CERTIFICATION PRACTICE STATEMENT (CPS)

TELESEC SHARED BUSINESS CA

DEUTSCHE TELEKOM SECURITY GMBH

VERSION:	14.00
VALID FROM:	MAY 15, 2021
STATUS:	RELEASE
CLASSIFICATION:	PUBLIC
LAST REVIEW:	MAY 10, 2021

PUBLICATION DETAILS

PUBLISHED BY

DEUTSCHE TELEKOM SECURITY GMBH
Bonner Talweg 100
53113 Bonn

Phone: +49 228 181-0
E-mail: info@telekom.de
Internet: www.telekom.de/security
Compulsory Statement: www.telekom.com/compulsory-statement-dtsec

Supervisory Board: N.N (chairman)
Management Board: Thomas Fetten (Spokesman), Dr. Klaus Schmitz, Thomas Tschersich

Trade Register: District Court Bonn HRB 15241
Registered Office Bonn
Tax Iditification Number DE 254595345
WEEE-Register Number DE 56768674

Brief summery:	This document describes the Certification Practice Statement (CPS) of PKI Service TeleSec Shared Business CA.
File name:	Shared-Business-CA_CPS_14.00_EN.docx
Document number:	n.n.
Document title:	Certification Practice Statement (CPS) of PKI Service TeleSec Shared Business CA.
Version:	14.00
Valid from:	May 15, 2021
Status:	release
Classification:	Public
Last review:	May 10, 2021
Author:	Telekom Security
Contents reviewed by:	Telekom Security
Approved by:	Telekom Security, Head of TC Products, Netphen, May 12, 2021
Contact:	tc-solutions.lastlevel@t-systems.com

CHANGE HISTORY

VERSION:	LAST REVISED:	EDITED BY:	CHANGES / COMMENTS:
1.0	April 6, 2010	UV	Final coordination
1.1	July 1, 2012	CD, UV	Requirements from Version 1.0 of the CA/Browser Forum baseline requirements incorporated
01.20	March 27, 2013	UV	Complete revision
01.21	July 2, 2013	UV	Incorporation of changes by Lothar Eickholt
02.00	July 18, 2013	AT	Release of this version
02.10	April 7, 2014	UV	Revision of sections 1.1.1, 1.2, 1.3.1.1, 1.3.1.2, 2.2, 3.1.1, 3.1.1.2 to 3.1.1.14, 3.2.2, 3.2.5.1, 3.2.5.2, 4.5.1, 4.6.1, 4.9.1, 5.5.2, 7.1.2.9, 7.1.3, 7.1.6.2, 7.2, 7.3, 9.2, 9.9, 9.16.5, A.1, A.2, C.1, removal of section 1.3.1.3, insertion of new section 3.1.1.15
02.20	April 4, 2014	LE	Quality assurance for vers. 02.10 and release of this version
02.30	April 22, 2016	UV	Complete revision
02.31	May 19, 2016	VM, MS, UV	Quality assurance for vers. 02.30
03.00	May 20, 2016	ME	Release of this version
03.10	April 21, 2017	UV	Revision
03.20	May 9, 2017	LE	Quality assurance, Section 3.1.1.1, 3.1.1.1.1, 3.1.1.1.8, 3.1.1.1.9, 4.1.2.2.2 and 4.9.1
04.00	June 19, 2017	AJ	Release of this version
04.10	June 19, 2018	UV	Revision of Section 1, 1.3.1.1.1, 1.3.1.1.2, 1.3.1.2.1, 1.3.1.2.2, 1.5.3, 1.5.4, 2.2, 2.3, 3.1.1, 3.1.1.1, 3.1.1.1.1, 3.1.1.1.6, 3.1.1.1.8, 3.1.1.1.9, 3.1.1.1.12, 3.1.3, 3.1.6, 3.2.2.1, 3.2.3.1, 3.2.3.2, 3.2.5.3, 3.3, 4.1.1, 4.1.2.2.2, 4.2.1.2, 4.2.2, 4.2.2.1.1, 4.2.2.1.2, 4.2.2.2, 4.3.1.1, 4.3.1.2, 4.4.2, 4.6.1, 4.6.2, 4.7, 4.7.1, 4.7.3, 4.9.1.1, 4.9.1.2, 4.9.2, 4.9.3.1, 4.9.3.2.1, 4.9.3.3.2, 4.9.3.5, 4.10.1, 5, 5.1.1, 5.2, 5.3.3.1, 5.4.2, 5.4.3, 5.4.4, 5.4.5, 5.4.8, 5.5.1, 5.5.2, 5.6, 5.8.2, 6.3.2, 6.5, 7.1, 7.1.11, 7.3, 7.3.1, 8, 8.4, 8.6, 9.4.1, 9.7, 9.8.1, 9.8.2, 9.9, C.1, C.2, Addition of Section 3.2.2.2 ff, 4.4.4, 7.1.2.9.1, 7.1.2.9.2 Replacement of picture 2
05.00	July 3, 2018	UV	Release of this version
05.10	July 24, 2018	UV	Revision of Section 1.2, 1.3.1, 1.3.1.3.1, 1.5.1, 1.5.4, 2.1, 2.2, 2.4, 3.1.1.1.6, 3.2.2.1, 3.2.2.2.1, 3.2.2.2.4.2, 3.2.2.2.4.3, 3.2.2.2.4.7, 3.2.2.2.6, 3.2.5.2, 4.1.2.1, 4.1.2.2.1, 4.1.2.2.2, 4.2, 4.2.2.1.1, 4.3, 4.9.1.1, 4.9.1.1, 4.9.7, 4.10.1, 5, 5.2, 5.3.4.1, 5.4, 5.4.8, 5.7.1, 5.8.1, 6, 6.2.1, 6.5, 6.5.1.1, 6.6.1, 6.6.3, 6.7, 7.1.3, 7.2, 7.3.2, 8, 9.4.1, C.1, C.2, References
05.20	July 27, 2018 August 15, 2018	LE UV	Quality assurance of Vers. 05.10 Submission to TÜV
05.30	October 10, 2018	LE	Acceptance of changes,

VERSION:	LAST REVISED:	EDITED BY:	CHANGES / COMMENTS:
			Addition of test certificates Update of Section 1.5.2 Change of „27 months“ into „825 days” in sections 3.2.2.1, 3.2.5.2, 3.3, 4.2.2.1.1, and 6.3.2 Update of Section 3.2.5.3 Update of internet address in Section 3.4, Updates in chapter 4.1.1, 4.9.3 and 4.9.5,New Section 9.17.1
05.31	October 10, 2018	GK	QS
06.00	October 10, 2018	DD	Release of version 06.00
06.10 to 06.60	May 23, 2019	UV, LE, AJ	Revision of Sections 1.2, 1.3.1.1.1, 1.3.1.1.2, 1.3.1.2.1, 1.3.1.2.2, 1.3.2.2, 1.3.2.2.2, 1.5.1, 1.5.2, 2.1, 2.2, 3.1.1.1, 3.1.1.1.6, 3.1.1.1.9, 3.1.1.1.10, 3.1.1.1.11, 3.1.1.1.12, 3.1.1.2, 3.1.1.2.3, 3.1.1.2.3, 3.1.6, 3.2.2.1, 3.2.2.2, 3.2.2.2.4.3, 3.2.2.2.4.5, 3.2.2.2.4.6, 3.2.2.2.4.7, 3.2.2.2.5, 3.2.2.2.5.1, 3.2.2.2.5.2, 3.2.2.2.5.3, 3.2.2.2.5.4, 3.2.2.2.5.5, 3.2.2.2.5.6, 3.2.2.2.5.7, 3.2.3.3, 3.2.5.1, 3.2.5.3, 4.2.1.1, 4.4.2, 4.9.1.1, 4.9.3.2, 4.9.7, 4.12, 5.1.1, 5.5.1, 5.5.2, 5.5.3, 5.7.4, 5.8.1, 6.1.1, 6.1.2, 6.1.6, 6.2, 6.2.4, 6.2.4.3, 6.2.5,, 6.2.6, 6.2.7, 6.2.8.3, 6.2.8.3, 6.2.8.4, 6.2.9, 6.5, 6.5.1.1, 7.1, 7.1.2.9.1, 7.1.2.9.2, 7.1.3, 7.1.4.1, 7.1.4.2, 7.1.4.3, 7.1.6.2, 7.1.6.3, 7.1.6.4, 7.2, 8.7, 9.6.4, 9.7
06.61	May 27,2019	GK	QS
07.00	May 27, 2019	ME	Release of version 07.00
07.10	August 21, 2019	UV, AJ	All entries deleted regarding Shared Business CA3, Shared Business CA 4 and Deutsche Telekom Root CA 2 (Sections 1.1.2, 1.3.1.1.1, 1.3.1.2.1, 1.3.3, 1.3.5, 1.5.4, 2.2, 3.1.1.1.5, 3.2.3.4, 3.2.4, 4.1.1, 4.2.1.2, 4.2.2.1.1, 4.2.2.2, 4.5.1, 4.9.7, 6.1.4, 6.3.2, 7.1.2.4, 7.1.2.9.1, 7.1.6.1, 8.1, 8.4, 9.6.3 and references) Addition Sub-CA Internal Business CA 5 (Section 1.3.1.2.2, 2.2, 6.3.2, 7.1.2.4), Definitions of terms
07.20	August 21,2019	GK	QS
08.00	August 23, 2019	ME	Release of version 08.00
08.10	February 5, 2020	UV	Revision of Section 1.1.1, 2.2, 3.1.1.1.1 bis 3.1.1.1.9, 3.2.2.2.4.1, 3.2.2.2.4.6, 3.2.2.2.4.12 bis 3.2.2.2.4.19, 3.2.2.2.5 ff, 4.1, 4.1.2.2.2, 4.2, 4.2.1.2, 4.4.4, 4.5.1, 4.9.1.1, 4.9.6, 4.9.9, 4.9.10, 4.9.14 bis 4.9.16, 4.10.1, 4.11, 5.2.1, 5.3.6.1, 5.4, 5.5.2, 5.8.2, 6.1.5, 6.1.6, 7.1.3, 7.1.4.3, 7.1.6.3.1 bis 7.1.6.3.3, 7.3.2, 9.6.1, C.2, References, Revision of all tables
08.20	February 5, 2020	UV	Harmonisation version
08.30	March 16, 2020	UV	Addition of harmonisation version of section 2.3, 3.1.1.1.6, 3.1.1.1.7, 3.1.1.1.13, 3.1.1.2, 3.2.3 (headline), 3.2.5 (headline), 3.2.5.3, 3.2.6, 4.2, 4.2.2.1.2, 4.2.2.2, 4.3 (headline), 4.9.1.1, 4.9.3 (headline), 4.10.1, 6.2.5, 6.3, 7.1, 7.1.2.1, 7.1.2.3, 7.1.2.5, 7.1.2.9.1, 7.1.4.2, 7.1.5, 7.1.6.3.2, 8, 8.1, 8.3, 8.4, 8.6, 8.7, 9.12.1

VERSION:	LAST REVISED:	EDITED BY:	CHANGES / COMMENTS:
08.40	March 20, 2020	AJ	Revision of Section 1.3.1.1.1, 1.3.1.1.2, 1.3.1.2.1, 1.3.1.2.2, 1.3.3, 3.1.1, 3.1.1.1.2, 3.1.1.1.6, 3.1.1.1.13, 3.1.3, 5.2.1
08.50	March 23, 2020	UV	Finalisation
08.90	March 23, 2020	GK	QS
09.00	March 23, 2020	HH	Release of version 09.00
09.10	May 28.05.2020	UV	Organizational change to Deutsche Telekom Security GmbH
09.20	May 29, 2020	UV	Finalisation
09.30	May 29, 2020	GK	QS
10.00	June 03 2020	HH	Release of version 10.00
10.10	June 9, 2020	UV	Change of short name Telekom Security
10.20	June 16, 2020	UV	Revision of Section 1.1.1, 1.1.2, 1.3.1, 1.3.1.3.2, 1.3.2.2.1, 1.3.2.2.2, 1.3.4, 2.1, 3.2.2.1, 3.3, 4.1.2.2.1, 4.1.2.2.2, 4.2.1.1, 4.9.1.2, 4.9.3.2, 4.9.3.2.2, 5.4.1.3, 5.5.1, 5.5.2, 5.5.5, 6.1.1, 6.3.2, 6.2.4, 6.2.4.2, 6.2.4.3, 6.2.5, 6.4.2.2, 6.5.2, 7.1.2.9.2, 8.7, Annex A, Annex B
10.90	August 31, 2020	Telekom Security	Formal QS
11.00	August 31, 2020	Telekom Security	Release of version 11.00
11.20	March 02, 2021	Telekom Security	Dividing CP/CPS, e.g. new section 1.1.3
11.90	March 02, 2021	Telekom Security	Formal QS
12.00	March 02, 2021	Telekom Security	Release of version 12.00
12.10	April 14, 2021	Telekom Security	Revision of Section 5.7.1 und 6.5.2
12.20	April 28, 2021	Telekom Security	Revision of Section 4.9.12
12.90	April 29, 2021	Telekom Security	Formal QS
13.00	April 29, 2021	Telekom Security	Release odf Version 13.00
13.90	May 10, 2021	Telekom Security	Revision of Section 3.2.2.2
13.91	May 11, 2021	Telekom Security	Formal QS
14.00	May 12, 2021	Telekom Security	Release of Version 14.00

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

The Trust Center is operated by the Group unit Deutsche Telekom Security GmbH (hereinafter referred to as “Telekom Security”), which emerged after a transfer of operations from T-Systems International GmbH on July 1, 2020.

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.

In 2013, an information security management system (ISMS) was established for the Trust Center of Telekom Security. The ISMS provides procedures and rules to allow information security to be controlled in a targeted manner, monitored, checked, permanently improved and maintained.

1.1 Overview

1.1.1 The TeleSec Shared Business CA PKI service

TeleSec Shared Business CA (also referred to as “SBCA” in the following) is a central PKI service, operated in the Trust Center of Telekom Security, for generating and managing various X-509v3 certificate types that are used for e-mail security, strong authentication (client server), remote VPN, servers and active network components (e.g., routers, gateways), in particular.

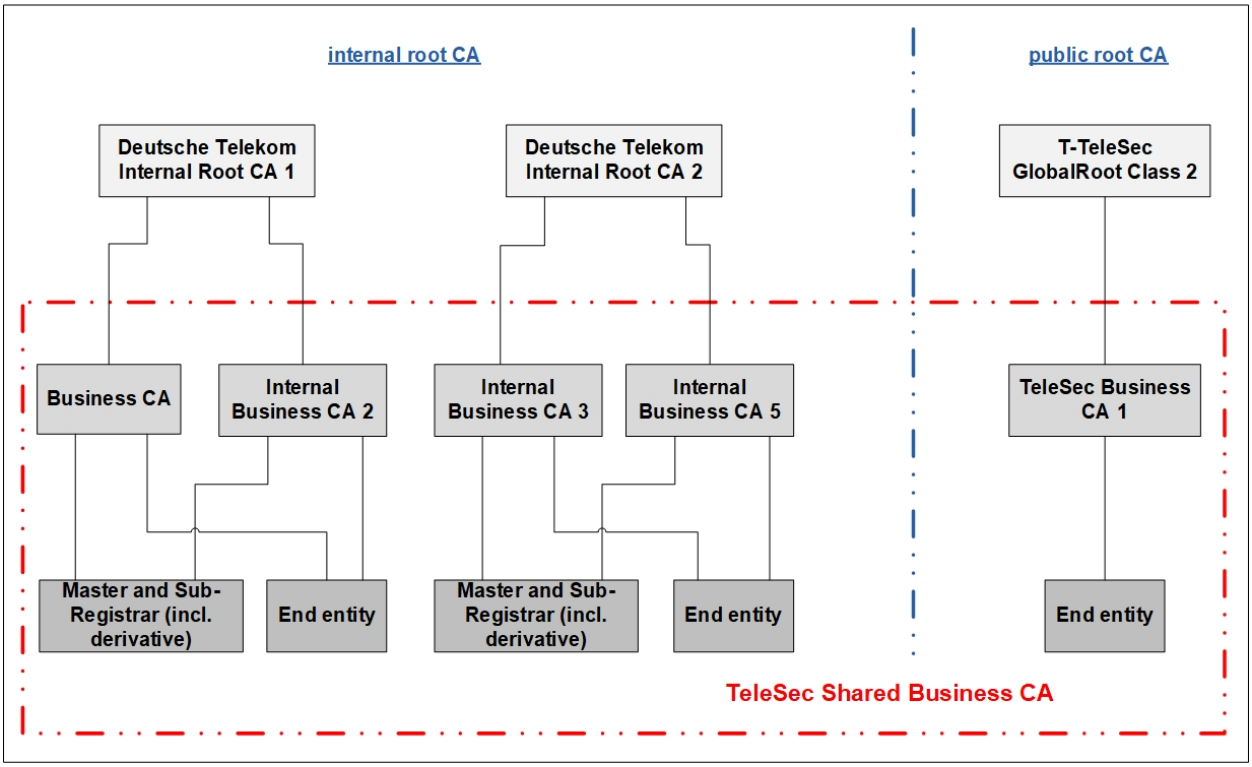
With TeleSec Shared Business CA (SBCA), Telekom Security provides customers with a complete PKI solution with an infrastructure that is installed in the highly secure Trust Center of Telekom Security and operated by qualified personnel. To ensure secure delimitation and management of their own data inventory, each customer– also referred to as “tenant” in the following– receives a master domain that is set up specifically for him. To map the organizational structure, the customer can arrange the master domain into individual, independent areas of responsibility within which he can independently request and manage certificates for end entities (users, devices).

All customers receive dedicated access (secured by means of a certificate-based SSL/TSL client authentication) to their own PKI tenant (master domain) so that they can use the PKI functions. All security-relevant actions are performed via an encrypted connection (HTTPS).

Various Intermediate CAs (also known as sub-CAs) are subsumed under the TeleSec Shared Business CA PKI service itself, which are also hierarchically subordinate to various root certification authorities.

TeleSec Shared Business CA shows an overview of the “TeleSec Shared Business CA” PKI service with all its root and intermediate-CAs respectively sub-CAs in a diagram. The scope of this document includes the intermediate certification authorities (sub-CAs) of this figure contained in the red dashed area.

Figure 1: Overview of the “TeleSec Shared Business CA” PKI service with the corresponding root- and intermediate-CAs respectively sub-CAs.



There are separate Certificate Policies (CP) and Certification Practice Statements (CPS) for each of the roots.

The Telekom Security Certification Practice Statement (CPS) of the TeleSec Shared Business CA (SBCA) service, referred to for short as “CPS” in the following, includes security specifications and guidelines regarding technical and organizational aspects and describes the activities of the Trust Center operator in the roles of Certification Authority (CA) and Registration Authority (RA) as well as the Registration Authority’s (RA) delegated third party.

The CPS covers the following regulations in detail:

- Publications and directory service
- Authentication of PKI subscribers
- Issue of certificates
- Renewal of certificates (re-certification)
- Revocation and suspension of certificates
- Structural and organizational security measures
- Technical security measures
- Certificate profiles
- Auditing
- Binding information regarding using and checking certificates
- Various general conditions.

The formal structure of this CPS follows international standard RFC3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” [RFC3647] of the Internet Society.

Legal and commercial aspects of the TeleSec Shared Business CA are contractually regulated.

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

The Trust Center of Telekom Security ensures that the “T-Telesec GlobalRoot Class 2” root CAs with the corresponding intermediate-CAs meet and comply with the requirements and regulations of the respective currently published version of the [CAB-BR] (https://cabforum.org/baseline-requirements/).

In the event that this document and the [CAB-BR] contradict one another, the regulations from the [CAB-BR] have priority.

1.1.3 Compliance with the overarching certification guidelines of the Trust Center

The Trust Center guarantees that for TeleSec Shared-Business-CA the requirements of the overarching certification guidelines of the Trust Center of Telekom Security [Trust Center CP] with OID 1.3.6.1.4.1.7879.13.42 are implemented or complied with. The [Trust Center CP] is published on the Internet at https://www.telesec.de/de/service/downloads/pki-repository/.

In case of a contradiction between this document and the [Trust Center CP], the provisions of the [Trust Center CP] take precedence.

1.2 Document name and ID

This document represents the CP / CPS of the PKI service TeleSec Shared Business CA of Telekom Security.

Name:	Certification Practice Statement (CPS)
Version:	14.00
Valid from:	May 15, 2021
Last revision:	May 10, 2021
OID of this CPS:	1.3.6.1.4.1.7879.13.25

The use of further object identifiers (OID) is described in section 7.1.6.

1.3 Parties 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. The intermediate certification authority or other intermediate certification authorities, in turn, are hierarchically subordinate to a root certification authority (root CA), which represents the “trust anchor” (root CA certificate).

Various root certification authorities and intermediate certification authorities (root CAs and sub-CAs) are available to the TeleSec Shared Business CA, depending on the requirement. Requirements for the root CAs as well as the intermediate-CA certificates issued by the Root CA are documented in the CP/CPS of the respective root CA.

Intermediate certification authorities that no longer productively issue end-user certificates are still used for signing revocation lists and/or OCSP responses.

The root certification authority and the corresponding intermediate certification authority may vary

- if the certificate from the root certification authority is not yet implemented as trustworthy in the application used (e.g., web browser), or
- if the application used (e.g. web browser) follows a validation logic that does not check for the direct root certification authority.

In such cases, reference is optionally made to another defined root certification authority.

The validation model is based on the shell model, that is, each certificate is valid at the maximum for as long as the issuing certificate above it.

1.3.1.1 Root certification authority

1.3.1.1.1 Public certification authorities

Regulations regarding public certification authorities are documented in the “T-TeleSec GlobalRoot Class 2” [CP/CPS Class2] CP and CPS.

Table 1 shows the complete Issuer and Subject Distinguished Names (Issuer DN, Subject DN) of the named certification authority according to the name forms according to Section 3.1.1 ff, as well as their certificate validity.

Table 1: Subject DN “T-TeleSec GlobalRoot Class 2”

Issuer	
Country Name (C):	DE
Organization Name (O)	T-Systems Enterprise Services GmbH
Organizational Unit Name (OU):	T-Systems Trust Center
Common Name (CN):	T-TeleSec GlobalRoot Class 2
Subject	
Country Name (C):	DE
Organization Name (O):	T-Systems Enterprise Services GmbH
Organizational Unit Name (OU):	T-Systems Trust Center
Common Name (CN):	T-TeleSec GlobalRoot Class 2
Signature hash algorithm:	SHA-256
Valid from:	01-Oct-08
Valid until:	01-Oct-33
Fingerprint algorithm:	SHA-256
Fingerprint:	91 E2 F5 78 8D 58 10 EB A7 BA 58 73 7D E1 54 8A 8E CA CD 01 45 98 BC 0B 14 3E 04 1B 17 05 25 52
Fingerprint algorithm:	SHA-1
Fingerprint:	59 0d 2d 7d 88 4f 40 2e 61 7e a5 62 32 17 65 cf 17 d8 94 e9

1.3.1.1.2 Internal root certification authorities

Regulations regarding the internal root certification authorities are documented in the “Deutsche Telekom Internal Root CA 1” [CP/CPS DTIRCA1] and “Deutsche Telekom Internal Root CA 2” [CP/CPS DTIRCA2] CP/CPS.

Table 2 and Table 3 shows the complete Issuer and Subject Distinguished Names (Issuer DN, Subject DN) of the named certification authority according to the name forms according to Section 3.1.1 ff, as well as their certificate validity.

Table 2: Subject DN “Deutsche Telekom Internal Root CA 1”

Issuer	
Country Name (C):	DE
Organization Name (O)	Deutsche Telekom AG
Organizational Unit Name (OU):	Trust Center

Common Name (CN):	Deutsche Telekom Internal Root CA 1
Subject	
Country Name (C):	DE
Organization Name (O)	Deutsche Telekom AG
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Deutsche Telekom Internal Root CA 1
Signature hash algorithm:	SHA-1
Valid from:	15-Nov-07
Valid until:	15-Nov-27
Fingerprint algorithm:	SHA-256
Fingerprint:	E0 1A B4 F7 CE 75 0F F4 3B FE 52 13 78 79 FE 11 A0 83 66 CE 9C C5 40 75 1A 33 38 A4 9F BB 7B D4
Fingerprint algorithm:	SHA-1
Fingerprint:	15 33 9a a2 30 f5 34 0e 7b fc aa fd 75 4a a1 4c ed d4 98 58

Table 3: Subject DN „Deutsche Telekom Internal Root CA 2“

Issuer	
Country Name (C):	DE
Organization Name (O)	T-Systems International GmbH
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Deutsche Telekom Internal Root CA 2
Subject	
Country Name (C):	DE
Organization Name (O)	T-Systems International GmbH
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Deutsche Telekom Internal Root CA 2
Signature hash algorithm:	SHA-256
Valid from:	03-Aug-2017
Valid until:	03-Aug-2037
Fingerprint algorithm:	SHA-256
Fingerprint:	C3 2A E6 04 47 39 1E 48 63 C2 44 55 1D EB C8 7B 40 FF 51 80 45 19 3E E4 67 33 86 57 9D 50 D0 FD
Fingerprint algorithm:	SHA-1
Fingerprint:	12 f7 14 bd ec 4d 2e 3c 27 82 ce 1f cb 8a fe 19 b8 4a ed 8c

1.3.1.2 Intermediate certification authorities

1.3.1.2.1 Certification authorities below a public root certification authority

End entity certificates (e.g., for users or servers) for which the intended use requires a public root are issued by the following subordinate certification authorities (intermediate certification authorities):

- TeleSec Business CA 1

In the event that the intended use of certificates does not meet the specifications of a “public root certification authority” (e.g., regarding administering the PKI tenants, routers and domain controllers) or specifications or provisions (e.g., root programs of the operating system and browser manufacturers, baseline requirements of the CA/Browser Forum [CAB-BR]) restrict or prevent this intended purpose, these certificates will be issued by an intermediate certification authority that is hierarchically subordinate to the “Deutsche Telekom Internal Root CA 1” or “Deutsche Telekom Internal Root CA 2”.

The common name (CN) of the issuer refers to the responsible root certification authority.

Table 4 shows the complete Issuer and Subject Distinguished Names (Issuer DN, Subject DN) of the named certification authority according to the name forms according to Section 3.1.1 ff, as well as their certificate validity.

Table 4: Issuer and subject DNs “TeleSec Business CA 1”

Issuer	
Country Name (C):	DE
Organization Name (O)	T-Systems Enterprise Services GmbH
Organizational Unit Name (OU):	T-Systems Trust Center
Common Name (CN):	T-TeleSec GlobalRoot Class 2
Subject	
Country Name (C):	DE
Organization Name (O)	T-Systems International GmbH
Organizational Unit Name (OU):	T-Systems Trust Center
Common Name (CN):	TeleSec Business CA 1
Signature hash algorithm:	SHA-256
Valid from:	November 29, 2012
Valid until:	November 29, 2024
Fingerprint algorithm:	SHA-256
Fingerprint:	44 EB F0 12 3E 27 FF 1D B0 49 7B D2 DA E1 81 55 B2 A4 14 E6 BC D9 C6 C8 FB 8F 48 39 84 49 B9 E9
Fingerprint algorithm:	SHA-1
Fingerprint:	57 a8 c5 b5 26 0e 20 63 53 d4 c3 46 e3 f6 09 39 e4 f8 b8 59

1.3.1.2.2 Certification authority below an internal root certification authority

End entity certificates (e.g., for registrars, users (SmartCard logon), routers/gateways, domain controllers) that fulfil the conditions for use of an “internal root certification authority (internal root)” are issued by the following subordinate certification authorities (intermediate certification authorities):

- Internal Business CA 3
- Internal Business CA 5
- Internal Business CA 2
- Business CA

The common name (CN) of the issuer refers to the responsible root certification authority.

Table 5 to Table 8 shows the complete Issuer and Subject Distinguished Names (Issuer DN, Subject DN) of the named certification authority according to the name forms according to Section 3.1.1 ff, as well as their certificate validity.

Table 5: Issuer and subject DNs “Internal Business CA 2”

Issuer	
Country Name (C):	DE
Organization Name (O)	Deutsche Telekom AG
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Deutsche Telekom Internal Root CA 1
Subject	
Country Name (C):	DE
Organization Name (O)	T-Systems International GmbH
Organizational Unit Name (OU):	T-Systems Trust Center
State (S):	Nordrhein Westfalen
PostalCode:	57250
Locality (L):	Netphen
Street:	Untere Industriestr. 20
Common Name (CN):	Internal Business CA 2
Signature hash algorithm:	SHA-256
Valid from:	11-Feb-14
Valid until:	15-Nov-27
Fingerprint algorithm:	SHA-256
Fingerprint:	F1 50 C0 1B 68 79 11 62 59 01 F1 1E 71 AD D8 EB DE 58 10 D8 3E 92 F4 96 F8 B5 0E 24 82 6A 65 B5
Fingerprint algorithm:	SHA-1
Fingerprint:	68 19 96 1d d2 59 10 16 b7 ec e0 c6 6f 2b 04 78 08 7f 11 44

Table 6: Issuer and subject DNs “Business CA”

Issuer	
Country Name (C):	DE
Organization Name (O)	Deutsche Telekom AG
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Deutsche Telekom Internal Root CA 1
Subject	
Country Name (C):	DE
Organization Name (O)	T-Systems International GmbH
Organizational Unit Name (OU):	T-Systems Trust Center
Common Name (CN):	Business CA
Signature hash algorithm:	SHA-1
Valid from:	08-Nov-11
Valid until:	08-Nov-23
Fingerprint algorithm:	SHA-256
Fingerprint:	DD 9B C2 05 FC 9C 72 0D C9 C5 2E 62 59 34 E6 6F 56 10 41 68 01 78 6F F2 9A C1 9B 68 DE 7F 77 54
Fingerprint algorithm:	SHA-1
Fingerprint:	8b 52 1b 55 f0 be 1c 79 50 ca a5 d4 af 37 06 a2 60 b6 35 50

Table 7: Issuer and subject DNs “Internal Business CA 3”

Issuer	
Country Name (C):	DE
Organization Name (O)	T-Systems International GmbH
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Deutsche Telekom Internal Root CA 2
Subject	
Country Name (C):	DE
Organization Name (O)	T-Systems International GmbH
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Internal Business CA 3
Signature hash algorithm:	SHA-256
Valid from:	03-Aug-2017
Valid until:	03-Aug-2029
Fingerprint algorithm:	SHA-256
Fingerprint:	6F 32 57 FE 69 12 70 37 65 DE 86 59 F1 37 51 6B 53 99 A3 8A 72 93 7D 1C AB 94 1D DC 4B EC 9C 85
Fingerprint algorithm:	SHA-1
Fingerprint:	ee fa 12 59 ca d4 93 a3 c8 04 a3 2f ac 18 59 b4 31 0c e5 18

Table 8: Issuer and subject DNs “Internal Business CA 5”

Issuer	
Country Name (C):	DE
Organization Name (O)	T-Systems International GmbH
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Deutsche Telekom Internal Root CA 2
Subject	
Country Name (C):	DE
Organization Name (O)	T-Systems International GmbH
Organizational Unit Name (OU):	Trust Center
Common Name (CN):	Internal Business CA 5
Signature hash algorithm:	SHA-256
Valid from:	10-Sep-2019
Valid until:	10-Sep-2031
Fingerprint algorithm:	SHA-256
Fingerprint:	81 13 F5 8B 3C 55 4B D4 18 88 87 54 11 6C 79 1D 6F D0 4A B6 B0 81 57 63 FB 4A 0C 45 E9 2F DB CB
Fingerprint algorithm:	SHA-1
Fingerprint:	cc 78 ef 3c 34 89 38 df 05 7b 1d 1f 4f 9a b6 7e ae 3c b1 68

1.3.1.3 Certificates to support PKI operation

1.3.1.3.1 Web server of the „TeleSec Shared Business CA" PKI service

The tenant accesses the PKI functions of the SBCA via the Internet. The SBCA web server has an SSL certificate, meaning that all actions are executed via the secure HTTPS protocol. The functions are provided following successful role-based authentication.

