Qualified.ID / Qualified.ID Seal

PKI Disclosure Statement (PDS)

Deutsche Telekom Security GmbH

public

Version:	2.0	Valid from:	28.06.2023
Status:	final	Last review:	28.06.2023

With the publication of this document all previous versions lose their validity!

Table of contents

1 Introduction

The certification service consists of several "Trust Services" for issuing qualified certificates.

- Qualified.ID: Certification service to issue qualified X509 certificates.
- Qualified.ID Seal: Certification service to issue qualified X509 certificates.

The Certificate Policy (CP) and further information on certificate management are described in the "Certification Practice Statement" (CPS), see chapter 8.

This document summarizes the key points of the CPS 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 TSP contact info

The TSP can be reached via the following contacts:

- Address: Deutsche Telekom Security GmbH,
  Untere Industriestraße 20, D-57250 Netphen
- Phone: + 49 1805 / 26 82 04
  (Festnetzpreis 14 ct/Min., Mobilfunkpreis max. 42 ct./Min)
- E-Mail: trust_center_notary@telekom.de
- Internet: https://www.telesec.de

The revocation service (“Sperr-Notruf 116 116 e.V.”) is to be reached 7x24 hours as follows:

Phone Germany:	116 116
Phone International:	+49 30 4050 4050

3 Certificate type, validation procedures and usage

The following certificates are issued:

- One qualified X509 certificate for the creation of qualified electronic signatures (QES), issued by the Trust Service Qualified.ID.
- Or one qualified X509 certificate for the creation of qualified electronic seal (QSeal), issued by the Trust Service Qualified.ID Seal.

Each applicant is personally identified by means of a valid official ID card according to predetermined procedures.

4 Reliance limits

Deutsche Telekom Security 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.

5 Obligations of subscribers

The obligations of the subscribers are listed in the terms and conditions ("Allgemeine Geschäftsbedingungen"), the document is available on the Internet: https://www.telesec.de/de/service/downloads/allgemeine-geschaeftsbedingungen/.

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

- 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,
- 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 Limited warranty and disclaimer/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 general terms and conditions (GTC) („Allgemeine Geschäftsbedingungen“ (AGB)) or individually negotiated.

8 Applicable agreements, CPS, CP

This PDS, the CPS are available on the Internet: https://www.telesec.de/de/service/downloads/pki-repository/.

Terms and conditions („Allgemeine Geschäftsbedingungen“) are available on the Internet: https://www.telesec.de/de/service/downloads/allgemeine-geschaeftsbedingungen/.

9 Privacy policy

Deutsche Telekom Security must store and process personal data electronically for the purpose of providing the service. Deutsche Telekom Security ensures the technical and organizational security precautions and measures to protect the data in accordance with the applicable data protection regulations. Concerning the retention period of the data the provisions of chapter 4 apply.

10 Refund policy

Refund of fees by Deutsche Telekom 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

11 Applicable law, complaints and dispute resolution

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 TSP and repository licenses, trust marks, and audit

Certificates are issued subject to the requirements of the Regulation (EU) Nr. 910/2014 of the European Parliament and the Council („eIDAS“)

In order to ensure conformity, Deutsche Telekom Security meets the requirements of

- [ETSI EN 319 401]: General Policy Requirements for TSPs
- [ETSI EN 319 411-1]: General Policy and security requirements for TSPs
- [ETSI EN 319 411-2]: Requirements for TSPs issuing EU qualified certificates
- [ETSI EN 319 412-2]: Certificate profile for certificates issued to natural persons
- [ETSI EN 319 412-5]: Certificate Profiles: QCStatements

To verify conformity, Deutsche Telekom Security 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).