

Service and Usage Agreement TeleSec Shared Business CA

Please read these Service and usage agreement carefully. Only request a certificate if you agree to these Terms of Use.

If you do not agree to these Terms of Use you may neither request nor accept or use a certificate.

These Service and usage agreement refer to the applicant / certificate holder / authorized person who receives the certificates from the PKI service "TeleSec Shared Business CA " within a PKI tenant (requested, issued, revoked, renewed).

The provider (TSP) named in Chapter 2.1 is responsible for the operation of this Public Key Infrastructure (PKI).

1 Introduction

1.1 General

The PKI service "TeleSec Shared Business CA" issues certificates for various purposes (e-mail, VPN, server, etc.), based on the X.509v3 standard. Depending on usage, the "TeleSec Shared Business CA" uses different intermediate certification authorities (intermediate CAs), which are hierarchically subordinated to a public or internal root CA.

This document represents the "Service and Usage Agreement of TeleSec Shared Business CA", which is contained in the product portfolio of Deutschen Telekom Security GmbH.

In the relevant literature, the terms "terms and conditions" or "terms of use" can also be found for this document.

1.2 Definition of terms

What is a certificate?

An electronic document that uses a digital signature to bind a public key generated for cryptographic purposes to an identity (e.g. person, device).

Applicant/certificate holder/authorized person

The natural or legal person who requests a certificate (or its renewal). Once the certificate has been issued, the applicant is called "certificate holder" and is legally bound by the Service and usage agreement.

In the case of certificates issued for devices, the applicant is the organization that controls or operates the device listed on the certificate, even if the device sends the actual certification request. Frequently, device certificates are requested via an authorized person (e.g., administrator) and installed on the component.

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 or device.

2 Service component TeleSec Shared Business CA

2.1 Trust Service Provider contact info

Trust Service Provider (TSP) Deutschen Telekom Security GmbH can be reached via the following contacts:

Address: Deutschen Telekom Security GmbH
Trust Center & ID Solutions
Untere Industriestraße 20
57250 Netphen
Germany

Phone: +49 (0) 1805-268204 ¹
E-Mail: telesec_support@t-systems.com
Internet: <https://www.telesec.de>

Cases of certificate misuse can be reported by:

Phone: +49 (0) 1805-268204 ²
eMail: telesec_support@t-systems.com
Internet: <https://www.telesec.de> "Contact | Suspected abuse of certificate"

2.2 Certificate types, validation procedures and key usage

With the PKI service TeleSec Shared Business CA, Deutschen Telekom Security GmbH shall provide a multitenant company public key infrastructure (PKI), which the customer may use to issue and administrate (revoke, renew) his own digital certificates according to the X.509v3 standard for a wide range of applications (such as e-mail security (S/MIME), VPN, client-server authentication, Microsoft domain registration).

The following certificate types are provided as standard:

- Users (key division: single, dual, triple key)
 - For natural persons, groups of people and functions, pseudonyms
- Server
- Mail gateway
- Router/gateway
- Domain controller

Depending on the respective certificate types, the Shared Business CA provides the following certification authorities:

Public Certification Authority

- T-TeleSec GlobalRoot Class 2 (RSA, SHA-256, October 1, 2008 – October 1, 2033)
 - TeleSec Business CA 1 (RSA, SHA-256, November 29, 2012 – November 29, 2014)

The following types of certificates can be issued under a public certification authority, which is subject to ETSI certification every year (see Chapter 2.6):

- User (key separation single, dual, triple key (except SmartCard LogOn))
- Server
- Mail gateway

Internal Certification Authority

- Deutsche Telekom Internal Root CA 1 (RSA, SHA-1, November 15, 2007 – November 15, 2027)
 - Internal Business CA 2 (RSA, SHA-256, February 11, 2014 – November 15, 2027)
 - Business CA (RSA, SHA-1, November 8, 2011 – November 9, 2023)
- Deutsche Telekom Internal Root CA 2 (RSA, SHA-256, August 3, 2017 – August 3, 2039)
 - Internal Business CA 3 (RSA, SHA-256, August 3, 2017 – August 3, 2029)
 - Internal Business CA 5 (RSA, SHA-256, September 10, 2019 – September 10, 2031)

All of the above certificate types can be issued under an internal Deutschen Telekom Security GmbH certification authority.

The certificate extensions "key usage" and "extended key usage" as well as the „validity period“ of the certificates depends on the certificate type and the requirements / regulations (e.g., root programs of the operating system and browser manufacturers, baseline requirements of the CA/Browser Forum) for the operation of public certification authorities.

