SERVICE DESCRIPTION

TeleSec Shared Business CA

Deutsche Telekom Security GmbH
Version 04.00
Stand October 15, 2021

LIFE IS FOR SHARING.

PUBLICATION DETAILS

PUBLISHED BY

DEUTSCHE TELEKOM SECURITY GMBH
Bonner Talweg 100
53113 Bonn

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

Supervisory Board: Adel Al-Saleh (Chairman)
Management Board: Thomas Fetten (Spokesman), Dr. Klaus Schmitz, Thomas Tschersich

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

Brief summery:	This document describes the Service Description of PKI Service TeleSec Shared Business CA.
File name:	Shared-Business-CA_SD_04.00_EN.docx
Document number:	n.n.
Document title:	Service Description of PKI Service TeleSec Shared Business CA.
Version:	04.00
Valid from:	October 15, 2021
Status:	Release
Classification:	public
Last review:	October 15, 2021
Author:	Telekom Security
Contents reviewed by:	Telekom Security
Approved by:	Telekom Security
Contact:	tc-solutions.lastlevel@t-systems.com

CHANGE HISTORY

VERSION:	LAST REVISED:	EDITED BY:	CHANGES / COMMENTS:
00.10	October 8, 2020	Telekom Security	New Word template, revision of company modification
00.20	October 12, 2020	Telekom Security	QA
01.00	October 12, 2020	Telekom Security	Release of version 01.00
01.01	October 30, 2020	Telekom Security	Compulsory statement and cover sheet
01.02	November 2nd, 2020	Telekom Security	Formatting in an accessible cover sheet
01.10	November 10, 2020	Telekom Security	Revision of the structure
01.20	November 16, 2020	Telekom Security	QA
01.20	November 17, 2020	Telekom Security	Formal QA
02.00	November 17,2020	Telekom Security	Release of version 02.00
02.10	March 2nd, 2021	Telekom Security	Adjustment of chapte 3.2
02.90	March 2nd, 2021	Telekom Security	Formale QA
03.00	March 3rd, 2021	Telekom Security	Release of version 03.00
03.10	October 15, 2021	Telekom Securty	Revision of chapter 3.3 limited SAN Entries
03.90	October 21, 2021	Telekom Security	Formal QA
04.00	October 22, 2021	Telekom Securty	Release of version 04.00

CONTENTS

1 INTRODUCTION

With the TeleSec Shared Business CA PKI service, Deutsche Telekom Security GmbH (hereinafter referred to as DT Security) shall provide a company public key infrastructure (PKI), which the customer may use to issue and administrate (revoke, renew) its own digital certificates according to the X.509v3 standard for a wide range of applications (such as email security (S/MIME), VPN, client-server authentication, or Microsoft domain registration). TeleSec Shared Business CA makes it possible to set up and use a PKI for inhouse identity management within just a few days.

Deutsche Telekom Security GmbH shall provide the customer with the infrastructure and accesses needed to this so that the customer can access the PKI components in DT Security' secure Trust Center from the customer's location.

Note: The product and company names stated in this document are brand names of the respective trademark owners.

2 TELEKOM SECURITY SERVICES

2.1 Provisioning

2.1.1 General

2.1.1.1 Domain concept

The customer is set up as an independent tenant within TeleSec Shared Business CA. Within its tenant, the customer can issue and manage certificates independently and autonomously, depending on the authorizations (entitlement) assigned to it. Within the scope of the TeleSec Shared Business CA, the tenant is also referred to as the master domain and the subdivision into each area of responsibility is referred to as the subdomain. The name of the PKI tenant and of the area of responsibility is an integral component of the requester in the certificate.

This two-stage domain concept thus makes it possible to map the customer's organizational structures.

2.1.1.2 Certification authority

Certificates are usually issued by an intermediate certification authority (also known as sub-CA) which, in turn, is hierarchically governed by a root certification authority (root CA).

Depending on the type or template, the certificate can be issued by an intermediate certification authority that is governed by either a public or an internal root certification authority. The certificate of the "T-TeleSec GlobalRoot Class 2" root certification authority is already preinstalled in many certificate stores and applications as a trusted certification authority (trust anchor). The "Deutsche Telekom Internal Root CA 2" and "Deutsche Telekom Internal Root CA 1" authorities however, require subsequent installation.

