Deutsche Telekom Corporate PKI (DTAG cPKI)

Certificate Policy (CP) & Certificate Practice Statement (CPS)

Deutsche Telekom Security GmbH

Version:	08.00		
Revision:	8.0	**Status:**	Released
Valid from:	14.07.2020	**Classification:**	Public
Author:	Deutsche Telekom Security GmbH		

DEUTSCHE TELEKOM SECURITY GMBH
Address: Bonner Talweg 100, 53113 Bonn | Postal address: Bonner Talweg 100, 53113 Bonn
Phone: +49 228 181-0 | E-mail: info@telekom.de | Internet: www.telekom.de/security
Board of Management: Thomas Fetten (spokesperson), Dr. Klaus Schmitz, Thomas Tschersich
Commercial register: Bonn, local court, HRB 15241, registered office, Bonn | VAT identification no. DE 254595345
WEEE-Reg.-Nr. DE 56768674

Publication details

Published by

Deutsche Telekom Security GmbH
Trust Center Operations
Untere Industriestrasse 20
57250 Netphen
Germany

File name	Document number	Document name
CP-CPS_CPKI DTAG_SecureEmail_20200714_v.08.00_EN.pdf	08.00	Certificate Policy (CP) and Certification Practice Statement (CPS) of Telekom AG (DTAG) Corporate PKI

Version	Last revised	Status
08.00	24.07.2020	Released

Contact	Phone/fax	Email
Deutsche Telekom Security GmbH Trust Center Operations	+49 1805-268204 1	telesec_support@t-systems.com

Brief summary

Certificate Policy (CP) and Certification Practice Statement (CPS) of Telekom AG (DTAG) Corporate PKI Next Generation (cPKI). This document describes the security level required for operating the cPKI and includes security instructions as well as explanations of technical, organizational, and legal aspects.

DEUTSCHE TELEKOM SECURITY GMBH
Address: Bonner Talweg 100, 53113 Bonn | Postal address: Bonner Talweg 100, 53113 Bonn
Phone: +49 228 181-0 | E-mail: info@telekom.de | Internet: www.telekom.de/security
Board of Management: Thomas Fetten (spokesperson), Dr. Klaus Schmitz, Thomas Tschersich
Commercial register: Bonn, local court, HRB 15241, registered office, Bonn | VAT identification no. DE 254595345
WEEE-Reg.-Nr. DE 56768674

Change history/release notes

Version	Last revised	Author/editor	Changes/comments
0.1	Feb. 14, 2008	CR	First draft
0.1a	Mar. 11, 2008	SK	Changes for RFC 3647-conformity
0.1b	Mar. 18, 2008	SK	Changes for European Bridge CA
0.2	Mar. 25, 2008	SK	English headlines, new Corporate Design
0.3	May 28, 2008	SK	Added remarks for European Bridge CA-conformity after meeting with ChR, TP.
0.4	Oct. 7, 2008	SK	General changes
0.5	Oct. 10, 2008	SK	Revised version, first official draft
0.6	Dec. 23, 2009	JP	Completion for coordination and formal release
0.7	Apr. 2, 2010	KK TP JP MD	Additions
0.8	Jun. 22, 2010	MD	Change of headings to English, cPKI expansion stage 1 (CMO)
0.9	Jun. 23, 2010	MD	cPKI expansion stage 2 (FMO)
0.91	Jul. 15, 2010	JP	Separation of CPS documents for CMO and FMO
0.99	Nov. 24, 2010	JP KHR	Review and processing of open items
1.0	Jun. 15, 2011	CR, SK, JP, MD	Final review and creation of version 1.0
1.1	May 12, 2014	JP	Review and change due to the rollout of cPKI as the successor service to the previous iPKI/cPKI. Establishment of web trust conformity. Highlighting of items that still need to be clarified.
1.2	Mar. 25, 2015	KHR OS	Content checked Released
1.3	Oct. 10, 2015	KHR	Adjusted for pseudonym certificates.
1.4	Mar. 4, 2016	KHR	Review and change due to the rollout of function, group, and pseudonym certificates. Establishment of web trust conformity
1.5	Nov. 9, 2016	KHR	Change of CAs to SHA-256 including the new fingerprints. Adjustment to ensure ETSI-conformity Revision of Chapters 1, 2.2, 6, 7, 8, and A.2
2.0	Nov. 21, 2016	KHR, OS	Content checked Line breaks applied, spelling, missing references updated, code signing and computer certificates added to Chapter 7.1.2 Tele-Grotesk font formatting
2.01	Nov. 22, 2016	KHR, TB, OS	Content checked Spelling, adjustment to Chapter 1 (division into internal and public CAs), 1.4.1 (replacement graphic) and additions in 7.1.2

2.02	Nov. 22, 2016	KHR, OS	Content checked Released
2.03	Nov. 1, 2017	KHR, OS	Annual review, content checked Released
2.1	Apr. 18, 2018	KHR, OS	Chapters 1 et seq. and 2 et seq. adjusted due to the commissioning of new CAs Content checked Released
3.18	Aug. 2, 2018	KHR	Full revision based on ETSI Change to CAs Trust Center relocation Version for review
3.19	Aug. 2, 2018	OS	Quality assurance/review
3.20	Aug. 3, 2018	KHR	Finalization, release, and publication of this version
3.21	Aug. 30, 2018	KHR	Adjustment to Chapters 3.23: 4.1.2.1; 5.2.3.2; 5.3.1.2; 5.3.2.2: 5.3.3.2: 5.3.4.2; 5.3.6.2; 5.3.8.2 change from registration to authentication, or identification.
3.22	Sep. 25, 2018	KHR	Adjustment Chapters 3.2.3 and 3.2.5 authorization deadlines Chapter 1.3.1.2.1 usage period of issuing CA 1 under GlobalRoot Class 2 Chapter 1.5.4 duplicate sections deleted Link to the cPKI website adjusted to https://corporate-pki.telekom.de and updated in the entire document Chapter 4.10.1 OCSP RFC 2560 updated to RFC 6960 Chapter 7 et seq. – missing text inserted in footnotes
3.23	Sep. 26, 2018	KHR	Management of user access rights added to Chapter 6.7 and Trust Center connection changed
3.24	Oct. 10, 2018	KHR	Changes due to requirements in Mozilla 2.61 = CA communication Sep. 2018 Update CP/CPS and CAB Ballot SC6 Version 3: Revocation Timeline Extension: Chapters 1.3.1, 1.5.2, 2.1, 2.2, 2.4, and 3.1.1.1.6 added; in Chapters 3.2.2.2.1, 3.2.5.2, 3.3, 4.2.2.1.1, and 6.3.2 "27 months" has been replaced with "825 days"; Chapter 3.2.2.2 updated; Chapters 3.2.5.2, 3.2.5.3, and 4.1.2.2 updated; Chapter 3.4 internet address updated; Chapter 4.3 updated; Chapters 4.9.7, 4.9.1.1, 4.9.3.2, and 4.10.1 updated; changes to Chapters 5 and 6; Chapters 7.2 and 8 updated; Chapter 9.17.1 added; Chapter 9.17.1 added
3.25	Nov. 5, 2018	KHR	Adjustments due to TÜV queries; inclusion of Chapter 8.17.1 Accessibility More details on the position of the certificate request by the requester (subject) and consent to the Terms of Use in Chapters 4.1.1 and 4.1.2.1
3.26	Nov. 14, 2018	KHR	Adjustment of certificates for legal persons in Chapters 3.2.3, 3.2.3.5, 4.1.2.2.1, 4.1.2.4, 4.2.1.2, 4.2.3.2.1, and 4.3.1.2.1 Incorporation of assurance of data consistency between the various directory inquiry services (OCSP and CRL) 4.9.7

3.27	Jan. 9, 2019	KHR	Adjustment to Chapter 3.1 Naming rules et seq. Due to inclusion of GivenName and Surname for natural persons in the SDN
3.28	Jan. 28, 2019	OS	Review
4.00	Feb. 7, 2019	KK	Released
4.01	05.05.2019	KHR	Adjustment to 1.3 u. Chapter 7 Inclusion of new CAs
4.02	05.09.2019	KHR	Adjustment to Chapter 1.3, Chapter 7 Inclusion of Deutsche Telekom AG authentication CA, inclusion of the Mobile Device Sig and LogOn certificates, deletion of the Mobile Device Client certificate,
4.03	29.09.2019	KHR	Adjustment to Chapter 3.2.3 insert an additional graphic for international users and additions in the text
4.04	08.10.2019	TB	Review
4.05	14.10.2019	MB	Review
4.06	24.10.2019	KHR	Review results incorporated and finalized version
04.90	29.10.2019	GK	QS
05.00	30.10.2019	KK	Released
05.01	20.01.2020	KHR	Chapter 4.9.6 and 4.9.4 Incorporating the requirement “An entry MUST NOT be removed from the CRL until it appears on one regularly scheduled CRL issued beyond the revoked certificate's validity period”
05.02	29.01.2020 30.01.2020	KHR	Adaptation wording Chapter 1.5.3 Adjustment Chapter 1.3.3, 4.9.1.1, 4.9.1.2, 4.9.6, 4.9.7, 4.9.10, 4.10.1, 4.10.3
05.03	04.02.2020	KHR	Adaptation Chapter 6.3.2 Validity of OCSP Signer Certificates Adjustments in chapters 1,4.1.3, 1,4.1.4, 1,4.1.5, 3.1.3, 3.2.3, 4.5.1, 6.1.1, 7.1.4, C.2 due to changes in pseudonyms, robots and function groups, as well as inclusion of new CAs
05.04	07.02.2020	KHR	Adjustments in chapters 1.3.1, 6.3.2, 7.1, 7.1.2.4, 7.1.2.5, 7.1.2.9.1, 7.1.2.9.2, 7.1.4, C.2 due to changes in pseudonyms, robots and function groups, as well as inclusion of new CAs
05.05	08.02.2020	KHR	Adjustments in chapters 1.3.1, 1.3.3, 2.2, 2.4, 3.1.1.1.9 due to changes in pseudonyms, robots and function groups as well as inclusion of new CAs
05.06	10.02.2020	OS	Review
05.07	28.02.2020	OS	Quality assurance/review
05.08	04.03.2020	KHR	Adding the operation date of the new CAs. Review results incorporated and version finalized. Creation of the final draft for approval
5.09	17.03.2020	JL	Translation to English
5.10	18.03.2020	KHR	Review results incorporated and finalized version
5.90	18.03.2020	GK	QS
06.00	18.03.2020	DD	Released
06.01	07.04.2020	KHR	Updated Figure 5
06.02	06.05.2020	KHR	Incorporation of the comments of TÜV IT from the last audit in Chapters: 5.3.4.1, 5.2.1, 5.4.1.3, 2.1, 5.4.1, 5.4.1.3, 5.7.3
06.03	30.05.2020	KHR	Change of company name and address of the legal entity due to the transfer of operations from T-Systems International GmbH to Deutsche Telekom Security GmbH as of July 1st, 2020

06.04	03.06.2020	KHR	Adaptation of the footer 1st page
06.05	03.06.2020	OS	Review
06.06	22.06.2020	JL	Review of the English translation
06.07	24.06.2020	KHR	Adjustment of tables 11, 12, 13, 14 due to the change in the CA for pseudonyms, robot accounts, group and function accounts
06,08	25.06.2020	GK	QS
07.00	26.06.2020	DD	Released
07.01	03.07.2020	KHR	Change of Board of Management:
06,08	03.07.2020	GK	QS
07.00	03.07.2020	DD	Released
07.01	24.06.2020	KHR	Modification of tables 11, 12, 13, 14 Due to the change of CA for pseudonyms, robot accounts, group and function accounts
07.02	09.07.2020	KHR	Modification of the footer of the 1st page, inclusion of Thomas Fetten as spokesman of the management. Addition of new CA "Deutsche Telekom AG secure email CA E03" in Chapters 1.1.1, 1.1.2, 1.2, 1.3.1.1.1, 1.3.1.2.1, 2.2, 2.4, 3.2.4, 3.2.5.2, 4.1.2, 6.3.2, 7.1.2 ff, 7.1.5
7.03	14.07.2020	KHR	Addition of new CA "Deutsche Telekom AG secure email CA E03" in Chapters 1.1.1, 1.1.2, 1.2, 1.3.1.1.1, 1.3.1.2.1, 2.2, 2.4, 3.2.4, 3.2.5.2, 4.1.2, 6.3.2, 7.1.2 ff, 7.1.5
7.04	21.07.2020	KHR	Translation of the adaptations from german into english
7.05	23.07.2020	OS	Review
7.06	24.07.2020	GK	QS
8.00	27.07.2020	KK	Released

Contents

List of figures

List of tables

1 INTRODUCTION

The trust center is operated by the Group business unit Deutsche Telekom Security GmbH (hereinafter referred to as "Telekom Security"), which was formed due to the transfer of operations from T-Systems International GmbH as of July 1st, 2020.

In 1998, the Trust Center (under the name of "Trust Center der Deutsche Telekom" (Deutsche Telekom Trust Center)) started operating as the first certification service provider to be accredited in accordance with the German Digital Signature Act (*Signaturgesetz – SigG*).

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

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

Both the structural and the organizational infrastructures meet the strict requirements of the German Digital Signature Act. The services offered by the Telekom Security Trust Center include the TeleSec Public Key Service (PKS), which covers the process of issuing qualified certificates in accordance with the European eIDAS Regulation. The portfolio also includes further services for a wide range of PKI solutions that represent "advanced signatures" in accordance with the specifications of the Digital Signature Act; additional features include one-time password procedures and qualified time stamps.

In 2013, an information security management system (ISMS) was established for the Telekom Security Trust Center, which is certified on the basis of IT baseline protection in accordance with ISO27001. 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 Deutsche Telekom Corporate PKI (cPKI)

The Deutsche Telekom AG Corporate Public Key Infrastructure (hereinafter also referred to as "cPKI") is a central PKI operated in the Telekom Security Trust Center for generating and managing various X-509v3 certificate types that are used for email security, strong authentication (client server), remote VPN, servers, and active network components (e.g., routers, gateways), in particular.

With cPKI, Deutsche Telekom Security GmbH (hereinafter referred to as "Telekom Security") operates a complete PKI solution as an affiliate for Deutsche Telekom AG (hereinafter referred to as "DTAG") represented by Deutsche Telekom IT GmbH (hereinafter referred to as "customer"), whose infrastructure is installed in the highly secure Telekom Security Trust Center and operated by qualified personnel. This PKI creates and manages certificates as electronic proof of identity for employees of the DTAG Group. By using the functions provided by the PKI, each employee is given the opportunity to authenticate themselves reliably to electronic services and to securely exchange information with other communication partners via signature and encryption (e.g., email medium).

The main tasks of the cPKI are the CA processes for issuing, providing, and managing certificates in accordance with the X.509 standard. These processes ensure integrated certificate management in Deutsche Telekom's system infrastructure and management of the key material (encryption key) for interaction with IT systems and users.

All DTAG employees with an Active Directory (AD) account in Germany receive dedicated access to the cPKI, secured by certificate-based SSL/TLS client authentication, in order to use the PKI functions. All security-relevant actions are performed via an encrypted connection (HTTPS).

Various sub-CAs are subsumed under the cPKI itself, which are also hierarchically subordinate to various root certification authorities.

Figure 1 shows the currently valid overview of the "cPKI" service with the root and sub-CAs from which certificates are issued from the certificate issue date July 14, 2020 onwards.

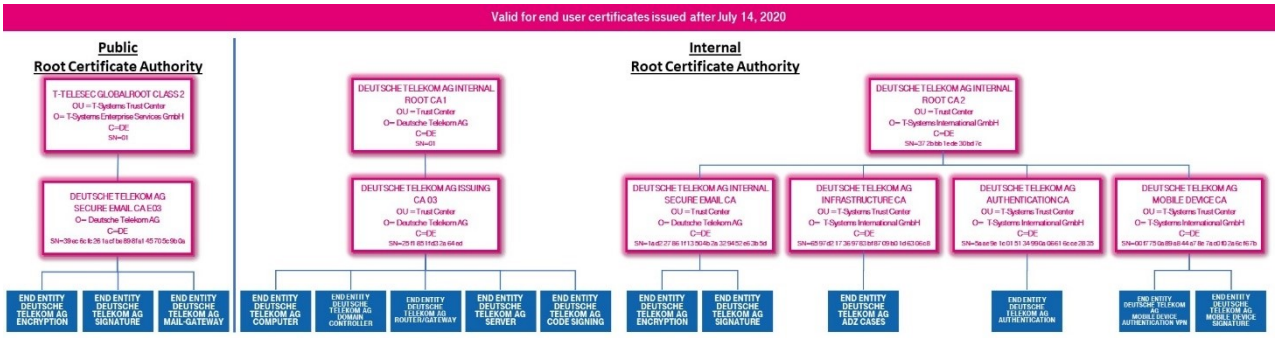

Figure 1: Overview of the "cPKI" service with the root and sub-CAs from the certificate issue date July 14, 2020

Figure 2 shows a graphical overview of the "cPKI" service with the root and sub-CAs from which certificates were issued between March 03, 2020 and July 14, 2020 onwards.

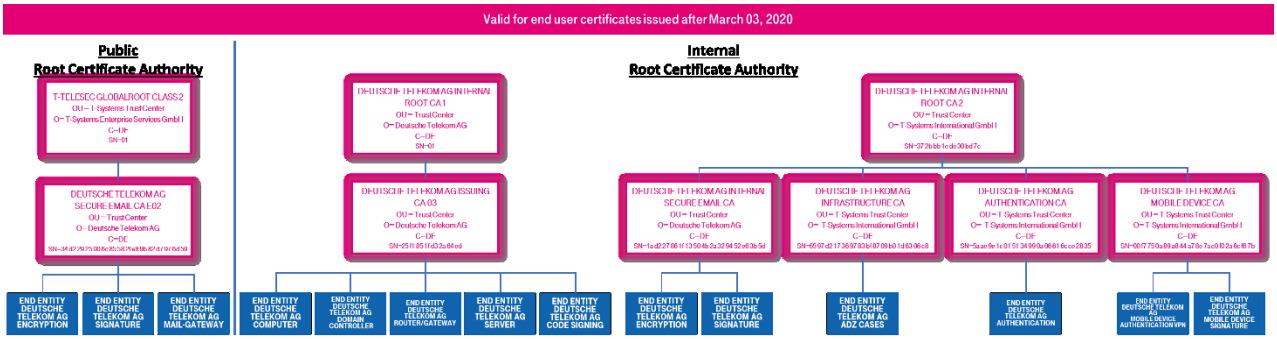

Figure 2: Overview of the "cPKI" service with the root and sub-CAs from the certificate issue date March 03, 2020

Figure 3 shows a graphical overview of the "cPKI" service with the root and sub-CAs from which certificates were issued between July 30, 2019 and March 03, 2020 onwards.

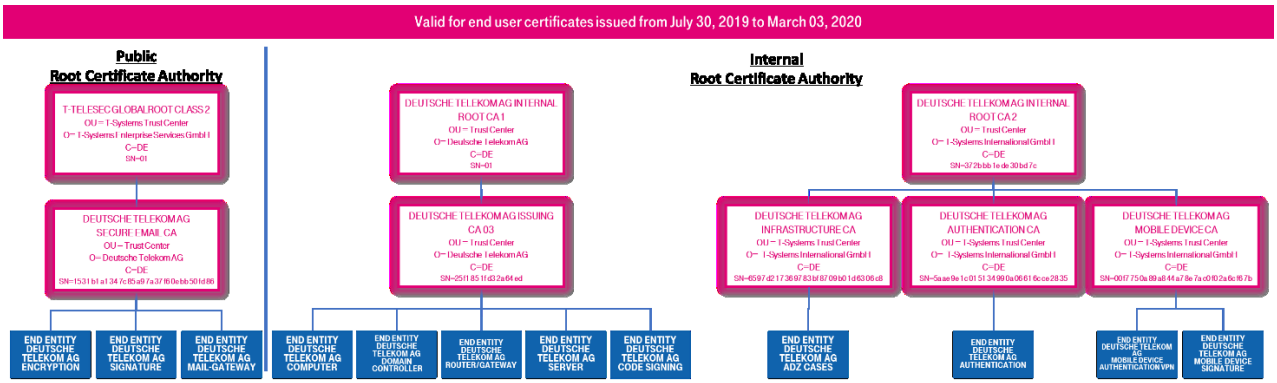

Figure 3: Overview of the "cPKI" service with the root and sub-CAs from the certificate issue date from July 30, 2019 to March 03, 2020

Figure 4 shows a graphical overview of the "cPKI" service with the root and sub-CAs from which certificates were issued between April 29, 2019 and July 30, 2019.

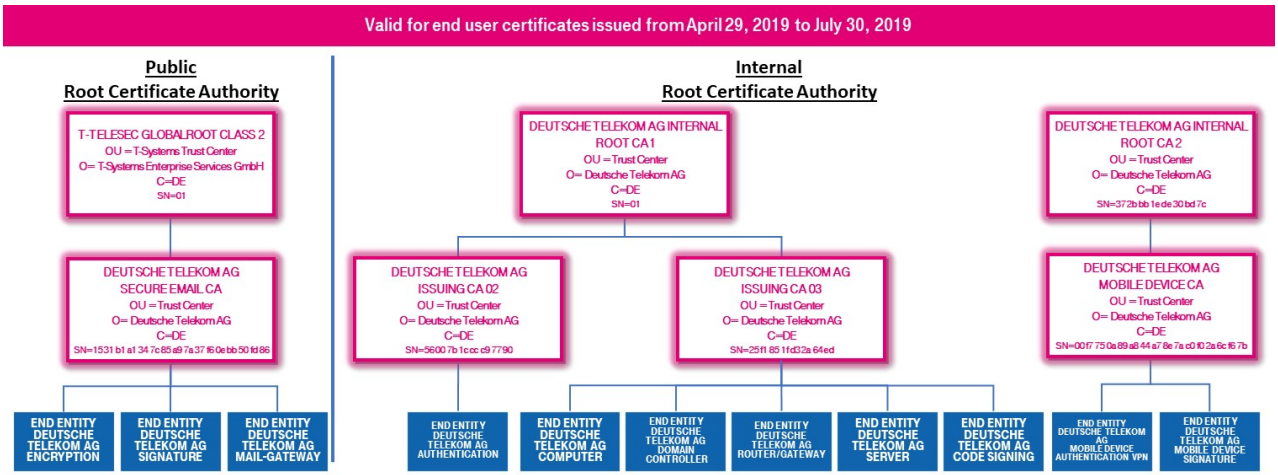

Figure 4: Overview of the "cPKI" service with the root and sub-CAs from the certificate issue date from April 18, 2018 to July 30, 2019

Figure 5 shows a graphical overview of the "cPKI" service with the root and sub-CAs from which certificates were issued between April 18, 2018 and April 29, 2019.

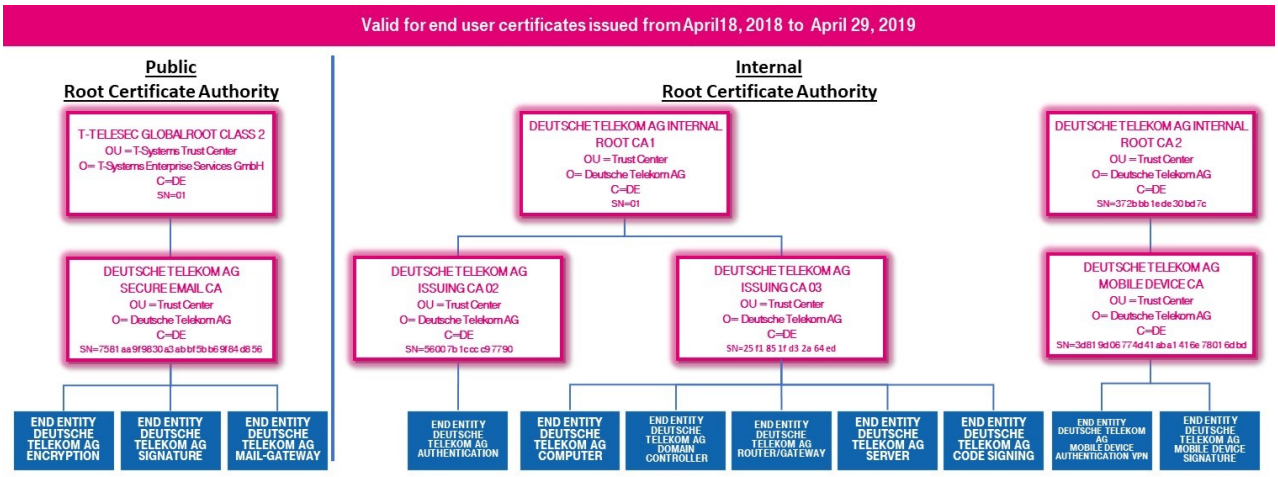

Figure 5: Overview of root and sub-CAs in the certificate issuance period from April 18, 2018 to April 29, 2019

Figure 6 shows a graphical overview of the "cPKI" service with the root and sub-CAs from which certificates were issued between November 8, 2016 and April 18, 2018.

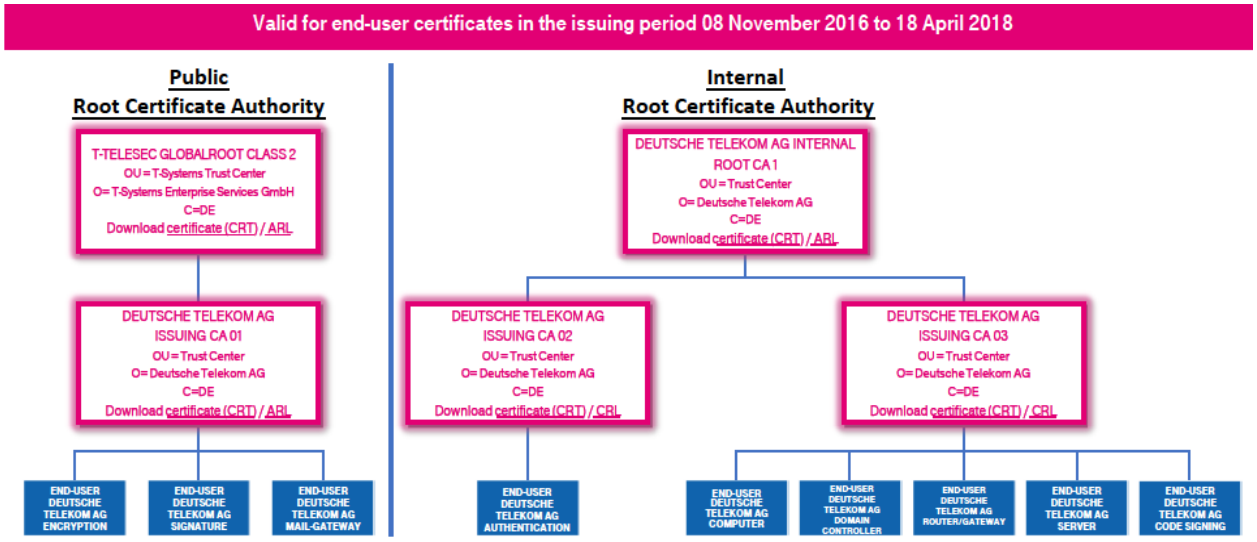

Figure 6: Overview of root and sub-CAs in the certificate issuance period from November 8, 2016 to April 18, 2018

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

The Telekom Security Certificate Policy (CP)/Certification Practice Statement (CPS) of the DTAG Corporate Public Key Infrastructure (cPKI) (hereinafter referred to as "CP/CPS") 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) as well as the registration of end entities.

It makes qualitative assessment of the service offered possible and serves as a decision-making basis for recognizing the certificates issued.

The CPS covers the following regulations in detail:

- Publications and directory service
- Registration 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 CP/CPS follows international standard RFC 3647 "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" [RFC3647] of the Internet Society.

Legal and commercial aspects of the cPKI are contractually regulated in the DTAG Group.

The following table provides an overview of the main user-related features:

Feature	available
Signature certificate (public root)	X
Encryption certificate (public root)	X
Authentication certificate (internal root)	X
Management of certificate life cycle	X
Backup and history for encryption certificates and keys	X
Self-service portal for users	X
Recovery of encryption certificates	X

Table 1: User-related features

The following table provides an overview of the essential features for devices and mobile devices from the internal certification authority:

Feature	available
Authentication certificate (internal CA) Devices, computer (802.1x) certificates (internal CA)	X
Authentication and signature certificates for users on mobile devices (internal CA)	X
Server certificates (internal CA)	X
Router/gateway (internal CA)	X
Domain controller (internal CA)	X
Backup and history for signature certificates and keys for mobile devices (internal CA)	X
Self-service portal for users	X

Table 2: Device- and mobile device-related features

Personal certificates for internal and external employees are always issued using a smart card (MyCard) as the key carrier medium. An exception arises when using mobile devices for encryption certificates of MyCard users and function and group accounts, as well as certificates for machines and certificates required in this context (e.g., authentication), as the deployment and use is software-based as a Software Personal Security Environment (soft PSE).

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

The Telekom Security Trust Center ensures that the "Deutsche Telekom Root CA 2" and "T-TeleSec GlobalRoot Class 2" root CAs with the corresponding sub-CAs meet and comply with the requirements and regulations of the respective currently published version of the [CAB-BR] (http://www.cabforum.org/documents.html).

Furthermore, the Telekom Security Trust Center ensures that the „Deutsche Telekom Issuing CA01“, „Deutsche Telekom AG secure email CA“, „Deutsche Telekom AG secure email CA E02“ and „Deutsche Telekom AG secure email CA E03“ sub-CA under the public root CA meets and complies with the requirements and regulations under ETSI 319411-1 Policy LCP and ETSI 319401.

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

1.2 Document name and ID

Name: Certificate Policy (CP) and Certification Practice Statement (CPS) of the cPKI

Version: 08.00

Last revised: 15.07.2020

OID of this CP/CPS: 1.3.6.1.4.1.7879.13.26

The use of additional object IDs (OID) is described in Chapter 7.1.6.

1.3 Parties involved in PKI

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).

For cPKI, different root and intermediate certification authorities (root CAs, sub CAs) are available, depending on the requirements. Requirements for the root CAs as well as the sub-CA certificates issued by the root CA can be referenced in the CP/CPS of the respective root CA.

Intermediate certification authorities (sub-CAs) that no longer issue end-entity certificates productively will continue to be used for signing revocation lists and/or OCSP responses until further notice.

The root CA and the corresponding sub CA may vary, if

- the certificate of the root certification authority has not yet been implemented as trusted in the application used (e.g., web browser), or
- the application used (e.g., web browser) follows a validation logic that does not check for the direct root certification authority.

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

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 authorities

1.3.1.1.1 Public root certification authorities

The Telekom Security Trust Center operates the "T-TeleSec GlobalRoot Class 2" root CA for advanced certification services. The root CA certificate is a self-signed certificate and is published by Telekom Security online. The publication allows a validity check of all certificates issued in these hierarchies beyond the scope of one's own intranet. The root CA only certifies certificates from direct subordinate certification authorities. In the case of the cPKI, this is "Deutsche Telekom AG Issuing CA 01" until April 18, 2018, the "Deutsche Telekom AG secure email CA" from April 18, 2018 to March 03, 2020, the "Deutsche Telekom AG secure email CA E02" from March 03, 2020 to July 14, 2020 and the "Deutsche Telekom AG secure email CA E03" from July 14, 2020.

The current structure of the CA hierarchy of the cPKI is shown graphically in Figure 1: Overview of the "cPKI" service with the root and sub-CAs from the certificate issue date July 14, 2020.

Regulations regarding public certification authorities are documented in the "Telekom Security PKI - Certificate Policy (CP) and CPS".
Further information as well as the CP and the CPS of the "T-TeleSec GlobalRoot Class 2" can be found at
https://www.telesec.de/de/public-key-infrastruktur/support/root-zertifikate/category/59-t-telesec-globalroot-class-2

Table 3 contains the full Subject Distinguished Name (Subject DN) of the specified certification authorities in accordance with the name forms in Chapter 3.1.1 et seq. as well as the certificate validity.

Issuer	
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
Key sizes of public keys	2048
Encryption algorithm of public keys	RSA
Valid from:	Oct. 1, 2008
Valid to:	Oct. 1, 2033
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

Table 3: Subject DN "T-TeleSec GlobalRoot Class 2"

1.3.1.1.2 Internal root certification authority

To issue certificates for which validation outside the Telekom intranet is not mandatory, the "Deutsche Telekom Internal Root CA 1" and "Deutsche Telekom Internal Root CA 2" are operated in the Telekom Security Trust Center. These root CA instances certify the intermediate certification authorities described in Chapter 1.3.1.1.2.

