CP/CPS TeleSec ServerPass

Deutsche Telekom Security GmbH

Certificate Policy and Certification Practice Statement (CP/CPS)

Version	14.00
Last revised	September 29, 2020
Status	Final

public

Publication details

Published by

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

File name	Document number	Document name
CP_CPS_TeleSec_ServerPass_EN_V14.00.docx		Certificate Policy and Certification Practice Statement (CP/CPS)

Version	Last revised	Status
14.00	September 29, 2020	Final

Brief info

Certificate Policy and Certification Practice Statement on TeleSec ServerPass (CP/CPS)

Change history

Version	Last revised	Edited by	Changes/comments
1.0	November 28, 2000	BREU	Initial version
2.0	September 1, 2001		Inclusion of new items
3.0	November 11, 2003	EICK	Adjustments to Section 10 Certificate hierarchy update, content revision, layout changes
3.4	May 4, 2007	EICK	Certificate hierarchy update Content revised 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	April 14, 2010	EICK, KOELSCH, VOELKEL	Replaces CPS_ServerPass_V3.4 and CPS_ServerPass_EV_V1.0 Structured as per RFC3647; all chapters have been revised and content updated accordingly; layout adapted.
2.0	July 1, 2013	UVOEL; MGRA, LEICK	The entire document was revised and extended. and further details added
3.0	March 25, 2015	UVOEL,LEICK, MBU;MET	The entire document was revised, updated and extended. and further details added
4.0	April 14, 2016	METR	revised and updated as part of the document review Release
5.0	April 19, 2017	LEICK, LREIT, MBURK METR, ATRE	Section 6.1.5 updated, Section 4.2.3 extended. Section 5.7.1 extended, Section 6.5.1 and Section 6.5.1.1, Section 6.1.1 und Section 5.4.8 extended, Section 1.3.1 extended EV um EV SAN extended, Kap. 4.11 extended Extensions for eIDAS Quality check and release
6.0	28.03.2018	METR	Release version
7.0	20.04.2018	LEICK	Release of M. Etrich
8.0	02.08.2018	METR	Release of M. Etrich
9.0	11.10.2018	DDIENS	Release of D. Dienst
10.00	16.10.2018	METR	Release of M. Etrich
11.00	31.10.2019	METR	Release of M. Etrich
12.00	04.03.2020	HH	release
12.01	25.06.2020	MG	Incorporation of Audit Findings; Update section 1, 1.5.1, 1.5.2, 2.2, 3.1.1.1, 3.2.5.2, 4.2.1.1, 4.2.1.2, 4.2.2, 4.9.7, 5.3.4, 5.4.1.3, 5.5.5, 6.3.2, 6.5.2, 7.3.1, 9.6.1; Change from T-Systems to Telekom Security
12.02	26.06.2020	MG	Quality check and preparation for release
12.03	26.06.2020	GK	QS
13.00	26.06.2020	HH	Release
13.01.	24.09.2020	LE	The term customer portal was replaced by service portal, T-Systems was replaces by certification authority or Trust Center, Changes of glossary. Updates in sections 1.5.2, 2.2, 3.2.2.1, 3.2.2.2, 3.4, 3.4.1, 7.1.2.9; figure 3 removed, Implementation of SC30 in section 3.2.2
13.02	28.09.2020	LE	QS
13.03.	29.09.2020	LE	QS

Version	Last revised	Edited by	Changes/comments
14.00	29.09.2020	HH	Release

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

Table of contents

List of figures

List of tables

1 Introduction

Deutsche Telekom AG is operating a Trust Center (Telekom Trust Center) since 1994, which in 1998 became the first nationwide Trust Center to produce certificates for digital signatures in accordance with the german signature law (Deutsches Signaturgesetz, SigG).
The Trust Center was operated by the Group unit T-Systems International GmbH and has been certified according to ISO 9002 since 1996 and ISO 9001:2000 since January 2001.
The operation went on as part of a spin-off to Deutsche Telekom Security GmbH (hereinafter referred to as "Telekom Security") on July 01, 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. This division from chapter 1.5.1 is responsible for ensuring that the described processes, activities, systems, roles and security measures are also enforced in the event that 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 certificate owner, 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.

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.

TeleSec ServerPass SAN/UCC:
ServerPass SAN/UCC likewise 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

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 [CAB-BREV] for example (see Section 10.2) and an enhanced registration process.

TeleSec ServerPass EV SAN:
ServerPass EV SAN likewise fulfills the general features outlined above and compared to ServerPass EV 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 and ServerPass EV SAN 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.

eIDAS:

All EV variants meet the eIDAS requirements for EU qualified certificates and the ETSI EN 319 411-2 policy for QCP-w. ServerPass EV meets the requirements for qualified trust service providers (TSP) or qualified trust services for website authentication in accordance with eIDAS regulation (EU) No 910/2014.

Websites that use extended validation certificates are highlighted in color in current 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. This makes the lengthier registration and validation process visually apparent to the user.

When registering ServerPass EV *and* also ServerPass, 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.

The present document contains the Certificate Policy (CP) and the Certification Practice Statement (CPS) of the TeleSec ServerPass service and includes security provisions and descriptions of technical, organizational and legal aspects. Furthermore, it describes the activities of the Trust Center operator in its function as Certification Authority (CA) and Registration Authority (RA).

It supplements the General Terms and Conditions for TeleSec products [GT&C] by describing the issuance and management procedures for TeleSec ServerPass as part of the certification-based Public Key Infrastructure (PKI). The CP/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 [CAB-BREV].

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

1.1.1 Complying with the baseline requirements of the CA/Browser Forum

The Trust Center ensures that SubCAs used for TeleSec ServerPass comply with and fulfill the requirements and regulations of the published [CAB-BR] as amended (http://www.cabforum.org/documents.html). In the event that this document and the [CAB-BR] contradict one another, the regulations from the [CAB-BR] have priority.

1.2 Document identification

Name:	CP/CPS TeleSec ServerPass
Version:	14.00
Last revised:	September 29, 2020

The present CP/CPS supports the following Certificate Policy OIDs:

ServerPass Standard and SAN/UCC:	(1.3.6.1.4.1.7879.13.2)
ServerPass EV / EV SAN:	(1.3.6.1.4.1.7879.13.24.1)
Compliance with [CAB-BR] Organizational Validation	(2.23.140.1.2.2)
Compliance with [CAB-BR] Domain Validation	(2.23.140.1.2.1)
Extended Validation [CAB-BREV]	(2.23.140.1.1)
Extended Validation Certificate Policy (EVCP) [ETSI POL]	(0.4.0.2042.1.4)
QCP-w: cert. policy for EU qual. website auth. cert. [ETSI POL]	(0.4.0.194112.1.4)

The present document refers exclusively to the product variants of the certification practice TeleSec ServerPass.

1.3 Parties involved in PKIs

The following 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/CPS 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 root certification authorities for each product variant. Depending on the product properties root-CA and/or sub-CA may vary. New trust points or Sub-CAs may be offered or existing ones may be removed from the market. The underlying reason are changing national or international requirements, new security standards, compromised existing security method or other reasons. If costs arise due to these changes for the customer, they are not chargeable to Deutsche Telekom Security GmbH.
The current root-certificates offer a high market penetration, compatibility and flexibility. With the help of the installation of intermediate certificates, interpretable security hints for the enduser will be reduced during a connection buildup. An overview of all certification authorities is listed 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 exclusively offer end-entity certificates and they are used to sign 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 bases on the shell model. This way each new certificate has a maximum validity time depending on the validity time of the issuing certificate.

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

There are various root certification authorities (Root CAs) available for TeleSec ServerPass. This can be selected during commissioning. An overview of the certification authorities is shown in the following figures. The scope of this document covers the sub-CA's and certificates within the red dashed areas of these figures.

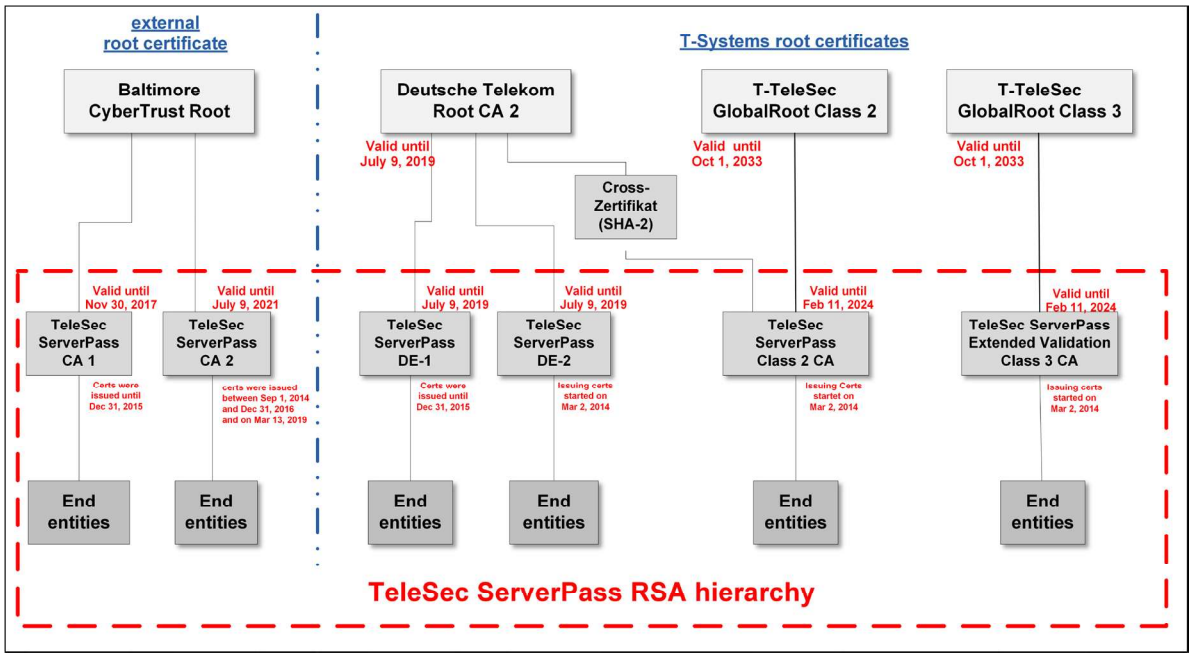

Figure 1: Overview of RSA certificate hierarchies for TeleSec ServerPass

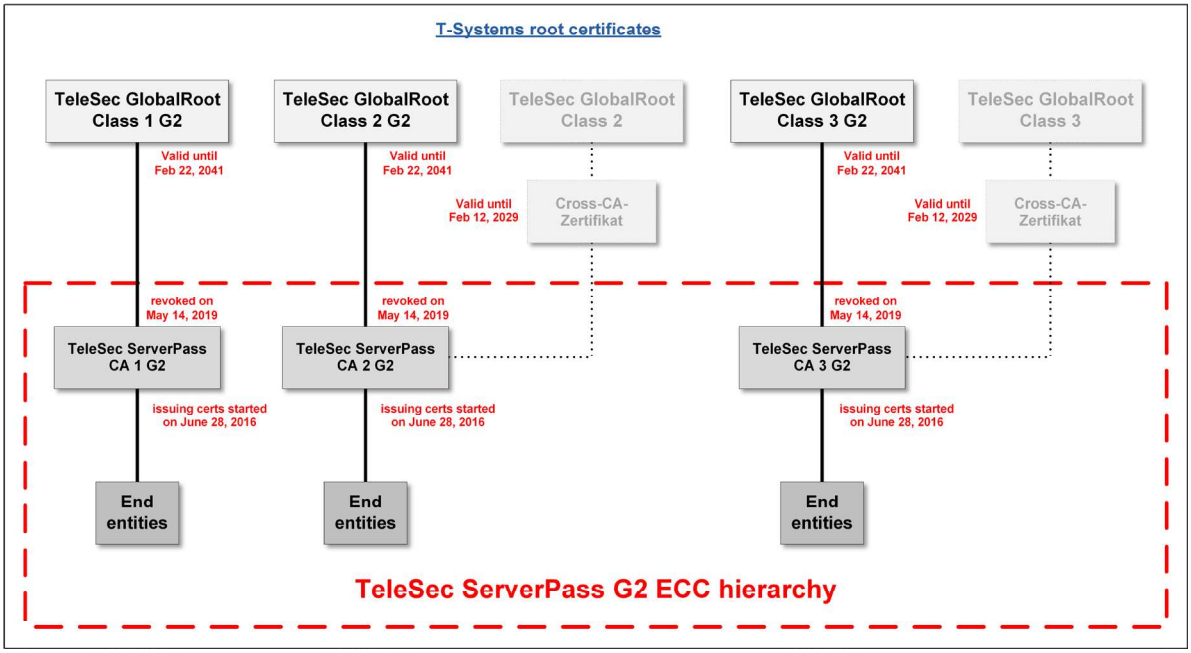

Figure 2: Overview of G2 ECC certificate hierarchies for TeleSec ServerPass

Both the root certification authority (Class 3 root-CAs) and the subordinate certificate authorities (Sub-CAs) are operated in compliance with the currently applicable guidelines for 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.