2.1.1.3 Registration authority

Before a certificate is issued, the requester (person or device) must be registered. The customer completes the registration itself in compliance with the requirements of the TeleSec Shared Business CA, in principle, stated in the Certificate Policy (CP) and the Certification Practice Statement (CPS). The TeleSec Shared Business CA provides two options.

- **Central registration**
  The certificate for persons and devices (see Item 2.3.1) is issued centrally by the competent subregistrar, once registration has been successfully completed. The subregistrar can also process (approve, reject, or resubmit) certificate requests that are received via SCEP, CMP, or email interfaces (see Item 2.3.2). The stipulations of the registration process are described in the CP/CPS.
- **Local registration**
  The requester (individual) can submit a certificate request from a user website. The competent subregistrar shall carry out the registration according the stipulations of the Certification Practice Statement and approves the request, provided that no objections exist. The certificate is then available to the requester for downloading. The stipulations of the registration process are described in the Certification Practice Statement (CPS).

2.1.2 Initial provision TeleSec Shared Business CA

In order to ensure the fast and straightforward use of the TeleSec Shared Business CA, the initial provision shall include the setup of a PKI tenant (master domain) and the delivery of a basic package of hardware and software components (smartcard reader, driver software), which forms the basis for accessing the Trust Center. The basic equipment supports the customer in issuing a soft

PSE (file consisting of the certificate and a private key) and in attaching certificates to a precoded smartcard (smartcard personalization).

The initial provisioning includes the following services:

- Setup of a customer-specific administrative area (tenant or master domain)
- Provision of a master registrar certification on smartcard for administrating the tenant within the TeleSec Shared Business CA
- Provision of subregistrar certification for administrating the areas of responsibility (subdomains) set up by the customer within TeleSec Shared Business CA
- A class-2 smartcard reader (with keypad)
- The associated CSP software or PKCS#11 module
- Documentation, consisting of the Certification Practice Statement (CPS), the Service Level Agreement (SLA), the installation instructions for the registrar PC, and the role-specific manuals.

The PKI tenant is set up in consultation with the customer.

The basic package is installed on an internet-capable standard PC of the customer.

2.1.3 Provision of certificates

In addition to the individual data about the certificate holder, the requested certificate types always include information about the PKI tenant (master domain) and the area of responsibility (subdomain) (see Item 2.1.1.1). Additional certificate information is documented in the Certificate Policy (CP) and the Certification Practice Statement (CPS).

The certificate validity can be set for one year, two years, or three years and is valid for the relevant configured PKI tenant. Optionally, other validity periods can be configured, which, however, must not violate the requirements of the standardization bodies, and so on.

2.1.3.1 Certificate for natural persons and person and function groups

According to the configuration, only certain certificate bundles can be requested. These are

a) Single key
Consists of a certificate that is suitable for the purposes of key encryption and digital signature. Extended key usage is not set.

b) Dual key
Consists of two separate certificates, one each for the purposes of key encryption and digital signature. Extended key usage is not set.

c) Triple key
Consists of three separate certificates, one each for the purposes of key encryption, digital signature, and smartcard-based login to Microsoft Windows domains. Smartcard login and client authentication are set as the extended key usage.

2.1.3.2 Certificates for devices

a) Server certificates
Server certificates for authenticating web servers in accordance with the SSL/TLS standard

b) Router/gateway certificates
Certificates for use in network components

c) Mail gateway certificates
Domain certificate for use in a mail gateway

d) Domain controller certificates
Certificates are issued for servers that are operated as domain controllers in a Microsoft server domain.

2.1.3.3 Certificates for registration employees including derivatives of the tenant

Registration employees are issued an administration certificate that is to be solely used for the relevant master and subregistrar and their associated activities.

This regulation also applies to the derivatives of the registrar certificates that are used for access to the CMP interface.

2.2 Operation

2.2.1 Trust Center operation

The TeleSec Shared Business CA provides a PKI infrastructure that is operated by competent staff in Telekom Security' highly secure Trust Center according to the provisions of the Service Level Agreement (SLA), the Certificate Policy (CP), and the Certification Practice Statement (CPS).

The customer can issue, revoke, and renew its own certificates within his administrative area (PKI tenant or master domain). The customer is therefore responsible for both key administration and registration.

2.2.2 On premise operation (PITF)

Operation at the customer's premises requires compliance with certain conditions regarding people, infrastructure and technology.

2.2.2.1 General personnel conditions

Further details are described in the document "Personnel, infrastructure, and technical framework conditions (PITF)."

