Server.ID PDS

PKI Disclosure Statement (PDS)

Deutsche Telekom Security GmbH

public

Version:	08.00	Last review:	09.02.2024
Status:	released	Valid from:	12.02.2024

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

Imprint

Editor	Deutsche Telekom Security GmbH Trust Center & ID Security Untere Industriestraße 20 57250 Netphen

Filename	**Valid from**	**Titel**
Server.ID_PDS_v08.00_12022024.docx	12.02.2024	Server.ID PDS

Version	**Status**
08.00	released

Contact person	**Phone**	**E-Mail**
Deutsche Telekom Security GmbH	+49 (0) 1805 268 204 (Festnetz 0,14 EUR/Minute, Mobilfunk-netze max. 0,42 EUR/Minute)	telesec_support@telekom.de

Short description
PKI Disclosure Statement. Server.ID according to ETSI EN 319 411-1 and ETSI EN 319 411-2

Table of contents

1 Introduction

Server.ID is a certification service for the issuance of different types of X.509v3 certificates for website authentication. The service is operated in a trust center of Deutsche Telekom Security GmbH.

The certification service Server.ID consists of "Trust Service Providers" (TSP) for issuing qualified and non-qualified certificates.

The service itself and all involved processes are described in the "Telekom Security Certification Practice Statement Public "[1] (CPS Public), see chapter 8.

This document summarizes the key points of the CPS Public, the Terms of Use for Public Certificates[2] and the general terms and conditions [refer to the general terms and conditions “IT-Leistungen“[3]](GTC) and serves as an overview for applicants and trusting third parties. To ensure comparability, it is designed according to ETSI EN 319-411-1 and ETSI EN 319 411-2.

2 TSP contact info

TSP T-Systems International GmbH for
“TeleSec ServerPass Extended Validation Class 3 CA” can be reached via the following contacts:

- Address:

T-Systems International GmbH
Represented by Deutsche Telekom Security GmbH
Trust Center & ID Security
Untere Industriestraße 20
57250 Netphen

- Phone: +49 (0) 1805 268 204 (landlines: EUR 0.14/minute, mobile networks: max. EUR 0.42/minute)
- E-mail: telesec_support@telekom.de
- Internet: https://www.telesec.de

Revocation service is available

- online 24 x 7: https://serverpass.telesec.de/serverpass/ts/ee/index.html
- Phone: +49 (0) 1805 268 204 (landlines: EUR 0.14/minute, mobile networks: max. EUR 0.42/minute)

Submit abuse report

- https://www.telesec.de/de/service/kontakt/zertifikatsmissbrauch-melden/

This TSP has been valid until: August 16, 2023

[1] https://www.telesec.de/de/service/downloads/pki-repository/

[2] https://www.telesec.de/de/service/downloads/pki-repository/

[3] https://www.telekom.de/is-bin/INTERSHOP.enfinity/WFS/EKI-PK-Site/-/-/-/ViewAGB-Start?wt_mc=alias_agb/direkt&AGBID=2744

TSP Deutsche Telekom Security GmbH (valid since: August 17, 2023) can be reached via the following contact information:

- Address:

Deutsche Telekom Security GmbH
Trust Center & ID Security
Untere Industriestraße 20
57250 Netphen

- Phone: +49 (0) 1805 268 204 (landlines: EUR 0.14/minute, mobile networks: max. EUR 0.42/minute)
- E-mail: telesec_support@telekom.de
- Internet: https://www.telesec.de

Revocation service is available

- online 24 x 7: https://serverpass.telesec.de/serverpass/ts/ee/index.html
- Phone: +49 (0) 1805 268 204 (landlines: EUR 0.14/minute, mobile networks: max. EUR 0.42/minute)

Submit abuse report

- https://www.telesec.de/de/service/kontakt/zertifikatsmissbrauch-melden/

3 Certificate type, validation procedures and usage

The Trust Service Provider issues and distributes domain-, organization- and extended-validated certificates. Depending on the product variant different public root certification authorities (root-CAs) and product related sub-CAs are available. The validation processes are described in the CPS Public. The end entity certificates refer entirely to the X.509v3 standard.