The direct root certification authority (Root CA) for a Sub-CA can vary.
This is the case if:

- The Root CA in the application being used (e.g. web browser) has not yet been defined as trusted.
- The application used (e.g. web browser) follows a validation logic that does not check for the direct Root CA.

Reference is made optionally in such cases to another defined root certification authority.

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

The tasks of the Trust Center registration authority are in particular:

- Accepting requests and checking the identification documents
- Checking the documents for authenticity and completeness
- Identifying the legal person (see Section 3.2)
  - Organization check
  - Identity check
  - Domain check
  - Authorization check
- Approval of certificate issuance
- Revocation of certificates if reasons for revocation exist (see Section 4.9)

No third-party registration authorities (external RA) 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 [CAB-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, 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 archive, for example.

1.3.5 Other subscribers

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

1.4 Certificate usage

1.4.1 Permitted usage of certificates

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.

1.4.1.1 Certificates for legal persons

Purpose of TLS/SSL certificates				
	Signature and/or encryption	Authentication	Secure online communication	Inspection/Proof level
TeleSec ServerPass Standard	✓	✓	✓	medium
TeleSec ServerPass SAN/UCC	✓	✓	✓	medium
TeleSec ServerPass EV / EV SAN (Extended Validation)	✓	✓	✓	high

Table 1: Use of certificates for legal persons

1.4.2 Prohibited usage of certificates

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, 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 (CP/CPS) is issued 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 (0) 1805 268 204 (landlines: EUR 0.14/minute, mobile networks: max. EUR 0.42/minute)
E-mail: telesec_support@t-systems.com
Internet: https://www.telesec.de

For general inquiries please use https://www.telesec.de/de/service/kontakt/anfragemitteilung/.

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

1.5.3 Authority, that decides upon the consistency of this document with the CP

The organization named in Section 1.5.1 is responsible for this document (CP/CPS) and the compliance to higher-level certificate policies..

1.5.4 Approval procedure of this document (CP/CPS)

The approval procedure depends on a formal document release process defined within the organization of the publisher.

This document (CP/CPS) 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 can be found in Section 12.

2 Responsibilities for publications and databases

2.1 Databases

The Trust Center operates a directory service and a database for the TeleSec ServerPass service and is responsible for the contents.
Extracts from these databases are provided, preprocessed and the basis for issuing certificate information and a certificate revocation list (CRL) on directory services or they may be used to provide status information for the validation service (OCSP responder).
Documents of relevance for publication are also made available via a central repository. These include, in particular, the relevant CP and/or CPS documents of the concerned root and subordinate certification authorities (root- and Sub-CAs). This directory is available 24/7. The maximum downtime is 1,5 days as a monthly average.

The Trust Center applies measures and mechanisms to protect the central repository against unauthorized manipulation (addition, change or deletion) of information.

2.2 Publication of certificate information

The certification authority publishes a certificate revocation list (CRL) at regular intervals. The certificate revocation list contains certificates that were issued by the TeleSec ServerPass CA and then revoked before reaching the expiry 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 Internet protocol "Online Certificate Status Protocol" (OCSP) and returns the status of X.509 certificates.

Current ServerPass documents are available at:
https://www.telesec.de/de/service/downloads/pki-repository/

Explanatory note regarding the structure:

- The ServerPass CP/CPS can be found under "Certificate Practice Statements (CPS) -> ServerPass"
- The ServerPass PDS can be found under "Practice Disclosure Statements (PDS)"
- The ServerPass Sub-CA certificates can be found under "Sub-CA Certificates -> ServerPass"

The corresponding Root-CA certificates can be found under "Root-CA Certificates"

Server certificates that contain a CT-Log entry (see Section 4.2.2) are published via log servers for third parties (e.g. Google).

In addition there are test pages (e.g. for software developers) which offer information about the current status (valid, suspended, invalid) of a webserver certificate depending on the root-CA.

Test pages are available at:

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

The information above will be published on the website of the certification service provider (www.telesec.de) under the section "Root program". In addition, in the event of security-critical incidents, the certificate holders are notified directly in writing, on the internet or by e-mail.

Changes to the information security policy of the TeleSec ServerPass-CA are forwarded to the auditors (see Section 8 forward) and/or the regulatory offices (information are forwarded from the Deutsche Telekom AG to the Federal Office for Information Security (BSI).

TeleSec ServerPass-CA offers a reverse search for end-entity certificates under https://www.telesec.de/de/root-programm/support/pki-service-ermitteln/

The following information is shown:

- Issuer-DN
- Subject-DN
- Serial number
- Valid not before
- Valid not after
- Public key size (bits)
- Signature algorithm
- Links to the:
  - Certificate Policy (CP) and Certification Practice Statement (CPS)
  - Service description
  - General Terms and Conditions (AGB)
  - Terms of use
  - PKI Disclosure Statement (PDS)
  - CA certificates

Notice: The reverse search is currently supported only by the browsers (full versions) Mozilla Firefox and Google Chrome.

2.3 Update of the information (Publication time and frequency)

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

The CP/CPS to hand is subject to an annual review independently of additional changes.
The department named in Section 1.5.1 is responsible for carrying out or coordinating the annual review.

The annual review will be documented in the change history of the CP/CPS, even if there are no changes of the content necessary. Current developments, changes or changed requirements (e.g. based on the CABF-BR) are monitored and added to the release plan.

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

2.4 Access to the databases 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 the revocation lists and OCSP-responses are guaranteed based on digital signatures of trustworthy signers (see Section 4.10.1).

Certificate holders and users also have unrestricted read access to information from the CA and root-CA (see Section 2.2) via the relevant websites. This likewise applies for the directory of published CP/CPS documents.

3 Identification and authentication

3.1 Naming conventions

A Distinguished Name (DN) is a unique, global name for directory objects according to 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)

3.1.1 Name forms

The certificate holder's identity is checked for all SSL/TLS certificate issued. The relevant information is transferred to the certificate.
At least the following 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. Deviations are clearly displayed. In order to correct these deviations without creating new requests, these fields can be changed manually by the client. The certificate issued with these changed fields will then no longer corresponds to the data of the original request. There can be applications and constellations (e.g. Microsoft IIS) in which problems during the installation (import) of the certificate may arise. It is therefore recommended to use a new certificate request for this assignment rather than the corrected request.

No domain validation certificates (DV) are issued.

With the exception of the field subject:organizationalUnitName (OU) only information that has been checked for correctness (accuracy and completeness) is entered in a subject field.
Use of "meta characters", such as "-", "." or " " (space) for indicating that a field is not filled with information of the certificate holder or is not relevant (n/a), is not permitted.

3.1.1.1 TeleSec ServerPass Standard and SAN/UCC: Conventions for naming elements

The English terms used below are also used to an extent in Germany these days.

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 by Telekom Security. 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.
Telekom Security no longer issues certificates from June 1, 2013 that contain an IP address or top-level domain from a reserved name 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.

OrganizationName (O) (mandatory field)
This field contains the organization name (e.g., company, institution, authority) of the certificate owner. The organization name in the certificate should have the official spelling of the organization, hence it should be identical to the respective register entry (commercial register or similar). The official abbreviation can also be used. In addition, the official spelling of the legal form can be deviated from, if a common abbreviation is used. It is not mandatory to specify the legal form. Example: O=sample company Limited Liability Company, O=sample company GmbH or O=sample company. The attribute "O" may only be specified once.
The certification authority checks this information during the course of the registration process based on the commercial register excerpt or equivalent, reliable directories/documents. Slight deviations in the spelling of the organization name can be accepted as long as the organization name is still unique (O=Alpha-Company Ltd or O=Alpha Company Ltd).
The certification authority will ask the applicant to correct it or document the accepted deviation from the official company name.

OrganizationalUnitName 1-5 (OU1) (optional)
This field is **optional** and 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. The attribute “OU” may be used more than once.
Examples: OU1=Procurement, OU2= Branch sample city
If information is provided in this field, so these will be verify it 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.

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 range 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.
For example: CN=www.example.com

The CommonName may contain the following characters: A-Z, a-z, 0-9, " . " (period), " * " (asterisk), " - "(hyphen)
The wildcard character (* asterisk) is only accepted to the extreme 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.

LocalityName (L) (mandatory field)
This field contains the name of the city in which the organization (e.g., company, institution, authority) is based.
The complete, official location name must be used.
If the location name exists several times in a country, the uniqueness must be additionally ensured by:
- Postleitzahl = postalCode
- and/or Bundesland = StateOrProvinceName (ST)
Example: L=Frankfurt am Main, L=Frankfurt (Oder)

The certification authority checks this information as part of the address during the registration process using the commercial register excerpt "HR excerpt" or equivalent, reliable directories/documents. Acceptable is also verifiable proof of a location other than the above document.

StateOrProvinceName (ST) (optional)
This field contains the 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 in brackets may also be used. The federal states of Bavaria, Saxony and Thuringia may also be prefixed with the designation "Free State".
Example: ST=Free State Bavaria

This information is checked during the registration process using the commercial register excerpt "HR excerpt" or equivalent, reliable directories/documents. Acceptable is also verifiable proof of a location other than the above document.

Country Name (C) (mandatory field)
This mandatory field contains a worldwide identification for a country. The code is made up of two letters, which is specified in ISO 3166-1, Alpha-2 (International Organization for Standardization). This field contains the name of the country in which the certificate owner has its registered place of business.

The certification authority checks this information as part of the address during the registration process using the commercial register excerpt "HR excerpt" or equivalent, reliable directories/documents. Acceptable is also verifiable proof of a location other than the above document.

Example: C=DE (for Germany/Deutschland)

Further details you may find at
http://www.unece.org/cefact/locode/subdivisions.html
http://www.nationsonline.org/oneworld/country_code_list.htm

StreetAddress (optional)
This field contains the name of the street where the organization (e.g., company, institution, authority) is based.
Example: street address=Sample street 17

This information is checked during the registration process using the commercial register excerpt "HR excerpt" or equivalent, reliable directories/documents. Acceptable is also verifiable proof of a location other than the above document.

Postal Code (optional)
This field contains the postal code/zip code of the city in which the organization (e.g., company, institution, authority) is based.
Example: postal code=12345

This information is checked during the registration process using the commercial register excerpt "HR excerpt" or equivalent, reliable directories/documents. Acceptable is also verifiable proof of a location other than the above document.

EmailAddress (E) (optional)
Data from the EmailAddress field is ignored and is not included in the certificate.

3.1.1.2 TeleSec ServerPass EV / EV SAN: Conventions for naming elements

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 either 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.

OrganizationName (O) (mandatory field)
This field contains the organization name (e.g., company, institution, authority) of the certificate owner. The organization name in the certificate should have the official spelling of the organization, hence it should be identical to the respective register entry (commercial register or similar). The official abbreviation can also be used. In addition, the official spelling of the legal form can be deviated from, if a common abbreviation is used. It is not mandatory to specify the legal form. Example: O=sample company Limited Liability Company, O=sample company GmbH or O=sample company. The attribute "O" may only be specified once.
The certification authority checks this information during the course of the registration process based on the commercial register excerpt or equivalent, reliable directories/documents. Slight deviations in the spelling of the

organization name can be accepted as long as the organization name is still unique (O=Alpha-Company Ltd or O=Alpha Company Ltd).
The certification authority will ask the applicant to correct it or document the accepted deviation from the official company name.

Organizational Unit Name 1 (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.
Examples: OU1=Procurement
If information is provided in this field, the certification authority will check and verify it in the course of the registration process. The certification authority will refuse to issue the EV certificate if a check is not possible or can only be carried out with great difficulty.

Common Name (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.
For example: CN=www.sampledomain.com
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.
The certification authority will check this information as well as the ownership relationships in the course of the registration process, using publicly accessible directories.