Regulations regarding the internal root certification authorities are documented in the "Deutsche Telekom Internal Root CA 1" [CP/CPS DTIRCA2] CP/CPS.

The Table 4 contains the full Subject Distinguished Names (Subject DNs) of the specified certification authorities in accordance with the names in Chapter 3.1.1 et seq. as well as the certificate validity.

Issuer		
Common Name (CN)	Deutsche Telekom Internal Root CA 1	Deutsche Telekom Internal Root CA 2
Subject		
Country Name (C)	DE	DE
Organization Name (O)	Deutsche Telekom AG	T-Systems International GmbH
Organizational Unit Name (OU)	T-Systems Trust Center	Trust Center
Common Name (CN)	**Deutsche Telekom Internal Root CA 1**	**Deutsche Telekom Internal Root CA 2**
Signature algorithm	SHA-256	SHA-256
Key sizes of public keys	2048	2048
Encryption algorithm of public keys	RSA	RSA
Valid from:	Nov. 15, 2007	Aug. 3, 2017
Valid to:	Nov. 16, 2027	Aug. 4, 2037
Fingerprint algorithm:	SHA-256	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	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	SHA-1
Fingerprint	15 33 9a a2 30 f5 34 0e 7b fc aa fd 75 4a a1 4c ed d4 98 58	12 f7 14 bd ec 4d 2e 3c 27 82 ce 1f cb 8a fe 19 b8 4a ed 8c

Table 4: Subject DN "Deutsche Telekom Internal Root CA 1 und Deutsche Telekom Internal Root CA 2"

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 mail gateways) for which the intended use requires a public root are issued by the following subordinate certification authority (intermediate certification authority):

- Deutsche Telekom AG Issuing CA 01
- Deutsche Telekom AG secure email CA
- Deutsche Telekom AG secure email CA E02
- Deutsche Telekom AG secure email CA E03

In the event that the intended use of certificates does not meet the specifications of a "public root certification authority" (e.g., for computers, 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."

From March 3rd, 2020, certificates for external employees and pseudonyms will only be issued from the internal non-public intermediate CA.

Table 5 contains the full Subject Distinguished Name (Subject DNs) of the specified certification authorities in accordance with the name forms in Chapter 3.1.1 et seq. as well as the certificate validity.

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

Issuer					
Common Name (CN)	T-TeleSec GlobalRoot Class 2	T-TeleSec GlobalRoot Class 2	T-TeleSec GlobalRoot Class 2	T-TeleSec GlobalRoot Class 2	T-TeleSec GlobalRoot Class 2
Subject					

Issuer					
Country Name (C)	DE	DE	DE	DE	DE
Organization Name (O)	T-Systems International GmbH	Deutsche Telekom AG	Deutsche Telekom AG	Deutsche Telekom AG	Deutsche Telekom AG
Organizational Unit Name (OU)	T-Systems Trust Center	Trust Center	Trust Center		
Common Name (CN)	**Deutsche Telekom AG Issuing CA 01**	**Deutsche Telekom AG secure email CA**	**Deutsche Telekom AG secure email CA**	**Deutsche Telekom AG secure email CA E02**	**Deutsche Telekom AG secure email CA E03**
Serialnumber	00 ee db 86 0e 52 3b 2e 43	75 81 aa 9f 98 30 a3 ab bf 5b b6 9f 84 d8 56	15 31 b1 a1 34 7c 85 a9 7a 37 f6 0e bb 50 fd 86	34 d2 29 25 00 6c 85 58 2f e8 9b 82 d7 97 6d 59	39 ec 6c fc 26 1a cf be 89 8f a1 45 70 5c 9b 0a
Signature algorithm	SHA-256	SHA-256RSA	SHA-256RSA	SHA-256RSA	SHA-256RSA
Key sizes of public keys	2048	2048	2048	2048	2048
Encryption algorithm of public keys	RSA	RSA	RSA	RSA	RSA
Valid from:	Jul. 13, 2016 14:51:48 (GMT)	Jan. 18, 2018 11:04:58 (GMT)	09.04.2019 13:00:18 (GMT)	25.02.2020 10:09:31 (GMT)	09.07.2020 08:22:06 (GMT)
Valid to:	Jul. 13, 2026 23:59:59 (GMT)	Jan. 18, 2028 23:59:59 (GMT)	09.04.2029 23:59:59 (GMT)	25.02.2030 23:59:59 (GMT)	09.07.2030 23:59:59 (GMT)
Fingerprint algorithm:	SHA-256	SHA-256	SHA-256	SHA-256	SHA-256
Fingerprint:	C6 19 30 77 C6 18 9D 1D FB BF 81 3B 87 DC 7C BF 04 98 AC F7 27 88 7B C7 EC 54 32 09 06 DE 9B C8	1A CF 28 AA 8C 53 03 EF E5 C3 01 18 62 39 36 B6 F5 01 F9 4D 3B B7 AD 35 B8 10 B7 64 34 5F 4F 01	D0 80 5A 3E 6A 62 8E 94 05 61 30 23 DE 87 82 7A 76 11 8D C1 16 B6 49 03 D3 E7 5B 9D DF 4B DB 97	02 93 79 11 8e 57 75 22 6c 54 d7 18 2a 36 7a 24 0b 51 77 0f 50 11 bb 35 17 7c fd 17 d9 b2 44 5a	38 CB C8 18 60 C9 04 BD F1 80 46 CD 0F B7 75 4E 44 D5 69 39 8D D1 4F BF 09 F7 2A A2 0F C3 5C CF
Fingerprint algorithm	SHA-1	SHA-1	SHA-1	SHA-1	SHA-1
Fingerprint	0b 76 71 e1 e6 68 a5 28 29 f8 a4 ef 67 7f 46 22 5c 9c e4 46	0a 0f 64 ea f7 22 fc 7c 9b 34 8b b5 09 2d ce 9e 74 27 99 73	34 cb 18 d4 0d e2 9f ae 82 db a9 25 ba e7 c6 02 c0 83 3a 2e	a3 23 2e 38 fb e4 4f 7b 9c cb aa b2 36 ce 26 29 7d 3f 67 87	75 c1 8d 78 fd 56 d2 ed 53 9f 8b 00 0e 5d 6c 8b 69 7e 5b ee
Issue of end-entity certificates	**Nov. 8, 2016 to Apr. 18, 2018**	**Apr. 18, 2018 to Apr. 29, 2019 15:59:52 (GMT)**	**Apr. 29, 2019 17:57:08 (GMT) to March 03, 2020 19:11:25 (GMT)**	**From March 03, 2020 19:33:16 (GMT) to July 14, 2020 17:30:24 (GMT)**	**From July 14, 2020 17:20:46 (GMT)**

Table 5: Issuer and Subject DN "Deutsche Telekom Issuing CA 01", "Deutsche Telekom AG secure email CA" and „Deutsche Telekom AG secure email CA E02“

Deutsche Telekom AG Issuing CA 01 issued end-entity certificates under T-TeleSec GlobalRoot Class 2 from November 8, 2016 to April 18, 2018.

Deutsche Telekom AG secure email CA with the serial number 75 81 aa 9f 98 30 a3 ab bf 5b b6 9f 84 d8 56 issued end-entity certificates from April 18, 2018 to April 29, 2019.

Deutsche Telekom AG secure email CA with the serial number 15 31 b1 a1 34 7c 85 a9 7a 37 f6 0e bb 50 fd 86 issued end-entity certificates from April 29, 2019 to March 03, 2020.

Deutsche Telekom AG secure email CA E02 with the serial number 34 d2 29 25 00 6c 85 58 2f e8 9b 82 d7 97 6d 59 issued end-entity certificates from March 03, 2020 to July 14, 2020.

All end-entity certificates issued under these CAs will remain valid until the expiry of these certificates, unless they have been prematurely revoked due to the reasons for revocation/cancellation described in Chapter 4.9.1.

End-entity certificates from July 14, 2020 are issued by Deutsche Telekom AG secure email CA E03 with the serial number 39 ec 6c fc 26 1a cf be 89 8f a1 45 70 5c 9b 0a.

Since March 03, 2020, certificates for pseudonyms are no longer issued under a public certification authority.

Only Deutsche Telekom AG Issuing CA 01, Deutsche Telekom AG secure email CA, Deutsche Telekom AG secure email CA E02 and Deutsche Telekom AG secure email CA E03 are relevant for further consideration regarding compliance with the baseline requirements of the CA/Browser Forum as well as ETSI 319411-1 Policy LCP and ETSI 319401, as these were the only ones issued by an ETSI-certified root certification authority, the "T-TeleSec GlobalRoot Class 2."

1.3.1.2.2 Certification authority below an internal root certification authority

End-entity certificates (e.g., for users (smartcard logon), computers, authentication and signature of mobile devices, servers, code signing, routers/gateways, or domain controllers) that fulfill the conditions for use of an "internal root certification authority (internal root)" are issued by the following subordinate certification authorities (intermediate certification authorities):

- Deutsche Telekom AG Issuing CA 02
- Deutsche Telekom AG authentication CA
- Deutsche Telekom AG Issuing CA 03
- Deutsche Telekom AG infrastructure CA
- Deutsche Telekom AG mobile device CA
- Deutsche Telekom AG internal secure email CA

Table 6 contains the full Subject Distinguished Names (Subject DN) of the specified certification authorities under Deutsche Telekom Internal Root CA 1 in accordance with the name forms in Chapter 3.1.1 et seq. as well as the certificate validity.

Table 7 contains the full Subject Distinguished Names (Subject DN) of the specified certification authorities under Deutsche Telekom Internal Root CA 2 in accordance with the name forms in Chapter 3.1.1 et seq. as well as the certificate validity.

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

Issuer Deutschen Telekom Internal Root CA 1				
Common Name (CN)	Deutsche Telekom Internal Root CA 1	Deutsche Telekom Internal Root CA 1	Deutsche Telekom Internal Root CA 1	Deutsche Telekom Internal Root CA 1
Subject				
Country Name (C)	DE	DE	DE	DE
Organization Name (O)	T-Systems International GmbH	T-Systems International GmbH	T-Systems International GmbH	T-Systems International GmbH
Organizational Unit Name (OU)	T-Systems Trust Center	T-Systems Trust Center	T-Systems Trust Center	T-Systems Trust Center
Common Name (CN)	**Deutsche Telekom AG Issuing CA 02**	**Deutsche Telekom AG Issuing CA 02**	**Deutsche Telekom AG Issuing CA 03**	**Deutsche Telekom AG Issuing CA 03**
Serial number				
Signature hash algorithm	SHA-256	SHA-256	SHA-256	SHA-256
Key sizes of public keys	2048	2048	2048	2048
Encryption algorithm of public keys	RSA	RSA	RSA	RSA
Valid from:	Jul. 13, 2016	Nov. 29, 2016	Jan. 14, 2010	Jul. 13, 2016
Valid to:	Jul. 14, 2026	Nov. 30, 2026	Jan. 15, 2026	Jul. 14, 2026
Fingerprint algorithm:	SHA-256	SHA-256	SHA-256	SHA-256
Fingerprint:	3E 7C 3F C1 DC 26 83 11 A6 6C 86 22 37 8E F6 8C 58 B4 23 30 78 08 CB 4F AD 1C C9 35 9A 31 DC 42	A4 6D F4 E3 2B F5 2E 1A D5 30 5F CC A5 39 C2 CB F0 8D EE D0 76 39 CA 74 33 97 2D B7 C4 04 5E 17	23 41 6B 82 18 0F 5F FF 0A 9B 7B 13 96 4B 21 E4 71 C5 42 6° 12 92 93 15 FB 85 61 E2 E6 27 0B 62	C6 42 29 E7 89 2D F4 68 EC 59 95 08 77 43 4F FD 26 9A A8 90 A8 C7 8E 0B DC 7C C6 46 2B 1E E1 B4
Fingerprint algorithm	SHA-1	SHA-1	SHA-1	SHA-1
Fingerprint	66 e6 d5 09 80 92 7f 22 4e 2c fa 92 e5 6d fb 82 52 1d 7a 64	aa 12 85 4e eb 5f ad 13 c6 18 e0 81 8b cd 06 98 34 49 d3 b7	97 92 1a 0a e2 47 94 52 13 16 40 75 e1 28 1f 38 26 2d 11 82	a4 82 45 cd 46 0c 9a 9e b1 48 5d 80 3d 18 d0 2f f7 f8 94 a8
Issue of end-entity certificates	**Nov. 8, 2016 to Jun. 12, 2017**	**From Jun. 12, 2017**	**Through Nov. 8, 2016**	**From Nov. 8, 2016**

Table 6: Issuer and Subject DN of the internal certification authorities under Deutschen Telekom Internal Root CA 1

End-entity certificates for user authentication will no longer be issued by the internal CA "Deutsche Telekom AG Issuing CA 02" from July 30, 2019, but by the internal CA "Deutsche Telekom AG Authentication CA" with the serial number 5a ae 9e 1c 01 51 34 99. 0a 06 61 6c ce 28 35 .

Issuer Deutschen Telekom Internal Root CA 2					
Common Name (CN)	Deutschen Telekom Internal Root CA 2	Deutschen Telekom Internal Root CA 2	Deutschen Telekom Internal Root CA 2	Deutschen Telekom Internal Root CA 2	Deutschen Telekom Internal Root CA 2
Subject					
Country Name (C)	DE	DE	DE		DE
Organization Name (O)	T-Systems International GmbH	T-Systems International GmbH	T-Systems International GmbH	T-Systems International GmbH	T-Systems International GmbH
Organizational Unit Name (OU)	T-Systems Trust Center	T-Systems Trust Center	T-Systems Trust Center	T-Systems Trust Center	T-Systems Trust Center
Common Name (CN)	**Deutsche Telekom AG mobile device CA**	**Deutsche Telekom AG mobile device CA**	**Deutsche Telekom AG authentication CA**	**Deutsche Telekom AG infrastructure CA**	**Deutsche Telekom AG internal secure email CA**
Serial number	3d 81 9d 06 77 4d 41 ab a1 41 6e 78 01 6d bd	00 f7 75 0a 89 a8 44 a7 8e 7a c0 f0 2a 6c f6 7b	5a ae 9e 1c 01 51 34 99 0a 06 61 6c ce 28 35	65 97 d2 17 36 97 83 bf 87 09 b0 1d 63 06 c8	1a d2 27 86 1f 13 50 4b 2a 32 94 52 e6 3b 5d
Signature hash algorithm	SHA-256RSA	SHA-256RSA	SHA-256RSA	SHA-256RSA	SHA-256RSA
Key sizes of public keys	2048	2048	2048	2048	2048
Encryption algorithm of public keys	RSA	RSA	RSA	RSA	RSA
Valid from:	Jan. 18, 2018	Apr. 09, 2019	Jun. 08, 2018	Jun. 08, 2018	25.02.2020
Valid to:	Jan. 19, 2028	Apr. 09, 2029	Jun. 08, 2028	Jun. 08, 2028	25.02.2030
Fingerprint algorithm:	SHA-256	SHA-256	SHA-256	SHA-256	SHA-256
Fingerprint:	38 D8 11 57 0D BD DC E5 0D 0A A4 9F 33 72 D5 22 1B BD B4 F2 A0 50 49 83 C7 17 01 0F 26 AA BA B4	5C 97 98 7B 87 AE 2B 3E 67 AC 4E 56 E4 4D 13 81 30 DF 7B FF 8E 88 B1 C9 7E EA D7 0F A4 6C 82 F0	1C 32 62 C3 2F 1E 57 68 08 4F FE 24 50 20 55 17 55 C0 54 0A 1E 4C 52 C7 10 26 9C 1E B9 47 2C D9	87 88 43 10 BD 00 2F 37 23 78 E7 90 F0 34 95 02 7B 86 A2 0B BB 28 04 B6 76 D5 4E 48 D9 69 52 C1	69 1a 2e 6d b6 d1 43 76 6c 06 ac 78 41 48 03 d9 ce 82 46 5a fc d2 7c 50 0c 6a 28 b5 dd 3a 77 e3
Fingerprint algorithm	SHA-1	SHA-1	SHA-1	SHA-1	SHA-1
Fingerprint	01 6b ab f7 5f 56 98 d0 96 a3 e0 13 61 d1 66 d9 20 df 5f 1f	0b 90 49 79 27 2a bb 87 c3 52 1b 5a 74 8d 83 cb 7a 79 fb 91	3d 0a e2 9b 92 25 57 b6 e4 d8 ee 83 b8 5a 7c f9 3b 6a 41 fd	5e da 75 d3 d6 20 fa 46 3d 0c 57 20 b2 f4 22 53 cf b6 29 51	76 7d 35 3d 5a 62 9a 16 a2 52 26 ba cf 99 fa 4d c4 75 da 7f
Issue of end-entity certificates	**Apr. 18, 2018 to 29.04.2019**	**From Apr. 29, 2019**	**From July 30, 2019**	**From July 30, 2019**	**From March 03, 2020**

Table 7: Issuer and Subject DN of the internal certification authorities under Deutschen Telekom Internal Root CA 2

All end-entity certificates issued under these CAs will remain valid until the expiry of these certificates, unless they have been prematurely revoked due to the reasons for revocation/cancellation described in Chapter 4.9.1.

End-entity certificates for mobile devices are by the internal Deutsche Telekom AG mobile device with the serial number 00 f7 75 0a 89 a8 44 a7 8e 7a c0 f0 2a 6c f6 7b from April 29, 2019, depending on the intended use.

End-entity certificates for pseudonyms will be issued from the internal "Deutsche Telekom AG internal secure email CA" with the serial number 1a d2 27 86 1f 13 50 4b 2a 32 94 52 e6 3b 5d as of March 03, 2020.

1.3.1.3 Certificates to support PKI operation

1.3.1.3.1 Web server of the "cPKI" PKI service

The end entity can only access the PKI functions of the cPKI via the DTAG intranet. The cPKI web server has an SSL certificate, meaning that all actions are performed using the secure HTTPS protocol. The functions are provided following successful role-based authentication.

Figure 7 presents the certificate hierarchy of the "https://mycard-portal.telekom.de" web server with the corresponding certificate from the root certification authority (root CA) and the intermediate certification authority (sub CA). This web server can only be accessed from the DTAG intranet.

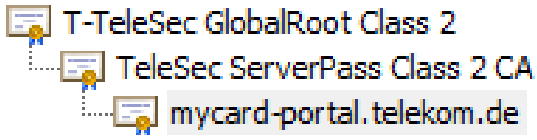

Figure 7: Overview of the certificate hierarchy of the "mycard-portal.telekom.de" web server

1.3.1.3.2 OCSP responder of the "cPKI" PKI service

Every sub 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 Chapter 7.3.

1.3.2 Registration authorities and trusted database

A registration authority (RA) is an authority that performs the authentication for certificate subjects, processes (approves, rejects, defers) certificate requests, processes or forwards revocation requests and, if required, creates certificate renewals and a copy of the key material (soft PSE) for a subject.
As a rule, every registration authority must guarantee that no unauthorized parties acquire a relevant certificate.

The following registration authorities have been established as part of the cPKI PKI service:

- Internal automatic registration authority based on HR data in the Corporate Identity and Access Management System (cIAM) of DTAG
- Internal manual registration authority operated in the Telekom Security Trust Center

1.3.2.1 Internal automated registration authority

The certificate management system of the cPKI has an automated registration authority.

The prerequisite for this is that DTAG employees are registered via HR in SAP HR and stored in DTAG's Corporate Identity Management System (cIAM).

SAPHR and cIAM are subject to

- Regular audits with the Internal Control System (ICS IT) by external auditors
- Implementation and release in a PRIVACY & SECURITY ASSESSMENT (PSA) procedure
- Implementation of penetration tests by Telekom Security experts
- Certification in accordance with ISO 27001

cIAM is therefore regarded by the DTAG Group as a trusted database for cPKI's certificate life cycle management based on the requirements and regulations of ETSI 319411-1 Policy LCP.

Systems involved:

- SAP HR management system (HR systems)
- cIAM (Corporate Identity & Access Management system)
- Active Directory as the central reference directory for the cPKI
- TAdmin2 as provisioning platform for the cPKI
- cPKI of DTAG

See also Figure 8: Authenticating a natural person (Germany) in EMEA1 and Figure 9: Authenticating a natural person (International) in EMEA 2.

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

- Accepting certificate requests
- Checking the requests in accordance with the specified policies
- Approving these certificate requests following a successful check; otherwise rejecting the request
- Requesting the certificate(s) following approval of the certificate request
- Authenticating subjects
- Providing the certificates to the certificate owner or an authorized person
- Accepting and verifying certificate revocation requests
- Revoking certificates following a positive check of a revocation order

1.3.2.2 Internal manual registration authority

In addition to the automated registration authority, the "Deutsche Telekom Issuing CA 01" and "Deutsche Telekom AG secure email CA" also have a manually operated registration authority that provides copies of encryption certificates and keys of certificate owners for authorized bodies (representatives) for certificate holders (end entities) or due to company law conditions (corporate security, legal requirements).

Furthermore, the manual registration authority checks certificate requests that have been rejected by the automated certification authority due to incorrect data or data that does not meet the eligibility criteria, initiates a correction of the data, if necessary, and reenters the request.

The manual registration authority also checks certificate requests for devices, routers, gateways, or domain certificates from the internal certification authority.

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

- Accepting certificate requests
- Checking the requests in accordance with the specified policies
- Approving these certificate requests following a successful check; otherwise rejecting the request
- Requesting the certificate(s) following approval of the certificate request
- Receiving the certificate(s) generated by the relevant certification authority and providing them to the certificate owner or an authorized person
- Accepting and verifying certificate revocation requests
- Revoking certificates following a positive check of a revocation order

1.3.3 End entity/certificate holder

In the context of the cPKI, 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:

- Natural persons (users, registrars, role owners, pseudonyms)
- Functional mailboxes
- Person and function groups
- Legal persons (e.g., foundations under civil law, corporations under private law such as stock corporations, registered associations, limited liability companies, registered cooperatives)
- Robots
- Devices (e.g., servers, routers, gateways, mail gateways, domain controllers, firewalls, or other devices)

Certificate holders of the cPKI in the context of natural persons include:

- Employees of DTAG and its subsidiaries
- Their respective external employees, if required
- Business partners who work on behalf of Deutsche Telekom or one of its subsidiaries, if required

Certificate holders can be persons with a personal email address, a pseudonym, persons responsible for function groups (functional mailbox managers), or co-users of function groups (authorized users of functional mailboxes) with an impersonal email address, see Chapters 1.4.1.3 and 1.4.1.4.

To meet the technical requirements, the cPKI provides various different certificate types for the end entities. The following Table 8 shows the assignment of the types to the respective end entities.

Type of certificate	Area of application (example)	End entity
User	Email 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	Natural persons
Pseudonyms	Mail security (S/MIME) for pseudonym accounts to log in as a TLS/SSL client on a web-based application/appliance, log in on a Microsoft network, log in on a Citrix appliance	Natural persons
Functional mailboxes	Mail security (S/MIME) for functional and group mailboxes,	People and function groups only (functional mailbox),
Function and group accounts	Mail security (S/MIME) for function and group accounts, to log in as a TLS/SSL client on a web-based application/appliance, log in on a Microsoft network, log in on a Citrix appliance	People and function groups, role holders with an AD user account with a mailbox and myCard
Robots	Mail security (S/MIME) for robot accounts to log in as a TLS/SSL client on a web-based	Robots (Devices with an AD user account and a mailbox)

Type of certificate	Area of application (example)	End entity
	application/appliance, log in on a Microsoft network, log in on a Citrix appliance	
Function and group certificate	Email security (S/MIME) for function mailboxes, pseudonym accounts for 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	Person and function groups, role owners, pseudonyms
Domain controllers	Authentication of the registration authority within a Microsoft network	Devices
Computers	Client authentication on a Microsoft network and VPN	Devices, legal persons
Servers	TLS/SSL server authentication	Devices, legal persons
Routers/gateways	VPN authentication within router networks	Devices, legal persons
Mail gateway	Virtual post office, authentication of a mail gateway/appliance	Devices, legal persons and groups of functions
Code signing	Natural persons, person and function groups, role owners, pseudonyms	Natural persons, person and function groups, role owners, pseudonyms

Table 8: Assignment of certificate types to end entities

In the following chapters, 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, person and function groups, pseudonyms; in the case of pseudonym certificates, natural persons whose name does not match the name in the official ID document,, 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 cPKI service but are not provided to the customer.

The area of application of the end-entity certificates is described in Chapter 1.4. The provisions of Chapter 4.5.1 also apply.

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

Deutsche Telekom in the role of customer or tenant is not to be understood as the end entity. An end entity is therefore not to be understood as an authorized representative of DTAG or its subsidiaries or holdings. 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 Deutsche Telekom AG).

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 party

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

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

1.3.5 Other subscribers

A person and function group, a legal person, or a device always lies in the responsibility of an authorized person who has been authorized for this task by Deutsche Telekom or its subsidiaries or holdings. The authorized person (e.g., a function mailbox manager) is identified and registered like a natural person and 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 (see Chapter 9.6.5).

1.4 Certificate usage

1.4.1 Permitted usage of certificates

cPKI certificates must be used within the permitted and legally valid scope only. This applies particularly to the relevant country-specific import and export provisions. Furthermore, the use of the certificates by DTAG employees or agents is only permitted within the scope of their official activities.

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 emails) 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.

Table 9 presents the security levels based on the intended uses.

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

Table 9: Use of certificates for users and devices

1.4.1.2 Certificates for users and devices

The certificate types provided by the corporate PKI are used for authentication, digital signatures, and encryption as part of various applications depending on the assignment of the "key usage" and "enhanced key usage" extensions and the CP/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 this CP/CPS or other agreements.

Some examples include:

- Authentication as part of communication protocols (e.g., SSL, IPsec, S/MIME, 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)

1.4.1.2.1 User certificates

For natural persons, the following certificates are made available as triple keys via automated, secured workflows: signature, encryption, and authentication.

Users are authenticated by the HR department when the employee is hired or, in the case of partners and external employees, by the responsible authorized representative.

Signature certificate

A key pair on the MyCard is used for the signature certificate. This key pair is applied during the production of the MyCard, the private part of the key pair is specially protected and cannot be exported. The cPKI certifies the public part of the selected key pair, but never comes into possession of the private key.

Encryption certificate

For encryption, a key pair is created in the cPKI and applied to the MyCard (for key generation and distribution, see Chapter 6.1).
The cPKI stores the key pair and the certificate protected in the certification authority.

Authentication certificate

A key pair on the MyCard is used for the authentication certificate. This key pair is applied during the production of the MyCard, the private part of the key pair is specially protected and cannot be exported. The cPKI certifies the public part of the selected key pair, but never comes into possession of the private key.

For details and use cases for restoring archived key material, see Chapter 4.12.

1.4.1.2.2 Devices (computer, server, and gateway certificates)

Server and gateway certificates are not issued by a CA that is subject to the policies of the CA Browser Forum. The internal CA3 is used for this. See Chapter 1.3.1 for more details.

1.4.1.3 Certificates for pseudonyms

In contrast to the standard creation of a master data record for a natural person, the first and/or last name specified in the certificate differs from the name in the official ID document. For this reason, so-called pseudonym accounts are created. These accounts are subject to certain requirements, which are described below.

A pseudonym account has the property that the name entered in the certificate does not indicate who is working with the account or respectively the underlying certificate. This can be the case in certain organizational units or in accounts that, for technical reasons, have an additional name to the name noted in the official ID.

One requirement is that such accounts must follow a certain nomenclature in order to be identifiable and the responsible user (key owner) can be easily identified behind this account.

It must be possible at any time to uniquely identify the subject and the owner of the certificate.

For pseudonym accounts, starting March 03. 2020 the real name of the certificate holder can be seen in SAP HR.

The certificate holder concealed behind the pseudonym is the key owner and is therefore responsible for the proper use of the pseudonym account and the certificates issued for it. In the event of tortious acts or criminal offenses, this person is held responsible. This can have consequences under labor law as well as criminal law.

The certification service provider is entitled to transmit the identity of a signature key owner, encryption key owner, or authentication key owner with a pseudonym (key owner) to the responsible departments if this is necessary in order to prosecute crimes or offenses, avert dangers to public security or order, or to fulfill the statutory requirements of the

federal and state-based authorities for the protection of the constitution, the German Federal Intelligence Service, the German Federal Armed Forces Counter-Intelligence Office, or the financial authorities or where courts have requested this in the context of pending proceedings in accordance with the relevant applicable provisions.

In order to identify the subject and the real identity of the certificate holder, the issuing certification authority is entitled to retrieve all necessary data from DTAG's HR management systems (SAP HR) or to store it in its IT systems.

The certificates for pseudonyms are issued as triple keys analogous to the user certificates, but are marked with "PN-" on the certificate to flag them as pseudonym certificates and contain no first and last name (see Chapter 3.1.3).

Starting 04.04.2020, certificates for pseudonyms will only be issued from the internal, non-public intermediate certification authorities.

1.4.1.4 Function/Group certificates

In certain cases it is necessary for encrypted messages to be read or sent by different recipients.

These are among other things the case:

- If several people jointly perform one role,
  e.g. in customer service, sales or a central mail entry point.
- If it regards test systems, training or trade fair accounts that are used by one group.
- If the certificate is not bound to a function but to a person.
- If representation must be ensured due to time-critical processes, the sender can only determine this with great effort and business processes could be disrupted by non-accessibility.
- If automated IT processes are to receive encrypted mails or automated processing is carried out by an application.
- If automated IT processes are to send signed emails, e.g. an automated invoice dispatch from DTAG

Here a distinction is made between function and group accounts with their own AD account and function and group mailboxes without their own AD account.

Function and group accounts with a SAP HR master data record and AD user account: for people and function groups, e.g. Reception, test systems, training courses and trade fair computers

Function and group accounts are created via the DTAG SAP HR system with a master data record and just like a natural person possesses an AD account with an associated mailbox. Authentication, **signature and encryption certificates (triple key)** are issued for these.

Since these certificates cannot be assigned to a natural person

A function and group account has the feature that its name, which is maintained in the HR system, does not indicate who is working with the account or the underlying certificate, therefore these accounts are subject to certain requirements, which are described below:

- Function and group accounts must follow a certain nomenclature in order to be identifiable
- The person responsible for the key behind this account must be easy to determine.
- A clear identification of the applicant and the certificate holder must be possible at all times.
- The manager or the head of the organizational unit to which the master record or account is assigned is the key owner and is therefore responsible for the proper use of the function and group accounts and the certificates issued for them. In the event of tortious acts or criminal offenses, this person is held responsible. In the event of tortious acts or criminal offenses, this person is held responsible. This can have consequences under labor law as well as criminal law.

The certification service provider is authorized to convey the identity of a signature key, encryption key and authentication key holder (person responsible for the key) to the responsible authorities. Insofar as necessary for the prosecution of criminal offenses or administrative offenses, to avert dangers to public security or order or to meet the legal requirements of the federal and state Constitutional Protection Authorities, the Federal Intelligence Service, the Military Counter Espionage Service or the financial authorities. Or the courts order to do so in the course of pending proceedings in accordance with the applicable provisions.

To determine the applicant or the person responsible for the key, the certification service provider is authorized to query all the data required for this from the DTAG (SAP HR) personnel management systems or to save it on their IT systems.

The certificates for function and group accounts are issued as a triple key in the same manner as the user certificates, but are marked with "GRP-" in the certificate as function and group accounts certificates (see Chapter 3.1.3)

Starting 04.04.2020, certificates for Function and group accounts will only be issued from the internal, non-public intermediate certification authorities.

Function and group mailboxes/Functional mailbox (FMB):

In contrast to certificates for function and group accounts, certificates for function mailboxes are still issued under the public CA.

Signature and encryption certificates are issued as single keys for function and group mailboxes without their own AD user account.

For encryption and signing, a key pair (single key) is created in the cPKI and applied to the MyCard (for key generation and distribution, see Section 6.1).

The cPKI stores the key pair and the certificate in a protected manner in the Certification Authority.

To do this, a key pair with a corresponding certificate can be jointly used by a group for signing and encryption.

The signatures are then to be understood as integrity assurance within the meaning of a company stamp for the members of the group.

If the security requirements permit the application case, it offers itself in such situations to use one key pair for several people. To do so, a key pair with a certificate is generated. However, unlike personal key pairs, access to the secret key is granted to several people. Whether the group members use one or more PSEs, hardware or software PSEs, individual or shared passwords to access the private key or the certificate depends on the respective application case.