Figure 2 presents the certificate hierarchy of the "sbca.telesec.de" web server with the corresponding certificate from the root certification authority (root CA) and the intermediate certification authority (subordinate certification authority, sub CA).

Figure 2: Overview of the "sbca.telesec.de" web server's certificate hierarchy

1.3.1.3.2 OCSP responder of the „TeleSec Shared Business CA" PKI service

Every intermediate-CA issues certificates for the OCSP responder so that the OCSP service can be performed. This certificate type is available exclusively to the PKI operator Telekom Security.

For technical details regarding the OCSP, see Section 7.3 ff.

1.3.2 Registration authorities

A registration authority (RA) is an authority that performs authentication for certificate requesters, processes certificate applications (approves, rejects, defers), processes or forwards revocation applications and, if required, creates certificate renewals and a backup copy of the key material (soft PSE) for an applicant.

Generally, every registration authority must guarantee that no unauthorized parties acquire a relevant certificate.

The following registration authorities have been established as part of the TeleSec Shared Business CA PKI service:

- Internal Telekom Security registration authority
- External registration authority (or authorities) operated at the tenant's premises

1.3.2.1 Internal registration authority

The trusted role of the Trust Center operator, located in the Trust Center of Telekom Security, performs the task of internal registration authority. There are no other internal registration authorities.

The internal registration authority performs the following tasks, in particular:

- Receiving orders and checking the identification documents for setting up (configuring) the master domain(s) or PKI tenants
- Setting up the master domain(s) and issuing master registrar certificates on a smartcard for administration of the tenant
- Configuring and modifying configurations of the master domain(s) following a successful check of the identification documents

- Issuing further master registrar certificates on a smartcard
- Revoking master registrar certificates

The internal registration authority can also revoke master registrar, sub-registrar and end-entity certificates across master domains if the tenant has requested this or improper use is suspected or proved.

This registration authority thus takes on higher level functions and is responsible for approving and revoking subordinate registration authorities located at the tenant's premises.

1.3.2.2 External registration authority

The trusted roles of the master registrar and sub-registrar perform the task of the external registration authority that is located at the tenant's premises or those of a third-party authorized by the tenant. There are no other external registration authorities.

The external registration authority performs the following tasks, in particular:

- Receiving certificate requests within the defined area of responsibility
- Checking the applications in accordance with the specified guidelines (e.g., work instructions)
- Requesting the certificate(s) following approval of the certificate request
- Approving these certificate requests following a successful check; otherwise rejecting or deferring (resubmitting) the application
- Receiving the certificate(s) generated by the SBCA and transferring them to the certificate owner or an authorized person
- Receiving and checking certificate revocation orders within the defined area of responsibility or, if appropriate, forwarding these to the internal registration authority or service desk
- Revoking certificates following a positive check of a revocation order
- Generating a new and therefore up-to-date certificate revocation list (CRL).

The external registration authority (external RA), also referred to as the "delegated third party", is operationally and contractually assigned to the Trust Center operation and is subject to the regulations of this CPS. It is irrelevant whether the registration authority issues certificates for its own company/corporate Group only (enterprise RA) or for third parties as well.

1.3.2.2.1 Master registrar

The master registrar is the highest hierarchical role of an external registration authority and is the tenant's responsibility. The administration function is available via the master registrar website. Telekom Security issues master registrar certificates on a smartcard only (see Section 1.3.2.1).

The master registrar performs the following tasks, in particular:

- Representing the tenant vis-à-vis the registration authority
- Setting up, configuring and managing areas of responsibility (sub-domains)
- Issuing of sub-registrar certificates for people the tenant specifies
- Revoking sub-registrar certificates if there is a reason for revocation/revocation order
- Revoking end entity certificates if there is a reason for revocation/revocation order.

The tenant is fully responsible for the external registration authority. The user uses the master registrar certificate as authorization for the master registrar website. The regulations in Section 4.5.1 also apply.

1.3.2.2.2 Sub-registrar

The sub-registrar is the lowest hierarchical role of an external registration authority, as well as the operational role, and is the tenant's responsibility. The functions (e.g. issuing, approving, revoking and renewing certificates) are available following successful certificate-based SSL/TLS client authentication on the sub-registrar website. The master registrar provided the sub-registrar certificate on a smartcard or as a soft PSE (see Sections 1.3.2.2.1, 6.1.1, 6.4.2.2).

The sub-registrar performs the following tasks, in particular:

- Authenticating requesters
- Approving, rejecting or deferring certificate applications following a successful identity check (see also Decentral registration, Section 3.2.3)
- Applying for and calling up end entity certificates following a successful identity check (see also Central registration, Section 3.2.3)
- Revoking end entity certificates if there is a reason for revocation/revocation order.

The sub-registrar (incl. derivatives) that the master registrar issues includes a unique name for the SBCA (common name).

The tenant is fully responsible for this registration authority. The tenant uses the sub-registrar certificate as authorization for the sub-registrar website. The regulations in Section 4.5.1 also apply.

As a further optional function, an interface is available that is based on the CMP protocol (Certificate Management Protocol) and supports certificate management of X.509 certificates within a public key infrastructure (PKI).

With regard to the TeleSec Shared Business CA, the certification authority (CA) provides a server-based interface that can be reached by an application (client) at the tenant's (external registration authority's (RA)) premises in order to apply for, revoke and renew certificates (for further details, see the „TeleSec Shared Business CA service description" document).

To interact via the CMP interface, the tenant's "CMP client" has to log in via a certificate-based SSL/LTS client authentication.

The following derivative of the sub-registrar is available for this purpose:

- Sub-RA-CMP

There is an option to separate the roles for this certificate derivative. If this role separation is activated, no other roles (Sub-RA, Sub-RA-PWD, Sub-RA-P12) can be assigned to the CMP role. If this role separation is deactivated, the CMP certificate can also be used as a sub-RA certificate.

In the following sections, these roles and certificate types are also referred to as "derivatives" of the sub-registrars.

1.3.3 End entity

In the context of the TeleSec Shared Business CA, end entities are understood to be all certificate users to which a certificate can be issued that do not themselves represent a role of a certification authority. Specifically, these are:

- User certificates
    - Natural persons

    - Pseudonym
    - Legal persons
    - People, function groups and roles
    - Robots and automata
- Device certifcates
    - Server
    - Router
    - Gateways
    - Mail-Gateways
    - Domain-Controller

To meet the technical requirements, SBCA provides various different certificates for the end entities. Table 9 to Table 15 shows the assignment of the types to the various end entities.

Table 9: Assignment of certificate type User to end entities

Type of certificate:	User
Area of application (example):	E-mail security (S/MIME), logging in on a web-based application/appliance as a TLS/SSL client, logging in on a Microsoft network, logging in on a Citrix appliance
End entity:	Natural persons, pseudonyms, legal persons, People, function groups and roles, robots and automata

Table 10: Assignment of certificate type Server to end entities

Type of certificate:	Server
Area of application (example):	TLS/SSL server authentication
End entity:	Devices

Table 11: Assignment of certificate type Router/gateways to end entities

Type of certificate:	Router/gateways
Area of application (example):	VPN authentication within router networks
End entity:	Devices

Table 12: Assignment of certificate type Mail gateway to end entities

Type of certificate:	Mail gateway
Area of application (example):	Virtual post office, authentication of a mail gateway/appliance
End entity:	Devices

Table 13: Assignment of certificate type Domain controller to end entities

Type of certificate:	Domain controller
Area of application (example):	Authentication of the registration authority within a Microsoft network
End entity:	Devices

Certificates for the role Master registrar and Sub-Registrar are always certificate types of the sub-type "natural persons".

In the following sections, the name of the certificate type is largely used as a synonym for the end entity in question. This means that the certificates for natural persons, groups of people and functions, pseudonyms and role owners are subsumed under user certificates; device certificates are understood to refer to all server, router/gateway, mail gateway and domain controller certificates.

Certificates for OCSP responders also come under end entities but are not considered in more detail at this point as they are only used to provide the TeleSec Shared Business CA service but are not provided to the customer.

The area of application of the end entity certificates is described in Section 1.4.1.2. The regulations in Section 4.5.1 also apply.

In contrast to natural persons, in the case of devices, the subject (certificate requester) does not correspond to the end entity that the certificate refers to. The subject is either the certificate holder or a device that is under the certificate holder's control or is operated by this person. The end entity is the owner of the private and public key and is ultimately responsible for the use and backup of the private key and the corresponding certificate. In the case of natural persons, the end entity is also the subject.

The end entity should not be understood as the institution customer/contract partner or tenant (e.g. Sample Company). However, it is still possible for an end entity certificate to be issued for this representative (e.g., Sam Sample as the authorized representative of Sample Company).

The significance of using the terms "end entity" and "subject" in each individual case therefore depends on the context in which the terms are used.

1.3.4 Relying parties

A relying party is a natural person or subject who/that relies on the trustworthiness of the certificate issued by the SBCA in accordance with the presentation in this CPS and/or the digital signature.

Relying parties also include software manufacturers who integrate the SBCA root and intermediate-CA certificates into the certificate archive, for example.

1.3.5 Other subscribers

A group of people or devices or a device always lies in the responsibility of an authorized person who has been authorized for this task by the tenant. The authorized person is identified and registered in the same way as a natural person. The authorized person is responsible for the secure distribution, use and, if necessary, revocation of the certificate. In the event that the authorized person should not be responsible for distribution or revocation, this function is transferred to the holder of the "key owner" role.

1.4 Certificate usage

1.4.1 Permitted usage of certificates

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

1.4.1.1 Security level

Certificates with a medium security level are certificates that are suitable for securing various business processes (e.g., digital signature and encryption of e-mails) within and outside of companies, organizations, public authorities and institutions that require a medium security level to prove the authenticity, integrity and trustworthiness of the end entity. In addition, these certificates are suitable for end entity authentication on applications and networks or for authenticating active network components among themselves.

1.4.1.2 Certificates for users and devices

These certificate types are used for authentication, digital signatures and encryption as part of various applications depending on the assignment of the “key usage” “enhanced key usage” extensions and the CPS specifications.

However, the prerequisite for this is that a relying party can trust the certificate appropriately and that the area of application is not prohibited by law or based on restrictions of the [Trust Center CP] or other agreements. Some examples include:

- Authentication as part of communication protocols (e.g., SSL, IPSec, XML SIG, SOAP)
- Authentication as part of processes (Windows logon, hard drive encryption)
- Encryption as part of communication protocols (e.g., SSL, IPSec, S/MIME, XML ENC, SOAP)
- Digital signature as part of communications protocols (e.g., S/MIME)

Table 14 presents the security levels based on the intended uses.

Table 14: Security level related to intended use

Security level:	Medium
Intended use:	Signature and/or encryption
Intended use:	Authentication

1.4.2 Prohibited usage of certificates

SBCA certificates must not be used for the following purposes:

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

Using end entity certificates as CA or root CA certificates is prohibited.

1.5 Policy administration

1.5.1 Responsibility for the statement

This CPS is published by:

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

57250 Netphen
Germany

1.5.2 Contact information

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

Phone: +49 (0) 1805-268204
Fixed network: EUR 0.14/minute, mobile network: max. EUR 0.42/minute
E-mail: telesec_support@t-systems.com
Internet: https://www.telesec.de

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

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

The publisher named in Section 1.5.1 is responsible for this document (CPS). Approval is issued by the publisher's Change Advisory Board.

1.5.4 Approval procedure for this CPS

This document (CPS) remains valid as long as it is not revoked by the publisher (see Section1.5.1). It is updated when required and is then assigned a new ascending version number (see also Sections 9.12.1 and 9.12.2).

The publisher named in Section 1.5.1 is responsible for this document (CPS). It is released via a formal document release process.

Relevant change requests or changes to the ongoing PKI operation of the TeleSec Shared Business CA are functionally assessed in good time and checked to ensure that they comply with this and the higher level CP/CPS of the "T-TeleSec GlobalRoot Class 2", "Deutsche Telekom Internal Root CA 1" and "Deutsche Telekom Internal Root CA 2" root CAs. If required, the changes are incorporated into the document in question.

1.6 Acronyms and definition of terms

Acronyms and term definitions can be found in Annex A: Acronyms and Annex B: Definition of terms. The The list of references can be found in Appendix C:References.

2 PUBLICATIONS AND DIRECTORY SERVICES

2.1 Directory services

Telekom Security operates a directory service and central data archive for the TeleSec Shared Business CA service. Telekom Security is responsible for the content of these.

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

In addition, documents that are relevant to the public are made available in the form of a central data repository. These include, in particular, the relevant CP/CPS documents of the root and intermediate-certification authorities involved. This directory is available around the clock. As a monthly average the downtime is 1.5 days of the time.

2.2 Publication of certificate information

TeleSec Shared Business CA publishes the following information about https://www.telesec.de/de/sbca. Please switch the current language of the website to EN if possible. Some information are only available in German language.

- This Certification Practice Statement (CPS) from the PKI TeleSec Shared Business CA service in the current and previous versions (https://www.telesec.de/de/service/downloads/pki-repository).
- PKI Disclosure Statement (PDS) https://www.telesec.de/de/service/downloads/pki-repository
- All root- and corresponding sub-CA certificates used in the TeleSec Shared Business CA PKI service (https://www.telesec.de/de/root-programm/root-programm/ueberblick)
- Download area for
  - Service specification of TeleSec Shared Business CA
  - General terms and conditions (https://www.telesec.de/en/service/downloads/terms-of-service)
- Important news
  - News of the PKI service TeleSec Shared Business CA (https://www.telesec.de/de/produkte/shared-business-ca/ankuendigungen)

In addition, all master registrars will be informed

- In case of compromise or suspicion of compromising the private key of a root CA or sub CA,
- decommissioning the root CA or revoking a sub CA,
- Security-relevant changes to this Certification Practice Statement (CPS).

In addition, in the event of security-critical incidents, the master registrar and additional known contacts of the PKI tenant are notified directly in writing or by e-mail.

TeleSec Shared Business CA offers a reverse search via the link https://www.telesec.de/GetServiceByCert/en.html. After uploading an end user certificate (binary or base64 encoded), the following informations are displayed:

- Issuer (Issuer-DN)
- Subject (Subject-DN)
- Certificate serial number

- Valid not before
- Valid not after
- Public key size (bits)
- Signature algorithm
- Link to the Certification Practice Statement (CPS)
- Link to the Service description
- Link to the General terms and conditions
- Link to the PKI Disclosure Statement (PDS) and Service and Usage Agreement TeleSec Business CA
- Link to the CA certificates

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

At regular intervals, Telekom Security publishes certificate revocation lists (CRL), which contain all the certificates revoked by the SBCA with their revocation date and time. Only certificates that are valid at the time of revocation are revoked.

All revoked CA certificates (but no root CA certificates) are published in the revocation list for certification authorities (CARL).

The distribution points of the evocation list are stored in the issued certificates and can be accessed via http and a directory service (LDAP).

The task of the directory service is to provide all parties involved with the PKI with all certificates that are due to be published as well as the current revocation information by means of standard-compliant revocation lists (CRL, CARL). Access to the directory service is via the LDAP (Lightweight Directory Access Protocol) and can be configured with regard to access protection (public or username/password protection).

An LDAP query that returns multiple results is subject to a quantitative restrictions (size limit).

Telekom Security publishes exclusively user and mail gateway certificates only on a public directory service as long as the tenant has agreed to the publication of these certificates.

End entities can search for other tenant's certificates via a user website as long as permission to publish them has been granted.

The following certificate types are not published:

- Master registrar certificates
- Sub-registrar certificates and its derivatives
- Device certificates (router/gateway and domain controller certificates, servers)

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

Furthermore, the SBCA provides a validation service (OCSP responder), which can be accessed via the Internet protocol "Online Certificate Status Protocol" (OCSP) and returns the status of X.509 certificates to the requester.

The address of the OCSP responder is entered in the certificate and is published additionally in the "TeleSec Shared Business CA certificate and configuration datasheet" document. The respective OCSP certificates are not available for download via website.

Further details on CA certificates can be found in Table 15.

Table 15: Specifications for publishing certificates (Production (SBCA-PU))

Type of certificate:	Requirements:
"T-TeleSec GlobalRoot Class 2" root CA certificate	This certificate is preinstalled in the common certificate stores of operating system and application certificate archives as a "trustworthy root certification authority" or is subsequently installed online and supports certificate validation for end entities and relying parties. If required, the certificate can be called up via the SBCA directory service or the Internet.
"TeleSec Business CA 1" sub-CA certificate	This sub-CA certificate was issued by the "T-TeleSec GlobalRoot CA 2" root certification authority and supports certificate validation for end entities and relying parties. If required, the certificate can be called up via the SBCA directory service or the Internet.
"Deutsche Telekom Internal Root CA 1" root CA certificate	This certificate is not preinstalled in operating system and application certificate archives as a "trustworthy root certification authority" but has to be installed additionally later. The root CA certificate supports certificate validation for end entities and relying parties. If required, the certificate can be called up via the SBCA directory service or the Internet.
"Deutsche Telekom Internal Root CA 2" root CA certificate	This certificate is not preinstalled in operating system and application certificate archives as a "trustworthy root certification authority" but has to be installed additionally later. The root CA certificate supports certificate validation for end entities and relying parties. If required, the certificate can be called up via the SBCA directory service or the Internet.
"Business CA" sub-CA certificate	This sub-CA certificate was issued by the "Deutsche Telekom Internal Root CA 1" root certification authority and supports certificate validation for end entities and relying parties. If required, the certificate can be called up via the SBCA directory service or the Internet.
"Internal Business CA 2" sub-CA certificate	This sub-CA certificate was issued by the "Deutsche Telekom Internal Root CA 1" root certification authority and supports certificate validation for end entities and relying parties. If required, the certificate can be called up via the SBCA directory service or the Internet.
"Internal Business CA 3" sub-CA certificate	This sub-CA certificate was issued by the "Deutsche Telekom Internal Root CA 2" root certification authority and supports certificate validation for end entities and relying parties. If required, the certificate can be called up via the SBCA directory service or the Internet.
"Internal Business CA 5" sub-CA certificate	This sub-CA certificate was issued by the "Deutsche Telekom Internal Root CA 2" root certification authority and supports certificate validation for end entities and relying parties. If required, the certificate can be called up via the SBCA directory service or the Internet.

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

Server certificates

https://active.tbca1.test.telesec.de

https://revoked.tbca1.test.telesec.de

https://expired.tbca1.test.telesec.de

User and Mail gateway certificates

https://www.telesec.de/de/service/downloads/produkte-und-loesungen

The assessment bodies/auditors (Section 8 ff.) and the supervisory authority (forwarding of Deutsche Telekom AG's Group Management Center to BSI, BNetzA) are notified of changes to the information security policy of TeleSec Shared Business CA.

2.3 Updating the information (point in time, frequency)

This CPS undergoes an annual review, regardless of any other amendments [CAB-BR]. This shall also apply even if no changes are made to contents.

Updates to the CPS are published as described in Section 9.12 ff and noted in the change history.

Current developments, amendments and changed requirements (for example by CABF-BR) are tracked and considered in the release planning.

The department named in Section 1.5.1 is responsible for carrying out or coordinating the review.

Certificates are published at the time they are generated, provided the tenant does not explicitly request access protection for the partial hierarchy (master domain level) of the directory service. The customer informs Telekom Security in writing whether publication of the certificates at the level of the master domain is desired. The customer is free to set up a certificate publication for individual subdomains (area of responsibility).

The revocation lists are published as described in Section 4.9.7.

2.4 Access to the directory services

The end entities (Section 1.3.3), relying parties (Section 1.3.4) and registration authorities (Section 1.3.2) are not subject to an access control for calling up the revocation lists (CRL, CARL) and using the OCSP service.

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

Searching for certificates via the directory service and read access to this information is not subject to an access control. However, the tenant decides whether the certificates should be published. The number of search results is limited.

Searching for certificates via the role-specific websites is possible only following successful authentication by means of a certificate or username/password. However, the search result depends on the tenant’s requested certificate publication.

Read access for certificate holders and users to information from the root and intermediate certification authority certificates (root and intermediate CA) and the published CPS (see Sections 2.1 and 2.2) via relevant websites is also not subject to an access control.

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)

The Issuer DN represents the unique name of the issuing certification authority (CA) and is described in Section 1.3.1 ff. However, the same naming conventions as for the Subject DN apply.

3.1.1 Name forms

For all certificate requests, the certificate holder's identity is checked. Depending on the certificate type (Sections 1.3.3 and 7.1), the relevant information is entered in various mandatory fields or optional fields that are provided in accordance with the X.509v3 standard.

For all certificate types, at least the following fields must be completed:

- Country Name (C):
- Organization Name (O)

For server certificates, the following additional fields must be completed:

- Locality Name (L), or
- State or Province Name (ST)

Optional fields (e.g., OU3, FQDN) that do not contain any information (empty fields) or are not relevant must not contain any filler characters (metacharacters) such as "-", ".", „*“, " " (Space) or „n/a“.

3.1.1.1 Conventions for the components of the “Subject DN

This section specifies conventions for Subject DNs (requesters) that apply to all end-entity certificates. The following uses the English terms that are commonly used today.

Within the subject DN, the following characters are allowed:

A – Z, a – z, ä, ö, ü 0 – 9, ( ) + - . / : = ? @ and Space (Blank)

Due to the different coding rules for the various certificate fields, not all of the above characters can be used in these input fields (e.g., no umlauts (ä, ö, ü) in the e-mail address(see Section 3.1.1.1.8, 3.1.1.2.1) or FQDN at Common Name field (see Section 3.1.1.1.7) and accordingly Subject Alternative Name field (see Section 3.1.1.2.3) of a server certificate).

However, it should be noted that, depending on the certificate type (e.g. user, server , mail gateway), not all fields of the subject DN (see Section 3.1.1.1.1 to 3.1.1.1.14) are used and that the field lengths are limited.

3.1.1.1.1 Country Name (C):

This mandatory field contains the international country code. This is a code made up of two letters, which is specified in ISO 3166-1, Alpha-2 (International Organization for Standardization). This field specifies the country where the certificate owner is located. This information is verified using a public directory (e.g., extract from the commercial register) or other comparable directories or documents.

Examples: C = “DE “for Germany. C = “US” for United States of America

For more information please see:

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

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

As part of the check for “setting up a master domain (tenant)” or “permitted Internet domains” (Section 3.2.2), the Country Name (C), Organization Name (O) (Section 3.1.1.1.2), Locality Name (L) (Section 3.1.1.1.9) and State of Province Name (ST) (Section 3.1.1.1.10) attributes are added to the tenant’s configuration as a fixed value pair (tuple).

3.1.1.1.2 Organization Name (O)

This mandatory field contains the organization name (e.g. company, institution, authority) of the certificate holder. The organization name in the certificate should have the official spelling of the organization, i.e. it should be identical to the respective register entry (commercial register or similar). The official abbreviation may also be used. In addition, there may be deviations from the official spelling of the legal form if a common abbreviation is used. The legal form is not mandatory.

If the maximum field length (64 characters) is exceeded, the certification authority reserves the right to use a meaningful abbreviation.

Example: O=model company limited liability company, O=model company GmbH or O=model company

Telekom Security verify this information in the course of the registration process using the extract from the commercial register or equivalent, reliable directories/documents. Slight deviations in the spelling of the organization name can be accepted as long as the organization name is still unique (e.g. O = Alpha-Company Inc. <-> O = Alpha Company Inc.) and the postal code also ensures uniqueness.

Telekom Security will inform the applicant about the correction and document the accepted deviation from the official company name.

As part of the check for “setting up a master domain (tenant)” or “permitted Internet domains” (Section 3.2.2), the Organization Name (O), Country Name (C) (Section 3.1.1.1.1), Locality Name (L) (Section 3.1.1.1.9) and State or Province Name (ST) (Section 3.1.1.1.10) fields are added to the tenant’s configuration as a fixed value pair (tuple).

3.1.1.1.3 Organizational Unit Name 1 (OU)

This mandatory field contains the DNS identifier for the tenant’s Internet domain, for the purpose of achieving global uniqueness, or another meaningful name. The Organizational Unit Name 1 is specified before the first master RA certificate is generated for a master domain and cannot be changed after this (see Sections 1.3.2.1 and 3.2.2 for more information). The Organizational Unit Name 1 is listed in the certificate and configuration datasheet.

Examples: OU1 = samplecompany.de, OU1 = t-systems.com

3.1.1.1.4 Organizational Unit Name 2 (OU2)

For the end entity, group, function, role and sub-RA certificates, this mandatory field contains an area of responsibility (sub-domain). An area of responsibility must be clearly assigned to a master domain.

Examples: OU2 = munich-branch, OU2 = headquarters or OU2 = ssl-vpn.

Please note: The master registrar requests the area of responsibility and it is available for use only after approval by Telekom Security.

3.1.1.1.5 Organizational Unit Name 3 (OU3)

For end entity and group, function and role certificates, this optional field (which can be activated/deactivated via the tenant configuration) can be used for a further assignment of the certificate holder to an organizational unit.

Examples: OU3 = Sales, OU3 = Duesseldorf branch, OU3 = <first name surname> (if CN (Section 3.1.1.1.7) is not a meaningful combination of numbers or letters (e.g., personnel number)).

The following entries in the OU3 field are prohibited:

- Entries/data that suggest authorizations that the certificate holder does not possess. Furthermore, slogans or names with racist, discriminating or sexist/pornographic connotations or names suspected of falsely assuming or concealing the identities of organizations are prohibited.
- Entries/data that do not contain any information (empty fields) or are not relevant must not contain any filler characters (metacharacters) such as "-", ".", „*“, " " (Space) or „n/a“.
- Entries/data that are usually entered in the Organization Name (O) field (Chapter 3.1.1.1.2) or other organizational data.
- Entries/data that represent the name choice of trademarks, brand names, trademarks.

Please note: If the OU3 field is activated, the content is checked using a positive list (white list) when the certificate is requested. If the information does not correspond to the list, the request is prevented.

3.1.1.1.6 Given name, Surname

Depending on the type of certificate, the mandatory fields "Given name" and "Surname" contain the name of a natural person. The given name and surname is also required as separate subject content for the Common Name (CN) (Chapter 3.1.1.1.7). Both parts of the name are separated by a blank space.

First name and last name may contain all characters of the character tables UTF-8. However, the following special characters are prohibited:

@ / \ [ ] | < > ? % $? ! ^ # ~ * ´ ` { } , ;

Greek or Cyrillic characters in UTF-8 encoding are currently not supported.

Name parts must not start and/or end with spaces or special characters. The length of the Common Name (made up of given name and surname) including spaces must not exceed 64 characters (spaces are counted as 64 characters and are inserted later), 63 characters maximum).

3.1.1.1.7 Common Name (CN)

Depending on the certificate type, the mandatory "Common Name" field contains the name of the end entity (see Section 1.3.3). These are as follows:

- The first name and surname for user certificates
- The server name (FQDN) for server certificates
- The IP address for router certificates
- The prefix and server name (FQDN) for mail gateway certificates and
- The server name (FQDN) for domain controller certificates.

Examples: CN = Peter Smith, CN = web1.samplecompany.de, CN = <IP address>

Applies to user certificates: The following IDs should be added to the front of the Common Name to identify certificates for group, function and role certificates or when using pseudonyms (see Section 3.1.3 for more information).

- Prefix "GRP:" identifies a group, function or role certificate
- Prefix "PN:" identifies a pseudonym certificate
- Prefix "SYS:" identifies a system or device certificate

Examples: CN = GRP: Technical Support functional mailbox, CN = PN: Sam Sample (see Section 3.1.3 for more information).

For server, router, mail gateway, and domain controller certificates, the Common Name is added to the "Subject Alternative Name" (Section 3.1.1.2ff) enhancement following certificate generation.

For server certificates: All Server names (DNS name, FQDN) has a restricted character set. Allowed characters are:

A - Z, a - z, 0 - 9, . (dot), - (hyphen), * (asterisk), umlauts (ä, ö, ü)

For server certificates: the wildcard character (* asterisk) is only accepted to the far left in the FQDN.

Certain combinations of wildcard characters and characters and/or letters (e.g., h*l.example.com) as well as more than one wildcard character (e.g., *.*.example.com) per FQDN are not accepted.

For server- and router certificates: Umlauts (ä, ö, ü) in the FQDN must be converted as an IDN form into an ACE string.

Example:

IDN-Form: überall-ist.de

ACE-String: xn–berall-ist-8db.de

Restrictions: Certificates that contain a reserved or private IP address or one or more non-public or non-separable DNS names (in particular internal DNS names) in the common name – which applies

particularly to the server, router, mail gateway and domain controller certificate types – must not be issued by a public intermediate certification authority (see Section 1.3.1.2.1).

Alternatively, these certificate types can be issued by an internal intermediate certification authority (see Section 1.3.1.2.2).

3.1.1.1.8 E-mail address (E)

The mandatory "E-mail Address" (E) field contains:

- The e-mail address of the certificate holder (S/MIME) or e-mail address of the associations of individuals, groups, functions and roles, etc. in the case of user certificates
- The e-mail address of an administrator or a function mailbox in the case of devices (servers, routers/gateways, mail gateways, domain controllers)
- The e-mail address of the master registrar or a function mailbox in the case of master registrar certificates
- The e-mail address of the sub-registrar or a function mailbox in the case of sub-registrar certificates.

The mail address is also required for the delivery of notification emails (e.g. issuing, revoking and renewing certificates) and for requesting for and delivering certificates via the mail interface.

The e-mail address is made up of a local part and a domain part. The local part is the part of the e-mail address before the @ symbol and which uniquely identifies the address within the e-mail provider's domain. The domain part is after the @ symbol and the DNS syntax rules apply.