Locality (L) (mandatory field)

This field contains the name of the city where the organization has its registered place of business.
The complete, official location name must be used. Abbreviations, as well as other spellings or additions are not allowed.
For example: locality=Sample city

The certification authority checks this information as part of the address during the registration process using the commercial register excerpt "HR excerpt" or equivalent, reliable directories/documents. Acceptable is also verifiable proof of a location other than the above document.

State or Province (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 in brackets may also be used. The federal states of Bavaria, Saxony and Thuringia may also be prefixed with the designation "Free State".
Example: ST=North Rhine-Westphalia

The certification authority checks this information as part of the address during the registration process using the commercial register excerpt "HR excerpt" or equivalent, reliable directories/documents. Acceptable is also verifiable proof of a location other than the above document.

Country Name (C) (mandatory field)

This field contains the name of the country in which the certificate owner has its registered place of business. This is a code made up of two letters, which is specified in ISO 3166-1, Alpha-2 (International Organization for Standardization).
For example: C=DE
More details can be found here:
http://www.unece.org/cefact/locode/subdivisions.html
http://www.nationsonline.org/oneworld/country_code_list.htm

The certification authority checks this information as part of the address during the registration process using the commercial register excerpt "HR excerpt" or equivalent, reliable directories/documents. Acceptable is also verifiable proof of a location other than the above document.

Street Address (Street) (optional)

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

For example: street address=Sample street 17

The certification authority checks this information as part of the address during the registration process using the commercial register excerpt "HR excerpt" or equivalent, reliable directories/documents. Acceptable is also verifiable proof of a location other than the above document.

Postal Code (optional)

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

For example: postal code=12345

The certification authority checks this information as part of the address during the registration process using the commercial register excerpt "HR excerpt" or equivalent, reliable directories/documents. Acceptable is also verifiable proof of a location other than the above document.

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.

For example: businessCategory=Private organization

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

Jurisdiction of Incorporation or Registration (mandatory fields)

These **EV/EV SAN-specific** fields (according to the classifications named 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 state or province and city. The place of jurisdiction for a registering authority on a state/province level contains information about the country, but not the state or 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).

For example: jurisdictionOfIncorporationLocalityName=Sample locality
jurisdictionOfIncorporationStateOrProvinceName=Sample province
jurisdictionOfIncorporationCountryName=SC (Sample Country)

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 according to ISO 8601: YYYY-MM-DD. The details in the Registration Number field are stored in the certificate subject in the SERIALNUMBER field.

For example: SERIALNUMBER=HRB3244
SERIALNUMBER=2005-10-23

EmailAddress (E) (optional)

Data from the EmailAddress field are ignored and not taken over by the certificate.

3.1.2 Meaningful names

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

3.1.3 Anonymity and pseudonyms of the certificate owners

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

3.1.4 Rules on the interpretation of different name formats

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 that the choice of name does not infringe upon any brand names, trademarks, 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 Initial identity verification

An initial order may only happen after a successful registration at the service portal <myServerPass> and an identity verification.

3.2.1 Methods to prove possession of private key

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

3.2.2 Authentication of organization identity

Order information have to be verified based on at least one of the following check methods. A list with information about the Incorporating Agencies and Registration Agencies used to fulfil the verification requirements has been published in the online repository (https://www.telesec.de/de/service/downloads/pki-repository/) under the section “Validation Resources”.

3.2.2.1 Identity

The information about subject identity and address of the customer are verified according to at least one of the following methods:

1. A public authority in the territory of the lawful establishment, existence, or recognition of the customer (https://www.handelsregister.de, 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 DBA/trade name

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

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

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

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

3.2.2.4 Validation of Domain Authorization or Control

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

3.2.2.4.1 Validating the applicant as a domain contact

No stipulation.

3.2.2.4.2 Contact via e-mail, fax, SMS, or postal mail to domain contact

A random value will be sent via e-mail, fax, SMS (text message), or letter to the identified domain contact. The process waits for a corresponding reply with the help of the received random value. The process bases on the process of [CAB-BR] Section 3.2.2.4.2). It has to be considered that:

- an e-mail, fax, SMS, letter may confirm the ownership of several authorized domain-names
- the generated e-mail, fax, SMS or letter may be sent to different recipients. Precondition: The domain name registrar listed the recipients for the validated FQDN as representatives of the domain name registrant.
- the random value send via e-mail, fax, SMS or letter has to be unique
- an e-mail, fax, SMS or letter may be resent with the old random value, if the entire content and the recipients of the e-mail, fax, SMS or letter stay identical.
- the random value is valid for 30 days. In this time frame the recipient may send his reply / confirmation.
- as soon as the FQDN has been validated, other certificates for the FQDN may be issued. These additional certificates will end with the same validated FQDN.
- this method will also be applied for the validation of wildcard domain names

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

3.2.2.4.3 Phone contact with domain contact

No stipulation.

3.2.2.4.4 Constructed e-mail to domain contact

To confirm that the customer has the control over the domain, the domain administrator will send an e-mail using an e-mail address that is preceded by "admin," "administrator," "webmaster," "hostmaster," or "postmaster," followed by the "at" sign ("@"), then the domain name of the FQDN. The e-mail message MUST contain a random value that MUST be included in the reply mail. (Based on the process of [CAB-BR] Section 3.2.2.4.4.) It has to be considered that:

- each e-mail may confirm the rights for several FQDNs. Precondition: The authorized domain name in the e-mail is an authorized domain name for each FQDN which has to be confirmed.
- the random value of each value is unique
- the e-mail may be resent with the old random value, if the entire content and the recipients of the e-mail stay identical.
- the random value is valid for 30 days. In this time frame the recipient may send his reply / confirmation.
- as soon as the FQDN has been validated, other certificates for the FQDN may be issued. These additional certificates will end with the same validated FQDN.
- this method will also be applied for the validation of wildcard domain names

3.2.2.4.5 Domain authorization document

No stipulation.

3.2.2.4.6 Agreed-upon change to website

The customer must demonstrate the practical control of the commissioned FQDN. This is proven by the customer making an agreed upon change on a website.
To prove this, a one-time text file is to be stored under a specified path on the server (/.wellknown/pki-validation/serverpassdv.txt) by the customer.

- The certification authority must be able to access it via HTTP/HTTPS.
- A one-time, constructed random value is used.
- The random value is valid for a maximum of 30 days after its creation.
- The recipient inserts the random value at the defined location.

Once the FQDN has been validated using this method, certificates may also be issued for other FQDNs that end with all labels of the validated FQDN.

3.2.2.4.7 DNS change

In this validation process, the domain control is demonstrated through the targeted insertion of unique information in the DNS.

- A one-time, constructed random value is used.
- The random value is valid for a maximum of 30 days after its creation.
- The recipient inserts the random value in the DNS of the FQDN which is to be tested.

Once the FQDN has been validated using this method, certificates may also be issued for other FQDNs that end with all labels of the validated FQDN.
This method is also used to validate wildcard domain names.

3.2.2.4.8 IP address

No stipulation.

3.2.2.4.9 Test certificate

No stipulation.

3.2.2.4.10 TLS using a random number

No stipulation.

3.2.2.4.11 Any Other Method

No stipulation.

3.2.2.4.12 Validating Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact. This method may only be used if the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.
Note: Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

A contract with the domain management of Deutsche Telekom AG (registrar) contains a list of defined domains that are owned by the Telekom Group and may be used by defined Group entities. The commissioned FQDN of an internal customer is checked against this list.
In the case of internal orders from other group units, the registration employee will have the customer confirmed as an authorized domain contact by the domain management.

3.2.2.4.13 E-mail to DNS CAA Contact

No stipulation.

3.2.2.4.14 E-mail to DNS TXT Contact

No stipulation.

3.2.2.4.15 Phone Contact with Domain Contact

No stipulation.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

No stipulation.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

No stipulation.

3.2.2.5 Authentication for an IP address

This chapter describes the allowed processes and procedures to determine that the customer (or the parent company, the subsidiary company or the affiliated company of the customer, collectively referred to as the "customer" for the purpose of this section) is in possession or control of an IP address included in the certificate. Before issuing the certificate, it must be confirmed that each included IP address has been verified by at least one of the following procedures.

It is checked that the customer has or is in control of each IP address listed in a certificate at the time the certificate is issued.
The following methods are possible:

3.2.2.5.1 Agreed-Upon Change to Website

The customer must demonstrate the practical control of the commissioned IP address. This is proven by the customer making an agreed upon change on a website.
To prove this, a one-time text file is to be stored under a specified path on the server (/.wellknown/pki-validation/serverpassdv.txt) by the customer.

- The certification authority must be able to access it via HTTP/HTTPS.
- A one-time, constructed random value is used.
- The random value is valid for a maximum of 30 days after its creation.
- The recipient inserts the random value at the defined location.

3.2.2.5.2 E-mail, fax, text message or mailing address of the contact person

Sending a random value via e-mail, fax, text message or letter mail and subsequently receiving a confirmation response using the sent random value. The random value is sent to an e-mail address, fax/mobile phone number or mailing address which was identified as the domain contact.
The following applies:

- An e-mail, fax, text message or letter mail can confirm the authorization for multiple IP addresses.
- The created e-mail, fax, text message or letter mail can be sent to several recipients, provided that this recipient is listed for the IP address being validated at the registration office.
- The random value sent via e-mail, fax, text message or letter mail is a one-time consignment.
- An e-mail, fax, text message or letter mail consignment, including the reuse of the random value can be resent. The prerequisite for this is 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 after its creation.

3.2.2.5.3 Reverse lookup of the IP address

The control over the IP address is confirmed by first finding an assigned domain name through reverse lookup and then performing the verification using the allowed procedures in Chapter 3.2.2.4.

3.2.2.5.4 Other methods

No stipulation.

3.2.2.5.5 Telephone contact to the IP address contact

The IP address contact can confirm each IP address from the certificate request via telephone call with the CA..

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 in the left label of the CN or "subjectAltName." More than one wildcard character (e.g. *.*.example.com) per CN or "subjectAltName" is not acceptable.
If a wildcard character appears in a label immediately to the left of a "registry-controlled" or "public suffix", the issuance MUST be rejected (e.g., "*.co.uk" or "*.de"), unless the customer can prove that he has legal control over the entire domain namespace.

3.2.2.7 Reliability of the data source

Reliable data sources are only trustworthy internal data sources. Not allowed / not reliable are data sources which are self maintained or maintained at external connected organizations.

3.2.2.8 CAA records

See Section 3.2.5.2 and 4.2.2.4.2.1.2

3.2.3 Authentication of end entities

3.2.3.1 Identity check on an organization

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 an authorized signatory or authorized proxy 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 registers (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 comparable registers. 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 comparable directories. If required, a Dun & Bradstreet report can be used as a trustworthy, 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.

TeleSec ServerPass EV / EV SAN:
The required checks are carried out in accordance with [CAB-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 data. Next to the validation steps in Section 3.2.2 it will be checked (if possible) if the data are plausible, complete, fitting, and clear.

3.2.5 Validation of Authority

3.2.5.1 Ensuring the authenticity of the certification request

TeleSec ServerPass Standard and SAN/UCC:
Every ServerPass customer concludes 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.
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 a comparable register. 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 applicant.

TeleSec ServerPass EV/EV SAN:
The authorization is checked according to the EV Guidelines [ETSI EV].

3.2.5.2 Checking CAA entries in the DNS

During the authorization check all FQDN entries are validated against the CAA entries in the DNS (Certification Authority Authorization; CAA records for Fully Qualified Domain Names).
If one or more CAA resource records are found, of which no issue or issuewild property contains "telesec.de", then the certificate request is rejected. If the issuewild property contains a semicolon ";", a wildcard certificate request is always rejected.
If no CAA Resource Record has been stored or if its issue or issuewild property contains "telesec.de", the verification process is continued.
8 CNAME chain entries are processed and the length of the chain is limited to a maximum of 10 as recommended.

3.2.6 Criteria for Interoperation or Certification

If a sub-CA uses a policy OID that represents fulfillment of and compliance with the [CAB-BR] in a certificate that it has issued, the corresponding CP or CPS of the sub-CA must contain an explicit assurance that all certificates issued by the sub-CA that contain this policy OID correspond to and comply with the specifications issued by the [CAB-BR].

No other sub-CA certificates are issued under the sub-CA certificates for TeleSec ServerPass.

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

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.

TeleSec ServerPass EV / EV SAN:
Re-certification in the actual sense does not take place in the case of 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 398 days at the time the certificate is issued.

3.3.1 Identification and authentication for routine key renewal

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.

TeleSec ServerPass EV / EV SAN:
Routine key renewal does not take place.