Example 1:

A key pair with a certificate is to be created for a functional mailbox and the employees with access authorization on this functional mailbox are to be provided with the corresponding key pair for decrypting, encrypting and signing emails from this functional mailbox.

For this purpose, the functional mailbox manager (owner) applies for a certificate for this functional mailbox on the cPKI portal. For this, a certificate-based logon using the holder's personal MyCard to the cPKI portal is mandatory. This logon will be checked against the cPKI. In addition, Deutschen Telekom's backend systems check whether the person is actually the functional mailbox manager. Upon successful validation of the logon data and the ownership of the functional mailbox, a certificate (key pair for signature and encryption) can be ordered for this functional mailbox. To ensure the integrity of the order, the order is signed with the personal signature certificate of the function mailbox manager and saved in the cPKI in a revision-proof manner.

By creating a key for this functional mailbox, the owner of this mailbox becomes the key owner.

In a second step, the key owner selects the employees whose MyCard the PSE is to be written on.

The selected functional mailbox users (employees) are then notified by email and can refuse or accept the assignment. Upon acceptance, the PSE for the functional mailbox is written on the personal MyCard of the functional mailbox user. The use of this certificate or the private key on the personal MyCard of the functional mailbox user is only possible with the personal PIN of the MyCard. A shared password/PIN is hereby excluded.

Example 2:

An application that is to receive, send or sign encrypted e-mails requires a key pair.

Here, an application encryption gateway (email encryption gateway) is being used at the Deutschen Telekom. For this gateway, the key pair is required as a soft PSE.

The application owner must submit a written request to the RA of the Deutschen Telekom; after checking the identity and the power of attorney, the RA site issues a software PSE for this application. This software PSE is transferred in encrypted form to the application owner who through this action becomes key owner. Encryption takes place for the personal key owner's certificate. Furthermore, the password for the Soft-PSE is also encrypted and transmitted in a separate email.

Access to the email address of his application is enabled via the application encryption gateway.

The key owner can then load the key pair into the application encryption gateway.

1.4.1.5 Robots and machines

A robot or machine is understood to mean a device that, like a natural person, has an AD account and a mailbox and can independently carry out activities via programming or AI algorithms and, if necessary, communicate in encrypted form or authenticate itself certificate based on applications.

Therefore, certificates can be issued for robots and machines if required. The corresponding accounts are created through the SAP HR system from DTAG with a master data record and then like a natural person have an AD account with the associated mailbox. Authentication, signature and encryption certificates (triple key) are issued for this.

Because these certificates cannot be assigned to a natural person

A robot account has the feature that its name, which is maintained in the HR system, does not indicate who is working with the account or the underlying certificate. Therefore, these accounts are subject to certain requirements, which are described below:

- Robot accounts must follow a certain nomenclature in order to be identifiable
- The responsible key owner behind this account must be easy to determine.
- A clear identification of the applicant and the certificate holder must be possible at any time.
- The manager or the head of the organizational unit to which the master record or account is assigned is the key owner and is therefore responsible for the proper use of the robot accounts and the certificates issued for them. This can have consequences under labor law as well as criminal law.

The certification service provider is authorized to convey the identity of a signature key, encryption key and authentication key holder (person responsible for the key) to the responsible authorities. Insofar as necessary for the prosecution of criminal offenses or administrative offenses, to avert dangers to public security or order or to meet the legal requirements of the federal and state Constitutional Protection Authorities, the Federal Intelligence Service, the Military Counter Espionage Service or the financial authorities. Or the courts order to do so in the course of pending proceedings in accordance with the applicable provisions.

To determine the applicant or the person responsible for the key, the certification service provider is authorized to query all the data required for this from the DTAG (SAP HR) personnel management systems or to save it on their IT systems.

The certificates for robot accounts are issued as a triple key in the same manner as user certificates, but are marked with "„Robot-" in the certificate as robot account certificate (see Chapter 3.1.3)

Starting 04.04.2020, certificates for Function and group accounts will only be issued from the internal, non-public intermediate certification authorities.

1.4.2 Non-permissible certificate usage

cPKI 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)
- Use for non-official purposes
- Use for private purposes

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

The certificates of the corporate PKI do not support the attribute "non-repudiation" in connection with an identity or authorization

1.5 Policy administration

1.5.1 Responsibility for the statement

This CP/CPS is published by:

Deutsche Telekom Security GmbH
Trust Center Operations

Untere Industriestrasse 20

57250 Netphen

Germany

1.5.2 Contact information

Deutsche Telekom Security GmbH
Trust Center Operations

Untere Industriestrasse 20

57250 Netphen

Germany

Phone: +49 1805-268204[1]

Email: telesec_support@t-systems.com

Intranet and internet: https://corporate-pki.telekom.de/

The report of misuse or compromise of certificates and keys of the Telekom Security Trust Center can be sent 24/7 at https://www.telesec.de/de/kontakt-de. Reports are prioritized by selecting "Report suspected certificate misuse" in the "Subject" contact form field. The "Text" field should be as precise and comprehensive as possible, so that Telekom Security can assess the situation at an early stage and initiate appropriate measures. Telekom Security usually responds within 24 hours with an initial assessment of the communication channels specified. If necessary, Telekom Security will involve law enforcement and supervisory authorities. The entry of the report is deemed agreement that data can be passed on to authorities without further consent in such a case.

[1] Fixed network: EUR 0.14/minute, mobile network: max. EUR 0.42/minute

1.5.3 Maintenance of the policy

This document (CPS) remains valid as long as it is not revoked by the publisher (see chapter 1.5.1). It is updated as required (at least once a year) with an incremented version number (see also chapters 9.12.1 and 9.12.2).

1.5.4 Approval procedure for this CP/CPS

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

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

Relevant change requests or changes to the ongoing PKI operation of the cPKI 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." If required, the changes are incorporated into the document in question.

In addition, a document review is carried out at least once a year, even if no changes to the content are required.

The department named in Chapter 1.5.2 is responsible for evaluating the change request and for carrying out or coordinating the review.

The change history is updated accordingly.

1.6 Acronyms and definitions

Acronyms and term definitions can be found in Chapter C.

2 PUBLICATIONS AND DIRECTORY SERVICES

2.1 Directory services (repositories)

Telekom Security operates a directory service and central data storage for the cPKI service. Telekom Security is responsible for their content.
Edited extracts of these databases provide the basis for publishing certificate information and certificate revocation lists (CRL) on the directory service or supplying the Online Certificate Status Protocol (OCSP) responder validation service 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 of the root and intermediate certification authorities (root-CAs and sub-CAs) involved. This directory is available round the clock. The maximum downtime is on average 1,5 days per month

Telekom Security uses appropriate mechanisms to protect the central data repository against unauthorized manipulation attempts (add, delete, or change).

2.2 Publication of certificate information

At regular intervals, Telekom Security publishes certificate revocation lists (CRL), which contain all the certificates revoked by the cPKI 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).

Telekom Security publishes all end-entity certificates issued by the cPKI on an internal directory service in DTAG's INTRANET. The task of the directory service is to provide 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). The revocation information for all PKI participants and the certificates are only published internally by DTAG. 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). Furthermore, the certificates can be accessed internally in the DTAG Active Directory's Global Address List and in DTAG's Group directory by employees of the Group.

The cPKI also provides a validation service (OCSP responder), which can be accessed via the "Online Certificate Status Protocol" (OCSP) internet protocol and returns the status of cPKI certificates to the requester.

The address of the OCSP responder is entered on the certificate and is also published in this document.

Telekom Security publishes the current CP/CPS as well as the CA and Root CA certificates at:

https://corporate-pki.telekom.de/

The root CA certificate of "T-TeleSec GlobalRoot Class 2" is preinstalled in the common operating system and application certificate archives as a "trust anchor" or is installed later online and supports certificate validation for end entities and relying parties.

The publication of the certificates depends on the certificate type and the provisions in Table 10.

Certificate type/issuer:	Requirements:
"Deutsche Telekom root CA 2" root CA certificate	This certificate is preinstalled in the common operating system and application certificate archives as a "trusted root certification authority" or is installed later online and supports certificate validation for end entities and relying parties. If required, the cPKI certificate can be retrieved via the intranet or the internet.

Certificate type/issuer:	Requirements:
Deutsche Telekom AG Issuing CA 01	This sub-CA certificate was issued by the "Deutsche Telekom Root CA 2" root certification authority and supports certificate validation for end entities and relying parties. If required, the cPKI certificate can be retrieved via the intranet or the internet.
"T-TeleSec GlobalRoot Class 2" root CA certificate	This certificate is preinstalled in the common operating system and application certificate archives as a "trusted root certification authority" or is installed later online and supports certificate validation for end entities and relying parties. If required, the cPKI certificate can be retrieved via the intranet or the internet.
Deutsche Telekom AG Issuing CA 01	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 cPKI certificate can be retrieved via the intranet or the internet.
Deutsche Telekom AG secure email CA	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 cPKI certificate can be retrieved via the intranet or the internet.
Deutsche Telekom AG secure email CA E02	This sub-CA certificate was issued by the root certification authority “T-TeleSec GlobalRoot Class 2” and supports certificate validation for end entities and relying parties. If required, the cPKI certificate can be retrieved via the intranet or the Internet.
Deutsche Telekom AG secure email CA E03	This sub-CA certificate was issued by the root certification authority “T-TeleSec GlobalRoot Class 2” and supports certificate validation for end entities and relying parties. If required, the cPKI certificate can be retrieved via the intranet or the Internet.
"Deutsche Telekom Internal Root CA 1" root CA certificate	This certificate is not preinstalled in the operating system and application certificate archives as a "trusted 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 cPKI certificate can be retrieved via the intranet or the internet.
Deutsche Telekom AG Issuing CA 02	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 cPKI certificate can be retrieved via the intranet or the internet.
Deutsche Telekom AG Issuing CA 03	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 cPKI certificate can be retrieved via the intranet or the internet.
"Deutsche Telekom Internal Root CA 2" root CA certificate	This certificate is not preinstalled in the operating system and application certificate archives as a "trusted 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 cPKI certificate can be retrieved via the intranet or the internet.
Deutsche Telekom AG mobile device CA	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 cPKI certificate can be retrieved via the intranet or the internet.

Certificate type/issuer:	Requirements:
Deutsche Telekom AG internal secure email CA	This sub-CA certificate was issued by the root certification authority "Deutsche Telekom Internal Root CA 2" and supports certificate validation for end entities and relying parties. If required, the cPKI certificate can be retrieved via the intranet or the Internet.
Certificates for end entities from a CA under the public root	These certificates are only published on DTAG internal directory services – these are currently the Global Address List of DATG, the group directory of DTAG, and the internal cPKI LDAP. In coordination with the tenant DTAG, however, the certificates can be published in other directory services on the DATG intranet. On the cPKI LDAP, certificates can be searched by connected applications via LDAP
Certificates for end entities from a CA under the internal root	These certificates are not currently published. In coordination with the tenant DTAG, however, additional certificate types can be published on the DATG intranet.
OCSP certificates	These certificates are not available to download.

Table 10: Specifications for the publication of certificates

The above-mentioned information is published on the website of the certification service provider for the cPKI at https://corporate-pki.telekom.de/.

In addition, in the event of security-critical incidents, the customer's known contact persons within DTAG are notified directly in writing or by email.

The assessment bodies/auditors (Chapter 8 et seq.) and the supervisory authority (forwarding of DTAG's Group Situation Center to BSI, BNetzA) are notified of changes to the information security policy of the cPKI.

In addition to the CAs mentioned above, two development and test and acceptance environments are operated in encapsulated DTAG networks (e.g., for software developers, as well as for tests and acceptance).

These environments are set up close to production with all DTAG infrastructure components required for the cPKI. Certificates and CRL and CARL are available within these environments for certificate validation and status information (valid, revoked, and expired).

Root, intermediate, and issuing CA and end-entity certificates are not published outside these development, testing and acceptance environments and are not accessible over the internet.

2.3 Updating the information (point in time, frequency)

Updates to the CP/CPS are published as described in Chapter 9.12 and noted in the change history.

This CP/CPS undergoes an annual review, regardless of any other amendments. This also applies even in the event that no changes are made to contents.

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

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

Certificates intended for publication will be published at the time of generation. Depending on the replication time of DTAG's internal systems such as the Global Address List, it may take up to 12 hours until newly issued certificates are available to all DTAG users. End-entity certificates are only published on the DTAG intranet.

The revocation lists and the OCSP responses are published as described in Chapter 4.9.7.

2.4 Access to directory services (repositories)

The retrieval of revocation lists (CRL, CARL) and the use of the OCSP service for end entities (Chapter 1.3.3), relying parties (Chapter 1.3.4), or registration authorities (Chapter 1.3.2) are not subject to access control.

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

As a rule, the search for certificates via the directory service and read access to this information within the DTAG network is not subject to access control. In addition to the cPKI directory service, DTAG employees can display certificates via the Global Address List (GAL) by calling up a contact entry. However, it is not possible to search for end-entity certificates from the internet.

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

The Public and Internal intermediate certification authorities are published as shown in the tables below:

The LDAP server of the cPKI or the Active Directory of the respective Windows domain is used to provide revocation lists.

	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG secure email CA	Deutsche Telekom AG secure email CA E02	Deutsche Telekom AG secure email CA E03
CRL Distribution Points (CDP)					
CDP [1] http	URL=http://cpki.telekom.de/cdp/Deutsche%20Telekom%20Root%20CA%202.crl	URL=http://crl-cpki.telekom.de/rl/GlobalRoot_Class_2.crl	URL=http://crl-cpki.telekom.de/rl/GlobalRoot_Class_2.crl	URL=http://crl-cpki.telekom.de/rl/GlobalRoot_Class_2.crl	URL=http://crl-cpki.telekom.de/rl/GlobalRoot_Class_2.crl
CDP [2] ldap	URL=ldap://ldap-cpki.telekom.de/cn=Deutsche%20Telekom%20Root%20CA%202,ou=T-TeleSec%20Trust%20Center,o=Deutsche%20Telekom%20AG,C=DE?authorityRevocationList	URL=LDAP://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?authorityRevocationList	URL=ldap://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?authorityRevocationList	URL=ldap://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?authorityRevocationList	URL=ldap://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?authorityRevocationList
CDP [3] AD	-	-	-	-	-
Deutsche Telekom AG Employee Encryption	X	X	X	X	X

	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG secure email CA	Deutsche Telekom AG secure email CA E02	Deutsche Telekom AG secure email CA E03
Deutsche Telekom AG Employee Signature	X	X	X	X	X
Deutsche Telekom AG Employee Authentication	-	-	-	-	-
Deutsche Telekom AG External Workforce Encryption (For certificates issued until March 3rd, 2020)	X	X	X	-	-
Deutsche Telekom AG External Workforce Signature (For certificates issued until March 3rd, 2020)	X	X	X	-	-
Deutsche Telekom AG External Workforce Authentication	-	-	-	-	-
Deutsche Telekom AG Function groups Encryption (For certificates issued until March 3rd, 2020)	X	X	X	-	-
Deutsche Telekom AG Function groups Signature (For certificates issued until March 3rd, 2020)	X	X	X	-	-
Deutsche Telekom AG Function groups Authentication	-	-	-	-	-

	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG secure email CA	Deutsche Telekom AG secure email CA E02	Deutsche Telekom AG secure email CA E03
Deutsche Telekom AG Robot Encryption (For certificates issued until March 3rd, 2020)	X	X	X	-	-
Deutsche Telekom AG Robot Signature (For certificates issued until March 3rd, 2020)	X	X	X	-	-
Deutsche Telekom AG Robot Authentication	-	-	-	-	-
Deutsche Telekom AG Pseudonyme Encryption (For certificates issued until March 3rd, 2020)	X	X	X	-	-
Deutsche Telekom AG Pseudonyme Signature (For certificates issued until March 3rd, 2020)	X	X	X	-	-
Deutsche Telekom AG Pseudonyme Authentication	-	-	-	-	-
Deutsche Telekom AG Telekom Computer	-	-	-	-	-
Deutsche Telekom AG Domain Controller	-	-	-	-	-
Deutsche Telekom AG Print Server	-	-	-	-	-

	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG secure email CA	Deutsche Telekom AG secure email CA E02	Deutsche Telekom AG secure email CA E03
Deutsche Telekom AG Code Signing	-	-	-	-	-
Deutsche Telekom AG OCSP Signing	X	X	X	X	-
Archiving of the private key	X	X	X	X	X

Table 11: Assignment of the certificates to the CAs and the respective CRL Distribution Points for certificates from the public root certification authority

	Deutsche Telekom AG Issuing CA 02	Deutsche Telekom AG Issuing CA 03	Deutsche Telekom AG mobile device CA	Deutsche Telekom AG infrastructure CA	Deutsche Telekom AG authentification CA	Deutsche Telekom AG internal secure email CA
CRL Distribution Points (CDP)						
CDP [1] http	URL=http://crl-cpki.telekom.de/rl/DT_Internal_Root_CA_1.crl	URL=http://crl-cpki.telekom.de/rl/DT_Internal_Root_CA_1.crl	URL=http://crl-cpki.telekom.de/rl/DT_Internal_Root_CA_2.crl	URL=http://crl-cpki.telekom.de/rl/DT_Internal_Root_CA_2.crl	URL=http://crl-cpki.telekom.de/rl/DT_Internal_Root_CA_2.crl	URL=http://crl-cpki.telekom.de/rl/DT_Internal_Root_CA_2.crl
CDP [2] ldap	URL=LDAP://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?authorityRevocationList	URL=LDAP://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?authorityRevocationList	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?authorityRevocationList	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?authorityRevocationList	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?authorityRevocationList	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?authorityRevocationList
CDP [3] AD	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,CN=InternalRootCA,CN=CDP,CN=Public%20K	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,CN=InternalRootCA,CN=CDP,CN=Public%20K	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,CN=InternalRootCA,CN=CDP,CN=Public%20K	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,CN=InternalRootCA,CN=CDP,CN=Public%20K	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20S	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,CN=InternalRootCA,CN=CDP,CN=Public%20K

	Deutsche Telekom AG Issuing CA 02	Deutsche Telekom AG Issuing CA 03	Deutsche Telekom AG mobile device CA	Deutsche Telekom AG infrastructure CA	Deutsche Telekom AG authentification CA	Deutsche Telekom AG internal secure email CA
	ey%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?certificateRevocationList?base?objectClass=CRLDistributionPoint	ey%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?certificateRevocationList?base?objectClass=CRLDistributionPoint	ey%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?certificateRevocationList?base?objectClass=CRLDistributionPoint	ey%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?certificateRevocationList?base?objectClass=CRLDistributionPoint	ervices,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?certificateRevocationList?base?objectClass=CRLDistributionPoint	ey%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?certificateRevocationList?base?objectClass=CRLDistributionPoint
Deutsche Telekom AG Employee Encryption	-	-	-	-	-	-
Deutsche Telekom AG Employee Signature	-	-	-	-	-	-
Deutsche Telekom AG Employee Authentication	X	-	-	-	X	-
Deutsche Telekom AG External Workforce Encryption (For certificates issued from March 3rd, 2020 and later)	-	-	-	-	-	X
Deutsche Telekom AG External Workforce Signature (For certificates issued from March 3rd, 2020 and later)	-	-	-	-	-	X
Deutsche Telekom AG External Workforce Authentication	X	-	-	-	X	-
Deutsche Telekom AG Function	-	-	-	-	-	X

	Deutsche Telekom AG Issuing CA 02	Deutsche Telekom AG Issuing CA 03	Deutsche Telekom AG mobile device CA	Deutsche Telekom AG infrastructure CA	Deutsche Telekom AG authentification CA	Deutsche Telekom AG internal secure email CA
groups Encryption (For certificates issued from March 3rd, 2020 and later)						
Deutsche Telekom AG Function groups Signature (For certificates issued from March 3rd, 2020 and later)	-	-	-	-	-	X
Deutsche Telekom AG Function groups Authentication	X	-	-	-	X	-
Deutsche Telekom AG Robot Encryption (For certificates issued from March 3rd, 2020 and later)	-	-	-	-	-	X
Deutsche Telekom AG Robot Signature (For certificates issued from March 3rd, 2020 and later)	-	-	-	-	-	X
Deutsche Telekom AG Robot Authentication	X	-	-	-	X	-
Deutsche Telekom AG Pseudonyme Encryption (For certificates issued from March 3rd, 2020 and later)	-	-	-	-	-	X
Deutsche Telekom AG	-	-	-	-	-	X

	Deutsche Telekom AG Issuing CA 02	Deutsche Telekom AG Issuing CA 03	Deutsche Telekom AG mobile device CA	Deutsche Telekom AG infrastructure CA	Deutsche Telekom AG authentification CA	Deutsche Telekom AG internal secure email CA
Pseudonyme Signature (For certificates issued from March 3rd, 2020 and later)						
Deutsche Telekom AG Pseudonyme Authentication (For certificates issued from March 3rd, 2020 and later)	X	-	-	-	X	-
Deutsche Telekom AG Telekom Computer	-	X	-	X	-	-
Deutsche Telekom AG Domain Controller	-	X	-	X	-	-
Deutsche Telekom AG Print Server	-	X	-	X	-	-
Deutsche Telekom AG Code Signing	-	X	-	X	-	-
Deutsche Telekom AG Mobile Device Authentication Certificate for VPN	-	-	X	-	-	-
Deutsche Telekom AG Mobile Device Signature for Email Signature on Mobile Devices	-	-	X	-	-	-
Deutsche Telekom AG OCSP Signing	X	X	X	X	X	X

	Deutsche Telekom AG Issuing CA 02	Deutsche Telekom AG Issuing CA 03	Deutsche Telekom AG mobile device CA	Deutsche Telekom AG infrastructure CA	Deutsche Telekom AG authentification CA	Deutsche Telekom AG internal secure email CA
Archiving of the private key	X	X	X	X	-	X (omly Encryption)

Table 12: Assignment of the certificates to the CAs and the respective CRL Distribution Points for certificates from the internal root certification authority

Provision of certificate status data via the OCSP protocol

	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG secure email CA	Deutsche Telekom AG secure email CA E02	Deutsche Telekom AG secure email CA E03
Authority Information Access (AIA)					
AIA [1] ocsp (OCSP Access (1.3.6.1.5.5.7.48.1))	URL=http://ocsp-cpki.telekom.de/ocsp	URL=http://ocsp-cpki.telekom.de/ocspr	URL=http://ocsp.telekom.de/ocspr	URL=http://ocsp.telekom.de/ocspr	URL=http://ocsp.telekom.de/ocspr
AIA [2] http (Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	URL=http://corporate-pki.telekom.de/aia/Deutsche%20Telekom%20Root%20CA%202.crt	URL=http://crt-cpki.telekom.de/crt/GlobalRoot_Class_2.cer	URL=http://crt-cpki.telekom.de/crt/GlobalRoot_Class_2.cer	URL=http://crt-cpki.telekom.de/crt/GlobalRoot_Class_2.cer	URL=http://crt-cpki.telekom.de/crt/GlobalRoot_Class_2.cer
AIA [3] ldap (Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Root%20CA%202,OU=T-TeleSec%20Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate	URL=LDAP://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?cACertificate	URL=ldap://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?cACertificate	URL=ldap://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?cACertificate	URL=ldap://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?cACertificate
AIA [4] AD (Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	-	-	-	-	-

	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG secure email CA	Deutsche Telekom AG secure email CA E02	Deutsche Telekom AG secure email CA E03
Deutsche Telekom AG Employee Encryption	X	X	X	X	X
Deutsche Telekom AG Employee Signature	X	X	X	X	X
Deutsche Telekom AG Employee Authentication	-	-	-	-	-
Deutsche Telekom AG External Workforce Encryption	X	X	X	-	-
Deutsche Telekom AG External Workforce Signature	X	X	X	-	-
Deutsche Telekom AG External Workforce Authentication	-	-	-	-	-
Deutsche Telekom AG Function groups Encryption	X	X	X	-	-
Deutsche Telekom AG Function groups Signature	X	X	X	-	-
Deutsche Telekom AG Function groups Authentication	-	-	-	-	-
Deutsche Telekom AG Robot Encryption	X	X	X	-	-

	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG Issuing CA 01	Deutsche Telekom AG secure email CA	Deutsche Telekom AG secure email CA E02	Deutsche Telekom AG secure email CA E03
Deutsche Telekom AG Robot Signature	X	X	X	-	-
Deutsche Telekom AG Robot Authentication	-	-	-	-	-
Deutsche Telekom AG Pseudonyme Encryption	X	X	X	-	-
Deutsche Telekom AG Pseudonyme Signature	X	X	X	-	-
Deutsche Telekom AG Pseudonyme Authentication	-	-	-	-	-
Deutsche Telekom AG Telekom Computer	-	-	-	-	-
Deutsche Telekom AG Domain Controller	-	-	-	-	-
Deutsche Telekom AG Print Server	-	-	-	-	-
Deutsche Telekom AG Code Signing	-	-	-	-	-
Deutsche Telekom AG OCSP Signing	X	X	X	X	-

Table 13: Assignment of the certificates to the CAs and the respective AIA URLs for certificates from the public root certification authority

Provision of certificate status data via the OCSP protocol

	Deutsche Telekom AG Issuing CA 02	Deutsche Telekom AG Issuing CA 03	Deutsche Telekom AG mobile device CA	Deutsche Telekom AG infrastructure CA	Deutsche Telekom AG authentification CA	Deutsche Telekom AG internal secure email CA
Authority Information Access (AIA)						
AIA [1] ocsp (OCSP Access (1.3.6.1.5.5.7.48.1))	URL=http://ocsp-cpki.telekom.de/ocspr	URL=http://ocsp-cpki.telekom.de/ocspr	URL=http://ocsp.telekom.de/ocspr	URL=http://ocsp.telekom.de/ocspr	URL=http://ocsp.telekom.de/ocspr	URL=http://ocsp.telekom.de/ocspr
AIA [2] http (Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	URL=http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_1.cer	URL= http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_1.cer	URL=http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_2.cer	URL=http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_2.cer	URL=http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_2.cer	URL=http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_2.cer
AIA [3] ldap (Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate	URL=ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate
AIA [4] AD (Certification Authority Issuer (1.3.6.1.5.5.7.48.2)	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base=objectClass=certificationAuthority	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base=objectClass=certificationAuthority	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base=objectClass=certificationAuthority	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base=objectClass=certificationAuthority	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base=objectClass=certificationAuthority	URL=ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base=objectClass=certificationAuthority

	Deutsche Telekom AG Issuing CA 02	Deutsche Telekom AG Issuing CA 03	Deutsche Telekom AG mobile device CA	Deutsche Telekom AG infrastructure CA	Deutsche Telekom AG authentification CA	Deutsche Telekom AG internal secure email CA
Deutsche Telekom AG Employee Signature	-	-	-	-	-	-
Deutsche Telekom AG Employee Encryption	-	-	-	-	-	-
Deutsche Telekom AG Employee Signature (Mobile Devices only)	-	-	X	-	-	-
Deutsche Telekom AG Employee Authentication	X	-	X	-	X	-
Deutsche Telekom AG External Workforce Encryption (For certificates issued from March 3rd, 2020 and later)	-	-	-	-	-	X
Deutsche Telekom AG External Workforce Signature (For certificates issued from March 3rd, 2020 and later)	-	-	X	-	-	X
Deutsche Telekom AG External Workforce Authentication	X	-	X	-	X	-
Deutsche Telekom AG Function groups Encryption	-	-	-	-	-	X

	Deutsche Telekom AG Issuing CA 02	Deutsche Telekom AG Issuing CA 03	Deutsche Telekom AG mobile device CA	Deutsche Telekom AG infrastructure CA	Deutsche Telekom AG authentification CA	Deutsche Telekom AG internal secure email CA
(For certificates issued from March 3rd, 2020 and later)						
Deutsche Telekom AG Function groups Signature (For certificates issued from March 3rd, 2020 and later)	-	-	-	-	-	X
Deutsche Telekom AG Function groups Authentication	X	-	-	-	X	-
Deutsche Telekom AG Robot Encryption (For certificates issued from March 3rd, 2020 and later)	-	-	-	-	-	X
Deutsche Telekom AG Robot Signature (For certificates issued from March 3rd, 2020 and later)	-	-	-	-	-	X
Deutsche Telekom AG Robot Authentication	X	-	-	-	X	-
Deutsche Telekom AG Pseudonyme Encryption (For certificates issued from March 3rd, 2020 and later)	-	-	-	-	-	X

	Deutsche Telekom AG Issuing CA 02	Deutsche Telekom AG Issuing CA 03	Deutsche Telekom AG mobile device CA	Deutsche Telekom AG infrastructure CA	Deutsche Telekom AG authentification CA	Deutsche Telekom AG internal secure email CA
Deutsche Telekom AG Pseudonyme Signature (For certificates issued from March 3rd, 2020 and later)	-	-	-	-	-	X
Deutsche Telekom AG Pseudonyme Authentication	X	-	-	-	X	-
Deutsche Telekom AG Telekom Computer	-	X	-	X	-	-
Deutsche Telekom AG Domain Controller	-	X	-	X	-	-
Deutsche Telekom AG Print Server	-	X	-	X	-	-
Deutsche Telekom AG Code Signing	-	X	-	X	-	-
Deutsche Telekom AG Mobile Device Authentication Certificate for VPN	-	-	X	-	-	-
Deutsche Telekom AG Mobile Device Signature for Email Signature on Mobile Devices	-	-	X	-	-	-
Deutsche Telekom AG OCSP Signing	X	X	X	X	X	X

Table 14: Assignment of the certificates to the CAs and the respective AIA URLs for certificates from the internal root certification authority

More information on this is available at https://corporate-pki.telekom.de/.

Provision of the certificates for obtaining the public keys for data encryption via the LDAP server of the corporate PKI NG, the Global Address List, or the X.500 Group directory.

These directories can only be accessed via the DTAG intranet.

Source	URL
LDAP server of DTAG's corporate PKI	ldap://corporate-pki.telekom.de:389/C=DE
Global Address List of the AD domains EMEA1 and EMEA2	

Table 15: Interfaces for providing the certificates for obtaining the public keys for data encryption

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming rules

Within the corporate PKI of DTAG, a Distinguished Name (DN) is a unique name for directory objects in accordance with the X.500 standard. Distinguished Names allow people and systems to be clearly distinguished. The DN is intended to ensure 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 represented graphically in Chapter 1.3.1. However, the same naming conventions as for the Subject DN apply.

3.1.1 Name forms

For all certificate requests, the identity of the certificate holder is checked or verified via the trusted database (cIAM) (see Chapter 3.2.3).

Depending on the certificate type (Chapters 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 natural persons and pseudonyms, the subject field must contain the following attributes in accordance with the ITU-T X.520[6] recommendation:
- - CountryName
- - Choice between first and last name or pseudonym
- - CommonName

Server certificates are only issued under the internal CA. However, due to DTAG's internal specifications, the following fields must also be filled in:

- Locality Name (L) or
- State or Province Name (S)

Details on the contents of the Issuer DN and the Subject DN can be found in Chapter 7.

In optional fields (e.g., OU3, FQDN) that do not contain any information (empty fields) or are not relevant, the use of fill characters (metacharacters), such as [-], [.], [*], or [ ] (space), is prohibited.

3.1.1.1 Conventions for the components of the "Subject DN"

This chapter specifies conventions for Subject DNs (requesters) that apply to all end-entity certificates. The English terms, which are currently common in this field, are used below.

The following characters are permitted within the Subject DN:
A – Z, a – z, ä, ö, ü 0 – 9, ( ) + - . / : = ? @ and space (blank)

Due to the different coding rules of the respective certificate fields, not all of the above-mentioned characters may be used in some input fields (e.g., no umlauts (ä, ö, ü) in email addresses).

3.1.1.1.1 Country Name (C)

This mandatory attribute 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 (T-SIS) 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 "permitted internet domains" check (Chapter 3.2.2), the Country Name (C) and Organization Name (O) (Chapter 3.1.1.1.2) attributes are included in the configuration of the cPKI as a fixed value pair.

3.1.1.1.2 Organization Name (O)

This mandatory attribute contains the organization name (e.g., company, institution, authority) of the certificate owner. This information is verified using a public directory (e.g., extract from the commercial register) or other equivalent directories or documents.

Examples:

O = Sample company GmbH

O = Deutsche Telekom AG

O = DTAG

As part of the "permitted internet domains" check (Chapter 3.2.2), the Organization Name (O) and Country Name (C) (Chapter 3.1.1.1.1) attributes are included in the configuration of the cPKI as a fixed value pair.

In the event that the requester cannot be assigned to a unique organization, the field must be filled with "Deutsche Telekom AG" or "DTAG," as only certificate requests from employees or agents of the Deutsche Telekom Group or one of its subsidiaries or holdings are processed.

