Service Specifications & Additional Terms and Conditions
Business.ID

Last revised: September 12, 2022

Publication details

Published by

Deutsche Telekom Security GmbH

Bonner Talweg 100

53113 Bonn, Germany

Germany

hereinafter referred to as “Telekom”

WEEE reg. no. DE 56768674

For the information we are obliged to provide by law, please go to: http://www.telekom.com/pflichtangaben-dtsec

Confidentially Class: Public

CONTENTS

1 INTRODUCTION

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

Deutsche Telekom Security GmbH shall provide the customer with the infrastructure and accesses needed for this so that the customer can access the PKI components in Deutsche Telekom Security GmbH's 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 FEATURES

The Business.ID 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
- Individuals (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 Business.ID is documented in the Certificate Policy (CP) and the Certification Practice Statement (Business.ID CPS).

2.1 Certificate management

2.1.1 Website

In terms of managing the Business.ID, the customer (e.g., company, authority, institution) names at least one responsible person to whom a master registrar certificate is issued and who shall then perform the functions of the master registrar.

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. The subregistrar's role is to initiate the issue of subscriber certificates within his area of responsibility (see Item 2.1 Central registration) or to process certificate requests (approve, reject, resubmission, Item 2.1 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.

If users are to request their own certificates, a separate website is available.

The customer accesses the Business.ID website via an SSL-secured internet connection (HTTPS protocol). Only upon successful authentication (access control) can the customer's role holder use his specific Business.ID functions.

Depending on the assigned functional role (master registrar, subregistrar, or user), the following range of functions is available to the customer.

a) Website for the "Master registrar" role

- 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.
- Manage the tenant by posting advisories, posting customer documents, and changing login data.
- Display information such as advisories and download Business.ID documents.

- Renew the master registrar certificate.
- Generate statistics within the master domain.

b) Website for the “Subregistrar” role

- Issue, approve, find, and process end user 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.
- Manage the customer-specific domain by posting advisories, posting customer documents, and setting default user input.
- Display information such as advisories and download Business.ID documents.
- Renew the subregistrar certificate.
- Optional: pre-authentication 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 pre-authentication 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

- 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 Business.ID documents.

2.1.2 SCEP (Simple Certificate Enrollment Protocol

The Business.ID supports the request and administration of certificates for network components (routers, gateways) via the SCEP protocol.

2.1.3 Email

The Business.ID 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.

2.1.4 CMP (Certificate Management Protocol)

The Business.ID supports the request and administration of certificates (users, servers) via the CMP protocol. To be able to use this interface, however, the customer must individually develop a CMP client.

2.2 Directory service

Deutsche Telekom Security GmbH provides a central directory service for the Business.ID, which allows the current revocation lists (CRL), authority revocation lists (ARL), as well as user certificates to be retrieved. Access to the directory service is public or protected by a username/password, depending on the agreement or on necessity.

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

2.3 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 2.1). If necessary, the creation of a new revocation list can be triggered manually after a revocation.

Revoked CA certificates are published in a certification authority revocation list (CARL). They are created by Business.ID on a situation-specific basis but no more than six months later.

2.4 Online certificate validation

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

2.5 Default settings in data fields

When using public root and intermediate certification authorities, Business.ID shall be responsible for prepopulating 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.

2.6 Information and messages

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

3 SERVICES PROVIDED BY TELEKOM

3.1 Initial provision

3.1.1 General information

3.1.1.1 Domain concept

The customer is set up as an independent tenant within Business.ID. 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 Business.ID, the tenant is also referred to as the master domain and the subdivision into areas of responsibility is referred to as the subdomain. The name of the PKI tenant and the area of responsibility are an integral component of the requester in the certificate.

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

3.1.1.2 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 pre-installed 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 of the relevant certificates in the respective certificate stores and applications.

3.1.1.3 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 Business.ID, in principle, stated in the Certificate Policy (CP) of Telekom Security (Telekom Security Certificate Policy (CP)) and the Certification Practice Statement (CPS). The Business.ID provides two options.

- **Central registration**
  The certificate for persons and devices (see Item 2.1) 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 2.1).
- **Local registration**
  The requester (individual) can submit a certificate request from a user website. The competent subregistrar shall carry out the registration in accordance with 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.

