification authority becomes aware of a reason for revocation, the certificates in question will be revoked in a timely manner.

9.6.2 Assurances and guarantees of the registration authority (RA)

All registration authorities commit 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 request 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 Assurances and guarantees of the end entity

End entities commit to the following:

- To generate a certificate request (PKCS#10) that meets the technical requirements from Section 6.1.6.
- To protect their private key against unauthorized access by third parties. In the case of private keys of legal persons, the protection is provided by authorized persons.
- To only use the end-entity certificate in the intended way and not to misuse it.
- That the certificate is validly used (not expired and not revoked).
- To check that the certificate contents of the subjectDN included in the end-entity certificate reflect the truth. In the case of legal persons, the certificate contents are checked by authorized persons.
- To bear the legal consequences arising from non-fulfillment of the obligations described in this CPS
- In the event of loss or suspected compromising of the private key, to carry out the revocation of the corresponding end-entity certificate or to arrange for this to be done by the registration authority.
- In the event that the private key is compromised, use of this private key must be ceased immediately and permanently.

- That the certificate issued is only used for authorized and legal purposes that correspond to this CPS and do not contradict the provisions of this statement.
- That all statements made in the certificate request, which resulted in the certificate being issued, correspond to the truth.
- That the end entity is in fact an entity and does not carry out any CA functions, such as signing of certificates or revocation lists, with its private key assigned to the public key contained in the certificate.
- To immediately revoke the end entity certificate and therefore declare it invalid if the certificate statements are no longer correct or if the private key has been lost, stolen, compromised, or thought to have been otherwise misused.

Note: DT Security GmbH reserves the right to agree other obligations, assurances, consents, and guarantees vis-à-vis the end entity.

9.6.4 Assurances and guarantees of relying partiesr

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.

Relying parties should

- Check the validity of the certificates via the status services offered in accordance with Sections 4.9.10 and 4.10.
- Take into account the restrictions on the use of the certificates set out in the terms of use or in the certificate.
- Take any other precautions that may be required of third parties under agreements or other provisions.

9.6.5 Assurances and guarantees of other participants

No stipulation.

9.7 Exclusion of liability

The exclusion of liability is regulated in the applicable TeleSec-ServerPass General Terms and Conditions [GT&C].

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. In all other respects, liability for damage resulting from a breach of obligations due to negligence will be governed by the TeleSec-ServerPass General Terms and Conditions [GT&C] or by individual contracts.

9.9 Claims for damages

Claims for damages are regulated in the applicable TeleSec-ServerPass General Terms and Conditions [GT&C].

9.10 Term and termination

9.10.1 Term

The CPS comes into effect when it is published on the Trust Center websites.

Changes also take effect when they are published on the public websites (see Section 2.3).

9.10.2 Termination

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

9.10.3 Effect of termination and continuance

When the TeleSec ServerPass service ends, all users remain bound by the regulations contained in the CPS until the last certificate issued expires or is revoked.

9.11 Individual notices and communications with participants

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

9.12 Amendments to the CPS

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

9.12.1 Procedure for amendment

Amendments to the CPS can only be made by the Trust Center Change Advisory Board. With every official amendment, 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 Trust Center Change Advisory Board will decide on how to proceed.

9.12.2 Notification procedures and periods

Resellers will be notified of amendments and given the opportunity to object within six weeks. If no objections are made, the new document version enters into force as specified in Section 9.12.1. Any claims beyond this for individual end users to be notified are explicitly excluded.

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

9.13 Provisions for settling disputes

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

9.14 Applicable law

The law of the Federal Republic of Germany shall apply.

9.15 Compliance 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.

9.16 Miscellaneous provisions

9.16.1 Complete contract

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability clause

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

Telekom Security shall not be liable if, due to force majeure, the contractual performance is significantly impeded or the proper execution of the contract is temporarily impeded or impossible.

9.17 Other provisions

9.17.1 Barrier-free accessibility

Access to the TC services is essentially browser-based. Operating systems offer a variety of different accessibility features to make it easier for disabled persons to access the web portals of the Trust Center Services. In particular, these compensate for visual and hearing impairments, physical disabilities, and sensory disorders (e.g., "Information on barrier-free accessibility for IT experts").

If the above-mentioned measures are insufficient, the Trust Center also offers disabled persons free telephone support for assistance with the application for, acceptance, and revocation of certificates.