3.1.1.1.3 Organizational Unit Name 1 (OU)

This mandatory attribute OU1 contains the corporate ID (CID) of the employee for the user. This ID is used to achieve uniqueness if the first and last names are the same. The CID is generated in cIAM when the employee master record is created and accompanies the employee during the entire employment relationship or, in the case of external employees, during their assignment relationship.

FMB or GRP is entered in OU1 for groups, function certificates, and role certificates.

The uniqueness of groups, function certificates, and role certificates is ensured by the SAM account name in the CN (see Chapter 3.1.1.1.7).

Example:

OU = C-123456

OU = FMB, OU = GRP

3.1.1.1.4 Organizational Unit Name 2 (OU2)

This mandatory attribute contains the end entity, group, function, role, and employee types.

Examples:

OU = Employee

OU = External workforce

OU = Internal

OU = ssl-vpn

3.1.1.1.5 Organizational Unit Name 3 (OU3)

This attribute can be used to differentiate between natural persons and groups, function certificates, role certificates, and user certificates for mobile devices.

Examples:

OU = Person (natural person or pseudonym)

OU = Users (groups, function certificates, role certificates)

OU = Mobile (user certificates for mobile devices)

3.1.1.1.6 Organizational Unit Name (OU4)

This attribute is used for groups, function certificates, and role certificates, in addition to the attribute C (Country), to identify the worldwide country code. This is a code made up of two letters, which is specified in ISO 3166-1, Alpha-2 (International Organization for Standardization).

Examples:

OU = DE

This value is set on the basis of the attributes that are exported from DTAG's Active Directory.

3.1.1.1.7 Given Name

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

- For user certificates the first name as it is stored in the trusted "cIAM" database.

Examples:

G = Max>

- The GivenName attribute is not set if a pseudonym attribute exists or if it is a group, function, or role certificate.

3.1.1.1.8 Surname

Depending on the certificate type, the mandatory "Surname" field contains the last name of the end entity (see Chapter 1.3.3).

These are as follows:

- For user certificates: the first name as it is stored in the trusted "cIAM" database is entered here.

Examples:

SN = Sample>

The Surname attribute is not set if a pseudonym attribute exists or if it is a group, function, or role certificate.

3.1.1.1.9 Pseudonym

Instead of the real first and last name, user certificates can contain a pseudonym as stored in the trustworthy „cIAM“ database.

Depending on the certificate type, the Pseudonym field may exist instead of the mandatory "GivenName" and "Surname" fields of the end entity (see Chapter 1.3.3).

These are as follows:

Examples:

PN = PN- <Pseudonym>

The pseudonym attribute is not set if there is a first and last name attribute in the certificate, it is a certificate from an internal certification authority or it is a group, function or role certificate.

Starting April 4, 2020, certificates for pseudonyms will only be issued from Deutsche Telekom's non-public internal secure email CA. The OID 2.5.4.65 does not apply here. The certificates will be marked with PN- in the common name.

3.1.1.1.10 Common Name (CN)

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

- The first name and last name for user certificates
- The name with prefix FMB or GRP and the SAM account name from the Active Directory as suffix for group, function, and role certificates
- The server name (FQFN) for server certificates
- The IP address for router certificates
- The server name (FQDN) for email gateway certificates
- The server name (FQDN) for domain controller certificates

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

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.

Examples:

CN = Sam Sample

CN = web1.telekom.de

CN = <IP address>

CN = FMB Functional mailboxes Technical Support.S09876543

CN = PN- <Pseudonym> (see also Chapter 3.1.3)

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 Chapter 3.1.3 for more information).

- The "FMB-" or "GRP-" prefix identifies group, function, and role certificates
- The "PN" certificate identifies the pseudonym

In contrast to user certificates and certificates for pseudonyms, the uniqueness of group, function, and role certificates is not established via the OU1=CID but via the <.SAM Account Name> suffix.

Restrictions: certificates for computers, servers, routers, mail gateways, and domain controllers are only issued by an internal certification authority (see Chapter 1.3.1.2.2).

The "ServerPass" product is available for DTAG servers that are publicly accessible. For more information about ServerPass, see: https://www.telesec.de/de/serverpass

3.1.1.1.11 Email Address (E)

The mandatory "Email Address" field contains:

- The email address of the certificate owner (S/MIME) or email address of the associations of individuals, groups, functions, and roles, etc. in the case of user certificates
- The email address of an administrator or a Functional mailboxes in the case of devices (servers, routers/gateways, mail gateways, domain controllers)

The email address is made up of a local part and a domain part. The local part is the part of the email address that appears before the @ symbol and uniquely identifies the address within the email provider's domain. The domain part appears after the @ symbol and the DNS syntax rules apply.

Example:

E = sam.sample@telekom.de

E = PKI_FMB_TESTBOX2@telekom.de

3.1.1.1.12 Locality Name (L)

This attribute is currently only used for server certificates from the internal CA. This mandatory field contains the name of the city in which the organization (e.g., company, institution, or authority) is registered. This information is verified using a public directory (e.g., extract from the commercial register) or other comparable directories or documents.

Examples:

L = Berlin

L = Munich

L =Frankfurt/Main

As part of the "permitted internet domains" check (Chapter 3.2.2), the Locality Name (L), Country Name (C) (Chapter 3.1.1.1.1), Organization Name (O) (Chapter 3.1.1.1.2), and State or Province Name (S) (Chapter 3.1.1.1.9) attributes are included in the configuration of the cPKI as a fixed value pair (tuple).

3.1.1.1.13 State or Province Name (S)

This attribute is currently only used for server certificates from the internal CA. This mandatory field contains the name of the constituent state or territorial administrative unit (e.g., federal state, canton, or Département) in which the organization (e.g., company, institution, authority) is located or registered. 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:
  S = "Berlin"
  S = "Bavaria"
  S = "Hesse"
- After an established abbreviation of the "State or Province Name" (Subdivision Name).
  Examples:
  S= "NW" for North Rhine-Westphalia
  S = "BRU" for Région de Bruxelles-Capitale
  S = "75" for Paris

More details are available here:
http://www.unece.org/cefact/locode/subdivisions.html
e.g.,: https://www.iso.org/obp/ui/#iso:code:3166:DE (changing the country code in accordance with ISO 3166-1 ("DE" in the example) allows the selection of a different, country-specific "State or Province Name (Subdivision)").

As part of the "permitted internet domains" check (Chapter 3.2.2), the State or Province Name (S), Country Name (C) (Chapter 3.1.1.1.1), Organization Name (O) (Chapter 3.1.1.1.2), and Locality Name (L) (Chapter 3.1.1.1.8) attributes are included in the configuration of the cPKI as a fixed value pair (tuple).

3.1.1.1.14 Street Address (STREET)

This attribute is currently only used for server certificates from the internal CA. This optional field contains the name of the street where the organization (e.g., company, institution, or authority) is based. This information is verified using a public directory (e.g., extract from the commercial register) or comparable directories or documents.

Example:

STREET = Sample Street 17

STREET = 5th Avenue

3.1.1.1.15 Postal Code (PostalCode)

This attribute is currently only used for server certificates from the internal CA. This optional field contains the postal code of the city in which the organization (e.g., company, institution, or authority) is registered. This information is verified using a public directory (e.g., extract from the commercial register) or comparable directories or documents.

Example:

PostalCode = 57250

PostalCode = AZ23G7

3.1.1.1.16 Subject DN Serial Number (SN)

The SN attribute is not used within the cPKI.

3.1.1.1.17 Unstructured Name

Further information on the "unstructured name" can be found in Chapter 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 (Chapter 3.1.1.1.6)
- Email address (Chapter 3.1.1.1.7)

- User Principal Name (Chapter 3.1.1.2.2)
- DNS Name (Chapter 3.1.1.2.3)
- IP Address (Chapter 3.1.1.2.4)

as well as from optional fields such as:

- Email address (Chapter 3.1.1.1.7)
- DNS Name (Chapter 3.1.1.2.3)

Restrictions to certificate content are described in Chapter 3.1.1.1.6.

3.1.1.2.1 RFC822 name

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

3.1.1.2.2 User Principal Name (Prinzipalname)

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 Principal Name" is a user-friendly (i.e., easy to remember) name that is used as a Windows login for the domain or Active Directory. It 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 email address.

For user certificates as well as group and/or function certificates, the UPN is shown in the "Subject Alternative Name" (Chapter 7.1.2.3) extension as the "Principal Name."

Examples:

Prinzipalname = sam.sample@telekom.de

Prinzipalname = sam.sample@local-server.com

RFC822 name = PKI_FMB_TEST @telekom.de

However, the UPN can also be as follows:
Prinzipalname = S01234567@emea1.cds.t-internal.com

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."

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 group, function, and role certificates and for pseudonyms, Telekom Security can request from the tenant DTAG that the certificate owner's true identity be revealed to authorized third parties.

3.1.3 Pseudonymity or anonymity of the certificate owner

User certificates that contain a pseudonym are identified with the prefix "PN-" in the Common Name (CN) (see Chapter 3.1.1.1.7 for more information).

User certificates for group, function, or role certificates are marked with the prefix "FMB-" or "GRP-" in the Common Name (CN) and additionally with the entry FMB or GRP in the Organization Unit (OU).

User certificates for a robot or machine will be identified with the prefix "Robot-" in the Common Name (CN) field and additionally in the Organization Unit (OU) field with the entry "Robot"

Examples:

Pseudonym:

CN=PN-Novalis
CN=PN-George Sand

Group, function, role certificates:

CN = FMB-Trust Center Test.S09750343
OU = GRP

Alternatively, the designation FMB can be used instead of GRP.

Example:

CN=FMB-Technical Support
OU=FMB

Roboter und Automaten:

CN = Robot-pcwdm
OU = Robot

The choice of pseudonyms or group, function and groups, role or Robot designations is subject to various name restrictions. Excluded are names that suggest permissions (such as Telekom CA) that the certificate owner does not have, political slogans, offensive names, or any infringement of trademark rights.

The DTAG Trust Center reserves the right to refuse the issue of a pseudonym. The rejection does not require a statement of reasons.

For more details on issuing certificates for pseudonyms and person and function groups, see Chapters 1.4.1.3 and 1.4.1.4.

3.1.4 Rules on the interpretation of different name formats

No provisions.

3.1.5 Uniqueness of names

Telekom Security makes sure that user certificates (from different users) with the same subject-DN (see Chapter 3.1.1.1 et seq.) only occur once within the cPKI. This is ensured by entering the Corporate ID (CID) in the Subject DN (see Chapter 3.1.1.1.3).

For group, function, and role certificates the uniqueness is guaranteed by the SAM Account Name suffix in the CN (see Chapter 3.1.1.1.7). The separator between function name and Sam Account Name is a dot character.

For users, it is possible to issue one, two, or three certificates that have the same unique Subject DN but differ in terms of the key usage or enhanced key usage and the certificate serial number. With the renewal, multiple revoked certificates with the same subject DN and the same key usage may be available for a limited period of time

There may be multiple certificates for devices with the same Subject DN (see Chapter 3.1.1 et seq.).

3.1.6 Recognition, authentication, and role of trademarks

There is a particular duty of care when selecting the names of trademarks, trademark rights, etc. in certificates (e.g., Organization Name (O), Organizational Unit Name (OU)). It is the responsibility of the customer 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 of the cPKI is not obligated to check such rights. Any resulting claims for damages are at the expense of the customer.

3.2 Identity check for new request

3.2.1 Method for proving ownership of the private key

In the event of a new order, the certificate owner must prove to the certification authority in a suitable manner that they own the private key that is mapped to the public key to be certified. Proof of ownership is furnished by the PKCS#10 method. This requirement does not apply if the key is generated by the certification authority itself, e.g., for key pairs for the encryption certificate (see Chapter 3.2.3.3). In this case the assignment between public and secret key is implicit.

3.2.2 Authentication of the organization and domain identity

A basic requirement for being able to use the cPKI is to set up a PKI tenant within the cPKI's PKI service.

The cPKI service is used solely by the tenant DTAG. All DTAG users belong to a DTAG organization or have a defined contractual relationship with DTAG.

When authenticating organizations, Telekom Security ensures that the names used are checked.

Telekom Security performs the following checks:

- Determination of the existence of the organization by means of corresponding up-to-date organizational documents of DTAG (e.g., T-SIS) issued by a competent Group office confirming the existence of the organization
- Check of the domain name(s) against a whitelist of "permitted domains" before issuing certificates
- Technical limitation of the permitted domains (domain constraints) in the certification authority secure email CA (see Chapter 7.1.5)

Organizational changes (e.g., change of name) must be notified immediately in writing to the publisher (see Chapter 4.9.1) of this CP/CPS. In this case, Telekom Security will not issue any further certificates to this organization. Certificate renewals are issued as of the organizational change (e.g., change of name) to the organization that is valid at that time.

Telekom Security will immediately revoke issued certificates in the event of the reasons for revocation stated in Chapter 4.9.1.

To fulfill and comply with the [CAB-BR], Telekom Security will repeat the process of authenticating the relevant organization's identity after 27 months at the latest. For domains that are used for other certificate types, the check is performed after a maximum of 825 days (also refer to Chapter 3.3). A comparison with the Telekom – Subsidiaries Information System (T-SIS) is carried out for this purpose.

The task and objective of T-SIS is to provide basic information on the Telekom Group companies for internal and external use. T-SIS provides the basic information for this on a daily basis. All information can be retrieved for any given key date. The history can also be traced back further within the basic information of the legal units.

The information stored in T-SIS is released by DTAG's legal department and updated daily by Deutsche Telekom Services Europe (DTSE).

Additional checks are carried out as required.

O=DTAG or O=Deutsche Telekom AG is set in the certificate for all organizations belonging to the Deutsche Telekom AG Group or an external organization that has a defined contractual relationship with the Deutsche Telekom AG Group.

The designation DTAG is a trademark of Deutsche Telekom AG registered under registration number 30118939.

3.2.3 Authenticating the identity of end entities

In the DTAG Group, the identity or identification of end entities (see Chapter 1.3.3) is authenticated by HR when the employee is hired and the employee is created in DTAG's SAP HR system.

In the case of external employees, this is done by a cost center owner or by an employee whom the cost center owner has commissioned with this task. All employees who are allowed to authenticate the identity or identification of an external employee are trained by DTAG. The training must be proven by a subscriber certificate and stored in SAP HR. You cannot create external employees without this specification.

Pseudonyms, robots, function- und group- accounts are authenticated locally by a cost center owner (or by an employee whom the cost center owner has commissioned with this task) in whose area or department the pseudonym is used. The same process applies as for external users. Furthermore, the CostO assumes key responsibility for the certificate and key material issued to the pseudonym, the robot or groups of persons and functions (see Chapter 1.4.1.3).

The data of the authenticated internal or external employees as well as pseudonyms, robots, function and group accounts is then transferred from SAP HR to cIAM.

When internal employees are hired or external employees assigned, these departments create a master record for a person in the SAP HR system, save it, and make it available to the Corporate Identity Management System (cIAM).

cIAM generates orders to create or update user records for downstream systems (such as TAdmin2, MyIT and Email Backbone (EMBB)).

TAdmin2 provides or updates the records for German employees of DTAG to the following systems: Active Directory, Exchange, Remote Access, cPKI. In addition, these systems also manage the life cycle (change, cancellation, or deletion) of master records and the associated other data attributes.

MyIT is responsible for provisioning or updating the data records for international DTAG employees to the Active Directory, Exchange and, if necessary, Remote Access. Data records for provisioning or updating for the PKI are also sent for international users from CIAM to the cPKI via TAdmin2 as for German employees.

Each of these systems guarantees confidentiality, availability, and integrity of generated, processed, or stored data as well as their secure transfer to other systems.

The authenticity, verifiability, and trustworthiness of data relating to a natural person are based on defined processes in the Deutsche Telekom Group's HR management. An overview of the systems to be considered in the context of the cPKI and the identification of natural persons as end entities is shown in the following diagram. cIAM is therefore regarded by the DTAG Group as a trusted database for cPKI's certificate life cycle management based on the requirements and regulations of ETSI 319411-1 Policy LCP (see also Chapter 1.3.2 et seq.).

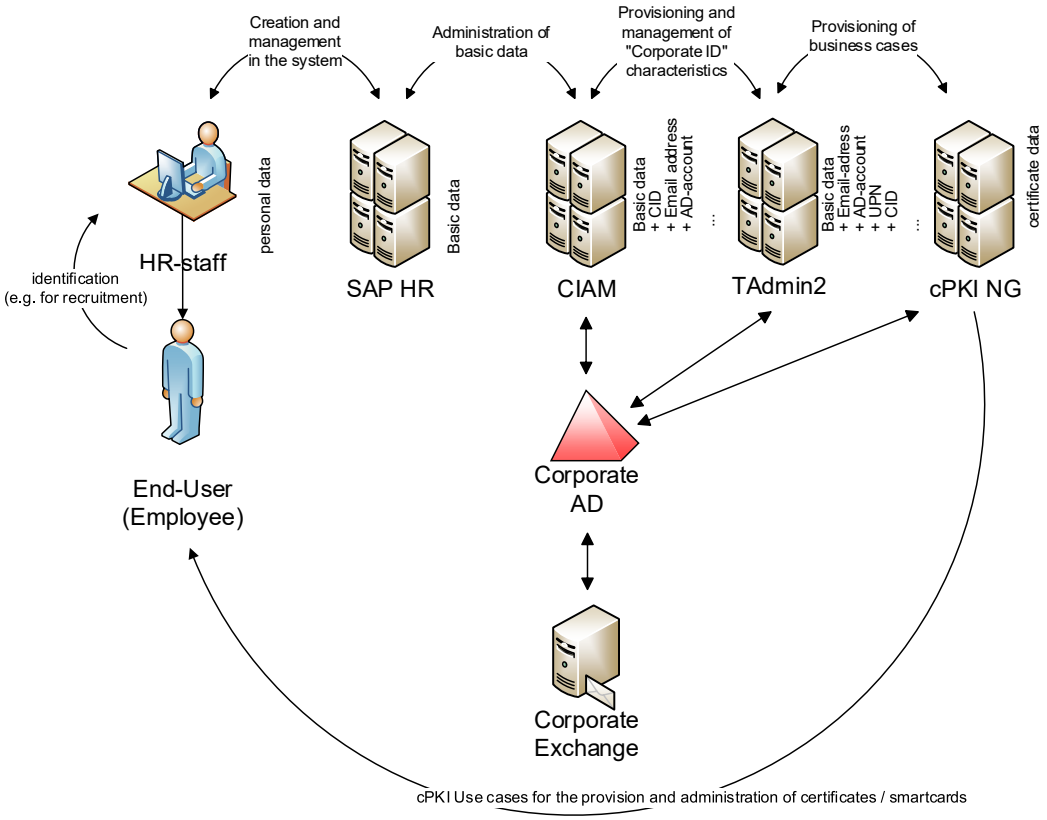

Figure 8: Authenticating a natural person (Germany) in EMEA1

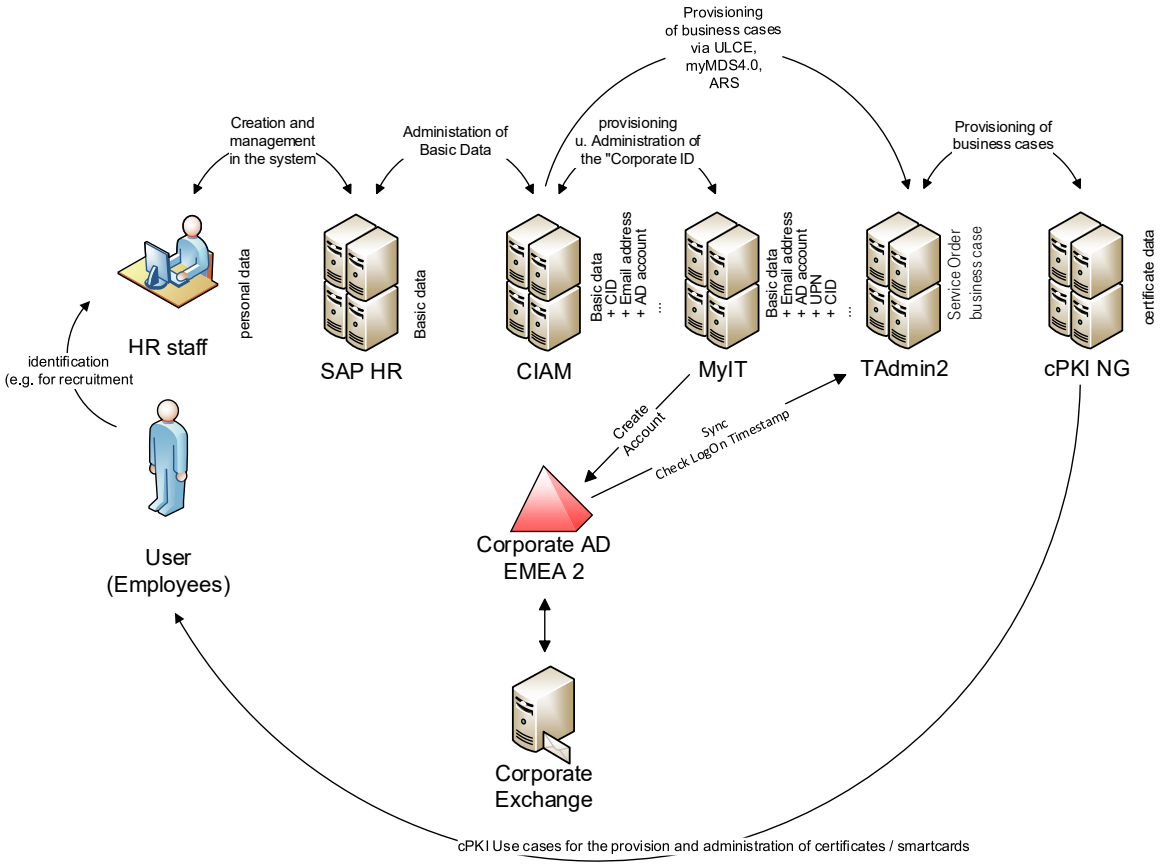

Figure 9: Authenticating a natural person (International) in EMEA 2

An automatic renewal function is available for user certificates, which is made available as often as required. For this purpose, the life cycle management of the cPKI generates a certificate renewal order. In any case, the current data from cIAM is used for all certificate renewals, thus ensuring that any certificate-relevant changes are taken into account during certificate renewals. No renewal function is available for device certificates.

Legal persons are identified and verified by the RA employees of the Trust Center.

3.2.3.1 Registration of DTAG-internal users

The registration of internal users (natural persons) is based on the trusted database cIAM.

3.2.3.2 Registration of external users working for DTAG

The registration of external users (natural persons) is based on the trusted database cIAM.

3.2.3.3 Registration of person and function groups

Person and function group are registered by the owner of the person and function group account. For this purpose, the owner of the person and function group account must log on to the cPKI with his authentication certificate. Based on the certificate, the cPKI checks whether the registered user is actually the owner. This ensures that a certificate can be requested by the actual person and function group address (see Chapter 1.4.1.4).

3.2.3.4 Registration of pseudonyms

The registration of pseudonyms is based on the trusted database cIAM.

The CostO assumes key responsibility for the certificate and key material issued for the pseudonym in the area or department in which the pseudonym is used (see Chapter 1.4.1.3). Device registration

Computers (802.1x) are registered automatically by auto-enrollment when the computer is included in the EMEA1 and EMEA2 domains.

Other devices (servers, routers/gateways, mail gateways, and domain controllers) are registered centrally or locally by the relevant device administrator. To do this, the administrator must submit a request to the certification authority (see Chapter 1.4.1.2.2).

3.2.3.5 Registration of von Robots and Bots

The registration of robots and bots is based on the trustworthy database cIAM.

The key responsibility for the certificate and key material issued to the robot is assumed by the cost center manager in whose area or department the robot is deployed. (see Chapter 1.4.1.3). Registration of devices

3.2.3.6 Registration of legal persons

Legal entities are registered through the manual RA point of the Trust Center.

3.2.3.7 Registration of Computers

The computer registration (802.1x) is automatically performed by autoenrollment when the computer is entered in the EMEA1 or EMEA2 domain.

3.2.3.8 Registration of Other Devices (Server, Router/Gateway, Mail Gateway and Domain Controller)

The registration of other devices (server, router/gateway, mail gateway and domain controller) is performed centrally or decentrally by the respective device administrator. For this, the administrator must submit an application to the certification authority (see chapter 1.4.1.2.2).

3.2.4 Non-verified subscriber information

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

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

Certificates issued under the "Deutsche Telekom AG Issuing CA 01", "Deutsche Telekom AG Issuing CA 02", and "Deutsche Telekom AG secure email CA", „Deutsche Telekom AG secure email CA E02“ and „Deutsche Telekom AG secure email CA E03“ sub-CAs contain information verified by Telekom Security. All information included in the certificate originates from the DTAG backend systems and is to be regarded as validated.

Authorization check:
Users are entitled to receive certificates if they have a valid employment contract with DTAG or one of its subsidiaries or if they have a defined contractual relationship (external employees and partners) and are administered in Deutsche Telekom's backend systems (SAP HR, cIAM, Corporate-AD, TAdmin2).

Certificates that are issued under the "Deutsche Telekom AG Issuing CA 03", „Deutsche Telekom AG infrastructure CA“ and "Deutsche Telekom AG mobile device CA" sub-CAs may contain information that has not been verified.

3.2.5 Authorization check

3.2.5.1 Ensuring the authenticity of the certification request

To determine the authenticity of the data from SAP HR, cIAM, and TAdmin2, the following actions are carried out for the specified systems:

- Regular audits with the Internal Control System (ICS) by external auditors
- Implementation and release in a PRIVACY & SECURITY ASSESSMENT (PSA) procedure
- Implementation of penetration tests by Telekom Security experts
- Certification in accordance with ISO 27001

3.2.5.2 Checking domains and IP addresses

The issuing of certificates is limited to domains of Deutsche Telekom; for this purpose a limitation to permitted email domains is implemented in the certificate management of the cPKI. A domain constraint in the certificate will no longer apply to public certification authorities from February 25, 2020 as the CAs have been audited in accordance with ETSI 319411-1 Policy LCP and are included in the CCADB.

CA certificates with an issue date before February 25, 2020 also contain a domain constraint (name restriction) in the CA certificate on approved mail domains.

DTAG notifies Telekom Security of the domains for which certificates are to be issued so that Telekom Security can check them and include and maintain them in the tenant's PKI configuration as "permitted internet domains."

The check is carried out on the basis of documents provided by the customer.

In addition, the specifying domains are validated against the Office 365 Azure AD (Cloud). For the domains stored in DTAG's Office 365 Azure AD, Microsoft checked whether DTAG actually owns these domains.

All relevant domains have been verified by Microsoft.

After verification by Telekom Security, the "approved domains" are included in or removed from the "Deutsche Telekom AG secure email CA" and in the PKI configuration of the cPKI.

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.

For internal certification authorities, the restriction of the permitted domains is also only takes place in the certificate management of the cPKI.

To fulfill and comply with the [CAB-BR], Telekom Security will verify the usage rights of the domain(s) after 825 days at the latest. Telekom Security is entitled to request a complete list of all domains registered to DTAG and its subsidiaries and holdings from the customer.

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 Chapter 7.1.6.2), 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 "cPKI" PKI service. This is ensured by the basic restrictions placed on the sub-CAs (path length limitation=0).

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/MyCard, soft PSE).

Key renewal for MyCards

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 do not forbid or prevent this. Otherwise a

subsequent certificate must be issued on a new smartcard. The provisions described in Chapters 3.2.3 et seq. and 4.2.1 apply. 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 to decide whether a key renewal takes place. The provisions of Chapter 6.1 must be taken into account.

3.3.1 Identification and authentication for routine key renewal

Before the certificate is drawn up, it is checked whether the user exists in the relevant DTAG systems and the data is correct.

New certificates are issued for all intended uses. In the case of encryption certificates, new cryptographic key material is always generated.

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.
Only the Replace option is available here.

Before the certificate is drawn up, it is checked whether the user exists in the relevant DTAG systems and the data is correct.

With regard to user certificates, new certificates are issued for all intended uses. In the case of encryption certificates, new cryptographic key material is always generated.

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 available is that of validation by the manual registration authority, which can reactivate the certificate renewal in the cPKI after the described identity check.

3.4 Identification and authentication for revocation orders

Revocation requests are authenticated using a question or answer stored in the system by the certificate owner. After the secret answer has been verified by the Service Desk, the certificate is revoked or replaced. A Replace also results in the immediate revocation of all certificates of the user.
If revoked, the certificate is included in a revocation list.

The revocation of certificates can be ordered by telephone at the Service Desk. The input channels of the relevant Service Desk communicated within the DTAG Group must be used when issuing a revocation request by phone.

If any misuse of a certificate is suspected, this can be reported to the Service Desk by stating the issuing certification authority, the Common Name and email address, or the serial number of the certificate, as well as by describing the nature of the misuse. Telekom Security checks and evaluates this case. In the event of substantiated certificate misuse, Telekom Security is authorized and obligated to revoke the certificate immediately (Chapters 4.9.1 and 4.9.2).

Cases of misuse can be reported by:
- Phone (see Chapter 1.5.2)
- Email (see Chapter 1.5.2)
- Internet: https://corporate-pki.telekom.de/ "Kontakt | Zertifikatsmissbrauch melden" [Contact | Report certificate misuse]

- By employees of the DTAG Group via the communicated input channels of the relevant responsible Service Desks and via the DTAG Group Situation Center 24 hours a day

4 OPERATIONAL REQUIREMENTS IN THE LIFE CYCLE OF CERTIFICATES

4.1 Certificate request

4.1.1 Who can request certificates?

The following conditions apply when requesting certificates:

- The requester is an employee of DTAG, a subsidiary, or a holding or has a contractual relationship with DTAG and works on behalf of DTAG.
- The requester is set up in cIAM and has an active employment relationship.
- The requester has an active domain account and an email address from a permitted mail domain.
- The requester (subject) requests the certificate by clicking on the link in the email to the user and subsequently registering at the web portal.
- The requester accepts the Terms of Use of the DTAG Corporate PKI by clicking on the link to personalize and activate the MyCard in the enrollment email.
- Successful registration of the requester at the cPKI web portal
- Possession of a MyCard (DTAG smartcard)
- For computers, the requester must have a computer account in a permitted AD domain.
- Optional: access data for SCEP and REST interface

The following persons can request a certificate:

- Authorized persons who appear as the subject of the certificate (internal or external DTAG employees with an active contract)
- Authorized persons from groups of persons and functions, legal persons, robots and devices
- Authorized persons who are entitled to request pseudonym accounts
- Organizations represented by authorized representatives of DTAG

Authorized persons are defined as natural persons who have suitable login details and fulfill the above-mentioned requirements.

4.1.2 Registration process and responsibilities

4.1.2.1 Automated registration authority

Subscribers are registered via upstream identification, authentication, and provisioning processes in Deutsche Telekom's IT infrastructure.

This means that the registration data has already been processed and verified by the upstream systems. The certificates are then issued on the basis of the trusted data from cIAM. See Chapters 1.3.2 and 3.2.3 for more information.

The responsibility for the correctness of the data is taken over by the relevant recording authority or the authority responsible for the operation of the respective systems.

The establishment and further maintenance of the "permitted internet domains" are based on the successful authentication of the identity of organizations as described in Chapter 3.2.2.

The requester (subject) requests the certificate by clicking on the link in the enrollment email and subsequently registering at the web portal. By clicking on the link for activation and personalization of the MyCard, the certificate request for the DTAG corporate PKI is executed on the basis of the data from the trusted database (cIAM) and the end entity acknowledges the Terms of Use of the corporate PKI Deutsche Telekom (cPKI) and declares that they have read and understood them. The corresponding notice and the link to the Terms of Use are included in the enrollment email.

4.1.2.2 Manual registration authorities

4.1.2.2.1 Trust Center registration authority employee

Key material and certificates for legal persons that are securely stored in the Trust Center are recovered manually by trained and security-checked Trust Center staff using the manual registration authority.

Several different people with different roles and permissions are required for recovery.