3.3.2 Identity check in the event of key renewal following certificate revocation

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

3.4 Identification and authentication for revocation orders

Authorized end entities can revoke their certificates themselves via the service portal <myServerPass>.
After the certificate to be revoked has been selected, the revocation request can 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 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 by giving the CommonName or serial number of the certificate and describing the nature of the misuse to the service desk. These cases are passed on to the Trust Center or the registration authority. 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 contact purposes:
Internet: https://www.telesec.de/de/service/kontakt/zertifikatsmissbrauch-melden/ (Subject: Suspected abuse of certificate)
Telephone: +49 (0) 1805 -268204 (fixed networks: EUR 0.14/minute, mobile networks: max. EUR 0.42/minute)
E-mail: telesec_support@t-systems.com

4 Operational requirements in the life cycle of certificates

4.1 Certificate request

4.1.1 Who can order a certificate?

The role of technical contact in the ServerPass service portal is assigned to a corresponding natural person, who is authorized to issue certificate requests. This person is authorized by means of a test call made by the applicant representative, who has signed the contract with Deutsche Telekom Security GmbH.
There is a defined process in the service portal for transferring the role of technical contact to another natural person.
At the written request of the customer, the registration authority (RA) employees can name the individuals who currently fill the role of technical contact via the system and inform the customer of the names.

4.1.2 Ordering procedure and obligations

4.1.2.1 End entity

All end entities undertake to comply with these statements (CP/CPS, „Leistungen und Nutzungsbedingungen“ (“Services and Conditions of use”) and Privacy Policy).

The end entity also commits to the following:

- To ensure that the statements made in the certificate request are true and correct
- To generate key pair(s) or order their generation
- To transmit its public key with its certificate data to the certification authority for certificate generation
- To provide proof of ownership of the private key, which is connected to the certified public key

4.2 Processing of certificate requests

The following process description is binding for the TSP, even if he issues certificates in his own name.

4.2.1 Initial and one-time preparations

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

4.2.1.1 Subscriber and terms-of-use agreement

If the certificate holder and the issuing CA belong to a mutual legal person (affiliate), the applicant’s representative has to accept the applicant’s “General Terms of Use” before issuing a certificate. If the certificate holder is not a group company (commissioned third party or non affiliate), the applicant has to consent to the “General Terms and Conditions of use” for ServerPass in a legally enforceable manner.
Both the general terms of use and the general terms and conditions are managed in a corresponding electronic form in the ServerPass service portal.
Agreement of the subscriber agreement or consent to the terms of use is repeated for every request, renewal or re-issue.

4.2.1.2 Performing identification and authentication

To validate a request, the certification authority only uses documents, documentation or other information not older than 398 days at the time the certificate is issued.

Denied List
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 certification 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.

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.

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 certification requests

If all necessary checks based on Sections 3.2 and 3.3 have been successful, the certification request is approved and the certificate issued.

By allocating a reference number to the certificate commissioning, the unique mapping from an issued certificate to the corresponding order documents and additional documents (e.g. power of attorney) is established.

A certificate request must be rejected if:

- The request does not contain at least one fully qualified domain name or IP address, which is transferred to the SAN extension.
- The public key falls short of the minimum length of 2048 bits.
- If the result of checking the Debian weakness is positive.
- If a public key is to be used for a new request, which is already used for another ServerPass certificate.
- if an CAA resource record is found whose issue or issuewild property does not contain "telesec.de".
- if all required tests do not run successfully.

The Trust Center regularly checks (maximum every 30 days) on the ICANN website (https://newgtlds.icann.org) whether new gTLDs have been released or canceled. In the event of changes, a check is carried out to determine whether certificates have been issued for this gTLD and stops issuing new certificates until control over the domain name or the applicant's exclusive right to use the domain name has been demonstrated.

If proof is not provided or the gTLD is canceled, all certificates issued with this TLD in the domain name will be blocked within 120 days (see Section 4.9.1.1).
If a request is deferred or rejected, the technical representative of the certificate holder will be notified by e-mail 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 Actions during Certificate Issuance

Circumstances can lead to the issuance of a certificate being delayed.
Possible reasons for this are:

- Further information is needed in order to identify and authenticate the required end-entity information according to Section 3.2.
- There is a delay in providing additional documents that may be necessary and requested.
- The end entity does not reply to queries or when contacted.

The end entity shall be informed by e-mail if a certificate is delayed.

4.3.2 Notification of end entities about the issuing of certificates

The technical point of contact shall receive a notification about the issuance of the certificate in an e-mail containing all the relevant information. The certificate issued will be listed in the service portal <myServerPass> under 'My Certificates'.

4.4 Certificate acceptance

4.4.1 Acceptance by the certificate holder

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.

4.4.2 Publication of the certificate by the CA

The customer can decide in the course of the certificate request whether its certificate is to be published in several public Certificate Transparency (CT) log servers.
Important hint: If the certificate is not published the usage may be limited, e.g. applications may not accept or reject the certificate.

4.4.3 Notification of other authorities about certificate issuance by the CA

The notification of other authorities is not envisaged.

4.4.4 Certificate transparency

TeleSec ServerPass supports certificate transparency.
All issued EV certificates contain the Certificate Transparency extension by default. This is for the security and transparency of the certificate issuance. The CT extension can be deselected at the customer's request. You can find more details at https://www.certificate-transparency.org.

4.5 Use of key pair and certificate

4.5.1 Use of the private key and the certificate by the certificate owner

The certificate and the associated private key may only be used in accordance with the General Terms and Conditions (GT&Cs), the respective subscriber agreement or the terms of use and the present CP/CPS.
End entities must protect their private key against unauthorized access and may no longer use the private key once the validity period has expired or the certificate is revoked.

4.5.2 Use of public keys and certificates by relying parties

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

- Check that the information contained in the certificate is correct before using it
- 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
- Use the certificate for authorized and legal purposes only, in accordance with the present document on certification practice. The certification authority is not responsible for assessing the suitability of a certificate for a specific purpose
- Check the technical usage purpose, which is established via the attributes "key usage" and "extended key usage" shown in the certificate

Relying parties must use appropriate software and/or hardware to check certificates (validation) and the associated cryptographic procedures.

4.6 Renewal of certificates (re-certification)

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 himself whether a new public key of a newly generated key pair is to be used for the re-certification. A prerequisite for using the same 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.

TeleSec ServerPass EV / EV SAN:
Re-certification is not currently offered.

4.6.1 Conditions for re-certification

TeleSec ServerPass Standard and SAN/UCC:
Re-certification is possible at any time whilst the current certificate remains valid. Expired certificates cannot be renewed. A certificate that has been renewed cannot be renewed again. The certificate that is no longer required must be revoked immediately.

TeleSec ServerPass EV / EV SAN:
Re-certification is not currently offered. Instead, a new request can be initiated as conveniently as a re-certification, by using the service portal <myServerPass>.

4.6.2 Who may request re-certification?

TeleSec ServerPass Standard and SAN/UCC:
Re-certification is only ordered by registered and authorized persons. The authorized person has the required login details as well as the certificate service password.

TeleSec ServerPass EV / EV SAN:
Re-certification is not currently envisaged.

4.6.3 Processing renewals

TeleSec ServerPass Standard and SAN/UCC:
The request for re-certification is checked electronically and can be approved automatically following successful verification of all relevant data.

TeleSec ServerPass EV / EV SAN:
Re-certification is not currently envisaged.

4.6.4 Notification of the certificate holder about the issuance of a new certificate

TeleSec ServerPass Standard and SAN/UCC:
The regulations in Section 4.3.2 apply.

TeleSec ServerPass EV / EV SAN:
Re-certification is not currently envisaged.

4.6.5 Acceptance of re-certification

TeleSec ServerPass Standard and SAN/UCC:
The regulations in Section 4.4.1 apply.

TeleSec ServerPass EV / EV SAN:
Re-certification is not currently envisaged.

4.6.6 Publication of a re-certification by the CA

TeleSec ServerPass Standard and SAN/UCC:
The regulations in Section 4.4.2 apply.

TeleSec ServerPass EV / EV SAN:
Re-certification is not currently envisaged.

4.6.7 Notification of other authorities about a re-certification by the CA

TeleSec ServerPass Standard and SAN/UCC:
The regulations in Section 4.4.3 apply.

TeleSec ServerPass EV / EV SAN:
Re-certification is not currently envisaged.

4.7 Re-key of certificates

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).

TeleSec ServerPass EV / EV SAN:
A re-key is not currently offered.

4.7.1 Conditions for re-key

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.
TeleSec ServerPass EV / EV SAN:
A re-key is not currently offered.

4.7.2 Who may request the certification of a new public key?

TeleSec ServerPass Standard and SAN/UCC:
The statements in Section 4.6.2 apply accordingly.

TeleSec ServerPass EV / EV SAN:
A re-key is not currently offered.

4.7.3 Processing of re-key requests

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.

TeleSec ServerPass EV / EV SAN:

A re-key is not currently offered.

4.7.4 Notification of the certificate holder about certificate issuance

TeleSec ServerPass Standard and SAN/UCC:
The regulations in Section 4.3.2 apply.

TeleSec ServerPass EV /EV SAN:
A re-key is not currently offered.

4.7.5 Acceptance of a renewal with new key material

TeleSec ServerPass Standard and SAN/UCC:
The regulations in Section 4.4.1 apply.

TeleSec ServerPass EV / EV SAN:
A re-key is not currently offered.

4.7.6 Publication of a certificate with new key material by the certification authority

TeleSec ServerPass Standard and SAN/UCC:
The regulations in Section 4.4.2 apply.

TeleSec ServerPass EV / EV SAN:
A re-key is not currently offered.

4.7.7 Notification of other authorities regarding certificate generation by the certification authority

The regulations in Section 4.4.3 apply.

4.7.8 Re-issuing a certificate

TeleSec ServerPass Standard and SAN/UCC:
Under certain circumstances the opportunity to perform a certificate re-issue for the remaining period of the existing certificate will be offered in order to support end-to-end authentic and secure electronic communication. Such a situation occurs, for example, if the private key becomes unusable, has been deleted, or no longer corresponds to the public key as a result of a relocation or modernization of web server hardware or software owing to work errors. These individual cases generally also result in the certificate becoming unusable without it actually being compromised.

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, a new issue date but the expiry date as the preceding certificate. It is recommended to generate a new key pair and to 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 holder 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.

TeleSec ServerPass EV / EV SAN:
The re-issue is the same as for ServerPass Standard und SAN/UCC. Exception: always a new key pair must be used.

4.7.9 Conditions for re-issue

A certificate re-issue is possible at any time whilst the current certificate remains valid. 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 was revoked by the costumer. After 30 days, the system performs a forced revocation.

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.

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

The regulations in Section 4.3.2 apply.

4.7.13 Acceptance of the re-issue

TeleSec ServerPass Standard and SAN/UCC:
The regulations in Section 4.4.1 apply.

TeleSec ServerPass EV / EV SAN:
A re-issue is currently not 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 changes

No stipulation.

4.8.4 Notification of the certificate holder about the issuance of a certificate

No stipulation.

4.8.5 Acceptance of a certificate change

No stipulation.

4.8.6 Publication by the CA of a certificate with changed data

No stipulation.

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

No stipulation.

4.9 Certificate revocation and suspension

4.9.1 Reasons for revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

The following reasons require the revocation of the certificate by the certificate holder:

- 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, are incorrect, or are not compliant to the naming conventions (see Section 3.1). This also applies to domain names which are no longer owned by the domain owner or which have been withdrawn by authorized authorities (e.g. ICANN) (e.g. generic top-level domains (gTLDs)
- 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 certificate holder expressly requests the revocation of the certificate

The CA revokes a certificate within 24 hours if at least one of the following reasons exists:

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

The CA revokes a certificate within 5 days if one or more of the following occurs:

- The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;

- The CA has evidence that the certificate has been misused;
- The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
- The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- The CA is made aware of a material change in the information contained in the Certificate;
- The CA is made aware that the Certificate was not issued in accordance with the requirements of the CA-Browserforum or the CA's Certificate Policy or Certification Practice Statement;
- The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate or misleading;
- The certification authority ceases operations for any reason and has not made arrangements for another CA to provide revocation support.
- The CA's right to issue Certificates under the requirements of the CA-Browserforum expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the certificates;
- Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or
- The technical content or format of the certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time)
- The CA is made aware that there is a method by which the private key corresponding to a public key can be easily calculated. (similar to the Debian weak key, http://wiki.debian.org).
- There are legal regulations or adjudications or instructions of a supervisory authority.

