

T-Systems Public Key Service

PKI Disclosure Statement (PDS)

T-Systems International GmbH
TC Solutions

public

Version:	1.0	Valid from:	30.06.2017
Status:	final	Last review:	30.06.2017

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

Copyright © 2017 by T-Systems International GmbH, Frankfurt am Main

All rights, including reproduction in extracts, photomechanical reproduction (including microcopy), as well as evaluation by databases or similar facilities, are reserved.

Changes

Version	Date	Editor	Changes / Comments
1.0	30.06.2017	SK/DD	Approved Version

Table of contents

1	Introduction	3
2	TSP contact info	3
3	Certificate type, validation procedures and usage	4
4	Reliance limits	4
5	Obligations of subscribers	4
6	Certificate status checking obligations of relying parties.....	4
7	Limited warranty and disclaimer/Limitation of liability.....	5
8	Applicable agreements, CPS, CP	5
9	Privacy policy	5
10	Refund policy	5
11	Applicable law, complaints and dispute resolution.....	5
12	TSP and repository licenses, trust marks, and audit.....	5

1 Introduction

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

- TSP QES PKS: Certification service to issue qualified X509 certificates.
- TSP X.509 nonQES PKS: Certification service to issue non-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 319-11-1.

2 TSP contact info

TSP T-Systems can be reached via the following contacts:

- Address: T-Systems International GmbH, Trust Center Services,
Untere Industriestraße 20, D-57250 Netphen
- Phone: +49 271 708 1699
- E-Mail: trustcenter.notary@t-systems.com
- 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 for each PKS:

- One qualified X509 certificate for the creation of qualified electronic signatures (QES), issued by the TSP X.509 QES PKS.
- Three non-qualified X509 certificates issued by the TSP X.509 nonQES PKS.

All certificates are issued as part of one request- and issuing process, so the same requirements for identification, registration and verification apply to all certificates.

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

4 Reliance limits

T-Systems 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 ("Nutzungsbedingungen"), the document is available on the Internet: <https://www.telesec.de/de/signaturkarte/support/downloadbereich>.

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 and the terms and conditions („Nutzungsbedingungen“) are available on the Internet: <https://www.telesec.de/de/signaturkarte/support/downloadbereich>.

9 Privacy policy

T-Systems must store and process personal data electronically for the purpose of providing the 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 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 subject 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 319 412-2]: Certificate profile for certificates issued to natural persons
- [ETSI EN 319 412-5]: Certificate Profiles: QCStatements

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).