- Recovery Manager
- Recovery Approver
- Recovery Operator

Process in detail:

1. The requester completes a standardized form for the recovery of a specific encryption key for a specific user and forwards the process to Corporate Security, Privacy, and the Works Council for authorization. After authorization and digital signing of all parties involved, the request is encrypted, signed, and emailed to the Trust Center.
2. The Recovery Manager checks the following points: receipt of the order, process authorization, digital signatures, requester (subject) data, user data, and shipping data.
3. The Recovery Manager logs on to the cPKI with their MyCard and starts the "Certificate Recovery" workflow. This order must be approved by the Recovery Approver. The Recovery Approver is requested by email to approve the order.
4. The Recovery Approver logs on to the cPKI with their MyCard and starts the "Approve Certificate Recovery" workflow. After approval, the Recovery Operator is notified by email that there is an approved recovery request.
5. The Recovery Operator logs on to the cPKI with their MyCard and starts the "Execute Certificate Recovery" workflow. MyID selects the certificates to be recovered from the cPKI. The encryption keys are stored on a dedicated smartcard (recovery card). A user PIN for the smartcard is assigned by the server and also stored on the card.
6. The cPKI automatically generates a letter, which the Recovery Operator sends to the requester together with the smartcard. Furthermore, the Recovery Operator sends an encrypted email containing the user PIN information to the requester.
7. The recovery process is logged in the cPKI. The request form is archived.
   All order processes are signed with the personal digital signature of the relevant role owner.

4.1.2.2.2 End entities including registration authority employees

All end entities acknowledge the current version of the "Certificate Policy (CP)/Certification Practice Statement (CPS)" document and agree to comply with the rules described therein.

Furthermore, the end entity and registration authority employee guarantee:

- That the information stated in the certificate request is true and correct
- 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

- To comply with DTAG's "Data protection requirement – access to the personal communication and filing environment."

The above obligations also apply to the TSP, which issues certificates in its name.

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

4.1.2.3 Manual registration authority for certificates

The manual internal registration authority can only issue certificates from the internal CA and "Deutsche Telekom AG secure email CA E03."

Registration is performed through

- another appropriate process (e.g., request via the user website, email, SCEP interface), which clearly indicates the end entity's identity. The subject data of the certificate may be based on a tenant database with integrity. Evidence of the generation of the data inventory must be provided to the certification authority on request.
- the administrator as the key owner for devices. Authorized administrators are authenticated by the Trust Center. The administrator must control or operate the device specified in the certificate.
- Trust Center employees

The registration authority undertakes to perform the following tasks:

- The naming conventions in accordance with Chapter 3.1.1 et seq. must be complied with.
- In the case of device certificates, the domain part of the email address or the DNS name (top level domain and other FQDN sub-domains) must be checked for the "permitted internet domains" entered in the PKI configuration, depending on the certificate type.
- If the customer 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 (see also Chapter 3.2.2).
- If the names are identical, the registration authority must render them unique.
- Only DTAG data (Country Name (C), Organization Name (O), Organizational Unit Name, domain part of the email address and, if applicable, User Principal Name (UPN), top-level and other sub-domains of the fully qualified domain name (FQDN), also refer to Chapter 3.1.1 et seq.) may be used.

4.1.2.4 Manual registration authority for legal persons

The manual registration authority for issuing certificates for legal entities is operated by trained and security-certified personnel of the Trust Center.

The registration and issue of certificates takes place on the basis of a standardized certificate request form.

4.2 Processing certification requests

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

4.2.1 Performing identification and authentication

4.2.1.1 Automated registration authority

End entities are identified and authenticated within the framework of established HR processes by HR management (DTSE) units within the DTAG Group (see Chapter 3.2.3). The SAP HR data is transferred to cIAM after the master record has been created.

The Subject DN of certificates is based on the database of the Corporate Identity and Access Management (cIAM), which builds on the SAP HR data and is also supplemented by information (e.g., email address, Corporate ID) through the cIAM system and transferred to TAdmin2 for creating the user account and mailbox and for commissioning the cPKI (certificate request).

In the case of international users, the user account creation of MyID is based on the cIAM data and TAdmin2 receives a service order from cIAM and starts a PKI workflow after recognizing the user's initial login to the user account and transfers the registration data/certificate request to the cPKI.

The cPKI receives the certificate requests in electronic form from TAdmin2 as the applying authority and checks them for integrity. Misleading request data will be rejected to the requesting system. The email address is then electronically verified by sending an email containing a URL and a one-time password for the generation or retrieval of certificates by a user. This ensures that the end entity is the owner of the email address. In addition, the domain part of the email address (optionally also the UPN) is checked for the "permitted mail domains" entered in the PKI configuration and the name restrictions stored in the CA certificate.

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 or the groups of persons/functions must be authenticated as well.

In the case of device certificates, the domain part of the email address or the DNS name (top level domain and other FQDN sub-domains) is to be checked for the "permitted mail domains" entered in the PKI configuration, depending on the certificate type.

For function certificates, the real identity of the responsible requester or deputy is verified by means of certificate-based login to the cPKI portal and by checking the owner of function mailboxes in the Active Directory.

The issue of end-entity certificates is based on a successful authentication at the cPKI web portal. This requires, as a minimum, logging in with the domain account of the end entity as well as entering an order-related One Time Password (OTP). For other certificate types, e.g., certificates for FMB, the key owner can only be authenticated by means of a personal smartcard certificate.

4.2.1.2 Manual registration authority

The manual registration authority provides certificates or key material for the special cases described in Chapter 1.3.2.2:

The end entities are authenticated by the registrars of the TSP (see Chapter 1.3.2.2).

In the case of a certificate request for a legal person, the requester must prove in an appropriate manner that they are entitled to request a certificate for a legal person.

The registration authority undertakes to perform the following tasks:

- Registration is performed through
  - personal appearance of the end entity, their deputy, or key owners who can authenticate themselves by presenting appropriate ID documents and who are responsible for the proper preparation of the certification request and the certificate installation, or

- another appropriate process (e.g., request via the user website, email, SCEP interface), which clearly indicates the end entity's identity. The subject data of the certificate may be based on a DTAG database with integrity (see Chapter 1.3.2.1)

- 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 certification request, verifies its integrity and authenticity, and checks the details it contains against the digital signature or unique identification documents presented by the requester (e.g., company ID, personal ID[2], or the trusted database of DTAG (cIAM)) for authenticity (whether they are genuine and trusted), integrity (whether they have not been tampered with), as well as correctness, truth, and completeness. Reliable internal and public data sources may be used to authenticate the request data.
- If the customer has additional domains to which certificates are to be issued, Telekom Security must be informed about the additional domain. After a successful domain check, these are included in the PKI configuration of the cPKI (see also Chapter 3.2.2).
- Requesters providing misleading request details are to be rejected.
- 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 email address and, if applicable, User Principal Name (UPN), top-level and other sub-domains of the fully qualified domain name (FQDN), also refer to Chapter 3.1.1 et seq.), then a power of attorney or authorization document from the requester is required.
- The unique identification documents and requests submitted by the requester must be archived for at least seven years in an audit-proof manner as a copy. This archive must be protected against unauthorized access. To do this, the documents are stored electronically in the management system of the cPKI in an audit-proof manner.
- In the event of audits or other reviews (e.g., random checks), the registration documents must be disclosed to the auditor by TSP.
- The registration authority employees are obliged to report any suspicions of compromised keys, certificate misuse, or other (attempted) fraud in relation to certificates via the TSP reporting channels immediately.

4.2.2 Acceptance or rejection of certificate requests

A reference number (correlation ID) is issued during the certificate request to provide a clear assignment of an issued certificate to the relevant request).

4.2.2.1 Automated registration authority

Certification requests are automatically rejected in the event of data inconsistencies and missing authorizations. If the orders are correct, the requests are automatically accepted and further processing is initiated.

4.2.2.2 Manual registration authorities

Only after the certificate holder has registered successfully will a certification request be processed further (see Chapters 3.2.3, 4.1.2.4 and 4.2.1.2). Depending on the type of certificate (see Chapter 3.2.3), the registrar enters the certification request electronically via their website or approves the request, which has already been submitted electronically.

A certificate request must be rejected if:

- The certificate request and the identification are not complete, true, or correct
- The certificate request and the identification are from an untrustworthy source

[2] The access number on the front should be blacked out for security reasons, as this can be used for online functions.

- The certificate request and the identification do not lead to a clear positive registration result
- The public key falls short of the minimum length of 2,048 bits
- The public exponent does not meet the specifications of the [CAB-BR]
- The result of checking for Debian weakness is positive

If the request is rejected, the certificate holder's technical contact will be notified by email giving reasons.

4.2.3 Processing period for certificate requests

4.2.3.1 Automated registration authority

Processing of the certificate request starts within a suitable period following receipt of the request. The subscriber has 21 days after acceptance of the certificate request to register on the cPKI portal and to enroll the certificates. If a subscriber has not retrieved their certificates by the end of this period, the corresponding order will be canceled and the user account revoked.

4.2.3.2 Manual registration authorities

4.2.3.2.1 Trust Center registration authority employee

The processing of certificate applications based on the "cPKI Request Key Backup" or "Certificate Request for Legal Entities" document takes place within a reasonable period of time after receipt of the complete documents.

Certificate requests rejected by the automated registration authority are processed on the basis of "Order Receipt + 1 WD."

4.2.3.3 Manual registration authority for certificates from the internal CA

The processing time of certificate requests for device certificates (except auto-enrollment for 802.1x computer certificates) is the responsibility of the respective registered device administrator operating the device or exercising control over it.

4.3 Issuing of certificates

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 Automated registration authority

After the certificate request has been approved, the certificate management checks the certificate request for the "approved email domains" entered in the PKI configuration and the CA system for the "approved email domains" entered in the name restrictions on the CA certificate. If the check is positive, the end entity receives an email with a one-time password (OTP) and the URL to the cPKI portal. If the certificates are issued for the first time, users must authenticate themselves to the cPKI portal with their AD account and the OTP stated in the email.

After successful login and OTP verification, a check is carried out to ensure that a new smartcard (MyCard) with a PIN code is in the card reader. The end entity then sets up two questions and answers and a 6-digit smartcard PIN. The certificates are issued immediately afterwards and written to the smartcard (MyCard) (For key generation, see Chapter 6.1)

When renewing a certificate, the registration can alternatively be performed with the subscriber certificate for authentication or the two set questions and answers. The smartcard (MyCard) registered to the end entity can continue to be used when the certificate is renewed. The serial number of the inserted smartcard is checked against the smartcard

stored in the certificate management system. A different smartcard that is not in the zero-pin state (PIN code) cannot be used and will be rejected by the PKI system.

4.3.1.2 Manual registration authorities

4.3.1.2.1 TSP registration authority

After the KeyBackup request has been approved, the KeyBackup is immediately written to the smartcard.

Following approval of the certificate request for legal persons, the certificate is immediately issued as a soft PSE.

No new certificates from the public certification authority are issued through this registration authority, apart from the above-mentioned certificates for legal persons.

4.3.1.3 Manual registration authority for certificates from the internal CA

Following approval of the certificate request, the CA system checks the certificate request for the "permitted internet domains" entered in the PKI configuration. If the result is positive, the certificate is issued immediately.

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 responsible registered device administrator is informed via an information message.

4.3.2 Notification of end entities

4.3.2.1 Automated registration authority

After acceptance of the certificate application, the certificate owner is notified by email. This email contains a URL and an OTP (one-time password).

The certificate owner calls up the URL, enters the OTP in the appropriate place, and inserts the card into the card reader connected to the user PC.

The MyCard is then personalized by the respective certificate owner by entering the PIN, i.e., his certificate is provided from the corresponding CA and written to the card.

In the event that the encryption certificate is to be assigned to a group or function member or a deputy, a notification is also sent to the deputy.

The deputy will be notified by email. This email contains a URL.

The group or function member or deputy calls up the URL and inserts the card into the card reader connected to the user PC.

The Personal Security Environment (PSE) of the deputy is written to the MyCard after entering the PIN.

After successful application of the certificate, a success message with the details of the rolled out certificate(s) is displayed on the cPKI for the end entity.

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
- If the end entity does not raise an objection to the certificate or its contents with the Trust Center within a time period defined by DTAG after receiving the certificate

- If the Trust Center does not receive an objection within a time period defined by DTAG after receiving the certificate or the certificate content
- Use of the certificate

By accepting the certificate, the certificate owner agrees to the provisions in this document and assures that all details and explanations regarding the information contained in the certificate are true.

4.4.2 Publication of the certificate by the certification authority

Certificates are published via the DTAG Corporate Active Directory and a cPKI directory service. The following rules apply:

- The publication of the certificates depends on the certificate type and the provisions in Table 10: Specifications for the publication of certificates.
- In addition, certain certificate types (see Table 10) can be published by agreement.
- Additional data such as the MyCard serial number or CID can be published in the directory service of the cPKI by agreement.
- The cPKI directory service and the DTAG Corporate Active Directory can only be accessed from the DTAG intranet.

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

Notifications can be sent by email or via system interfaces (approval notification) to other instances and persons (e.g., registrars, administrators, owners of function groups, function groups, IT systems).

4.5 Use of the key pair and the certificate

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

The certificate and the associated private key may only be used in accordance with the Terms of Use of this CP/CPS and the DTAG Internal Subscriber Agreement.

The use of the private key with the corresponding certified public key is permitted only once the end entity has accepted the certificate (Chapter 4.4.1).

Use of the certificate is determined by the specifications and intended use in the DTAG-internal rules. 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 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 emails)

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

- The key owner (Chapters 1.3.3 and 1.4.1.4) 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 CP/CPS when using the private key.
- Temporary certificate revocations can be transferred to individuals from the group of end entities.

- Final certificate revocations can only be initiated by the key owner. To do this, the key owner must provide the details of the revocation reasons and the question and answer required for the revocation.
- 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 withdrawing the certificate from this user. If it is not possible to withdraw the certificate, the certificate must be revoked immediately.
- A transfer of responsibility to a new or additional key owner for pseudonyms, robots or function- and group-accounts takes place in DTAG's HR system and must be documented there. The new key owner needs to be identified and registered in accordance with this CP/CPS and evidence must be produced of their authorization as a key owner.
- A transfer of responsibility to a new or additional key owner for function groups (Functional mailboxes) takes place in the cPKI system and must be documented there. The new key owner is identified in accordance with this CP/CPS, their authorization as key owner (owner of the mailbox) is checked against DTAG's Active Directory.

The certificate must be revoked immediately if the information in the certificate is no longer correct or if the private key has been compromised (see Chapter 4.9).

4.5.2 Use of the certificate by relying parties

Every relying party who uses a certificate issued by the cPKI should do the following:

- 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 Certificate Policy. 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, deputy, or other instance is informed about the renewal of the certificate by email (renewal notification). This email contains the relevant certificate information.

This notification is sent 30 calendar days before the certificate expires and will be sent repeatedly until the certificate has either been renewed or has expired.

When a certificate is renewed, a new certificate with a new serial number, a new validity period, and the same Subject DN (as long as no changes have been made since the last certificate request, see Chapter 3.1.1.1) are issued to the certificate holder.

A certificate renewal feature is implemented only for user certificates and computer certificates (auto-enrollment for computers in the DTAG domain). The user of the device does not receive a notification (auto-enrollment) for certificate renewals for computer certificates.

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.

Smartcards can still be re-certified even after the existing certificate has expired. It is not possible to renew an expired soft PSE certificate. As a matter of principle, it is not possible to renew a revoked 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 certificate renewal

If no reasons argue against it (e.g., contract termination, termination of the employment contract, leave granted), users must procure a new certificate before the validity of their current certificate expires in order to ensure the continuity of the certificate usage.

For renewal, the certificate must be available including the private key.

4.6.2 Who may request re-certification?

Only the user or the key owner may order a renewal.

The user or key owner must be in an active employment relationship or, in the case of external employees, in an ongoing assignment. Furthermore, no certificate renewal is possible without an active domain account in DTAG's Active Directory.

4.6.3 Processing of certificate 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.

Certificates are renewed by the certificate owners themselves. The end entity may hold two valid certificates for a transitional period of no more than 24 hours. In addition, the provisions of Chapter 3.3 apply.

4.6.4 Notification of the requester following a certificate renewal

The provisions of Chapter 4.3.2 apply.

4.6.5 Acceptance of re-certification

The provisions of Chapter 4.4.1 apply.

4.6.6 Publication of the certificate by the certification authority

The provisions of Chapter 4.4.2 apply.

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

The provisions of Chapter 4.4.3 apply.

4.7 Key renewal (re-key) of certificates

Renewal of keys for certificates ("re-key") is another form of request for a new certificate to be issued 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).

4.7.1 Reasons for key and certificate renewals

To increase the security aspect, key renewal can be useful, for example, to minimize possible risks for access to private keys when using keys stored in software (PKCS#12, .pfx files, software PSE) (Chapter 4.6.1).

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

The provisions of Chapter 4.6.2 apply.

4.7.3 Processing of re-key requests

The provisions of Chapters 3.3 and 4.6.3 apply.

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

The provisions of Chapter 4.3.2 apply.

4.7.5 Acceptance of a certificate renewal with new key material

The provisions of Chapter 4.4.1 apply.

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

The provisions of Chapter 4.4.2 apply.

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

The provisions of Chapter 4.4.3 apply.

4.8 Amendment of certificate data

4.8.1 Reasons for a certificate amendment

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, OU, CN, email, see also Chapter 3.1.1).

In the case of certificate data for certificates under the public CA, the contents of these certificates, in particular data of the certificate owner, are stored in the SAP HR, cIAM, Corporate AD, and TAdmin2 reference systems and the automatic workflows ensure that the cPKI receives a change request in the event of a change to certificate-relevant contents, which in any case leads to a new issue of certificates, see also Chapters 3.2 and 4.1.2.

4.8.2 Who may request a certificate change?

The provisions of Chapter 4.6.2 apply.

4.8.3 Certificate modification process

If the contents of a certificate change (see Chapter 3.1 et seq.), authentication to the cPKI is required again (see Chapter 3.2). The predecessor certificate must be revoked immediately.

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

The provisions of Chapter 4.3.2 apply.

4.8.5 Acceptance of a certificate renewal with changed certificate data

The provisions of Chapter 4.4.1 apply.

4.8.6 Publication by the certification authorities of a certificate with modified data

The provisions of Chapter 4.4.2 apply.

4.8.7 Notification of other instances regarding a certificate creation by the certification authority

The provisions of Chapter 4.4.3 apply.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for revoking an end-entity certificate

The following reasons require that the certificate be revoked by the certificate holder and published in the certificate revocation list (CRL):

- 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 (see also Acronyms and Definition of terms, Chapter A2 Compromise).
- The details in the certificate (except for unverified end-entity information) are no longer up to date, are invalid, or incorrect or do not correspond to the provisions of the naming convention (also refer to Chapters 3.1 et seq. and 4.8.1).
- The certified key (public key) or the cryptographic algorithms and parameters 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.
- There is unauthorized use or suspicion of unauthorized use of the key by unauthorized persons.
- Use and handling of the certificate that violates contractual provisions or this CP/CPS
- Revocation of the certificate to be renewed following the renewal process
- On expiry or termination of the contract between DTAG and the end entity, if there is no agreement to the contrary
- Legal provisions or court verdicts justify certificate revocation.
- The certificate is no longer required or the certificate owner expressly requests the revocation of the certificate.
- The certificate owner leaves the company and therefore no longer requires a certificate (temporary revocation takes place on the leaving date, final revocation takes place 30 days after the leaving date).

The Telekom Security Trust Centers or the DTAG Service Desk revokes end-entity certificates within 24 hours and publishes them in the certificate revocation list (CRL) and OCSP database if at least one of the following reasons exists:

- The certificate holder, key representative, or other responsible person calls the revocation service and orders the revocation. This requires authentication by means of a question and secret answer.
- The customer or a responsible contact person provides the information that the underlying certificate request was not authorized and that the authorization will not be given retroactively.
- The certificate holder, key representative requests in writing that the certification authority revokes the certificate.
- The certification authority has evidence that the private key of the certificate holder has been compromised or no longer meets the requirements of Chapters 6.1.5 and 6.1.6.
- The certificate authority is made aware of a proven or tried and tested method that could compromise the subscriber's private key or methods have been developed that could calculate the private key based on the public key or if there is clear evidence that the specific method failed to generate the private key.
- The certification authority becomes aware that a certificate holder has violated one or more of its essential obligations from the contract or the terms of use
- It becomes known that the private key has gone astray (e.g., lost, stolen, or handed over to a non-authorized person or delegated third party).

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

- the email address, an IP address or the domain name in the certificate is no longer permitted by law
- (e.g. a court or arbitrator has revoked the registration of a domain name or a power of attorney has expired.)
  - the right to use the domain name (FQDN), a corresponding license or service agreement between the domain name registrant and the applicant has been terminated,
  - the registrant of the domain name has not renewed the domain name.

- The certification authority becomes aware of one or more serious breaches of contract by the certificate holder.
- The certification authority becomes aware that the right to use an FQDN or an IP address has expired (e.g., a court forbids its use, a power of attorney expires, etc.).
- . The certification authority becomes aware that a wildcard certificate for the authentication of a misleading subordinate FQDN is being fraudulently used.
- The certification authority becomes aware of a relevant change in the certificate entries.
- The certification authority is informed that the certificate has not been issued in accordance with the rules as described in the requirements of the CA Browser Forum or the applicable CP or CPS.
- The certification authority determines that information in the certificate is incorrect, misleading or inaccurate.
- The certification authority ceases operations and has not made any arrangements for the revocation support to be continued by another CA in the event of cessation of operations.
- Proof of the CA's conformity with the CA Browser Forum has lost its validity. The need for revocation does not apply if the certification authority has taken precautions to ensure that the CRL and the OCSP service continue to be maintained and made available.
- The CA becomes aware of a possible compromise of the private key of a sub-CA that is used for issuing certificates.
- The CP and/or CPS of the issuing certification/registration body provides for revocation.
- From a technical point of view, the content or format of the certificate represents an unacceptable risk for application software manufacturers or relying parties, e.g., if the CA Browser Forum indicates such a risk and the certificate should therefore be revoked and replaced.
- There are statutory provisions, court judgments, or instructions from a supervisory authority.

- The right of the certification authority to issue certificates expires, is revoked or is terminated unless the certification authority has taken precautions to maintain the CRL/OCSP repository.

4.9.1.2 Reasons for revocation of a sub-CA certificate

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

- . The subordinate certification authority or an authorized representative requests in writing that the certificate be revoked.
- The authority that issued the certificate or an authorized person requests the certificate revocation in writing.
- . The subordinate certification authority notifies the issuing certification authority that the certificate request has not been authorized and that the approval has not been granted retroactively or that the powers of attorney or rights of use have in the meantime expired.
- The certified public key and/or the associated private key or the cryptographic algorithms and parameters used with it no longer meet current requirements.
- There is a case of misuse or the suspicion of misuse of the certificate by the certificate holder or other persons authorized to use the key.
- . It is pointed out to the issuing certification authority that the certificate was not issued in accordance with the applicable CP or CPS or that the use and handling of the certificate by the subordinate certification authority contradicts contractual regulations or the applicable CP/CPS,
- Legal provisions or court verdicts require certificate revocation.
- The issuing certification authority is informed that the private key of the subordinate certification authority has been compromised, lost, stolen or disclosed; or there is an urgent suspicion that this has happened.
- The issuing certification authority determines that one or more pieces of information contained in the certificate is incorrect or misleading
- The issuing certification authority or subordinate certification authority ceases to operate for any reason and has not taken any precautions to ensure that another certification authority supports the revocation of the certificate
- The right of the issuing certification authority or the subordinate certification authority to issue certificates expires, is revoked or is terminated, unless the issuing certification authority has taken precautions to maintain the CRL/OCSP repository
- Additional revocation events occur, as published by the issuing certification authority (CA) in their policy documentation (CP and/or CPS).

4.9.2 Who can request that a certificate be revoked?

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

- cIAM via the "Employee leave" IT process
- Authorized persons who are listed as the subject of the certificate
- Authorized persons from groups of persons and functions, legal persons, and devices (e.g., HR management employees)
- Authorized persons who act as key owners or are authorized to perform revocations
- Authorized persons from the Telekom Security Trust Center
- 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 cPKI service (e.g., Change Advisory Board of Telekom Security)

4.9.3 Revocation procedure

Persons authorized for revocation may request a certificate to be revoked by telephone seven days a week. A person is authenticated and authorized in a suitable way (e.g., by calling the help desk and identifying the caller by question/answer).

If the conditions for revocation are met, the revocation is carried out and the revoked certificate is included in the certificate revocation list (CRL).

The certificate owner is informed of the revocation in an appropriate manner (by email).

In addition, revocations are carried out by automated workflows via the WCF interface of the cPKI, for example, when an employee's employment relationship is terminated or the assignment of an external employee is terminated. For this purpose, HR or an authorized representative stores a leaving date in HR and cIAM. This date is forwarded to the cPKI life cycle management by means of a Suspend request via the WCF interface and the certificates are temporarily revoked on this leaving date. Four weeks after the leaving date, cIAM/TAdmin2 initiates the final revocation of the end-entity certificates through a revoke request.

4.9.3.1 Revocation types

Depending on the role and authorization, the subscribers to this PKI have various revocation types available to them seven days a week. Certificates can be revoked via

- the revocation service website of the Telekom Security Service Desk
- the WCF interface (requests from cIAM via TA2)
- the revocation services of the TSP (for devices only)
- REST interface (for devices (mobile devices) and user authentication certificate as well as the signature certificate on the mobile device from the internal certification authority)
- the life cycle management certificate of the cPKI for the revocation operators of the TSP revocation service

Table 16 presents the revocation types depending on the certificate types.

Type of certificate:	User website:	Revocation service website of the DTAG Service Desk:	WCF interface	For devices Revocation service Revocation service of the TSP	REST interface	cPKI Life Cycle Management for revocation operators of the TSP
Users	✗	✓	✓	✗	✓	✓
Devices (e.g., servers, routers/gateways)	✗	✗	✗	✓	✓	✗

Table 16: Revocation types

Regardless of the above revocation type, the Telekom Security Trust Center reserves the right to revoke certificates if at least one of the revocation reasons listed in Chapter 4.9.1.1 applies.

4.9.3.2 Revocation of end-entity certificates

A certificate revocation can be initiated seven days a week by a role or instance listed in Chapter 4.9.2. Here, it is sufficient that one of the revocation reasons listed in Chapter 4.9.1 applies.

In every case, the content of the certificate owner's Subject DN (e.g., email address or CID) is required in order to select the certificate to be revoked. In the case of end-entity certificates for email, authentication for revocation takes place at the Service Desk via the question and answer known only to the certificate owner.

The revocation is permanent. With the daily cycle of the CA system (Chapter 4.9.7), the certificate is published in the certificate revocation list (CRL). Following the revocation, the revocation information is immediately available via OCSP.

The certification authority reserves the right to revoke certificates if at least one of the reasons for revocation listed in Chapter 4.9.1 applies.

Telekom Security enables end entities, relying parties (e.g., software manufacturers), and other subscribers to report suspicions of compromised keys, certificate misuse, or other (attempted) fraud in relation to certificates, see also Chapter 3.4.

Telekom Security begins investigating within 24 hours of receiving notification of suspected misuse in order to determine whether further measures are to be taken (e.g., revocation).

Within these 24 hours, a first report of the facts and the results of the analysis will be prepared and given as feedback to the certificate owner and the person who reported the problem. Having inspected the facts and environmental parameters, the certification authority will discuss the analysis results with the certificate holder/delegate or the reporting person and decide to what extent a certificate revocation will be necessary

In this context, the revocation date is determined. The period between receipt of the certificate problem report or revocation request and the published revocation must not exceed the time limits for revocation required in Chapter 4.9.1.

The further procedure is determined based on the following criteria:

- What exactly is the problem?
- Are there already other cases of misuse for this certificate or this customer?
- Who submitted the suspicion of misuse (for example, report by official authority in connection with criminal proceedings or illegal activities)?
- Have legal provisions been violated?

The following factors must be considered when setting the revocation date:

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

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

4.9.3.3 Revocation of user certificates

The following role owners and websites or interfaces are involved in revoking user certificates (Chapter 4.9.3):

- By the user via the DTAG Service Desk
- By cIAM via TAdmin2 and the interface to the cPKI

- By revocation operators of the TSP

4.9.3.4 Revocation of device certificates

The following role owners and websites or interfaces are involved in revoking device certificates (Chapter 4.9.3):

- By the device administrator via the TSP revocation service for device certificates
- Optional: REST interface
- By the revocation operator of the TSP revocation service

4.9.3.5 Revocation of certificates to support PKI operation

The web server and OCSP certificates described in Chapter 1.3.1.3.1 and 1.3.1.3.2 are used to support PKI operation of the cPKI.

Requests for these certificate revocations are reported to the TSP via the DTAG Service Desk.

4.9.3.6 Revocation of external web server certificates

Telekom Security undertakes to revoke the cPKI website web server certificate (Chapter 1.3.1.3.1) as soon as a compromised key is suspected. 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 and 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.

4.9.3.7 Revocation of the OCSP responder certificate

Telekom Security undertakes to revoke the OCSP responder certificate (Chapter 7.3 et seq.) as soon as a compromised key is suspected. 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 and is announced via the certificate revocation list (CRL). A revoked web server certificate is replaced with a new one immediately.

4.9.3.8 Revocation of sub-CA certificates

Telekom Security undertakes to revoke the sub-CA certificate (Chapter 1.3.1.2) as soon as a compromised key is suspected or provisions require this.

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

4.9.4 Deadlines for a revocation order

4.9.4.1 Service Desk of the Trust Centers

After the Trust Center Service Desk receives a complete revocation order (only in the event of certificate misuse), Telekom Security revokes the end-entity certificates within 24 hours and publishes them in the certificate revocation list (CRL) and the OCSP database.

4.9.4.2 DTAG Service Desk

The DTAG Service Desk (delegated third party) is responsible for ensuring that revocation deadlines are adhered to. As soon as a revocation reason in accordance with Chapter 4.9.1 applies to end-entity certificates, the revocation order must be submitted as quickly as possible within an economically reasonable period by the end entity, key owner, or person authorized for revocations.

4.9.5 Certification authority's processing deadlines for revocation orders

Revocation by the end entity, key owner, or person authorized for revocations takes place by telephone using the valid telephone number of the DTAG Service Desk, which is available daily from 8:00 a.m. to 6:00 p.m. including weekends and will trigger the revocation process immediately after receipt of the revocation request. The corresponding interfaces (WCF and REST) are available to the connected systems on a 24/7 basis. The revocation process is passed on directly to the connected systems. The OCSP service that accesses these systems therefore has 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 cPKI's directory service (see Chapter 2.2).

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

Telekom Security ensures that the revoked certificate is included in at least the next CRL 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 Chapter 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 Trust Center can manually generate the certificate revocation list (CRL).

All revoked CA certificates (no root CA certificates) that are issued by the root certification authority (root CA) in question are published in the revocation lists for certification authorities (CARL). Figure 1 and Figure 6 present the root and subordinated certification authorities (sub-CAs) in the form of a graph. CARLs are updated every six months or depending on events, and publication takes place via the corresponding directory service.

Revoked certificates that are outside the validity period will be removed from the revocation list, but Telekom Security will ensure that revoked certificates are at least included in the next CRL after the certificate expires.

The OCSP data source (repository) is updated after fifteen (15) minutes at the latest. The OCSP responses are valid for a maximum of five (5) days.

The OCSP status information update is event-based, i.e., a revocation event at the CA will also be online in the OCSP within a period of < 15 minutes. OCSP and CRL are both based on the data of the respective CA, therefore the consistency of the different information services is ensured at the time the CRLs are created.

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 generation is a few minutes.

4.9.9 Online availability of revocation/status information

In addition to the revocation information via the CRL and CARL (Chapters 2.3 and 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 Chapter 7.1.2.9).

4.9.10 Requirements for an online checking process

Relying 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 OCSP responses from end-user certificates issued by cPKI comply with the requirements of RFC 6960.

The OSCP responder supports the HTTP GET method as described in RFC 6960 and/or RFC 5019.

The OCSP replies to requests for serial numbers that have not been issued with "unknown". Furthermore, the OCSP responder is monitored for requests for "unused" certificate serial numbers.

The Root CA updates the OCSP information at least every 6 months. In the event of a revocation of a subordinate certification authority, the OCSP information is updated within 24 hours after revocation.

4.9.11 Other available forms of publishing revocation information

Depending on the certificate type, the certificate holder, requester, deputy, or another instance is informed that the certificate has been revoked (revoke notification).