10 OTHER APPLICABLE DOCUMENTS AND REFERENCES

10.1 Other applicable documents

Table 9: Other applicable documents

Reference/no.	Document name	Link
[GT&C]	TeleSec-ServerPass General Terms and Conditions	https://telesec.de/de/service/downloads/allgemeine-geschaeftsbedingungen/
[PDS]	PKI Disclosure Statement	https://telesec.de/de/service/downloads/pki-repository/

10.2 References

Table 10: References

Reference	Document name
[BDSG]	Federal Data Protection Act [Bundesdatenschutzgesetz]
[CABF-BR]	Current version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" document published by CA/Browser Forum (https://cab-forum.org).
[CABF-BREV]	Guidelines For The Issuance and Management Of Extended Validation Certificates, The CA/Browser Forum
[ETSI EN TSP]	ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures
[ETSI EV]	ETSI EN 319 411-1, policy EVCP. "Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates," European Telecommunications Standards Institute
[ETSI POL]	ETSI EN 319 411-1, policy OVCP. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
[ETSI QC]	ETSI EN 319 412-5, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[ETSI QCP-w]	ETSI EN 319 411-2, policy QCP-w. "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates."
[ETSI WEB]	ETSI EN 319 412-4, Electronic Signatures and Infrastructures (ESI);

	Certificate Profiles; Part 4: Certificate profiles for web site certificates issued to organizations
[PKCS]	RSA Security Inc., RSA Laboratories "Public Key Cryptography Standards" http://www.rsa.com/rsalabs/
[PKIX]	RFCs and specifications by the Public Key Infrastructure (X.509) IETF working group
[RFC2560]	X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol - OCSP
[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
[RFC6844]	DNS Certification Authority Authorization (CAA) Resource Record, P. Hallam-Baker, R. Stradling IETF, 2013
[RFC6960]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, S. Santesson et. al., IETF, 2013
[SOGIS]	Senior Officials Group Information Systems Security (https://www.sogis.eu/)
[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), http://www.itu.int/rec/T-REC-X.509/en/https://www.itu.int/rec/T-REC-X.509/en/

11GLOSSARY

Table 11: Glossary

Abbreviation	Description
Authentication	Checking an identity based on claimed characteristics.
Authority Revocation List (ARL)	List containing revoked digital certificates of certification authorities (CA and 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.
Certificate	See Digital certificate
Certification authority authorization (CAA)	A procedure that allows the domain owner to specify in the DNS which certification authority (or authorities) can issue certificates for its domain(s).
Certification authority revocation list (CARL)	See ARL
Certificate Signing Request (CSR)	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.
Certificate Policy (CP)	Defines the guidelines for generating and managing certificates of a certain type.
Certificate revocation list (CRL)	See Revocation list.
Certificate transparency	A Google project for certificate transparency: issued certificates are written to publicly verifiable, tamper-proof log servers to be able to identify and revoke improperly or incorrectly issued TLS/SSL certificates more quickly. The requisite CT log servers are contacted while the certificate is being issued. These, in turn, return one SCT each in their response, which are then stored in the certificate and prove that the certificate was registered in a log server.
Certification Authority	Component that issues digital certificates by digitally signing a data record consisting of a public key, name, and various other data. The certification authority also issues revocation information.
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.
Certificate subscriber	A natural or legal person who is issued a certificate and is legally bound by a subscriber agreement or terms of use.
Cross-certificate	A sub-CA certificate issued by an established root certificate for a new root certificate that does not yet have high market penetration. It ensures that certificate validation is successful by using an alternative validation path to a second root certification authority.
crt.sh	A search engine to search for certificates in all public CT logs (certificate transparency).

Digital signature	A checksum created with a special mathematical procedure. Guarantees the authenticity of the signatory and the integrity of the data.
Digital certificate	Data record that contains the name of a person or a system, its public key and, if necessary, a few other details and a signature of a certification authority.
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 Name Systems	Hierarchical directory service that manages the namespace of the internet. It is mainly used to resolve domain names into IP addresses.
Electronic signature	See Digital signature.
End entity	See also certificate 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.
Device certificate	X.509 V3 certificate that contains either a host name or an IP address in the commonName field (CN) of the subscriber's distinguishedName (subject) field and/or in at least one subjectAltName extension.
Period of validity	The period from the issue date (not before) until the expiry date (not after).
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.
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).
Legal person	A company, group, partnership, sole trader, trust, government authority, or legal entity with legal standing within the legal system of a country.
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.
Cryptography	Science dealing with the encryption of data and related issues (such as digital signatures).
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.
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.
Terms of use	Provisions regarding safekeeping and permitted usage of an issued certificate in accordance with the specified requirements if the subject/certificate subscriber is an affiliated company of the certification authority (CA), for example.
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.
Online Certificate Status Protocol (OCSP)	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.
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).
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 device certificate	A device certificate that a sub-CA issues in the CA hierarchy below a root certificate.
Phishing	Method of internet attack to get at (private) data (e.g., PINs, TANs, passwords) of an internet user. The victims are usually lured to forged websites and asked to enter data. Since the website appears to be official at first glance, the user is often willing to provide this data.
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 Key Infrastructure X.509 (PKIX)	IETF standard that standardizes all relevant parts of a PKI.
Policy	Guidelines that determine the security level for creating and using certificates. A distinction is made between Certificate Policy (CP) and Certification Practice Statement (CPS).
Public Key Infrastructure	Total sum of the components, processes, and concepts that are involved in using public key processes. Typically, a public key infrastructure consists of central components such as a certification authority and a directory service and different client components.
Registration authority	Component with which a person or a system must communicate to obtain a digital certificate.
Registration Authority (RA)	Component with which a person or a system must communicate to obtain a digital certificate.

