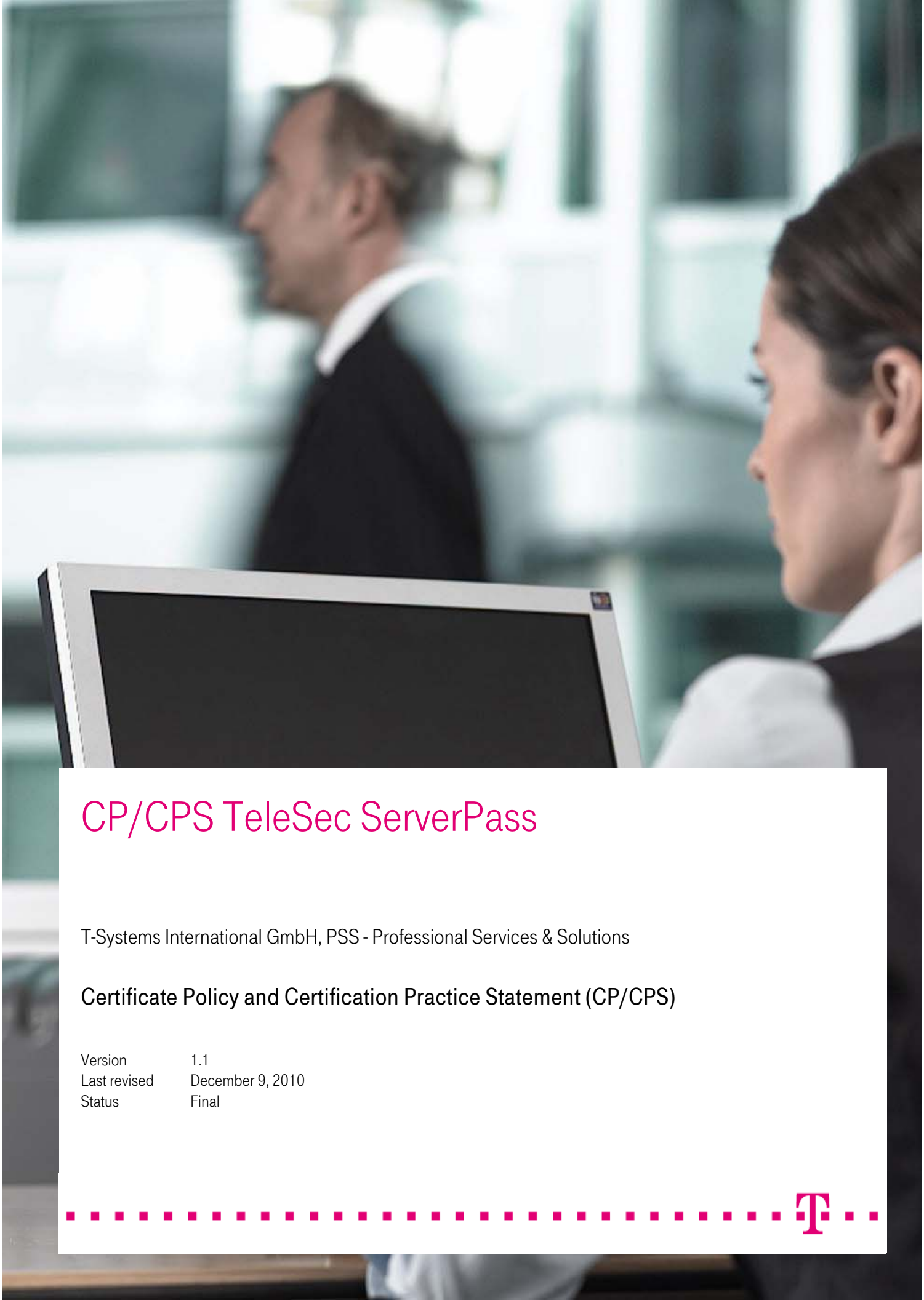

CP/CPS TeleSec ServerPass

T-Systems International GmbH, PSS - Professional Services & Solutions

Certificate Policy and Certification Practice Statement (CP/CPS)

Version	1.1
Last revised	December 9, 2010
Status	Final

Publishing Information

Published by

T-Systems International GmbH
ICT Operation, PSS – Professional Services & Solutions
Trust Center Services
Untere Industriestraße 20, 57250 Netphen, Germany

File name	Document number	Document name
CP_CPS_TeleSec ServerPass_EN_V1.1.doc		Certificate Policy and Certification Practice Statement (CP/CPS)

Version	Last revised	Status
1.1	December 9, 2010	Final

Summary

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

Change history

Version	Last revised	Revised by	Changes/comments
1.0	November 28, 2000	BREU	Initial version
2.0	September 1, 2001		Inclusion of renewal
2.1	December 1, 2001	EICK	Adaptation of Section 10
3.0	November 11, 2003	EICK	Certificate hierarchy update, contents revision, layout changes
3.1	December 1, 2003	EICK	Certificate hierarchy update
3.2	February 21, 2005	EICK	Certificate hierarchy update, revision of contents
3.3	February 9, 2006	EICK	Certificate hierarchy update Contents revised
3.4	May 4, 2007	EICK	Layout adaptation, update of Section 14
Merging the products TeleSec ServerPass Standard and TeleSec ServerPass EV (Extended Validation) and therefore 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 Structure according to RFC3647; all chapters have been revised and contents updated accordingly; layout adaptation.
1.1	December 9, 2010	EICK	Expanded by the variant TeleSec ServerPass SAN/UCC, Section 1.1 updated, Section 1.3.1 updated, Section 3.1.1.1 Country Name (C) updated, Section 6.3.2 updated

Table of contents

List of figures

List of tables

1 Introduction

The Trust Center is operated by the Group unit T-Systems International GmbH ("T-Systems").
In 1998, the Trust Center (under the name of "Trust Center of Deutsche Telekom") started operating as the first certification service provider that is accredited in accordance with the German Digital Signature Act (Signaturgesetz, SigG).
In addition to the precisely specified and certified operational processes, the T-Systems 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.
Both the structural and the organizational infrastructure meet the strict requirements of the German Digital Signature Act. The services offered by the T-Systems Trust Center include the TeleSec Public Key Service (PKS), which covers the process of issuing qualified certificates in accordance with the German Digital Signature Act (Signaturgesetz, SigG). The portfolio also includes further services for a wide range of PKI solutions, as well as one-time password procedures and timestamps.

1.1 Overview

TeleSec ServerPass is a service operated in the T-Systems Trust Center.
The TeleSec ServerPass (SSL/TLS certificate) makes an Internet/Intranet server identifiable and links the organization's identity to it.
TeleSec ServerPass is composed of the verified information from the subscriber, the public key of the web server, data on the certificate issuer and the signature of the T-Systems 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).

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 is offered in various product variants.

TeleSec ServerPass Standard:
The standard server certificate offers the abovementioned features and contains one domain name.

TeleSec ServerPass SAN/UCC:
The ServerPass SAN/ICC certificate offers the abovementioned features and compared to ServerPass Standard it has the additional option of documenting further SAN fields. The certificate can contain up to six domain names.
The domain names are composed of a public domain and up to

- 5 subdomains of the public domain or
- 5 multi-level domains of the public domain or
- 5 private IP/localhost addresses.

TeleSec ServerPass EV:
The product variant TeleSec ServerPass EV (Extended Validation) offers the abovementioned features as well as the additional security provided by stricter issuance rules according to [WTEVGUIDE] (see Section 10.1) and a more lengthy registration process, amongst other things.

Other purposes of ServerPass EV are:

- Making phishing and fraudulent activities more difficult in connection with 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.