Examples: e- mail = sam.sample@samplecompany.de, e-mail = pki-registrator@example.com

3.1.1.1.9 Locality Name (L)

This mandatory field contains the name of the town in which the organization (e.g., company, institution, authority) is located or registered, has branch offices or in which the device (e.g., server) is run. This information is verified using a public directory (e.g., extract from the commercial register) or other comparable directories or documents.

Examples: locality = Berlin, locality = Munich, locality = Frankfurt am Main

As part of the check for "setting up a master domain (tenant)" or "permitted Internet domains" (Section 3.2.2 ff), the Locality Name (L), Country Name (C) (Section 3.1.1.1.1), Organization Name (O) (Section 3.1.1.1.2) and State or Province Name (ST) (Section 3.1.1.1.10) attributes are added to the tenant's configuration as a fixed value pair (tuple).

3.1.1.1.10 State or Province Name (ST)

This mandatory field contains the name of the constituent state or territorial administrative unit (e.g., federal state, canton, Departement) in which the organization (e.g., company, institution, authority) is located or registered, has branch offices or in which the device (e.g., server) is run. The entries and spellings are specified in accordance with ISO 3166-2 (International Organization for Standardization). This information is verified using a public directory (e.g., extract from the commercial register) or other comparable directories or documents.

The following spellings are allowed:

- Full written form of the "State or Province Name" (Subdivision Name).
- Examples: state or province = Berlin, state or province = Bavaria, state or province = Hesse
- Using an established abbreviation of the "State or Province Name" (Subdivision Name).

Examples: state or province = “NW” for Nordrhein-Westfalen, state or province = “BRU“ for Région de Bruxelles-Capitale, state or province = “75“ for Paris

Official English translations of the country-specific spelling.

For more information please see:

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

e.g.: https://www.iso.org/obp/ui/#iso:code:3166:DE (changing the country code according to ISO 3166-1 (in the example “DE”) allows the selection of a different “State or Province Name (Subdivision)”).

As part of the check for “setting up a master domain (tenant)” or “permitted Internet domains” (Section 3.2.2 ff), the State or Province Name (ST), Country Name (C) (Section 3.1.1.1.1), Organization Name (O) (Section 3.1.1.1.2) and Locality Name (L) (Section 3.1.1.1.9) attributes are added to the tenant’s configuration as a fixed value pair (tuple).

3.1.1.1.11 Street Address

This optional field contains the name of the street where the organization (e.g., company, institution, authority) is based. This information is verified using a public directory (e.g., extract from the commercial register) or comparable directories or documents.

Examples: street address = 17 Sample Street, street address = 5th Avenue

3.1.1.1.12 Postal Code

This mandatory field contains the zip code of the city in which the organization (e.g., company, institution, authority) is based. This information is verified using a public directory (e.g., extract from the commercial register) or comparable directories or documents.

Examples: postal code = 57250, postal code = AZ23G7

3.1.1.1.13 Subject DN Serial Number (SN)

Within an area of responsibility (sub-domain), it can happen that certificates have the same Subject DN. To distinguish between them, a numeric serial number is assigned in the Subject DN. If user, server or router/gateway certificates are issued manually via the sub-RA and user websites, this attribute and its value are automatically generated by the CA system (certification authority) and the value is incremented by one (1).

In principle, this also applies to certificate applications in the bulk process and via e-mail interface. Optionally, the sub-registrar can also specify the Subject DN serial number manually. The same rule applies for certificate requests via the CMP interface.

Examples: SN = 1 for first Sam Sample and SN = 2 for second Sam Sample within the same area of responsibility.

Note: Filling the Subject DN serial number with an alphanumeric value, name, e-mail address, FQDN, organization name or other designation is prohibited.

3.1.1.1.14 Unstructured Name

Further information on the “unstructured name” can be found in Section 3.1.1.2.3.

3.1.1.2 Conventions for “Subject Alternative Name” (SAN) components

The entries in the “Subject Alternative Name” (SAN) field depend on the certificate types in question (user, sever, router/gateway, domain controller and mail gateway). The Subject Alternative Name enhancement must contain at least one entry. The entries in the SAN come from mandatory fields such as:

- Common Name (Section 3.1.1.1.7)
- E-mail address (Section 3.1.1.1.8)
- User Principal Name (Section 3.1.1.2.2)
- DNS Name (Section 3.1.1.2.3)
- IP address (Section 3.1.1.2.4)

as well as from optional fields such as:

- E-mail address (Section 3.1.1.1.8), in case of more than one address.
- DNS Name (Section 3.1.1.2.3)

Restrictions to certificate content are described in Section 3.1.1.1.7.

3.1.1.2.1 RFC822 name

The RFC822 name corresponds to the e-mail address. Optionally, up to three (3) further e-mail addresses can be added to a user certificate. The e-mail address(es) are automatically added in the Subject Alternative Name (SAN) field.

3.1.1.2.2 User Principal Name (UPN)

The “User Principal Name” (UPN) field in the user certificate is optional except as a mandatory entry in the smartcard logon certificate (triple key). The “User Principle Name” is a user-friendly (i.e., easy to remember) name that is used as a Windows login for the domain or Active Directory. This consists of a user account name (also known as a login name) and the domain in which the user account is saved (“user account name”@“domain name”).

The UPN can but does not have to correspond to the e-mail address.

Examples: UPN = sam.sample@samplecompany.de, UPN = sam.sample@local-server.com

For user certificates, the UPN is shown in the “Subject Alternative Name” (Section 7.1.2.3) extension as the “Principal Name”.

3.1.1.2.3 DNS name

The complete name of a domain (also known as the absolute address) is called the fully qualified domain name (FQDN) and labels an exact position in the tree structure of the DNS hierarchy. The “FQDN” field is made up of at least a top level and further sub-domains.

Examples: FQDN = www.example.com, FQDN = s-server.pki.example.de

For server certificates, the FQDN is entered as the “Common Name” as a mandatory field in the Subject DN and is displayed as “DNS Name” in the “Subject Alternative Name” extension.

Optionally, up to four (4) further server names can be added to a server certificate. The server names are automatically transferred to the Subject Alternative Name (SAN) as “DNS Name”.

The wildcard character (* asterisk) is only accepted to the far left in the FQDN.

Certain combinations of wildcard characters and characters and/or letters (e.g., h*l.example.com) as well as more than one wildcard character (e.g., *.*.example.com) per FQDN are not accepted.

For router certificates, the optional FQDN field is entered as an “unstructured name” in the Subject DN and is displayed as “DNS Name” in the “Subject Alternative Name” extension.

3.1.1.2.4 IP Address

For router certificates, the IP address is entered as a component of the “Common Name” in the Subject DN and is displayed as “IP address” in the “Subject Alternative Name” extension.

3.1.1.2.5 Other Name

For domain controller certificates, the mandatory “Microsoft GUID” (MSGuid) field is displayed as the entry “DNS Object Guid” under “Other Name” in the “Subject Alternative Name” extension.

3.1.2 Meaningful names

The name must contain the end entity or certificate holder with a generally understandable meaning and must also be unique and verifiable.

In the case of certificates for groups of people and functions and for pseudonyms, Telekom Security can request that the certificate holder’s true identity be revealed to authorized third parties.

3.1.3 Pseudonymity or anonymity of the certificate holder

User certificates that contain a pseudonym are identified with the prefix “PN:” in the Common Name (CN) (see Section 3.1.1.1.7 for more information).

User certificates for role owners that are groups of people or functions are identified with the prefix “GRP:” in the Common Name (CN).

Transitional arrangement: The old spelling of a colon (:) instead of the underscore (_) is tolerated until the next reissue of the certificate.

Examples: “PN: Novalis”, “PN: George Sand”, “GRP:Procurement“ “GRP: Technical Support”

The use of group and function certificates or pseudonyms is subject to various naming restrictions. Names that suggest authorizations that the certificate holder does not possess as well as political slogans, etc. are not permitted.

3.1.4 Rules on the interpretation of different name formats

No provisions.

3.1.5 Uniqueness of names

Telekom Security ensures that user certificates with the same Subject DN (see Section 3.1.1.1 ff) only appear once within the area of responsibility (sub-domain). This is ensured by assigning a serial number in the Subject DN (see Section 3.1.1.1.13).

For users, one, two or three certificates can be issued that have the same unique Subject DN but differ in terms of the key usage or enhanced key usage (e.g., signature, key encryption, client authentication, smartcard logon) and the certificate serial number. With the renewal function, multiple certificates with the same Subject DN can also be created for a limited period of time.

There may be multiple certificates for devices with the same Subject DN (see Section 3.1.1.1 ff).

3.1.6 Recognition, authentication and role of trademarks

There is a particular duty to take care when selecting the names of trademarks, brand names, trademark rights, etc. in certificates (e.g. Organization Name (O), Organizational Unit Name (OU). It is the responsibility of the tenant to ensure that the choice of name does not infringe upon any trademarks, trademark rights, etc., or the intellectual property rights of third parties. The certification authority SBCA and the internal registration authority of Telekom Security are not obligated to check such rights. Any resulting claims for damages are at the expense of the tenant.

3.2 Identity check for new request

3.2.1 Method for proving the ownership of the private key

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

This requirement does not apply if the key is generated within the certification authority (for bulk, see Sections 3.2.3.4 and 3.2.3.5).

3.2.2 Authentication of organization and domain identity

3.2.2.1 Setting up a PKI tenant

A basic requirement for being able to use SBCA is to set up a PKI-tenant (also known as a master domain) within the TeleSec Shared Business CA PKI service. The technical configuration of the PKI client is based on the filled-in and signed “request for the setup of a master domain”. For proper identification purposes and, consequently, to prove the existence of the organization, Telekom Security requires an official and current document (e.g., certified copy of the extract from the commercial register or similar document) which must not be older than 30 calendar days. In the case of authorities, the official seal and signature of a person authorized to act on behalf of the authority are sufficient for this request.

Checking the request for the setup of a master domain also involves checking the identity of the customer (tenant, delegated third party).

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

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

In the event that a third party is to manage the certificate (incl. the private key) on behalf of the PKI-tenant (delegated third party), a written agreement is required between the two parties with regard to the duty to take due care in performing the transferred work and to comply with the CPS of the SBCA ("transfer of rights and duties" authorization document).

During the authentication, Telekom Security ensures that no names are contained in the Organization (O) and Organizational Unit Name (Ou1 to OU3) fields that suggest authorizations that the certificate holder does not possess. Furthermore, slogans or names with racist, discriminating or sexist/pornographic connotations or names suspected of falsely assuming or concealing the identities of organizations are prohibited.

Telekom Security performs the following checks:

- Verifying the organization's existence through a third party ID checking service/database or through the relevant current organizational documents which were issued by or submitted to a competent office/authority and which confirm the organization's existence (e.g., extract from commercial register or similar document which must not be older than 30 days, official seal)
- Checking the domain name(s) against publicly accessible databases (e.g., WhoIs query via Denic eG) or using a procedure as described in Section 3.2.2.2 ff,
- Verifying the existence of the responsible contact as specified in the "Request for master domain setup" document, who has been identified as the master registrar. Furthermore, checks must be carried out to determine whether the person specified does work for the organization (tenant) or has been given authority to act on behalf of the organization
- Additional checks as required (e.g., to meet the U.S. export provisions and licenses of the United States Bureau of Industry and Science (BIS)).

Telekom Security makes sure that the name of the master domain exists only once within the TeleSec Shared Business CA. The master domain is usually named after the domain names (top-level domain and second-level domain, optional additional sub-level domains permitted) of the PKI tenant. The domain check is described in Section 3.2.5.2. The name of the PKI tenant must be permanently set as the attribute "Organizational Unit Name 1" (OU1) (see Section 3.1.1.1.3) in the Subject DN of the certificate.

If the domain name cannot be used as part of the name, a different naming method may also be used. The name must allow clear conclusions to be drawn about the tenant.

When setting up the master domain, for all the supplied certificate types (user, server, mail gateway, router/gateway and domain controller) only those domains for which the client is able to provide the relevant proof will be set up. The domain names are valid for the entire master domain and are also passed on to areas of responsibility (sub-domains).

Der Name der Master-Domäne(n) wird, sofern es sich um einen DNS-Namen handelt, auch in der Konfiguration der Master-Domäne (PKI-Mandant, externe Registrierungsstelle) or „permitted Internet domains" for the relevant certificate type (e.g., user, server).

The master registration authority acts as an administrator of the PKI tenant (master domain) and is the highest registration authority within the tenant (Section 1.3.2.2.1). The registration process of the master registration authority is described in Section 3.2.3.2.

Organizational changes (e.g., change of company name) or changes to the person acting as master registrar must be reported to the issuer (see Section 4.9.1) of this CPS in writing immediately. The check of an organization change is performed in accordance with the same procedure as described above.

Additional checks are carried out as required.

To fulfill and comply with the [CAB-BR] as well as various root programs, Telekom Security will verify the usage rights of the domain(s).

Depending on the configured certificate type, the „permitted Internet domains“ are checked after the following periods:

- Public Server Certificates
  - after 13 months or 398 days at the latest
- All other public or internal certificates
  - After 39 months at the latest

Telekom Security reserves the right to request current identification documents of the master domain’s owner and/or a third party at that person’s expense.

The following facts are expressly not checked at the time of registration:

- 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.

3.2.2.2 Additional identity checks

The identity checks described in the following chapters refer to all certificate types (chapter 1.3.3) that are issued under a public certification authority (chapter 1.3.1.2.1).

Certificates that do not comply with one of these identity checks may only be issued by an internal certification authority (Chapter 1.3.1.2.2).

3.2.2.2.1 Identity

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

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

3.2.2.2.2 Company name/trade name

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

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

3.2.2.2.3 Verifying the country code

The CA MUST verify the country belonging to the subject in subject:countryName field using one of the following methods:

1. The allocation of the IP address range by the country to (i) the IP address of the website, as specified by the DNS entry for the website, or (ii) the IP address of the customer,
2. The ccTLD of the requested domain name or
3. Information provided by the domain name registrar.

3.2.2.2.4 Validation of Domain Authorization or Control

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

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

3.2.2.2.4.1 Validating the Applicant as a Domain Contact

No stipulation.

3.2.2.2.4.2 Checking the customer by means of contact via e-mail, fax, SMS or letter

No stipulation.

3.2.2.2.4.3 Checking the customer by phone

No stipulation.

3.2.2.2.4.4 Checking the customer by means of a designed e-mail

To confirm that the customer has control over the domain, an e-mail is sent to one or more addresses using the prefix ‘admin’, ‘administrator’, ‘webmaster’, ‘hostmaster’ or ‘postmaster’, followed by the at symbol (“@”), followed by the domain name of the FQDN to be checked. The e-mail message MUST contain a random value that MUST be included in the reply e-mail. (Procedure in accordance with Section 3.2.2.4.4 of the [CAB-BR]). The following applies:

- Every e-mail can confirm the authorization for several FQDNs provided the authorization domain name used in the e-mail is an authorization domain name for every FQDN that is to be confirmed.
- The random value is unique in every e-mail.
- The e-mail may only be resent in its entirety, including re-use of the random value, provided the entire content and the recipients remain unchanged.
- The random value remains valid for use in a confirmation response for a maximum of 30 days following creation.
- As soon as the FQDN is validated using these methods, certificates can also be created for other FQDNs that end with all labels from the validated FQDN.
- This method is also used for validating wild card domain names.

3.2.2.2.4.5 Domain Authorization Document

Alternatively, a domain authorization letter is requested for the organization, which was issued by the domain holder, registrant or admin C.

It is verified whether the domain authorization letter was issued on or after the date of the certification request and that the WHOIS entry has not been changed since the proxy was issued. (Procedure in accordance with Section 3.2.2.4.5 of the [CAB-BR]).

This method is not applicable to server certificates that are to be issued under a public certification authority on August 1, 2018.

3.2.2.2.4.6 Agreed-upon change to website

No stipulation.

3.2.2.2.4.7 Change in DNS

With this validation procedure, domain control is demonstrated for each FQDN listed in the certificate by the targeted insertion of unique information in the DNS.

- A unique, constructed random value is used.
- The random value is valid for a maximum of 30 days after its creation.
- The receiver inserts the random value in the DNS of the FQDN under test.

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

This method is also used to validate wildcard domain names.

(Procedure in accordance with Section 3.2.2.4.7 of the [CAB-BR]).

3.2.2.2.4.8 IP address

No stipulation.

3.2.2.2.4.9 Test certificate

No stipulation.

3.2.2.2.4.10 TLS using a random number

No stipulation.

3.2.2.2.4.11 Any Other Method

No stipulation.

3.2.2.2.4.12 Validating Applicant as a Domain Contact

Validation of the applicant examines whether the applicant is the domain contact of the commissioned fully qualified domain name (FQDN). This method can only be used if the certification authority (CA) is also the domain name registrar or an affiliate of the registrar of the main domain name.

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

A contract with the domain management of Deutsche Telekom AG (registrar) contains a list of defined domains that are owned by the Telekom Group and may be used by defined group entities. The commissioned FQDN of an internal customer is checked against this list.

In the case of internal orders from other corporate units, the registration employee has confirmed the applicant as an authorized domain contact by the domain management. (Procedure in accordance with Section 3.2.2.4.12 of the [CAB-BR]).

3.2.2.2.4.13 Email to DNS CAA Contact

No stipulation.

3.2.2.2.4.14 Email to DNS TXT Contact

No stipulation.

3.2.2.2.4.15 Phone Contact with Domain Contact

No stipulation.

3.2.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

No stipulation.

3.2.2.2.4.17 Phone Contact with DNS CAA Phone Contact

No stipulation.

3.2.2.2.4.18 Agreed-Upon Change to Website v2

The control over the FQDN is verified by checking whether the customer has stored a request token as the content of a file on the website. This is done by executing of an HTTP request. The request token does not appear in this request.

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

The file containing the request token

- is queried with the domain name, which is used for the authorization of the FQDN, and
- is read from the path "http: // <CommonName> /.well-known/pki-validation/sbcadv.txt", and
- is retrieved using either the "HTTPS" or "HTTP" scheme and port 443 or 80.

Redirects are tracked when

- they are initiated at the HTTP protocol level, and
- the HTTP response contains the status code 3xx, and
- the redirects lead to resource URLs that can be accessed via the "HTTPS" or "HTTP" scheme and via port 443 or 80.

The Request Token contains a timestamp, a unique random value, and a reference number, if applicable. The Request Token is valid for a maximum of 30 days after its creation.

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

This method is also used to validate wildcard domain names.

(Procedure in accordance with Section 3.2.2.4.18 of the [CAB-BR]).

3.2.2.2.4.19 Agreed-Upon Change to Website - ACME

No stipulation.

3.2.2.2.4.20 TLS Using ALPN (Application-Layer Protocol Negotiation)

No stipulation.

3.2.2.2.5 Authentication for an IP address

No stipulation.

3.2.2.2.5.1 Agreed-Upon Change to Website

No stipulation.

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

No stipulation.

3.2.2.2.5.3 Reverse Address Lookup

No stipulation.

3.2.2.2.5.4 Any Other Method

No stipulation.

3.2.2.2.5.5 Phone Contact with IP Address Contact

No stipulation.

3.2.2.2.5.6 ACME “http-01” method for IP Addresses

No stipulation.

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

No stipulation.

3.2.2.2.6 Verification of a wildcard domain

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

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

3.2.2.2.7 Reliability of the data source

Only trusted data sources are used as reliable data sources, but no data sources that are self-maintained or maintained by affiliated companies.

3.2.2.2.8 CAA records

See section 3.2.5.3 and 4.2.2 ff.

3.2.3 Authentication of individual identity

3.2.3.1 General

The identity or identification of end entities (see Section 1.3.3) is authenticated by the registration authority set up at the tenant's premises (see Section 1.3.2 ff).

The following registration methods are available for SBCA as standard:

- Central registration (central registration model), i.e., following successful registration of the end entity, the sub-registrar requests the certificate from the sub-registrar website (using a web form or in bulk) and directly receives this certificate or the key material for the end entity (excluding the registrar certificate)
- Local registration (central registration model), i.e., the user requests the certificate from the user website or by sending an e-mail request, or the device uses its SCEP interface to request the certificate which is processed by the sub-registrar (approval, rejection or deferral (resubmission))

Please refer to the "Service Specifications for TeleSec Shared Business CA" for a more detailed description of the two registration models.

The following rules apply here:

- An end entity is always registered via the responsible sub-registrar. An exception is the automated bulk generation of key material.
- The sub-registrar decides whether the certification request is approved, rejected or deferred (resubmitted).
- A renewal function, which can be used any number of times provided that the certificate data (e.g., organization) does not change, is available for user certificates. It is up to the tenant to decide whether this renewal function may be used in principle. No renewal function is available for device certificates.

With the initial setup of a PKI tenant, the customer domain, as described in Section 3.2.2 ff, is added to the PKI configuration as a permitted Internet domain. To issue certificates from a public certification authority (see Section 1.3.1.2.1), the verified organization data (see 3.1.1.1.1, 3.1.1.1.2,

3.1.1.1.9 and 3.1.1.1.10) is prefilled in the PKI tenant for a specified time and linked to the customer domain.

Additional domains can be added as “permitted Internet domains” as required and added to the PKI configuration with a link to the relevant organization data. The basis for this is one of the verification methods listed in Section 3.2.2.2.

The following facts are expressly not checked at the time of registration:

- That the end entities named in the certificate are engaged in an active business activity.
- That the end entities named in the certificate are conducting their activity in conformity with the law.
- That the end entities named in the certificate are conducting their business activity in a trustworthy, honest or serious manner.
- That it is safe or not dangerous to conduct business with the end entity named in the certificate.

3.2.3.2 Registration of a master registrar

Telekom Security registers the master registrar as part of the identity check of an organization (see Section 3.2.2 ff).

The master registrar certificate required for administration of the master domain (PKI tenant) is issued to a natural person and contains a unique name for the PKI system (Common Name). The natural person is an employee of the organization (PKI tenant) or a delegated third party. An ID copy (e.g. Personal ID card, passport, company ID) and a verification phone call are accepted as proof of identity.

The procedure described above is performed to issue additional master registrar certificates.

Due to these authorizations, master registrar certificates are always issued on smartcards. Invalid or revoked master registrar certificates can no longer be used and must be requested again with a corresponding identity check.

3.2.3.3 Registration of a sub-registrar

The tenant can arrange for one or more areas of responsibility (sub-domains) to be administrated by sub-registrars. The following rules apply:

The tenant’s master registrar registers a sub-registrar and issues the sub-registrar certificate.

The registration is issued to the sub-registrar in person or on the basis of a tenant database with integrity.

The same procedure also applies to sub-registrar derivative (see Section 1.3.2.2.2) that is required for the optional “CMP interface”.

3.2.3.4 User registration

Users (natural person, groups of persons/functions, pseudonym) are registered centrally or locally by the sub-registrar. The guidelines described in Section 4.2.1.2 apply.

3.2.3.5 Device registration

Devices (server, router/gateway, mail gateway and domain controller) are registered centrally or locally by the sub-registrar. The guidelines described in Section 4.2.1.2 apply.

3.2.4 Non-verified subscriber information

Unverified information is information that is included in the certificate without being checked and includes:

- Other information that is identified as unverified in the certificate (e.g., key usage, extended key usage).

Certificates that are issued under the “TeleSec Business CA 1” sub-CA contain information that has been verified by Telekom Security.

Certificates that are issued under the “Internal Business CA 1” and “Business CA” sub-CAs may contain information that has not been verified.

3.2.5 Validation of authority

3.2.5.1 Ensuring the authenticity of the certification request

Every tenant or delegated third party concludes a contract with Telekom Security for the „TeleSec Shared Business CA” PKI service. The delegated third party provides Telekom Security with the name of an employee who takes on the role of master registrar. To verify the authenticity of the named master registrar, a call is made to the delegated third party’s central telephone number that is stored in the commercial register or a comparable directory. The Telekom Security registration authority employee performing this task (TC Operator) asks the switchboard to be connected to the aforementioned representative of the customer and thus confirms the authenticity of this person.

The delegated third party also names the employees who are to take on the role of sub-registrar (derivatives of the sub-registrar, where appropriate). The named employees must be documented in writing at the registration authority and archived (for at least seven years).

3.2.5.2 Checking domains and IP addresses

The delegated third party notifies Telekom Security of the domain(s) for which certificates are to be issued so that Telekom Security can check them, include them in the tenant’s PKI configuration as “permitted Internet domains” and maintain them.

Name changes to the domain(s) and/or changes to the ownership rights to the domain(s) in question must be reported to Telekom Security in writing immediately.

The Telekom Security registration authority employee checks the relevant entries to see whether the tenant has the necessary rights to the domain in question. This involves querying the online database of the country-specific NIC unit (e.g., Denic eG for Germany) for geographic top level domains (ccTLDs) or the online WhoIs database for generic top-level domains (gTLDs. To check an IP address, adequate online databases are queried.

gTLDs may only be used for naming PKI tenants and/or issuing certificates after the gTLD operator has proven ownership to the TSP and the ICANN agreement (registry agreement) has been published on the ICANN website [www.ICANN.org].

The TSP checks whether the applicant is the domain name registrant or can prove control of the domain name, using the validation methods described (Section 3.2.2.2.4 ff).

If this does not lead to a successful result, it is checked whether the customer or delegated third party has been authorized by the applicant to use the domain or IP address. The applicant is the user or representative of an organization, who controls or operates the device listed on the certificate, even if the device sends the actual certification request. The written authorization must be issued by the user, domain owner or admin C of the device.

For user certificates that are used for mail security (S/MIME certificates) and contain an e-mail address of an Internet Service Provider (ISP), a general power of attorney from the domain owner in

question (e.g., t-online.de, gmx.de, 1und1.de) will be accepted by Telekom Security when using a public intermediate certification authority (see Section 1.3.1.2.1).

In the event that a certificate from an internal intermediate certification authority is issued for this certificate type (see Section 1.3.1.2.2), a copy of an identification document (e.g., company ID, personal ID) is sufficient. Note: The access number on the front of the peronal ID should be blacked out for security reasons, as this can be used for online functions.

To fulfill and comply with the [CAB-BR] as well as various root programs, Telekom Security will verify the usage rights of the domain(s).

Depending on the configured certificate type, the „permitted Internet domains“ are checked after the following periods:

- Public Server Certificates
  - after 13 months or 398 days at the latest
- All other public or internal certificates
  - After 39 months at the latest

Telekom Security reserves the right to request current identification documents of the master domain's owner and/or a third party at that person's expense.

3.2.5.3 Checking CAA entries in the DNS

The following applies for the issue of server certificates from a public certification authority (see Section 1.3.1.2.1):

All FQDN entries are checked against the CAA entries in the DNS (Certification Authority Authorization; CAA Records for Fully Qualified Domain Names) in the scope of the authorization check.

If one or more CAA resource records are found whose issue or issuewild property differs from "telesec.de", the certificate request will be rejected. If the issuewild property contains a semicolon ";", then a wildcard certificate request is always rejected.

If there is no CAA resource record or the issue or issuewild-property of the CAA resource record is "telesec.de" the check will be completed.

„TeleSec Shared Business CA" processes 8 CNAME chain records and limits the length of the chain to a maximum of 10 as recommended.

3.2.5.4 Additional checks by the tenant

If the certification request shows that the name of a natural person is linked to the name of an organization in such a way that it becomes clear that the person is able to act on behalf of this organization, the tenant's registration authority shall:

- Check whether the organization exists. This involves using a third party ID checking service/database or requesting documents from the government/authority responsible, which confirm the existence of the organization, and
- Obtain business information that confirms whether the person requesting the certificate is employed by the organization and, if necessary, whether the person is authorized to act on behalf of the organization.

3.2.6 Criteria for interoperability

If a sub-CA uses a policy OID that represents fulfillment of and compliance with the [CAB-BR] in a certificate that it has signed (see Section 7.1.6.3.2), the corresponding CP or CPS of the sub-CA

must contain an explicit assurance that all certificates issued by the sub-CA that contain this policy OID are issued and managed in conformity with the [CAB-BR].

No other sub-CA certificates are issued under the „TeleSec Shared Business CA" PKI service.

The PKI service „TeleSec Shared Business CA" currently does not use cross certificates (see Figure 1).

3.3 Identification and authentication for key renewal orders

In order to continuously provide authentic and secure communications, the end entity must procure a new certificate before the old one expires. Whether a new key pair is required for the subsequent order depends on the application and key pair used (smartcard, soft PSE).

Key renewal for smartcard

In the event of a subsequent order, the current smartcard can be used with the key pair on it as long as technical specifications (e.g., insecure crypto algorithms) or functional restrictions (e.g., failed log on attempt counter has run out) do not forbid or prevent this. Otherwise a subsequent certificate must be issued on a new smartcard. The rules for registration apply as described in Sections 3.2.3 ff and 4.2.1. If the smartcard supports internal key generation, new key pairs can be used for the subsequent order.

Key renewal for soft PSE

In the case of subsequent orders as soft PSE, generally new key pairs are generated; however, for certain devices (e.g., web servers) the existing key can also be reused. It is up to the certificate holder or tenant to decide whether a key renewal takes place. The rules in Section 6.1 ff must be taken into account.

The following applies for the issue of certificates for end entities (except servers) from a public certification authority (see Section 1.3.1.2.1):

- To validate a renewal request, Telekom Security only uses documents, documentation or other information not older than 39 months at the time the certificate is issued.

The following applies for the issue of certificates for end entities (for servers only) from a public certification authority (see Section 1.3.1.2.1):

- To validate a renewal request, Telekom Security only uses documents, documentation or other information that were
  - until August 31, 2020: not older than 825 days or 27 month.
  - from September 1, 2020: are not older than 398 days or 13 month

3.3.1 Identification and authentication for routine key renewal

Routine key renewal is the responsibility of the tenant, who must take into account Section 6.1. The identification and authentication correspond to that for an initial order (see Sections 3.2.2 ff and 3.2.3 ff).

3.3.2 Identity check and authentication for a key renewal following certificate revocation

It is not possible to renew the key of a revoked certificate. The only option is a new order and thus the described identity check (see Sections 3.2.2 ff and 3.2.3 ff).

3.3.3 Identity check following the end of the validity period

It is not possible to renew a certificate once the validity period has ended. The only option is a new order and thus the described identity check (see Sections 3.2.2 ff and 3.2.3 ff).

3.4 Identification and authentication for revocation orders

Revocation orders are authenticated by providing certificate content (e.g., Common Name, organization/company, e-mail address) in order to search for and select the certificate to be revoked. The revocation order is authorized using the revocation password that the certificate holder knows (see section 4.9.2).

4 OPERATIONAL REQUIREMENTS IN THE LIFE CYCLE OF CERTIFICATES

4.1 Certificate request

The certificate request (see Section 4.1 ff) is submitted in electronic form via a website (sub-registrar, user) or technical interfaces (SCEP or mail interface) depending on the registration model (Section 3.2.3).

Due to the requesting procedure or the interface, a certificate request is already assigned to the relevant certificate profile (e.g., server, router).