TeleSec ServerPass EV / EV SAN:
In addition to these reasons, there are a number of specific reasons named in [CAB-BREV] which the certification authorityrecords 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 Conditions of use were disregarded.
- The certificate violates the provisions and conditions with regard to the issuing of EV certificates.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

- No stipulation.

4.9.2 Who can request that a certificate 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 in the service portal. The revocation function is available 24x7. The revocation is authorized by the service password and is definitive. The certificate holder is automatically informed by e-mail about the revocation status.

The Trust Center reserves the right to revoke certificates (24x7) if at least one of the reasons for revocation listed in Section 4.9.1 applies.

The certification authority 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.

Within 24 hours after receiving a certificate problem report, the Trust Center will investigate the facts and circumstances related to a certificate problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the certificate problem report.
After reviewing the facts and circumstances, the CA shall work with the certificate holder and any entity reporting the certificate problem report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate. The period from receipt of the certificate problem report or revocation-related notice to published revocation must not exceed the time frame set forth in section 4.9.1. The date selected by the CA considers the following criteria:

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

If there is a high prioritized certificate problem report, Trust Center is able to respond internally at any time and to decide whether it is necessary to involve a law enforcement agency or to revoke a certificate that is the subject of a report.

4.9.4 Deadlines for a revocation order

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 24x7 and is passed on to the linked systems immediately after the revocation process in the service portal <myServerPass>. The OCSP service that uses these systems therefore also has access to the current certificate status.
After the service desk receives a revocation request, the certification authority takes economically suitable steps to process the revocation request without delay.

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 certification authorityensures that the revoked certificate, even after it expires, is at the least included in the next CRL.

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 and published by the directory service.
The revoked CA certificates are listed in the revocation list for certification authorities (ARL). Updates of the ARL are carried out every 3 months or depending on events, and publication takes place via the corresponding directory service.
The revocation list (CRL) also contains certificates that are outside of the validity period.

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 (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 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 issued by end-user certificates comply with the requirements of RFC 6960.
The OCSP responder replies to requests for certificate serial numbers not issued by the TeleSec ServerPass service with "unknown". In addition, the OCSP responder is monitored for inquiries about "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 five (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 e-mail of the revocation of the certificate (revoke notification) containing the relevant certificate information.

4.9.12 Special requirements for compromised private keys

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

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.

4.9.15 Suspension procedure

No stipulation.

4.9.16 Limitation of the suspension period

No stipulation.

4.10 Status information services for certificates

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

4.10.1 Operational properties

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 can contain the following statuses:

- good, that means that
  - the issuer is a ServerPass issuer and
  - the certificate is valid and
  - the certificate is not revoked.

- revoked, that means that
  - the issuer is a ServerPass issuer and
  - the certificate is valid and
  - the certificate is revoked.

- Unknown, that means that
  - the certificate is invalid or
  - the certificate is valid but the certificate was not issued by an issuer of ServerPass or
  - the certificate is valid but does not correspond to the requested issuer.

The certification authority applies security mechanisms for the revocation status services (CRL, ARL, OCSP) to prevent non authorized access attempts, to hinder manipulations of the revocation status information (adding, deleting or changing).
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 ten seconds.

4.10.3 Additional features

No stipulation.

4.11 Cessation of certificate usage

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 storage and restoration

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 Physical, organizational and personnel-related security measures

The TeleSec ServerPass CAs are under the scope of the T-Systems International GmbH ISO/IEC 27001:2013-certification and maintain an extensive security program with all aspects that are demanded by CABF.
The physical, organizational and personnel-related security measures applied are defined in a security concept ,with their effectiveness being demonstrated on the basis of a threat analysis.
The security measures required for operational purposes are described in the Operating Guidelines for the Trust Center.
The requirements from [ETSI EN 319 401] chapters 5, 6.3 and 7.3 are implemented, i.e. specifications are outlined in relation to:

- Risk assessment in the framework of ISMS
- Information security guidelines
- Asset management
- Regular reviews

The management approves the risk assessment and accepts the identified remaining risk.

5.1 Physical security measures

The Trust Center is authorized as a certification authority under signature law and has been eIDAS-compliant since July 1, 2016 and thus fulfills very strict requirements concerning physical security. The measures are described in detail in the security concept.

5.1.1 Location and structural measures

The Trust Center operates its own services in data centers which are compliant to technical and physical requirements of the Deutsche Telekom group.
The Trust Center is installed in data centers which are located geo redundant inside of Germany with a minimal distance of at least 10 km.
The Trust Center is implemented in each of the data centers in a separated cage which is secured via a physical access control system.
The Trust Center or data center is set up and operated in line with the relevant guidelines of the Federal Office for Information Security (BSI), the German Association of Indemnity Insurers (Verband der Schadenversicherer e.V., VDS)/new: German Insurance Association (*Gesamtverband der Deutschen Versicherungswirtschaft – GDV*), the relevant DIN standards on fire protection, smoke protection, and blocking of attacks. The Trust Center is accepted by VdS/GDV in terms of security technology.
The technical measures are supplemented by organizational elements that include the handling of security-relevant techniques and regulations regarding access to security zones for employees and third parties (visitors, external staff and cleaning staff), delivery of materials (hardware, accessories, resources) and tidiness at the work station as well as in computer rooms.

5.1.2 Access

The Trust Center is subject to an access regulation that regulates access rights for employees, employees of third party companies and guests in the individual security zones. Access between the security areas is only possible via turnstiles. Controlled access to the various security areas is also protected by means of a computer-controlled access control system. Guests are only received in exceptional cases and subject to prior notification. Specific security rules apply here.

5.1.3 Power supply and air conditioning

The suction openings for outside air are arranged in such a manner that pollutants such as dust or dirt as well as corrosive, poisonous, or highly flammable gases cannot enter. The systems are operated using a very low proportion of outside air. The required fresh air openings are access-protected. Filters are installed to protect against air pollution resulting from floating particles. The fresh air intake is continuously checked for aggressive

gases. In the event of an emergency (e.g., fire in the surrounding area), the fresh air intake is automatically closed by means of air flaps.
To protect against power supply failure, an independent alternating current supply is installed in accordance with VDE regulations. It provides protection against variations in voltage, short-term bridging that is free of interruptions as well as long-term bridging with two separate stationary emergency generators with a performance corresponding to the full load of the data center.

5.1.4 Water risk

The Trust Center is situated in a protected area, i.e., it is not situated close to any body of water or in low-lying areas (danger of flooding). Any fire is extinguished using inert gas.

5.1.5 Fire safety

The applicable fire regulations (e.g., DIN 4102, requirements of the local fire department, regulations regarding fire resistance, VDE-compliant electrical installation) are complied with. All fire doors have automatic locking mechanisms. As agreed with the fire department, water will only be used to put out fires in extreme emergencies.
Fire sections are secured by fire-resistant components. Passages through fire protection walls are equipped with self-closing fire doors.
In areas with double floors as well as suspended ceilings the fire protection walls go right through to the ceilings/floors of the story.
Early fire detection systems (suction systems) are installed in all system rooms, system operator rooms, archive rooms, UPS rooms as well as in other selected rooms. The supply air and exhaust air of the air conditioning devices in the individual rooms are monitored. Fire alarms are installed in the other rooms.

5.1.6 Storage of data media

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

5.1.7 Disposal

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

5.1.8 External backup

The Trust Center carries out routine backups of critical system data, audit log data and other confidential information. The backup copies are kept in a different room from the original data.

5.2 Organizational security measures

The organizational measures are set out in the security concept [SRK TC] and in the ServerPass security concept and are implemented on the basis of the Trust Center's operations plan. The relevant requirements from [ETSI EN 319 401] chapter 7.4 b, c, d, e are implemented.

5.2.1 Trustworthy roles

Trustworthy persons are all persons (Telekom Security employees, contractors and consultants) with access to or control over authentication or cryptographic processes, which can have a considerable impact on the following:

- the validation of information in certificate requests
- the acceptance, rejection or other processing of certificate requests, revocation requests or renewal requests

- The issue or withdrawal of certificates, including staff who have access to the database systems
- the handling of information or requests from end entities.

Trustworthy persons are in particular:

- Trust Center staff (e.g., system administration, internal registry authority employees)
- staff of cryptographic departments
- security staff
- responsible technical personnel and
- managerial staff responsible for managing the trustworthy infrastructure.

The above-named trustworthy persons must fulfill the requirements set out in this CP/CPS (see Section 5.3.1). The above Trustworthy people must be assigned the relevant role(s). Via written confirmation (e.g. via e-mail), these people accept their assigned role(s).

These trustworthy persons must be freed of conflicts of interest to ensure that the roles they hold can be exercised impartially and without prejudice. The employees explicitly accept the role of trustworthy person and undertake to acknowledge and adhere to the Group's "Code of Conduct".

The Change Advisory Board of the Trust Center is responsible for initiating, performing, and controlling the methods, processes, and procedures that are illustrated in the security plans, in the CP/CPS of the certification authorities operated by the Trust Center.

5.2.2 Number of persons required for a task

The operational maintenance of the certification authority and the directory service (administration, backup, restoration) is carried out by knowledgeable and trustworthy staff.
Work on highly sensitive components (e.g., key generation system, HSM) is governed by special internal control procedures and carried out by at least two members of staff.

TeleSec ServerPass EV / EV SAN:
The dual control principle stipulated in the EV guidelines [CAB-BREV] for the release and approval process of an EV / EV SAN certificate is implemented by the certification authority according to the requirements. Technical means are in place to prevent circumvention of the dual control principle.

5.2.3 Identification and authentication for every role

Telekom Security employees who are classed as especially trustworthy and who carry out especially trustworthy activities are subject to a Trust Center internal security check (see Section 5.3.2).
The Trust Center ensures that employees have achieved a trustworthy status and the department has given its approval before these employees:

- Receive access devices and can access the necessary facilities
- receive electronic authorization to access the TeleSec ServerPass CA and other IT systems
- Are permitted to carry out certain tasks in connection with these systems

The Trust Center employees are formally appointed by the head of the Trust Center following a positive check.

5.2.4 Roles that require a separation of functions

The following roles require a separation of functions and are therefore supported by different employees:

- request validation and request release (only ServerPass EV / EV SAN)
- backing up and restoring databases and HSMs
- key lifecycle management of CA and root CA certificates.

5.3 Personnel-related security measures

Telekom Security 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 trustworthy role are required by the certification authority to prove that they have the qualifications and experience necessary to fulfill their prospective work obligations in a competent and satisfactory manner.
A new certificate of good conduct must be submitted to the staff supervisor at regular intervals.

5.3.2 Security check

Before starting work in a trustworthy role, the Trust Center runs a security check which includes the following:

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

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 trustworthy person being rejected can include

- False statements by the candidate or the trustworthy person
- Particularly negative or unreliable employment references, and
- Certain previous convictions.

Reports containing such information are evaluated by employees of the HR department and security personnel, who determine the appropriate course of action. The measures involved in the course of action can even lead to candidates for trustworthy positions having their employment offer withdrawn or to trustworthy 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 towards the individual work areas and include, for example:

- Advanced PKI knowledge
- Procedures according to ITIL
- Data protection
- Data and telecommunications privacy
- Information protection
- Access protection
- Anti-corruption
- Security and operational guidelines and procedures of Deutsche Telekom group
- Use and operation of the hardware and software in use
- Reporting and handling of faults and compromises, as well as
- 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

The staff of the Trust Center will receive refresher and advanced training courses to the extent required and at the latest after 12 months.

5.3.5 Frequency and sequence of workplace rotation

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 CP/CPS and the procedures described therein, and to initiate corresponding 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 trustworthy positions. These persons are subject to the same functional and security criteria as employees of the Trust Center in comparable positions.
The above persons, who have not yet concluded or successfully completed the security check described in Section 5.3.2, are given access to the secure facilities at the Trust Center only under the condition that they are accompanied and directly supervised by trustworthy persons.

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 aids and documents they need for this (training documents, procedural instructions).

5.4 Log events

The logging concept and the installation handbook of the service define which data and events have to be logged in which time interval. In addition it is regulated how long the log / protocol data has to be stored (currently 6 weeks) and they have to be secured from theft, loss or unauthorized access.
Requirements of [ETSI EN TSP] Section 7.10 are implemented in this context.