2.2.2.2 General infrastructure conditions

Further details are described in the document "Personnel, infrastructure, and technical framework conditions (PITF)."

2.2.2.3 General technical conditions

2.2.2.3.1 Registrar workstation

Certificates are issued and administered from the TeleSec Shared Business CA via webbased components of a workstation computer (PC), which must meet defined requirements.

Further details are described in the document "Personnel, infrastructure, and technical framework conditions (PITF)."

2.2.2.3.2 General conditions for applications and devices

Further details are described in the document "Personnel, infrastructure, and technical framework conditions (PITF)."

2.2.2.4 Code of conduct for registration authorities

Further details are described in the document "Personnel, infrastructure, and technical framework conditions (PITF)."

2.3 Functions

The TeleSec Shared Business CA service issues certificates for the following subscribers, depending on their functional roles:

- Registration employees of the domain operator (master registrar, subregistrar, and their derivatives (CMP)) as subordinate registration authorities
- Natural persons (end users, pseudonyms) as single, dual, and triple key certificates
- Person and function groups as single, dual, and triple key certificates
- Devices (e.g., machines such as routers, gateways, servers, domain controllers, and mail gateways)

Following successful authentication, certificates are administrated on a role-specific basis (master/subregistrar, user) via SSL-protected websites. The handling of TeleSec Shared Business CA is documented in the Certificate Policy (CP) and the Certification Practice Statement (CPS).

2.3.1 Certificate administration via role-specific websites

The customer accesses the TeleSec Shared Business CA website via an SSL-secured internet connection (HTTPS protocol). Only upon successful authentication (access control) can the customer's role holder use his specific TeleSec Shared Business CA functions. The customer can use the following range of functions, depending on the assigned role.

a) Website for the "Master registrar" role
For administrating the PKI tenant (master domain), the customer (e.g., company, authority, institution) shall name a responsible person to whom a master registrar certificate is issued and who will then perform the functions of the master registrar.
The following functions are available to the master registrar on the website:
   - Create, find, and process areas of responsibility (subdomains)
   - Issue, find, and revoke subregistrar certificates; optional: role assignment of subregistrar certificates (derivatives) for the CMP interface
   - Find and process subscriber certificates
   - Initiate and download Certificate Revocation Lists (CRL)
   - Display and download CA and root CA certificates
   - Administrate the tenant by posting advisories, posting customer documents, and changing login data
   - Display information such as advisories and download TeleSec Shared Business CA documents
   - Renewal of the master registrar certificate
   - Generate statistics within the master domain

   At least one area of responsibility (subdomain) must be defined according to the customer's specifications in order, for example, to properly map the organizational structure. The master registrar creates the area of responsibility and issues a subregistrar certificate for the authorized person. A subregistrar can also have the rights to administrate multiple areas of responsibility.

b) Website for the "Subregistrar" role
The subregistrar's role is to initiate the issue of subscriber certificates within his area of responsibility (see Item 2.1.1.3 Central registration) or to process certificate requests

(approve, reject, resubmission, Item 2.1.1.3 Local registration). The subregistrar registers the subscribers in accordance with the stipulations of the Certificate Practice Statement (CPS). He is also responsible for renewing and revoking certificates.
The following functions are available to the subregistrar on the website:

- Issue, approve, find, and process end subscriber certificates. In handling the request, attention should be paid to whether the certificate is to be placed on a smartcard or if key material is to be generated as a soft PSE. In order to facilitate the smartcard personalization process, certificate data can be uploaded and accepted for the request.
- Request soft PSEs in bulk mode (bulk generation of key materials, including certificate)
- Create and download certificate revocation lists (CRL)
- Display and download CA and root CA certificates
- Administrate the customer-specific domain by posting advisories, posting customer documents, and setting default user input
- Display information such as advisories and download DT Security documents
- Renew the subregistrar certificate
- Optional: preauthentication data can be uploaded as the result of the registration process. Certificate requests that arrive via the user website, email, or SCEP interface are checked against the preauthentication data and processed accordingly. In a positive scenario, the certificate is issued directly. Otherwise the subregistrar has to manually process the request.

c) Website for the "user" role
If users are to request their own certificates, a separate website is available and provides the following functions:

- Request, retrieve, find, revoke, and renew user certificates after successfully logging into the website
- Download certificate revocation lists (CRL)
- Display and download CA and root CA certificates
- Display information such as advisories and download DT Security documents