4.1.1 Who can request a certificate?

The following conditions apply when requesting certificates:

- Conclusion of a contractual relationship regarding the provision and handover of the TeleSec Shared Business CA PKI service between the tenant (external registration authority) or person authorized to act on behalf of the tenant and Telekom Security
- Setup of a master domain/PKI tenant (Section 1.3.2.1)
- Successful login with the role in question (master or sub registrar, user) to the role-specific website
- Optional: access data for the e-mail, SCEP and CMP interface.

The following people can request a certificate:

- Authorized persons of an external registration authority (master registrar, Section 1.3.2.2.1)
- Authorized persons of an external registration authority (sub-registrars and their derivatives, Section 1.3.2.2.2)
- Authorized persons who appear as the subject of the certificate
- Authorized persons who act as an applicant representative
- Authorized persons from groups of persons and functions and devices
- Authorized persons from the Telekom Security internal registration authority in the scope of setting up and managing a master domain (Section 3.2.2 ff).

Authorized persons are understood to be natural persons who either have a valid registrar certificate or suitable logon data.

4.1.2 Registration process and responsibilities

4.1.2.1 Internal registration authority

The setup and further maintenance of the master domain (PKI tenant), the “permitted Internet domains” and issue of the master registrar certificate are based on successful authentication of the identity of organizations, which is described in Section 3.2.2. ff

PKI tenants that are set up and maintained for the TSP are subject to the same requirements of the registration processes.

4.1.2.2 External registration authority

4.1.2.2.1 Setting up the tenant

For setup of the master domain, the tenant's customer agrees to complete the "Request for the setup of a master domain for the TeleSec Shared Business CA" document truthfully, have it signed by an authorized person and present it to Telekom Security together with the required identification documents so that T-System can perform the identity check in accordance with Section 3.2.2. ff. The master registrar is also named in this document. After the master registrar certificate has been issued, it will be sent to the master registrar, including the „TeleSec Shared Business CA Service and Usage Agreement", which must be accepted in writing. This consent must be repeated online every time the certificate is renewed via the web portal.

The tenant/external registration authority also agrees to transfer the confirmation of compliance with the rules of this CPS document in its currently valid version to its registration authority employees (master and sub-registrar and their derivatives, Section 1.3.2.2.2) and end entities. The certification authority will announce new versions in good time.

The TeleSec Shared Business CA PKI service supports two registration authorities, as described in Section 3.2.3 ff. The delegated third party is responsible for selecting the registration model.

PKI tenants that are set up and maintained for the TSP are subject to the same requirements of the registration processes.

When using the SBCA with foreign procurement, the valid national export and import conditions must also be taken into account.

4.1.2.2.2 End entities including registration authority employees

All end entities including registration authority employees (master and sub-registrar and their derivatives, Section 1.3.2.2 ff) acknowledge the current version of the "Certificate Policy (CP)/Certification Practice Statement (CPS)" document as well as the Service and Usage Agreement TeleSec Business CA including data privacy statement and agree to comply with the rules described therein.

Furthermore, the end entity and registration authority employee guarantee:

- that the statements made in the certificate request are true and correct, and at the same time meet the naming requirements (see Section 3.1.1.1.1 ff)
- To transfer the public key and the certificate data to Telekom Security for certificate generation
- To provide proof of ownership of the private key, which is connected to the certified public key

Before the sub-registrar certificate is issued, the sub-registrar must accept the Service and Usage Agreement TeleSec Business CA in writing. This consent must be repeated online every time the certificate is renewed via the web portal.

Before the end entity certificate is issued, the requester or the requester's representative must accept the "Service and Usage Agreement TeleSec Business CA" or the "Subscriber Agreement". Depending on the registration procedure (e.g. web form, bulk), this consent must be repeated online each time the certificate is renewed.

If the certificate holder and the issuing CA belong to a mutual legal person (affiliated company), the issuer's representative has to accept the requester's "Service and Usage Agreement TeleSec Business CA" before issuing a certificate. If the certificate holder is a delegated third party who has the certificates for "own use" (enterprise RA) and does not sell them on to third parties as a reseller, he must accept the "Service and Usage Agreement TeleSec Business CA" before a certificate is issued.

If the certificate holder orders/requests a certificate via a delegated third party as a reseller, the certificate holder must accept the “Subscriber Agreement” before a certificate is issued.

If the requester and the registration authority employee are the same person, the certificate request must be confirmed in writing by a third party (e.g., supervisor).

The following process description also applies to the TSP itself if it issues certificates in its name.

Telekom Security reserves the right to agree other obligations, assurances, consents and guarantees towards the end entity.

4.2 Certificate application processing

The following process description also applies to the TSP itself if it issues certificates in its name.

A certificate request that originates from a device or an application is checked for defined content from the Subject DN (see Section 3.1.1 ff) and the use of forbidden characters. Prefilled content in the Organizational Unit Name 1 and 2 attributes (Sections 3.1.1.1.3 and 3.1.1.1.4) are always overwritten with the entries assigned to the sub-registrar responsible when the certificate is approved or issued.

Contents that go beyond the Subject DN (e.g., key usage, extended key usage) are ignored without a message or note. The version of the certificate profile in question as described in Section 7.1 ff applies.

The use of characters that are not permitted is shown during the check or the requester is informed by e-mail.

4.2.1 Performing identification and authentication

4.2.1.1 Internal registration authority

The master registrar certificate is issued based on the successful authentication of the identity of organizations. This is described in Section 3.2.3 ff. The naming conventions in accordance with Section 3.1.1 ff must be complied with.

The existence of the master registrar reported by the tenant is reviewed annually by the TSP in writing (e.g. by email).

4.2.1.2 External registration authority

End users are authenticated by sub-registrars (see Section 1.3.2.2 ff.) within the registration authority responsible that has been set up at the client.

The external registration authority undertakes to perform the following tasks:

- Registration is performed through
  - Personal appearance of the end user, his deputy or a key owner who can authenticate himself by presenting appropriate ID documents and who is responsible for the proper preparation of the certification request and the certificate installation, or
  - Another appropriate process (e.g., request via the user website, e-mail, SCEP or CMP interface), which clearly indicates the end user’s identity. The subject data of the certificate may be based on a client database with integrity. Evidence of the generation of the data inventory must be provided to the certification authority on request.
- Where certificates are requested for devices or groups of persons/functions, the natural person (e.g., administrator) who controls or operates the device listed in the certificate must also be authenticated as the key owner.
- The registration authority employee accepts the electronic or paper-based certification request, verifies its integrity and authenticity and checks the details it contains against

unique identification documents presented by the applicant (e.g., company ID, personal ID (Note: The access number on the front should be blacked out for security reasons, as this can be used for online functions), ERP system) for authenticity (whether they are genuine and trustworthy), integrity (whether they have not been tampered with), correctness, truth and completeness. Reliable internal and public data sources may be used to authenticate the request data.

- The naming conventions in accordance with Section 3.1.1 ff must be complied with.
- In the case of user certificates that are used for e-mail security (S/MIME certificates) and are issued by the "TeleSec Business CA 1" sub-CA, the external registration authority must perform an electronic check of the e-mail address. This is done on the basis of a challenge response procedure where the end user is requested to verify the existence of the e-mail address.
- If the certificate is requested electronically via the relevant website or e-mail interface, the domain part of the e-mail address (optionally also the UPN) is checked for the "permitted Internet domains" entered in the PKI configuration.
- In the case of device certificates, the domain part of the e-mail address or the DNS name (top level domain and other FQDN sub-domains) is to be checked for the "permitted Internet domains" entered in the PKI configuration, depending on the certificate type.
- If the client has additional domains for which the certificates are to be issued, Telekom Security must be notified of the additional domains. Following a successful domain check, these will be included in the PKI configuration of the master domain (PKI tenant) (see also Sections 3.2.2 and 4.2.1.1).
- Applicants providing misleading request details are to be rejected.
- If the names are identical, the registration authority must render them unique.
- In the event that the request data does not correspond to the tenant's data (Country Name (C), Organization Name (O), Organizational Unit Name, domain part of the e-mail address and, if applicable, User Principal Name (UPN), top-level and Other sub-domains of the fully qualified domain name (FQDN), also refer to Section 3.1.1 ff), then a power of attorney or authorization document from the requester is required.
- In the case of certificates for group/functions or pseudonyms, the information provided in Section 3.1.3 applies.
  - For group/function certificates, the identity of the applicant responsible or his deputy must be checked and assessed by the sub-registrar, and then documented following approval.
  - If a pseudonym is used, the official identity of the end entity or certificate holder must be checked, assessed and documented by the sub-registrar.
  - This is the tenant's responsibility.
- Copies of the unique ID documents presented by the applicant must be archived for at least seven years at the expense of the client/external registration authority in a tamper-proof manner. This archive must be protected against unauthorized access.
- In the event of audits or other reviews (e.g., random checks), the registration documents must be disclosed to Telekom Security or a qualified auditor appointed by Telekom Security.
- Depending on the registration model (Section 3.2.3), a check must be carried out to establish whether the applicant or deputy accepts the subscriber agreement and/or Service and Usage Agreement TeleSec Business CA. If acceptance of any of these documents is refused, the entire certification request must be denied.
- When issuing server certificates through the "TeleSec Business CA 1" sub-CAs, the registration authority employees must meet the requirements of the respective current version of the [CAB-BR], Section 7.1.4.2 ff (Subject Information) and 3.2.2 ff (Authentication of Organization and Domain Authority).

- The registration authority employees are obliged to report any suspicions of compromised keys, certificate misuse or other (attempted) fraud in relation to certificates to Telekom Security immediately.
- Certification requests with entries that match those in the “Denied List” (Section 4.2.2.2) must also be approved by the Trust Center of Telekom Security.
- Certification requests with entries that match those in the “High Risk List” (Section 4.2.2.2) must be checked by the registration authority employee with particular care.
- Electronic entry of registration data by the sub-registrar (optional function). This “pre-authentication data” supports automatic issuing of the certificate as long as the request data that is created via the user websites, SCEP or CMP interface corresponds with the pre-authentication data.

If the certification request is made via the websites, the certification authority checks it for increased risk resulting from entries in the following lists:

- **Denied List**: Telekom Security maintains an internal database containing certificates which have been revoked in connection with phishing, misuse or fraud attempts. This information is used to be able to identify future suspicious certification requests.
- **High Risk List**: Telekom Security maintains a database containing organizations as well as domain names or IP addresses which may become a target of phishing, misuse or fraud attacks due to their attractiveness. These certification requests are identified automatically to notify the registration authority employees to take particular care. A documented process is followed here. This is to generate additional vigilance and attentiveness when checking request data. In individual cases, the verification process can have the effect that a requested certificate is not issued.

If the certification request matches entries in the “High Risk List” additional approval is required from the Trust Center of Telekom Security.

If the certification request matches entries in the “High Risk List”, the applicant is notified that he is in the process of requesting a certificate which meets the “High Risk Criteria” and that the security requirements for the registration process and therefore also for the registration authority employee are particularly high here. In addition, this verification is to be confirmed in the electronic request in writing.

4.2.2 Approving or denying certification requests

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

4.2.2.1 Internal registration authority

4.2.2.1.1 Master registrar certificate

If the authentication of the required end user information according to Sections 3.2.2 and 4.2.1.1 has been successful, the certification request is approved and the master registrar certificate issued for management of the tenant.

To validate a request that leads to the issuing of a Master registrar certificate, Telekom Security only uses current and valid documents, documentation or other information (e.g. copy of ID, telephone call to the master registrar).

In the event that the identification data do not match the verification data, the certificate request must be rejected.

4.2.2.1.2 Checking of domain and organization data

The internal registration authority performed the following checks:

- That the domains exist and belong to a tenant (Section 3.2.2 ff, 3.2.3 ff, 3.2.5 ff).
  - The following applies to gTLD: Telekom Security regularly checks (maximum every 30 days) on the ICANN website (https://newgtlds.icann.org) whether new gTLDs have been released or canceled. In the event of changes, a check is carried out to determine whether certificates already contain domain names with this gTLD. Furthermore, any further certificate issuance for this gTLD will be suspended until control over the domain name or the applicant's exclusive right to use the domain name has been proven. In the event that proof cannot be provided or the gTLD has been terminated, all certificates issued with this TLD in the domain name must be revoked within 120 days (Section 4.9.1.1).
- Verification and organization data (organization name (Section 3.1.1.1.2) and location (country, federal state, place see Section 3.1.1.1.1, 3.1.1.1.10 and 3.1.1.1.9)).

Following a successful domain check, this is added to the corresponding tenant configuration as a “permitted domain” of the relevant certificate type (e.g., user, server).

Optionally, it is possible to add the organization data with the domain to the tenant configuration as a default (prefilling of organization data).

These requests are processed within a suitable period following receipt of the complete documents.

4.2.2.2 External registration authority

Only after the subscriber has registered successfully will a certification request be processed further (see Sections 3.2.3 and 4.2.1.2). Depending on the registration model (see Section 3.2.3), the sub-registrar enters the certification request electronically via his website or approves the request, which has already been submitted electronically.

If the submitted identification documents are incomplete, untrue or incorrect, the certification request must be denied in an appropriate manner (e.g., by e-mail or phone), specifying the reasons.

If the identification documents are incomplete, the registration authority employee may apply for resubmission.

A certificate request must be rejected if:

- The certificate request and the identification documents are not complete, true or correct
- The certificate request and the identification documents are from an untrustworthy source
- The certificate request and the identification documents do not lead to a clear positive registration result
- The public key falls short of the minimum key length of 2048 bits (exceptions are possible when using the sub-CA “business CA”)
- The public exponent does not meet the specifications of the [CAB-BR]
- The result of checking for Debian weakness (Debian weak key) is positive
- If application data match with high risk criteria
- In the case of server certificates issued by the sub-CA “TeleSec Business CA 1”, a CAA resource record of type 257 is found that does not contain the entry (tag=issue respectively issuewild-Property, value=telesec.de)

If the identification documents are incomplete, the registration authority employee may apply for resubmission.

If the request is delayed or rejected, the certificate holder's technical contact will be notified by e-mail giving reasons.

4.2.3 Processing period for certificate requests

4.2.3.1 Internal registration authority

The certificate request for master registrars based on the "Request for the setup of a master domain for the TeleSec Shared Business CA" or "Subsequent request for further master registrar certificates" document is processed within a reasonable time following receipt of one of the complete documents.

4.2.3.2 External registration authority

The processing duration for certificate requests for end entity certificates (other than master registrar certificates) is the responsibility of the tenant.

4.3 Certificate issuance

The following process description also applies to the TSP itself if it issues certificates in its name.

4.3.1 Measures of the CA during the issuing of certificates

4.3.1.1 Internal registration authority

Once the certificate request has been approved by the internal registration authority, the certification authority (CA system) immediately issues the master registrar certificate.

Circumstances can lead to the issuance of a certificate being delayed if

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

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

4.3.1.2 External registration authority

Following approval by the external registration authority, the CA system checks the certificate request for the "permitted Internet domains" entered in the tenant's PKI configuration (master domain) and, if applicable, the "prefilled organization data" (Section 4.2.2.1.2). In the event that the result is good, the certificate is issued immediately.

Requests via the CMP interface may involve deviations from this process. Optionally, the certificate can also be issued without approval from the sub-registrar responsible.

In the event that the certificate request contains information that does not correspond to the "permitted Internet domains", the certificate is not issued and the sub-registrar responsible is informed via an information message.

Certificate requests that correspond to the pre-authentication data are released without the approval of the sub-registrar and the certificates are issued directly.

If the optional pre-authentication function is set up for the client and the sub-registrar has entered pre-authentication data, all certificate requests that are made via the user website, SCEP or CPM interface are issued directly.

4.3.2 Notification of end entities about the issuing of certificates

Depending on the certificate type, the certificate holder, requester or representative is informed that the certificate has been issued (approval notification). This e-mail contains the relevant certificate information.

4.4 Certificate acceptance

4.4.1 Acceptance by the certificate owner

The following behavior constitutes acceptance of a certificate:

- The end entity downloading and installing a certificate based on a message or an attachment to a message.
- Acceptance of the key material including PIN or password (smartcard or soft PSE) that was issued for the end entity or registrar.
- If the end entity does not raise an objection to the certificate or its contents with the registration authority responsible within a time defined by the tenant after receiving the certificate.
- If the registration authority responsible does not receive an objection within a time defined by the tenant after receiving the certificate or the certificate content.

4.4.2 Publication of the certificate by the certification authority

Certificates are published via a directory service or web-based access to a database. The following rules apply:

- The publication of the certificates depends on the certificate type and the regulations in accordance with Table 15.
- Certain certificate types (see Table 15) can be published additionally in agreement with the tenant.
- Whether the directory service is public or protected is up to the tenant and is configured when setting up the master domain. Any agreements that are relevant to data protection are the tenant's responsibility. The master registrar can also configure additional access protection in the lower level areas of responsibility (sub-domains).

For the publication of server certificates by a public certification authority (Section 1.3.1.2.1), the CT function (Certificate Transparency) can be activated within the tenant configuration. In this case, the SCT entry is added to the server certificate and published on several CT log servers:

Important note: non-publication via CT log server results in a restriction of the service scope and may lead to the application refusing to accept or rejecting the server certificate.

4.4.3 Notification to further instances regarding the issuing of the certificate by the certification authority

Notification of other instances (e.g., registrars, administrators, function groups) by e-mail (approval notification) can be configured in the master domain.

4.4.4 Certificate transparency

TeleSec Shared Business CA supports certificate transparency (CT). Further details can be found: https://www.certificate-transparency.org and [RFC6962].

All server certificates issued by a public certification authority (CA) (Section 1.3.1.2.1) contain the extension "Certificate Transparency (CT)" (Section 7.1.11) by default. This extension can also be deactivated on customer request.

4.5 Use of the key pair and certificate

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

The certificate and the corresponding private key may be used only in accordance with the regulations in the individual contract, this CPS, the Subscriber Agreement or the Service and Usage Agreement TeleSec Shared Business CA.

The use of the private key with the corresponding certified public key is permitted only once the end entity has accepted the certificate (Section 4.4.1). Use of the certificate is determined by the tenant's specifications and intended use. The technical certificate usage is defined in the certificate as the "key use" and "extended key use" attribute.

All end entities and registrars are obligated to:

- Protect their private key against unauthorized use
- Refrain from transferring or revealing their private key to third parties, even as representatives
- Refrain from continued use of the private key following expiry of the validity period or revocation of the certificate, other than to view encrypted data (e.g., decrypting e-mails).

For certificates belonging to groups of persons and functions and devices, the following additional requirements apply:

- The key owner (Section 1.3.3) is responsible for copying or forwarding the key to the end entity or entities.
- The key owner must obligate the end entity/all end entities to comply with this CPS when dealing with the private key.
- Certificate revocations can be transferred to individuals from the group of end entities. The key owner must provide those who are authorized to perform revocations with the details of events that lead to revocation and the revocation password.
- After a person leaves the group of end entities (e.g., termination of the employment relationship), the user or key owner must prevent misuse of the private key by revoking the certificate.
- Transfer of the responsibility to a new or additional key owner must be requested from the registration authority responsible, who must document this. The new key owner must be identified and registered in accordance with this CPS and his authorization as a key owner proved.

4.5.2 Use of public keys and certificates by relying parties

Every relying party who uses a certificate issued by the TeleSec Shared Business 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 this CPS. Telekom Security is not responsible for assessing the suitability of a certificate for a specific purpose
- Check the technical usage purpose, which is established via the “key usage” and “extended key usage” attributes shown in the certificate.

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

4.6 Renewal of certificates (re-certification)

Depending on the certificate type, the certificate holder, requester, representative or other instance is informed about the renewal of the certificate by e-mail (renewal notification). This e-mail contains the relevant certificate information.

This notification is sent 30 calendar days before the certificate expires and is repeated multiple times until the certificate has either been renewed or has expired.

For a certificate renewal, the certificate owner will be issued a new certificate with a new serial number, new validity period and the same Subject DN (Section 3.1.1.1).

A certificate renewal function is implemented for user certificates only.

For other certificate types, it is necessary to request a new certificate even if it is still possible to access the original technical request data.

A certificate renewal is only ever possible with a valid certificate and possession of the private key. It is not possible to renew a revoked or expired certificate. A certificate can be renewed with or without generating a new key, depending on the key material (smartcard or soft PSE). However, a prerequisite for using the same key pair is that the unique mapping of the certificate holder and the key is retained, the key is not compromised and the cryptographic parameters (e.g., key length) are still sufficient for the period of validity of the new certificate.

4.6.1 Reasons for a renewal

If no reasons speak against it (e.g., contract termination, name change), the user must procure a new certificate before the validity of his current certificate expires in order to ensure the continuity of the certificate usage.

Renewal is only possible within 30 calendar days of expiry of the existing certificate (user, registrars). For renewal, the certificate must be available including the private key.

4.6.2 Who may request re-certification?

Generally, renewal is at the discretion of the tenant and must be defined in advance as part of the “key backup concept”. Only the user or the key owner may order a renewal.

Re-certification is requested only by registered persons (if the private key is available) or authorized persons (key owner, device administrator). The authorized person has the required login details as well as the certificate service password.

4.6.3 Processing renewals

The renewal procedure must guarantee that only authorized certificate holders (users, key owners) can perform this process.

For the renewal of end entity certificates, possession of the complete key material (certificate and private key) is required as an authentication characteristic.

The certificate owner performs the renewal of registrar certificates (master RA and sub-RA certificates and their derivatives, Section 1.3.2.2.2) himself. Please note that certificates to be renewed are not automatically revoked following the renewal process. The registrar has two valid certificates for a transitional period (renewal time period until the certificate expires). The hierarchically higher level registrar can revoke the certificate to be renewed during this period (Section 4.9.3.3 ff).

When setting up the area of responsibility (sub-domain) a configuration is made regarding whether the end entity certificate to be renewed is automatically revoked at the time of renewal. Thus, the end entity may have two valid certificates for a transitional period (renewal time period until the certificate expires). It is up to the tenant or authorized person (registrar, user) to revoke the certificate to be renewed at the end of this period (Section 4.9.3.2ff).

If a key backup (refer to Section 1.3.2.2.2) is defined, instead of the certificate renewal, the sub-registrar responsible should request a new certificate.

4.6.4 Notification of the certificate owner following a certificate renewal

The regulations in Section 4.3.2 apply.

4.6.5 Acceptance of re-certification

The regulations in Section 4.4.1 apply.

4.6.6 Publication of a renewal by the certification authority

The regulations in Section 4.4.2 apply.

4.6.7 Notification of other instances regarding a certificate renewal by the certification authority

The regulations in Section 4.4.3 apply.

4.7 Re-key of certificates

Renewal of keys for certificates (“re-key”) is another form of requesting the issue of a new certificate using a new key pair. The certificate content and identification data remain unchanged.

Whether key renewal is supported depends on the technical specifications of the application (e.g. web server) and is the customer’s responsibility.

4.7.1 Reasons for a re-key

A re-key makes sense to increase the security level. This measure is at the tenant’s discretion.

Re-certification with re-key can only be carried out during a period 30 calendar days before the certificate expires and only by the authorized customer. The certificate to be extended must not be revoked and not be invalid/expired.

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

The regulations in Section 4.6.2 apply.

4.7.3 Processing of re-key requests

In the case of certificates for users, masters and sub-registrars that meet the specifications from Section 4.7.1, the certificate is issued directly following renewal. Renewal is possible until the requester's certificate data changes (Section 4.8 ff), a reason for revocation occurs or certificate use (Section 4.9 ff) is no longer desired.

For other certificate types (server, router, mail gateway, domain controller), the responsible sub-registrar processes the certificate renewal (key renewal) (Section 4.2.2.2 and 4.3).

4.7.4 Notification of the certificate holder about the issuing of new key material

The regulations in Section 4.3.2 apply.

4.7.5 Acceptance of a renewal with new key material

The regulations in Section 4.4.1 apply.

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

The regulations in Section 4.4.2 apply.

4.7.7 Notification of other authorities regarding a certificate renewal by the certification authority

The regulations in Section 4.4.3 apply.

4.8 Amendment of certificate data

4.8.1 Reasons for a certificate change

It is mandatory to issue a new certificate if the certificate content (with the exception of the public key) has changed in comparison to the certificate that had been issued until now (e.g., C, O, OU1, OU2, OU3, CN, e-mail, also refer to Sections 3.1.1.1.1 to 3.1.1.1.10).

4.8.2 Who may request a certificate change?

The regulations in Section 4.6.2 apply.

4.8.3 Processing certificate changes

If the contents of a certificate change (see Section 3.1), renewed authentication is required, as in the case of a new request (see Sections 3.2.3.3 to 3.2.3.5). The predecessor certificate must be revoked immediately.

4.8.4 Notification of the certificate owner about the issuing of a certificate

The regulations in Section 4.3.2 apply.

4.8.5 Acceptance of a renewal with changed key material

The regulations in Section 4.4.1 apply.

4.8.6 Publication by the CA of a certificate with changed data

The regulations in Section 4.4.2 apply.

4.8.7 Notification of other instances regarding a certificate creation by the CA

The regulations in Section 4.4.3 apply.

4.9 Certificate revocation and suspension

4.9.1 Reasons for revocation

4.9.1.1 Reasons for revocation of an end-entity or registrar certificate

The following circumstances require that the certificate be revoked by the certificate holder or CA:

- The CA receives adequate evidence that the private key has been compromised, lost, stolen or disclosed (this does not apply in connection with a key backup) or there is strong suspicion that this has happened;
- The details in the certificate (except for unverified end-entity information) are no longer up-to-date, are invalid, incorrect, or do not meet the requirements for naming (see Section 3.1 ff). This also applies to domain names that are no longer owned by the domain owner or that have been retrieved by authorized entities (e.g. ICANN) (e.g., generic top-level domains (gTLD);
- The former internal top-level domain becomes a public top-level domain (collision of domain names),
- The certified key (public key) or the cryptographic algorithms used with it no longer meet current requirements;
- A case of misuse by the persons authorized to use the key has occurred or is suspected to have occurred;
- Use and handling of the certificate that violates contractual regulations or these CPS (in particular section 1.4.2);
- The certificate was not issued in accordance with this CPS.
- The certificate was issued in violation of the then-current version of these requirements.
- The CA obtains reasonable evidence that the certificate has been used for a purpose outside of that indicated in the certificate or in the CA's Service and Usage Agreement;
- The CA receives notice or otherwise becomes aware that a subscriber has violated one or more of its material obligations under the Service and Usage Agreement or subscriber agreement;
- Revocation of the certificate to be renewed following the renewal process;
- On expiry or termination of the contract between the tenant and the end entity, if there is no agreement to the contrary;
- Legal specifications or court verdicts justify certificate revocation;
- The certificate is no longer required or the certificate holder expressly requests the revocation of the certificate;

The CA revokes end entity and registrar certificates within 24 hours if at least one of the following reasons applies:

- The Subscriber requests in writing that the CA revoke the Certificate;

- The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
- The CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
- The certification authority attains knowledge about that which should not be dependable validation of the domain authorisation or domain control for a completely certified domain name or an IP address in the certificate;

The CA revokes end entity and registrar certificates within 5 days if one or more of the following occurs:

- The certificate complies no longer with the requirements of Sections 6.1.5 or 6.1.6;
- The CA obtains evidence that the Certificate was misused;
- The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Service and Usage Agreement TeleSec Business CA;
- The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
- The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
- The CA is made aware of a material change in the information contained in the Certificate;
- The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;
- The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository
- The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate (all certificates issued by this sub-CA are revoked);
- Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement;
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time);
- The certification authority becomes aware that there is a method by which the private key corresponding to a public key can be easily calculated. (comparable to the Debian weak key, http://wiki.debian.org).
- There are legal regulations or adjudications or instructions of a supervisory authority.

The CA revokes end entity and registrar certificates within 120 days,

- if the certificate contains a domain name with a gTLD that has been withdrawn by authorized entities (e.g. ICANN).

4.9.1.2 Reasons for revocation of a sub-CA certificate

The Trust Center of Telekom Security revokes a sub-CA certificate within 7 hours if at least one of the following reasons exists:

- The Subordinate CA requests revocation in writing;
- The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
- The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6,
- The Issuing CA obtains evidence that the Certificate was misused;
- The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
- The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate
- The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
- Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement; or
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).
- The issuing CA SHOULD revoke a certificate after evaluation or a time limit if one or more of the following occurs

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

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

4.9.2 Who can request that a certificate be revoked?

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

- Authorized persons of an external registration authority (master registrar, Section 1.3.2.2.1)
- Authorized persons of an external registration authority (sub-registrars and their derivatives, Section 1.3.2.2.2)
- Authorized persons who are listed as the subject of the certificate
- Authorized persons from groups of persons and functions and devices
- Authorized persons who act as key owners or are authorized to perform revocations
- Authorized persons from the internal registration authority of Telekom Security in the scope of setting up and managing a master domain (Section 3.2.2).
- Any natural person who would like to report a suspicion of misuse of a certificate.

The following persons are normally authorized to initiate the revocation of a sub-CA certificate:

- Authorized person(s) of the PKI TeleSec Shared Business CA (e.g., Change Advisory Board of Telekom Security)

4.9.3 Procedure for revocation request

4.9.3.1 Revocation types

Depending on the role and authorization, the subscribers to this PKI (Section 1.3.2 ff, 1.3.3, 1.3.4 and 1.3.5) have various ways of revocation (24x7) available to them. Certificates can be revoked via

- The user website for all users (except master and sub-RA and their derivatives (Section 1.3.2.2.2))
- The sub-RA website for all users and devices (except master and sub-RA and their derivatives)
- The master RA website for all users, devices and sub-registrars (incl. derivatives, except master RA)
- The Service Desk of Telekom Security revocation service website for master RAs only and
- Optional: CMP interface.

Table 16 to Table 19 presents the revocation types depending on the certificate types (Sections 1.3.2.2 ff and 1.3.3).

Table 16: Revocation options Master registrar certificate

Certificate type:	Master registrar certificate
Revocation via:	Revocation service website of the Service Desk

Table 17: Revocation options Sub-registrar certificate and derivates

Certificate type:	Sub-registrar certificate and derivatives
Revocation via:	Master registrar website

Table 18: Revocation options User certificates

Certificate type:	User certificates
Revocation via:	Sub-registrar website, Master registrar website, User website, CMP interface

Table 19: Revocation options Device certificates

Certificate type:	Devices (e.g., servers, routers/gateways)
Revocation via:	Sub-registrar website, Master registrar website, CMP interface

Regardless of the above revocation type, the Trust Center of Telekom Security reserves the right to revoke certificates if at least one of the revocation reasons listed in Section 4.9.1 applies.

4.9.3.2 Revocation of end-entity certificates

A certificate revocation can be initiated 24x7 via one of the ways of revocation listed in Section 4.9.2. Here, it is sufficient that one of the revocation reasons listed in Section 4.9.1.1 applies.