Websites that use extended validation certificates are displayed in current browsers (Internet Explorer version 7 onwards, Firefox version 3 onwards, Opera version 9.5 onwards, Safari version 3.2 onwards) with a green address bar as well as additional information about 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 (cf. [WTEVGUIDE}):

- 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 is the Certificate Policy (CP) and the Certification Practice Statement (CPS) of the TeleSec ServerPass service and contains 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 ServerPass [AGB] 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 [WTEVGUIDE}.

1.2 Document name and identification

Name:	CP/CPS TeleSec ServerPass
Version:	1.1
Last revised:	December 12, 2010

The present CP/CPS supports the following Certificate Policy OIDs:
ServerPass Standard: (1.3.6.1.4.1.7879.13.2)
ServerPass EV: (1.3.6.1.4.1.7879.13.24.1)

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

1.3 PKI participants

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.

TeleSec ServerPass Standard until December 15, 2010:
The SSL certificates of the ServerPass Standard product variant issued in the T-Systems Trust Center are below the GlobalSign root CA and the GTE CyberTrust global root in the hierarchy (Figure 1).

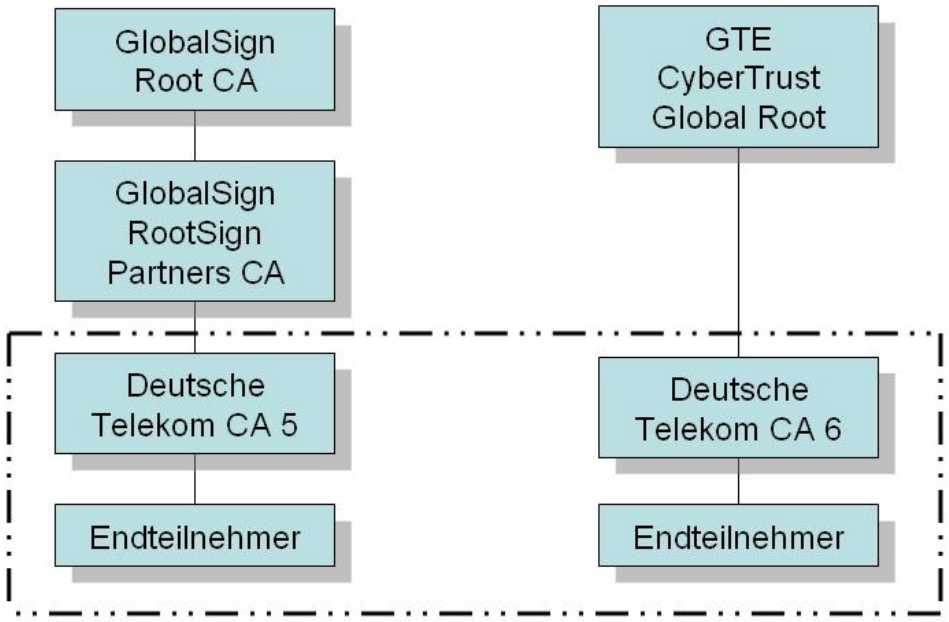

Figure 1: Overview of the certificate authorities for TeleSec ServerPass Standard until December 15, 2010

Legend:
Endteilnehmer = End entity

TeleSec ServerPass Standard and SAN/UCC as from December 16, 2010
The SSL certificates of the ServerPass Standard and SAN/UCC product variants issued in the T-Systems Trust Center are issued under the Baltimore CyberTrust root (Figure 2).

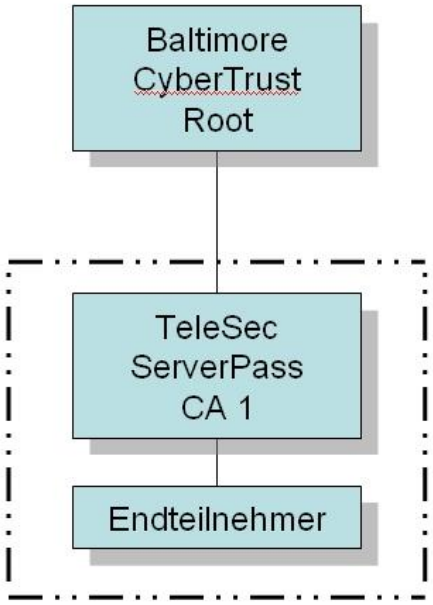

Figure 2: Certification authorities for TeleSec ServerPass Standard and SAN/UCC as from December 16, 2010

TeleSec ServerPass EV:
The T-TeleSec Extended Validation SSL CA Class 3 is operated in conformity with the currently applicable guidelines on the issuance and management of extended validation certificates ("Guidelines") which are published under http://www.cabforum.org. If there is a discrepancy between this document and the Guidelines, the Guidelines shall prevail.

The certification authorities for TeleSec ServerPass EV are shown in Figure 3.

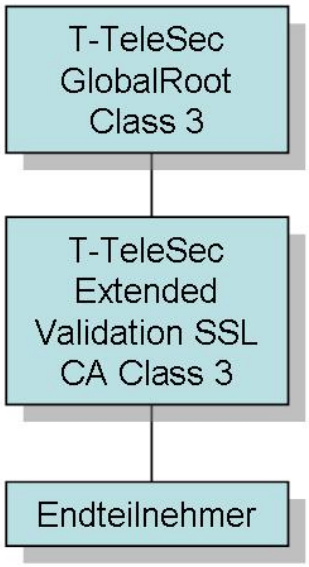

Figure 3: Overview of all certification authorities involved for TeleSec ServerPass EV

The trust chain can deviate from the hierarchy shown in Figure 2 if the highest trust anchor is not available.

1.3.2 Registration authorities

A registration authority (RA) is an authority that carries out the identification and authentication of customers, issues certificates for them or processes certificate requests (approves, rejects, resubmits), processes or forwards revocation requests.
In principle, every registration authority must ensure that no unauthorized person or machine gains possession of a certificate.

1.3.2.1 T-Systems Trust Center registration authority

The tasks of the T-Systems 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).

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

1.3.2.2 Third party registration authorities

TeleSec ServerPass Standard:
Third parties who enter into a contractual relationship with T-Systems can operate their own RA. The issuance of end entity certificates is done by the T-Systems CA. Third party RAs are obliged to comply at least with all the provisions of the root CP, of the TeleSec ServerPass CP/CPS (this document) and the contract concluded with T-Systems. Additional requirements for registration procedures can be implemented.

TeleSec ServerPass EV:
No third party registration authorities are permitted for registration of TeleSec ServerPass EV certificates.

1.3.3 End entity

End entities are understood to be all participants 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 party

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

1.3.5 Other participants

Not applicable.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

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

1.4.1.1 Certificates for legal persons

Purpose of SSL certificates					
		Signature and/or encryption	Authentication	Secure online communication	Security level
TeleSec ServerPass		✓	✓	✓	Medium
TeleSec ServerPass (Extended Validation)	EV	✓	✓	✓	High

Table 1: Use of certificates for legal persons

1.4.2 Prohibited certificate usage

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 where 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 must not be used as CA or Root CA certificates.

1.5 Policy administration

1.5.1 Organization administering the document

This document (CP/CPS) is published by T-Systems International GmbH, ICTO-SDM CSS & Special Services–PSS-Security Solutions- Trust Center Services.

1.5.2 Contact information

T-Systems International GmbH
Trust Center Services
Untere Industriestrasse 20
57250 Netphen
Germany

Tel: +49 (0) 1805 268 204 (landlines: EUR 0.14/minute, mobile networks: max. EUR 0.42/minute)
E-mail: telesec_support@t-systems.com
Fax: +49 (0) 2151 36607972
Web: http://www.telesec.de

1.5.3 Maintenance of the document

This document (CP/CPS) remains valid as long as it is not revoked by the publisher (see Section **Fehler! Verweisquelle konnte nicht gefunden werden.**). It is updated when required and is then assigned a new ascending version number (see also Sections 9.12.1 and 9.12.2).