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, saving, back-up 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 and also 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 orders
f) Issuing 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 the PKI 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) When people access and leave Trust Center facilities
g) Results of network checks (vulnerability scans)
h) Start and end of the logging process

5.4.2 Processing interval of the 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 Storage period for audit logs

Audit logs/history data/logging files are archived after processing according to 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 Assessment of vulnerabilities

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 processed via the defined ISMS process. Critical vulnerabilities which have been communicated to the TSP, have to be evaluated by the ISMS team in the timeframe of 48h hours including the

suggestion of a solution scenario. If an immediate and complete clearance is not possible, a plan with measures will be created. The measures should aim to reduce the criticality of the vulnerabilities.

5.5 Data archiving

5.5.1 Type of archived datasets

The certification authority archives the following data:

- hard copy of request documents
- all audit/event logging files recorded pursuant to Section 5.4

5.5.2 Storage period for archived data

The following records and storage periods are stipulated:

- Order documents, in particular information regarding certificate requests, their validation and the certificates resulting from this and revocations executed are retained for 10 years after the certificate validity expires,
- for ServerPass EV until the end of operations, but at least 10 years after the certificate validity,
-
- 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 trustworthy persons are given access to data 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 timestamps of datasets

Data records such as certificates, certificate revocation lists, OSCP responses, logging files contain information about the date and time. An NTP appliance (with GPS and DCF77 antenna) serves as the time source, from which the UTC time is derived. The individual systems compare the system time with the time source several times a day.

5.5.6 Archive recording system (internal or external)

The Trust Center only uses internal archiving systems.

5.5.7 Procedures for obtaining and checking archive information

Only authorized and trustworthy personnel receive 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 Compromising and restoring private keys and disaster recovery

5.7.1 Handling of incidents and compromised situations

The Trust Center has implemented an IT-service management according to ITIL as well as ISMS processes. Incidents and compromised situations are processed based on these standard processes.

The service operates a framework SLA, which describes the fundamental incident process.
Incidents are submitted via the contacts defined in Section 1.5.2 and processed in the context of service management.

The specification of all necessary contacts, departments, IT-service management-systems, on-call duty and MoD (Manager on duty) shall ensure that the work on incidents and security threats can start short-term. These precautions shall keep the possible damage or the effects of a security threat to a minimum and eliminate it quickly.

The Service Desk is informed of the processing status by the functional department.

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 (to the information security officer). The event initiates a corresponding escalation, incident investigation, incident response and finally incident resolution. Disaster recovery is performed in accordance with the incident classification. Any hardware and software that is needed to provide the TeleSec ServerPass service is managed as an asset and application in Telekom Security configuration management.

5.7.3 Procedure in the event of private keys of certification authorities being compromised

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) 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 catastrophes or catastrophes of human origin) and to restore the availability of critical business processes as quickly as possible. This also includes all Trust Center processes, components, systems and services. This plan is checked, tested and updated accordingly at least once a year to enable a targeted and structured response in the event of a catastrophe.

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 catastrophe (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 Cessation of operations

Only Telekom Security may initiate a cessation of operations
A cessation plan has been drawn up by the certification authority to deal with the situation of the certification service ceasing operation. Notifications will be given to the relevant parties in a business friendly way.
If there is a cessation of operations the certification authority follows the guidelines of the [ETSI EN TSP] Section 7.12 and has developed a cessation plan which 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 issued CA certificates
- 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 concerned and to ensure that all those involved 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 and revocation lists as well as paper documents are archived so that they can be accessed as evidence in court cases should this be necessary.

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 guidelines of [ETSI EN TSP] Section 7.5 are being implemented.

6.1 Generation and installation of key pairs

6.1.1 Generation of key pairs

All key pairs for CA certificates are generated and stored by trained and trustworthy specialist staff in a low-radiation room on a security-checked hardware security module (FIPS 140-2/level 3 evaluated) in the so-called "key ceremony".
All activities during the key ceremony are logged and signed by all persons involved. These records are stored for auditing and tracking purposes for a period deemed suitable by the Trust Center.
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.

The key pair for a public certification authority (public root) and the corresponding sub-CA certificate are generated on the offline CA and the assigned cryptographic hardware module (HSM) under the supervision of an independent and qualified auditor.
The key pair for a subordinate certification authority (sub-CA) is generated on the cryptographic hardware module (HSM) assigned to the TeleSec ServerPass in online operation. The corresponding CA certificate is generated on the offline CA.
All keys generated and certificates issued by the offline CA are logged by means of a verification log and video recording and documented in an audit-proof manner.

The offline CA systems consisting of a certification instance, cryptographic hardware module (HSM) (incl. backup token) and browser – are operated “offline”, i.e., without a connection to any network structure.
The offline CA systems are stored in a separate rack cabinet under separate lock

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.

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.
The Trust Center accepts an RSA key length of at least 2048 bits for end-entity certificates. The request system automatically rejects key lengths that are shorter than 2048 bits during the first request step. Key lengths of at least 256 bits are accepted for ECC.
The Baseline Requirements are fulfilled for Root CA, Sub-CA and end-user certificates

6.1.6 Generating the parameters of public keys and quality control

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

- The public key is not a Debian weak key,
- the exponent of the public key corresponds to the current Baseline Requirements [CAB-BR],
- zLint and crt.sh tests were successfully carried out,
- the public key is unique for the certification authority,
- the cryptographic procedure RSA or ECC (prime256v1 [Windows display ECDH_P256], secp384r1 [Windows display ECDH_P384],) was used for generation,
- the minimum key length for RSA keys is 2048 bits and
- SHA-256 is permitted as a signature hash algorithm. (SHA-1 is currently still being approved. However, a warning is displayed that switching to SHA-256 is recommended.)

If one of the parameter checks fails, the corresponding certificate request is stopped with a message "rejected". A new certificate request with correct parameters must be used.

6.1.7 Key usage (according to the X.509v3 “Key usage” extension)

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 the cryptographic devices during their operation, transport and storage T-Systems adheres to the manufacturer specific mechanisms which have been validated during the FIPS- and CC-certification checks. The devices are stored separately to the PED-keys (which are needed for operation) to prevent the compromise of one locality and in consequence the compromise and misuse of the devices.
Before startup or shutdown a component performance and integrity checks are performed.

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

The Trust Center has implemented technical, organizational, and procedural mechanisms that require the participation of several trustworthy 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 with trustees will not be stored with any 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 and 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 Transfer of private keys in or by a cryptographic module

The Trust Center generates Sub CA certificates on the cryptographic hardware security modules (HSM) of the offline CA. 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 an online cryptographic hardware security module (HSM). The public key to be certified with the Subject DN data is securely transmitted in electronic form (PKCS#10-Request) to the offline CA which generates the sub CA certificate. Afterwards, the sub CA certificate is securely transferred to the HSM of the online CA and assigned to the private key. The transfer of the key material and the associated sub CA certificate between the hardware security module (HSM) in online operation is performed in encrypted mode.

6.2.7 Storage of private keys on cryptographic modules

The Trust Center saves CA keys in a secure form 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 CP/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 (according to 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 trustworthy 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 **Table 2**.
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.

Type of certificate:	Period of validity:
TeleSec ServerPass Standard and SAN/UCC	
Baltimore CyberTrust Root	25 years
Deutsche Telekom Root CA 2 (expired)	20 years
TeleSec GlobalRoot Class 1 G2	25 years
TeleSec GlobalRoot Class 1 G3	25 years
TeleSec GlobalRoot Class 2 G2	25 years
TeleSec GlobalRoot Class 2 G3	25 years
TeleSec ServerPass CA 1 G2 (revoked)	10 years
TeleSec ServerPass CA 1 G3	10 years
TeleSec ServerPass CA 2	7 years
TeleSec ServerPass CA 2 G2 (revoked)	10 years
TeleSec ServerPass CA 2 G3	10 years
TeleSec ServerPass DE-2 (expired)	5 years 5 months
T-TeleSec GlobalRoot Class 2	25 Jahre
End-entity certificates	1 or 2 years. The period of grace is 5 days.
TeleSec ServerPass EV / EV SAN	
TeleSec GlobalRoot Class 3 G2	25 years
TeleSec GlobalRoot Class 3 G3	25 years
TeleSec ServerPass CA 3 G2 (gesperrt)	10 years
TeleSec ServerPass CA 3 G3	10 years
TeleSec ServerPass Extended Validation Class 3 CA	10 years
T-TeleSec GlobalRoot Class 3	25 years
End-entity certificates	1 or 2 years. The period of grace is 5 days.
Other certificates	
OCSP-Signer <Root-CA>	3 months
OCSP-Signer <Sub-CA>	1 month

Table 2: Validity of certificates

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 checks

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

The systems are monitored continuously regarding their functions and capacity. This way (if necessary) an extension of the resources is possible in a short time. The security measures of computer of the certification authority (e.g. network security, access control, monitoring) are documented in the security concept. The guidelines of [ETSI EN 319 401] Section 7.4 are being implemented in this context.

The systems for development, test unit (TU) and production unit (PU) are totally separated from each other and they are located at different hardware devices in different network segments. This way interdependencies are not possible.

6.5.1 Specific technical requirements for computer security

The Trust Center ensures that the management of CA systems is protected against unauthorized third-party access. The CA components must be physically and logically separated from other systems and only authorized personnel should be able to access them. Up-to-date protection mechanisms (e.g., firewalls, access protection, dual control principle) are used to protect the CA functions, directory services and OCSP responder against internal and external intruders. The CA uses intrusion detection systems (IDS) and intrusion prevention systems (IPS) implemented at network level that detect unusual or unauthorized access attempts and send an alert. Direct access to CA databases that support the CA functions is restricted to appropriate, trained and trustworthy operating personnel.

6.5.1.1 Security of systems

The security measures include:

- Physical security and securing of the environment
- The CA systems are configured such that any ports, accounts, applications, services and unsecure communication protocols not required are either deactivated or removed
- Measures to protect the system integrity, including at least configuration management, protection of security applications, and malware detection and prevention
- Network security and firewall management, including port blocking and IP address filtering as well as an intrusion detection system (IDS) and intrusion prevention system (IPS).
- User management, authorization matrix, clarification, raising awareness, and training/education as well as
- Procedure checks, activity logging, and switch-off in the event of timeouts

Workstations on which the issuing of certificates is authorized are secured through multi-factor authentication.

The TSP runs a penetration test (PEN-test) on the TSP systems (which he values as important)

- after the first configuration
- after extensive upgrades or changes to the infrastructure or the applications
- at least once a year

The TSP documents that each PEN-test has been executed by a person or organization that has the abilities, tools, knowledge, ethical principles and independency to create a reliable report.

6.5.2 Assessment of computer security

After every significant system or network change, an automated vulnerability scan takes place within a week, but at least once per calendar quarter. Possible weak points are analyzed, evaluated and registered. Based on the evaluation, measures are defined and implemented in a defined plan. The vulnerability checks, their results and actions (fixes, replacements) are documented.
Critical weaknesses are processed in the ISMS. Critical weaknesses are evaluated within 48 hours by the ISMS team and a solution scenario is shown. If immediate and complete elimination of the vulnerability is not possible, a treatment plan will be drawn up that will address the critical vulnerability mitigation.
In addition, penetration tests are carried out once a year. Here too, appropriate measures are derived and implemented, if this is necessary. The penetration tests and vulnerability scans are carried out by trained personnel. The tools used correspond to the current state of the art.

6.6 Technical checks on the lifecycle

6.6.1 System development checks

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

The system administrators manage the PKI systems (CA, HSM, web server) via a separated network which is only offered to this role. A management of other IT-systems (non PKI) via this network is not allowed.

Telekom Security's established change management is used.

6.6.2 Security management checks

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

The system accounts of the Trust Center administrators are checked after 90 calendar days at the latest.
Accounts that are no longer needed are deactivated.

6.6.3 Security checks on the lifecycle

The Trust Center has implemented mechanisms and control processes so that security patches are installed in a reasonable time after they have been provided. The integrity check of the security patches is executed manually before the installation starts.

A security patch will not be installed if additional security gaps or instabilities are generated and the advantages of the patch are nullified or outweighed. The reasons for the non-applicability of the security patches will be documented.

6.7 Network security checks

The following network security measures have been implemented for the TeleSec ServerPass service.

- The networks of the certification service are secured by multi-layered firewalls and located in different security zones.
- Security-critical components and systems that are accessible from the Internet (e.g., directory service, OCSP responder) are separated from the Internet and the internal networks by firewalls. All other security-critical components and systems (e.g., CA, DB, Signer) are located on separate networks.
- The internal networks of the certification service are divided according to the protection requirements of the systems and components and are separated from each other by firewalls.