In every case, the content of the certificate owner's Subject DN (e.g., Common Name) is required in order to select the certificate to be revoked. The revocation is authenticated using the revocation password that the certificate owner knows.

The revocation is permanent. After this, the master or sub registrar or the revocation service operator has to generate a new certificate revocation list (CRL) manually. Otherwise the revocation will only be published in the certificate revocation list (CRL) during the daily cycle of the CA system (Section 4.9.7). Following the revocation, the revocation information is immediately available via OCSP.

The CA revokes certificates if at least one of the reasons for revocation listed in Section 4.9.1.1 applies.

Telekom Security enables end entities, relying third parties (e.g., software manufacturers) and other subscribers to report suspicions of compromised keys, certificate misuse or other (attempted) fraud in relation to certificates.

Within 24 hours after receiving a certificate problem report, the Telekom Security will investigate the facts and circumstances related to a certificate problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the certificate problem report.

After reviewing the facts and circumstances, the CA shall work with the certificate holder and any entity reporting the certificate problem report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate. The period from receipt of the certificate problem report or revocation-related notice to published revocation must not exceed the time frame set forth in section 4.9.1.1.

The further procedure is determined by the following criteria:

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

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

4.9.3.2.1 Revocation of user certificates

The following role owners and websites or interfaces are involved in revoking user certificates (Section 4.9.3.1):

- The user using the relevant user website.
- The sub-registrar responsible (or his derivative).
- The master registrar responsible via the master registrar website.
- Optional: CMP interface.

4.9.3.2.2 Revocation of device certificates

The following role owners and websites or interfaces are involved in revoking device certificates (Section 4.9.3.1):

- The user using the relevant user website.
- The sub-registrar responsible (or his derivative).
- The master registrar responsible via the master registrar website.

- Optional: CMP interface.

4.9.3.3 Revocation of registrar certificates

4.9.3.3.1 Revocation of master registrar certificates

The following role owners and websites or interfaces are involved in revoking master registrar certificates (Section 4.9.3.1):

- The Service Desk of Telekom Security via the revocation service website.

4.9.3.3.2 Revocation of a sub-registrar certificate or its derivatives

The following role owners and websites or interfaces are involved in revoking master registrar certificates (Section 4.9.3.1):

- The master registrar responsible via the master registrar website.

4.9.3.4 Revocation of certificates to support PKI operation

The web server and OCSP certificates described in Sections 1.3.1.3.1 and 1.3.1.3.2 are used to support operation of the TeleSec Shared Business CA PKI.

Requests for these certificates to be revoked are reported to the Service Desk of Telekom Security. The current contact data of the Service Desk can be found in the “Service Level Agreement” (SLA) document.

4.9.3.4.1 Revocation of external web server certificates

Telekom Security is obligated to revoke the SBCA website web server certificate (Section 1.3.1.3.1) as soon as suspicion of a compromised key arises. Telekom Security 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. The revocation is announced via the certificate revocation list (CRL). A revoked web server certificate is replaced with a new one immediately.

Telekom Security blocks access to the web server if its security is put at risk by the revocation of this certificate.

4.9.3.4.2 Revocation of the OCSP responder certificate

Telekom Security is obligated to revoke the OCSP responder certificate (Section 7.3 ff) as soon as suspicion of a compromised key arises. Telekom Security 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. The revocation is announced via the certificate revocation list (CRL). A revoked web server certificate is replaced with a new one immediately.

4.9.3.5 Revocation of sub-CA certificates

Telekom Security is obligated to revoke the sub-CA certificate (Section 1.3.1.2 ff) as soon as suspicion of a compromised key arises or specifications require this.

There is an internal Telekom Security business process for the revocation of sub-CA certificates.

4.9.4 Revocation request grace period

4.9.4.1 Service Desk of Telekom Security

After the Service Desk of Telekom Security receives a complete revocation order (only for master registrar certificates or in the event of misuse), Telekom Security revokes the end entity and registrar certificates within 24 hours and publishes this in the certificate revocation list (CRL) and the OCSP database.

4.9.4.2 External registration authority and tenant's revocation service (optional)

The delegated third party is responsible for ensuring that revocation deadlines are adhered to. As soon as a revocation reason in accordance with Section 4.9.1 applies for end entity certificates, the end entity, key owner or person authorized for revocations must place the revocation order as soon as possible within an economically viable deadline.

4.9.5 Time within which CA must process the revocation request

Revocation via the respective websites is available to end entities, registrars, key owners and Service Desk of Telekom Security employees responsible for revocation round the clock and is forwarded to the connected systems immediately after the revocation procedure. The OCSP service that uses these systems therefore has access to the current certificate status.

4.9.6 Checking requirements for relying parties

Relying parties must be given the opportunity to check the status of certificates. The OCSP responder can be used for this purpose. This transmits the current status of an end entity, registrar or OCSP certificate.

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 SBCA's directory service.

Revoked CA certificates (except root CA certificates) are published in the standardized certificate authority revocation list (CARL) and can thus be checked using applications that comply with the standard.

Telekom Security ensures that the revoked certificate is at least included in the next CRL even after it expires.

4.9.7 Publication frequency of revocation information

The certificate revocation list (CRL) and certification authority revocation list (CARL) are published via the directory service, as described in Section 2.3.

The certificate revocation list (CRL), which contains the certificate revocations of end entities, is updated automatically at least once a day by the CA system and published via the directory service. Within this automatic cycle, the tenant/external registration authority can generate the certificate revocation list (CRL) manually through the master and sub-registrar role owners.

All revoked CA certificates (no root CA certificates) that are issued by the certification authority (root CA) in question are published in the revocation lists for certification authorities (CARL). Figure 1 presents the root and subordinated certification authorities (sub-CAs) in the form of a graph. All CARLs are updated after three (3) months at the latest or within 24 hours of revocation of a subordinate CA certificate, depending on the event. Publication takes place via the corresponding directory service.

4.9.8 Maximum latency period of revocation lists

The latency period of the certificate revocation list (CRL) following automatic generation is a few minutes.

The latency period for the certification authority revocation list (CARL) following manual publication is a few minutes.

4.9.9 Online availability of revocation/status information

In addition to the revocation information via the CRL and CARL (Sections 2.3, 4.9.7), Telekom Security provides online information regarding the certificate status via OCSP. The URL of the OCSP responder is listed in the certificate under the “Authority Information Access” extension (see Section 7.1.2.9). The OCSP responses output by the SBCA for end entity certificates meet the specifications of RFC6960.

4.9.10 Requirements for an online checking process

Relying third parties have to check the status of a certificate that they wish to rely on. 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).

The OSCP responder supports the GET method.

The OCSP data source (repository) for end entity certificates is updated after ten (10) minutes at the latest. The OCSP responses are valid for a maximum of five (5) days.

The OCSP data source (repository) for sub-CA certificates will be updated after six (6) months at the latest. Once a CA certificate has been revoked, the update takes place within twenty-four (24) hours.

The OCSP responder reply to requests for certificate serial numbers with "unknown" if they cannot be assigned to the PKI service „TeleSec Shared Business CA”.

The TSP monitors the OCSP responder as part of its security responsibility for requests for "unused" serial numbers.

4.9.11 Other available forms of publishing revocation information

Depending on the certificate type, the certificate holder, requester, representative or other instance is informed about the revocation of the certificate by e-mail (revoke notification). This e-mail contains the relevant certificate information.

4.9.12 Special requirements for compromised private keys

Parties that want to report a key compromise are requested to use the contact options described in Section 1.5.2. They have to provide sufficient information or references to information that is proof for a compromise, e.g. provide a CSR signed by the compromised private key with a commonName of “Compromised Key”. The effected certificate itself should be referenced as well.

If a private key is compromised, the relevant certificate must be revoked immediately (Section 4.9.1).

4.9.13 Suspension of certificates

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

4.9.14 Who can request that a certificate be suspended?

No stipulation.

4.9.15 Suspension procedure

No stipulation.

4.9.16 Limitation of the suspension period

No stipulation.

4.10 Status information services for certificates

The status of end entity and registrar certificates is available directly via the OCSP service (Sections 2.1 and 2.2) and the certificate revocation list (CRL).

4.10.1 Operating characteristics

The OCSP responses are signed by an OCSP responder, whose certificate is in turn signed by the intermediate certification authority (subordinate certification authority, sub-CA) that issued the end entity certificate in question.

Figure 1 presents the relevant assignments of the end entities to the root and subordinate certification authorities (sub-CAs) in the form of a graph.

The OCSP response contains one of the following statuses:

- good means:
  - it is an issuer of the PKI service and
  - the certificate is valid (within the certificate validity time) and
  - the certificate is not revoked.
- revoked means:
  - it is an issuer of the PKI service and
  - the certificate is valid (within the certificate validity time) and
  - the certificate has been revoked
- unknown means:
  - the certificate is invalid (outside the certificate validity term) or
  - the certificate is valid but has not been issued by the queried issuer of the PKI service or
  - the certificate is valid, but was not issued by the issuer of the PKI service.

The OCSP responder's certificate contains the extension described in Section 7.3.2.

The certificate revocation list (CRL) issued by the SBCA meets the specifications of RFX 5280.

The respective sub-CA issues and publishes the certificate revocation lists (CRL), while the root CA issues, signed and publishes the revocation lists for certification authorities (CARL) on the LDAP directory service. Figure 1 presents the respective assignments of the issuing root and subordinate certification authorities (sub-CAs) in the form of a graph.

Telekom Security has implemented mechanisms to protect the revocation status service (CRL, CARL, OCSP) against unauthorized attempts to prevent manipulation of revocation status information (add, delete, change).

The TSP does not offer OCSP stapling.

4.10.2 Availability of the service

Both the OCSP service and the CRL/CARL on the LDAP directory service are available around the clock. Under normal operating conditions, the response time of the OCSP responder and the LDAP directory service is less than ten seconds.

4.10.3 Optional functions

No stipulation.

4.11 Termination of the contractual relationship

In the event that the tenant or Telekom Security terminates a contract, first the provided certificate types are deactivated. As a consequence, it is also not possible to request new end entity certificates or renewals. It is still possible to log in to the website to revoke existing certificates. With the deactivation of the master domain, all functions for logging into the website in question, issuing of new certificates, renewal and revocation of certificates are prevented; however, certificate validation via the certificate revocation list and OCSP is still supported.

Certificates that were subject to a fee in accordance with the Classic and Classic Pro tariff model remain valid until the validity of the certificate expires. Renewal is not possible.

Certificates that were subject to a fee in accordance with the Advanced tariff model are revoked after the termination date and become invalid. A special transitional rule can be agreed in the individual contract in question.

If an external registration authority is terminated or terminated (e.g. termination of contract, name change, bankruptcy), the customer must meet his archiving obligation (Section 5.5 ff) At the request of the TSP, the customer must grant access rights to this data free of charge. In the event of insolvency (bankruptcy), the customer must inform the TSP in good time and immediately grant access rights to this data free of charge.

4.12 Key storage and restoration

The key pairs of the subordinate certification authorities (sub-CA) (see Figure 1) used in the scope of the „TeleSec Shared Business CA" PKI service are saved on a security-checked hardware security module (HSM) and operated in a secure environment. The key material is only stored on further HSMs for key back-up purposes, so that qualified and security-checked staff (trusted role) at the Trust Center can restore and maintain the service. Key storage (Escrow) at third parties (e.g., trustee, notary) is not implemented.

4.12.1 Guidelines for key storage and restoration

No stipulation.

4.12.2 Session key encapsulation and guidelines for restoration

No stipulation.

5 BUILDING, ADMINISTRATION AND OPERATION CHECKS

The Trust Center of Telekom Security is housed in a specially protected building and operated by expert 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 Trust Center of Telekom Security.

The physical, organizational and personnel-related security measures applied are defined in a security concept [SBCA security concept], with their effectiveness being demonstrated on the basis of a threat analysis.

The security measures required for operational purposes are described in the service and organization manual, system manual as well as in the operating guidelines for the Trust Center.

The requirements from [ETSI EN TSP] Sections 5, 6.3 and 7.3 are implemented, i.e. specifications are outlined in relation to:

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

Management approves the risk assessment and accepts the identified residual risk.

5.1 Physical checks

5.1.1 Location and structural measures

Telekom Security own services are operated in data centers that meet the Group specifications regarding technical and physical security.

The Trust Center of Telekom Security is located in data centers at two geo-redundant sites in Germany that are a minimum distance of more than 10 km apart.

In the data center in question, the Trust Center of Telekom Security is set up in a separate area (cage) and secured by means of an access control system.

The Trust Center or data center is set up and operated in observance of the relevant guidelines of the Federal Office for Information Security (BSI) and the German Association of Indemnity Insurers (Verband der Schadenversicherer e.V., VDS)/new: German Insurance Association (Gesamtverband der Deutschen Versicherungswirtschaft, GDV), the pertinent DIN standards on fire protection, smoke protection and blocking of attacks. The Trust Center is accepted by VdS/GDV in terms of security technology.

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

5.1.2 Physical access

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

5.1.3 Power supply and air conditioning

The suction openings for outside air are arranged in such a manner that pollutants such as dust or dirt as well as corrosive, poisonous, or highly flammable gases cannot enter. The systems are operated using a very low proportion of outside air. The required fresh air openings are access-protected. Filters are installed to protect against air pollution resulting from floating particles. The fresh air intake is continuously checked for aggressive gases. In the event of an emergency (e.g., fire in the surrounding area), the fresh air intake is automatically closed by means of air flaps.

To protect against power supply failure, an independent alternating current supply is installed in accordance with VDE regulations. It provides protection against variations in voltage, short-term bridging that is free of interruptions as well as long-term bridging with two separate stationary emergency generators with a performance corresponding to the full load of the data center.

5.1.4 Water risk

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

5.1.5 Fire safety

The applicable fire regulations (e.g., DIN 4102, requirements of the local fire department, regulations regarding fire resistance, VDE-compliant electrical installation) are complied with. All fire doors have automatic locking mechanisms. As agreed with the fire department, water will only be used to put out fires in extreme emergencies.

Fire sections are secured by fire-resistant components. Passages through fire protection walls are equipped with self-closing fire doors.

In areas with double floors as well as suspended ceilings the fire protection walls go right through to the ceilings/floors of the story.

Early fire detection systems (suction systems) are installed in all system rooms, system operator rooms, archive rooms, UPS rooms and in other selected rooms. The supply air and exhaust air of the air conditioning devices in the individual rooms are monitored. Fire alarms are installed in the other rooms. Any fire is extinguished using inert gas.

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 Telekom Security' regular disposal guidelines.

5.1.8 External backup

Telekom Security 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 measures

The organizational measures are set out in the Framework security concept of the Trust Center information network [FSC TC] and are implemented on the basis of the Trust Center's operations plan. The relevant requirements from [ETSI EN TSP] Section 7.4 b, c, d, e are implemented.

5.2.1 Trustworthy roles

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

- The validation of information in certificate requests
- The acceptance, rejection or other processing of certificate requests, revocation requests or renewal requests
- The issue or withdrawal of certificates, including staff who have access to the database systems
- The handling of information or requests from end entities.

Trustworthy persons are in particular:

- Trust Center staff (e.g., system administration, internal registration authority employees)
- Employees of the tenant's registration authority (external registration authority employees)
- Staff of cryptographic departments
- Security personnel
- Responsible technical personnel and
- Managerial staff responsible for managing the trustworthy infrastructure.

The abovenamed trustworthy persons must fulfill the requirements set out in this CPS (see Section 5.3.1) and the respective role (s) must be assigned. With a written confirmation (e.g. via email), these people accept their assigned role (s). This evidence MUST be archived for at least 7 (seven) years.

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

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

5.2.2 Number of involved persons per task

The operational maintenance of the certification instance and directory service is carried out by expert and trustworthy persons.

Work on highly sensitive components (e.g., key generation system, HSM) is governed by special internal control procedures and carried out by at least two members of staff.

In the event of a fault, the Trust Center system administrators have additional master and sub-registrar or Trust Center operator rights for the purpose of resolving the fault.

5.2.3 Identification and authentication for every role

5.2.3.1 Trust Center employees

Telekom Security internal registration authority employees who are classed as particularly trustworthy and who carry out particularly trustworthy activities, are subject to a Telekom Security internal security check (see Section 5.3.2).

Telekom Security 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 SBCA and other IT systems
- Are permitted to carry out certain tasks in connection with these systems

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

5.2.3.2 Employees of the external registration authority

The tenant/external registration authority must ensure that only trustworthy persons (master or sub-registrar) perform the registration authority tasks.

5.2.4 Roles that require a separation of functions

The following roles are subject to a separation of functions:

- Creating, installing or destroying sub-CA and root CA certificates
- Backing up and restoring databases and HSMs

5.3 Staff measures

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

The personnel are not subject to any cost pressure, quantity structure or other restrictions that may pose a challenge to the quality requirements when checking request documents.

5.3.1 Required qualifications, experience and security checks

5.3.1.1 Employees of Telekom Security

For the operation of the PKI services described in Section 1, Telekom Security requires that its employees who are to assume a trusted role submit relevant evidence of qualifications and experience that are necessary for them to perform their planned work obligations in a competent and satisfactory manner.

A new certificate of good conduct must be submitted to the staff supervisor at regular intervals.

5.3.1.2 Employees of the external registration authority

The tenant must ensure that the deployed personnel (master or sub-registrars) are sufficiently qualified and responsible to perform the tasks of a registration authority. It must also be possible to provide evidence of the qualifications and reliability check to auditors.

Before a master registrar certificate is issued, the identity of the master registrar must be proved. For this purpose, the tenant or his representative provides a copy of an identification document belonging to the master registrar.

5.3.2 Security check

5.3.2.1 Employees of Telekom Security

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

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

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

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

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

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

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

5.3.2.2 Employees of the external registration authority

No stipulation.

5.3.3 Education and training requirements

5.3.3.1 Employees of Telekom Security

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

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

- Advanced PKI knowledge
- Procedures according to ITIL

- Data and telecommunications privacy
- Information protection
- Access protection
- Anti-corruption
- Data protection
- Security and operational guidelines and procedures of Telekom Security
- Use and operation of the hardware and software in use
- Reporting and handling of faults and compromises, as well as
- Procedures for disaster recovery and business continuity.

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

- Guidelines, procedures and current developments regarding validation methods
- Contents and particularly relevant amendments to this CPS and the corresponding CP
- Relevant requirements and specifications from the certification standards [CAB-BR]
- General threat and attack scenarios regarding the validation methods (e.g., social engineering)

The training must be documented in writing and the course contents confirmed annually in an examination.

5.3.3.2 Employees of the external registration authority

Telekom Security provides the tenant or master registrar with appropriate training documents that specify the functions, processes and supporting documentation.

The master registrar is obligated to train new registration authority employees in accordance with the requirements before they begin their registration task. This training must be documented in writing and evidence provided to Telekom Security or a delegated third party on request.

As part of quality assessment self-audits, the master registrar holds an annual training session for the sub-registrars responsible including derivatives. This training must be documented in writing and evidence provided to Telekom Security or a delegated third party on request.

5.3.4 Follow-up training intervals and requirements

5.3.4.1 Employees of Telekom Security

The staff of the Trust Center receive refresher training and further training courses to the extent required and at the intervals required. The requirements are reviewed annually and incorporated into the training program.

5.3.4.2 Employees of the external registration authority

In the event that Telekom Security provides new training documents that contain relevant training topics, the master registrar must hold a special training session together with the sub-registrars responsible (and derivatives). This training must be documented in writing and evidence provided to Telekom Security or a delegated third party on request.

5.3.5 Frequency and sequence of workplace rotation

No stipulation.

5.3.6 Sanctions in the event of unauthorized activities

5.3.6.1 Employees of Telekom Security

Telekom Security reserves the right to punish unauthorized activities or other violations of this CPS and the Service and Usage Agreement TeleSec Business CA and procedures described therein, and to implement corresponding disciplinary measures. These disciplinary measures are determined by the frequency and severity of the unauthorized actions and can include measures up to and including dismissal.

5.3.6.2 Employees of the external registration authority

It is up to the tenant/external registration authority to impose penalties for any infringements.

5.3.7 Requirements for independent contractors

Telekom Security 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 Telekom Security in comparable positions.

The above persons, who have not yet concluded or successfully completed the security check described in Section 5.3.2.1, are given access to the secure facilities at Telekom Security only under the condition that they are accompanied and directly supervised by trustworthy persons.

5.3.8 Documentation for the staff

5.3.8.1 Employees of Telekom Security

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

5.3.8.2 Employees of the external registration authority

Telekom Security provides relevant documentation, which provides information on the functions and operation of registration authorities.

5.4 Log events

What data and events are recorded by whom and at what intervals is defined in the logging concept as well as the installation manual.

In addition, rules are laid down that govern how long the log data is stored (currently 6 weeks) and how it is protected against loss and unauthorized access.

Here the requirements under [ETSI EN TSP] Section 7.10 are implemented.

5.4.1 Type of events recorded

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

5.4.1.1 CA key pairs and CA systems

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

- Generation, destruction, saving, back-up and restoration as well as archiving of the key pair or parts of the key pair
- Events in the lifecycle management of cryptographic devices (e.g., HSM) as well as the CA software in use

5.4.1.2 EE and CA certificates

For the lifecycle management of EE and CA certificates and their validation, the Trust Center of Telekom Security logs at least the following events for TeleSec Shared Business CA:

- Request and revocation of certificates
- Request for renewal with and without a change of key (renewal and re-key)
- All activities relating to the verification of information
- The event, as well as the date/time and phone number of phone calls relating to the verification and the name of the contact person
- Acceptance or rejection of certificate orders
- Issuing of a certificate
- Generation of revocation lists (CRL) and OCSP entries

5.4.1.3 Other security-related events

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

- Successful and unsuccessful attempts to access the PKI systems
- Actions performed on and by the PKI and other systems that are relevant for security
- Changes to the security profile
- System crashes, hardware failures and other anomalies
- Firewall and router activities
- When people access and leave Trust Center facilities
- Results of network checks (vulnerability scans)
- Start and end of the logging process

5.4.2 Processing interval of the logs

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

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

5.4.3 Storage period for audit logs

Audit logs/history data/logging files are archived after processing according to Section 5.5.2.

5.4.4 Protection of audit logs

Audit logs/history data/logging files are protected against unauthorized access by means of operating system mechanisms.

5.4.5 Backup procedures for audit logs

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

5.4.6 Audit recording system (internal vs. external)

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

5.4.7 Notification of the subject that triggered the event

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

5.4.8 Assessment of vulnerabilities

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

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

5.5 Data archiving

5.5.1 Type of archived datasets

Telekom Security archives the following data:

- Order documents on paper (e.g., quotations, orders)
- Information in certificate requests and regarding the certificate life cycle (e.g., revocation and renewal requests)
- Soft PSEs that were requested in bulk
- All audit/history data/event logging files recorded pursuant to Section 5.4

5.5.2 Storage period for archived data

The following records and storage periods are stipulated:

- Order documents, in particular information regarding certificate requests, their validation and the certificates resulting from this and revocations executed are retained for seven (7) years after the certificate validity expires.
- Soft PSE that have been requested for in bulk will be max. archived for thirty (30) days,

- Audit, history and event logging data are archived up to forty-two (42) days.

5.5.3 Protection of archives

Telekom Security ensures that only authorized and trusted persons gain access to the data media archives. Archive data is protected against unauthorized read access, changes, deletions or other forms of manipulation.

5.5.4 Backup procedures for archives

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

Telekom Security retains data media that contain archive data and applications that are required for processing the archive data in order to ensure that the archive data is retained for the archiving period specified in this CPS.

5.5.5 Requirements for timestamps of datasets

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

5.5.6 Archive recording system (internal or external)

Telekom Security only uses internal archiving systems.

5.5.7 Procedures for obtaining and checking archive information

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

5.6 Key change

Certificates become invalid once the validity period has expired.

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

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

A key change for registrar and end entity certificates is the tenant's responsibility. New certificates and their fingerprints are published (see Section 2.3).

The generation of new CA and root CA keys as well as OCSP responder 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).

Telekom Security immediately informs all tenants before the new CA and root CA certificates are integrated into the relevant services to ensure a smooth transition from the old to the new key pair.

Expired or revoked CA and root CA certificates are available on the website for validation until the last end-entity certificate has expired and has been deleted following the statutory archiving period.

5.7 Compromised situations and disaster recovery

5.7.1 Handling of incidents and compromised situations

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

Telekom Security has established an IT service management in accordance with ITIL and ISMS processes that evaluates problems and security incidents in line with defined standard processes.

By stipulating all required contacts and appropriately established groups in the IT service management system as well as establishing an on-call service and the MoD (Manager on Duty), it is ensured that the handling of faults and security incidents begins promptly, so that damage is minimized and can be eliminated quickly.

The TeleSec Shared Business CA has a service level agreement (SLA) in which the fault process is described in detail.

The end entity submits faults to the Service Desk via the contacts defined in the service level agreement (SLA) and they are then processed as part of service management.

The Service Desk staff first evaluates the fault based on the fault classes defined in the service level agreement (SLA) before the fault is entered into the Telekom Security fault resolution application, prioritized and forwarded to the functional department(s) for fault resolution. All the information is saved in the IT application in a transparent and audit-proof manner so that the processing status of the fault can be traced at any time up until resolution.

The functional department informs the Service Desk about the processing status in accordance with the fault class so that the Service Desk can provide the delegated third party with relevant information.

If required, affected customers are informed as quickly as possible – but at the latest within 24 hours - and integrated in the process.

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 security department (to the information security officer). The event initiates a corresponding escalation, incident investigation, incident response and finally incident resolution. Disaster recovery is carried out depending on the incident classification.

All hardware and software that is required for provision of the TeleSec Shared Business CA PKI service is available as an asset and application in Telekom Security' configuration management.

This application also forms the basis for problem management.

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

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

The tenant is informed about the potentially compromised key in writing (see Section 2.3 for information on this). If necessary, the certificate(s) must be immediately revoked and the corresponding certification authority revocation list (CARL) generated and published. The generation of new keys and certificates must be documented in accordance with the work

instructions and monitored in accordance with the conditions of the relevant security plan. New certificates and their fingerprints must be published (see Section 2.3).

5.7.4 Business continuity after an emergency

Telekom Security has developed, implemented and tested an emergency plan for data center operation in order to alleviate the effects of catastrophes of all kinds (natural catastrophes or catastrophes of human origin) and to restore the availability of critical business processes as quickly as possible. This also includes all Trust Center processes, components, systems and services. This plan is checked, tested and updated accordingly at least once a year to enable a targeted and structured response in the event of a catastrophe.

The emergency plan contains at least the following information:

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

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

5.8 Cessation of a certification or registration authority's operations

5.8.1 Cessation of the certification authority

Only Telekom Security can announce the cessation of operations at the Telekom Security certification authority (Section 1.3.1 ff) or internal registration authority (Section 1.3.2.1).

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

- Notification of tenants, 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 involved Sub-CA certificates
- Any transitional regulations required for a successor CA
- Reimbursement of costs depending on the content of existing individual agreements
- Retention of the documentation and archives of the certification authority (CA)

All possible measures will be taken prior to cessation of the service in order to minimize the potential damage for all concerned. 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, relying third parties, registration authorities of tenants and Telekom Security) as soon as possible.

Following this, all certificates that are still valid must be revoked. All rights are then withdrawn from the employees of the certification authority and the registration authorities, and the private keys of the CA are destroyed.

All electronically recorded data is deleted with the exception of the certificates and revocation lists. The certificates and revocation lists as well as paper documents are archived so that they can be accessed as evidence in court cases should this be necessary.

5.8.2 Cessation of the external registration authority

A tenant's registration authority (external registration authority) (Section 1.3.2.2) ceases operations following termination either by the tenant themselves or by Telekom Security. In addition, Telekom Security can deactivate a PKI tenant in the event of a serious breach of duty (e.g., misuse, multiple prosecuted violations of this CPS) on the part of the owner, his or her employees or commissioned third parties.

The internal registration authority initially deactivates the issue and renewal of end-entity certificates. The end-entity certificates are revoked in agreement with the customer. In the event of a serious breach of duty (e.g., misuse, multiple prosecuted violations of this CPS), Telekom Security is entitled to revoke all of a tenant's end-entity certificates immediately.

6 TECHNICAL SECURITY CONTROLS

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

6.1 Generation and installation of key pairs

6.1.1 Generation of key pairs

All key pairs for CA certificates are generated and stored by trained and trustworthy specialist staff (trusted roles) in a low-radiation room on a security-checked hardware security module (FIPS 140-2/level 3-evaluated) in what is known as the “key ceremony”.

In the case of CA and root CA certificates for advanced certification authorities, the private keys are generated and stored on an evaluated HSM (FIPS 140-1/level 3-evaluated).

All activities during the key ceremony are logged and signed by all persons involved. These records are stored for auditing and tracking purposes for a period deemed suitable by Telekom Security.

The key pair for a certificate for a public certification authority (public root) and the corresponding certificate for an intermediate certification authority (sub-CA) are generated on the offline CA and the assigned cryptographic hardware security module (HSM) under the supervision of an independent and qualified auditor.

The key pair for an intermediate certification authority (sub-CA) is generated on the cryptographic hardware security module (HSM) assigned to the TeleSec Shared Business CA in online operation. The corresponding intermediate certification authority certificate is generated on the offline CA.

All keys generated and certificates issued on the offline CA are logged by means of a verification log and video recording and documented in an audit-proof manner.

The offline CA systems– consisting of a certification instance, cryptographic hardware security module (HSM) (incl. backup token) and browser – are operated “offline”, i.e., without a connection to any network structure. The systems of the offline-CA are kept in a lockable computer rack and secured against opening and replacement. The seal is checked and documented every time the offline-CA is used.

The internal registration authority of Telekom Security usually generates master registrar certificates using the key on the smartcard.

The following rule applies to the issue of the sub-registrar certificate:

- In case that end entity certificates are to be issued by a public certification authority (Section 1.3.1.2.1), the sub-registrar certificate must be issued on a smart card. This regulation does not apply to the derivatives of the sub-registrar certificate (Section 1.3.2.2.2).
- For end entity certificates that are to be issued by an internal certification authority (Section 1.3.1.2.2), the sub-registrar certificate may also be issued as a soft PSE.

The tenant is responsible for generating the end entity key pairs. He can use the keys on a smartcard or the keys generated in the operating system, browser or an application (e.g., server, OpenSSL).

The TeleSec Shared Business CA bulk function is an exception. Here, the key pair is generated via a key generator in the CA.

6.1.2 Assignment of private keys to end entities

The tenant or a person authorized by the tenant (master or sub-registrar) assigns private keys to end entities via a secure method (e.g., personal assignment). Pre-personalized smartcards must require

a PIN letter and must be sent to the end entity separately via a secure method. To protect the private key, the soft PSE must be assigned a secure password.

The tenant is responsible for deciding the delivery method. The receipt of the end entity's smartcard or soft PSE must be documented. To increase security, we recommend sending at different times via a commercial postal service.