1.5.4 Approval procedure of this document (CP/CPS)

The publisher named in Section **Fehler! Verweisquelle konnte nicht gefunden werden.** is responsible for this document (CP/CPS). The approval is given by the Change Advisory Board.

1.6 Acronyms and definitions

Acronyms and term definitions can be found in Section 12.

2 Publication and repository responsibilities

2.1 Repositories

T-Systems operates databases for the TeleSec ServerPass (EV) service and is responsible for the contents.
Extracts from these databases are provided in prepared form as a certification revocation list (CRL) on repositories or can be accessed via the validation service (OCSP responder).

2.2 Publication of certificate information

T-Systems 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 until the revocation time 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.
T-Systems publishes the current CA and Root CA certificates at: http://www.telesec.de/serverpass/support_rootca_akzeptanz.html.

2.3 Publication frequency

Updates to the CP/CPS are published as described in Section 9.12. The certificate revocation list is published as described in Section 4.9.7.

2.4 Access to the information services

Access to the revocation lists (CRL, ARL) and the OCSP service is not subject to any access control for subscribers (Section 1.3.3) or relying parties (Section 1.3.4). Read access to this information is not restricted.
Subscribers and users also have unrestricted read access to information from the CA and root CA (see Section 2.2) via the relevant websites.

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

3.1.1.1 TeleSec ServerPass Standard: Conventions for the components of the Subject DN

Conventions for Subject DN are defined in this section.
The English terms used below are also used in Germany these days.

Organization Name (O) (mandatory field)
This field contains the organization name (e.g., company, institution, authority) of the subscriber.
Example: O=Sample company Ltd

This information is verified using the commercial register excerpt "HR Auszug" or comparable registers/documents.

Organizational Unit Name 1-5 (OU1) (optional)
This field contains an organizational unit (department, area) or division/subdivision or group, team.
Example: OU1=Procurement, OU2= Branch sample city

This information is not verified.

Common Name (CN) (mandatory field)
The Common Name field must contain the FQDN (Fully Qualified Domain Name).
Example: CN=www.sampledomain.com
The Common Name may contain the following characters: `A-Z,a-z,0-9,',(,),+,,,-,.,/,:,=,space`
This information is verified using publicly accessible directories (e.g., DENIC).

Locality (optional)
This field contains the name of the city in which the organization (e.g., company, institution, authority) is based.
Example: locality=Sample city

This information is not verified.

State or Province (optional)
This field contains the state or province where the organization (e.g., company, institution, authority) is based.
Example: state or province=sample province

This information is not verified.

Country Name (C) (mandatory field)

This is a **mandatory field** and contains the name of the country in which the subscriber has his 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).
T-Systems will check this information in the course of the registration process.
Example: C=DE

Street Address (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 not verified.

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 not verified.

3.1.1.2 TeleSec ServerPass EV: Conventions for the components of the Subject DN

Organization Name (O)
This is a **mandatory field** and contains the organization name (e.g., company, institution, authority) of the subscriber. The organization name in the certificate must use the official spelling of the organization, i.e., it must be identical to the respective entry in the register (commercial register or similar).
T-Systems will check this in the course of the registration process and take appropriate action if this requirement has not been met.
Example: O=Sample company Ltd

Organizational Unit Name 1 (OU)
This field is **optional** and contains an organizational 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 must be avoided. If information is provided in this field, T-Systems will check and verify it in the course of the registration process. T-Systems will refuse to issue the EV certificate if a check is not possible or can only be carried out with great difficulty.
Example: OU1=Procurement

Common Name (CN)
This is a **mandatory field** and contains the FQDN (Fully Qualified Domain Name).
T-Systems will check this information as well as the ownership relationships in the course of the registration process, using publically accessible directories.
Example: CN=www.sampledomain.com

Locality
This is a **mandatory field** and contains the name of the city where the organization has its registered place of business.
T-Systems will check this information in the course of the registration process.
Example: locality=Sample city

State or Province
This is a **mandatory field** and contains the state or province where the organization has its registered place of business.
T-Systems will check this information in the course of the registration process.
Example: state or province=sample province

Country Name (C)

This is a **mandatory field** and contains the name of the country in which the subscriber has his 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).

T-Systems will check this information in the course of the registration process.

Example: C=DE

Street Address

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

If information is provided in this field, T-Systems will check it in the course of the registration process.

Example: street address=Sample street 17

Postal Code

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

If information is provided in this field, T-Systems will check it in the course of the registration process.

Example: postal code=12345

Business Category

This **EV-specific** field is a **mandatory field** and provides information on the business category. The correct value of this field is set by T-Systems based on the specified business category.

The business category is checked by T-Systems in the course of the registration process.

Example: businessCategory=V1.0, Clause 5.(b)

Jurisdiction of Incorporation or Registration

These **EV-specific** fields are **mandatory fields** (according to the classifications named below) and 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).

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

Registration Number

This **EV-specific** field is a **mandatory field** and contains the unique registration number. In the event that no registration number is/was issued, this field contains the date of registration in the format according to ISO 8601: YYYY-MM-DD.

Example: serialNumber=HRB3244
serialNumber=2005-10-23

3.1.2 Meaningful names

End entity and CA certificates must contain names in the subject of the certificate with a commonly understood 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 subscribers

No certificates with pseudonyms or anonymous certificates are issued.

3.1.4 Rules on the interpretation of different name formats

No rules.

3.1.5 Uniqueness of names

End entities can own two or more certificates with the same unique Subject DN. These do however 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 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 Identity checks upon the initial request

3.2.1 Methods for proving the ownership of the 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 obtained using the PKCS#10 method.

3.2.2 Identity check on an organization

TeleSec ServerPass Standard:
The initial request can only be placed after successful registration in the customer portal <myServerPass>.
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 business category:

Legal person:
The request form signed by an authorized signatory.

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:

- Is the information on the request form identical to the information in the Certificate Signing Request (CSR) of the online request?
- Does the company name of the organization/company correspond to the entry in the electronic commercial register or comparable directories? Do current organization documents (no more than 30 days old) issued by a competent authority also confirm the organization's existence (e.g., register of associations or comparable document, official stamp)?
- The authorization of the responsible contact at the organization named in the request (legal person),
- Does the domain name correspond to the official directories? Does the customer own the domain; i.e., has he been given the exclusive right of use by means of a corresponding authorization?
- 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
- Are any necessary Whois entries available.

Additional checks are carried out as required.

TeleSec ServerPass EV:
The initial request can only be placed after successful registration in the customer portal <myServerPass>.
The required checks are carried out in accordance with [WTEVGUIDE] .

3.2.3 Identity check on a natural person

A TeleSec ServerPass is only issued for organizations.

3.2.4 Unverified entity information

TeleSec ServerPass Standard:
Unverified information is information that is incorporated in the certificate without being checked and includes:

- organizational unit (OU1-5),
- other information that is identified as unverified in the certificate (e.g., key usage, extended key usage).

TeleSec ServerPass EV:
A TeleSec ServerPass EV certificate does not contain any unverified information.

3.2.5 Authorization check

TeleSec ServerPass Standard:
The authorization is checked by means of an authorization call.

TeleSec ServerPass EV:
The authorization is checked according to the EV Guidelines [WTEVGUIDE].

3.2.6 Criteria for collaboration

Not applicable.

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

TeleSec ServerPass Standard:

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

TeleSec ServerPass EV:
Re-key in the actual sense does not take place in the case of ServerPass EV. Instead a new request is made in accordance with Section 3.2.2.

3.3.1 Identification and authentication for routine re-key

TeleSec ServerPass Standard:
Key renewal takes place exclusively in the customer portal and can only be requested by the authorized customer as part of re-certification. The identity and authenticity are checked by means of the correct access data and the service password required for renewal.