2.3.2 Additional interfaces

a) SCEP (Simple Certificate Enrollment Protocol)
The TeleSec Shared Business CA supports the request and administration of certificates for network components (routers, gateways) via the SCEP protocol.

b) Email
The TeleSec Shared Business CA makes it possible to request certificates for users (single key only) and servers by email. The request is sent to a defined email address in compliance with format standards (PKCS#10 request). After the subregistrar has approved the certificate request, the certificate is issued to the sender's email address.

c) CMP (Certificate Management Protocol)
The TeleSec Shared Business CA supports the request and administration of certificates (users, servers) via the SCEP protocol. To be able to use this interface, however, the customer must individually develop a CMP client.

2.3.3 Directory service

DT Security shall provide a central directory service for the TeleSec Shared Business CA which allows the current revocation lists (CRL), authority revocation lists (CARL), as well as user certificates to be retrieved. Access to the directory service is public or protected by a username/password.

Access takes place via the LDAP protocol (Lightweight Directory Access Protocol).

2.3.4 Revocation lists

Revoked end user and registrar certificates are published in a certificate revocation list (CRL), which is updated once a day. Revocation lists can also be initiated on a situation-specific basis (see Item 2.3.1).

Revoked CA certificates are published in an authority revocation list (CARL). They are produced by DT Security on a situation-specific basis but no more than six months later.

2.3.5 Online certificate validation

The online validation of end user and registrar certificates is supported via the OSCP protocol (Online Certificate Status Protocol).

2.3.6 Preallocation of data fields

When using public root and intermediate certification authorities, DT Security shall be responsible for preallocating the data fields (country code, organization, organizational unit, place, and Member State).

If an internal root and intermediate certification authority is used, the subregistrar can prepopulate specific data fields for the request with corresponding values.

2.3.7 Information and notifications

The TeleSec Shared Business CA provides the option of selectively distributing customer-specific items of information as well as information from DT Security (advisories and documents) within the role-specific websites (master registrar, subregistrar, and user).

2.4 One-sides service changes

Deutsche Telekom Security GmbH reserves the right to unilaterally change services and reduce charges in favor of the customer. The customer agrees to these adjustments.

In deviation from the agreed written form requirement, Deutsche Telekom Security GmbH will inform the customer of any adjustments by sending updated versions of the existing contractual documents by email, which replace the existing documents.

2.5 Additional services provided by Deutsche Telekom Security GmbH

By agreement and subject to technical and operational feasibility, DT Security shall in particular perform the following additional services against payment of a separate charge based on the valid list prices in effect when the order is placed:

2.5.1 Workshop

DT Security shall offer the customer a workshop for planning and integrating the TeleSec Shared Business CA. The goal is to develop a configuration concept that serves as a basis for integrating the TeleSec Shared Business CA. The workshop shall be tailored to individual customer requirements and generally takes place in the customer's location.

2.5.2 Training

DT Security shall offer the customer training in the configuration, use and operation of the TeleSec Shared Business CA. The goal is to familiarize the customer with the range of functions of the rolespecific websites, in particular the websites for users, master registrars, and subregistrars. The training generally takes place in the customer's location.

2.5.3 Customized services

Customized services that are provided for the customer within the scope of the TeleSec Shared Business CA (e.g., initial provision and installation of an LDAP replication or the development of a migration concept when changing operators).

2.5.4 Smartcard reader

Sales of the Card-reader Advanced smartcard reader (USB) with PIN pad for entering the card PIN (see data sheet).

2.5.5 Smartcards

Sale of the following smartcard types, which can be used in conjunction with the TeleSec Shared Business CA. The smartcards are based on the TCOS smartcard operating system and meet maximum security requirements.

a) Netkey IDkey
Smartcard with up to ten key pairs and a key length of 2,048 bits.

b) Netkey IDkey plugin
Same services as Netkey IDkey, but in the form of a SIM plugin.

c) Netkey 3.0
Smartcard with four key pairs and a key length of 2,048 bits.

d) Netkey 3.0 plugin
Same services as Netkey 3.0, but in the form of a SIM plugin.

2.5.6 Software card module TCOS 3.0 for base CSP

Sale of a software tool that enables Microsoft Base Smartcard CSPs to access and use the TCOS 3.0 card.

2.5.7 Software PKCS#11 SDK for TCOS 3.0

Sale of software PKCS#11 SDK for TCOS 3.0, which enables the TCOS 3.0 card to be accessed via a PKCS#11 interface.

