PDS Server.ID (Telesec ServerPass)
PKI Disclosure Statement (PDS)

Deutsche Telekom Security GmbH

public

version:	05.00		Valid from:	01.03.2022
status:	release		valid with:	publication

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

Impressum

Herausgeber	Deutsche Telekom Security GmbH

Dateiname	Valid from	Titel
Server.ID_PDS_v05.00.docx	01.03.2022	PDS Server.ID (Telesec ServerPass)

Version	Status
05.00	release

Ansprechpartner	Telefon	E-Mail
Deutsche Telekom Security GmbH	+49 (0) 1805 268 204 (Festnetz 0,14 EUR/Minute, Mobilfunknetze max. 0,42 EUR/Minute)	telesec_support@t-systems.com

Kurzbeschreibung
PKI Disclosure Statement. Server.ID (TeleSec ServerPass) according to ETSI EN 319 411-1 and ETSI EN 319 411-2

Inhaltsverzeichnis

1   Introduction

Server.ID (TeleSec ServerPass) 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 (TeleSec ServerPass) consists of several "Trust Service Providers" (TSP) for issuing qualified and non-qualified certificates.

The service itself and all involved processes are described in the " Certification Practice Statement on Server.ID (TeleSec ServerPass) " (CPS), see chapter 8.

This document summarizes the key points of the CPS Server.ID (TeleSec ServerPass) and the general terms and conditions (GTC) (please refer to "Allgemeine Geschäftsbedingungen TeleSec-Produkte (AGB)") 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 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@t-systems.com

▪   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 solely issues and distributes organization and extended validation certificates. Depending on the product variant different public root certification authorities (root-CAs) are available. The validation processes are described in CPS. The end entity certificates refer entirely to X.509v3.

3.1 Server.ID Test (TeleSec ServerPass Test)

Non-qualified X.509v3 certificates for website authentication only for testing under a nonpublic testroot-CA.

Registration
▪ The serviceportal is mandatory for registration

Validity period
▪ 30 days

Procedure of validation
▪ online-order required

▪ no order verification

3.2 Server.ID Standard, Wildcard and Multidomain (TeleSec ServerPass Standard, Wildcard and Multidomain)

Non-qualified X.509v3 certificates for website authentication under a public root-CA.

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)

Registration
▪ The service portal is mandatory for registration

Validity period
▪ 1 year (plus grace period of 5 days)

Procedure of validation
▪ online-order required

▪ Organization validation

3.3 Server.ID EV, EV Multidomain (TeleSec ServerPass EV, EV Multidomain)

X.509v3 certificates for website authentication under a public Root-CA with extended validation.

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)

Registration
▪ The service portal is mandatory for registration

Validity period
▪ 1 year (plus grace period of 5 days)

Procedure of validation
▪ online-order required
▪ Extended validation

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 Server.ID (TeleSec ServerPass). 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 general terms and conditions (GTC) (please refer to "Allgemeine Geschäftsbe-dingungen TeleSec-Produkte (AGB)"), see chapter 5e), Server.ID (TeleSec ServerPass) Services and Terms and Conditions and the CPS.

3.4 Server.ID EV (QWAC), EV Multidomain (QWAC) (TeleSec ServerPass EV (QWAC), EV Multidomain (QWAC))

Extended validation qualified X.509v3 certificates for website authentication under a public Root-CA with qc-statement.

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)

Registration
▪ The service portal is mandatory for registration

Validity period
▪ 1 year (plus grace period of 5 days)

Procedure of validation
▪ online-order required
▪ Extended validation
▪ POSTIDENT as Identification according to the Regulation (EU) Nr. 910/2014 of the European Parliament and the Council („eIDAS").

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 Server.ID (TeleSec ServerPass). 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 general terms and conditions (GTC) (please refer to "Allgemeine Geschäftsbe-dingungen TeleSec-Produkte (AGB)"), see chapter 5e), Server.ID (TeleSec ServerPass) Services and Terms and Conditions and the CPS.

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 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 CPS Server.ID (TeleSec ServerPass) and the general terms and conditions (GTC) (please refer to "Allgemeine Geschäftsbedingungen TeleSec-Produkte (AGB)"). The documents are available at:
https://www.telesec.de/de/service/downloads/produkte-und-loesungen/ and
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 general terms and conditions (GTC) (please refer to "Allgemeine Geschäftsbedingungen TeleSec-Produkte (AGB)") or individually negotiated.

8 Applicable agreements, CPS, GTC

This PDS, the CPS and the general terms and conditions (GTC) (please refer to "Allgemeine Geschäftsbedingungen TeleSec-Produkte (AGB)") are available at:

https://www.telesec.de/de/service/downloads/produkte-und-loesungen/ and
https://www.telesec.de/de/service/downloads/pki-repository/.

9 Availability of the service

The infrastructure of the Server.ID (TeleSec ServerPass) 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, ARLs), 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

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),

- 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.

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 (please refer to "Allgemeine Geschäftsbedingungen TeleSec-Produkte (AGB)") 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.

13   TSP and repository licenses, trust marks, and audit

13.1   Server.ID EV, EV Multidomain (TeleSec ServerPass EV, EV Multidomain)

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), qEV Multidomain (QWAC) (TeleSec ServerPass EV (QWAC), qEV Multidomain (QWAC))

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 319 412-5]: 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