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

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

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

3.4 Identification and authentication for revocation requests

Authorized end entities can revoke their certificates themselves via the customer 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, T-Systems reserves the right to carry out certificate revocations in the event of misuse or suspected misuse, (see also Sections 1.3.2.1, 4.9.1, 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 T-Systems 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 T-Systems or the registration authority. Appropriate investigative measures are implemented. If the justified misuse of a certificate is confirmed, T-Systems can revoke this certificate.

The following input channels must be used for contact purposes:
Tel: +49 (0) 1805 -268204 (fixed network: EUR 0.14/minute, mobile networks: max. EUR 0.42/minute)
E-mail: telesec_support@t-systems.com
Fax: +49 (0) 2151-36607972

4 Operational requirements in the life cycle of certificates

4.1 Certificate application

4.1.1 Who can request a certificate

Every person who has registered in the customer portal <myServerPass> can request a certificate after filling in the mandatory fields. This is usually the authorized representative of a legal person.

4.1.2 Ordering procedure and obligations

4.1.2.1 End entity

All end entities undertake to comply with these statements (CP/CPS).

The end entity also commits to the following:

- That the statements made in the certificate request are true and correct
- To generate key pair(s) or request their generation
- To transmit its public key with its certificate data to T-Systems 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

4.2.1 Performing identification and authentication

TeleSec ServerPass Standard and ServerPass SAN/UCC:
The identification and authentication of the required end entity information is performed by T-Systems or an RA in accordance with Section 3.2.

TeleSec ServerPass EV:
The identification and authentication of the required end entity information is performed by T-Systems.

4.2.2 Approval or rejection of certification requests

If the identification and authentication of the required end-entity information according to Section 3.2 was successful, the certification request is approved and the certificate issued.

A certificate request can be rejected if:

- The identification and authentication of the required end-entity information according to Section 3.2 was not successful
- The end entity does not provide the additional documents that may be required and requested
- The end entity does not reply to queries or when contacted

If a request is rejected, the subscriber 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 Issuance of certificates

4.3.1 Measures of the CA during the issuance of certificates

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 subsciber about the issuance 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 customer portal <myServerPass> under 'My Certificates'.

4.4 Certificate acceptance

4.4.1 Acceptance by the subscriber

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

4.4.2 Publication of the certificate by the CA

The publication of certificates in public directories is not envisaged.

4.4.3 Notification of other authorities about certificate issuance by the CA

The notification of other authorities is not envisaged.

4.5 Use of key pair and certificate

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

The certificate and the associated private key may only be used in accordance with the General Terms and Conditions (GT&Cs) for TeleSec ServerPass 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 run out 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. T-Systems 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

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 Subject-DN (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 renewal.

TeleSec ServerPass EV:
Renewal is not currently offered in the case of ServerPass EV.

4.6.1 Conditions for renewal

TeleSec ServerPass Standard and SAN/UCC:
Renewal is possible at any time whilst the current certificate remains valid. Expired certificates cannot be renewed.

TeleSec ServerPass EV:
Renewal is not currently offered in the case of ServerPass EV. Instead, a new request can be initiated as conveniently as a renewal, by using the customer portal <myServerPass>.

4.6.2 Who may request a renewal?

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

TeleSec ServerPass EV:
Renewal is not currently envisaged.

4.6.3 Processing renewals

TeleSec ServerPass Standard and SAN/UCC:
The request for a renewal is electronically checked and automatically released.

TeleSec ServerPass EV:
Renewal is not currently envisaged.

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

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

TeleSec ServerPass EV:
Renewal is not currently envisaged.

4.6.5 Acceptance of a renewal

TeleSec ServerPass Standard and SAN/UCC:

The regulations in Section 4.4.1 apply.

TeleSec ServerPass EV:
Renewal is not currently envisaged.

4.6.6 Publication of a renewal by the CA

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

TeleSec ServerPass EV:
Renewal is not currently envisaged.

4.6.7 Notification of other authorities about a renewal by the CA

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

TeleSec ServerPass EV:
Renewal is not currently envisaged.

4.7 Re-key of certificates

TeleSec ServerPass Standard and SAN/UCC:
Re-key can be requested upon renewal. A requirement for this is the creation of a new key pair and the submission of the new public key in the server certificate request.
Whether the “old” key pair and therefore the “old" public key can be used again depends on the technical specifications for their use (e.g., server).
A prerequisite for using the same key pair is that the unique mapping of the subscriber and the key is retained, 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.

TeleSec ServerPass EV:
A re-key is not currently offered in the case of ServerPass EV. Instead, a new request can be initiated as conveniently as a re-key, by using the customer portal <myServerPass>.

4.7.1 Conditions for re-key

TeleSec ServerPass Standard and SAN/UCC:
Renewal with re-key can be carried out at any time during the current certificate's period of validity and only by the authorized customer.

TeleSec ServerPass EV:
A re-key is not currently offered in the case of ServerPass EV.

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:
A re-key is not currently offered in the case of ServerPass EV.

4.7.3 Processing of re-key requests

TeleSec ServerPass Standard and SAN/UCC:
If the authorized end customer requests the renewal (re-key) after entering the service password, the renewal certificate is automatically issued.

TeleSec ServerPass EV:
A re-key is not currently offered in the case of ServerPass EV.

4.7.4 Notification of the subscriber about the certificate issuance

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

TeleSec ServerPass EV:
A re-key is not currently offered in the case of ServerPass EV.

4.7.5 constituting acceptance of a re-keyed certificate

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

TeleSec ServerPass EV:
A re-key is not currently offered in the case of ServerPass EV.

4.7.6 Publication of a re-keyed certificate by the certification authority

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

TeleSec ServerPass EV:
A re-key is not currently offered in the case of ServerPass EV.

4.7.7 Notification of other entities about a certificate issuance by the certification authority

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

TeleSec ServerPass EV:
A re-key is not currently offered in the case of ServerPass EV.

4.8 Certificate modification

If information in the existing certificate changes, a new certificate must be requested.

4.8.1 Conditions for a certificate modification

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 (see also Section 3.1.1 on the subject of certificate contents).

4.8.2 Who may request a certificate modification

TeleSec ServerPass Standard and SAN/UCC:
The statements in Section 3.4 apply accordingly.

TeleSec ServerPass EV:
Not applicable.

4.8.3 Processing of certificate modifications

TeleSec ServerPass Standard and SAN/UCC:
If the contents of a certificate change, renewed identification is required, the same as with a new request (see Section 3.2 et seq.).

TeleSec ServerPass EV:
Not applicable.

4.8.4 Notification of the subscriber about the issuance of a certificate

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

TeleSec ServerPass EV:
Not applicable.

4.8.5 Acceptance of a certificate modification

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

TeleSec ServerPass EV:
Not applicable.

4.8.6 Publication by the CA of a certificate with modified data

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

TeleSec ServerPass EV:
Not applicable.

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

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

TeleSec ServerPass EV:
Not applicable.

4.9 Certificate revocation and suspension

4.9.1 Reasons for revocation

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

- The private key has been compromised, lost, stolen or disclosed or there is strong suspicion that this has happened
- The details in the certificate (except for unverified end-user information) are no longer up-to-date, are invalid or incorrect
- The certified key (public key) or the cryptographic algorithms used with it no longer meet current requirements
- A case of misuse by the persons authorized to use the key has occurred or is suspected to have occurred
- Legal requirements or court judgments
- The certificate is no longer required or the subscriber expressly requests the revocation of the certificate.