In the event that the end entity generates the key pair himself via the operating system or application or uses a different key medium (pre-encrypted smartcard), no private key is assigned to the end entity.

6.1.3 Assignment of public keys to certification authorities

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

6.1.4 Assignment of public certification authority keys to relying parties

The “T-TeleSec GlobalRoot Class 2” root certificate that is required to form the chain of trust (certificate validation) is made available to all end entities and relying parties by means of embedding in the common certificate stores of the operating systems and applications.

The “Deutsche Telekom Internal Root CA 1” and “Deutsche Telekom Internal Root CA 2” root certificate that is required to form the chain of trust (certificate validation) has to be subsequently installed in the certificate stores.

The sub-CA certificate that is subordinate to the root certificate in question is either sent by the sender (source) as part of a signature or authentication by the application for certificate validation or has to be subsequently installed in the certificate stores in question.

All root certificates and sub-CA certificates are available for download on the public website www.telesec.de, on the TeleSec Shared Business CA role-specific websites (master and sub-registrar, user) and on the directory service.

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.

All certificates (intermediate certification authority, end entity) that are issued by a public root certification authority, including this certificate itself, complied with the specifications of the version of the Baseline Requirements [CAB-BR] that was valid at the time of release and publication.

The internal root and intermediate certification authority certificates have an RSA key length of at least 2,048 bits (Section 1.3.1.1.1 and 1.3.1.2.1).

All end entity certificates that are issued by an internal intermediate certification authority (Section 1.3.1.2.2) must have an RSA key length of at least 1,024 bits.

Telekom Security recommends using a sufficient key length of at least 2,048 bits for registrars.

The key length based on elliptic curve cryptography (ECC) is 256 or 384 bits, depending on the curve parameters.

6.1.6 Generating the parameters of public keys and quality control

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

- The cryptographic method RSA or ECC is used for the key generation.

- The signature algorithm RSA with SHA-256, RSASSA-PSS with SHA-256 or ECDSA with SHA-256 is used for the certificate generation.
- The algorithm parameter of the public key is used:
  - RSA 05 00
  - ECC prime256v1 (also known as secp256r1, NIST P-256) or ECC secp384r1 (also known as NIST P-384)
- SHA-256 is permitted as a signature hash algorithm, SHA-1 is only allowed as a signature hash algorithm when using an internal certification authority.
- Is the minimum length of the RSA key 2,048 bits (for restrictions see Section 6.1.5), the length of the ECC key is 256 or 384 bits.
- The check of the public exponent corresponds to the specifications of the current Baseline Requirements [CAB-BR].
- The public key is not a Debian weak key.
- For server certificates that are to be issued under a public certification authority (CA), the zLint and crt.sh tests were successfully carried out.

If one of the parameter checks fails, the corresponding certificate request is rejected with an information text.

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

See Section 7.1.2.1.

6.2 Protection of private keys and technical checks of cryptographic modules

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

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

6.2.1 Standards and checks for cryptographic modules

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

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

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

Telekom Security has implemented technical, organizational, and procedural mechanisms that require the participation of several trustworthy and trained persons of the Trust Center of Telekom Security (trusted roles) to be able to carry out confidential cryptographic CA operations. The usage of private keys is protected by a divided authentication process (Trusted Path Authentication with Key) known only to the persons responsible for it. Every person involved in the process has secrets that only enable certain activities in their entirety.

6.2.3 Storage of private keys

Private keys (CA and root CA keys) are not stored with trustees outside Telekom Security (Section 4.12 ff).

6.2.4 Backup of private keys

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

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

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

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

Telekom Security does not save copies of private keys for the master and sub-registrar certificate.

The tenant must take security precautions to ensure that only the end entity or authorized personnel (e.g., sub-registrars and derivatives, Section 1.3.2.2.2) can request, back up and download key material via the website.

Restoration of the end entity key material is permitted provided the end entity or key owner agrees to the restoration. If this permission is not granted, the tenant may still have the restoration performed if there are legal reasons for this such as:

- Requirements in legal or official proceedings
- In the scope of criminal investigations
- Legal or government regulations
- Tenant's organizational directives

6.2.4.1 Securing and restoring the encryption key using enrollment software

When personalizing the smartcard using suitable enrollment software, the sub-registrar can save both the password-protected soft PSE (private key encryption key incl. encryption certificate) and the corresponding password file (contains the password for the soft PSE) in encrypted form.

To comply with the dual control principle, the soft PSE and the password file have to be separately encrypted on dedicated certificates that are used exclusively in the backup and restoration process.

We recommend encrypting the soft PSE on certificate no. 1 and the password file on certificate no. 2. To restore, decrypt the password file with the private key from certificate no. 2. Then decrypt the soft PSE using certificate no. 1. The soft PSE can only be imported into the certificate store once the password has been entered.

6.2.4.2 Backing up and restoring soft PSEs via the operating system

When backing up soft PSEs that have been issued by an internal certification authority (Section 1.3.1.2.2), the key material can be exported via the operating system (certificate store) and saved at the tenant's premises in encrypted form. The tenant selects a storage medium that meets his requirements.

The soft PSE is saved in encrypted form with a session key and secured with a password. The password must be entered to use the soft PSE.

6.2.4.3 Backing up and restoring soft PSEs via the bulk function

Key materials and password files that are generated via the bulk function remain encrypted and are saved in the Trust Center of Telekom Security. The sub-registrar can also download these within a defined period.

The sub-registrar authenticates himself to the website using a certificate (TLS/SSL client authentication). The soft PSE and password are also available to download by entering the processing number (Bulk ID).

6.2.5 Archiving of private keys

In the event that the validity period of certificates of the root certification authority, intermediate certification authority (sub-CA) or the OCSP service is exceeded, the key material for the certificate in question shall be destroyed. This is not archived.

The Trust Center of Telekom Security archives copies of end entities' private keys within a defined period:

- That the CA system generated as part of an automated mass generation of user certificates (bulk, see Section 3.2.3.4) and that are to be accessible at a later time.

The archiving of private keys of end users whose certificates were issued by a public certification authority (Section 1.3.1.2.1) may not be archived by the master or sub-registrars of the tenant.

6.2.6 Transfer of private keys in or by a cryptographic module

The key material for an intermediate certification authority (sub-CA) certificate is generated on a cryptographic hardware security module (HSM) in online operation. The public keys to be certified with the data of the subject DN are transferred in electronic form (PKCS#10 request) via secure means to the offline-CA, which generates the sub-CA certificate. The sub-CA certificate is then transferred to the HSM via secure means and assigned to the private key. The transfer of the key material and the corresponding sub-CA certificate between the HSM in online operation is carried out in encrypted form.

Private keys cannot be exported for smartcards that already contain keys or that generate keys themselves. During a key back-up, only the key material from the encryption certificate can be imported to the card.

6.2.7 Storage of private keys on cryptographic modules

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

Smartcards save externally generated or self-generated keys in a secure form.

6.2.8 Method for activating private keys

All end entities (incl. registrars) and key owners must protect the activation data (e.g., PIN, import password) for their private key or one they have been entrusted with against loss, theft, change, disclosure and unauthorized usage in accordance with this CPS.

The private key for the certificate within an intermediate certification authority (sub-CA) remains active until the validity period has been exceeded or a there is a revocation reason that triggers revocation of the certificate.

6.2.8.1 Private keys of end entities and sub-registrars (and their derivatives)

The end entity including the sub-registrar (and its derivatives, Section 1.3.2.2.2) must comply with the following specifications to protect the private key:

- A password or a PIN must be set (according to Section 6.4.1) or a similar security measure must be implemented in order to authenticate the end entity or sub-registrar prior to activation of the private key. This can also include a password for operating the private key, for example. The previous condition does not apply for device certificates.
- Economically suitable measures must be taken to physically protect the PC workstation, registrar workstation or device to reliably prevent use of the workstation/device in combination with the use of the corresponding private key without the permission of the registrar, end entity or authorized person.

If end-entity certificates and their corresponding private keys are deactivated (expired, revoked), they may only be retained in encrypted form and/or with password or PIN protection.

6.2.8.2 Master registrars' private keys

The master registrar must comply with the following provisions to protect the private key:

- A smartcard must be used and a PIN set in accordance with Section 6.4.1 or a comparable security measure must be implemented in order to authenticate the master registrar prior to activation of the private key.
- Measures must be taken to physically protect the master registrar's workstation to reliably prevent use of this workstation in combination with the corresponding private key without the approval of the registrar.

6.2.8.3 Root and intermediate certification authorities' private keys

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

The private key belonging to the CA certificate remains active until the certificate loses its validity or there is a reason for revocation (Section 4.9.3.1).

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

If certificates and their corresponding private keys are deactivated (revoked, expired), they may only be retained in encrypted form and/or with password or PIN protection.

6.2.8.4 Trust Center administrators and operators' private keys

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

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

6.2.9 Method for deactivating private keys

The deactivation of CA and root CA keys is event-based and the responsibility of the Trust Center staff at Telekom Security.

The deactivation of private keys (end entities, registrars) is the tenant's responsibility.

6.2.10 Method for destroying private keys

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

Telekom Security uses an integrated deletion function of the HSM for secure destruction of keys.

End entities or the tenant are responsible for destroying their own private keys.

6.2.11 Evaluation of cryptographic modules

See Section 6.2.1.

6.3 Other aspects of managing key pairs

6.3.1 Archiving of public keys

The certificates (CA, root CA and end entity certificates) are backed up and archived during Telekom Security regular backup measures.

6.3.2 Validity periods of certificates and key pairs

The validity of certificates begins with generation of the certificate and ends when the validity period expires or through revocation. The validity period of key pairs is the same as the validity period for the corresponding certificate. However, the certificates can continue to be used for decryption and signature validation provided the corresponding private key is available.

Table 20 to Table 24 shows the maximum validity periods of the certificates involved in the hierarchy that were issued at the time this CPS came into force.

Telekom Security ensures that the CA and root CA certificates are changed before they expire in order to guarantee the relevant certificate validity of end-entity certificates.

Table 20: Validity of Root-CA certificates (Section 1)

Type of certificate:	T-TeleSec GlobalRoot Class 2
Period of validity:	25 years

Table 21: Validity of Root-CA certificates (Section 2)

Type of certificate:	Deutsche Telekom Internal Root CA 1, Deutsche Telekom Internal Root CA 2
Period of validity:	20 years

Table 22: Validity of Sub-CA certificates

Type of certificate:	TeleSec Business CA 1, Internal Business CA 2, Internal Business CA 3, Internal Business CA 5, Business CA
Period of validity:	12 years or at least 12 years

Table 23: Validity of End Entity certificates

Type of certificate:	All End Entity certificates (Master registrar, Sub-registrar incl. derivates, User, Devices)
Period of validity:	12, 24 or 36 months by default (or 1, 2 or 3 years); a different term of x months can be administered by agreement. Please note: The certificate validity is set when the master domain is set up and is passed on to the areas of responsibility (sub-domains). Within the master domain, no differing validity periods are possible for certificates with the same name. For server certificates issued by a public certification authority (Section 1.3.1.2.1), the following applies ▪ Until 31.08.2020: max 825 days or 27 months ▪ From 01.09.202: max. 398 days or 13 months

Table 24: Validity of OCSP certificates

Type of certificate:	OCSP-Signer T-TeleSec GlobalRoot Class 2
Period of validity:	Max. 6 month
Type of certificate:	OCSP-Signer per Sub-CA (Chapter 1.3.1.2 ff)
Period of validity:	Max. 6 month

6.4 Activation data

6.4.1 Generation and installation of activation data

6.4.1.1 Telekom Security

In order to protect the private keys of the CA and root 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.

6.4.1.2 External registration authority

Depending on the input media (e.g., PC keyboard, keypad of a smartcard reader), for exporting soft PSEs or activating/using the private key Telekom Security recommends assigning secure passwords or pass phrases that match the following syntax:

- Character lengths of at least 8 alphanumeric digits and characters, incl. special characters such as !, ?; /, etc.
- Lower/upper case letters
- No common terms that can be found in dictionaries
- No user names

6.4.2 Protection of activation data

6.4.2.1 Telekom Security

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

6.4.2.2 External registration authority

The tenant is responsible for implementing the protection in accordance with Section 6.4.1.

The rules as described in Section 6.1.1 apply to the issuing of the sub-registrar certificate. At least a 6-digit PIN and an 8-digit PUK must be assigned to use smart cards.

Telekom Security urgently recommends putting the sub-registrar certificate and the two derivatives on a smartcard that has suitable PIN protection.

When using a software PSE, Telekom Security recommends the following rules:

- When exporting, the file must be assigned a secure password and saved in a secure environment.
- When importing this file, the “Mark key as exportable” function must be deactivated, while the “High security for private key” function and the “High” security level are activated so that a suitably difficult to guess password can be assigned. This prevents the soft PSE from simply being exported and supports a password query when using the private key (e.g., signature procedure, decryption).

  Please note: All above descriptions for importing private keys depend on the browser and may therefore be different.

The tenant can procure a written confirmation from the end entities for handling the activation data.

To increase security, Telekom Security recommends regularly changing the pass phrase or PIN for the end-entity 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 protect the transfer with the help of methods for protecting against loss, theft, changes, unauthorized disclosure or use of these private keys.

When using a combination of user name and password to log on to networks as activation data for an end entity, the passwords to be transmitted in a network also need to be protected against access by unauthorized third parties.

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 checks

Telekom Security carries out all PKI functions with the help of trustworthy and appropriate systems. The function and capacity of the systems are continuously checked by monitoring systems so that resources can be expanded promptly if necessary.

The security regulations for computers of the certification authority (e.g., network security, access control, monitoring etc.) are described in the security concept [SBCA security concept]. Here the requirements under [ETSI EN 319 401] Section 7.4 are implemented.

The data on CPU, memory and disk utilization collected in the monitoring (periodically every 5 minutes) are provided with warning and alarm thresholds. At the latest when the warning level occurs, the resource planning is checked and, if necessary, adapted by means of extensions (for example hardware retrofitting, relocation of services to other systems or assignment of additional resources to virtual machines).

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

6.5.1 Specific technical requirements for computer security

6.5.1.1 Telekom Security

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

The security procedure includes:

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

Operating systems that support the implementation of security settings are used on the Trust Center's systems. None of the systems can be used without user registration.

Security-critical settings (user accounts for instance) will only be modified using the dual-control principle.

The enforcement of access restrictions on the systems is supported by the implemented restrictive password policy. Particularly security-critical applications (such as certificate generation) also require authentication of the user at the Trust Center.

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

The TSP performs a penetration test (PEN test) on the TSP systems

- upon setup,
- when comprehensive upgrades or changes are performed on the infrastructure or applications,
- but at least once per year,

which the TSP deems to be critical.

The TSP provides evidence that each penetration test has been conducted by a person or organization that has the skills, tools, knowledge, ethics, and independence required to produce a reliable report.

6.5.1.2 External registration authority

The master and sub-registrar (incl. derivatives) manage the master domain (PKI tenant) from a PC workstation that the tenant operates entirely independently.

Telekom Security provides the tenant or external registration authority with trustworthy, suitable hardware and software components for the master and sub-registrars to operate the registrar functions on the registrar PCs.

The security measures for the tenant's (delegated third party) or external registration authority's computers are described in the "Personal, infrastructure and technical framework conditions for the TeleSec Shared Business CA (SCBA)" document [SBCA PITR].

In addition, Telekom Security recommends using passwords as described in Section 6.4.1.

6.5.2 Assessment of computer security

After every significant system or network change, an automated vulnerability scan takes place within a week, but at least once per calendar quarter.

The vulnerability tests are carried out by persons or organizations who have the skills, tools, abilities, ethical principles and independence required for reliable testing and documentation. The implementation of a vulnerability test with details of the qualifications of the person or organization being tested is controlled by the ISMS and documented together with the results.

Possible weak points are analyzed, evaluated and registered. Based on the evaluation, measures are defined and implemented in a defined plan.

Critical weaknesses are processed in the ISMS. Critical weaknesses are evaluated within 48 hours by the ISMS team and a solution scenario is shown. If immediate and complete elimination of the vulnerability is not possible, a treatment plan will be drawn up that will address the critical vulnerability mitigation.

In addition, penetration tests (PEN test) are carried out once a year. Here too, appropriate measures are derived and implemented, if this is necessary.

The PEN tests are carried out by persons or organizations who have the skills, tools, abilities, ethical principles and independence required for reliable testing and documentation. The implementation of a PEN test with details of the qualifications of the person or organization being tested is controlled by the ISMS and documented together with the results.

6.6 Technical checks on the lifecycle

6.6.1 System development checks

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

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

After successful testing of the software in the development environment, a software package of the manufacturer is created, which is located on a test system (test environment, test unit) in the network or location of Telekom Security (SBCA-TU).

Installation on Telekom Security' live system (SBCA-PU) in Telekom Security' georedundant data center only takes place after successful tests on the test system.

Telekom Security’ established change and release management is used.

The PKI systems (CA, HSM, web server, etc.) are administered by the trust center administrators (system administrators) via a separate network that is exclusively available to these role holders [SBCA security concept] and [FSC TC].

6.6.2 Security management checks

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

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

6.6.3 Security checks on the lifecycle

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

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

6.7 Network security checks

The following network security measures have been implemented for the TeleSec Shared Business CA service.

- The networks of the certification service are secured by multi-level firewalls and classified in different security zones.
- Security-critical components and systems that are accessible from the Internet (e.g., directory service, OCSP responder) are separated from the Internet and the internal networks by firewalls. All other security-critical components and systems (e.g., CA, DB, signer) are in separate networks or, in the case of the offline CA, not connected to any 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.
- Vulnerability scans are performed at regular intervals. Further details can be found in Section 5.4.8.
- All authorized users must authenticate themselves to the systems using established mechanisms, while accounts that are no longer required are deleted or deactivated.

- The Trust Center is connected georedundantly with both the telematics infrastructure and the Internet via separate feeders. Transition from the telematics infrastructure to the Internet or vice versa is prevented by several firewall systems.

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

6.8 Time stamp

Certificates, revocation lists, online status checks and other important information contain date and time information derived from a reliable time source (see Section 5.5.5). A cryptographic time stamp is not used.

7 CERTIFICATE LIST, REVOCATION LIST AND OCSP PROFILES

7.1 Certificate profile

The certificates issued by Telekom Security meet the following requirements:

- [RFC5280]
- [X.509]
- [CAB-BR]
- [ETSI NCP OVCP]

X.509v3 certificates must include at least the contents listed in Table 25.

Table 25: Certificate attributes in accordance with X509.v3

Field:	**Value or value limitation:**
Version:	Certificate version (Section 7.1.1)
Certificate serial number:	Unique value to identify the certificate. The certificate serial numbers are generated by SBCA using a cryptographically suitable random number generator (CSPRNG) as at least 64-bit random values (entropy). For server certificates the random value (entropy) is 126 bits.
Signature algorithm:	RSA - SHA-256, RSASSA-PSS – SHA256 or RSA - SHA-1 (depending on the issuing sub-CA (see chapters 1.3.1.2.1 and 1.3.1.2.2)
Issuer:	Certification authority (Sections 1.3.1.2.1 and 1.3.1.2.2)
Valid from:	Time basis Coordinated Universal Time (UTC). Coded according to RFC5280.
Valid until:	Time basis Coordinated Universal Time (UTC). Coded according to RFC5280.
Requester:	Unique name (Section 7.1.4); user certificates: 3.1.1.1.13
Public key:	Coded according to RFC5280.
Extensions:	**Reference to:**
Key usage:	Section 7.1.2.1
Certificate Policy:	Section 7.1.2.2
Alternative subject name:	Section 7.1.2.3
Basic constraints:	Section 7.1.2.4
Enhanced key usage:	Section 7.1.2.5
Revocation list distribution point:	Section 7.1.2.6
Subject key identifier:	Section 7.1.2.7
Authority key identifier:	Section 7.1.2.8
Access to authority information:	Section 7.1.2.9
Certificate template name:	Section 7.1.2.10

Additional extensions and properties are described in more detail in the sections that follow.

7.1.1 Version number(s)

The X.509 certificates issued by the TeleSec Shared Business CA are the latest version (currently version 3). Additional extensions and properties are described in more detail in the sections that follow.

The CA certificates are also of the X.509v3 type.

7.1.2 Certificate extensions

To meet the X.509v3 standard, Telekom Security enhances the certificate profile with various extensions, which are described in Sections 7.1.2.1 to 7.1.2.10.

The tenant cannot add any additional extensions to the certificate profile.

7.1.2.1 “Key usage” extension (KeyUsage)

The key usage is based on the rules of RFC5280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” and is described therein.

In Table 26 to Table 29, the “key usage” extension is assigned to the different certificate profiles.

Table 26: Assignment of the “key usage” extension, part 1

Certificate profile:	**User**
Certificate template:	Single key
Use:	A certificate for signature and encryption
Description:	digitalSignature (Bit 0) and keyEncipherment (Bit 2)
Hex value:	A0
Certificate profile:	**User**
Certificate template:	Dual key
Use:	A separate certificate for signature and encryption
Description:	digitalSignature (Bit 0)
Hex value:	80
Bezeichnung:	keyEncipherment (Bit 2)
Hex-Wert:	20
Certificate profile:	**User**
Certificate template:	Triple key
Use:	A separate certificate for signature, encryption and LogOn
Description:	digitalSignature (Bit 0)
Hex value:	80
Description:	keyEncipherment (Bit 2)
Hex value:	20
Description:	digitalSignature (Bit 0) and keyEncipherment (Bit 2)
Hex value:	A0

Table 27: Assignment of the “key usage” extension, part 2

Certificate profile:	**Server**
Certificate template:	Single key
Use:	A certificate for authentication and encryption
Description:	digitalSignature (Bit 0) and keyEncipherment (Bit 2)
Hex value:	A0
Certificate profile:	**Mail gateway**
Certificate template:	Single key
Use:	A certificate for signature and encryption
Description:	digitalSignature (Bit 0) and keyEncipherment (Bit 2)
Hex value:	A0

Certificate profile:	**Router/gateway**
Certificate template:	Single key
Use:	A certificate for authentication
Description:	digitalSignature (Bit 0) and keyEncipherment (Bit 2)
Hex value:	A0
Certificate profile:	**Domain controller**
Certificate template:	Single key
Use:	A certificate for authentication
Description:	digitalSignature (Bit 0) and keyEncipherment (Bit 2) and dataEncipherment (Bit 3)
Hex value:	B0

Table 28: Assignment of the “key usage” extension, part 3

Certificate profile:	**Master registrar**
Certificate template:	Single key
Use:	A certificate for signature and encryption
Description:	digitalSignature (Bit 0) and keyEncipherment (Bit 2)
Hex value:	A0
Certificate profile:	**Sub-registrar and derivates**
Certificate template:	Single key
Use:	A certificate for signature and encryption
Description:	digitalSignature (Bit 0) and keyEncipherment (Bit 2)
Hex value:	A0

Table 29: Assignment of the “key usage” extension, part 4

Certificate profile:	**Root-CA**
Certificate templatee:	Single key
Use:	Ein Zertifikat für Signatur von Zertifikatsschlüssel und CRL-Signatur
Description:	keyCertSign (Bit 5) und CRLSign (Bit 6)
Hex value:	06
Certificate profile:	**Sub-CA**
Certificate templatee:	Single key
Use:	Ein Zertifikat für Signatur von Zertifikatsschlüssel und CRL-Signatur
Description:	keyCertSign (Bit 5) und CRLSign (Bit 6)
Hex value:	06
Certificate profile:	**OCSP**
Certificate templatee:	Single key
Use:	A certificate for signature and encryption
Description:	digitalSignature (Bit 0) and nonRepudiation (Bit 1)
Hex value:	C0

The criticality (Risk value) of this extension is set to “critical”.

At the customer’s request, further values from the above table (e.g., dataEncipherment) can be added to the certificate profile (except CA certificates) with the “key usage” extension.

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

Although the nonRepudiation bit is not set in the “Key usage” extension, Telekom Security supports non-repudiation for these “advanced” signature certificates. It is currently not essential to set the nonRepudiation bit in this certificate type, as the PKI industry has not yet reached a consensus regarding the actual significance of the nonRepudiation bit. Until a consensus of this type has been reached, the nonRepudiation bit has no significance for potential relying parties.

In addition, the most common applications (e.g., e-mail) do not evaluate the nonRepudiation bit. For this reason, defining the bit is not helpful for relying parties when deciding on the trustworthiness.

7.1.2.2 “Certificate Policies” extension

The “Certificate Policy” extension consists of object identifiers (OID; see also Section 7.1.6) and a URL, via which this CPS can be accessed. The criticality of this extension is set to “not critical”.

7.1.2.3 “Subject Alternative Name” extension (subjectAltName)

In Table 30, the “Subject Alternative Name” extension is assigned to the different certificate profiles.

Table 30: Assignment of the “Subject Alternative Name” extension (subjectAltName)

Certificate type:	**User**
Certificate template:	Single key
Use:	A certificate for signature and encryption
Description:	RFC822 name, optional Principalname
Certificate type:	**User**
Certificate template:	Dual key
Use:	A separate certificate for signature and encryption
Description:	RFC822 name, optional Principalname
Certificate type:	**User**
Certificate template:	Triple key
Use:	A separate certificate for signature, encryption and LogOn
Description:	RFC822 name, optional Principalname
Certificate type:	**Server**
Certificate template:	Single key
Use:	A certificate for authentication and encryption
Description:	One or more DNS names
Certificate type:	**Mail gateway**
Certificate template:	Single key
Use:	A certificate for signature and encryption
Description:	RFC822 name
Certificate type:	**Router/gateway**
Certificate template:	Single key
Use:	A certificate for authentication
Description:	RFC822 name, IP address, optional: DNS name
Certificate type:	**Domain controller**
Certificate template:	Single key
Use:	A certificate for authentication
Description:	RFC822 name, DNS name, Other name (DS-Objekt-Guid)

The criticality (Risk value) of this extension is set to “not critical”.

7.1.2.4 “Basic constraints” extension

The “basic constraints” extension defines the following content:

- User type (subjectType) and
- Restriction of the certification path (pathLenConstraint)

The user type specifies whether the issued certificate is intended for an end entity (CA = false) or certification authorities (CA).

A restriction of the certification path specifies the maximum number of certification authorities that may appear in the certificate hierarchy.

Table 31 shows the root and sub-Ca certificates used by the „TeleSec Shared Business CA” PKI service. The „TeleSec Shared Business CA” PKI service does not provide further sub-CA certificates that are hierarchically subordinate to one of the sub-CAs shown.

Table 31: Assignment of the “basic constraints” extension

Certificate type:	**Root-CA**
Certificate name:	T-TeleSec GlobalRoot Class 2
Restriction of the certification path:	None
Certificate type:	**Root-CA**
Certificate name:	Deutsche Telekom Internal Root CA 1
Restriction of the certification path:	1
Certificate type:	**Root-CA**
Certificate name:	Deutsche Telekom Internal Root CA 2
Restriction of the certification path:	None
Certificate type:	**Sub-CA**
Certificate name:	TeleSec Business CA 1
Restriction of the certification path:	0
Certificate type:	**Sub-CA**
Certificate name:	Internal Business CA 2
Restriction of the certification path:	0
Certificate type:	**Sub-CA**
Certificate name:	Internal Business CA 3
Restriction of the certification path:	0
Certificate type:	**Sub-CA**
Certificate name:	Internal Business CA 5
Restriction of the certification path:	0
Certificate type:	**Sub-CA**
Certificate name:	Business CA
Restriction of the certification path:	0
Certificate type:	**End entity**
Certificate name:	Varius end entities (User, devices, registrars, OCSP)
Restriction of the certification path:	None

The criticality (Risk value) of this extension is set as "critical" for all certification authorities, that for all end entities (participants) as "non-critical".

7.1.2.5 “Extended key usage” extension (ExtendedKeyUsage)

Table 32 and Table 33 assigns the extended key usages to the different certificate profiles.

Table 32: Assignment of the „Extended key usage“ extension, part 1

Certificate type:	**User**
Certificate template:	Single key
Use:	A certificate for signature and encryption
Description:	Secure E-Mail (1.3.6.1.5.5.7.3.4) or Client authentication (1.3.6.1.5.5.7.3.2) or both values
Certificate type:	**User**
Certificate template:	Dual key
Use:	A separate certificate for signature and encryption
Description:	Secure E-Mail (1.3.6.1.5.5.7.3.4) or Client authentication (1.3.6.1.5.5.7.3.2) or both values
Certificate type:	**User**
Certificate template:	Triple key
Use:	A separate certificate for signature, encryption and LogOn
Description for signature / encryption:	Secure E-Mail (1.3.6.1.5.5.7.3.4) or Client authentication (1.3.6.1.5.5.7.3.2) or both values
Description for LogOn:	Client authentication (1.3.6.1.5.5.7.3.2) and MS SmartcardLogon (1.3.6.1.4.1.311.20.2.2)

Table 33: Assignment of the „Extended key usage“ extension, part 2

Certificate type:	**Server**
Certificate template:	Single key
Use:	A certificate for authentication and encryption
Description:	Server authentication (1.3.6.1.5.5.7.3.1) or Client authentication (1.3.6.1.5.5.7.3.2) or both values
Certificate type:	**Mail gateway**
Certificate template:	Single key
Use:	A certificate for signature and encryption
Description:	Secure E-Mail (1.3.6.1.5.5.7.3.4)
Certificate type:	**Router/gateway**
Certificate template:	Single key
Use:	A certificate for authentication
Description:	No value set
Certificate type:	**Domain controller**
Certificate template:	Single key
Use:	A certificate for authentication
Description:	Server authentication (1.3.6.1.5.5.7.3.1) and Client authentication (1.3.6.1.5.5.7.3.2)
Certificate type:	**OCSP**
Certificate template:	Single key
Use:	A certificate for signature and encryption
Description:	OCSPSigning (1.3.6.1.5.5.7.3.9)

The criticality (Risk value) of this extension is set to “not critical”. Upon customer request, this extension can be marked as "critical".

Registrar certificates do not receive “extended key usage”.

7.1.2.6 "Revocation list distribution point" extension (cRLDistributionPoint)

All end entity certificates have a revocation list distribution point, through whose URL (HTTP and partly LDAP) the current and associated certificate revocation list (CRL) can be accessed. Relying parties need this URL for certificate validation. The criticality of this extension is set to “not critical”.

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

The root CA certificates do not receive revocation list distribution points.

7.1.2.7 “Subject key identifier” extension (SubjectKeyIdentifier)

In all end-entity and registrar certificates, the “subject key identifier” extension contains an SHA-1 hash value as the attribute value. This hash value is formed individually from the public key in question.

The “subject key identifier” extension of the TeleSec Shared Business CA certificate contains an SHA-1 hash value as the attribute value. This hash value is formed from the public key of the TeleSec Shared Business CA. This value corresponds mathematically to the value of the “authority key identifier” extension (see Section 7.1.2.8) of the end-entity and registrar certificate.

The rules for the respective hierarchically higher level certification instance also apply.