3.1 Server.ID DV products

Server.ID DV products are domain-validated X.509v3 certificates for website authentication. For the domain validation different methods of the TLS Baseline Requirements, section 3.2.2.4, are supported.

Customers may order different variants of Server.ID DV, such as certificates with one domain entry, multi-domain certificates with several SAN-entries or wildcard certificates.

The products use the following public root Cas and sub-CAs:

root CAs:

- CN=T-TeleSec GlobalRoot Class 2 (valid until Oct. 10, 2033)

  sub-CAs:

  - CN=Telekom Security DV RSA CA 21 (valid until Apr. 21, 2031)
  - CN=Telekom Security DV RSA CA 22 (valid until Feb. 22, 2032)

Registration
▪ Initial registration process for ACME-interface
Validity period
▪ 1 year (plus grace period up to 5 days)
Procedure of validation
▪ online-order required
▪ Domain validation

3.2 Server.ID OV products

Server.ID OV products are organization-validated X.509v3 certificates for website authentication. Next to domain validation (see 3.1), the existence of the organization and its authorization of the certificate request are validated.

Customers may order different variants of Server.ID OV, such as certificates with one domain entry, multi-domain certificates with several SAN-entries or wildcard certificates.

The products use the following public root CAs and sub-CAs:

root CAs:

- CN=T-TeleSec GlobalRoot Class 2 (valid until Oct. 10, 2033)

  sub-CAs:

  - CN=TeleSec ServerPass Class 2 CA (valid until Feb. 11, 2024)
  - CN=Telekom Security ServerID OV Class 2 CA (valid until Aug. 2, 2027)
  - CN=Telekom Security OV RSA CA 22 (valid until Jun. 21, 2032)

Registration

- The service portal is mandatory for registration

Validity period

- 1 year (plus grace period up to 5 days)

Procedure of validation

- online-order required
- Organization validation

3.3 Server.ID EV / EV QWAC products

Server.ID EV products are extend-validated X.509v3 certificates for website authentication. Next to the domain validation (see 3.1), an extended validation of the existence of the organization will be done. In addition, the EV-order form and its authorization will be validated as well as the identity of at the involved stakeholder(s).

Customers may order different variants of Server.ID EV, such as certificates with one domain entry or multi-domain certificates with several SAN-entries.

Server.ID EV QWAC products are qualified extended-validated X.509v3 certificates for website authentication containing a qc-statement. The identification process follows the Regulation (EU) Nr. 910/2014 of the European Parliament and the Council („eIDAS“).

Customers may order different variants of Server.ID EV QWAC, such as certificates with one domain entry or multi-domain certificates with several SAN-entries.

The root of trust for the validation of a certificate can be traced in the EU/EEA Trusted List / Germany in the ServiceDigitalIdentity attribute of the Trust Service Server.ID qualified entry.

The products use the following public root CAs and sub-CAs:

root-CA:

- CN=T-TeleSec GlobalRoot Class 3 (valid until Oct.01, 2033)

  sub-CA:

  - CN=TeleSec ServerPass Extended Validation Class 3 CA (valid until Feb. 11, 2024)
  - CN=Telekom Security ServerID EV Class 3 CA (valid until Aug. 2, 2027)

- CN=Telekom Security EV RSA CA 23A (valid until Jun. 19, 2033)

- CN=Telekom Security TLS RSA Root 2023 (valid until Mar. 27, 2048)

  sub-CA:

  - CN=Telekom Security EV RSA CA 23 (valid until Mar. 27, 2033)

- CN=Telekom Security TLS ECC Root 2020 (valid until Aug. 25, 2045)

  sub-CA:

  - CN=Telekom Security EV ECC CA 21 (valid until Apr. 21, 2031)

Registration
▪ The service portal is mandatory for registration
Validity period
▪ 1 year (plus grace period up to 5 days)
Procedure of validation
▪ online-order required
▪ Extended validation
▪ POSTIDENT (by branch as Identification according to the Regulation (EU) Nr. 910/2014 of the European Parliament and the Council („eIDAS“).)