Request	English term for "Auftrag." Taken to mean a certificate request in this context.
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-CA)
Secure Multipurpose Internet Mail Extension (S/MIME)	Secure Multipurpose Internet Mail Extension. Extension of the MIME email format, which describes additions for cryptographic services that guarantee the authenticity, integrity, and confidentiality of messages.
Key	In cryptography, a key refers to secret information (private key) or an official opposite to it (public key). There are procedures where data is encrypted and decrypted using the same private key and where a public key is used for encryption and a private one is used for decryption.
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.
Secure Socket Layer (SSL)	Term used previously to describe Transport Layer Security. For further explanations, refer to Transport Layer Security.
Signature	See Digital signature.
Smartcard	Chip card with computing function that can be used for cryptographic purposes.
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.
Revocation authority	Component that revokes the certificates.
Revocation list	List of digital certificates that have been revoked. Before a digital certificate is used, a revocation list should be used to check whether it may still be used. It is also referred to as certificate revocation list (CRL).
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-CA).
Subject Alternative Name	Additional fields in a certificate. The fields must contain at least one additional name of the certificate holder and are a standard extension of the X509 standard.
Subject Distinguished Name (Subject-DN)	Subject = person or machine. Format with which unique names can be specified in accordance with the X.500 and the LDAP standard. The subjectDN clearly identifies the subscriber.
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 the subscriber.
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 registrar.

Trust Center Advisory Board	A board within DT Security GmbH that decides on PKI functions.
Transport Layer Security (TLS)	Crypto protocol for ensuring end-to-end connections on the internet. Can be used instead of the more complex IPSec in many cases.
Unified Communications Certificates (UCC)	Certificates that allow the Subject Alternative Name fields to be used. This allows several names to be covered by one certificate.
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).
Validation	Evidence of the reproducibility of a result from a described procedure under defined conditions. The more precisely a procedure is described and the fewer unknown influencing factors there are, the more certain it is that corresponding results will be produced. A description of the goal and method is required for a validation. In this context, valid means that the method leads to the result in a repeatable manner. In the context of a PKI, there is a validation process at the following points for example: ▪ Determining and checking an identity (e.g., natural person, device) for a certificate request. ▪ Algorithm to check a certificate for its validity period, issuing certification authorities and certificate status (valid, revoked).
Affiliated company (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.
Relying parties	An individual person or legal entity (e.g., company, organization) that acts in reliance on the functioning of a certificate.
Directory service	Database that enables certificates and information about certificates (especially revocation lists) to be called up.
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).
Web request	Variant of a certificate request where the data is transmitted to the certification authority via a web form.
WebTrust	Checking and confirmation for certification authorities (WebTrust for Certification Authorities) by an independent auditing firm that the PKIs are operated in accordance with the WebTrust criteria "American Institute of Certified Public Accountants" (AICPA). The aim of WebTrust audits is to strengthen demand-side trust in electronic business transactions.
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.
Root certification authority	Root certification authority (root-CA)

X.509	Standard, whose most important element is a format for digital certificates. Version X.509v3 certificates are supported in all common public key infrastructures.
zLint	A tool that checks certificates for consistency with RFC5280 and [CABF-BR].
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 subject.

12ACRONYMS

Table 12: Acronyms

Acronym	Explanation
GT&C	General Terms and Conditions
AICPA	American Institute of Certified Public Accountants
ASP	Application Service Provider
ARL	Authority Revocation List
CA	Certification Authority
CAA	Certification Authority Authorization
CP	Certificate Policy
CPS	Certification Practice Statement
CN	Common Name
CRL	Certificate Revocation List
CT	Certificate transparency
DCF77	Time signal transmitter (long wave transmitter) in Mainflingen near Frankfurt am Main
DIN	German Institute for Standardization
DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name Systems
DTAG	Deutsche Telekom AG
eIDAS	Regulation on electronic identification and trust services (electronic Identification and Signature)
ETSI	The European Telecommunications Standards Institute. ETSI is a non-profit organization officially recognized by the European Union as a European Organization for Standardization and aims to create worldwide standards for information and communication technologies.
EV	Extended Validation
EVCP	"Extended Validation" Certificate Policy
FQDN	Fully Qualified Domain Name
GPS	Global Positioning System
GR	Identifies a group, function, or role certificate
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IETF	Internet Engineering Task Force
IPSec	Internet Protocol Security
ISMS	Information Security Management System

ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
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
PU	Productive Unit (live environment)
RA	Registration authority
RAOP	RA Operator (order processing / validation expert / validation specialist)
RFC	Request for Comments
RSA	Rivest Shamir Adleman
SCT	Signed Certificate Timestamp
S/MIME	Secure Multipurpose Internet Mail Extension
SAN	See Subject Alternative Name
SigG	Signaturgesetz (German Digital Signature Act)
SigV	Signaturverordnung (German Digital Signature Regulation)
SOAP	Simple Object Access Protocol
SOGIS	Senior Officials Group Information Systems Security
SSL	Secure Socket Layer
TLS	Transport Layer Security
TU	Test Unit (test environment)
UCC	Unified Communications Certificates.
UPN	User Principal Name
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
XML	Extensible Markup Language