The T-Systems Trust Center revokes end-entity certificates for the following reasons:

- It becomes known that the private key has been lost (e.g., loss or theft)
- The private key has been or is suspected to have been compromised
- Considerable payment default beyond the payment periods agreed in the contract
- The details in the certificate (except for non-verified end entity information) are no longer correct
- There is a case of misuse or the suspicion of misuse of the certificate by the subscriber or other persons authorized to use the key
- The certificate is used or handled in conflict with the GT&C (General Terms and Conditions) or the certificate policy or certification practice statement (CP/CPS)
- The certified key or the algorithms used with it no longer meet current requirements
- It comes to light that an essential requirement for issuing the certificate has neither been fulfilled nor had its fulfillment waived
- The certification authority ceases operations
- Legal requirements or court judgments
- The subscriber is no longer authorized to use the certificate

TeleSec ServerPass EV:
In addition to these reasons, there are a number of specific reasons named in [WTEVGUIDE] which T-Systems records and logs accordingly:

- The EV certificate is not authorized. This means that, for example, it is later discovered that the EV certificate was issued under false pretences.
- The usage agreements were not complied with.
- The certificate violates the provisions and conditions with regard to the issuing of EV certificates.
- The CA is no longer permitted to issue certificates and also no longer provides a repository.

4.9.2 Who can request revocation

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

- Authorized persons representing legal persons.
- Registration staff from the T-Systems 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 itself. The revocation is final. The subscriber is automatically informed by e-mail about the revocation status.

The T-Systems Trust Center reserves the right to revoke certificates if at least one of the reasons for revocation listed in Section 4.9.1 applies.

4.9.3.2 Revocation of a CA or root CA certificate

T-Systems undertakes to revoke a T-Systems CA certificate as soon as it suspects that a key is compromised. T-Systems reserves the right to revoke the certificate if this becomes necessary for operational reasons. The revocation of this certificate is carried out by a responsible employee of the Trust Center. This is an internal T-Systems process and is not described in more detail here. The revoked certificate is added to the certification authority revocation list (ARL).

4.9.4 Grace period for a revocation request

As soon as there is a reason for revocation according to Section 4.9.1, the revocation request must be made as soon as possible within an economically suitable period.

4.9.5 Periods for processing a revocation request by the CA

The revocation by the end entity is passed on to the linked systems immediately after the revocation process in the customer 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, T-Systems 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 repository.

4.9.7 Frequency of publication of revocation information

The certificate revocation list (CRL) and certification authority revocation list (ARL) are published via the repository, as described in Section 2.3.
The certificate revocation list (CRL), which contains the revoked certificates of end entities, is updated twice a day and published by the repository.
The revoked CA certificates are listed in the revocation list for certification authorities (ARL). Updates are carried out every 6 months or depending on events, and publication takes place via the corresponding repository.
Revoked certificates that are outside of the validity period are removed from the revocation list.

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

Online information on the certificate status is available via OCSP.
For further information, 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. Another way of checking the status is via the current certificate revocation list (CRL).

4.9.11 Other available forms of communicating revocation information

No other forms of communication are used at present.

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

Not applicable.

4.9.15 Suspension procedure

Not applicable.

4.9.16 Limitation of the suspension period

Not applicable.

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

Not applicable.

4.10.2 Availability of the service

The certificate status service is available 24/7.

4.10.3 Optional features

Not applicable.

4.11 End of subscription

4.11.1 Ending the end entity's use of a certificate

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

4.12 Key storage and recovery

4.12.1 Guidelines and practices for key storage and recovery

For the certification authority TeleSec ServerPass operated at the T-Systems 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 backup purposes, so that qualified staff 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

Not applicable.

5 Building, administration and operational checks

The T-Systems Trust Center is housed in a specially protected building and operated by knowledgeable staff. All processes for generating and managing certificates from the certification authorities operated there are defined in detail. All technical security measures are documented.
The following statements apply to the certification authorities operated by the T-Systems Trust Center.

5.1 Physical controls

5.1.1 Location and structural measures

T-Systems operates a Trust Center, consisting of two fully redundant parts, two separate energy wings (electrical, air conditioning, water) with property management system and emergency power supplies as well as an administration wing.
The Trust 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: the German Insurance Association (Gesamtverband der Deutschen Versicherungswirtschaft, GDV) and the applicable DIN standards on fire protection, smoke protection and blocking of attacks. The Trust Center is approved by VdS/GDV in terms of security technology.
The technical controls are supplemented by organizational elements that include the handling of security-relevant techniques and regulations regarding access to security zones for employees and third parties (visitors, external staff and cleaning staff), delivery of materials (hardware, accessories, resources) and tidiness at the work station as well as in computer rooms.

5.1.2 Physical access

The Trust Center is subject to access rules that regulate 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 intakes 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 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 exposure

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 (flood risk). Any fire is extinguished using inert gas.

5.1.5 Fire protection

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 in extreme emergencies for putting out fire.
Fire sections are secured by fire-resistant components. Passages through fire protection walls are equipped with self-closing fire protection doors.
In areas with double floors as well as suspended ceilings the fire protection walls go right through to the ceilings/floors of the storey.
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 is being 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 and logical 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 T-Systems' regular disposal guidelines.

5.1.8 External backup

T-Systems 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 controls

5.2.1 Trustworthy roles

Trustworthy persons are all persons (T-Systems 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 issuance 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:

- rust Center staff (e.g., system administration)
- staff of cryptographic departments
- security personnel
- 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 Change Advisory Board of the T-Systems 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 T-Systems Trust Center.

5.2.2 Number of persons required for a task

The operational maintenance of the certification authority and the repository (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:
The dual control principle stipulated in the EV guidelines [WTEVGUIDE] for the release and approval process of an EV certificate is implemented by T-Systems according to the requirements. Technical means are in place to prevent circumvention of the dual control principle.

5.2.3 Identification and authentication for each role

T-Systems employees who are classed as trustworthy and who carry out trustworthy activities, are subject to a T-Systems internal security check (see Section 5.3.2).
T-Systems 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

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)
- backing up and restoring databases and HSMs
- key lifecycle management of CA and root CA certificates.

5.3 Personnel controls

5.3.1 Required qualifications, experience and security check

Employees who wish to work as trustworthy persons are required by T-Systems to prove that they have the qualifications and experience necessary to fulfill their prospective work obligations in a competent and satisfactory manner.
T-Systems must be provided with a certificate of good conduct at regular intervals, but no later than after three years.

5.3.2 Security check

Before starting work in a trustworthy role, T-Systems 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, T-Systems 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 controls 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 controls is governed by the applicable law.

5.3.3 Education and training requirements

The staff at T-Systems undergo the training measures required to fulfill their work obligations in a competent and satisfactory manner. T-Systems keeps records of these training measures.
The training programs at T-Systems are tailored towards the individual work areas and include, for example:

- advanced PKI knowledge
- procedures according to ITIL
- data protection
- security and operational guidelines and procedures of T-Systems
- 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.

5.3.4 Retraining frequency and requirements

The staff at T-Systems receive refresher training and further training courses to the extent required and at the intervals required.

5.3.5 Frequency and sequence of job rotation

Not applicable.

5.3.6 Sanctions in the event of unauthorized activities

T-Systems reserves the right to punish unauthorized activities or other violations of this CP/CPS and the procedures described therein, and to implement 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

T-Systems 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 T-Systems in comparable positions.
The above persons, who have not yet concluded or successfully completed the security check described in Section 5.3.2, are only given access to the secure facilities at T-Systems 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, T-Systems provides its employees with all the aids and documents they need for this (training documents, procedural instructions).

5.4 Log events

5.4.1 Type of events recorded

Changes in the life cycle of the TeleSec ServerPass certification authority key are logged. In detail, this refers to the following events:

- generation
- storage
- backup
- recovery
- archiving
- destruction
- changes to hardware and software
- certificate request (successful/failed processing and included documents)
- generation of certificates
- certificate revocation
- renewal
- re-key
- certificate revocation lists
- logging of internal and external audits

5.4.2 Processing interval of the protocols

The audit logs/logging files are permanently examined for important events relevant to security and operations. Furthermore, T-Systems 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/logging files are archived after processing according to Section 5.5.2.

5.4.4 Protection of audit logs

Audit logs/logging files are protected against unauthorized access.

5.4.5 Backup procedures for audit logs

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

5.4.6 Audit recording system (internal vs. external)

Audit data/logging files at an application, network and operating system level are automatically generated and recorded. Manually generated audit data is recorded by T-Systems 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 regular working hours.