4.9.12 Special requirements for compromised private keys

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

4.9.13 Circumstances of a suspension

Reasons for the suspension of certificates may be:

- Temporary non-availability of a certificate carrier medium (e.g., forgotten MyCard)
- Longer planned absence of employees
- Suspicion of unauthorized use of the certificate carrier medium
- Execution of the "Employee Leave" process in the cIAM system, whereupon the user will be suspended for 30 days before a revoke order for final revocation is placed

4.9.14 Who can request that a certificate be suspended?

- cIAM via TAdmin2 through the "Employee leave" IT process
- Authorized persons who are listed as the subject of the certificate
- Authorized persons from groups of persons and functions, legal persons, and devices (e.g., HR management employees)
- Authorized persons who act as key owners or are authorized to perform revocations
- Authorized persons from the Telekom Security Trust Center

4.9.15 Suspension procedure

Authorized persons can request the temporary revocation of a certificate by calling the DTAG Service Desk. A person is authenticated and authorized in an appropriate manner.

If the conditions for suspension are met, a temporary revocation is carried out and the revoked certificate is included in the revocation information. With the daily cycle of the CA system (Chapter 4.9.7), the certificate is published in the certificate revocation list (CRL). Following the revocation, the revocation information is immediately available via OCSP.

The certificate owner is informed of the suspension by email.

Irrespective of this, the Telekom Security Trust Center as operator of the cPKI reserves the right to temporarily or permanently revoke certificates if at least one of the reasons listed in Chapters 4.9.1 and 4.9.13 is present.

4.9.16 Limitation of the suspension period.

The maximum suspension period of a suspension via the automated registration authority (cIAM) is 30 calendar days, which can be shortened depending on the certificate validity. If the validity of the certificate has not expired, cIAM will be instructed by TAdmin2 to permanently revoke it after 30 calendar days.

Suspensions via the Service Desk do not automatically lead to the permanent revocation of the certificates after a certain period of time. In this case, the validity of the suspension is limited by the validity of the certificate.

4.10 Status information services of certificates

The status of end-entity certificates is available directly via the OCSP service (Chapters 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 (sub-CA) that issued the end-entity certificate in question Figure 1 and Figure 6 present 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 term) and
  - the certificate is not revoked
- revoked means:
  - it is an issuer of the PKI service and
  - the certificate is valid (within the certificate term) and
  - the certificate has been revoked
- unknown means:
  - the certificate is invalid (outside the certificate 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 Chapter 7.3.2.

The certificate revocation lists (CRL) issued by the cPKI meet the specifications of RFC 5280. The respective sub-CA issues and publishes the certificate revocation lists (CRL), while the respective root CA issues the revocation lists for certification authorities (CARL) and publishes them on the LDAP directory service. Figure 1 and Figure 6 present the

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

Revoked certificates are removed from the certificate revocation list (CRL) only once their validity has expired.

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, or 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/cessation of operations

In the event of termination of the contract by the customer or Telekom Security as operator of the cPKI, the provided certificate types will be deactivated immediately. As a consequence, it is no longer possible to request new end-entity certificates or renewals. In addition, certificates are revoked after the termination date and lose their validity.
All functions for logging into the website in question, issuing of new certificates as well as renewal and revocation of certificates are prevented; however, certificate validation via the certificate revocation list and OCSP is still supported.

In the event of cessation of operation of the cPKI, the following measures are taken:

- Notification of all certificate holders and relying parties with a lead time of at least three months
- Revocation of all user certificates and the certificates of the certification authorities
- Destruction of the private keys of the certification authorities
- Publication of the relevant CA and root CA revocation lists

However, a separate transitional arrangement can be additionally made in writing in individual contracts.

4.12 Key deposit and recovery

The key pairs of the intermediate certification authorities (sub-CA) (see Figure 1 and Figure 6) used in the scope of the "cPKI" 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 backup purposes so that qualified and security-checked staff (trusted role) at the Trust Center can recover and maintain the service. Key deposit (escrow) at third parties (e.g., trustee, notary) is not planned.

In addition, a key backup is performed in the CA database in the Trust Center's operating environment for end-entity encryption certificates. Access is secured with a key from the HSM.

4.12.1 Guidelines and practices for key deposit and recovery

Key recovery is tied to the consent of the certificate owner. The recovery of encryption keys or certificates is limited to provision for the certificate owners themselves (MyCard or mobile devices) and for deputies expressly authorized by the certificate owners (MyCard). Orders for the recovery of encryption keys are only authorized after prior authentication and authorization check of the requester.

Key recovery to third parties without the consent of the certificate owner is tied to the consent of the responsible bodies in the Group for IT security, data privacy, and HR personnel representation in accordance with the German Works Constitution Act (*Betriebsverfassungsgesetz – BetrVG*). The consent of all the bodies mentioned is required for this purpose.

See chapter 4.1.2.2 for procedures and policies in the context of recovery processes.

The cPKI is operated in the certified high-security environment of the Telekom Security Trust Center. All functions and processes are subject to strict security measures, which are documented in an operating concept (not publicly available).

4.12.2 Session key encapsulation and guidelines for recovery

No Stipulation.

5 BUILDING, ADMINISTRATION AND OPERATION CHECKS

The Telekom Security Trust Center 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 Telekom Security Trust Center.

The physical, organizational, and personnel-related security measures applied are defined in the Trust Center's security framework concept [SRK TC], 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 as well as the Operating Guidelines for the Trust Center.

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

- Risk assessment in the framework of ISMS
- Information security policies
- 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 operates a trust center consisting of two fully redundant data centers (Twin Core).

The Trust 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. Particular security requirements apply here.

5.1.3 Power supply and air conditioning

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

floating particles. The fresh air intake is continuously checked for aggressive gases. In 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 whose performance corresponds to the full load power consumption 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 data 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 documented in the security framework concept [SRK TC] and the security concept of the cPKI [Siko cPKI] and are implemented by the operating concept of the Trust Center. The relevant requirements from [ETSI EN TSP] Chapter 7.4 b, c, d, e have been implemented.

5.2.1 Trusted roles

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

- The validation of information in certificate orders
- The acceptance, rejection, or other processing of certificate requests, revocation requests, or renewal requests
- The granting or withdrawal of certificates, including personnel who have data access and physical access to database systems
- The way informational orders are dealt with by end entities

Trusted persons are in particular:

- Trust Center staff (e.g., system administration)
- Employees of cryptography departments
- Security personnel
- Responsible technical personnel
- Managerial staff responsible for managing the trusted infrastructure

The above-mentioned trusted persons must meet the requirements set out in this document (see Chapter 5.3.1).

These persons accept their assigned role(s) by means of a written confirmation (e.g. by e-mail). This confirmation must be archived for at least 7 (seven) years.

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

5.2.2 Number of involved persons per task

The operational maintenance of the certification authority and directory service is carried out by expert and trusted employees.

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 Service Desk, registrar or Trust Center operator rights for the purpose of resolving the fault.

5.2.3 Identification and authentication of each 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 Chapter 5.3.2).

Telekom Security ensures that employees have achieved trusted 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 cPKI 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 Customer employees who authenticate or identify persons

The customer must ensure that only trusted persons perform activities for the authentication of persons, groups or function groups. This applies in particular to HR, employees of the cIAM database, which is in breach of contract, and agents, who create external employees in the HR systems

5.2.4 Roles that require a separation of duties

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

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

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. In the Trust Center, the deployment of qualified trained personnel is mandatory. The staff measures are documented in the security framework concept [SRK TC] and in the security concept of the cPKI [Siko cPKI].

The personnel are not subject to any cost pressure or quantity structure or other constraints whose observance would possibly compete with the quality requirements in reviewing request documents.

5.3.1 Qualifications, experience, and clearance requirements

5.3.1.1 Telekom Security employees

For the operation of the PKI services described in Chapter 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 police certificate of good conduct must be submitted to Telekom Security at regular intervals.

5.3.1.2 DTAG employees who authenticate or identify persons

The customer must ensure that the deployed personnel are able to perform the tasks of authenticating or identifying persons in terms of expertise and reliability. It must also be possible to provide evidence of the qualifications and reliability check to auditors (see Chapter 1.3.2.1).

5.3.2 Security check

5.3.2.1 Telekom Security employees

Before an employee starts work in a trusted 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 trusted person being rejected can include

- The candidate or trusted person providing false details
- Particularly negative or unreliable employment references
- 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 trusted positions having their employment offer withdrawn or to trusted persons being dismissed.

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

5.3.2.2 DTAG employees who authenticate or identify persons

No Stipulation

5.3.3 Education and training requirements

5.3.3.1 Telekom Security employees

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 toward the individual work areas and include, for example:

- Advanced PKI knowledge
- Procedures in accordance with ITIL
- Data and telecommunications privacy
- Information protection
- Access protection
- Anti-corruption
- Data protection
- Telekom Security security and operating policies and procedures
- Use and operation of the hardware and software in use
- Reporting and handling of faults and compromises
- Procedures for disaster recovery and business continuity

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

- Guidelines, procedures, and current developments regarding validation methods
- Contents and particularly relevant amendments to this CP/CPS

- Relevant requirements and specifications from the [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 DTAG employees who authenticate or identify persons

Telekom Security provides the customer with appropriate training documents that specify the functions, processes, and supporting documentation.

The customer is obliged to train new 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.

5.3.4 Follow-up training intervals and requirements

5.3.4.1 Telekom Security employees

Telekom Security staff attend refresher courses and further training courses to the necessary extent and at the required intervals. The requirements are reviewed annually and incorporated into the training program.

5.3.4.2 DTAG employees who authenticate or identify persons

In the event that Telekom Security provides new training documents that contain relevant training topics, the customer must hold a special training session and adapt procedural instructions. 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 Telekom Security employees

Telekom Security reserves the right to punish unauthorized activities or other violations of this CP/CPS and the Subscriber Agreement/Terms of Use 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 DTAG employees who authenticate or identify persons

It is up to the customer to impose penalties for any infringements.

This person responsible will be held responsible in the event of tortious acts or criminal offenses. This can result in disciplinary action being taken under labor law as well as criminal law.

5.3.7 Requirements for independent contractors

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

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

5.3.8 Documentation supplied to personnel

5.3.8.1 Telekom Security employees

Telekom Security provides its employees with all the requisite documents (training documents, procedural instructions) that they need in order to be able to fulfill their professional duties appropriately.

5.3.8.2 DTAG employees who authenticate or identify persons

Telekom Security provides appropriate training documents that show the functions, processes, and accompanying documentation relating to the authentication and identification of persons.

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] Chapter 7.10 are implemented.

5.4.1 Type of events recorded

In general, 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 life cycle management of CA key pairs or CA systems, the Telekom Security Trust Center logs at least the following events for the cPKI:

- Generation, destruction, storage, backup, recovery, and archiving of the key pair or parts of the key pair
- Events in the life-cycle management of cryptographic devices (e.g., HSM) and the CA software used

5.4.1.2 EE and CA certificates

For the life cycle management of EE and CA certificates and their validation, the Telekom Security Trust Center logs at least the following events for the cPKI:

- Initial request and revocation of certificates
- Request for renewal with and without a change of key (renewal and re-key)
- All activities relating to the verification of information
- The event, the date/time and phone number of phone calls relating to the verification, and the name of the contact person are documented in DTAG's SM9 ticket system.
- Acceptance or rejection of certificate orders
- Issue of a certificate
- Generation of revocation lists (CRL) and OCSP entries

5.4.1.3 Other security-related events

In addition, the Telekom Security Trust Center logs all security-related events for operation of the cPKI 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
- Entering and exiting of Trust Center facilities
- Results of network checks (vulnerability scans)
- Starting and shutting down of the systems
- Start and end of the logging process

5.4.2 Frequency of processing 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 cPKI.

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

5.4.3 Retention period for audit log

Audit logs/logging files are archived after processing in accordance with Chapter 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 capture system

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 Telekom Security employees.

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 Vulnerability assessments

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

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

5.5 Data archiving

5.5.1 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 PSE
- All audit/event logging files recorded in accordance with Chapter 5.4
- Central key backups of soft PSEs

5.5.2 Retention period for archived data

The following records and retention periods are stipulated:

- Order documents, in particular information regarding certificate requests, their validation, as well as the resulting certificates and completed revocations are retained for seven (7) years after the certificate validity expires.
- Audit and event logging data is archived in accordance with the legal provisions.

5.5.3 Protection of archives

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

5.5.4 Archive backup procedures

A full backup of the electronic data 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 CP/CPS.

5.5.5 Requirements for time-stamping of datasets of datasets

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

5.5.6 Archiving system (internal/external)

Telekom Security only uses internal archiving systems.

5.5.7 Procedures to obtain and verify archive information

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

5.6 Key change

Certificates become invalid once the validity period has expired.

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

- The key material is compromised
- The cryptographic algorithm needs to be changed
- The key size needs to be changed
- The certificate content is changed

Any key change for end-entity certificates is the customer's responsibility. New certificates and their fingerprints are published (see Chapter 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 Chapter 2.3).

Telekom Security immediately informs the DTAG-internal customer 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 still 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

Telekom Security has established an IT service management in accordance with ITIL and ISMS processes that processes faults 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 cPKI has a service level agreement (SLA) in which the incident process and the service chain are described in detail.

Incidents are submitted by the end entity via the contacts defined in the service level agreement (SLA) and then processed as part of service management.

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

The specialist department informs the Service Desk about the processing status in accordance with the incident class so that the Service Desk can provide the relevant information.

If required, the customer is informed as quickly as possible 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 DTAG security/Telekom Security department. The event entails a corresponding escalation, incident investigation, incident response, and finally incident resolution. Disaster recovery is carried out depending on the incident classification.

All hardware and software that is required for provision of the cPKI is available as an asset and 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 key of a CA or root CA is compromised, the incident is immediately investigated and assessed and the necessary steps are taken. The client will be informed of the possible compromise in writing (see chapter 2.2). 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 concept. New certificates and their fingerprints must be published (see Chapter 2.2).

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 disasters (natural disasters or disasters of human origin) and to restore the availability of critical business processes as quickly as possible. This also includes all Trust Center processes, components, systems, and services. This plan is reviewed at least once a year, tested, and updated accordingly, so as to be able to respond in a targeted and structured manner in the case of a disaster.

The emergency plan contains at least the following information:

- The necessary criteria for activating the plan
- Possible emergency measures (depending on the situation)
- Fallback procedures
- Restart procedure
- Procedure for regular maintenance, updating, and further development
- Awareness raising measures
- Training requirements for the affected personnel
- The responsibilities of the individuals (role description and assignment)
- Recovery time objective (RTO)
- Regular execution of the emergency plans for test purposes
- A procedure for maintenance or timely restoration of the cPKI business activities following an interruption or failure of critical business processes
- An obligation to back up or keep critical cryptographic devices and information at a different location
- Specification of the maximum tolerable downtime (MTD) and corresponding restoration times
- Frequency at which backups are created of critical business information and the software used including its configuration

- Physical distance between the backup locations or facilities and the cPKI main office or the Trust Center data center
- Procedure for securing the business premises and facilities as well as possible following a disaster (emergency operation) until secured normal operation in line with the requirements is restored

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

Key material of the end entity issued on MyCards (smartcards) is not covered under this emergency plan.

5.8 Termination of operation of a certification or registration authority

Only Telekom Security can announce the cessation of operations at the Telekom Security certification authority (Chapter 1.3.1 et seq.) or of the automated as well as internal registration authority (Chapter 1.3.2).

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

- Notification of the DTAG-internal customer, end entities, and relying parties about the planned cessation of the service
- Continuation of revocation functions, including the regular generation of revocation lists, retrieval of certificate status information, and Service Desk functions
- Revocation of issued CA certificates
- Any transitional regulations required for a successor CA
- 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 parties, the DTAG-internal customer, and Telekom Security) as early as possible.

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

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

6 TECHNICAL SECURITY CONTROLS

The technical security measures are defined in a security framework concept of the Trust Center [SRK TC] and the security concept of the cPKI [Siko cPKI], the effectiveness of which is proven on the basis of a threat analysis. The requirements under [ETSI EN TSP] Chapter 7.5 are implemented.

6.1 Generation and installation of key pairs

6.1.1 Generation of key pairs (CA)

All key pairs for CA certificates are generated and stored by trained and trusted specialist staff in a low-radiation room on a security-checked hardware security module (FIPS 140-2/level 3 evaluated) in 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).

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

The key pair for a public root certificate and the associated certificate for a sub-CA is generated on an offline CA and the assigned cryptographic hardware module (HSM) under the supervision of an independent and qualified auditor.

The key pair for a sub-CA is generated on the cryptographic hardware module (HSM) assigned to the cPKI in online operation. The corresponding certificate of the intermediate certification authority (sub-CA) 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 module (HSM) (including 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 sealed against opening and replacement. The integrity of the seal is checked and documented each time the offline CA is used.

Key pairs for issued signature and authentication certificates of end entities in terms of natural persons are based on the MyCard as the carrier medium. They are generated by the manufacturer of the MyCard in a special, shielded environment, securely stored on the card by the TCOS chip card operating system and delivered with a special transport seal.

Key pairs for end-entity encryption certificates in terms of natural persons are generated centrally by the cPKI in a specially protected environment using Hardware Security Modules (HSM) and stored securely on the MyCard during personalization.

The key pair for the signature and encryption certificate of a function and group mailbox is a single key. This is generated by the cPKI centrally in a specially protected environment using hardware security modules (HSM) and saved securely on the MyCard or made available as soft PSE for applications and mail gateways.

6.1.2 Assignment of public keys to end entities

If a MyCard is used, the keys applied to the card during production are used for signature and authentication. These private keys are not transferred outside a MyCard. Encryption keys are generated by the server and securely transferred to the smartcard via a TLS-encrypted connection after prior authentication of the end entity by the offered login procedures and entry of an individual one-time password.

In the case of soft PSE, a secure password is assigned to the soft PSE to protect the private key. This also applies to key material (soft PSE) that was generated as part of a key backup.

The retrieval of keys and certificates that were created as part of a "central key backup" can:

- search for the key material and certificates and download them to a smart card (MyCard) via an encrypted TLS/SSL connection through the manual registration authority of the Trust Center and in compliance with the procedure described in Chapter 4.1.2.2.
- be installed on a smartcard (MyCard) via the automated registration authority as a key backup when creating a new smartcard via an encrypted TLS/SSL connection.
- be transferred to the Enterprise Mobile Device Management (EMM) operated by DTAG via an encrypted TLS/SSL connection as part of the provision of key material for mobile devices via the automated registration authority. The customer is responsible for storing, backing up, dispatching, and installing the keys in the EMM and on the mobile devices.

In the event that the end entity generates the key pair itself 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 certificate issuers

Following successful authentication, all end entities and registrars submit the public key to be certified to the cPKI 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, publication of the certification authority's public keys

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 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 of workplace systems. In the case of managed DTAG workplace systems, this is done by means of GPO or automated software distribution.

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 by the application for certificate validation or has to be subsequently installed in the certificate stores in question.

All root CA certificates and sub-CA certificates can be downloaded from the public website https://corporate-pki.telekom.de/ and from the cPKI 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 entities) issued by a public root certification authority (including this certificate itself) fulfilled the requirements of the Baseline Requirements [CAB-BR] in the current version at the time of release and publication.

All certificates (root and intermediate certification authorities, end entities) have an RSA key length of at least 2,048 bits.

6.1.6 Generating the parameters of public keys and quality control

The public keys submitted with the certificate request are checked for the following quality parameters:

- The RSA encryption method was used for generation
- The minimum key length for RSA keys is 2,048 bits
- The exponent of the public key is e >1 and odd
- SHA-256 is permitted as a hash algorithm

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

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

- For key usage, see Chapter 7.1.2.1.
- For extended key usage, see Chapter 7.1.2.5.

6.2 Protection of private keys and technical checks of cryptographic modules

The Telekom Security Trust Center has implemented physical, organizational, and procedural mechanisms to ensure the security of CA and root CA keys. This also applies to the key material that is stored for the customer as part of "central key archiving."

As a rule, the use of private keys is always protected by possession (PSE, token) and knowledge (PIN) of the authorized role bearer.

In the case of private keys for certification authorities, they are stored securely on an HSM in the Trust Center and protected against unauthorized use.

End entities are obliged to take all necessary precautions to prevent loss, disclosure, or unauthorized use of their 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 Chapter 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 control (m of n) for private keys

Telekom Security has implemented technical, organizational, and procedural mechanisms that require the participation of several trusted and trained persons of the Telekom Security Trust Center 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.

The storage of end-entity keys is described in Chapter 4.12 et seq.

6.2.4 Private key backup

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

In addition, backups of the private CA keys for the respective cPKI 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 recovery may only be performed within the high security zone of the Telekom Security Trust Center.

Under the existing contract and as part of the agreed services, the Telekom Security Trust Center will archive the private key. Information regarding backing up private end-entity keys is described in Chapters 4.12 et seq. and 6.2.3.

The recovery of key material from end entities is permitted in the following situations:

- If the end entity or key owner agrees to the recovery
- In the case of automatic key recovery as part of the issue of a new smartcard (MyCard)
- If is the provision of the key material for Enterprise Mobility Management (EMM)

If this permission is not granted, the customer may still have the recovery 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
- Organizational policies of DTAG
- Recovery was requested by an authorized DTAG office in compliance with legal data protection requirements (GDPR) and the framework conditions of the Works Constitution Act (*Betriebsverfassungsgesetz – BetrVG*).

6.2.4.1 Backup and recovery of the encryption key using enrollment software

The PSE for the current encryption certificate and existing key history certificates is securely transferred to the MyCard when the MyCard is personalized using suitable enrollment software

6.2.4.2 Backup and recovery of soft PSEs via the operating system

The keys cannot be exported.

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 Backup and recovery of soft PSEs via the Trust Center

With central key backup by the Telekom Security Trust Center, the password-protected soft PSE and the corresponding password file (contains the password of the soft PSE) are stored separately in encrypted form. Two separate roles are required for recovery.

6.2.5 Archiving of private keys

If the validity period of the certificates of the intermediate certification authority (sub-CA) or the OCSP service is exceeded, the key material of the respective certificate will be destroyed. They are not archived.

The Telekom Security Trust Center archives copies of end entities' private keys

- that the CA system generated as encryption keys as part of a smartcard personalization of triple-key certificates and that are to be accessible at a later time in connection with the central key backup

6.2.6 Transfer of private keys in or by a cryptographic module

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

When a certificate of an intermediate certification authority (sub-CA) is renewed, the key pair is retained; however, in the case of operational or security-related requirements, a new key pair can be generated on the connected HSM and securely stored there. The public key to be certified, with the data of the Subject DN, is transferred securely in electronic form (PKCS#10-Request) to the offline CA, which generates the sub-CA certificate. The sub-CA certificate is then securely transferred to the hardware module (HSM) and assigned to the private key.

Private keys cannot be exported for smartcards that already contain keys or that generate keys themselves. During a key backup, 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 Telekom Security Trust Center saves CA keys in a secure form on cryptographic hardware modules (HSM) that are evaluated in accordance with FIPS 140-2/level 3.

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

6.2.8 Method for activating private keys

All end entities (including 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 CP/CPS.

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

6.2.8.1 Private keys of end entities

The end entity must comply with the following provisions to protect the private key:

- A password or a PIN must be set (in accordance with Chapter 6.4.1) or a similar security measure must be implemented in order to authenticate the end entity 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 to device certificates.
- Economically suitable measures must be taken to physically protect the PC workplace or device to reliably prevent use of the workplace/device in combination with the use of the corresponding private key without the permission of the end entity or an 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 Private keys of registrars

No Stipulation as no separate key material is issued to registrars – keys and certificates issued to end entities are used. The assignment of roles takes place in the life cycle management of the cPKI.

6.2.8.3 Private keys of root and intermediate certification authorities

Key material for CA and root CA certificates is activated accordingly by the authorized persons and stored on cryptographic hardware modules (HSM) (Chapters 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 (Chapter 4.9.3).

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 Private keys of Trust Center administrators and operators

No Stipulation as no separate key material is issued to Trust Center administrators and operators – keys and certificates issued to end entities are used.

The Trust Center administrator or operator must take appropriate measures to physically protect the administrator or operator workplace from unauthorized access in order to protect the private key.

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 end-entity keys is the responsibility of the end entity.

Deactivating private keys that were created as part of a central key backup requires a regulation in the individual contract.

6.2.10 Method for destroying private keys

The destruction of CA keys requires the participation of several trusted persons (trusted roles) from the Trust Center. After the key has been destroyed, it needs to be ensured that there are no residual fragments that 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 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 and archiving 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 17 shows the maximum validity periods of the certificates involved in the hierarchy that were issued at the time this CP/CPS entered 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.

Type of certificate	Period of validity
T-TeleSec GlobalRoot Class 2 (public root CA)	25 years
Deutsche Telekom AG Issuing CA 01	8 years
Deutsche Telekom AG secure email CA	10 years
Deutsche Telekom AG secure email CA E02	10 years
Deutsche Telekom AG secure email CA E03	10 years
Deutsche Telekom Internal Root CA 1 (internal root CA)	20 years
Deutsche Telekom Internal Root CA 2 (internal root CA)	20 years
Deutsche Telekom AG Issuing CA 01	8 years
Deutsche Telekom AG Issuing CA 02	8 years
Deutsche Telekom AG Issuing CA 03	16 years
Deutsche Telekom AG mobile device CA	10 years
Deutsche Telekom AG **infrastructure** CA	10 years
Deutsche Telekom AG **authentication** CA	10 years
Deutsche Telekom AG internal secure email CA	10 years
End-entity certificates:	12 or 36 months by default (or 1 or 3 years)
Deutsche Telekom AG Employee Encryption	3 years
Deutsche Telekom AG Employee Signature	3 years
Deutsche Telekom AG Employee Authentication	3 years
Deutsche Telekom AG External Workforce Encryption	1 year
Deutsche Telekom AG External Workforce Signature	1 year
Deutsche Telekom AG External Workforce Authentication	1 year
Deutsche Telekom AG Fuctionalmailboxes Signature und Encryption	2 year
Deutsche Telekom AG robot Encryption	1 year
Deutsche Telekom AG robot Signature	1 year
Deutsche Telekom robot Authentication	1 year

Type of certificate	Period of validity
Deutsche Telekom AG Function and Group Account Encryption	1 year
Deutsche Telekom AG Function and Group Account Signature	1 year
Deutsche Telekom Function and Group Account Authentication	1 year
Device certificates:	24, 36, or 72 months by default (or 2, 3, or 6 years); a different term can be administered by agreement
CodeSigning certificates	3 years
OCSP-Signer <Root-CA> certificates	6 months
OCSP-Signer <Sub-CA> certificates	1 months

Table 17: Validity periods of certificates

6.4 Activation data

Certificates of certificate owners (end entities)

The activation of certificates is basically linked to knowledge (one-time secret and/or PIN) and the possession of a key carrier medium (smartcard or software PSE).

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 in accordance with the requirements described in Chapter 6.2.2 of this CP/CPS and the "key ceremony" document. The generation and distribution of secret shares is logged.

6.4.1.2 End entity

For certificates from certificate owners (end entities), one-time secrets are generated by the PKI and sent to the subscriber's email address stored in the certificate request.

A PIN (MyCard or software PSE) is issued during activation by the respective certificate owner.

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, including special characters such as !, ?; /, etc.
- Lower/upper case letters
- No common terms that can be found in dictionaries
- No user names

The following PIN policy is stored for the issue of the smartcard (MyCard) PIN, a deviation from this is technically prevented by the cPKI.

- PIN length: 6
- Permitted characters: 0-9
- Maximum number of repeated characters: = 2
  This setting prevents PINs with adjacent, repetitive characters from being used. Example: 111222 as PIN is prevented

- Maximum number of sorted characters: = 3
  This setting prevents PINs with adjacent consecutive or sequential characters (e.g., 1234567890) from being used.

6.4.2 Protection of the 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 and OCSP certificates.

6.4.2.2 End entity

The end entity undertakes to protect the secret shares (OTP, PIN, passwords) for the activation of the private end-entity key.

To increase security, Telekom Security recommends regularly changing the PIN for end-entity certificates.

The customer is responsible for implementing the protection.

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 username 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 (Chapter 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 trusted 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 framework concept [SRK TC]. The requirements under [ETSI EN 319 401] Chapter 7.4 are implemented.

The systems for development, testing (cPKI CAST1 and CAST2), and production (cPKI-PROD) 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 requirements for technical security measures

Telekom Security ensures that the management of CA systems is protected against unauthorized third-party access. The CA components must be 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, multi-factor authentication) 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 trusted operating personnel.

The security measures include:

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

6.5.2 Assessment of computer security

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

6.6 Technical controls of the life cycle

6.6.1 System development controls

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 (cPKI CAST1 or cPKI CAST2).

Installation on Telekom Security' live system (cPKI-PROD) in Telekom Security' georedundant data center only takes place after successful testing and acceptance of 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 owners [Siko cPKI]. Administration of other IT systems (not PKI systems) via this network is not permitted.

6.6.2 Security management checks

Telekom Security has implemented mechanisms and/or guidelines to be able to control and monitor the configuration of the cPKI systems in the Trust Center. 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 Life cycle security controls

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 controls

The following network security measures were implemented:

- The networks of the certification service are secured by 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, or 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 in accordance with the protection requirements of the systems and components and are separated from each other by firewalls.
- Only the directory services, OCSP responder, and CRL are accessed from the internet. Furthermore, information on the cPKI and the CP/CPS is stored on a separate website and can be accessed from the internet.
  Access from the internet to CAs, certificate management, or registration authorities is not possible.
- Vulnerability scans are performed at regular intervals. Further details can be found in Chapter 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 immediately.
  - The management of user access rights for all users is based on a roles and rights concept.
  - An account for the end entities is created in the certificate life cycle management of the cPKI by means of the first order over the automatic registration authority. End entities must authenticate themselves for this account by means of their Active Directory accounts and through two-factor authentication at the web portal of the cPKI.
  - Certificates can only be issued if an order has been previously placed for the end entity via the RA and verified as valid.
  - Administrators and support staff must always log in using two-factor authentication (smartcard with valid authentication certificate) and are assigned their rights depending on their role.

- Service accounts are stored in a password safe and are only accessible to administrators with the appropriate roles using smart card authentication.
- Regular checks are carried out to establish whether administrative or service accounts are still needed. If accounts are identified that are no longer needed, they are immediately deleted, deactivated, or the rights of the users are withdrawn.

- The Trust Center is connected georedundant with both the cPKI infrastructure and the internet via separate feeds. Transition from the cPKI infrastructure to the internet or vice versa is prevented by several firewall systems. The same applies to transitions to the internet for the provision of directory services and repositories.

The requirements under [ETSI EN 319 401] Chapter 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 Chapter 5.5.5). A cryptographic time stamp is not used.

7 CERTIFICATE LIST, REVOCATION LIST, AND OCSP PROFILES

7.1 Certificate profiles

Depending on the registration model (Chapter 4.2), the certificate request (see Chapter 4.1 et seq.) is sent in electronic form via technical interfaces.

Due to the requesting procedure or the interface, a certificate request is already assigned to the relevant certificate profile (e.g., user, external, internal, or server). Table 18 assigns the certificate types provided by cPKI to the respective certificate templates.

Certificate types:	Certificate template:	Use:
Users (natural persons, pseudonyms, robots, function and group accounts)	Single key (mobile devices only)	Sig
	Triple key	Sig
		Enc
		LogOn
Group, function, role certificates	Single key	Sig/Enc
Servers	Single key	Sig/Enc
Router/gateway	Single key	Sig/Enc
Mail gateway	Single key	Sig/Enc
Domain controller	Single key	Sig/Enc
Computer certificate 802.1x	Single key	Client authentication
Mobile Device Web Auth.	Single Key	LogOn
Code signing	Single key	Code Sig
OCSP	Single key	Sig/Enc

Table 18: Assignment of certificate profiles and templates

A certificate request that originates from a device or an application is checked for defined content of the Subject DN (see Chapter 3.1.1 et seq.) and the use of forbidden characters. The version of the certificate profile in question as described in Chapter 7.1 et seq. applies. The use of unauthorized characters is indicated with the check during manual registration or notified to the requester. In the case of certificate applications via the automated registration authority, the orders are rejected with an error message (notification).

The certificates issued by Telekom Security meet the following requirements:

- [RFC 5280]
- [X.509]
- [CAB-BR]
- [ETSI 319411-1 Policy LCP]

Issued X.509v3 certificates must include at least the contents listed in Table 19.