3 CUSTOMER'S DUTIES TO COOPERATE AND ITEMS THAT ARE NOT INCLUDED IN THE SCOPE OF THE SERVICE

The certified "TeleSec Shared Business CA" PKI service offers customers life cycle management for electronic certificates. Due to the extensive requirements of the standardization committees (eg., ETSI, CAB), operating system and browser manufacturers as well as other user committees, which make it possible for the certificates of the TeleSec Shared Business CA to be recognized worldwide, the functional scope of the TeleSec Shared Business CA is largely fixed and is verified annually by external audits. Individual adjustments within the scope of the services are therefore only possible to a limited extent.

The prerequisites (hardware, network connection, configuration, protective measures, etc.) for using the TeleSec Shared Business CA are documented and must be implemented accordingly. It is not planned to provide support as part of the TeleSec Shared Business CA service. Assistance for TeleSec Shared Business CA deployment scenarios, including support and validation services, is not part of this PKI service. Both are usually performed by the customer itself or its IT service provider.

The use of the TeleSec Shared Business CA requires extensive knowledge in the development and operation of a PKI on the part of the customer. The installation, configuration, and scope of services of the TeleSec Shared Business CA and the registration activities to be performed are described in detail in the accompanying documents for the TeleSec Shared Business CA.

3.1 The customer's duties to cooperate

- Using technical and personnel resources, the customer shall undertake all efforts necessary to successfully integrate the "TeleSec Shared Business CA" PKI service in the customer environment and operate it on a permanent basis.
- Comprehensive support of the registration authority in incident, problem, and change management as well as in security incidents of any kind in connection with the TeleSec Shared Business CA.
- Implementation of instructions issues by the certification authority (TeleSec Shared Business CA).
- Prompt and comprehensive implementation of changes to the Certificate Policy (CP) and Certification Practice Statement (CPS) (source: https://www.telesec.de/de/service/downloads/pki-repository/) or of measures resulting from changes in the requirements of relevant sources of requirements
- Full support in audits of the TeleSec Shared Business CA by the registration authority or external auditors within the framework of the certification of the TeleSec Shared Business CA.

3.2 Services not included, Not part of the service

- The following services are not included in the TeleSec Shared Business CA standard service. The provision or procurement of these services is the responsibility of the customer.
- Procurement, installation, configuration, and operation of the registrar PC(s) (PC workstation(s)) of the registration authority/ies required for certificate administration (issuing, renewing, or revoking) within the PKI tenant(s).
- Procurement, installation, configuration, and operation of all hardware and software components, such as internet access, telephone, storage media, antivirus software, access

protection, or software updates required to enable the use of registrar PCs and certificate management.

- Validation and configuration of mass data (organizational data and internet domains) by the Sub-CA
- Registration process of all end users and registrars (except master registrar) leading to the issue, renewal, and revocation of any certificates.
- Certificate management (issuing, renewing, and revoking) including key backup, recovery of any certificate types.
- Rollout/deployment: certificate distribution of soft PSE and/or smartcards with corresponding PIN letter to the certificate requester or certificate holder or other technical components (e.g., customer-specific LDAP directory service, Active Directory) if the standard processes (user website, email, SCEP, CMP) do not reflect this.
- Personalization of smartcards via a personalization system, creation of customer-specific PIN letters via a printer, enveloping, shipping, and postage.
- Shipping and distribution of smartcard readers and/or smartcards to certificate requesters or certificate holders.
- Scripting of software of any kind (e.g., drivers, middleware).
- Automatic and/or manual software distribution and software installation (e.g., CA certificates, soft PSE, drivers, or middleware (CSP, PKCS#11 module)).
- Provision and distribution of additional validation information (such as certificate revocation lists or OCSP accesses) of the Trust Center's PKI infrastructure.
- Development, testing, integration, and maintenance of a customer-specific CMP client that interacts with the CMP server interface of the TeleSec Shared Business CA (see current CMP specification).
- Development or deployment, maintenance, and configuration of application software (such as email or VPN software, network login) of any kind that supports X.509v3 certificates.
- Support of technical certificate requests for server, gateway, etc.
- 1st and 2nd level service and support for end users – except master registrars – (see Service Level Agreement for details).
- Creation and maintenance of additional customer-specific documents that result in a technical and/or process-oriented certificate integration into the customer applications.
- Support of any kind, such as analysis, project planning, consulting, support, engineering, which results in an integration of the PKI service into the customer's network.
- Development or deployment, maintenance of software components of any kind that support synchronization and/or replication of an LDAP directory service for certificates and revocation lists.