5.4.8 Vulnerability assessments

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

5.5 Data archival

5.5.1 Type of archived datasets

T-Systems 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:

- request documents: At least ten (10) years after the certificate validity period expires
- audit/event logging data 7 years

5.5.3 Protection of archives

T-Systems ensures that only authorized and trustworthy persons are given access to 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

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

5.5.6 Archive recording system (internal or external)

T-Systems 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 changeover

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

- the key material is compromised
- the cryptographic algorithm needs to be changed
- the key length needs to be changed
- 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 restoration of private keys and disaster recovery

5.7.1 Handling of incidents and compromised situations

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

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 T-Systems security department. The event entails a corresponding escalation, incident investigation, incident response and finally incident resolution. Disaster recovery is carried out, depending on the incident classification.

5.7.3 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 certificate authority revocation list (ARL) generated and published.

5.7.4 Business continuity after an emergency

T-Systems has developed, implemented and tested an emergency plan to mitigate all kinds of disasters (natural disasters or disasters of human origin). This plan is tested and updated on a regular basis so that the IT components, software and data can be restored as quickly as possible in the event of a disaster.

5.8 Cessation of operations

Cessation of operations may only be invoked by T-Systems.
If a T-Systems certification authority has to cease operating, a cessation plan will be developed. Economically suitable efforts (or efforts promised in the individual agreements) will be made to notify in advance any subordinate authorities affected by these cessations of operations (end entities, registration authorities of resellers and T-Systems).
A cessation plan may include the following regulations:

- 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 transition regulations required for a successor CA
- reimbursement of costs depending on the content of existing individual agreements
- retention of the documentation and archives of the certification authority (CA)

6 Technical security controls

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 140-1/level 2 evaluated) in the so-called "key ceremony".
All activities during the “key ceremony” are documented and signed by all persons involved. These records are stored for auditing and tracking purposes for a period deemed suitable by T-Systems.
Keys pairs are not generated for end entities. The end entity generates the key pair of its own accord using tools provided by the server application.

6.1.2 Delivery of private keys to end entities

The end entity's private key always remains with the end entity. Private keys are not delivered to end entities.

6.1.3 Delivery 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 Delivery 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 T-Systems Trust Center accepts key lengths of 2048 and 4096 bits for extended validation end-entity certificates. Key lengths shorter than 2048 bits (for ServerPass EV) or 1024 bits (for ServerPass Standard) are automatically rejected by the request system in the very first request step.
For end entity certificates, the T-Systems Trust Center generally recommends a key length of 2048 bits.

6.1.6 Generating the parameters of public keys and quality control

Not relevant.

6.1.7 Key usage (according to the X.509v3 expansion "Key usage")

See Section 7.1.2.5.

6.2 Protection of private keys and technical checks of cryptographic modules

T-Systems 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 a security-checked hardware security module (FIPS 140-1/level 2 evaluated). The keys are backed up using high-quality multi-person backup techniques (see also Section 6.2.2)

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

T-Systems has implemented technical, organizational and procedural mechanisms that require the participation of several trustworthy and trained persons of the T-Systems Trust Center to be able to carry out confidential cryptographic CA operations. The usage of the private key is protected by a divided authentication process (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

The storage of private keys with trustees outside T-Systems is not permitted.

6.2.4 Backup of private keys

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

6.2.5 Archiving of private keys

CA, root CA and OCSP keys are destroyed when they reach the end of their validity periods. They are not archived.

6.2.6 Transfer of private keys in or by a cryptographic module

T-Systems generates CA keys on cryptographic hardware modules (HSM). Copies of these keys are made for restoration and disaster recovery purposes (see Section 6.2.4 and 6.2.5). In this case the transfer between both modules takes place in encrypted form.

6.2.7 Storage of private keys on cryptographic modules

T-Systems stores CA keys in secure form on cryptographic hardware modules (HSM).

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.

6.2.8.1 Keys of end entities

The end entity is entitled to take economically suitable controls 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 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 a similar security control, 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.
- Taking appropriate controls to physically protect the administrator or operator workplace against unauthorized access.

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

6.2.10 Method for destroying private keys

The destruction of CA keys requires the participation of several trustworthy persons of 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.
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

T-Systems backs up and archives the certificates (CA, root CA and end entity certificates) as part of regular backup controls.

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 T-Systems certificates are described in **Table 2**.
T-Systems 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:	Validity:
TeleSec ServerPass Standard and SAN/UCC	
Deutsche Telekom CA 5	7 years
Deutsche Telekom CA 6	7 years
TeleSec ServerPass CA 1	7 years
End entity certificates	1, 2 or 3 years. The period of grace is 5 days.
TeleSec ServerPass EV	
T-TeleSec GlobalRoot Class 3	25 years
T-TeleSec Extended Validation SSL CA Class 3	10 years

End entity certificates	One (1) year. The period of grace is 14 days.

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 T-Systems undertake to protect the secret shares for activating the private keys of 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 6.2.10) the activation data is no longer worth protecting.

6.5 Computer security controls

T-Systems carries out all PKI functions with the help of trustworthy and appropriate systems.

6.5.1 Specific technical requirements for computer security

T-Systems ensures that the management of CA systems is protected against unauthorized third-party access. T-Systems uses protection mechanisms (e.g., firewalls, access protection, dual control principle), to protect the CA functions, repositories and OCSP responder against internal and external intruders. Direct access to CA databases that support the CA functions is restricted to appropriate, trained and trustworthy operating personnel.

6.5.2 Assessment of computer security

As part of the security concept, which is based on the Digital Signature Act [Signaturgesetz], different threat analyses are carried out to test the effectiveness of all controls implemented.

6.6 Technical controls on the lifecycle

6.6.1 System development controls

No provisions.

6.6.2 Security management controls

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

6.6.3 Security controls on the lifecycle

No provisions.

6.7 Network security controls

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

- The networks of the certification service are separated from the Internet by firewalls and limit the data traffic to the amount necessary for the functions.
- Security-critical components and systems that are accessible from the Internet (e.g., repository, 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 a separate network.
- 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.

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, revocation list and OCSP profiles

7.1 Certificate profile

The certificates issued by T-Systems meet the following requirements:

- [RFC 5280]
- [X.509]
- [WTEVGUIDE]

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

Field:	Value or value limitation:
Version:	Certificate version
Serial number:	Definitive value
Signature algorithm:	RSA - SHA-1 (alternatively RSA-SHA-256)
Issuer:	corresponding 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

Table 3: Certificate attributes according to X509.v3

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 correspond to the latest Version 3. The additional extensions and properties are explained in more detail in the following sections.
The CA certificates are also of the X.509v3 type.

7.1.2 Certificate extensions

In order to fulfill the standard X.509v3 and the guidelines for EV certificates [WTEVGUIDE], T-Systems 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 according to Section 1.2 ,
(EV policy OID).
certificatePolicies:policyQualifiers:policyQualifierId = id-qt 1.
certificatePolicies:policyQualifiers:qualifier = URI to this document (CP/CPS).

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, through whose URI (HTTP and LDAP) the current certificate revocation list (CRL) can be accessed on the repository. 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 repository. 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

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 CA certificates are given the user type "certification authority" with the path length "1". The criticality of this extension is set to "critical".

7.1.2.4 "Extended key usage" extension (ExtendedKeyUsage)

The end entity certificates are given the extended key usage TLS Web Server Authentication (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 table in **Table 4** assigns key usages to the different certificate profiles.

