PKI DISCLOSURE STATEMENT (PDS)

BUSINESS.ID

DEUTSCHE TELEKOM SECURITY GMBH

VERSION:	04.00
VALID FROM:	FEBRUARY 18, 2022
STATUS:	RELEASE
CLASSIFICATION:	PUBLIC
LAST REVIEW:	FEBRUARY 17, 2022

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

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

Brief summary:	This document describes the PKI Disclosure Statement (PDS) of PKI Service Business.ID.
File name:	BusinessID_PKI-Disclosure-Statement_04.00_EN.docx
Document number:	n.n.
Document title:	PKI Disclosure Statement (PDS) of PKI Service Business.ID.
Version:	04.00
Valid from:	February 17, 2022
Status:	release
Classification:	Public
Last review:	February 17, 2022
Author:	Uwe Völkel, Netphen, October 1, 2020
Contents reviewed by:	Andreas Jud, Netphen, February 17, 2022
Approved by:	Hubertus Halbe, Netphen, February 18, 2022
Contact:	tc-solutions.lastlevel@t-systems.com

CHANGE HISTORY

VERSION:	LAST REVISED:	EDITED BY:	CHANGES / COMMENTS:
00.10	June 11, 2018	Uwe Völkel	Initial version
00.20	July 27, 2018	Lothar Eickholt	Quality assurance for vers. 00.10 and release of this version
01.00	July 27, 2018	Uwe Völkel	Release of this version
01.10	June 6, 2019	Uwe Völkel	Addition chapter 3, 5, 7, 8, 10.1, 10.2 ff, 12.1, 12.2
01.20	February 4, 2020	UV	Harmonisation version
01.30	February 5, 2020	LE, UV	Revision
01.40	March 2, 2020	LE, UV	Revision
01.50	March 24, 2020	AJ	QA
02.00	March 25, 2020	UV	Release of this version
02.10	October 1, 2020	UV	New Word template, revision of company modification
02.20	October 8, 2020	AJ	QA
02.30	October 9, 2020	GK	QS
03.00	October 9, 2020	HH	Release of this version
03.90	February 17, 2022	Telekom Security	QS
04.00	February 18, 2022	Telekom Security	Release of this version

CONTENTS

1 INTRODUCTION

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

The processes of Deutsche Telekom Security GmbH (hereinafter referred to as “DT Security”) are subject to regular annual audits (ETSI EN 319 411-1, policy OVCP, and policy NCP) by independent third parties. The subject of certification are all processes used for the application, issue, revocation, and renewal of end user certificates in connection with a public certification authority (TeleSec Business CA 1). The Deutsche Telekom Security GmbH also performs quality assessment self-audits at regular intervals.

This document summarizes the key points of the particular Certificate Policy (CP) and Certification Practice Statement (CPS) (see Chapter 8) and serves as an overview for applicants and trusting third parties. To ensure comparability, it is designed according to ETSI EN 319 411-1.

2 TRUST SERVICE PROVIDER (TSP) CONTACT INFO

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

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

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

Cases of certificate misuse can be reported by:
Phone: +49 (0) 1805-268204
Fixed network: EUR 0.14/minute, mobile network: max. EUR 0.42/minute
E-mail: telesec_support@t-systems.com
Internet: https://www.telesec.de/de/service/kontakt/zertifikatsmissbrauch-melden/

3 CERTIFICATE TYPES, VALIDATION PROCEDURES AND KEY USAGE

With the PKI service Business.ID, Deutsche 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)
- Server
- Domain controller
- Router/gateway
- Mail gateway

Depending on the respective certificate types, the Business.ID 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, 2024)

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 Deutsche Telekom Security GmbH certification authority.

The following types of certificates can be issued under a public certification authority, which is subject to ETSI certification every year (see Chapter 13):

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

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 thirty-six (36) months. An exception applies to server certificates with a maximum validity of thirteen (13) months.

Certificates issued by an internal certification body are valid for a maximum of sixty (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/de/service/downloads/pki-repository/

The PKI client is managed by the role owner master and sub-registrar of the customer. These role owners are also responsible for issuing and revoking certificates. A certificate of the above-mentioned type is revoked by the responsible sub-registrar of the customer. User certificates can optionally be revoked via a website, provided that the customer supports this. A sub-registrar certificate is revoked by the responsible master registrar of the customer. A revocation order for the master registrar certificate is accepted by the contact of the TSP (see Chapter 2).

4 RELIANCE LIMITS

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

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.

The paper documents and electronically recorded request and certificate data as well as the data from the certificate history are archived for a further ten years plus a waiting period beyond the certificate validity. For a certificate renewal, the retention period of the original documents and data is extended accordingly.

The same requirements apply to the external registration authority that is established at the customer.

5 OBLIGATIONS OF SUBSCRIBERS

The obligations of the end users are listed in the document “Service and Usage Agreement Business.ID”.

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

6 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. Deutsche 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.

7 LIABILITY EXCLUSION, LIMITATION OF LIABILITY

The certification authority is liable indefinetly 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 terms-of-use TeleSec-products or individually negotiated.

8 APPLICABLE AND CONTRACTUAL AGREEMENTS

The following documents are available online under https://www.telesec.de/de/service/downloads/pki-repository/ :

- Service and Usage Agreement Business.ID
- 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)

9 AVAILABILITY OF THE SERVICE

The infrastructure of the Business.ID 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, CARLs), 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.

10 PRIVACY POLICY

Within Business.ID, DT Security must store and process personal data electronically in order to provide its services.

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

10.1 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 and how it is protected against loss and unauthorized access.

Here the requirements under [ETSI EN TSP] Section 10.2 are implemented.

10.2 Data archiving

10.2.1 Type of archived datasets

DT Security archives the following data:

- Order documents on paper (e.g., quotations, orders),
- Information in certificate requests and regarding the certificate life cycle (e.g., revocation and renewal requests),
- Soft PSEs that were requested in bulk.
- 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 10.1.

10.2.2 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.
- Audit, history and event logging data are archived up to forty-two (42) days.

11 REFUND POLICY

Refund of fees by DT Security is based on the legal regulations of German law. In addition, the provisions of the applicable GTC or other contractual arrangements agreed with the customer apply.

12 APPLICABLE LAW, COMPLAINTS AND DISPUTE RESOLUTION

12.1 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 Deutsche Telekom Security GmbH in Bonn, Germany.

12.2 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.

13 AUDITING

The processes of Deutsche Telekom Security GmbH are subject to regular annual audits (ETSI EN 319 411-1, policy OVCP, and policy NCP) by independent third parties. The subject of certification are all processes used for the application, issue, revocation, and renewal of end user certificates in connection with a public certification authority (currently TeleSec Business CA 1). Deutsche Telekom Security GmbH also performs quality assessment self-audits at regular intervals.

To verify conformity, the public certification authority Business.ID is audited by internal auditors as well as by a recognized body according to [ETSI EN 319 403]. Within the scope of the audits, the implementation of the processes and compliance with the requirements are checked in addition to the documentation (security concept, operating concept and other internal documents).

To ensure compliance, the public certification authorities meet the requirements of

[ETSI NCP OVCP]	ETSI EN 319 411-1 V1.1.1 (2016-02), European Telecommunications Standards Institute, „Electronic Signatures and Infrastructures (ESI); Policy Requirements for certification authorities issuing public key certificates“, policy NCP and OVCP
[ETSI EN TSP]	ETSI EN 319 401 V2.1.1 (2016-02), Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers supporting Electronic Signatures

ANNEX A: ACRONYMS

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certification Revocation List
CARL	CA Revocation List
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation
GTC	General Terms and Conditons
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