3.1.2 Provisioning of Business.ID

In order to ensure the fast and straightforward use of the Business.ID, the initial provision includes the setup of a PKI tenant (master domain) and the delivery of a basic package of hardware and software components (smartcards, master-registrar certificate, tools), which form the basis for accessing the Trust Center. The basic equipment supports the customer both 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 Business.ID
- Provision of one or more subregistrar certificate(s) for administrating the areas of responsibility (subdomains) set up by the customer within the Business.ID
- SmartBridge: help tool for generating key pairs and communicating with the CA
- 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 standard service includes the validation of organizational data and the associated domains up to a maximum of 5 organizations and a maximum of 15 internet domains. A larger number must be agreed separately in individual cases and ordered as an optional service for a fee.

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.

Note: a necessary smartcard reader is not included in the scope of delivery of Business.ID. A commercially available card reader or the onboard card reader of the customer's respective standard PC can be used here.

3.1.3 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 3.1.1.1). Additional certificate information is documented in the Certificate Policy (CP) of Telekom Security and the Certification Practice Statement (CPS).

The certificate validity can be set in x days and is valid for the relevant configured PKI tenant. This makes it easy to map, for example, one-, two-, or three-year terms. Optionally, other validity periods can be configured, which, however, must not violate the requirements of the standardization bodies, and so on.

3.1.3.1 Certificate for natural persons and person and function groups

According to the configuration, only certain certificate types can be requested. These include

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 smart card-based login to Microsoft Windows domains. Smartcard login and client authentication are set as the extended key usage.

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

For server certificates, up to four (4) additional server names (SAN) can be entered alongside the "Common Name." No further entries are possible besides this.

3.1.3.3 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.

3.2 Operation

3.2.1 Trust Center operation

The Business.ID provides a PKI infrastructure that is operated by competent staff in Telekom Security's highly secure Trust Center in accordance with 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 "life cycle management" of the certificates, the key management, as well as the registration are therefore the responsibility of the customer.

3.2.2 On-site operation (PITF)

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

All general conditions and rules of conduct are described in the document "Personnel, infrastructure, and technical framework conditions (PITF)."

In particular, this document contains the regulations for the registrar workstation.

3.3 Optional services

By agreement and subject to existing technical and operational feasibility, Deutsche Telekom Security GmbH 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:

3.3.1 Workshop

Business.ID shall offer the customer a workshop for planning and integrating Business.ID. The goal is to develop a configuration concept that serves as a basis for integrating the Business.ID. The workshop shall be tailored to individual customer requirements and generally takes place online or in coordination at the customer's location.

3.3.2 Training

Business.ID shall offer the customer training for configuring, using, and operating the Business.ID. The goal is to familiarize the customer with the range of functions of the role-specific websites, in particular the websites for users, master registrars, and subregistrars. The training generally takes place in the customer's location.

3.3.3 Smartcards

The sale of the following smart card types, which can be used within the scope of the Business.ID, is possible separately on request. 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

4 COOPERATION SERVICES ON THE PART OF THE CUSTOMER

The Business.ID PKI service is ETSI-certified and offers customers life cycle management for electronic certificates. Due to the extensive requirements of the standardization committees (e.g., CAB or root programs) of the operating system and browser manufacturers as well as other user committees, which make it possible for the certificates of the Business.ID to be recognized world-wide, the functional scope of the Business.ID is largely fixed and is verified annually by external audits.

The prerequisites (hardware, network connection, configuration, protective measures, etc.) for using the Business.ID are documented and must be implemented accordingly. It is not planned to provide support as part of the Business.ID service. Assistance for Business.ID 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 Business.ID requires extensive knowledge in the development and operation of a PKI on the part of the customer. The installation, configuration, and scope of Business.ID services and the registration activities to be performed are described in detail in the accompanying documents for the Business.ID. The documents are offered for download in the respective Business.ID frontends.

4.1 The Customer’s duties to cooperate

The customer undertakes to cooperate in order to ensure due provision of the required services; in particular, it is obliged to provide the following, free-of-charge, on-time, and to the required extent:

The customer undertakes to, and shall oblige its staff to, comply with the Trust Center Certificate Policy (CP), and the Certification Practice Statement (CPS). In particular, the customer is obliged to ensure that all information on the establishment of the master domain and on the issuing and administration of the certificates is accurate. Proof of identification must be provided for the establishment of the master domain. The customer must notify Telekom immediately in writing of any organizational changes.