		TeleSec ServerPass Standard			TeleSec ServerPass EV		
		EE certificate	Deutsche Telekom CA 5	Deutsche Telekom CA 6	EE certificate	T-TeleSec Extended Validation SSL Class 3 CA	T-TeleSec GlobalRoot Class 3
	Criticality	critical	critical	critical	critical	critical	critical
Bit	Name						
0	digitalSignature	✓	×	×	✓	×	×
1	nonRepudation	×	×	×	×	×	×
2	keyEncipherment	✓	×	×	✓	×	×
3	dataEncipherment	×	×	×	×	×	×
4	keyAgreement	×	×	×	×	×	×
5	keyCertSign	×	✓	✓	×	✓	✓
6	CRLSign	×	✓	✓	×	✓	✓
7	encipherOnly	×	×	×	×	×	×
8	decipherOnly	×	×	×	×	×	×

Table 4: 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 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: http://ocsp.serverpass.telesec.de/ocspr

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

7.1.3 Object IDs (OIDs) of algorithms

The end entity certificates are signed using the following algorithm:
sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}, -> 1.2.840.113549.1.1.5

7.1.4 Forms of names

The end entity certificates are given a distinguished issuer name (issuer DN) for this service and a distinguished subject name (subject DN) as described in Section 3.1.1.

7.1.5 Name constraints

Name constraints can result from the character set used and/or field lengths.

7.1.6 Object IDs (OIDs) of certificate policies

If the CertificatePolicies extension is used, certificates receive the object ID for the certificate policies which correspond to the relevant product variant of the ServerPass service (see Section 1.2). For older certificates which were issued before this CP/CPS was published and which contain the CertificatePolicies extension, the certificates refer to the previous CPS_ServerPass.

7.1.7 Usage of the "policy constraints" extension

No provisions.

7.1.8 Syntax and semantics of policy identifiers

The current CP/CPS is always stored. Older versions are stored in the corresponding repository.

7.1.9 Processing semantics for the "critical certificate policies" extension

No provisions.

7.2 CRL profile

The revocation lists issued by T-Systems 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:	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-1
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
CRL 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: CRL attributes according to X509.v2

7.2.1 Version number(s)

T-Systems supports certificate revocation lists in the X.509 Version 2 format which fulfill the requirements according to RFC 5280.

7.2.2 CRL and CRL 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 "CRL 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. The reasons for revocation are stored internally by T-Systems and are not added to the revocation list. This extension is therefore not elaborated on here.

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 certificate, issued by T-Systems, contains the "extended key usage" attribute with the OID "1.3.6.1.5.5.7.3.9" (OCSP noCheck); i.e., the OCSP certificate is not validated.
The OCSP responder used fulfils the requirements of RFC 2560.

7.3.1 Version number(s)

Version 1 is supported pursuant to the OCSP specification according to RFC 2560.

7.3.2 OCSP extensions

T-Systems does not offer any OCSP extensions.

8 Compliance audits and other assessments

TeleSec ServerPass Standard and SAN/UCC:
A registration authority that is not installed at T-Systems is regularly checked by T-Systems as part of compliance audits.
Based on this CP/CPS, T-Systems is also entitled to carry out Trust Center-specific compliance audits as required, in order to ensure the trustworthiness of a registration authority. This includes the following:

- Carrying out a compliance audit at a registration authority at any time, at its sole and exclusive discretion, in the event of "imminent danger", if T-Systems has reason to assume that the audited authority has not complied with regulations (especially of this CP/CPS) and/or standards, an incident or compromising situation has occurred at the authority, or the authority carried out or refrained from an act which resulted in the incident, compromising situation or act of the audited authority representing an actual or potential threat to the security of TeleSec ServerPass. This audit must also be carried out if abuse of the PKI service is suspected or T-Systems' image is expected to be harmed.
- T-Systems is entitled to carry out "additional risk management checks" at a registration authority due to incomplete or exceptional results of a compliance audit or as part of the overall risk management process in the context of proper business operations.

The entities that undergo an audit, a check or an investigation, must support T-Systems and/or a contracted third party so that the case under investigation can be resolved as quickly as possible.
Furthermore, T-Systems may be contractually entitled to commission third parties to perform these audits, checks and investigations on its behalf (Section8.2).

TeleSec ServerPass EV:
The T-Systems processes are regularly subjected to routine audits by independent third parties ("WebTrust for Certification Authorities" and WebTrust for Certification Authorities - Extended Validation").
In addition, T-Systems carries out internal audits at regular intervals (see also Section 8.1).

8.1 Interval and reason for audits

TeleSec ServerPass Standard and SAN/UCC:
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.

TeleSec ServerPass EV:
WebTrust audits take place on an annual basis.
Internal audits take place continually, but at least once a year.

8.2 Identity/qualification of the auditor

The Trust Center-specific compliance audits are carried out by qualified employees of T-Systems 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.

8.3 Relationship of the auditor to the entity to be audited

The auditor for the WebTrust certifications is an independent third party (auditing company).
Internal audits are carried out by suitably qualified T-Systems staff.

8.4 Audit areas covered

The scope of the audit is determined by the auditor himself. 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)
- certificate revocations
- access protection
- authorization and role concept
- anti-burglary controls
- Human Resources

TeleSec ServerPass EV:
The audits also cover the points named in [WTEVGUIDE] that require particular attention for the issuance of extended validation certificates.

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 shall decide 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 T-Systems.
T-Systems reserves the right to publish results or partial results if misuse occurred or the image of T-Systems was harmed.

The relevant WebTrust audit reports are published on the website http://cert.webtrust.org.

9 Other business and legal provisions

9.1 Fees

9.1.1 Fees for issuing or renewing certificates

T-Systems is entitled to charge for issuing, renewing and managing end entity certificates. The fees are regulated in the applicable General Terms and Conditions (GT&C) TeleSec ServerPass.

9.1.2 Fees for access to certificates

T-Systems does not charge for access to certificates in the repository of TeleSec ServerPass CA.

9.1.3 Fees for access to revocation or status information

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

9.1.4 Fees for other services

T-Systems 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 **Fehler! Verweisquelle konnte nicht gefunden werden.**, 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 T-Systems.

9.1.5 Reimbursement of fees

T-Systems shall reimburse charges in accordance with the legal regulations under German law. Detailed provisions can be found in the document "General Terms and Conditions" for TeleSec ServerPass.

9.2 Financial responsibilities

Financial responsibilities are determined in the General Terms and Conditions (GT&C) for TeleSec ServerPass.

9.2.1 Insurance cover

The insurance cover is described in the General Terms and Conditions (GT&C) for TeleSec ServerPass. It is guaranteed that the requirements set out in the EV Guidelines regarding insurance cover are fulfilled.

9.2.2 Other financial means

Not applicable.

9.2.3 Insurance cover or guarantees for end entities

Not applicable.

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

T-Systems, 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 Privacy plan

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.
T-Systems shall ensure the technical and organizational security and other controls in accordance with § 9 BDSG [Federal Data Protection Act] and the annex to § 9 BDSG.
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.
The data protection concept can be provided in excerpts 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 provisions.

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

T-Systems reserves all intellectual property rights to certificates, revocation or status information, publicly accessible repositories 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, T-Systems gives its consent for certificates to be reproduced and published on a non-exclusive basis and free of charge.
T-Systems gives its consent for revocation lists and status information to be reproduced and published, especially to relying parties, on a non-exclusive basis and free of charge, provided that the use of revocation or status information and their contents and the origin of this certificate hierarchy are stated in full and not changed [sic].

9.5.2 Property rights of this CP/CPS

This document is copyright protected; all intellectual property rights belong to T-Systems. 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 **Fehler! Verweisquelle konnte nicht gefunden werden.**).

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 distinguished name.

9.5.4 Property rights to keys and key material

The intellectual property rights of the CA's key material remain with T-Systems, 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 T-Systems.

9.6 Assurances and guarantees

9.6.1 Assurances and guarantees of the certification authority

T-Systems commits to the following:

- not to include any essentially false statements in certificates which 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 essential requirements of this document.
- that the revocation functions and the use of the CA repository (directory service, OCSP responder) fulfill all the essential requirements of the applicable CP/CPS.