All of the certificates mentioned support the use of keys that are required to create a digital signature and encryption. Depending on the certificate type, Secure E-Mail, Client Authentication, Server Authentication and Smartcard-LogOn are available as "Extended Key Usage".

Certificates issued by a public certification authority are valid for a maximum of 36 months. An exception applies to server certificates with a maximum validity of 13 months from the date of issue September 1, 2020.

Certificates issued by an internal certification body are valid for a maximum of 60 months.

The certificate management process (issuance, renewal, and revocation) of all certificate types, the validation process, and key uses are described in detail in the Certificate Policy (CP) and Certification Practice Statement (CPS).

The currently valid document and all previous versions are available on the Internet at: <https://www.telesec.de/en/service/downloads/pki-repository/>

2.3 Availability of the service

The infrastructure of the Shared Business CA PKI service installed in the Trust Center comprises the following components:

- A certification authority (CA) which is accessible via an online web portal,
- The LDAP directory service, used to call up revocation lists (CRLs, ARLs), end-subscriber certificates (if these are to be published), and CA and root CA certificates,
- The OCSP online validation service, and
- the mail server.

As a monthly average the

- certification authority and web server are available 98.0 percent of the time.
- directory service is available 98.0 percent of the time.
- online validation service is available 98.0 percent of the time.
- the mail server is available 98.0 percent of the time.

2.4 Privacy policy

Within the Shared Business CA, Deutschen Telekom Security GmbH must store and process personal data electronically in order to provide its services.

If Deutschen Telekom Security GmbH is to process sensitive data in the meaning of Article 9 of the General Data Protection Regulation (GDPR) [EU GDPR], the customer must notify Deutschen Telekom Security GmbH of this in writing without undue delay.

2.4.1 Log events

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

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

Here the requirements under [ETSI EN TSP] Section 2.4.2.1 are implemented.

In the certificate history, all relevant events are recorded and integrity-protected archived, from the request process through the registration, the verification by the TSP, the production up to the publishing and, if necessary, the revocation.

2.4.2 Data archiving

2.4.2.1 Type of archived datasets

Deutschen Telekom Security GmbH archives the following data:

- Order documents on paper or electronic form (e.g., quotations, orders) when applying for a certificate for the first time and, if necessary, when renewing a certificate,
- Information in certificate requests (History) and regarding the certificate life cycle (e.g., revocation and renewal requests),
- Soft PSEs that were requested in bulk.
- Soft PSE of the encryption certificate that has been generated with smartcard personalization (triple key only),
- All audit/history data/event logging files recorded pursuant to Section 2.4.1.

2.4.2.2 Storage period for archived data

The following records and storage periods are stipulated:

- Order documents, in particular information regarding certificate requests, their validation and the certificates resulting from this and revocations executed are retained for seven (7) years after the certificate validity expires. This also applies to further certificate renewals.
- Audit, history and event logging data are archived up to forty-two (42) days.

2.5 Reliance limits

Deutschen Telekom Security GmbH does not set any reliance limits for the certificates it issues.

2.6 Auditing

The TeleSec Shared Business CA is subjected to a regular annual audit (ETSI EN 319 411-1, policy OVCP, and policy NCP) by independent third parties. The subject of certification is the PKI infrastructure as well as all processes that are used to apply for, issue, revoke and

renew end user certificates in connection with a public certification authority (currently TeleSec Business CA 1).

2.7 Liability exclusion, Limitation of liability

The certification authority is liable indefinitely for damage resulting from injury to life, body and health, as well as for damages resulting from intentional breaches of duty.

Apart from that, the liability for damage resulting from negligent breach of duty is regulated in the current version of Certificate Policy (CP) and Certification Practice Statement (CPS) in chapter 9.7 and 9.8 or General Terms and Conditions TeleSec-products or individually negotiated.

2.8 Applicable and contractual agreements

The following documents and files are available online under

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

<https://www.telesec.de/en/service/downloads/products-and-solutions/> :

- This document (Service and Usage Agreement TeleSec Shared Business CA)
- Certificate Policy (CP) / Certification Practice Statement (CPS) (Repository, current version and previous versions)
- PKI Disclosure Statement (PDS)
- Service description
- General Terms and Conditions TeleSec products
- All certificates of the root and intermediate certification authority (root and sub-CAs)
- All current certificate revocation lists (CRLs) and revocation lists of the certification authorities (CARLs)

2.9 Applicable law, complaints and dispute resolution

2.9.1 General

German law applies. In the case of disputes, the parties shall reach an agreement, taking into account made agreements, regulations and applicable laws. Place of jurisdiction is the seat of Deutschen Telekom Security GmbH in Bonn, Germany.