Field	Value or value limitation:
Version:	Certificate version (Chapter 7.1.1)
Certificate serial number:	Unique value to identify the certificate

Field	Value or value limitation:
Signature algorithm:	RSA – SHA-256[3]
Issuer:	Certification authority (Chapters 1.3.1.2.1 and 1.3.1.2.2)
Valid from:	Time basis Coordinated Universal Time (UTC). Coded in accordance with RFC 5280.
Valid to:	Time basis Coordinated Universal Time (UTC). Coded in accordance with RFC 5280.
Requester:	Unique name (Chapter 7.1.4); user certificates: 3.1.1.1.16
Public key:	Coded in accordance with RFC 5280.
Extensions:	
Key usage:	Chapter 7.1.2.1
Certificate Policy:	Chapter 7.1.2.2
Alternative requester (subject) name:	Chapter 7.1.2.3
Basic constraints:	Chapter 7.1.2.4
Enhanced key usage:	Chapter 7.1.2.5
Revocation list distribution point:	Chapter 7.1.2.6
Subject key identifier:	Chapter 7.1.2.7
Authority key identifier:	Chapter 7.1.2.8
Access to authority information	Chapter 7.1.2.9
Certificate template name	Chapter 7.1.2.10

Table 19: Certificate attributes in accordance with X509.v3

Additional extensions and properties are described in more detail in the chapters that follow.

7.1.1 Version numbers

The X.509 certificates for end entities issued by DTAG's cPKI are the latest version (currently version 3). Additional extensions and properties are described in more detail in the chapters that follow.

The CA and root 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 Chapters 7.1.2.1 to 7.1.2.10.

7.1.2.1 Key usage

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

In Table 20 to Table 22, the "key usage" extension is assigned to the different certificate profiles.

[3] Alternatively RSA - SHA-1

Device certificates

	Certificate profile:	Server	Router/ gateway	Mail gateway	Domain controller	Computer
	Criticality	critical	critical	critical	critical	critical
Bit	Designation	Sig/Enc	Sig/Enc	Sig/Enc	Sig/Enc	Client auth.
0	digitalSignature	✓	✓	✓	✓	✓
1	nonRepudiation	×	×	×	×	×
2	keyEncipherment	✓	✓	✓	✓	✓
3	dataEncipherment	×	×	×	✓	×
4	keyAgreement	×	×	×	×	×
5	keyCertSign	×	×	×	×	×
6	CRLSign	×	×	×	×	×
7	encipherOnly	×	×	×	×	×
8	decipherOnly	×	×	×	×	×
	Value (hex)	A0	A0	A0	B0	A0

Table 20: Assignment of the "key usage" extension, part 1

User certificates:

		Single key FMB/GRP	Single-Key Mobile Device Web-Authentication	Single key mobile device Signature	Triple key		
	Criticality	critical	critical	critical	critical	critical	critical
Bit	Designation	Sig/Enc	LogOn	Sig	Sig	Enc	LogOn
0	digitalSignature	✓	✓	✓	✓	×	✓
1	nonRepudiation	×	×	×	×	×	×
2	keyEncipherment	✓	✓	×	×	✓	×
3	dataEncipherment	✓	×	×	×	✓	×
4	keyAgreement	×	×	×	×	×	×
5	keyCertSign	×	×	×	×	×	×
6	CRLSign	×	×	×	×	×	×
7	encipherOnly	×	×	×	×	×	×
8	decipherOnly	×	×	×	×	×	×

User certificates:							
	Value (hex)	B0	A0	80	80	30	80

Table 21: Assignment of the "key usage" extension, part 2

CA certificates			
	Certificate profile:	**Sub-CA**	**Root CA**
	Criticality	critical	critical
Bit	Designation	Cert/CRL	Cert/CRL
0	digitalSignature	✓	×
1	nonRepudiation	×	×
2	keyEncipherment	×	×
3	dataEncipherment	×	×
4	keyAgreement	×	×
5	keyCertSign	✓	✓
6	CRLSign	✓	✓
7	encipherOnly	×	×
8	decipherOnly	×	×
	Value (hex)	86	06

Table 22: Assignment of the "key usage" extension, part 3

At the customer's request, further values from the above table 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., email) do not evaluate the nonRepudiation bit. For this reason, defining the bit is not helpful for relying parties when deciding on trustworthiness.

7.1.2.2 "Certificate Policies" extension

The "Certificate Policy" extension consists of object identifiers (OID; see also Chapter 7.1.6) and a URL, via which this CP/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 23 the "Subject Alternative Name" extension is assigned to the different certificate profiles.

Certificate profiles

	User certificate:			Server certificate:	Router/gateway certificate:	Mail gateway certificate:	Domain controller certificate:	Computer certificate:
Extension:	SK FMB	SK MD	TK					
RFC822 name	✓	✓	✓	×	✓	✓	✓	×
Principal name	✓	✓	✓	×	×	×	×	×
DNS Name	×	×	×	✓	×	×	✓	✓
IP address	×	×	×	×	✓	×	×	×
Other name (DS object Guid)	×	×	×	×	×	×	✓	×

Table 23: Assignment of the "Subject Alternative Name" extension (subjectAltName)

No alternative requester names are used for Mobile Device User Signature and Mobile Device Client Auth.

The criticality 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 24 shows the root and sub-CA certificates used by the cPKI. The cPKI service does not provide further sub-CA certificates that are hierarchically subordinate to one of the sub-CAs shown.

Basic constraints for root CA and sub-CA certificates

Name/type	Criticality	User type	Restriction of the certification type
T-TeleSec GlobalRoot Class 2	critical	Certification authority	none
Deutsche Telekom Root CA 2	non-critical	Certification authority	5
Deutsche Telekom Internal Root CA 1	critical	Certification authority	1
Deutsche Telekom Internal Root CA 2	critical	Certification authority	none
Deutsche Telekom AG secure email CA	critical	Certification authority	0
Deutsche Telekom AG secure email CA E02	critical	Certification authority	0
Deutsche Telekom AG secure email CA E03	critical	Certification authority	0
Deutsche Telekom AG infrastructure CA	critical	Certification authority	0

Basic constraints for root CA and sub-CA certificates

Deutsche Telekom AG authentication CA	critical	Certification authority	0
Deutsche Telekom AG Issuing CA 01	critical	Certification authority	0
Deutsche Telekom AG Issuing CA 02	critical	Certification authority	0
Deutsche Telekom AG Issuing CA 03	critical	Certification authority	0
Deutsche Telekom AG mobile device CA	critical	Certification authority	0
Deutsche Telekom AG internal secure email CA	critical	Certification authority	0
End entity	non-critical	End unit	none

Table 24: Assignment of the "basic constraints" extension

7.1.2.5 "Extended key usage" extension (ExtendedKeyUsage)

In the table below, the "extended key usage" is assigned to the different certificate profiles in tabular form.

Extended key usage for user certificates:

	Single key FMB/GRP	**Single key mobile device**	**Single-Key Mobile Device**	**Single key code signing**	**Triple key**		
Criticality	**non-critical**	**non-critical**	**non critical**	**non-critical**	**non-critical**	**non-critical**	**critical**
Designation	Sig/Enc	Sig	LogOn	Sig	Sig	Enc	LogOn
Secure email (1.3.6.1.5.5.7.3.4)	✓	✓	×	×	✓	✓	×
Code signing (1.3.6.1.5.5.7.3.3)	×	×	×	✓	×	×	×
Server authentication (1.3.6.1.5.5.7.3.1)	×	×	×	×	×	×	×
Timestamping (1.3.6.1.5.5.7.3.8)	×	×	×	×	×	×	×
Client authentication (1.3.6.1.5.5.7.3.2)	×	×	✓	×	×	×	✓
OCSP signing (1.3.6.1.5.5.7.3.9)	×	×	×	×	×	×	×
MS smartcard logon (1.3.6.1.4.1.311.20.2.2)	×	×	×	×	×	×	✓

Table 25: Assignment of the "extended key usage" extension for user certificates

Extended key usage for user certificates:

	Server Authentication	**Client Authentication**	**Code Signing**	**Secure Email**	**Smartcard Logon**
OID	1.3.6.1.5.5.7.3.1	1.3.6.1.5.5.7.3.2	1.3.6.1.5.5.7.3.3	1.3.6.1.5.5.7.3.4	1.3.6.1.4.1.311.20.2.2
DTAG Employee Encryption	×	×	×	✓	×

Extended key usage for user certificates:					
DTAG Employee Signature	✗	✗	✗	✓	✗
DTAG Employee Authentication	✗	✓	✗	✗	✓
DTAG External Workforce Encryption	✗	✗	✗	✓	✗
DTAG External Workforce Signature	✗	✗	✗	✓	✗
DTAG External Workforce Authentication	✗	✓	✗	✗	✓
DTAG Encryption for Pseudonyms	✗	✗	✗	✓	✗
DTAG Signature for Pseudonyms	✗	✗	✗	✓	✗
DTAG Authentication for Pseudonyms	✗	✓	✗	✗	✓
DTAG Signature and Encryption for Functional mailboxes (FMB)	✗	✗	✗	✓	✗
DTAG Encryption for Groups and Function Accounts	✗	✗	✗	✓	✗
DTAG Signature for Groups and Function Accounts	✗	✗	✗	✓	✗
DTAG Authentication for Groups and Function Accounts	✗	✓	✗	✗	✓
DTAG Encryption for robots	✗	✗	✗	✓	✗
DTAG Signature for robots	✗	✗	✗	✓	✗
DTAG Authentication for robots	✗	✓	✗	✗	✓
DTAG Employee Signature Mobile Devices	✗	✗	✗	✓	✗
DTAG Employee Web Authentication Mobile Devices	✗	✓	✗	✗	✗
DTAG Code Signing	✗	✗	✓	✗	✗

Table 26: Assignment of the "extended key usage" extension for user certificates

Extended key usage for device certificates						
Certificate profile:	**Server**	**Router/ gateway**	**Mail gateway**	**Domain controller**	**Computer**	**Roboter** Details see user cert..
Criticality	n/a	n/a	critical	critical	critical	critical

Extended key usage for device certificates						
Secure email (1.3.6.1.5.5.7.3.4)	×	×	✓	×	×	✓
Code signing (1.3.6.1.5.5.7.3.3)	×	×	×	×	×	×
Server authentication (1.3.6.1.5.5.7.3.1)	✓	×	×	✓	✓	×
Timestamping (1.3.6.1.5.5.7.3.8)	×	×	×	×	×	×
Client authentication (1.3.6.1.5.5.7.3.2)	✓	×	×	✓	✓	×
OCSP signing (1.3.6.1.5.5.7.3.9)	×	×	×	×	×	×
MS smartcard logon (1.3.6.1.4.1.311.20.2.2)	×	×	×	×	×	×

Table 27: Assignment of the "extended key usage" extension for device certificates

Extended key usage for device certificates	Criticality	Server authentication	Client authentication	Code signing	Secure email	Smartcard logon
OID		1.3.6.1.5.5.7.3.1	1.3.6.1.5.5.7.3.2	1.3.6.1.5.5.7.3.3	1.3.6.1.5.5.7.3.4	1.3.6.1.4.1.311.20.2.2
Server certificate	n/a	✓	×	×	×	×
Router/gateway certificate	n/a	✓	×	×	×	×
Mail gateway certificate	critical	×	×	×	✓	×
Domain controller certificate	critical	✓	✓	×	×	✓
Mobile device client auth.	critical	×	✓	×	×	×
Computer certificate	critical	✓	✓	×	×	×

Table 28: Assignment of the "extended key usage" extension for device certificates

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 LDAP) the current certificate revocation list (CRL) can be accessed on the directory service. 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 certificates, the "subject key identifier" extension contains a 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 CA certificates contains a SHA-1 hash value as the attribute value. This hash value is formed from the public key of the respective CA. This value corresponds mathematically to the value of the "authority key identifier" extension (see Chapter 7.1.2.8) of the end-entity 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" (authorityKeyIdentifier) extension

In end-entity certificates, the "authority key identifier" extension contains a SHA-1 hash value as the attribute value. This hash value corresponds mathematically to the value of the "subject key identifier" 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-entity certificates

In the end-entity certificate, 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, see also Chapter 2.2 under "Provision of certificate status data via the OCSP protocol."

Access to authority information access (AIA) in end-entity certificates
Object identifier (OID) 1.3.6.1.5.5.7.48.1

End-entity certificate issued by CA	OCSP path	Comments
Deutsche Telekom AG Issuing CA 01	http://ocsp-cpki.telekom.de/ocsp	
Deutsche Telekom AG Issuing CA 02	http://ocsp-cpki.telekom.de/ocspr	
Deutsche Telekom AG Issuing CA 03:	http://ocsp-cpki.telekom.de/ocspr	
Deutsche Telekom AG mobile device CA:	http://ocsp-cpki.telekom.de/ocspr	
Deutsche Telekom AG secure email CA E02	http://ocsp-cpki.telekom.de/ocspr	
Deutsche Telekom AG secure email CA:	http://ocsp-cpki.telekom.de/ocspr	
Deutsche Telekom AG authentication CA	http://ocsp-cpki.telekom.de/ocspr	
Deutsche Telekom AG internal secure email CA	http://ocsp-cpki.telekom.de/ocspr	

Table 29: "Authority information access" extension, part 1

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:

Access to authority information access (AIA) in intermediate certification authority certificates
Object identifier (OID) 1.3.6.1.5.5.7.48.1

CA certificate	OCSP path
Deutsche Telekom AG Issuing CA 01:	http://ocsp-cpki.telekom.de/ocsp

Access to authority information access (AIA) in intermediate certification authority certificates Object identifier (OID) 1.3.6.1.5.5.7.48.1	
Deutsche Telekom AG Issuing CA 01:	http://ocsp-cpki.telekom.de/ocspr
Deutsche Telekom AG Issuing CA 02	http://ocsp-cpki.telekom.de/ocsp
Deutsche Telekom AG Issuing CA 02	http://ocsp-cpki.telekom.de/ocspr
Deutsche Telekom AG Issuing CA 03:	http://ocsp-cpki.telekom.de/ocsp
Deutsche Telekom AG Issuing CA 03:	http://ocsp-cpki.telekom.de/ocspr
Deutsche Telekom AG authentication CA:	http://ocsp-cpki.telekom.de/ocspr
Deutsche Telekom AG infrastructure CA:	http://ocsp-cpki.telekom.de/ocspr
Deutsche Telekom AG mobile device CA:	http://ocsp-cpki.telekom.de/ocspr
Deutsche Telekom AG secure email CA:	http://ocsp-cpki.telekom.de/ocspr
Deutsche Telekom AG secure email CA E02:	http://ocsp-cpki.telekom.de/ocspr
Deutsche Telekom AG secure email CA E03	http://ocsp-cpki.telekom.de/ocspr
Deutsche Telekom AG internal secure email CA:	http://ocsp-cpki.telekom.de/ocspr

Table 30: "Authority information access" extension, part 2

The CA certificates also contain the object identifier (OID) 1.3.6.1.5.5.7.48.2 with the HTTPS and LDAP path specifications of the respective root CA certificate.

Access to authority information access (AIA) in root CA certificates Object identifier (OID) 1.3.6.1.5.5.7.48.2		
CA	**HTTP path**	**LDAP path**
Deutsche Telekom AG Issuing CA 01:	http://crt-cpki.telekom.de/crt/GlobalRoot_Class_2.cer	ldap://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?cACertificate
Deutsche Telekom AG Issuing CA 02	http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_1.cer	ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base=objectClass=certificationAuthority
Deutsche Telekom AG Issuing CA 03:	http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_1.cer	ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%201,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base=objectClass=certificationAuthority

Access to authority information access (AIA) in root CA certificates Object identifier (OID) 1.3.6.1.5.5.7.48.2		
Deutsche Telekom AG mobile device CA:	http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_2.cer	ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate ldap:///CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,CN=InternalRootCA,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=cds,DC=t-internal,DC=com?cACertificate?base=objectClass=certificationAuthority
Deutsche Telekom AG secure email CA:	http://crt-cpki.telekom.de/crt/GlobalRoot_Class_2.cer	ldap://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?cACertificate
Deutsche Telekom AG secure email CA E02	http://crt-cpki.telekom.de/crt/GlobalRoot_Class_2.cer	ldap://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?cACertificate
Deutsche Telekom AG secure email CA E03	http://crt-cpki.telekom.de/crt/GlobalRoot_Class_2.cer	ldap://ldap-cpki.telekom.de/CN=T-TeleSec%20GlobalRoot%20Class%202,OU=T-TeleSec%20Trust%20Center,O=T-Systems%20Enterprise%20Services%20GmbH,C=DE?cACertificate
Deutsche Telekom AG authentication CA	http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_2.cer	ldap://ldap-cpki.telekom.de/CN=Deutsche Telekom Internal Root CA 2,OU=Trust Center,O=Deutsche Telekom AG,C=DE?cACertificate ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate
Deutsche Telekom AG infrastructure CA	http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_2.cer	ldap://ldap-cpki.telekom.de/CN=Deutsche Telekom Internal Root CA 2,OU=Trust Center,O=Deutsche Telekom AG,C=DE?cACertificate ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate
Deutsche Telekom AG internal secure email CA	http://crt-cpki.telekom.de/crt/DT_Internal_Root_CA_2.cer	ldap://ldap-cpki.telekom.de/CN=Deutsche Telekom Internal Root CA 2,OU=Trust Center,O=Deutsche Telekom AG,C=DE?cACertificate ldap://ldap-cpki.telekom.de/CN=Deutsche%20Telekom%20Internal%20Root%20CA%202,OU=Trust%20Center,O=Deutsche%20Telekom%20AG,C=DE?cACertificate

Table 31: "Authority information access" extension, part 3

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

7.1.2.10 "Certificate template name" extension

For the "Domain controller" certificate profile, the "certificate template name" extension is filled with the "DomainController" name.

7.1.3 Algorithm object identifiers

Within DTAG's cPKI, 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-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 intermediate certification authority (sub-CA) must use the SHA-256 signature hash algorithm.

The SHA-1 signature hash algorithm is no longer recommended for security reasons and is not permitted in certificates issued by a public sub-CA.
SHA-1 is only allowed for interoperability reasons in certificates issued by an internal sub-CA.

7.1.4 Name forms

The end-entity certificates of the "cPKI" contain a unique Issuer DN from the certification authority in question (Chapter 1.3.1.2).

The content of the Subject DN (requester) depends on the certificate type (e.g., user, server, router/gateway) and is optionally made up of the fields as described in Chapter 3.1.1.1. The fields contain mandatory, optional, or automatically generated information.

Mandatory information for certificates for persons,

- which is taken from the trusted directory (cIAM), contains the following fields:
  - Common Name (CN) = <first name, last name>
  - Email Address (E) = <primary email address from the AD>
  - Given Name (G) = <first name>
  - Surname (SN) = <last name>
  - Organizational Unit Name (OU) = <corporate ID (CID)>
  - Organizational Unit Name (OU) = Employee or external workforce
- which is generated automatically by the system, contains the following fields:
  - Country Name (C): DE
  - Organization Name (O) = DTAG or Deutsche Telekom AG
  - Organizational Unit Name (OU) = Person

Mandatory information for certificates for pseudonyms,

- which is taken from the trusted directory (cIAM), contains the following fields:
  - Common Name (CN) = PN-<first name, last name>

- Email Address (E) = <primary email address from the AD>
- Pseudonym (PN) = <name of the pseudonym>
- Organizational Unit Name (OU) = <corporate ID (CID)>

- which is generated automatically by the system, contains the following fields:
  - Organization Name (O) = DTAG or Deutsche Telekom AG
  - Organizational Unit Name (OU) = Person
  - Country Name (C) = (DE)

Mandatory information for certificates for Functional mailboxes (FMB),

- that is taken from DTAG's Active Directory (AD), contains the following fields:
  - Common Name (CN) = <FMB name>.<SAM account name>,
  - Email Address (E) = <primary email address from the AD >,
  - Organizational Unit Name OU = <function group (FMB or GRP)>
  - Organizational Unit Name OU = Internal
- which is generated automatically by the system, contains the following fields:
  - Organization Name (O) = Deutsche Telekom AG
  - Country Name (C) = DE

Mandatory information for certificates for function and group accounts,

- which is taken from the trusted directory (cIAM), contains the following fields:
  - Common Name (CN) = <GRP-designation >,
  - Email Address (E) = <primary email address from the AD >,
  - Organizational Unit Name (OU) = <Corporate ID (CID)>
  - Organizational Unit Name OU = GRP or Function or Group Account
- which is generated automatically by the system, contains the following fields:
  - Organization Name (O) = Deutsche Telekom AG
  - Country Name (C) = DE

Mandatory information for certificates for robots,

- which is taken from the trusted directory (cIAM), contains the following fields:
  - Common Name (CN) = <Robot- designation >,
  - Email Address (E) = <primary email address from the AD >,
  - Organizational Unit Name (OU) = <Corporate ID (CID)>
  - Organizational Unit Name OU = < Robot
- which is generated automatically by the system, contains the following fields:
  - Organization Name (O) = Deutsche Telekom AG
  - Country Name (C) = DE

Mandatory information for certificates for legal persons

- Common Name (CN) = <name of the legal person>

  - Email Address (E) = <primary email address from the AD>
  - organizationIdentifier = WEEE registration no. <number>
- which is generated automatically by the system, contains the following fields:
  - Organization Name (O) = Deutsche Telekom AG
  - Organizational Unit Name (OU) = Person
  - Country Name (C) = (DE)

Mandatory information for certificates for Mobile Device Web authentication

  - E-Mail-Address (E) = <primäre eMail aus dem AD>,
  - Common Name (CN) = <A-Account Name>
  - Organizational Unit Name (OU) = <Corporate ID (CID)>
  - Organizational Unit Name (OU) = <SID>
- which is generated automatically by the system, contains the following fields:
  - OU = DTAGAuthenticationAppsMobile
  - OU = EMEA1-AuthCert-VMwareSDK
  - Organizational Unit Name (OU) = Person
  - Organization Name (O) = Deutsche Telekom AG
  - Country Name (C) = (DE)

Mandatory information for certificates for Mobile Device Signatur

  - E-Mail-Address (E) = <primäre eMail aus dem AD>,
  - Common Name (CN) = <Vorname Nachname>
  - Organizational Unit Name (OU) = <Corporate ID (CID)>
- which is generated automatically by the system, contains the following fields:
  - OU = Employee
  - Organizational Unit Name (OU) = Mobile
  - Organization Name (O) = DTAG oder Deutsche Telekom AG

Mandatory information for certificates for devices

- Computer certificate 802.1x
  - Common Name (CN) = Fully qualified domain name, FQDN
- Server
  - Common Name (CN) = Fully qualified domain name, FQDN
  - localityName (L) = <town/city>
  - stateOrProvinceName (S) = <state/province>
  - Organization Name (O) = <company/organization>
  - Country Name (C) = <country>

The following fields are optional:

- Organizational Unit Name 3 (OU3)
- User Principal Name (UPN)
- Other email addresses and server names (fully qualified domain name, FQDN)

The email address does not have to be the content of the Subject DN if this information is contained in the "subjectAltName" extension.

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.

The contents of the subject alternative name (subjectAltName) are also dependent on the certificate type (e.g. user, server, router/gateway) and can be composed as follows:

- User Principal Name (UPN)
- RFC822
- DNS Name

The issued certificates will always contain the "Issuer Distinguished Name" and "Subject Distinguished Name" fields:

Certificate	Issuer DN	Subject DN
Deutsche Telekom AG Employee Encryption	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN =<first name, last name> G = <first name> SN = <last name> OU = <CID> OU = Employee OU = Person O = DTAG or Deutsche Telekom AG C = DE
Deutsche Telekom AG Employee Signature	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN = <first name, last name> OU = <CID> AD> OU = Employee OU = Person O = DTAG or Deutsche Telekom AG C = DE

Certificate	Issuer DN	Subject DN
Deutsche Telekom AG Employee Authentication	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN = <first name, last name> G = <first name> SN = <last name> OU = <CID> OU = Employee OU = Person O = DTAG or Deutsche Telekom AG C = DE
Deutsche Telekom AG External Workforce Encryption	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN = <first name, last name> G = <first name> SN = <last name> OU = <CID> OU = External workforce OU = Person O = DTAG or Deutsche Telekom AG C = DE
Deutsche Telekom AG External Workforce Signature	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN = <first name, last name> G = <first name> SN = <last name> OU = <CID> OU = External workforce OU = Person O = DTAG or Deutsche Telekom AG C = DE
Deutsche Telekom AG External Workforce Authentication	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN = <first name, last name> G = <first name> SN = <last name> OU = <CID> OU = External workforce OU = Person O = DTAG or Deutsche Telekom AG C = DE
Deutsche Telekom AG Encryption for Pseudonyms	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN = PN-<first name, last name> OU = <CID> OU = Pseudonym OU = Person O = DTAG or Deutsche Telekom AG C = DE
Deutsche Telekom AG Signature for Pseudonyms	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN = PN-<first name, last name> OU = <CID> OU = Pseudonym OU = Person O = Deutsche Telekom AG

Certificate	Issuer DN	Subject DN
		C = DE
Deutsche Telekom AG Authentication for Pseudonyms	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN = PN-<first name, last name> OU = <CID> OU = Pseudonym OU = Person O = Deutsche Telekom AG C = DE
Deutsche Telekom AG Signature and Encryption for Functional mailboxes (FMB)	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	CN = FMB-<mailbox name>.<SAM account name > OU = FMB OU = Internal O = Deutsche Telekom AG C = DE
Deutsche Telekom AG Signatur für Gruppen und Funktionsaccounts	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN = GRP-<designation> OU = GRP OU = <CID> O = Deutsche Telkom AG C = DE
Deutsche Telekom AG Encryption für Gruppen und Funktionsaccounts	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN = GRP-<designation> OU = GRP OU = <CID> O = Deutsche Telkom AG C = DE
Deutsche Telekom AG Authentifizierung für Gruppen und Funktionsaccounts	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN = GRP-<designation> OU = GRP OU = <CID> O = Deutsche Telkom AG C = DE
Deutsche Telekom AG Signatur für Roboter	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN = Robot-<designation> OU = Robot OU = <CID> O = Deutsche Telkom AG C = DE
Deutsche Telekom AG Encryption für Roboter	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN = Robot-<designation> OU = Robot OU = <CID> O = Deutsche Telkom AG C = DE
Deutsche Telekom AG Authentifizierung für Roboter	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN = Robot-<designation> OU = Robot OU = <CID>

Certificate	Issuer DN	Subject DN
		O = Deutsche Telkom AG C = DE
Deutsche Telekom AG Signature for Users on Mobile Devices	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN = <first name, last name> OU = <CID> OU = Employee OU = Mobile O = DTAG
Deutsche Telekom AG Web authentication for Users of Mobile Devices	CN = <certification authority> OU = <organizational unit> O = <organization> C = <country>	E = <primary email address from AD> CN =<A-Account name> OU = <CID> OU = DTAGAuthenticationAppsMobile OU = EMEA1-AuthCert-VMwareSDK OU = <SID> OU = Person O = DTAG oder Deutsche Telkom AG C = DE

Table 32: Issuer DN and Subject DN

In addition, entries are made in the "Subject Alternative Name" for some certificates:

Certificate	Other Name	Principal Name	RFC822 Name
Deutsche Telekom AG Employee Encryption	None	UPN	Email address
Deutsche Telekom AG Employee Signature	None	UPN	Email address
Deutsche Telekom AG Employee Authentication	None	UPN	Email address
Deutsche Telekom AG External Workforce Encryption	None	UPN	Email address
Deutsche Telekom AG External Workforce Signature	None	UPN	Email address
Deutsche Telekom AG External Workforce Authentication	None	UPN	Email address
Deutsche Telekom AG Signature and Encryption for Functional mailboxes	None	UPN	Email address
Deutsche Telekom AG Encryption or Group and Function Accounts	none	UPN	Email address
Deutsche Telekom AG Signatur or Group and Function Accounts	none	UPN	Email address

Certificate	Other Name	Principal Name	RFC822 Name
Deutsche Telekom AG Authentication or Group and Function Accounts	none	UPN	Email address
Deutsche Telekom AG Encryption for robots	none	UPN	Email address
Deutsche Telekom AG Signatur for robots	none	UPN	Email address
Deutsche Telekom AG Authentication for robots	none	UPN	Email address
Deutsche Telekom AG Signature for Users on Mobile Devices	None	None	Email address
Deutsche Telekom AG Web authentication for Users on Mobile Devices	none	none	Email address
Deutsche Telekom AG Telekom Computer	DNS	None	None
Deutsche Telekom AG Domain Controller	DNS	None	None

Table 33: Entries in the Subject Alternative Name

7.1.5 Name constraints

Only names/domains administered by DTAG are permitted.

Certificate issuance is restricted to Deutsche Telekom domains. For this purpose, a restriction to approved mail domains is implemented in the cPKI certificate management. A domain constraint in the certificate will no longer be applied to public certification authorities from 25. February 2020 onwards, as the CAs have been audited in accordance with ETSI 319411-1 Policy LCP and are included in the CCADB.

CA certificates with an issue date prior to February 25, 2020 also contain a domain constraint (name restriction) in the CA certificate for approved mail domains

7.1.6 Object IDs (OIDs) for certificate policies

7.1.6.1 Object IDs for cPKI certificate policies

All end-entity and CA certificates contain a "certificate policies" extension. As well as the HTTP URL, the CP/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 registered private enterprises(1) T-TeleSec(7879) policy identifier(13) cPKI(26)} -> 1.3.6.1.4.1.7879.13.26

7.1.6.2 Object IDs for baseline requirements certificate policies

The CA/Browser Forum has defined the following policy OIDs in the Baseline Requirements [CAB-BR]:

- 2.23.140.1.2.1 (domain validated (DV)) and
- 2.23.140.1.2.2 (organizational validated (OV))
- 2.23.140.1.2.3 (individual validated (IV))

The following requirements, which the CAs of the cPKI under a public root adhere to, apply to 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 in SSL certificates:

- organizationName (Chapter 3.1.1.1.2)
- localityName (Chapter 3.1.1.1.12)
- stateOrProvinceName (Chapter 3.1.1.1.13)
- countryName (Chapter 3.1.1.1.1)

No server certificates are issued from the cPKI under the public CA with the policy OID 2.23.140.1.2.2.

The policy OIDs 2.23.140.1.2.1 and 2.23.140.1.2.3 are not used by the cPKI as no DV and IV certificates are issued by the CA under the public root.

7.1.7 Use of the "policy constraints" extension

No Stipulation.

7.1.8 Syntax and semantics of policy IDs

The certificates contain a "Policy Qualifier" entry as well as a reference (URI) to the CP/CPS valid at the time of issue.

The current CP/CPS is always stored. Older versions are stored in the corresponding repository. See Chapters 7.1.2.2 and 7.1.6

7.1.9 Processing semantics for the "critical certificate policies" extension

No Stipulation.

7.1.10 Subject DN Serial Number (SN)

No Stipulation.

7.1.11 Object IDs for "certificate transparency (CT)"

No Stipulation.

7.2 Revocation list profile

The revocation lists issued by Telekom Security meet the following requirements:

- **[RFC 5280]** Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- **[X.509]** Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks

Certificate revocation lists must include at least the contents described in Table 34:

Fields	Value
Version	Revocation list version (Chapter 7.2.1)
Issuer	Contains the instance that issued and signed the revocation list. Certification authority (Chapter 1.3.1)

Fields	Value
Valid from:	Time basis: Coordinated Universal Time (UTC). Coded in accordance with RFC 5280.
Next update:	Date and time of the next planned publication.
Signature algorithm:	RSA – SHA-256[4]
Revoked certificates:	List of revoked certificates including serial number with revocation date and time of the revoked certificate.
Extensions:	
Authority key identifier:	The regulations in accordance with Chapter 7.2.2.1 apply.
Revocation list number:	Unique value (Chapter 7.2.2.2)
Reason for revocation:	Coding of the revocation reason in accordance with RFC 5280 (Chapter 7.2.2.3).

Table 34: CRL profile (here: basic values)

7.2.1 Version number

The X.509 certificate revocation lists issued by the cPKI correspond to version 2.

7.2.2 Revocation list and revocation list entry extensions

Issued CRLs contain the following "extension" entries:

Fields	Value
Authority Key Identifier	This entry contains the key hash of the issuing instance.
CRL Number	Unique, ascending number of the revocation list
CA Version	Starting value: 0.0
Next CRL Publish	Date and time of the next revocation list publication

Table 35: CRL profile: extension entries

7.2.2.1 "Authority key identifier" (authorityKeyIdentifier) extension

The revocation lists are given the extension "authority key identifier" as described in Chapter 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 contain the "revocation list number" extension as a sequential serial number of the revocation list.
The criticality of this extension is set to "not critical."

7.2.2.3 "Reason for revocation" (Reason Code) extension

When revoking certificates, it is essential to state a reason for revocation. In accordance with Table 36 below, the following reason codes are implemented:

[4] Alternatively RSA - SHA-1

Event	Reasons for revocation in accordance with RFC 5280	Value of the reason for revocation in accordance with RFC 5280
Not specified	Unspecified	0
Key compromised	KeyCompromise	1
Information in the certificate is out of date	AffiliationChanged	3
Certificate revoked following renewal	Superseded	4
Temporary revocation	CertificateHold	6

Table 36: "Reason Code" extension

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

7.3 OCSP profile

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

The OCSP responder used fulfills the requirements of RFC 6960.