- Vulnerability scans are performed at regular intervals. Further details can be found in Section 5.4.8.
- All eligible users have to authenticate at the systems via defined mechanisms. No longer necessary accounts need to be deleted or deactivated.

For the network security checks guidelines and requirements of the [ETSI EN 319 401] section 7.4 are implemented.

6.8 Time stamp

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 list, revocation list and OCSP profiles

7.1 Certificate profile

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

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

X.509v3 certificates must include at least the contents listed in **Table 3**.

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
Issuer:	See Section 7.1.4
Valid from:	Time basis Coordinated Universal Time (UTC). Coded according to RFC 5280.
Valid until:	Time basis Coordinated Universal Time (UTC). Coded according to RFC 5280.
Subject:	Distinguished name (see Section 7.1.4)
Public key:	Coded according to 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
	Section 7.1.2.10

Table 3: Certificate attributes according to X.509.v3

The certificate serial numbers are assigned by ServerPass in non-sequential numbering and contain an 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 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 [CAB-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 = OID,
(EV policy OID).
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:policyQualifiers:policyQualifierId = id-qt 1.
certificatePolicies:policyQualifiers:qualifier = URI to this document (CP/CPS).
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)

The criticality of this extension is set to “not critical”.

7.1.2.2 “Revocation list distribution point” extension (cRLDistributionPoint)

All end-entity certificates have a revocation list distribution point (cRLDistributionPoint) to the current certificate revocation list (CRL). Relying parties need this URI 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 4**.

		TeleSec ServerPass Standard und SAN/UCC		
		EE certificates	Sub-CA certificates	Root-CA certificates
	Risk value (criticality)	Critical	Critical	Critical
Bit	Name			
0	digitalSignature	✓	×	×
1	nonRepudation	×	×	×
2	keyEncipherment	(✓) only RSA keys	×	×
3	dataEncipherment	×	×	×
4	keyAgreement	(✓) only ECC keys	×	×
5	keyCertSign	×	✓	✓
6	CRLSign	×	✓	✓
7	encipherOnly	×	×	×
8	decipherOnly	×	×	×

Table 4: Assignment of the "Key usage" extension

		TeleSec ServerPass EV / EV SAN		
		EE certificates	Sub-CA certificates	Root-CA certificates
	Risk value (criticality)	Critical	Critical	Critical
Bit	Name			
0	digitalSignature	✓	×	×
1	nonRepudation	×	×	×
2	keyEncipherment	(✓) only RSA keys	×	×
3	dataEncipherment	×	×	×
4	keyAgreement	(✓) only ECC keys	×	×
5	keyCertSign	×	✓	✓
6	CRLSign	×	✓	✓
7	encipherOnly	×	×	×
8	decipherOnly	×	×	×

Table 5: Assignment of the "Key usage" extension

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 1 (subjectAltName). The criticality of this extension is set to "not critical".

7.1.2.7 "Authority Key Identifier" (AKI) extension

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 service OCSP, as well as the HTTP address of the OCSP responder.

End-entity certificate issued by:

- TeleSec ServerPass CA 2: http://ocsp.serverpass.telesec.de/ocspr
- TeleSec ServerPass DE-2 : http://ocsp.serverpass.telesec.de/ocspr
- TeleSec ServerPass Class 2 CA : http://ocsp.serverpass.telesec.de/ocspr
- TeleSec ServerPass Extended Validation Class 3 CA : http://ocsp.serverpass.telesec.de/ocspr
- TeleSec ServerPass CA 1 G2: http://ocsp.serverpass.telesec.de/ocspr
- TeleSec ServerPass CA 2 G2: http://ocsp.serverpass.telesec.de/ocspr
- TeleSec ServerPass CA 3 G2: http://ocsp.serverpass.telesec.de/ocspr
- TeleSec ServerPass CA 1 G3: http://ocsp.serverpass.telesec.de/ocspr
- TeleSec ServerPass CA 2 G3: http://ocsp.serverpass.telesec.de/ocspr
- TeleSec ServerPass CA 3 G3: 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 CA 2: http://ocsp.omniroot.com/baltimoreroot
- TeleSec ServerPass DE-2 : http://ocsp02.telesec.de/ocspr
- TeleSec ServerPass Class 2 CA : http://ocsp.telesec.de/ocspr
- TeleSec ServerPass Extended Validation Class 3 CA: http://ocsp.telesec.de/ocspr
- TeleSec ServerPass CA 1 G2: http://grcl1g2.ocsp.telesec.de/ocspr
- TeleSec ServerPass CA 2 G2: http://grcl2g2.ocsp.telesec.de/ocspr
- TeleSec ServerPass CA 3 G2: http://grcl3g2.ocsp.telesec.de/ocspr

The criticality of this extension is set to “not critical”.

7.1.2.10 “qcStatements” extension

The “qcStatements” extension consists of the object identifiers (OID) in accordance with:

0.4.0.1862.1.1 = 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 Object IDs (OIDs) of algorithms

The following signature hash algorithms are available for signing the end-entity certificate:

From 1/1/2016
sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11} → 1.2.840.113549.1.1.11

ecdsa-with-SHA256 {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)} -> 1.2.840.10045.4.3.2

7.1.4 Name forms

7.1.4.1 Information about the issuer

CA certificates used by TeleSec ServerPass contain a unique issuer name (issuer DN) in accordance with the specifications in Chapter 3.1.1

The issued end user certificates contain an unique issuer name (issuer DN) from the respective certification authority.

7.1.4.2 Subject information of the end user certificates

The contents of the subject DN (applicant) from the end user certificates can be composed of the fields as described in Chapter 3.1.1. The fields contain mandatory and optional input.

7.1.4.1.1 Subject Alternative Name Extension

See Section 3.1.1.1 and 3.1.1.2.

7.1.4.1.2 Subject Distinguished Name Fields

See Section 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 (applicant) from the CA certificates can be composed of the fields as described in Chapter 3.1.1. The fields contain mandatory and if applicable, optionally generated input.

Mandatory input consist of the following fields:

- 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 doesn't operate Sub-CAs with technical constraints.

7.1.6 Object IDs (OIDs) for certificate policies

7.1.6.1 Reserved Certificate Policy Identifiers

See Section 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 CA 2

The service "ServerPass" uses the policy OIDs 1.3.6.1.4.16334.1.0 and 1.3.6.1.4.1.7879.13.2 in the sub-CA certificate "TeleSec ServerPass CA 2", which has been issued under a public root.

TeleSec ServerPass Class 2 CA

The service "ServerPass" uses the policy OIDs "anyPolicy" identifier (2.5.29.32.0) in the sub-CA certificate "TeleSec ServerPass Class 2 CA", which has been ssued under a public root.

TeleSec ServerPass Extended Validation Class 3 CA
The service “ServerPass” uses the policy OIDs “anyPolicy” identifier (2.5.29.32.0) in the sub-CA certificate “TeleSec ServerPass Extended Validation Class 3 CA”, which has been issued under a public root.

TeleSec ServerPass DE-2 (valid until July 09, 2019)
The service “ServerPass” uses the policy OIDs 2.23.140.1.2.2 and 1.3.6.1.4.1.7879.13.2. in the sub-CA certificate “TeleSec ServerPass DE-2”, which was issued under a public root.

TeleSec ServerPass CA 1 G2 (revoked on Mai 14, 2019)
The service „ServerPass“ uses the policy OIDs 2.23.140.1.2.1 and 1.3.6.1.4.1.7879.13.2. in the sub-CA certificate „TeleSec ServerPass CA 1 G2“, which has been issued under a public root.

TeleSec ServerPass CA 2 G2 (revoked on Mai 14, 2019)
The service „ServerPass“ uses the policy OIDs 2.23.140.1.2.2 and 1.3.6.1.4.1.7879.13.2 in the sub-CA certificate „TeleSec ServerPass CA 2 G2“, which has been issued under a public root.

TeleSec ServerPass CA 3 G2 (revoked on Mai 14, 2019)
The service „ServerPass“ uses the policy OIDs 2.23.140.1.1 and 1.3.6.1.4.1.7879.13.24.1 in the sub-CA certificate „ TeleSec ServerPass CA 3 G2“, which has been issued under a public root.

TeleSec ServerPass CA 1 G3
The service „ServerPass“ uses the policy OIDs 2.23.140.1.2.1 and 1.3.6.1.4.1.7879.13.2. in the sub-CA certificate „TeleSec ServerPass CA 1 G3“, which has been issued under a public root.

TeleSec ServerPass CA 2 G3
The service „ServerPass“ uses the policy OIDs 2.23.140.1.2.2 and 1.3.6.1.4.1.7879.13.2 in the sub-CA certificate „TeleSec ServerPass CA 2 G3“, which has been issued under a public root.

TeleSec ServerPass CA 3 G3
The service „ServerPass“ uses the policy OIDs 2.23.140.1.1 and 1.3.6.1.4.1.7879.13.24.1 in the sub-CA certificate „ TeleSec ServerPass CA 3 G3“, which has been issued under a public root.

7.1.6.4 End-entity certificates

A certificate issued for an end user 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 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.

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, the following fields of the subjectDN must be filled: commonName
The fields organizationName, localityName, stateOrProvinceName and countryName are not being used.

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 fulfills the requirements of [CAB-BR] during its lifetime.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

The end user certificates contain a URL to the storage location of the CP/CPS.
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 serial number (SN) added as differentiation 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 5**.

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 according to RFC 5280.
Next update:	Date and time of the next planned publication.
Signature algorithm:	RSA – SHA-256
Revoked certificates:	List of revoked certificates including serial number with revocation date and time of the revoked certificate.
Extensions	
Authority key identifier:	Section 7.2.2.1 applies accordingly
Revocation list number:	Serial number of the certificate revocation list (Section 7.2.2.2).
Reason for revocation:	(optional) coding of the reason for revocation according to RFC 5280; see Section 7.2.2.3

Table 5: Revocation list attributes according to X509.v2

7.2.1 Version number(s)

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

7.2.2 Revocation list and revocation list entry extensions

7.2.2.1 “Authority Key Identifier” (authorityKeyIdentifier) extension

The revocation lists are given the extension “authority key identifier” 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

The revocation lists are given 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. According to **Table 6**, the following reason codes are implemented:

Input value on website:	Reasons for revocation in accordance with RFC 5280:	Value of the reason for revocation in accordance with RFC 5280:
Not specified	Unspecified	0
Key compromised	keyCompromise	1
Information in the certificate is out of date	AffiliationChanged	3

Table 6: “Reason code” extension

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 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 319411-1, 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 regularly subject to an annual check (ETSI TS EN 319411-1, policy EVCP, ETSI TS EN 319411-2 QCP–w) by an independent third party.
In addition, the Trust Center carries out internal audits at regular intervals (see also Section 8.1).

Subject of certification are all processes used for the request, issuance, re-issuance, revocation or renewal of end-user certificates.

8.1 Interval and reason for audits

Compliance audits usually take place annually or as required (Section 8) and are carried out at the expense of the authority being audited. Notice of the start of a compliance audit must be given in writing at least one week in advance. Audits are performed 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/qualification of the auditor

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

Special requirements apply for 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 suitably qualified Telekom Security staff.

8.4 Audit areas covered

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

- identity checks on end entities
- certificate request procedures
- processing of certificate requests
- certificate renewal/re-certification (only TeleSec ServerPass standard, SAN/UCC),
- certificate revocations
- access protection
- authorization and role concept
- anti-burglary measures

- staff

In each case, the audit is performed in line with the currently valid version of the following audit criteria:
ETSI TS EN 319411-1policy OVCP

TeleSec ServerPass EV / EV SAN:
The audits also cover the points named in ETSI TS EN 319411-1 policy EVCP that require particular attention for the issuance of extended validation certificates.
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 particular need for protection 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., guidelines, procedures, security systems used, technologies, insurance policies) 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. The security plan is made up of processes, measures, and products to support assessment and management during the risk assessment of identified risks. 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 director 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 the 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 image of Telekom Security was harmed.

Audit reports that are saved at the request of by one or more application software providers and embed a Trust Center root certification certificate must be published at the latest three months after the audit period in question ends.
The required audits are saved for ServerPass. The corresponding reports are published on the website https://www.telesec.de/en/trust-center-en.

8.7 Self-audits

Self-audits are performed as described in Chapter 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 "Service Specifications and Charges" for TeleSec ServerPass.

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

9.1.5 Reimbursement of charges

Telekom Security reimburses charges in accordance with the legal regulations under German law. Detailed provisions can be found in the document “General Terms and Conditions for TeleSec Products”.