2.9.2 Extrajudicial settlement (Dispute settlement)

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

3 Obligations of subscribers

The applicant or certificate holder, the authorized person, or the key owner who requests and administrates one or more certificates for an end entity or a device undertakes:

- To correctly and in full provide the details of a natural person in the certificate request; the name and title must be evidenced in accordance with a valid proof of identity or another reliable data source. Where groups of persons and functions, or devices are concerned, the certificate will be requested by authorized persons or key owners.
- To check that the certificate contents included in the end-user certificate reflect the truth.
- The certificate(s) issued must be used solely as intended and for authorized and lawful purposes which are in line with the rules of the Certificate Policy (CP) and the Certification Practice Statement (CPS) of the Shared-Business-CA PKI service.
- To neither misuse the certificate nor act contrary to the rules of the aforementioned CP/CPS.
- To bear the legal consequences arising from non-fulfillment of the obligations described in the aforementioned CP/CPS.
- To use the keys and certificates only in the approved applications; the application must conform to the kinds of key usage set out in the certificate.
- Not to use the certificate(s) with applications or machines whose functions seem to be unknown, suspicious, or unreliable.
- To protect the private key appropriately and against unauthorized access and not to disclose it, and, in particular, to implement the requirements for technical protection measures for the private key. In the case of private keys of legal persons or devices, the protection is provided by authorized persons and key owners.
- To ensure 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.
- To ensure that every digital signature is made with the key material of a valid certificate that has not been revoked.
- To genuinely act as the end entity and not to carry out any CA functions, such as signing certificates or revocation lists, with its private key assigned to the public key contained in the certificate.
- To change the PINs of the smartcard or, where the secure use of the private key of a software certificate is concerned, the password at certain time intervals.
- To change the PIN or password immediately if there is any suspicion that someone may have discovered the PIN or password.

- To stop using the private key upon expiry of the validity of the certificate or upon its revocation, except for decryption.
- If the private key and/or PIN is lost, or if it is presumed to have been compromised or manipulated, if significant changes have been made to the details of the certificate, if its use has been discontinued (e.g., termination of contract), or in the case of presumed misuse, to revoke the end-user certificate in question or to have it revoked.
- In the event that the private key is compromised, the use of the certificate owner's private key must be ceased immediately and permanently.
- To stop using the certificate if it becomes known that the certificate of the certification authority has been compromised.

3.1 Prohibited usage of certificates

SBCA certificates must not be used for the following purposes:

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

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

3.2 Recommendation, advice

In addition, the end entity is advised:

- To ensure that the computer's software is up-to-date at all times.
- To use up-to-date anti-virus and firewall software.
- To protect the computer against unauthorized access by using passwords for BIOS, screen savers, etc. or by using a smartcard.
- To only ever sign information whose content has been checked beforehand.
- If in doubt about the creation of the electronic signature, to check it once more before sending it.

4 Certificate status checking obligations of relying parties

Trusting third parties must themselves have sufficient information and knowledge to assess the handling of certificates and their validation. The trusted third party is responsible for its decision making, whether the information provided is reliable and trustworthy.

Any trusted third party should therefore

- Check that the information contained in the certificate is correct before using it,
- verify the validity of the certificate by validating, among other things, the entire certificate chain up to the root certificate (certification hierarchy) as well as the validity period and the revocation information (CRLs or OCSP) of the certificate,
- Use the certificate for authorized and legal purposes only in accordance with this CP/CPS. Deutschen Telekom Security GmbH is not responsible for assessing the suitability of a certificate for a specific purpose
- check the purposes specified in the certificate by the attributes "key usage" and "extended key usage".

Trusted third parties must use appropriate software and / or hardware to verify certificates (validation) and the associated cryptographic procedures.

The certificate user, referred to hereunder as the "certificate holder," agrees to the obligations stated in this document and confirms that he will comply with the requirements and regulations set out above.

Place, date _____ Signature _____

A Acronyms and definitions of terms

AGB	Allgemeine Geschäftsbedingung (German law)
BGB	Bürgerliches Gesetzbuch (German law)
CA	Certification Authority
CARL	CA revokation list
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certification Revocation List
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation,
HTTPS	HyperText Transfer Protocol Secure
LDAP	Lightweight Directory Access Protocol
NCP	Normalized Certificates Policy
OCSP	Online Certificate Status Protocol
OVCP	Organizational Validation Certificates Policy
PDS	PKI Disclosure Statement
PKI	Public Key Infrastructur
PSE	Personal Security Environment
RA	Registration Authority
RSA	Asymmetric cryptographic method developed by Rivest, Shamir and Adleman
SHA	Secure Hash Algorithm
TSP	Trust Service Provider
VPN	Virtual Private Network
VSBG	Verbraucherstreitbeilegungsgesetz (german law)