3.4 Certificate usage

All certificates are issued by defined validation- and issuance-processes.

The certificates are to be used in the context of the intended use of the CPS Public. They may only be used according to the key usages defined in the certificates and not as a certification authority (sub-CA) or root certification authority (root-CA). The details are settled in the GTC, the Terms of Use for Public Certificates and the CPS Public.

4 Reliance limits

The TSP does not set any reliance limits for the certificates it issues, but the usage should adhere to the restrictions on liability (see chapter 7) as well as the intended purposes (see chapter 3).
In the certificate history, all relevant events are recorded and archived in a way to protect the integrity of the data. This includes all steps (if necessary) from the request process, the registration, the verification by the TSP, the production up to the revocation of a certificate.
Paper documents and electronically recorded requests as well as certificate data and data from the certificate history are archived for a further seven 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 CPS Public and the Terms of Use for Public Certificates. The documents are available at:
https://www.telesec.de/de/service/downloads/pki-repository/

6 Certificate status checking obligations of relying parties

Trusting third parties must 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 GTC or individually negotiated.

8 Applicable agreements, Terms of Use, CPS, GTC

This PDS, the Terms of Use for Public Certificates and the CPS Public are available at:

https://telesec.de/de/service/downloads/pki-repository/

The GTC is available at:

https://www.telekom.de/is-bin/INTERSHOP.enfinity/WFS/EKI-PK-Site/-/-/-/ViewAGB-Start?wt_mc=alias_agb/direkt&AGBID=2744

9 Availability of the service

The infrastructure of the Server.ID service installed in the Trust Center comprises the following components:

- A certification authority (CA) which is accessible via an online web portal,
- an ACME interface, and a REST interface,
- the LDAP directory service, used to call up revocation lists (CRLs), 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.
- ACME interface and REST interface 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

The TSP must store and process personal data electronically for the purpose of providing this service. The TSP 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.

10.1 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

The TSP archives the following data:

- Order documents on paper (e.g., quotations, orders),
- Other electronic order or validation documents,
- Information in certificate requests and regarding the certificate life cycle (e.g., revocation and renewal requests),
- 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 at least seven (7) years after the certificate validity expires.
- For Server.ID EV QWAC products they are archived until the end of operation.
- Audit, history and event logging data is archived in accordance with the current legal provisions.

11 Refund policy

Refund of fees by Deutsche Telekom Security GmbH is based on the legal regulations of German law. In addition, the provisions of the applicable GTC[4] or other contractual arrangements agreed with the customer apply.

12 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 53113 Bonn, Germany.

[4] https://www.telesec.de/de/service/downloads/allgemeine-geschaeftsbedingungen/

13 TSP and repository licenses, trust marks, and audit

13.1 Server.ID DV, OV and EV products

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

- [ETSI EN 319 401]: General Policy Requirements for TSPs
- [ETSI EN 319 411-1]: Policy and security requirements for TSPs

To verify conformity, the TSP is audited by internal auditors as well as by a recognized body according to [ETSI EN 319403]. 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).

13.2 Server.ID EV (QWAC) products

Certificates are issued subjects 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 GmbH meets the requirements of

- [ETSI EN 319 401]: General Policy Requirements for TSPs
- [ETSI EN 319 411-1]: Policy and security requirements for TSPs
- [ETSI EN 319 411-2]: Requirements for TSPs issuing EU qualified certificates
- ETSI EN 319 412-4]: Certificate profile for web site certificates
- [ETSI EN 319 412-5]: Certificate Profiles; Part 5: QC-Statements

To verify conformity, the TSP is audited by internal auditors as well as by a recognized body according to [ETSI EN 319403]. 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).

Please find the German list of accredited certification service providers on: https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/DE