9.2 Financial responsibilities

Financial responsibilities are determined in the “General Terms and Conditions for TeleSec Products”.

9.2.1 Insurance coverage

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

9.2.2 Other financial means

No stipulation.

9.2.3 Insurance cover or guarantees 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 Section 1.3.2 and 1.3.3) of the ServerPass CA, 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 ServerPass CA, which 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 PKI service provider, is responsible for the protection of confidential information and compliance with data protection provisions.

The registration authority of third parties must abide by the applicable statutory provisions and other regulations concerning data protection.

9.4 Protection of personal data (data protection)

Data protection and data security are part of the general business terms of the TeleSec products and services.

9.4.1 Data protection concept

Within the ServerPass CA, the registration authorities must store and process personal data electronically in order to provide their services.
A data protection concept is prepared for the ServerPass CA in line with the Group provisions. This data protection concept summarizes the aspects of the PKI service that are relevant to data protection.
Excerpts from the data protection 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 to be treated as non-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 according to Section 9.4.3.

9.4.6 Disclosure according to 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 shall inform the other contracting party about this, taking into account the legal provisions.

9.4.7 Other circumstances for disclosure of data

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 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 or 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 its contents and the origin of this certificate hierarchy are stated in full and not changed.

9.5.2 Property rights of this CP/CPS

This document is copyright protected; all intellectual property rights belong to Telekom Security. 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 Telekom Security, regardless of the medium on which they are stored. Copies of CA certificates may be duplicated in order to integrate them in trustworthy hardware and software components.

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

9.6 Assurances and guarantees

9.6.1 Assurances and guarantees of the certification authority

The certification authority takes responsibility for all aspects of the provision of the certification service, as well as for the activities that are outsourced to subcontractors. The certification authority has clearly defined the responsibilities and has taken suitable measures to allow the certification authority to carry out checks on third parties. The CA reserves the right to disclose relevant practices to parties.

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

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

The corresponding regulations “delegation of activities” of the [CAB-BR] also apply.

The Trust Center commits to the following:

- That certificates do not include any false statements that are known to or originate from the registration authorities that approve the certificate request 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.
- That all certificates comply with the requirements of this document.
- That the revocation functions and the use of the CA database (directory service, OCSP responder) fulfill all the essential requirements of the applicable CP/CPS.

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

1) A defined procedure is in place to ensure that the requester has the right to use the domains and/or IP addresses named in the certificate. Alternatively, that he has a relevant power of attorney that was issued by a person or an organization that has the right to this use.
2) The procedure described under 1) is followed and
3) The procedure described under 1) is specified in detail in this CP/CPS.

4) A defined procedure is followed to ensure that the certificate holder (subject) named in the certificate has approved the issuing of the certificate as well as that the applicant representative is authorized to make the request.
5) The procedure described under 4) is followed and
6) The procedure described under 4) is specified in detail in this CP/CPS.

7) A defined procedure is followed to check that, 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 and
9) The procedure described under 7) is specified in detail in this CP/CPS.

10) A defined procedure is followed to minimize the probability that the OU field of the Subject DN contains misleading information.
11) The procedure described under 10) is followed and
12) The procedure described under 10) is specified in detail in this CP/CPS.

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

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

The Trust Center additionally guarantees that:

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

9.6.2 Assurances and guarantees of the registration authority (RA)

All registration authorities commit to the following:

- Not to include any essentially false statements in certificates that are known to or originate from the registration authorities that approve the certificate request 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 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 the present CP/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: Telekom Security reserves the right to agree other obligations, assurances, consents, and guarantees towards the end entity.

9.6.4 Assurances and guarantees of relying parties

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

9.6.5 Assurances and guarantees of other entities

No stipulation.

9.7 Exclusion of liability

The exclusion of liability is regulated in the applicable General Terms and Conditions (GT&C).

9.8 Limitation of liability

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

9.9 Compensation for damages

Compensation is regulated in the applicable General Terms and Conditions (GT&C).

9.10 Term and termination

9.10.1 Term

The CP/CPS comes into effect when it is published on the Trust Center websites.
Changes likewise come into effect when they are published on the public websites (see Section 2.3).

9.10.2 Termination

This CP/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 CP/CPS until the last certificate issued expires or is revoked.

9.11 Individual messages and communication with subscribers

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

9.12 Changes to the CP/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 Amendment procedures

Amendments to the CP/CPS can only be made by the Trust Center Change Advisory Board. With every official change, this document receives a new ascending version number and publication date.
Amendments enter into force immediately upon publication (see also Section 2.3).
Updated versions result in the previous document versions becoming invalid. In the event of contradictory provisions, the 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 CP/CPS will enter into force immediately upon its release (see Section 9.12.1).

9.13 Provisions on dispute resolution

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 the 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 Various provisions

9.16.1 Complete contract

No stipulation.

9.16.2 Assignment of claims

No stipulation.

9.16.3 Severability clause

If a provision of this CP/CPS is or becomes ineffective or cannot be implemented, the validity of this statement is not otherwise affected as a result. In place of the ineffective and unimplementable provision, such a provision is considered agreed as comes closest to the economic purpose of this document in a legally binding way. The same applies for additions made in order to close contractual lacunas.

9.16.4 Execution (attorney's fees and waiver of rights)

No stipulation.

9.16.5 Force majeure

This regulation is intended to ensure that the contractual partner agrees with his end entities that he does not fall into arrears if the service is delayed or becomes impossible due to a force majeure.

9.17 Other provisions

9.17.1 Accessibility

The general access to the Trust Center services happens via web browser application. Operating systems offer users who need support due to disabilities (e.g. visual impairment) a variety of tools for better accessibility of applications or web pages.
Furthermore Trust Center analysis with its software developers if there is a necessity for any additional operation system independent support (e.g. webpages based on HMTL 5) next to the standard features mentioned above.
If the aforementioned technical measures are not sufficient, the Trust Center offers free support via phone for requesting, confirming or revoking a certificate.

10 Other applicable documents and references

10.1 Additional documents

Reference/no.	Document name	Last revised/version
GT&Cs	General Terms and Conditions for TeleSec products.	

10.2 References

Reference	Document name
[BDSG]	Federal Data Protection Act (Bundesdatenschutzgesetz), Federal Law Gazette
[CAB-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).
[CAB-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 TS EN 319411-1, 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 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 QC]	ETSI EN 319 412-5, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
[ETSI WEB]	ETSI EN 319 412-4, Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile 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
[RFC 2560]	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
[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/
[Siko SP]	ServerPass security concept
[SRK TC]	Framework security concept of the Trust Center information network

11 Glossary

Abbreviation	Description
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.
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.
Certificate holder	A natural or legal person who is issued a certificate and is legally bound by a subscriber agreement or terms of use.
Certificate Policy (CP)	Defines the guidelines for generating and managing certificates of a certain type.
Certificate Revocation List (CRL)	See Revocation list.
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 transparency	A Google project for certificate transparency: the certificates issued are written to publicly verifiable, manipulation-proof log servers in order to allow improperly or incorrectly issued TLS/SSL certificates to be identified faster and revoked. During the certificate issuing process necessary CT logserver will be contacted. These answer in form of a SCT, which will be stored in the certificate to protocol that the certificate has been registered on a logserver.
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 Authority Authorization (CAA)	A method for the domain owner to name which certification authorities may issue certificates for his domain(s).
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.
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.
Cross Certificate	A certificate that is used to establish a trust relationship between two Root CAs.
crt.sh	Certificate Transparency Log search engine
Cryptography	Science dealing with the encryption of data and related issues (such as digital signatures).
Device certificate	X.509 V3 certificate that contains either a host name or an IP address in the commonName field (CN) of the certificate holder's distinguishedName (subject) field and/or in at least one subjectAltName extension.
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.
Digital signature	A checksum created with a special mathematical procedure. Guarantees the authenticity of the signatory and the integrity of the data.
Directory service	Database that enables certificates and information about certificates (especially revocation lists) to be called up.
Distinguished Name	Format with which unique names can be specified according to the X.500 standard. A digital certificate must contain a DN.

Domain Name Systems	Hierarchical directory service for the management of the name space of the internet. The main purpose is to match / resolve domain names into IP addresses.
Electronic signature	See Digital signature.
End entity	See also certificate holder. 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.
Fully qualified domain name (FQDN)	Correct and complete domain name, i.e., a chain of all labels for a path in the domain name space (for further information see RFC 2181).
Hardware security module (HSM)	Hardware to generate and store private keys securely.
Hash value	In this context, a fixed length cryptographic checksum (the correct name is cryptographic hash value). It should be as unlikely as possible to calculate the entry from the hash value or to find several possible inputs for the same hash value (hash value is used as a synonym for fingerprint). In most cases a hash value is signed instead of a complete digital document.
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).
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.
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.
Legal person	A company, group, partnership, sole trader, trust, government authority, or legal entity with legal standing within the legal system of a country.
Lightweight Directory Access Protocol (LDAP)	Protocol for querying directories. This has displaced the significantly more complicated Directory Access Protocol (DAP) in many areas. LDAP provides 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.
Object identifier (OID)	A unique, alphanumeric or numeric identifier that is registered for a specific object or object class of the International Standards Organization (ISO) under the appropriate standard.
OCSP responder	An online server that is subordinate to the certification authority (CA) and is connected to its central repository to process certificate requests. Also see Online Certificate Status Protocol (OCSP)
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.
Period of validity	The period from the issue date (not before) until the expiry date (not after).
Permitted public data source	An authentication document or a data source (e.g., identity database, commercial register) that is used to check subject identity data, that is generally recognized by commercial companies and authorities (public administration) as reliable and that a third party created for a different purpose other than the issuing of certificates by the applicant.

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.
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).
Private key	The key from a key pair that the key owner keeps secret and uses to create digital signatures and/or decrypt electronic data and files that were encrypted using the corresponding public key.
Public device certificate	A device certificate that a sub-CA issues in the CA hierarchy below a root certificate.
Public key	The key from a key pair that the owner of the corresponding private key is permitted to make publicly available and that the relying side uses to verify digital signatures that were created using the owner's private key and/or to encrypt messages that can only be decrypted using the owner's corresponding private key.
Public key infrastructure	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.
Public Key Infrastructure X.509 (PKIX)	IETF standard that standardizes all relevant parts of a PKI.
Registration Authority (RA)	Component with which a person or a system must communicate to obtain a digital certificate.
Relying party	An individual person or legal entity (e.g., company, organization), which acts in reliance on the functioning of a certificate.
Request	English term for "Auftrag". Taken to mean a certificate request in this context.
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 a certificate revocation list (CRL).
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)
Root certification authority	Root certification authority (root-CA)
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).
Secure Multipurpose Internet Mail Extension (S/MIME)	Secure Multipurpose Internet Mail Extension. Extension of the MIME e-mail format, which describes additions for cryptographic services that guarantee the authenticity, integrity, and confidentiality of messages.
Secure Socket Layer (SSL)	Term used previously to describe Transport Layer Security. For further explanations, refer to Transport Layer Security.
Signature	See digital signature.
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.
Smartcard	Chip card with computing function that can be used for cryptographic purposes.
Subject	The natural person, device, system, unit or legal person that is named as the subject in a certificate. The subject is either the certificate holder or a device that is under the certificate holder's control or is operated by this person.

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 (subjectDN)	Subject = person or machine. Format with which unique names can be specified according to the X.500 and the LDAP standard. The subjectDN clearly identifies the certificate owner.
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).
Suspension	In the context of 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.
Terms of use	Provisions regarding safekeeping and permitted usage of an issued certificate in accordance with the specified requirements if the applicant/certificate holder is an affiliated company of the certification authority (CA), for example.
Transport Layer Security (TLS)	Crypto protocol for ensuring end-to-end connections on the Internet. Can be used instead of the more complex IPSec in many cases.
Trust Center Advisory Board	A board within the Trust Center that decides on PKI functions.
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.
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).
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.
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 X.509 certificate linter written in Go that checks for consistency with RFC 5280 and the CA/Browser Forum Baseline Requirements
Reliable Data Source	An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a certificate.

12 Acronyms

Acronym	Explanation
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
eIDAS	EU regulation on electronic identification and trust services for electronic transactions in the internal market (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
GT & C	General Terms and Conditions
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

RA	Registration Authority
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	German Digital Signature Act (Signaturgesetz)
SigV	German Digital Signature Regulation (Signaturverordnung)
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
TU	Test Unit
UCC	See Unified Communications Certificates.
UPN	User Principal Name
URL	Uniform Resource Locator
UTC	Universal Time Coordinated
XML	Extensible Markup Language