The customer shall notify its users about the details of this agreement in good time before usage starts and, in particular, about the rights and obligations in accordance with the General Terms and Conditions and the Certification Practice Statement (CPS). The customer shall be liable for any breaches of obligations by his users and other third parties where these breaches occur within the customer’s sphere of control, unless he provides evidence that the breach is not attributable to him.

Within the scope of this service, the customer undertakes to comply with the statutory provisions and requirements of the General Data Protection Regulation (GDPR) and to obtain the necessary consent of the respective data subject.

Using technical and personnel resources, the customer shall make every effort to successfully integrate the Business.ID PKI service in the customer environment and operate it on a permanent basis. That includes, in particular:

- Procurement, installation, configuration, and operation of the registrar PC(s) (PC workstation(s), card readers) of the registration authority/ies required for certificate administration (issuing, renewing, or revoking) within the PKI tenant(s)
- Procurement of the smartcard reader, which must be provided by the customer
- 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
- Registration process of all end users and registrars (except master registrar) leading to the issue, renewal, and revocation of any certificates
- Validation and configuration of mass data (organizational data and internet domains) by the Sub-CA
- 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
- Comprehensive support of the registration authority/ies in incident, problem, and change management as well as in security incidents of any kind in connection with the Business.ID
- Submitted documents must have been written in German or English.
- Implementation of instructions issued by the certification authority (Business.ID).
- 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 Business.ID by the registration authority or external auditors within the framework of the certification of the Business.ID

4.2 Services not included, not part of the service

The following services are not included in the Business.ID standard service. The provision or procurement of these services is the responsibility of the customer.

- 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 Business.ID (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

5 MINIMUM TERM/TERMINATION

5.1 Rate plans

5.1.1 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).

5.1.2 Classic

Within the "Classic" rate plan, billing is based on generated (issued) certificates with a validity of one year. This rate model can only be used by system houses/resellers.

5.1.3 Classic 2Y

Within the "Classic 2Y" rate plan, billing is based on generated (issued) certificates with a validity of two years. This rate model can only be used by system houses/resellers.

5.1.4 Classic Pro

Within the "Classic Pro" rate plan, billing is based on generated (issued) certificates with a validity of three years. This rate model can only be used by system houses/resellers.

5.2 Acceptance of the service

The service is considered accepted from the day of delivery of the management certificates. This starts the term of the agreement and the obligation to pay the fee.

5.3 Commencement, term, and termination of the agreement

The minimum provision period for Business.ID is 36 months from the date the agreement is signed, and this period automatically extends by 12 months unless terminated 3 months prior to the end of the minimum provision period or the respective extension period.

The validity period of the certificates of the Classic and Classic Pro rate models remain unaffected by the termination. Certificates issued on the basis of the Advanced rate model are revoked after the end of the agreement term and become invalid.

5.4 Payment terms

5.4.1 Monthly charges

Starting on the day on which the service has been provided ready for operation, monthly charges shall be payable for the rest of the month on a pro rata basis. These charges shall thereafter be payable monthly in advance. If the charge is to be calculated for parts of a calendar month, it shall be calculated on a pro rata basis for each day.

5.4.2 One-time charges

One-time fees shall be payable after the service has been provided.

5.5 Unilateral changes to the service

Deutsche Telekom Security GmbH reserves the right to make unilateral changes to the service and to 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 shall notify the customer of any adjustments by emailing updated versions of the existing contract documentation to replace the existing documentation.

6 OTHER APPLICABLE DOCUMENTS

The following documents apply in addition to these Service Specifications:

- GTC DTSec IT services
- Trust Center Certificate Policy (CP)
- Certification Practice Statement, Business.ID (CPS Business.ID)
- Service Level Agreement Business.ID (SLA BUSINESS.ID)
- Framework SLA for Trust Center services (Framework SLA)
- Business.ID’s terms of service and use
- Personnel, infrastructure, and technical framework conditions (PITF)

7 GLOSSARY/LIST OF ABBREVIATIONS

Term	Description
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 (German: Europäisches Institut für Telekommunikationsnormen)
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
SS	Service Specifications
LDAP	Lightweight Directory Access Protocol
OCSP	Online Certificate Status Protocol
PC	Personal Computer
PIN	Personal Identification Number
PITR	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
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