7.3.1 Version number

Version 1 is supported pursuant to the OCSP specification in accordance with RFC 6960.

7.3.2 OCSP extensions

The OCSP certificate, issued by the intermediate certification authority (sub-CA) (for an overview see Figure 1 and Figure 6), contains the "extended key usage" attribute with the OID "1.3.6.1.5.5.7.3.92 (OCSP noCheck, id-pkix-ocsp-nocheck); i.e., the OCSP certificate is not validated.

8 COMPLIANCE AUDITS AND OTHER ASSESSMENTS

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 (Chapter 8.2).

The Telekom Security processes are subject to a regular annual check (ETSI 319411-1 Policy LCP) by an independent third party. The subject of certification comprises all processes that are used for the application, issue, revocation, and renewal of end entity certificates in conjunction with a public certification authority (Chapters 1.3.1.1.1 and 1.3.1.2.1). In addition, Telekom Security performs quality assessment self-audits (Chapter 8.1) at regular intervals.

8.1 Interval and reason for audits

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

Quality assessment self-audits, which ensure the quality of service, take place regularly and as required (e.g., security incident). 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.

8.2 Identity and quality of auditors

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 to auditors who perform an audit in the Telekom Security Trust Center at the request of one or more application software providers. For cPKI, 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.

The quality assessment self-audits are carried out by a qualified Telekom Security employee with appropriate expertise in the areas of PKI, IAM, and ETSI requirements

8.3 Relationship of the auditor to the authority to be audited

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

Quality assessment self-audits are performed by Telekom Security employees who are qualified for this.

8.4 Audit areas covered

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

- Issue of certificates
- Data source/trusted database on which the end entities are registered
- Certification request process

- Processing certification requests
- Distribution of keys and secrets (password, OTP, PIN)
- Certificate acceptance
- Renewal of certificates (re-certification)
- Renewal of keys (re-key)
- Certificate revocations
- Physical access control
- Key backup and archiving
- Authorization and role concept
- Anti-intruder measures
- Human resources

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

- ETSI 319411-1 Policy LCP

Risk assessment and security plan

The Telekom Security Trust Center usually performs a risk assessment annually or as required, which also covers the cPKI PKI service.

The assessment covers at least the following items:

1. Identifying foreseeable potential external and external risks (i.e., especially their underlying vulnerabilities) which might 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, disruption, or failure of all or part of the certificate administration 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 Telekom Security Trust Center has developed a security plan that is regularly checked and, if necessary, modified. The security plan is made up of processes, measures, and products to support assessment and management during the risk assessment of identified risks. The security plan contains administrative, organizational, technical, and physical security measures according to the sensitivity of the data and the certificate management process.

8.5 Measures for resolving deficits

If a compliance audit of Telekom Security detects defects or errors, a decision will be made as to what corrective action is to be taken. The director of the Trust Center decides together with the auditor which suitable measures should be implemented in an economically suitable time frame. 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 time frame.

8.6 Communication of the results

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

Telekom Security reserves the right to publish results or partial results, e.g., if misuse occurred or the image of Telekom Security was possibly harmed.

Audit reports that are saved at the request of by one or more application software providers and refer to a Telekom Security root certification certificate must be published at the latest three months after the audit period in question ends.

For the cPKI, the required audits are saved in accordance with ETSI 319411-1 Policy LCP criteria. The corresponding reports are published on the website https://corporate-pki.telekom.de/.

9 OTHER BUSINESS AND LEGAL PROVISIONS

9.1 Charges

The fees for PKI services are specified in the respective contractual agreements with the customer; these fee agreements are not published.

9.1.1 Charges for issuing or renewing certificates

Telekom Security is entitled to charge for issuing, renewing, and managing end-entity certificates. This applies in particular to the provision and handover of the cPKi service.

9.1.2 Charges for access to certificates

Telekom Security does not charge for access to certificates in the cPKI's directory service.

Third parties require prior express permission in writing before marketing or making available for marketing the certificates that Telekom Security provides publicly.

9.1.3 Charges for revocation or status queries

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 or making available for marketing the revocation and status information that Telekom Security provides publicly.

9.1.4 Charges for other services

Telekom Security does not charge any fees for the retrieval and associated consideration of this "Certificate Policy (CP)/Certification Practice Statement (CPS)" document. Any other usage, e.g., reproduction, amendment, or production of a derived document, is subject to the written consent of the authority (Chapter 1.5.1) that owns the copyright (Chapter 9.5.2).

The use of this CP/CPS is also free of charge provided it is used as an applicable contract document for the contractual relationship between the customer 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 customer is obligated to ensure economically appropriate insurance cover from an insurer or via its own liability cover.

Telekom Security has appropriate business liability insurance and D&O liability insurance cover.

9.2.2 Other financial means

We recommend that the customer has sufficient financial means to be able to maintain its PKI operation and to meet the obligations for its operation that are described in and derived from this document. In addition, the customer must be capable of bearing the liability risk toward 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 Chapter 8 are an exception to this.

9.2.3 Insurance or guarantee for end entities

No Stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Confidential information is any information from parties involved in PKIs (see Chapters 1.3.2 and 1.3.3) of the cPKI, which is not covered by Chapter 9.3.2.

9.3.2 Scope of non-confidential information

Non-confidential information is any implicit and explicit information from the cPKI that is included in issued certificates (e.g., email 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 customer must abide by the applicable statutory provisions and other regulations concerning data protection.

9.4 Protection of personal data (data protection)

9.4.1 Data protection concept

Within the cPKI, Telekom Security must store and process personal data electronically in order to provide its services.

Telekom Security ensures the technical and organizational security and other measures in accordance with Article 32 GDPR and by national law pursuant to § 64 of the German Federal Data Protection Act (*Bundesdatenschutzgesetz – BDSG*).

In accordance with DTAG's corporate guidelines, a data protection concept was drawn up for cPKI as part of a mandatory procedure (PSA procedure). This data protection concept summarizes the aspects of the cPKI 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 Chapter 9.3.1 apply to personal data.

9.4.3 Data to be treated as non-confidential

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

9.4.4 Responsibility for the protection of personal data

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

9.4.5 Notification and consent to the use of confidential data

The certificate requester consents to the use of personal data by a cPKI insofar as it is necessary for service provision purposes.

The legal basis for the personal data processed within the cPKI for employees of DTAG, its subsidiaries and holdings, and for contractors who use the cPKI as part of their employment or contractual relationship is provided by Article (1b) letter b of the GDPR and by national law pursuant to § 26 BDSG "Data Processing for Employment Purposes". The use of the cPKI and the processing of personal data required for this are also regulated in a works agreement within DTAG.

Furthermore, all information that is not to be treated as confidential in accordance with Chapter 9.4.3 and for which the customer has not declined publication may be published.

The cPKI publishes data protection information which is available to all end entities on DTAG's intranet.

9.4.6 Disclosure in accordance with legal or administrative processes

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

9.4.7 Other disclosure circumstances

No provisions.

9.5 Intellectual property rights (copyrights)

The following Chapters 9.5.1 to 9.5.4 apply to 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 cPKI 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 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 CP/CPS

This "Certificate Policy (CP)/Certification Practice Statement (CPS)" document is copyrighted, all intellectual property rights are owned by Telekom Security. Any other use (e.g., duplication, use of texts and images, changes, or creation of a comparable or derived document, transmission to persons who are not interested in the service described in this document), including as excerpts, is subject to the express prior written consent of the publisher of this document (see Chapter 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 trusted hardware and software components.

Key material that the customer or its end entities generated themselves remains the property of the customer. This also applies to key material on MyCards that the customer has purchased.

9.6 Assurances and guarantees

9.6.1 Representations and guarantees of the certification authority

DTAG's "cPKI" 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 defined the responsibilities.

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

The certification instance has a documented agreement and current contractual relationship that supports the provision of the PKI service with regard to delivery or other agreements with third parties. The CA is operated by Telekom Security, and there will be no outsourcing of operating functions.

Telekom Security commits to the following:

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

Furthermore, Telekom Security guarantees that, at the time a [CAB-BR]-compliant certificate is issued, the following applies:

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 the requester has a relevant power of attorney that was issued by a person or an organization that has the right to this use.
2. The procedure described under 1) is followed.
3. The procedure described under 1) is specified in detail in this CP/CPS.
4. A defined procedure is followed to ensure that the certificate holder (subject) named in the certificate has approved the issuing of the certificate as well as that the requester's representative is authorized to make the request.
5. The procedure described under 4) is followed.
6. The procedure described under 4) is specified in detail in this CP/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.
9. The procedure described under 7) is specified in detail in this CP/CPS.
10. A defined procedure is followed to minimize the probability that the OU field of the Subject DN contains misleading information.
11. The procedure described under 10) is followed.
12. The procedure described under 10) is specified in detail.

The Telekom Security Trust Center additionally guarantees that:

13. In the event that the certificate owner belongs to an affiliated company or acts in the name of such a company on its behalf, the requester's representative must accept the "Terms of Use" before the certificate is issued.
14. 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.
15. 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.
16. The issued certificates will be revoked in the event of all reasons listed in the [CAB-BR].
17. 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 toward the customer for the operation of the cPKI.

9.6.2 Assurances and guarantees of the registration authority

Registration authorities commit to the following:

- To use the certificate of the registration authority (and its derivatives, Chapter 1.3.2) 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 authentication 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 specified by the customer and does not contradict the provisions of this CP/CPS
- To bear the legal consequences resulting from non-compliance with the obligations described in this Certificate Policy (CP)/Certification Practice Statement (CPS)
- To revoke the secret key at the request of the end entity or an authorized deputy in the event of loss or a suspected compromise
- That all certificates comply with the essential requirements of this document
- That the revocation functionalities and the use of the CA database (directory service, OCSP responder) comply with all essential requirements of this Certificate Policy (CP)/Certification Practice Statement (CPS)

Telekom Security reserves the right to agree other obligations, assurances, consents, and guarantees toward the customer for the operation of the cPKI.

9.6.3 Assurances and guarantees of the trusted database

The trusted databases commit to the following:

- To provide proof of the authenticity of data in the end-entity certificate request for users
- To conduct regular audits with the Internal Control System (ICS IT) by external auditors
- To implement and release in a PRIVACY & SECURITY ASSESSMENT (PSA) procedure
- To implement penetration tests by Telekom Security experts
- To certification in accordance with ISO 27001

9.6.4 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 legal persons or 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 legal persons or devices, the certificate contents are checked by authorized persons.
- To bear the legal consequences arising from non-fulfillment of the obligations described in this CP/CPS
- To ensure that their devices do not interfere with the technical interfaces of the cPKI (role-specific websites, LDAP, SCEP, email, OCSP, CRL) when applying for and issuing certificates as well as when validating certificates
- To arrange for/carry out the revocation of the corresponding end-entity certificate in the event of loss or suspected compromise of the secret key, significant changes to the certificate information, or suspected misuse
- In the event that the private key is compromised, use of the certificate holder'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 CP/CPS and do not contradict the provisions of this statement
- That the end entity is in fact an entity and does not carry out any CA functions, such as signing of certificates or revocation lists, with its private key assigned to the public key contained in the certificate

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

9.6.5 Assurances and guarantees of the key owners of function and group certificates

The key owner commits to the following:

- To identify and authenticate the group members
- To prove to the Trust Center that they are the owner of the function or group mailbox and thus the key owner
- That when handing over their responsibility to a new key owner, the guidelines for managing the key and the certificates are observed, such as the retirement of a group member, for example
- To inform all necessary offices within the organization as well as the Trust Center about the change or to ensure that the change is documented in the electronic systems connected to the Trust Center and that the current key owner can be retrieved
- To inform all other key owners (group members) of the obligation to comply with the special regulations for group certificates
- In the case of automated IT processes, to ensure the secure use of group certificates on the basis of this CPS, the compliance, data protection and security requirements of DTAG and, if necessary, a security concept
- To take responsibility for the revocation of the group certificates in accordance with the policy of the issuing CA and the specifications for group certificates and to carry it out if necessary
- After a group member has left, to check the risks of unauthorized access to the secret key. It ensures that misuse of the secret key and certificate by the retired group member is prevented. Since the corresponding secret key and the certificate for the group function account are written to the respective personal smartcards of the group members, the key owner must ensure that the corresponding secret key and certificate on the smartcard of the retiring group member is removed (deleted) by the key owner. If it is not possible or not successful to delete the secret key and the certificate, the key owner must check whether withdrawal of access to the application/mailbox or the secured data is sufficient or whether a key change is necessary. If required, the key owner then initiates the revocation or renewal of the function or group certificate. If necessary, misuse can also be prevented by the supervisor confiscating the personal smartcard (MyCard).
- If misuse of the key is feared or if compromise of the key material is suspected, to immediately revoke the certificate and immediately inform DTAG's Corporate Security department and Telekom Security' Trust Center of this incident.
- To take into account that a key change affects encrypted archived documents of the entire group and ensures the availability of these documents

9.6.6 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 no technical interfaces of the cPKI are affected during certificate validation (role-specific web pages, LDAP, SCEP, email, OCSP, CRL).

9.6.7 Assurances and guarantees of other subscribers

No Stipulation.

9.7 Disclaimer

Telekom Security shall always be liable to the customer

a. for any damage caused by willful intent or gross negligence on the part of Telekom Security or its legal representatives or vicarious agents;

b. in accordance with the Product Liability Act (*Produkthaftungsgesetz*);

c. for damage arising from loss of life, bodily injury, or damage to health caused by the provider or its legal representatives 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 (including damage to image) that occurs due to misused certificate content (Chapter 4.5.1, 5.8) or misuse of trademarks or trademark rights (Chapter 3.1.6) is at the expense of the customer.

9.8 Limitations 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 damage and financial losses 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 contract year. If a recurring payment is agreed upon, the 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 contract 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 Chapter 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 – shall be limited to a total of EUR 2.5 million. Liability as stipulated under Chapter 9.7 letter 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 Chapter 9.8.1.

In the event of loss of data, T– Systems 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, Chapters 9.7 and 9.8 shall apply accordingly.

9.8.2 Liability of the certificate holder

The certificate holder (certificate owner) 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 Chapters 9.7 and 9.8 et seq. shall apply to any claims for damages.

9.10 Term and termination

9.10.1 Term

The initial publication of this "CP/CPS" document as well as modifications to this document come into force at the time of publication on public Telekom Security websites (see Chapter 2.3).

9.10.2 Termination

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

9.10.3 Effect of termination and continuance

If the cPKI service is terminated, the customer and the users of the end-entity certificates issued there continue to be bound by the rules in the CP/CPS until the last certificate issued becomes invalid or is revoked.

9.11 Individual messages and communication with subscribers

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

9.12 Changes to the CPS

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 Procedure for amendment

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

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

Updated versions of this document result in the previous document versions becoming invalid. In the event of contradictory provisions, Telekom Security will decide on how to proceed.

Within existing contracts, the customer commissioning the operation of the CPKI must be informed about modifications to this CP/CPS in writing at least six weeks before they come into force. In the event of changes to the disadvantage of the customer, these shall be agreed upon with the contractor; exceptions to this shall be changes for which the Trust Center is not responsible (e.g., changes to specifications of the CAB BR or legal specifications). If the customer commissioning the operation of the cPKI does not object in writing within six weeks of receipt of the notification of change, the changes shall become part of the agreement effective at the time they take effect.

9.12.2 Notification procedures and periods

The contact persons designated in connection with individual contractual provisions shall be informed of any changes and shall be given the opportunity to lodge an objection within six weeks. If no objections are made, the new document version enters into force after the end of this period. Any claims beyond this for individual end users to be notified are explicitly excluded.

If Telekom Security is of the opinion that, for example, significant security-relevant amendments are required immediately, the new CP/CPS will enter into force immediately upon its release (see Chapter 9.12.1).

9.12.3 Reasons that lead to the object ID having to be changed

The Telekom Security Advisory Board decides whether the object ID of the CP/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 Bonn.

9.15 Compliance with the applicable law

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

9.16 Various provisions

9.16.1 Entire agreement

No Stipulation.

9.16.2 Assignment

No Stipulation.

9.16.3 Severability

Should any provision of this CP/CPS be or become invalid or unenforceable, this shall not affect the validity of the remainder of this CP/CPS. Instead of the invalid and unenforceable provision, a provision is deemed to have been agreed which comes closest to the economic purpose of this document in a legally effective manner. The same applies to additions made in order to close contractual lacunas.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No Stipulation.

9.16.5 Force majeure

The individual contractual provisions agreed with the customer shall apply.

Within the legally permissible framework, contracts with customers, 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 customers, relying third parties, or end entities that it 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

Access to the TC services of DTAG's corporate PKI is essentially browser-based. Operating systems offer a multitude of different accessibility features to make it easier for disabled persons to access the web portals of the Trust Center services. These compensate in particular for visual and hearing impairments, physical impairments, and perception disorders (e.g., "Information on accessibility for IT experts").

For the software and web portal used by the corporate PKI, there is an accessibility certificate from Telekom Security Multimedia GmbH dated March 4, 2014, in which accessibility is confirmed.

The independent and accredited Test and Integration Center (TIC) of Multimedia GmbH conducted an accessibility test with the aim of assessing accessibility. The application is used to set up and manage certificates and data under DTAG's corporate PKI.

In order to improve the accessibility of the contents of the application for persons with physical or motor

limitations, the assistive technologies and tools used by these user groups were first empirically examined for compatibility with the application (assistive technologies). Then a check for conformity with currently recognized standards and applicable legal guidelines was performed. Any test criteria that were not met were weighted according to severity and relevance as accessibility barriers, accessibility hurdles, or minor accessibility limitations.

User groups considered:

- Visually impaired users (S)
- Blind users (B)
- Users with motor disabilities (M)
- Deaf users (G)

The requirements used for the accessibility test are based on the Accessible Information Technology Ordinance according to the Disability Discrimination Act (*Behindertengleichstellungsgesetz – BGG*).

The Accessible Information Technology Ordinance (BITV 2.0) has various requirements that an application must meet to ensure accessibility for persons with disabilities. These requirements are divided into two priority levels and are largely based on the Web Content Accessibility Guidelines (WCAG 2.0).

When assessing desktop applications, the Guidance on Software Accessibility (DIN ISO 9241-171) was additionally used.

In addition, analyses are carried out with the SW development partners of the Trust Center to determine whether there are other meaningful, operating system-independent options for designing accessibility in addition to the standard board resources.

If the above measures are not sufficient, Telekom Security also offers free telephone support to disabled people to assist them in applying for, accepting, and revoking certificates.

A Supplementary literature

A.1 Basic documentation

- Service specifications (SS)
- Service level agreement (SLA)
- Framework SLA for Trust Center services
- Definitions of terms and acronyms
- Personnel, infrastructure, and technical framework conditions

A.2 Role-specific manuals

- User manual
- Operating manual

B Key

✓ Feature available
× Feature not available

C Acronyms and definition of terms

C.1 Acronyms

AIA	Authority Information Access
BNetzA	German Federal Network Agency for Electricity, Gas, Telecommunications, Post, and Railways (*Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*)
BR	Baseline Requirements
BSI	German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*)
C	Country
CA	Certification Authority
CAA	Certification Authority Authorization
CAB	CA/Browser Forum
CARL	Certification Authority Revocation List
cc	Country Coded
CN	Common Name
CP	Certificate Policy
cPKI	Corporate Public Key Infrastructure of DTAG
CPS	Certification Practice Statement
CN	Common Name
CRL	Certificate Revocation List
CT	Certificate Transparency
DIN	German industry standard (*Deutsche Industrie Norm*)
DK	Dual Key
DN	Distinguished Name
DNS	Domain Name Systems
GDPR	General Data Protection Regulation
DTAG	Deutsche Telekom AG
DV	Domain Validation
ECC	Elliptic Curve Cryptography
EDP	Electronic data processing
eIDAS	electronic Identification and Signature
ERP	Enterprise Resource Planning
ETSI	European Telecommunications Standards Institute (*Europäisches Institut für Telekommunikationsnormen*)
FIPS	Federal Information Processing Standard

FQDN	Fully Qualified Domain Name
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 (*Leistungsbeschreibung*)
LDAP	Lightweight Directory Access Protocol
MTO	Maximum Tolerable Outage
NCP	“Normalized” Certificate Policy
NIC	Network Information Center
n/a	not available
O	Organization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
opt.	optional
OU	Organization 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
PROD	Productive Unit (live environment)

PTC	Publicly-trusted certificate
RA	Registration Authority
REST	REpresentational State Transfer, API for Application Programming Interface
RFC	Requests for Comments
RSA	Rivest Shamir Adleman
RTO	Recovery Time Objective
S	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
S/MIME	Secure Multipurpose Internet Mail Extension
SCT	Signed Certificate Time Stamp
SHA	Signature Hash Algorithm
SigG	German Digital Signature Act (*Signaturgesetz – SigG*) (repealed on July 29, 2017 and replaced with the Trust Services Act (*Vertrauensdienstegesetz – VDG*) and eIDAS)
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
CAST	Test and acceptance environment
UPN	User Principal Name
URL	Uniform Resource Locator
UPS	Uninterruptible Power Supply
UTC	Universal Time Coordinated
XML	Extensible Markup Language

C.2 Definition of terms

Abbreviation	Description
Functional mailboxes (FMB)	Functional mailboxes are mailboxes for function groups. FMBs do not have their own AD account, but a manager, also known as the owner, can manage the FMB using his personal AD account and is authorized to submit certificate applications for the FMB in which he is registered as a manager.
Persons and function groups	A person and function group account has the feature that its name, which is maintained in SAP HR, does not indicate who is working with the account or the underlying certificate. This can happen in the organization e.g. for training accounts or function accounts. One requirement is that such accounts must follow a certain nomenclature in order to be identifiable and that the responsible user (key owner) behind this account can be easily identified.
Pseudonym account (PN)	A pseudonym account has the feature that the name of the certificate holder in the certificate does not correspond to the name in the official ID document. However, the Trust Center has the option in SAP HR to determine at any time who is hiding behind the pseudonym name. Another requirement is that such accounts have to follow a certain nomenclature in order to be identifiable
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 or legal person who requests a certificate (or its renewal). Once the certificate has been issued, the requester is referred to as the certificate owner. 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.
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.
Issuing certification authority (CA)	The certification authority (CA) that issued a specific certificate. This could be a root certification authority (root CA) or a subordinate certification authority (sub-CA).
Authentication	Checking an identity based on claimed characteristics.
Certification Authority (CA)	See Certification authority.
Certification Authority Authorization (CAA)	A procedure that allows the domain owner to specify in the DNS which certification authority (or authorities) can issue certificates for its domain(s).
Certification Authority Revocation List (CARL)	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.

Abbreviation	Description
Certificate policy (CP)	Defines the guidelines for generating and managing certificates of a certain type.
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 Revocation List (CRL)	See Revocation list.
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 MyCard. Smartcards can also be used for cryptographic applications.
Digital signature	A checksum created with a special mathematical procedure. Guarantees the authenticity of the signatory and the integrity of the data.
Distinguished Name	Format with which distinguished names can be specified in accordance with the X.500 standard. A digital certificate must contain a DN.
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.
eIDAS	EU regulation on electronic identification and trust services. The eIDAS Regulation contains binding Europe-wide regulations in the areas of "electronic identification" and "electronic trust services." The Regulation establishes a common framework for the cross-border use of electronic means of identification and trust services. As an EU regulation, this is directly applicable law in all EU member states as well as in the European Economic Area.
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.
Certification Practice Statement (CPS)	One of several documents that provide general and specific framework conditions. This contains, in particular, a description of the procedure the certification authority (CA) follows for issuing, managing, revoking, and renewing certificates.
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.
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. The cPKI is certified in accordance with Policy LCP

Abbreviation	Description
EU GDPR	The General Data Protection Regulation (GDPR) is a European Union regulation that harmonizes the rules on the processing of personal data by private companies and public bodies throughout the EU. On the one hand, this is intended to ensure the protection of personal data within the European Union and, on the other hand, to ensure the free movement of data within the European single market. The Regulation replaces Directive 95/46/EC of 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
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 a host name, an IP address, or an email address in the commonName field (CN) of the certificate holder's (subject's) distinguishedName and/or in at least one subjectAltName extension.
Valid certificate	A certificate that passes the validation procedure described in RFC 5280.
Period of validity	The period from the issue date (not before) until the expiry date (not after).
Hardware Security Module (HSM)	Hardware to generate and store private keys securely.
Hash value	In this context, a fixed length cryptographic checksum (the correct name is cryptographic hash value). It should be as unlikely as possible to calculate the entry from the hash value or to find several possible inputs for the same hash value (hash value is used as a synonym for fingerprint). In most cases a hash value is signed instead of a complete digital document.
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 server name	A server name (which may or may not contain a registered domain name) that cannot be dissolved with the public Domain Name System (DNS).
Issuer Distinguished Name (Issuer DN)	Format with which distinguished names can be specified in accordance with the X.500 and LDAP standards. The Issuer DN describes the CA issuing the certificate in a unique way.
Legal person	A company, group, partnership, sole trader, trust, government authority, or legal entity with legal standing within the legal system of a country.
Key backup	Mechanism for backing up keys. In order to be able to restore encrypted emails 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 history	Key protection mechanism that allows access to existing encrypted electronic documents or emails after changing the MyCard or reissuing certificates.
Key recovery	Mechanism for recovering keys. This can be necessary if users lose their key (such as through a damaged file).

Abbreviation	Description
Compromise	A private key is compromised if it is made known to unauthorized persons or can be used by them. A compromise could occur through a criminal attack, for example.
Cryptography	Science dealing with the encryption of data and related issues (such as digital signatures).
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.
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.
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 offers more options than HTTP and FTP (such as setting up a context that can be maintained using several queries). LDAP is used in particular to query digital certificates and revocation lists within public key infrastructures.
Mail security	Security functions such as digital signature and encryption that support standard email applications.
Information security management system (ISMS)	The information security management system (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 tenants on one installation. The respective tenants (e.g., legal units or companies) are unable to view the data, user administration or similar of the other parties/tenants.
MyCard	See Smartcard
Non-registered domain name	A domain name that is not a registered domain name.
Terms of Use	Provisions regarding safekeeping and permitted usage of an issued certificate in accordance with the specified requirements if the requester/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 applications. Also see Online Certificate Status Protocol (OCSP).

Abbreviation	Description
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.
One Time Password (OTP)	Password that is valid once
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 MyCard 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.
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 Infrastructure (PKI)	Hardware, software, persons, procedures, rules, guidelines and obligations that enable certificates and keys to be generated, issued, managed, and used reliably based on the public key cryptography.
Public Key Infrastructure X.509 (PKIX)	IETF standard that standardizes all relevant parts of a PKI.
Policy	Guidelines or explanation that determine(s) the security level for creating and using certificates. A distinction is made between Certificate Policy (CP) and Certification Practice Statement (CPS).
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 MyCard and is protected by a password or a PIN.
Pseudonym account	A pseudonym account is characterized by the fact that its name maintained in the SAP HR system does not indicate who is working with the account or the underlying certificate. This can occur in the organization, e.g., for training accounts or function accounts. One requirement is that such accounts must follow a certain nomenclature in order to be identifiable and the responsible user (key owner) can be easily identified behind this account.
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.
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.

Abbreviation	Description
Root CA	See Root certification authority.
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 customer who is responsible for the proper use (distribution, use and, if necessary, revocation) of the key pair and certificate that was issued for a group of persons or functions, legal person, or device.
Secure Multipurpose Internet Mail Extension (S/MIME)	Secure Multipurpose Internet Mail Extension. Extension of the MIME email format, which describes additions for cryptographic services that guarantee the authenticity, integrity, and confidentiality of messages.
Secure Socket Layer (SSL)	Crypto protocol for ensuring end-to-end connections on the Internet. Can be used instead of the more complex IPsec in many cases.
Service Desk	The Service Desk is an organizational unit within a company that serves as the customer'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. Also see MyCard.
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, legal person, or device. Authorization takes place via the certificate revocation password.
Revocation authority	An employee (staff member) or representative of an organization who performs certificate revocations.
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).
Statement of Auditing Standards 70 (SAS 70)	Statement of Auditing Standards (SAS) No. 70 titled "Service Organizations" – this is an internationally recognized standard that was created by AICPA.
Subject Alternative Name	Additional fields in a certificate. The fields can be used to enter additional names of the certificate owner and are a standard extension of the X509 standard.
Subject Distinguished Name (Subject DN)	Format with which distinguished names can be specified in accordance with the X.500 and LDAP standards. The Subject DN uniquely specifies a person or device.

Abbreviation	Description
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.
Suspension	In connection with the PKI, suspension means a provisional or temporary revocation. The certificate initially appears in the certificate revocation list but can be re-activated by the sub-registration authority.
Transport Layer Security (TLS)	Crypto protocol for ensuring end-to-end connections on the Internet.
Triple key certificate	Variant in which separate key pairs are used for encryption, signing, and Microsoft MyCard logon. This means the user has three corresponding certificates.
Telekom Security Advisory Board	A board within Telekom Security that decides on PKI functions.
Subordinate certification authority (sub-CA)	A certification authority whose certificate is signed by a root certification authority (root-CA) or another intermediate certification authority (sub-CA).
Validation	Evidence of the reproducibility of a result from a described procedure under defined conditions. The more precisely a procedure is described and the fewer unknown influencing factors there are, the more certain it is that corresponding results will be produced. A description of the goal and method is required for a validation. In this context, valid means that the method leads to the result in a repeatable manner. In the context of a PKI, there is a validation process at the following points: ▪ 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).
Validation specialist	Someone who performs the data validation tasks in accordance with the requirements in question. In the context of the cPKI, this is the role owner. Trust Center operator
Affiliate	For example, a company, partnership, joint venture, corporation, (capital) company, association, foundation, or other organization (legal person) that supervises, is supervised by, or is controlled together with another organization (legal person), facility, department, governmental unit, or unit that is directly subordinate to a governmental authority.
Relying parties	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.
Trusted certificate	A certificate that is trusted due to the fact that its corresponding root certificate represents a trust anchor in widely distributed application software.

Abbreviation	Description
Requester's representative	If different from the requester, a natural person or cost object, an employee of the requester, or an authorized representative who has the express authority to represent the requester: (i) who signs, submits, or approves a certificate request 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 terms of use in the name of the requester if the requester is an affiliated company (affiliate) of the certification authority (CA).
Directory service	Data repository for calling up certificates and certificate validation information (revocation list).
Fully qualified domain name (FQDN)	Correct and complete domain name, i.e., a chain of all labels for a path in the domain name space (for further information see RFC 2181).
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 cPKI.
X.509	Standard, whose most important element is a format for digital certificates. Certificates of version X.509v3 are supported in all common public key infrastructures.
Central repository	An online database that contains public PKI documents (e.g., Certificate Policies, Certificate Practice Statement, CA certificates) as well as additional information, either in the form of a CRL or an OCSP response.
Certificate	An electronic document that uses a digital signature to bind a public key to an identity (e.g., person, device).
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.
Certificate holder	A natural or legal person who is issued a certificate and is legally bound by a subscriber agreement or terms of use.
Certificate request	A request made in electronic or written form that contains data regarding a requester.
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 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 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 sub-CA certificates.
Certificate administration process	Processes, practices, and procedures relating to the use of keys, software and hardware that the certification authority (CA) uses to check certificate data, issue certificates, maintain a central data repository, and revoke certificates.
Certificate 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.

Abbreviation	Description
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).
Area of responsibility	Hierarchically subordinated sub-section of the master domain that is managed by a sub-registrar.
Reliable 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 requester.

C.3 References

[CAB-BR] Version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" document published by CA/Browser Forum at http://www.cabforum.org/documents.html valid at the time

[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 DTIRCA1] CP or CPS of the Deutsche Telekom Internal Root CA 2

[ETSI LCP] 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 LCP http://www.cabforum.org/documents.html

[ETSI EN TSP] ETSI EN 319 401 V2.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures

[EU GDPR] European General Data Protection Regulation 2016/679, entered into force on May 25, 2018

[ISAE 3402] ISAE3402 Report, International Standards for Assurance Engagements, http://isae3402.com/ISAE3402_reports.html

[PITR cPKI] Personnel, infrastructure, and technical framework conditions of the TDTAG corporate PKI (cPKI)

[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

[RFC 2560] X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol – OCSP

[RFC 3647] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Network Working Group, IETF, 2003

[RFC 5280] 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

[Siko cPKI] cPKI security concept

[SRK TC] Security framework 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