Telekom Security HBA

[HPC106] PKI Disclosure Statement (PDS)

Deutsche Telekom Security GmbH
Trust Center & ID Security

public

Version:	6.0	Valid from:	14.03.2024
Status:	geprüft	Last review:	08.03.2024

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

Changes

Version	Date	Editor	Changes / Comments
1.0	30.06.2017	SK/DD	Approved Version
1.1	01.03.2018	SK/DD	TSP contact info revised
1.2	03.02.2020	AK/DD	Annual review, no changes
1.3	26.06.2020	AK	Modifications due to carve out of Telekom Security
1.9	01.07.2020	Telekom Security	QS
2.0	04.07.2020	Telekom Security	Approved Version
2.1	03.02.2021	Telekom Security	Links updated due to new website telesec.de
2.1	09.02.2021	Telekom Security	QS
3.0	10.02.2021	Telekom Security	Approved Version
3.1	03.02.2022	Telekom Security	Chapter name and Links updated
3.2	04.02.2022	Telekom Security	QS
4.0	11.02.2022	Telekom Security	Approved Version
4.1	11.01.2023	Telekom Security	Annual review, typos corrected
4.2	13.01.2023	Telekom Security	QS
5.0	20.01.2023	Telekom Security	Approved Version
5.1	06.03.2024	Telekom Security	New card generation G2.1
5.2	08.03.2024	Telekom Security	QS
6.0	13.03.2024	Telekom Security	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 5

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 6

12 TSP and repository licenses, trust marks, and audit..... 6

1 Introduction

As part of the production of the Health Professional Card (HPC, in German "Heilberufsausweis", HBA) Telekom Security provides a certification service for physicians, dentists, psychotherapists and other Health professionals to issue certificates for the HBA.

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

- TSP X.509 QES HBA: Certification authority to issue qualified X509 certificates.
- TSP X.509 nonQES HBA: Certification authority to issue non-qualified X509 certificates.
- TSP CVC: Certification authority to issue Card Verifiable Certificates (CVC).
  The TSP CVC issues certificates for the card generations G2.1.

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 Telekom Security can be reached via the following contacts:

- Address: Deutsche Telekom Security GmbH, Trust Center & ID Security,
  Untere Industriestraße 20, D-57250 Netphen
- Phone: +49 271 708 1699
- E-Mail: Trust_Center_gematik@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

For information for submission of claims or complaints the customer-service can be reached as follows:

- Phone Germany (free): 0800 1183307
- E-Mail: service.map@telekom.de

3 Certificate type, validation procedures and usage

The following certificates are issued for each HBA:

- One qualified X509 certificate for the creation of qualified electronic signatures (QES), issued by the TSP X.509 QES HBA, one for each with RSA and ECC-Keypair (G2.1 Standard).
- Two non-qualified X509 certificates for encryption and authentication (ENC, AUT), issued by the TSP X.509 nonQES HBA, one for each with RSA and ECC-Keypair (G2.1 Standard).
- One CV certificate of generation 2, issued by the TSP CVC.

(During an interim phase all X509 certificates are produced in two versions, which only differs in the cryptographic algorithm used for signing the certificate)

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 predetermined procedures. In addition, the authorization to include the attribute for professional admission into the qualified certificates is examined by the responsible medical association as part of the approval process and confirmed to the TSP.

The certificates of the HBA are to be used in the context of the intended use within the telematics infrastructure. They can also be used for other purposes outside of the telematics infrastructure, but they may only be used according to the key usages defined in the certificates and not as a certification authority (CA) or root certification authority (root CA).The details are settled in the terms and conditions (see chapter 5) and the CPS (see chapter 8).

4 Reliance limits

Telekom Security does not set any reliance limits for the certificates it issues, but the restrictions on liability (see chapter 7) as well as the use according to the intended purposes must be observed.

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:

www.telesec.de ("Branchen & Eco-Systeme" > "Gesundheitswesen" > "Details“ > “Heilberufsausweis (HBA)")

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, liability for damage resulting from a breach of obligations due to negligence will be governed by individual agreement

8 Applicable agreements, CPS, CP

This PDS, the CPS and the terms and conditions (“Allgemeine Geschäftsbedingungen”) are available on the Internet:

www.telesec.de ("Branchen & Eco-Systeme" > "Gesundheitswesen" > "Details“ > “Heilberufsausweis (HBA)")

9 Privacy policy

Telekom Security must store and process personal data electronically for the purpose of providing the service. 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 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“)

To ensure conformity, 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, Telekom Security 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).