TeleSec ServerPass

PKI Disclosure Statement (PDS)

T-Systems International GmbH
Telekom Security

public

version:	2.4	date:	27.02.2019
status:	Final	valid with:	publication

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

Impressum

Herausgeber	T-Systems International GmbH Telekom Security

Dateiname	**Stand**	**Titel**
PDS ServerPass_EN_v2.4_Final_20190227.docx	27.02.2019	TeleSec ServerPass

Version	**Status**	**Freigegeben am**
2.4	final	27.02.2019

Ansprechpartner	**Telefon**	**E-Mail**
T-Systems – Telekom Security	+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 T-Systems TeleSec ServerPass according to ETSI EN 319 411-1 and ETSI EN 319 411-2

Inhaltsverzeichnis

1 Introduction 4

2 TSP contact info 4

3 Certificate type, validation procedures and usage 4

3.1 TeleSec ServerPass Test 5

3.2 TeleSec ServerPass Standard, Wildcard and SAN UCC 5

3.3 TeleSec ServerPass EV, EV SAN 6

4 Reliance limits 6

5 Obligations of subscribers 7

6 Certificate status checking obligations of relying parties 7

7 Limited warranty and disclaimer/Limitation of liability 7

8 Applicable agreements, CP/CPS, GTC 7

9 Privacy policy 7

10 Refund policy 8

11 Applicable law, complaints and dispute resolution 8

12 TSP and repository licenses, trust marks, and audit 8

1 Introduction

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 T-Systems International GmbH.

The certification service 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 "Certificate Policy and Certification Practice Statement on TeleSec ServerPass " (CP/CPS), see chapter 8.

This document summarizes the key points of the CP/CPS TeleSec ServerPass and the general terms and conditions (GTC) (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
  Digital & Security, Telekom Security, Delivery Telekom Security
  Trust Center & ID Solutions
  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)

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 CP/CPS. The end entity certificates refer entirely to X.509v3.

3.1 TeleSec ServerPass Test

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

Registration
▪ The customer portal is mandatory for registration
Validityperiod
▪ 30 days
Procedure of validation
▪ online-order required
▪ no order verification

3.2 TeleSec ServerPass Standard, Wildcard and SAN UCC

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

root CAs:

- CN=T-TeleSec GlobalRoot Class 2
- CN=TeleSec GlobalRoot Class 2 G2
- CN=Deutsche Telekom Root CA 2

sub-CAs:

- CN=TeleSec ServerPass Class 2 CA
- CN=TeleSec ServerPass CA 2 G2
- CN=TeleSec ServerPass DE-2

Registration
▪ The customer portal is mandatory for registration
Validityperiod
▪ 1 year, 2 years (plus grace period of 5 days)
Procedure of validation
▪ online-order required
▪ Organization validation

3.3 TeleSec ServerPass EV, EV SAN

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

root-CAs

- CN=T-TeleSec GlobalRoot Class 3
- CN=TeleSec GlobalRoot Class 3 G2

sub-CAs:

- CN = TeleSec ServerPass Extended Validation Class 3 CA
- CN = TeleSec ServerPass CA 3 G2

Registration
▪ The customer portal is mandatory for registration
Validityperiod
▪ 1 year, 2 years (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 CP/CPS 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) (Allgemeine Geschäftsbedingungen TeleSec-Produkte (AGB)), see chapter 5e) and the CP/CPS.

4 Reliance limits

T-Systems 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 CP/CPS TeleSec ServerPass and the general terms and conditions (GTC) (Allgemeine Geschäftsbedingungen TeleSec-Produkte (AGB)). The documents are available at: https://www.telesec.de/de/serverpass/support/downloadbereich

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) („Allgemeine Geschäftsbedingungen TeleSec-Produkte“ (AGB)) or individually negotiated.

8 Applicable agreements, CP/CPS, GTC

This PDS, the CP/CPS and the general terms and conditions (GTC) (Allgemeine Geschäftsbedingungen TeleSec-Produkte (AGB)) are available at: https://www.telesec.de/de/serverpass/support/downloadbereich.

9 Privacy policy

T-Systems must store and process personal data electronically for the purpose of providing this service. T-Systems 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 T-Systems is based on the legal regulations of German law. In addition, the provisions of the applicable GTC (Allgemeine Geschäftsbedingungen TeleSec-Produkte (AGB)) 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 T-Systems International GmbH in Frankfurt am Main, Germany.

12 TSP and repository licenses, trust marks, and audit

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, T-Systems 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 319 412-5]: Certificate Profiles: QC-Statements

To verify conformity, T-Systems 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://www.nrca-ds.de/en/index_e.html.