3.3 Further aspects

- Further information is provided in the document "Personnel, infrastructure, and technical framework conditions (PITF)."
- In addition to the "Common Name", up to four (4) other server names (SAN) can be entered for server certificates. No further entries are possible.
- As part of the standard service, organizational data and the associated domains are validated up to a maximum of 5 organizations and a maximum of 15 Internet domains. A larger number must be agreed separately in each individual case and charged as an optional service.
- In the event that the abovementioned services are to be provided in whole or in part, an individual agreement shall be required.

4 MINIMUM LEASE PERIOD / TERMINATION

4.1 Rate models

4.1.1 Advanced

Within the "Advanced" rate plan, billing is based on a defined maximum number of active certificates per identity, regardless of whether the certificate holder receives two or three certificates. The "Active" status means that the certificate is valid and has not been revoked on a particular date (the 16th day of a calendar month in this case).

4.1.2 Classic

Within the "Classic" rate plan, billing is based on generated (issued) certificates with a validity of one year.

4.1.3 Classic 2Y

Within the "Classic Pro" rate plan, billing is based on generated (issued) certificates with a validity of two years.

4.1.4 Classic Pro

Within the "Classic Pro" rate plan, billing is based on generated (issued) certificates with a validity of three years.

4.2 Contract terms

The minimum contract term for TeleSec Shared Business CA begins with the provision of the infrastructure (reader, driver software, master registrar certificate, certificate and configuration data sheet) and is one year, two years, or three years. It shall be extended automatically by 6 (six) months at each expiration.

4.3 Termination

a) This agreement may be terminated by either party, at the earliest with effect from the end of the minimum contractual term, by giving three months' notice in writing (e.g., by letter or email). If the agreement is not terminated, the contractual term shall be extended by six months in each case unless it is terminated in writing (e.g., by letter or email) at least one month prior to the end of the lease period.

   The validity period of the certificates of the Classic and Classic Pro rate models (see Items 4.1.2, 4.1.3 and 4.1.4) remain unaffected by the termination. Certificates issued on the basis of the Advanced rate model (see Item 4.1.1) are revoked after the termination date and become invalid. A special transitional rule can be agreed in the individual contract in question.

b) The right to terminate the agreement for good cause shall remain unaffected in all cases.

c) If Deutsche Telekom Security GmbH terminates the agreement prematurely due to a reason for which the customer is responsible, the customer shall be obliged to pay Deutsche Telekom Security GmbH compensation as a single, lump-sum payment amounting to half of the remaining monthly charges payable up to the end of the agreed term. The compensation payment shall be higher if Deutsche Telekom Security GmbH proves that the loss suffered was greater. It shall be lower or not payable at all if the customer proves that the loss suffered was essentially less or that a loss was not suffered at all.

SUPPLEMENTARY LITERATURE

- Offer TeleSec Shared Business CA including prices
- General Terms and Conditions TeleSec Products
- Service description TeleSec Shared Business CA (SD SBCA)
- Certificate Policy (CP) Certification Practice Statement (CPS)
- Service level agreement TeleSec Shared Business CA (SLA SBCA)
- Framework SLA for Trust Center services
- Personnel, infrastructure and technical framework conditions TeleSec Shared Business CA (PITF)
- Service and Usage Agreement TeleSec Shared Business CA

ACRONYMS

CA	Certification Authority
CAB	CA/Browser forum
CARL	Certification Authority Revocation List
CMP	Certificate Management Protocol
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Cryptographic Service Provider
ETSI	European Telecommunications Standards Institute
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PC	Personal Computer
PIN	Personal identification number
PITF	Personnel, infrastructure and technical framework conditions
PKCS	Public-Key Cryptography Standards
PKI	Public key infrastructure
PSE	Personal security environment
RA	Registration authority
SCEP	Simple Certificate Enrollment Protocol
SDK	Software Development Kit
SD	Service description
SIM	subscriber identity module
SLA	Service level agreement
S/MIME	Secure multipurpose Internet mail extension
SSL	Secure Socket Layer
TCOS	TeleSec Chipcard Operating System
TLS	Transport layer security
USB	Universal Serial Bus
VPN	Virtual Private Network