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

7.1.2.8 "Authority Key Identifier" extension (authorityKeyIdentifier)

In end-entity and registrar certificates, the “authority key identifier” extension contains an SHA-1 hash value as the attribute value. This hash value corresponds mathematically to the value of the “subject key identifier” (see Section 7.1.2.7) of the certificate from the hierarchically higher level certification instance (CA).

The rules for the respective hierarchically higher level certification instance also apply.

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

7.1.2.9 “Authority information access” extension

7.1.2.9.1 End entities certificates

In end entity and registration authority employee certificates, the “authority information access” extension contains the object ID (OID) 1.3.6.1.5.5.7.48.1 for the OCSP service, as well as the HTTP URL of the OCSP responder in question:

- End-entity certificate issued by:
  - Telesec Business CA 1: http://ocsp03.sbca.telesec.de/ocspr
  - Business CA 1: http://ocsp.sbca.telesec.de/ocspr
  - Telesec Business CA 2: http://ocsp.sbca.telesec.de/ocspr
  - Internal Business CA 2: http://ocsp.sbca.telesec.de/ocspr
  - Internal Business CA 3: http://ocsp.sbca.telesec.de/ocspr
  - Internal Business CA 5: http://ocsp.telesec.de/ocspr

Certificates that were issued after February 26, 2018 additionally receive the path specification (HTTPS) of the respective sub-CA certificate. The corresponding object identifier (OID) is 1.3.6.1.5.5.7.48.2.

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

7.1.2.9.2 Sub-CA certificates

In certificates from intermediate certification authorities, the “authority information access” extension contains the object ID (OID) 1.3.6.1.5.5.7.48.1 for the OCSP service, as well as the HTTP URL of the OCSP responder in question:

- CA certificate
  - Telesec Business CA 1: http://ocsp04.telesec.de/ocspr
  - Internal Business CA 2: http://ocsp.sbca.telesec.de/ocspr
  - Internal Business CA 3: http://ocsp-root.sbca.telesec.de/ocspr
  - Internal Business CA 5: http://ocsp.telesec.de/ocspr
  - Business CA 1: http://ocsp.sbca.telesec.de/ocspr

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

7.1.2.10 “Certificate template name” extension

For the “DomainController” certificate profile, the “certificate template name” extension is filled with the name “DomainController”.

7.1.3 Object IDs (OIDs) of algorithms

Within the „TeleSec Shared Business CA” PKI service, the following signature algorithms are available for signing certificates:

- sha-256WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}, -> 1.2.840.113549.1.1.11
- sha-256WithRSASSA-PSS (Probabilistic Signature Scheme) OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}, -> 1.2.840.113549.1.1.10
- ecdsa-with-SHA256 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA256(2)} -> 1.2.840.10045.4.3.2
- 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

These signature algorithms relate to all certificate types (root certification authority, intermediate certification authority and end entity).

For security reasons, all end-entity certificates and certificates from the subordinate certification authority (sub-CA) must use the signature hash algorithm SHA-256.

The signature hash algorithm SHA-1 is no longer recommended for security reasons and is not permitted in certificates that are issued by a public sub-CA.

SHA-1 is permitted exclusively in certificates that are issued by an internal Sub-CA for interoperability reasons only.

7.1.4 Name forms

7.1.4.1 Issuer Information

All CA certificates used by the „TeleSec Shared Business CA" contain a unique issuer name (Issuer DN) (sections 1.3.1.1 ff and 1.3.1.2 ff)

The end-entity and registrar certificates of the „TeleSec Shared Business CA" contain a unique issuer DN from the certification authority in question (Sections 1.3.1.2.1 to 1.3.1.2.2).

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

7.1.4.2 Subject Information – Subscriber Certificates

The content of the Subject DN (requester) of end-entity certificates depends on the certificate type (e.g., user, server, router/gateway) and is optionally made up of the fields as described in Sections 3.1.1.1.1 to 3.1.1.1.13. The fields contain mandatory, optional or automatically generated information or pre-assignments.

If not all the certificate request data can be entered in the Subject DN because technical or interoperability constraints (e.g., file size of the certificate, only one OU entry) in the certificates make using this impossible, deviations from the previous provisions are permitted. These certificates are issued through the "Business CA" subordinate certification authority (sub-CA).

The e-mail address does not have to be the content of the Subject DN if this information is contained in the "subjectAltName" extension.

Table 34 shows the components of the Subject DN and Subject Alternative Name for end participants per certificate type.

Table 34: Subject DN information for subscribers per certificate type

Certificate profile:	**User**
Certificate template:	Single key
Use:	A certificate for signature and encryption
Mandatory information in the subject:	Country Name (C), Organization Name (O), Given name and Surname, Common Name (CN), E-mail address (E)
Preassignments in the subject:	Organizational Unit Name 1 (OU1), Organizational Unit Name 2 (OU2)
Automatically generated information in the subject:	Subject-DN Serial Number (SN)
Optional information in the subject:	Organizational Unit Name 3 (OU3), User Principal Name (UPN), further E-Mail addresses
Data set entry in Subject Alternative Name:	One or more RFC822 names (Section 3.1.1.2.1), optional: User Principal Name (Section 3.1.1.2.2)
Certificate profile:	**User**
Certificate template:	Dual key
Use:	A separate certificate for signature and encryption
Mandatory information in the subject:	Country Name (C), Organization Name (O), Given name and Surname, Common Name (CN), E-mail address (E)
Preassignments in the subject:	Organizational Unit Name 1 (OU1), Organizational Unit Name 2 (OU2)
Automatically generated information in the subject:	Subject-DN Serial Number (SN)
Optional information in the subject:	Organizational Unit Name 3 (OU3), User Principal Name (UPN), further E-Mail addresses
Data set entry in Subject Alternative Name:	One or more RFC822 names (Section 3.1.1.2.1), optional: User Principal Name (Section 3.1.1.2.2)
Certificate profile:	**User**

Certificate template:	Triple key
Use:	A separate certificate for signature, encryption and LogOn
Mandatory information in the subject:	Country Name (C), Organization Name (O), Given name and Surname, Common Name (CN), E-mail address (E)
Preassignments in the subject:	Organizational Unit Name 1 (OU1), Organizational Unit Name 2 (OU2)
Automatically generated information in the subject:	Subject-DN Serial Number (SN)
Optional information in the subject:	Organizational Unit Name 3 (OU3), further E-mail addresses
Data set entry in Subject Alternative Name:	One or more RFC822 names (Section 3.1.1.2.1), User Principal Name (Section 3.1.1.2.2)
Certificate profile:	**Server**
Certificate template:	Single key
Use:	A certificate for authentication and encryption
Mandatory information in the subject:	Country Name (C), Organization Name (O), Locality Name (L), State or Province Name (St), Common Name (CN), E-mail address (E)
Preassignments in the subject:	Organizational Unit Name 1 (OU1), Organizational Unit Name 2 (OU2)
Automatically generated information in the subject:	Subject-DN Serial Number (SN)
Optional information in the subject:	Organizational Unit Name 3 (OU3), further Server names, Street address, Postal code
Data set entry in Subject Alternative Name:	One or more DNS names (Section 3.1.1.2.3)
Certificate profile:	**Mail gateway**
Certificate template:	Single key
Use:	A certificate for signature and encryption
Mandatory information in the subject:	Country Name (C), Organization Name (O), Common Name (CN), E-mail address (E)
Preassignments in the subject:	Organizational Unit Name 1 (OU1), Organizational Unit Name 2 (OU2)
Optional information in the subject:	Organizational Unit Name 3 (OU3)
Data set entry in Subject Alternative Name:	RFC822 name (Section 3.1.1.2.1)
Certificate profile:	**Router/gateway**
Certificate template:	Single key
Use:	A certificate for authentication
Mandatory information in the subject:	Country Name (C), Organization Name (O), Common Name (CN), E-mail address (E)
Preassignments in the subject:	Organizational Unit Name 1 (OU1), Organizational Unit Name 2 (OU2)
Automatically generated information in the subject:	Subject-DN Serial Number (SN)
Optional information in the subject:	Organizational Unit Name 3 (OU3), Unstructured Name
Data set entry in Subject Alternative Name:	IP address (Section 3.1.1.2.4), RFC822 name (Section 3.1.1.2.1), optional: DNS name (Section 3.1.1.2.3)
Certificate profile:	**Domain controller**
Certificate template:	Single key
Use:	A certificate for authentication

Mandatory information in the subject:	Country Name (C), Organization Name (O), Common Name (CN), Microsoft GUID, E-mail address (E)
Preassignments in the subject:	Organizational Unit Name 1 (OU1), Organizational Unit Name 2 (OU2)
Optional information in the subject:	Organizational Unit Name 3 (OU3)
Data set entry in Subject Alternative Name:	Other name (Section 3.1.1.2.5)

7.1.4.3 Subject Information – Root Certificates and Subordinate CA Certificates

The content of the Subject DN (requester) of CA certificates is optionally made up of the fields as described in Sections 3.1.1.1.1 to 3.1.1.1.13. The fields contain mandatory and if applicable optional generated information.

The following fields contain mandatory information:

- Country Name (C):
- Organization Name (O)
- Organizational Unit Name (OU)
- Common Name (CN)

The following fields are optional:

- StateOrProvince name (St)
- Locality (L)
- PostalCode
- StreetAddress (Street)

7.1.5 Name constraints

TeleSec Shared Business CA does not operate sub-CAs with name restrictions.

7.1.6 Object IDs (OIDs) for certificate policies

7.1.6.1 Object IDs for “Root CA certificates”

The Root-CA-certificates does not contain any certificate policies extension.

7.1.6.2 Object IDs for “Sub-CA certificates”

All CA certificate contain a “certificate policies” extension. As well as the HTTP URL, the CPS has the following object ID:

- policy OBJECT IDENTIFIER ::= {iso(1) iso identified organization(3) us department of defense(6) oid assignments(1) private(4) iana registrated private enterprises(1) T-TeleSec(7879) policy identifier(13) shared-business-ca(25)} -> 1.3.6.1.4.1.7879.13.25

Sub-CA certificates issued under a public CA (Chapter 1.3.1.2.1) use the Policy OID shown in Chapter 7.1.6.3.2.

7.1.6.3 Object IDs for “End-entity certificates”

7.1.6.3.1 Object ID for certificate policy TeleSec Shared Business CA

All end-entity certificates (including registrar certificates) contain a “certificate policies” extension. As well as the HTTP URL, the CPS has the following object ID:

- policy OBJECT IDENTIFIER ::= {iso(1) iso identified organization(3) us department of defense(6) oid assignments(1) private(4) iana registrated private enterprises(1) T-TeleSec(7879) policy identifier(13) shared-business-ca(25)} -> 1.3.6.1.4.1.7879.13.25

7.1.6.3.2 Object IDs for “Baseline Requirements certificate policies”

The CA/Browser Forum has defined the following policy OIDs in the Baseline Requirements [CAB-BR]:

- Domain Validation (DV): 2.23.140.1.2.1
- Organizational Validation (OV): 2.23.140.1.2.2
- Individual Validation (IV): 2.23.140.1.2.3
- Extended Validation (EV): 2.23.140.1.1

All end-entity certificates with an FQDN in the “Common Name” field (Sections 3.1.1.1.7 and 3.1.1.2.3) that are issued under the “TeleSec Business CA 1” sub-CA contain the following “Baseline Requirements of the certificate policies” OID in the “Certificate policies” field:

- policy OBJECT IDENTIFIER ::= {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baselinerequirements(2) subject-identity-validated(2)} -> 2.23.140.1.2.2

The following requirements, which the „TeleSec Shared Business CA” PKI service adheres to, apply for the policy OIDs that the CA/Browser Forum has defined in the [CAB-BR]: If the policy OID 2.23.140.1.2.2 is used in a certificate, it is mandatory to complete the following Subject DN fields:

- countryName (Section 3.1.1.1.1)
- organizationName (Section 3.1.1.1.2)
- localityName (Section 3.1.1.1.9)
- stateOrProvinceName (Section 3.1.1.1.10)

TeleSec Shared Business CA does not use policy OIDs 2.23.140.1.2.1, 2.23.140.1.2.3 and 2.23.140.1.1, as no DV, IV and EV certificates are issued.

7.1.6.3.3 Objekt-Kennungen für „Zertifizierungsrichtlinien des ETSI“

The European Telecommunications Standards Institute has defined the following policy OIDs in the respective European Standards [ETSI NCP OVCP, ETSI EN TSP]:

- NCP: Normalized Certificate Policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)} -> 0.4.0.2042.1.1
- NCP+: Normalized Certificate Policy OBJECT IDENTIFIER ::= {requiring a secure user device itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus (2)} -> 0.4.0.2042.1.2

- LCP: Lightweight Certificate Policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) lcp (3)} -> 0.4.0.2042.1.3
- EVCP: Extended Validation Certificate Policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) evcp (4)} -> 0.4.0.2042.1.4
- EVCP+: Extended Validation Certificate Policy requiring a secure user device OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) evcpplus (5)} -> 0.4.0.2042.1.5
- DVCP: Domain Validation Certificate Policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) dvcp (6)} -> 0.4.0.2042.1.6
- OVCP: Organizational Validation Certificate Policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7)} -> 0.4.0.2042.1.7
- IVCP: Individual Validation Certificate Policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ivcp (8)} -> 0.4.0.2042.1.8

All end-entity certificates with an FQDN in the “Common Name” field (Sections 3.1.1.1.7 and 3.1.1.2.3) (e.g. server certificates) that are issued under the “TeleSec Business CA 1” sub-CA contain the following “ETSI certificate policies” OID in the “Certificate policies” field:

- policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ovcp (7)} -> 0.4.0.2042.1.7

All end-entity certificates with a.) a given name and surname or prefix and FQDN in the “Common Name” field (Sections 3.1.1.1.7 and 3.1.1.2.3) and b.) an e-Mail address (Section 3.1.1.1.8) and c.) a RFC822 name (Section 3.1.1.2.1) (e.g. user and mail-gateway certificates) that are issued under the “TeleSec Business CA 1” sub-CA contain the following “ETSI certificate policies” OID in the “Certificate policies” field:

- policy OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp (1)} -> 0.4.0.2042.1.1

TeleSec Shared Business CA does not use policy OIDs 0.4.0.2042.1.2, 0.4.0.2042.1.3, 0.4.0.2042.1.4, 0.4.0.2042.1.5, 0.4.0.2042.1.6 and 0.4.0.2042.1.8, as no NCP+, LCP, EVCP, EVCP+, DVCP und IVCP certificates are issued.

7.1.7 Use of the “policy constraints” extension

No stipulation.

7.1.8 Syntax and semantics of policy identifiers

Please see Section 7.1.2.2. The current CPS is always stored. Older versions are stored in the corresponding repository.

7.1.9 Processing semantics for the “critical certificate policies” extension

No stipulation.

7.1.10 Subject DN Serial Number (SN)

More information on this can be found in Section 3.1.1.1.13.

7.1.11 Object IDs for “certificate transparency (CT)”

For server certificates that are issued under a public sub-CA (Section1.3.1.2.1), the “certificate transparency (CT)” function can optionally be activated for each PKI tenant.

After a server certificate is issued with the CT function, an extension with the OID “1.3.6.1.4.1.11129.2.4.2” is added to the certificate containing the respective “signed certificate time stamp” (SCT) as values.

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

7.2 Revocation list profile

The revocation lists issued by Telekom Security meet the following requirements:

- [RFC5280]
- [X.509]

Certificate revocation lists must include at least the contents described in Table 35.

Table 35: Revocation list attributes in accordance with X509.v2

Field:	**Value or value limitation:**
Version:	Revocation list version (Section 7.2.1)
Issuer:	Certification authority (Sections 1.3.1.2.1 and 1.3.1.2.2)
Valid from (this update):	Time basis Coordinated Universal Time (UTC). Coded according to RFC 5280.
Next update:	Date and time of the next planned publication.
Signature algorithm:	RSA - SHA-256 or RSA - SHA-1 (depending on the issuing sub-CA (see chapters 1.3.1.2.1 and 1.3.1.2.2)
Revoked certificates:	List of revoked certificates including serial number with revocation date and time of the revoked certificate.
Extensions:	**Reference to:**
Authority key identifier:	The regulations in accordance with Section 7.2.2.1 apply.
Revocation list number:	Unique value (Section 7.2.2.2)
Reason for revocation:	Coding of the revocation reason in accordance with RFC5280 (Section 7.2.2.3)

7.2.1 Version number(s)

The X.509 certificate revocation lists issued by the TeleSec Shared Business CA correspond to version 2.

7.2.2 Revocation list and revocation list entry extensions

7.2.2.1 “Authority Key Identifier” (authorityKeyIdentifier) extension

The revocation lists are given the extension “authority key identifier” as described in Section 7.1.2.8.

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

7.2.2.2 “Revocation list number” extension

The revocation lists are given the “revocation list number” extension as a sequential serial number of the revocation list.

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

7.2.2.3 “Reason for revocation” (Reason Code) extension

When revoking certificates, it is essential to state a reason for revocation. According to Table 36, the following reason codes are implemented:

Table 36: “Revocation reason” extension

Input value on website:	**Reasons for revocation in accordance with RFC5280:**	**Value of the reason for revocation in accordance with RFC5280:**
Not specified	Unspecified	0
Key compromised	KeyCompromise	1
Information in the certificate is out of date	AffiliationChanged	3
Certificate revoked following renewal	Superseded	4

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

7.3 OCSP profile

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

The OCSP responder used fulfills the requirements of RFC6960.

7.3.1 Version number(s)

Version 1 is supported pursuant to the OCSP specification according to RFC6960.

7.3.2 OCSP extensions

The OCSP certificate, issued by the intermediate certification authority (subordinate certification authority, sub-CA) (for an overview see Figure 1), contains OCSPSigning with the OID "1.3.6.1.5.5.7.3.9" in the X.509v3 extension “extended key usage. In addition, the extension "OCSP noCheck" (id-pkix-ocsp-nocheck) is encoded with the OID “1.3.6.1.5.5.7.48.1.5”, which means that the OCSP certificate is not validated.

The ArchiveCutOff extension is not used.

8 COMPLIANCE AUDITS AND OTHER CHECKS

8.1 Interval and reason for audits

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

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

The Telekom Security processes are subject to a regular annual check (ETSI EN 319411-1, policy OVCP and policy NCP) by an independent third party. The subject of certification are all processes that are used for the application, issue, revocation, and renewal of end user certificates in conjunction with a public certification authority (Sections 1.3.1.1.1 and 1.3.1.1.2).

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

8.2 Identity/qualification of the auditor

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

Special requirements apply for auditors who perform an audit in the Trust Center of Telekom Security at the request of one or more application software providers. For TeleSec Shared Business CA, the Trust Center commissions an auditor who is accredited for the ETSI certification. This ensures that the special requirements of the auditor (e.g., qualification, independence) are met.

8.3 Relationship of the auditor to the authority to be audited

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

8.4 Audit areas covered

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

- Issuing of sub-registrar certificates and their derivatives
- Authentication and registration by sub-registrars
- Identity checks on end entities
- Certification request process
- Processing certification requests
- Distribution of keys and secrets (password, PIN)
- Certificate acceptance
- Renewal of certificates (re-certification)
- Renewal of keys (Re-key)
- Certificate revocations
- Physical access control
- Access to registrar workstations
- Key backup and archiving

- Authorization and role concept
- Anti-burglary measures
- staff

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

- ETSI EN 319 411-1, Policy NCP
- ETSI EN 319 411-1, Policy OVCP

Risk assessment and security plan

The Trust Center of Telekom Security performs an annual risk assessment that includes the TeleSec Shared Business CA PKI service.

The assessment covers at least the following items:

1) Identification of foreseeable external and internal risks (i.e., in particular the underlying vulnerabilities) that may lead to:
   a) Unauthorized access to relevant data or systems,
   b) Handover or misuse of relevant data,
   c) Modification or destruction of relevant data,
   d) Impairment, interruption, or failure of parts of or the entire certificate management process.
2) Assessment of the likelihood of occurrence and the resulting potential damage (i.e., extent of damage) due to exploitation of a vulnerability. Here, the particular need for protection of certificate data and the certificate management process must be taken into account.
3) Assessment of the effectiveness and suitability of the countermeasures taken (e.g., guidelines, procedures, security systems used, technologies, insurance policies) to remove the danger or minimize the risk.

Based on the risk assessment, the Trust Center of Telekom Security has developed a security plan that is regularly checked and, if necessary, modified. The security plan is made up of processes, measures and products to support assessment and management during the risk assessment of identified risks. The security plan contains administrative, organizational, technical, and physical security measures according to the sensitivity of the data and the certificate management process.

8.5 Measures for resolving deficits

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

8.6 Communication of the results

The results of the audit are documented in a report prepared by the auditor and passed on to Telekom Security.

Telekom Security reserves the right to publish results or partial results if misuse occurred or the image of Telekom Security was harmed.

Audit reports that are saved at the request of by one or more application software providers and embed a Telekom Security root certification certificate must be published at the latest three months after the audit period in question ends.

For TeleSec Shared Business CA, the required audits are saved in accordance with ETSI EN 319 411-1 criteria. The corresponding reports (Audit Attestations) are published on the website https://www.telesec.de/en/service/downloads/pki-repository/.

8.7 Self-Audits

In addition, Telekom Security performs quality assessment self-audits (Section 8.1) at regular intervals.

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

As additional quality assessment self-audits, Telekom Security verifies data relating to the identity of the PKI tenant as well as its configuration is checked, e.g.

- Proof of the naming and the ownership of the PKI client (OU1 field, section 3.1.1.1.3)
- Rule compliance of the OU2 and OU3 fields (sections 3.1.1.1.4 and 3.1.1.1.5)
- Regular check of the organization and permitted Internet domains (sections 3.1.1.1.2, 3.2.2 ff, 3.2.2.1, 3.2.5.2)

Quality assessment self-audits are performed by Telekom Security employees who are qualified for this.

9 OTHER BUSINESS AND LEGAL PROVISIONS

9.1 Charges

9.1.1 Charges for issuing or renewing certificates

Telekom Security is entitled to charge for issuing, renewing and managing end entity and registrar certificates. This applies in particular to the provision and handover of the TeleSec Shared Business CA service.

9.1.2 Charges for access to certificates

Telekom Security does not charge for access to certificates in the directory service of TeleSec Shared Business CA.

Third parties require prior express permission in writing before marketing the certificates that Telekom Security provides publically or providing them for marketing.

9.1.3 Charges for access to revocation or status information

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

Third parties require prior express permission in writing before marketing the revocation and status information that Telekom Security provides publically or providing them for marketing.

9.1.4 Charges for other services

Telekom Security does not charge for accessing and viewing this “CPS” document. Any other usage, e.g., reproduction, amendment or production of a derived document, is subject to the written consent of the authority (Section 1.5.1) that owns the copyright (Section 9.5.2).

The use of this CPS is also free of charge provided it is used as an applicable contract document for the contractual relationship between the tenant and Telekom Security.

9.1.5 Compensation

Telekom Security reimburses charges in accordance with the legal regulations under German law.

9.2 Financial responsibilities

The regulations in the individual agreement apply.

9.2.1 Insurance coverage

As part of business liability insurance, the tenant is obligated to ensure economically appropriate insurance cover from an insurer or via his own liability cover. This insurance clause may not be applied in the case of local, regional and state authorities.

Telekom Security has appropriate business liability insurance and D&O liability insurance cover.

9.2.2 Other financial means

We recommend that the tenant has sufficient financial means to be able to maintain his PKI operation and to meet the obligations for its operation that are described in and derived from this

document. In addition, the tenant must be capable of bearing the liability risk towards end entities if this risk cannot be transferred.

Telekom Security will not request evidence of financial means as a matter of course. However, compliance audits as described in Section 8 ff are an exception to this.

9.2.3 Insurance cover or guarantees for end entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Confidential information is any information from parties involved in TeleSec Shared Business CA PKIs (see Sections 1.3.2 and 1.3.3) that 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 from the TeleSec Shared Business CA that is included in issued certificates (e.g., e-mail address, organization, first and last name), revocation lists and status information or can be derived from these.

9.3.3 Responsibility regarding the protection of confidential information

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

The tenant must abide by the applicable statutory provisions and other regulations concerning data protection (Section 9.4 ff).

9.4 Protection of personal data (data protection)

9.4.1 Data protection concept

Within the TeleSec Shared Business CA, Telekom Security must store and process personal data electronically in order to provide its services.

If Telekom Security is to process sensitive data in the meaning of Article 9 of the General Data Protection Regulation (GDPR) [EU-GDPR], the customer shall notify Telekom Security of this in writing without undue delay.

In accordance with the Group specifications of Deutsche Telekom AG, a data protection concept has been created for TeleSec Shared Business CA. This data protection concept summarizes the aspects of the PKI service that are relevant to data protection.

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

9.4.2 Data to be treated as confidential

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

9.4.3 Data to be treated as non-confidential

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

9.4.4 Responsibility for the protection of confidential data

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

9.4.5 Notification and consent for the use of confidential data

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

Furthermore, all information that is not to be treated as confidential in accordance with Section 9.4.3 and for which the tenant has not declined publication may be published.

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 reasons to disclose 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

Telekom Security reserves all intellectual property rights to certificates, revocation or status information, publicly accessible directory services and databases with the information contained therein, which the TeleSec Shared Business CA issues or manages.

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

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

9.5.2 Property rights of this CPS

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

9.5.3 Property rights to names

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

9.5.4 Property rights to keys and key material

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

Key material that the tenant or its end entities generated themselves remains the property of the tenant. This also applies to key material on smartcards that the tenant has purchased.

9.6 Assurances and guarantees

9.6.1 Assurances and guarantees of the certification authority

The „TeleSec Shared Business CA" certification authority is responsible for all aspects of providing the certification service as well as for activities that are outsourced to subcontractors. The certification authority has clearly regulated the responsibilities and made suitable provisions to allow the certification instance to perform checks at third parties. The CA reserves the right to reveal the relevant practices for parties.

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

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

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

Telekom Security guarantees:

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

Furthermore, Telekom Security guarantees that, at the time a [CAB-BR]-compliant certificate is issued:

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

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

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

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

The Telekom Security Trust Center additionally guarantees that:

16) In the event that the certificate holder belongs to an affiliated company or acts in the name of such a company on its behalf, the requester's representative must accept the "Service and Usage Agreement TeleSec Business CA" before the certificate is issued.
17) In the event that the certificate holder belongs to a delegated third party or acts in the name of such a party on its behalf, the requester concludes the "Subscriber Agreement" with Telekom Security in a legally enforceable form.
18) It operates a publicly accessible directory that contains status information regarding all certificates that have not expired (valid or revoked). This directory is available around the clock.
19) The issued certificates will be revoked in the event of all reasons listed in the [CAB-BR].
20) If the certification authority becomes aware of a compromise, the certificates in question will be revoked.

Telekom Security reserves the right to agree other obligations, assurances, consents and guarantees towards the tenant.

9.6.2 Assurances and guarantees of the registration authority

Registration authorities agree:

- To use the master or sub-registrar certificate (and its derivatives, Section 1.3.2.2.2) only for its intended purpose and not to misuse it.
- To keep their private key secret and protect it against unauthorized access by third parties.
- To have the master or sub-registrar certificate (and its derivatives) in question revoked in the event that the private key is lost or a compromise is suspected.
- Not to include any essentially false statements in certificates that are known to or originate from the registration authorities that approve the certificate request or issue the certificate.
- That the certificates do not contain any errors made by the staff of the registration authorities that approve the certificate request or issue the certificate and that can be attributed to improper or careless certificate issuance and management.
- That the certificate they use is used only for authorized and legal purposes that the tenant in question specifies and does not contradict the provisions of this CPS

- To bear the legal consequences arising from non-fulfillment of the obligations described in the present CPS.
- To ensure that, at the time of the certificate request and issue as well as certificate validation, their devices do not interfere with any technical interfaces of the TeleSec Shared Business CA PKI service (role-specific websites, CMP, LDAP, SCEP, e-mail, OCSP, CRL)
- To revoke the private key at the request of the end entity or an authorized representative in the event of loss or a suspected compromise.
- That all certificates comply with the essential requirements of this document.
- That the revocation functions of the master and sub-registrar and the use of the CA database (directory service, OCSP responder) fulfill all the essential requirements of the applicable CPS.

Telekom Security reserves the right to agree other obligations, assurances, consents and guarantees towards the tenant.

9.6.3 Assurances and guarantees of the end entity

End entities commit to the following:

- To only use the end-entity certificate in the intended way and not to misuse it.
- To protect their private key against unauthorized access by third parties. In the case of private keys of devices, the protection is provided by authorized persons.
- That every digital signature is generated using the private key that corresponds to the public key belonging to the certificate and that can be clearly assigned to the end entity.
- That every digital signature is made with the key material of a valid certificate that has not been revoked.
- That the certificate contents of the subject DN included in their end-entity certificate reflect the truth. In the case of devices, the certificate contents are checked by authorized persons.
- To bear the legal consequences arising from non-fulfillment of the obligations described in the present CPS.
- To ensure that, at the time of the certificate request and issue as well as certificate validation, their devices do not interfere with any technical interfaces of the TeleSec Shared Business CA PKI service (role-specific websites, CMP, LDAP, SCEP, e-mail, OCSP, CRL)
- To arrange for/carry out the revocation of the corresponding end entity certificate in the event of loss or suspected compromise of the private key, significant changes to the certificate information or suspected misuse.
- In the event that the private key is compromised, use of the certificate owner's private key must be ceased immediately and permanently.
- That the certificate they use is used only for authorized and legal purposes that correspond to this CPS and do not contradict the provisions of this statement.
- That the end entity is in fact an end entity and does not carry out any CA functions, such as signing of certificates or revocation lists, with its private key to which the public key contained in the certificate is assigned.

Telekom Security reserves the right to agree other obligations, assurances, consents and guarantees towards the end entity.

9.6.4 Assurances and guarantees of relying parties

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

The relying party must configure its device in such a way that, at the time of certificate validation, it does not impact any technical interfaces of the TeleSec Shared Business CA PKI service (role-specific websites, CMP, LDAP, SCEP, e-mail, OCSP, CRL).

9.6.5 Assurances and guarantees of other entities

No stipulation.

9.7 Exclusion of liability

Telekom Security shall be liable to the customer

a) for any damage caused by willful intent or gross negligence on its part or on the part of its legal representatives or vicarious agents,
b) in accordance with the Product Liability Act (Produkthaftungsgesetz) and
c) for damage arising from loss of life, bodily injury, or damage to health caused by the provider or its legal or vicarious agents.

Telekom Security shall not be liable in the event of slight negligence unless a significant contractual obligation has been violated whose fulfillment is a prerequisite for the proper performance of the agreement or the infringement of which jeopardizes the achievement of the purpose of the agreement, and upon whose compliance the customer can normally rely.