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 which 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 can be validly used (not expired and not revoked).
- to check that the certificate contents of the subject DN 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 the non-fulfillment of the obligations described in the present CP/CPS.
- in the event of loss or suspected compromising of the secret key, to arrange for/carry out the revocation of the corresponding end entity certificate.
- that the certificate issued is only used for authorized and legal purposes which 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: T-Systems 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 on whether the information provided is reliable and trustworthy.

9.6.5 Assurances and guarantees of other entities

No provisions.

9.7 Exclusion of liability

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

9.8 Limitations of liability

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

9.9 Compensation

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

9.10 Term and Termination

9.10.1 Term

The CP/CPS comes into effect when it is published on the T-Systems websites.
Changes also 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 Amendments to the CP/CPS

In order to respond to changing market requirements, security requirements and legislation, etc., T-Systems 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 T-Systems 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 T-Systems 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 T-Systems 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 exclusively.

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 Different provisions

9.16.1 Complete contract

Not applicable.

9.16.2 Assignment

Not applicable.

9.16.3 Severability

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)

Not applicable.

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 force majeure.

9.17 Other provisions

Not applicable.

10 Other applicable documents and references

10.1 Other applicable documents

Reference/no.	Document name	Last revised/version
[AGB]	General Terms and Conditions TeleSec ServerPass (Allgemeine Geschäftsbedingungen in German)	
[WTEVGUIDE]	Guidelines For The Issuance and Management Of Extended Validation Certificates, The CA / Browser Forum	Version 1.2, October 1, 2009

10.2 References

Reference	Document name
[BDSG]	Federal Data Protection Act (Bundesdatenschutzgesetz), Federal Law Gazette (Bundesgesetzblatt) I 2003 p.66
[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
[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
[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/
[WTEVAUDITGUIDE]	WebTrust for certification authorities – extended validation audit criteria, Version 1.1

11 Glossary

Abbreviation	Description
Authority Revocation List (ARL)	List which contains 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 Policy (CP)	Defines the guidelines for generating and managing certificates of a certain type.
Certificate Revocation List (CRL)	See Revocation List.
Certification Authority	See Certification Authority.
Certification authority	Component that issues digital certificates by digitally signing a dataset consisting of a public key, name and various other data. The certification authority also issues revocation information.
Certification Practice Statement (CPS)	Explanations for operating a certification authority. In particular, the CPS implements the provisions and policies of the CP of a certification authority.
Compromise	A private key is compromised if it is made known to unauthorized persons or can be used by them. A compromise could occur through a criminal attack for example.
Cryptography	Science dealing with the encryption of data and related issues (such as digital signatures).
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.
Distinguished Name	Format with which unique names can be specified according to the X.500 standard. A digital certificate must contain a DN.
Electronic signature	See digital signature.
End entity	See also subscriber. The term end entity is largely used in the X.509 environment.
Hardware Security Module (HSM)	Hardware box 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 an overall digital document.
Key	In cryptography, a key refers to secret information (secret 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.
Latency period	Period of time between an action and the occurrence of a delayed reaction (delay period). With latency periods, the action occurs unnoticed and is only discovered through the reaction.
Lightweight Directory Access Protocol (LDAP)	Protocol for querying directories that has displaced the clearly more complicated Directory Access Protocol (DAP) in many areas. LDAP offers more options than HTTP and FTP (such as setting up a context that can be maintained using several queries). LDAP is used in particular to query digital certificates and revocation lists within public key infrastructures.
Online Certificate Status	The Online Certificate Status Protocol makes it possible to query the validity of

Protocol (OCSP)	certificates online.
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. There is a difference between Certificate Policy (CP) and Certification Practice Statement (CPS).
Public Key Infrastructure	Total sum of the components, processes and concepts that are used for using public key processes. Typically, a public key infrastructure consists of central components such as a certification authority and a repository and different client components.
Public Key Infrastructure X.509 (PKIX)	IETF standard that standardizes all relevant parts of a PKI.
Public Key Service (PKS)	Service of the T-Systems Trust Center for issuing and administrating certificates that comply with the German Digital Signature Act.
Registration Authority	Component with which a person or a system must communicate to obtain a digital certificate.
Registration Authority (RA)	See Registration Authority.
Relying Parties	An individual person or legal entity (e.g., company, organization) which acts in reliance on the functioning of a certificate.
Repository	Database that enables certificates and information about certificates (especially revocation lists) to be called up.
Request	English term for “Auftrag”. Is 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 it used, a revocation list should be checked to see if it may still be used. It is also referred to as Certificate Revocation List (CRL).
Rivest Shamir Adleman (RSA)	Procedure for encryption, for the digital signature and for the secure transmission of keys that is named after the three cryptographs Rivest, Shamir and Adleman.
Root CA	See root certification authority.
Root certification authority	Top-level certification authority in a CA hierarchy whose certificate was thus not issued by another certification authority but signed by the root CA itself. This certificate constitutes the “trusted anchor” within the application.
Secure Multipurpose Internet Mail Extension (S/MIME)	Secure Multipurpose Internet Mail Extension. Extension of the MIME e-mail format which describes additions for cryptographic services that guarantee the authenticity, integrity and confidentiality of messages.
Secure Socket Layer (SSL)	Crypto protocol for ensuring end-to-end connections on the Internet. Can be used instead of the more complex IPSec in many cases.
Signature	See digital signature.
Simple Object Access Protocol (SOAP)	Simple Object Access Protocol: SOAP provides a simple mechanism for exchanging structured information between users in a decentralized, distributed environment.
Smartcard	Chip card with computing function that can be used for cryptographic purposes.
Statement of Auditing Standards (SAS) 70	Statement of Auditing Standards (SAS) No.70 titled “Service Organizations” – this is an internationally recognized standard that was created by AICPA.
Subject Alternative Name	Additional fields in a certificate. The fields can be used to enter additional names of the subscriber and is a standard extension of the X509 standard.
Subject Distinguished Name (Subject DN)	Subject = Person or machine. Format with which unique names can be specified according to the X.500 and the LDAP standard. The subject DN clearly identifies the

	subscriber.
Subscriber	Legal person using a certificate and the corresponding private key.
Suspension	In the context of PKI, suspension means a premature or temporary revocation. The certificate initially appears in the certificate revocation list, but can be re-activated by the sub-registrar.
T-Systems Advisory Board	A board within T-Systems that decides on PKI functions.
Unified Communications Certificates (UCC)	Certificates that allow the Subject Alternative Name fields to be used. This allows several domain names to be covered by one certificate.
Validation	In the context of PKI, the term “validation” is taken to mean checking the validity of certificates. Generally speaking, the period of validity based on the PC system clock, the revocation status (based on a revocation list or OCSP) and the certificate hierarchy (issuing CA) are checked.
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.
X.509	Standard, whose most important element is a format for digital certificates. Certificates of version X.509v3 are supported in all common public key infrastructures.

12 Acronyms

Acronym	Meaning
AICPA	American Institute of Certified Public Accountants
ARL	Authority Revocation List
ASP	Application Service Provider
CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DIN	German Institute for Standardization
DMZ	Demilitarized Zone
DN	Distinguished Name
DNS	Domain Name Systems
FQDN	Fully Qualified Domain Name
GR	Stands for Groups, function, Role certificate
GT&C	General Terms and Conditions
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IPSec	Internet Protocol Security
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PN	Stands for pseudonym
PSE	Personal Security Environment
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest Shamir Adleman
S/MIME	Secure Multipurpose Internet Mail Extension
SAS	Statement of Auditing Standards
SigG	German Digital Signature Act [Signaturgesetz]
SigV	Signature assignment [Signaturverordnung]
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TLS	Transport Layer Security
UPN	User Principal Name
URL	Uniform Resource Locator

UTC	Universal Time Coordinated
XML	Extensible Markup Language