Damage (incl. damage to image) that occurs due to misused certificate content (Section 4.5.1, 5.8) or misuse of trademarks, brand names or trademark rights (Section 3.1.6) is at the expense of the PKI-tenant.

9.8 Limitation of liability

9.8.1 Liability of the provider (Telekom Security)

This liability for any property damage or financial losses shall be limited to foreseeable damage that is typical for the agreement. This also applies to lost profits or savings that have not materialized. Liability for any less direct consequential damage shall be excluded.

If a one-time payment is agreed upon, liability for property or pecuniary damage shall be limited to 10 percent of the net order volume per damage event, and to 25 percent of the net order volume for all damage occurring within a single Agreement year. If a recurring payment is agreed upon, liability for property damage and other damage shall be limited to 10 percent of the net annual charge per damage event, and to 25 percent of the net annual charge for all damage occurring within a single Agreement year. Further liability can be agreed between the parties upon conclusion of the agreement for an additional charge. A separately agreed liability amount shall have priority. Liability as stipulated under Section 9.7 shall remain unaffected by this paragraph.

In addition and as a priority, Telekom Security' liability in the event of slight negligence – regardless of the legal reason – is limited to a total of EUR 2.5 million. Liability as stipulated under Section 9.7 b) will remain unaffected by this paragraph.

Telekom Security shall only be liable for claims for damages based on a guarantee if this is explicitly incorporated in the guarantee. In the case of slight negligence, this liability is subject to the limitations set out under Section 9.8.1.

In the event of loss of data, Telekom Security shall be liable for the cost of recovering the data only in cases where the customer has properly backed up the data. In the case of slight negligence on the part of Telekom Security, this liability shall apply only if the customer properly backed up the data immediately prior to the event leading to the data loss.

For claims to reimbursement of expenses and other liability claims on the part of the customer against Telekom Security, Sections 9.7 and 9.8 ff shall apply accordingly.

9.8.2 Liability of the certificate owner

The certificate owner (certificate holder) shall be liable to the provider (Telekom Security) and the involved parties for damage resulting from misuse, intentional misconduct, non-compliance with obligations under supervisory law or non-compliance with other provisions for the use of the certificate.

9.9 Compensation

The provisions set forth in Sections 9.7 and 9.8 ff. shall apply to any claims for damages.

9.10 Term and termination

9.10.1 Term

The initial publication of this “CPS” document as well as modifications to this document come into force at the time of publication on public Telekom Security websites (see Section 2.3).

9.10.2 Termination

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

9.10.3 Effect of termination and continuance

If the TeleSec Shared Business CA service is terminated, all tenants (master domain subscribers) and the users of the end-entity certificates issued there continue to be bound by the rules in the CPS until the last certificate issued becomes invalid or is revoked.

9.11 Individual messages and communication with subscribers

Provided there is no contractual agreement to the contrary, the respective valid contact information (address, e-mail, etc.) is provided for individual messages and communication with the TeleSec Shared Business CA certification authority (also refer to the “certificate and configuration datasheet” document).

9.12 Amendments

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

9.12.1 Amendment procedures

Amendments to this CPS can only be made by the Change Advisory Board of the publisher (Section 1.5 ff). With every official change, this document receives a new ascending version number and publication date. This also applies in the event that no changes were found after the annual review.

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

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

Within existing contracts, the delegated third party must be informed about modifications to this CPS in writing at least six weeks before they come into force. In the event of modifications to the detriment of the delegated third party, he has the right to special termination at the time the modifications come into effect. If the delegated third party does not terminate the agreement in writing within six weeks after receipt of the change notification, the changes shall become part of the agreement effective from the time they enter into force.

9.12.2 Notification procedures and periods

Tenants will be notified about amendments and are 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 Advisory Board of Telekom Security believes that, for example, significant security-relevant amendments are required immediately, the new CPS will enter into force immediately upon its release (see Section 9.12.1).

9.12.3 Reasons that lead to the object ID having to be changed

The Advisory Board of Telekom Security decides whether the object ID of the CPS needs to be changed. Otherwise modifications do not lead to the object ID of the Certificate Policy having to be changed.

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. The place of jurisdiction shall be Frankfurt am Main.

9.15 Compliance with the applicable law

This 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 this CPS becoming invalid.

9.16 Various provisions

9.16.1 Complete contract

No stipulation.

9.16.2 Assignment of claims

No stipulation.

9.16.3 Severability clause

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

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

No stipulation.

9.16.5 Force majeure

The regulations in the individual agreement apply.

Within the legally permissible framework, contracts with tenants, relying third parties or end entities must contain protection clauses regarding force majeure in order to protect Telekom Security.

This regulation is intended to ensure that Telekom Security agrees with its tenants, relying third parties or end entities that Telekom Security will not fall into arrears if the service is delayed or becomes impossible due to force majeure.

9.17 Other provisions

9.17.1 Accessibility

The general access to the Trust Center of Telekom Security services happens via web browser application. Operating systems offer users who need support due to disabilities (e.g. visual impairment) a variety of tools for better accessibility of applications or web pages.

Furthermore Trust Center of Telekom Security analysis with its software developers if there is a necessity for any additional operation system independent support (e.g. webpages based on HMTL 5) next to the standard features mentioned above.

If the aforementioned technical measures are not sufficient, Telekom Security offers free support via phone for requesting, confirming or revoking a certificate.

ANNEX A: ACRONYMS

BNetzA	German Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railways
BR	Baseline Requirements
BSI	German Federal Office for Information Security
C	Country
CA	Certification Authority
CAA	Certification Authority Authorization
CAB	CA/Browser Forum
CARL	Certification Authority Revocation List
cc	Country Coded
CMP	Certificate Management Protocol
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSPRNG	Cryptographically suitable random number generator
CT	Certificate Transparency
DCF77	Time signal transmitter (long wave transmitter) in Mainflingen near Frankfurt am Main
DIN	German industry standard (Deutsche Industrie Norm)
DK	Dual key
DN	Distinguished Name
DNS	Domain Name Systems
GDPR	General Data Protection Regulation
DV	Domain validation
EDP	Electronic data processing
eIDAS	electronic identification and signature
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standard
FQDN	Fully qualified domain name
GPS	Global Positioning System
GRP	Identifies a group, function or role certificate
GUID	Globally Unique Identifier
HSM	Hardware security module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion detection system
IETF	Internet engineering task force
IPS	Intrusion prevention system
IPSec	Internet Protocol Security
ISMS	Information security management system
ISO	International Organization for Standardization
ISP	Internet Service Providers
ITIL	Information Technology Infrastructure Library
IV	Individual validation
L	Locality
LB	Service specifications (German: Leistungsbeschreibung)

LDAP	Lightweight Directory Access Protocol
MTO	Maximum Tolerable Outage
NCP	“Normalized” Certificate Policy
NIC	Network information center
n.a.	not available
NTP	Network Time Protocol
O	Organisation
OCSP	Online Certificate Status Protocol
OID	Object identifier
opt.	Optional
OU	Organisation Unit Name
OV	Organizational validated
OVCP	“Organizational Validation” Certificate Policy
PED	PIN Entry Device
PIN	Personal identification number
PKI	Public key infrastructure
PKIX	Public key infrastructure X.509
PN	Identifies a pseudonym
PSE	Personal security environment
PU	Productive Unit (Wirkumgebung)
PUK	Personal Unblocking Key
PTC	Publicly trusted certificate
RA	Registration authority
RFC	Requests for comments
RTO	Recovery time objective
RTO	Recovery Time Objective
St	State or Province Name
SAN	Subject Alternative Name
SBCA	Shared Business CA
SCEP	Simple Certificate Enrollment Protocol
SK	Single key
SLA	Service level agreement
SMS	Short Message Service
SOAP	Simple Object Access Protocol
RSA	Rivest Shamir Adleman
RSASSA-PSS	RSA Probabilistic Signature Scheme
S/MIME	Secure multipurpose Internet mail extension
SCT	signed certificate timestamp
SHA	Signature Hash Algorithm
SigG	German Digital Signature Act
SN	Serial Number
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TC	Trust Center
TLD	Top Level Domain
TLS	Transport layer security
TK	Triple key
TSP	Trust Service Provider
TU	Test Unit (Test-Umgebung)
UPN	User principal name

URL	Uniform resource locator
UPS	Uninterruptible power supply
UTC	Universal time coordinated
XML	Extensible markup language

ANNEX B: DEFINITION OF TERMS

Abbreviation	Description
Affiliated company (affiliate)	For example, a company, partnership, joint venture, corporation, (capital) company, association, foundation, or other organization (legal person) that supervises, is supervised by, or is controlled together with another organization (legal person), facility, department, governmental unit, or unit that is directly subordinate to a governmental authority.
Application software provider	A provider of Internet browser software or other application software on the relying side that displays or uses certificates and contains root certificates.
Area of responsibility	Hierarchically subordinated sub-section of the master domain that is managed by a sub-registrar.
Authentication	Checking an identity based on claimed characteristics.
Authorization document	The documentation that proves a requester is authorized to request one or more certificates for a certain natural person, group of persons or functions or device. This may also be a document from the certification authority regarding communication with the person or organization in question.
Bulk	Function of the Shared Business CA with which the sub-registration authority can generate soft PSEs in bulk.
Central repository	An online database that contains public PKI documents (e.g., Certificate Policy, Certificate Practice Statement, CA certificates) as well as additional information, either in the form of a CRL or an OCSP response.
Central registration model	Following successful registration, the sub-registrar requests the certificate on the sub-registrar website (using a web form or in bulk) and directly receives this certificate or the key material for the end entity (except in the case of a registrar certificate)
Certificate	An electronic document that uses a digital signature to bind a public key to an identity (e.g., person, device).
Certificate data	Certificate requests and associated data (obtained from the requester or elsewhere) that is in the possession of the certification authority (CA), is subject to monitoring by the CA or that the CA has access to.
Certificate holder	A natural person who is issued a certificate and is legally bound by a Service and Usage Agreement TeleSec Business CA.
Certificate management process	Processes, practices and procedures relating to the use of keys, software and hardware that the certification authority (CA) uses to check certificate data, issue certificates, maintain a central data repository and revoke certificates.
Certificate Management Protocol (CMP)	The Certificate Management Protocol is a protocol developed by the IETF to manage X.509 certificates within a public key infrastructure (PKI). The protocol regulates the interaction between the components of a PKI. With regard to the TeleSec Shared Business CA, this is used between the certification authority (CA) and the delegated third party.
Certificate Policy (CP)	Defines the guidelines for generating and managing certificates of a certain type.
Certificate problem report	Complaints due to suspicion that the key is at risk, certificate misuse or with regard to other types of fraudulent behavior, risk, misuse or incorrect behavior in connection with certificates.
Certificate request	A request made in electronic or written form that contains data regarding a requester.

Certificate revocation list (CRL)	A regularly updated, time-stamped list of revoked certificates that is generated and signed digitally by the issuing certification authority (CA). The authority revocation list (CARL) is a special certificate revocation list (CRL), as it contains only revoked Intermediate CAs/sub-CA certificates.
Certificate signing request (CSR) [TC]	A certificate request that is created electronically by a device (e.g., server) and signed using the private key, which contains the public key and the certificate data in coded form. The syntax is described by the standard PKCS#11.
Certificate transparency (CT)	A Google project for certificate transparency: the certificates issued are written to publicly verifiable, manipulation-proof log servers in order to allow improperly or incorrectly issued TLS/SSL certificates to be identified faster and revoked. The requisite CT log servers are contacted while the certificate is being issued by ServerPass EV. These, in turn, return one SCT each in their response, which are then stored in the certificate and prove that the certificate was registered in a log server.
Certification authority (CA)	An organization that is responsible for generating, issuing, revoking and managing certificates. This term is used for both root certification authorities (root CA) and subordinate certification authorities (sub-CA).
Certification Authority Revocation List (CARL)	List showing digital certificates that have been revoked by certification authorities (except root CA). Before a digital certificate of a certification authority is used, the CARL should be used to check whether the certificate may still be used.
Certification Authority Authorization (CAA)	A procedure that allows the domain owner to specify in the DNS which certification authority (or authorities) can issue certificates for its domain(s).
Certificate Policy (CP)	A set of rules that specifies the options for using a named certificate in a certain community (parties involved in PKIs) and/or a PKI implementation with common security requirements.
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.
Chip card	Plastic card with an integrated computer chip. Telephone cards are an example of these. If the computer chip is able to perform calculations, it is also called a smartcard. Smartcards can also be used for cryptographic applications.
Compromise	A private key is compromised if it is made known to unauthorized persons or can be used by them. A compromise could occur through a criminal attack for example.
Country	Either a member of the United Nations or a geographical region that at least two member states of the UNO recognize as a sovereign state.
crt.sh	A Certificate Transparency Log search engine.
Cryptography	Science dealing with the encryption of data and related issues (such as digital signatures).
Delegated third party	A natural person who is not identical to the certification authority (CA) but is authorized by this authority to support the certificate management process by performing tasks to fulfill one or more requirements. The following “delegated third parties” can be found in the context of the Shared Business CA PKI solution: External registration authority (external RA); this also includes the “derivative” of the Registration authority of a company (enterprise RA)

Device	Component such as a router, server, gateway or application that supports certificate-based functions but cannot request certificates itself or can do so only to a limited extent. Frequently certificates are requested via an authorized person (e.g., administrator) and installed on the component.
Device certificate	X.509 V3 certificate that contains either a host name, an IP address or an e-mail address in the commonName field (CN) of the certificate holder's distinguishedName (subject) and/or in at least one subjectAltName extension.
Digital signature	A checksum created with a special mathematical procedure. Guarantees the authenticity of the signatory and the integrity of the data.
Directory service	Data repository for calling up certificates and certificate validation information (revocation list).
Distinguished Name	Format with which unique names can be specified according to the X.500 standard. A digital certificate must contain a DN.
Domain authorization document	The documentation that the domain name registrar, a registered domain owner (domain name registrant) or the person or organization that is listed as the registered domain owner in WHOIS (including all private, anonymous or proxy registration services) provides and that proves the requester's authorization to request a certificate for a particular domain name space. This may also be a document from the certification authority regarding communication with the person or organization in question.
Domain name	The name that is given to a node in the Domain Name System (DNS)
Dual key certificate	Variant in which separate key pairs are used for encryption and signing. This means the user has two corresponding certificates.
End entity	Also see certificate holder. The term end entity is largely used in the X.509 environment.
End-entity certificate	A certificate that does not use the "certification authority" basic constraint and therefore cannot sign certificates itself.
ETSI certification	Check and confirmation for certification authorities by an independent expert to ensure that the PKI is operated in accordance with the "ETSI EN 319 411-1" ETSI criteria. The aim of ETSI audits is to strengthen demand-side trust in electronic business transactions. For the Shared Business CA, certification is in accordance with the NCP/OVCP PTC-BR policy.
External registration authority	An employee (staff member) or representative of a company that is not affiliated with the certification authority (CA) (non-affiliate) that approves certificates for third parties. At the SBCA, these roles (trusted roles) are performed by the tenant's master and sub-registrar or authorized representative.
Fully qualified domain name (FQDN)	Correct and complete domain name, i.e., a chain of all labels for a path in the domain name space (for further information see RFC2181).
Hardware security module (HSM)	Hardware to generate and store private keys securely.
Hash value	In this context, a fixed length cryptographic checksum (the correct name is cryptographic hash value). It should be as unlikely as possible to calculate the entry from the hash value or to find several possible inputs for the same hash value (hash value is used as a synonym for fingerprint). In most cases a hash value is signed instead of a complete digital document.
Identification	The process of providing the identity of a subject or object (e.g., user, device) to a system. The identification is part of the validation.
Interface	An interface is part of a system that is used for communication (input and output).

Internal registration authority	An employee (staff member) or representative of a CA who checks the “domain” specified by the PKI tenant and provides it for the certificate request. At the SBCA, this role (trusted role) is performed by the Trust Center operator.
Internal server name	A server name (which may or may not contain a registered domain name) that cannot be dissolved with the public Domain Name System (DNS).
Issuer Distinguished Name (issuer DN)	Format with which unique names can be specified according to the X.500 and the LDAP standard. The issuer DN describes the CA issuing the certificate in a unique way.
Issuing certification authority (CA)	The certification authority (CA) that issued a specific certificate.
Key backup	Mechanism for backing up keys. In order to be able to restore encrypted e-mails in the event of key loss, we recommend backing up the key material of the encryption key. Key backup is also used as a synonym for key archiving.
Key compromise	A private key is considered to be compromised if its value is shared with an unauthorized person, an unauthorized person has access to it, or there is a practical method that an unauthorized person could use to find out its value.
Key pair	The private key and its corresponding public key.
Key owner	A natural person authorized by the delegated third party who is responsible for the proper use (distribution, use and, if necessary, revocation) of the key pair and certificate that was issued for a group of persons or functions or device.
Key backup	Mechanism for backing up keys. In order to be able to restore encrypted e-mails in the event of key loss, we recommend backing up the key material of the encryption key. Key backup is also used as a synonym for key archiving.
Key recovery	Mechanism for recovering keys. This can be necessary if users lose their key (such as through a damaged file).
Latency period	Period of time between an action and the occurrence of a delayed reaction (delay period). With latency periods, the action occurs unnoticed and is only discovered through the reaction.
Legal person	A company, group, partnership, sole trader, trust, government authority, or legal entity with legal standing within the legal system of a country.
LDAP server	Server that saves the information that can be called up via LDAP.
Lightweight Directory Access Protocol (LDAP)	Protocol for querying directories. This has displaced the significantly more complicated Directory Access Protocol (DAP) in many areas. LDAP provides more options than HTTP and FTP (such as setting up a context that can be maintained using several queries). LDAP is used in particular to query digital certificates and revocation lists within public key infrastructures.
Local registration model	The user requests the certificate via the user website or by sending an e-mail request, or the device uses its SCEP interface to request the certificate. This request is processed by the sub-registrar (approval, rejection or deferral (resubmission))
Mail security	Security functions such as digital signature and encryption that support standard mail applications.
Management system for information security (ISMS)	The management system for information security (ISMS) represents a set of procedures and rules within a company that serve to define, manage, monitor, maintain, and continually improve information security over the long term. The term is used in the ISO/IEC 27002 standard; ISO/IEC 27001 defines an ISMS.

Multi-tenant capability	In information technology (IT), multi-tenant capability refers to the property of software or a server to map multiple, fully separated clients on one installation. The respective tenants (e.g., legal units or companies) are unable to view the data, user administration or similar of the other parties/tenants.
Master domain	Independent administrative area within a Shared Business CA that has a unique name and is set up exclusively for a delegated third party. The delegated third party can approve and manage certificates within the tenant. The tenant is managed using the master registrar certificate. Further information is available under: Tenant
Master registrar	Natural person (trusted role) who manages the master domain.
Non-registered domain name	A domain name that is not a registered domain name.
Service and Usage Agreement TeleSec Business CA	Provisions regarding safekeeping and permitted usage of an issued certificate in accordance with the specified requirements if the applicant/certificate holder is an affiliated company of the certification authority (CA), for example.
Object identifier (OID)	A unique, alphanumeric or numeric identifier that is registered for a specific object or object class of the International Standards Organization (ISO) under the appropriate standard.
Online Certificate Status Protocol (OCSP) [BR]	A protocol for online certificate validation with the help of which the application software on the relying side can determine the status of an identified certificate. Also see OCSP responder
OCSP responder	An online server that is subordinate to the certification authority (CA) and is connected to its central repository to process certificate requests. Also see Online Certificate Status Protocol (OCSP)
Period of validity	The period from the issue date (not before) until the expiry date (not after).
Permitted Internet domains	A domain name that consists of the top-level domain and further sub-domains and is added to the tenant's PKI configuration (master domain) as a “permitted Internet domain” following a successful check by the internal registration authority.
Permitted public data source	An authentication document or a data source (e.g., identity database, commercial register) that is used to check subject identity data, that is generally recognized by commercial companies and authorities (public administration) as reliable and that a third party created for a different purpose other than the issuing of certificates by the applicant.
Personal identification number (PIN)	Secret code used at cash machines, for example.
Personal security environment (PSE)	Security-relevant information such as the private key is saved in the personal security environment. The PSE can be available as an encrypted file or on a smartcard and is protected by a password or a PIN.
Person authorized to revoke	A person who is authorized by the certificate holder or key owner to revoke a certificate for a group of persons or functions or device. Authorization is via the certificate revocation password.
Personal security environment (PSE)	Security-relevant information such as the private key is saved in the personal security environment. The PSE can be available as an encrypted file or on a smartcard and is protected by a password or a PIN.
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 or explanation that determine the security level for creating and using certificates. A distinction is made between Certificate Policy (CP) and Certification Practice Statement (CPS).
Power of attorney	Power of attorney is understood to be a power of representation founded on a legal transaction. The power of attorney is established through unilateral declarations of intent that the principal must communicate to the agent of the power of attorney.
Private key	The key from a key pair that the key owner keeps secret and uses to create digital signatures and/or decrypt electronic data and files that were encrypted using the corresponding public key.
Public key	The key from a key pair that the owner of the corresponding private key is permitted to make publicly available and that the relying side uses to verify digital signatures that were created using the owner's private key and/or to encrypt messages that can only be decrypted using the owner's corresponding private key.
Public device certificate	A device certificate that was issued in the CA hierarchy by an issuing CA below a public root certificate.
Public Key Infrastructure X.509 (PKIX)	IETF standard that standardizes all relevant parts of a PKI.
Public Key Service (PKS)	Service of the Trust Center of Telekom Security for issuing and administrating certificates that comply with the German Digital Signature Act.
Public Key Infrastructure	Hardware, software, persons, procedures, rules, guidelines and obligations that enable certificates and keys to be generated, issued, managed and used reliably based on the public key cryptography.
Qualified auditor	A natural or legal person who meets the specified criteria.
Registered domain name	A domain name that is registered with a domain name registration authority (registrar).
Registration authority (RA)	A legal person who is responsible for identifying and authenticating certificate subjects. However, this is not a CA and therefore does not sign or issue certificates. An RA can provide support when requesting or denying a certificate or in both cases. When "RA" is used as an adjective to describe a role or function, this does not necessarily refer to an independent authority. It can, however, be part of the CA. The following registration authorities can be found in the context of the Shared Business CA PKI solution: Internal RA External RA incl. enterprise RA derivative
Registration model	As standard, the Shared Business CA supports two different registration models: Central registration model (see that item) Decentral registration model (see that item)
Registration authority of a company (enterprise RA)	An employee (staff member) or representative of an organization that is not affiliated with the certification authority (CA) (non-affiliate) that approves certificates for third parties. At the SBCA, these roles (trusted roles) are performed by the tenant's master and sub-registrar or authorized representative.
Relying party	A natural or legal person who relies on a valid certificate. A provider of software is not a relying party if the software this provider sells merely contains information on a certificate.
Request for a certificate with increased risk	A request for which the CA provides an additional check with regard to internal criteria and databases that the CA runs. This can concern names that are subject to a high risk with regard to phishing or other fraudulent use, names that are contained in previously rejected certificate requests or revoked certificates, names that are on the

	MillerSmiles phishing list or the Google Safe Browsing list or names that the CA identifies based on its own risk-minimization criteria.
Requester	The natural person who requests a certificate (or its renewal). Once the certificate has been issued, the requester is referred to as the certificate holder. In the case of certificates issued for devices, the requester is the organization that controls or operates the device listed on the certificate, even if the device sends the actual certification request.
Requester's representative	If different from the requester, this is a natural person or cost bearer, an employee of the requester or an authorized agent who is explicitly authorized to represent the requester: (i) who signs, submits or approves a request for a certificate in the name of the requester and/or (ii) signs and submits a subscriber agreement in the name of the requester and/or (iii) acknowledges and agrees to the certificate's Service and Usage Agreement TeleSec Business CA in the name of the requester if the requester is an affiliated company (affiliate) of the certification authority (CA).
Revocation authority	An employee (staff member) or representative of an organization who performs certificate revocations.
Rivest Shamir Adleman (RSA)	Procedure for encryption, for digital signature, and for the secure transmission of keys that is named after the three cryptographers Rivest, Shamir, and Adleman.
Root CA	See root certification authority.
Root certification authority (root CA)	The highest level certification authority whose root certificate is distributed by application software providers and who issues the subordinate CA certificates (sub-certificates).
Root certification authority certificate (root certificate)	The self-signed certificate that the root certification authority (root CA) issues for self-identification. In addition, this certificate helps with the validation of issued sub-certificates.
Secure Multipurpose Internet Mail Extension (S/MIME)	Secure Multipurpose Internet Mail Extension. Extension of the MIME e-mail format, which describes additions for cryptographic services that guarantee the authenticity, integrity, and confidentiality of messages.
Secure Socket Layer (SSL)	Crypto protocol for ensuring end-to-end connections on the Internet, now replaced with the newer TLS procedure. Can be used instead of the more complex IPSec in many cases.
Service desk	The service desk is an organizational unit within a company that serves as the tenant or delegated third party's central contact point for all service and support requests and that conveys these within the company in accordance with the agreed business processes.
Simple Certificate Enrollment Protocol (SCEP)	Simple Certificate Enrollment Protocol. Protocol for ordering and loading certificates in IPSec devices.
Simple Object Access Protocol (SOAP)	Simple Object Access Protocol: SOAP provides a simple mechanism for exchanging structured information between applications in a decentralized, distributed environment.
Single key certificate	Variant in which the same key pair is used for encryption and signing. This means the user has one certificate.
Software PSE (Soft PSE)	An encrypted file for saving the certificate and the corresponding private and public keys.
Smartcard	A special plastic card with an integrated computer chip that can also be used for cryptographic applications.
Subscriber agreement	An agreement between the certification authority (CA) and the requester/certificate holder that specifies the rights and obligations of the parties.
Subject Alternative Name	Additional fields in a certificate. The fields can be used to enter additional names of the certificate holder. This is a standard extension of the X509 standard.

Subject Distinguished Name (Subject DN)	Format with which unique names can be specified according to the X.500 and the LDAP standard. The Subject DN uniquely specifies a person or device.
Subject	The natural person, device, system, unit or legal person that is named as the subject in a certificate. The subject is either the certificate holder or a device that is under the certificate holder's control or is operated by this person.
Subject identity data	Data that identifies the subject of the certificate. Subject identity data does not contain a domain name that is listed in the subjectAltName extension or the Subject commonName field.
Subordinate certification authority (sub-CA)	A certification authority whose certificate is issued by a root certification authority (root CA) or another subordinate certification authority (sub-CA).
Sub-registrar	Natural person (trusted role) who manages the area of responsibility.
Suspension	In the context of PKI, suspension means a provisional or temporary revocation. The certificate initially appears in the certificate revocation list, but can be re-activated by the sub-registrar.
Tenant	The tenant is a separate, logically self-contained unit with its own legal, organization and data management within the system. The tenant thus structures the use of the system. At SBCA, the master domains are known as tenants. Within the master domains, there are further subdivisions in the form of areas of responsibility (also known as sub-domains). Further information is available under: Tenant
Transport Layer Security (TLS)	Crypto protocol for ensuring end-to-end connections on the Internet.
Triple key certificate	Variant in which separate key pairs are used for encryption and signing and Microsoft smartcard logon. This means the user has three corresponding certificates.
Trustworthy certificate	A certificate that is trusted due to the fact that its corresponding root certificate represents a trust anchor in widely distributed application software.
Advisory Board of Telekom Security	A board within Telekom Security that decides on PKI functions.
Validation	Evidence of the reproducibility of a result from a described procedure under defined conditions. The more precisely a procedure is described and the fewer unknown influencing factors there are, the more certain it is that corresponding results will be produced. A description of the goal and method is required for a validation. In this context, valid means that the method leads to the result in a repeatable manner. In the context of a PKI, there is a validation process at the following points: Determining and checking an identity (e.g., natural person, device) for a certificate request. Algorithm to check a certificate for its validity period, issuing certification authorities and certificate status (valid, revoked).
Valid certificate	A certificate that passes the validation procedure described in RFC5280.
Validation specialist	Someone who performs the data validation tasks in accordance with the requirements in question. In the context of the Shared Business CA, this involves the following roles: ▪ Trust Center operator ▪ Master registrar ▪ Sub-registrars (and their derivatives)

Wildcard certificate	A certificate that has an asterisk (*) in the left-most position of a fully qualified domain name of the subject contained in the certificate. This feature is not supported in the context of the Shared Business CA.
X.509	Standard whose most important element is a format for digital certificates. Version X.509v3 certificates are supported in all common public key infrastructures.
zLint	A Certificate Transparency Log search engine.

ANNEX C: REFERENCES

[CAB-BR]	Version of the “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” document published by CA/Browser Forum at https://cabforum.org/baseline-requirements/ valid at the time.
[Trust Center CP]	Version of the „Telekom Security Certification Policy“ document published from the Trust Center at https://www.telesec.de/de/service/downloads/pki-repository valid at the time.
[CP/CPS Class2]	CP or CPS of the T-TeleSec GlobalRoot Class 2
[CP/CPS DTIRCA1]	CP or CPS of the Deutsche Telekom Internal Root CA 1
[CP/CPS DTIRCA2]	CP or CPS of the Deutsche Telekom Internal Root CA 2
[ETSI NCP OVCP]	ETSI EN 319 411-1 V1.1.1 (2016-02), European Telecommunications Standards Institute, “Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates”, policy NCP and OVCP
[ETSI EN TSP]	ETSI EN 319 401 V1.1.1 (2012-03), Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures
[EU-GDPR]	General Data Protection Regulation (GDPR) 2016/679, entered into force on May 25, 2018
[ISAE3402]	ISAE3402 Report, International Standards for Assurance Engagements, http://isae3402.com/ISAE3402_reports.html
[SBCA PITR]	Personnel, infrastructure and technical framework conditions of the TeleSec Shared Business CA (SBCA)
[PKCS]	RSA Security Inc., RSA Laboratories “Public Key Cryptography Standards”, http://www.rsasecurity.com/rsalabs
[PKIX]	RFCs and specifications by the Public Key Infrastructure (X.509) IETF working group
[RFC3647]	Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003
[RFC5280]	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
[RFC6844]	DNS Certification Authority Authorization (CAA) Resource Record, P. Hallam-Baker, R. Stradling IETF, 2013
[RFC6960]	X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, S. Santesson et. al., IETF, 2013
[RFC6962]	Certificate Transparency
[SBCA security concept]	Shared Business CA security concept, Ver. 04.00
[FSC TC]	Framework security concept of the Trust Center information network
[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
[Apple-Root-CA]	Apple Root CA Program, https://www.apple.com/certificateauthority/ca_program.html

ANNEX D: SUPPLEMENTARY LITERATURE

Basic documentation

- Service specifications (SS)
- Service level agreement (SLA)
- Framework SLA for Trust Center services
- Personnel, infrastructure and technical framework conditions (PITF)
- Installation instructions for RA workstation

Work instructions, interface descriptions and role-specific manuals

- Work instructions for customers
- Master registrars' manual
- Sub-registrars' manual
- User manual
- SCEP interface
- Mail interface