Trustcenter of Deutsche Rentenversicherung

Trust Service Provider Deutsche Rentenversicherung Bund according to eIDAS-RE

PKI Disclosure Statements of Certificate Authority DRV QC 70 MA CA

Document-OID: 1.3.6.1.4.1.22204.1.8.6.1.2

Version	01.02.00
Release	01.07.17
Document	TCDRV_PDS_DRV-QC-70-MA-CA_EN
Status	Released
Classification	Unrestricted

1 PKI Disclosure Statements

1.1 Scope

This document comprises the PKI Disclosure Statements for issuing qualified end-entity certificates (EE certificates) by Certificate Authority DRV QC 70 MA CA of TSP DRV Bund.

The qualified EE certificates will be issued to natural person on qualified electronic signature creation devices (QSCD) according to policy QCP-N-QSCD (refer to [2]).

1.2 Document Name and Identification

Document Name: PKI Disclosure Statements of Certificate Authority DRV QC 70 MA CA

Document-OID: 1.3.6.1.4.1.22204.1.8.6.1.2

PEN-DRV-Bund (1.3.6.1.4.1.22204).Trustcenter (1). Policies (8).
QC-DS (6). Productive System (1). QC-Sub-CA (2)

The document PKI Disclosure Statements is a subset of the document Certificate Policy:

- Certificate Policy of Certificate Authority DRV QC 70 MA CA
  Document-OID: 1.3.6.1.4.1.22204.1.8.1.1.2

1.3 Contact Addresses

Please use the following contact, if there are questions and/or comments to this policy document.

Postal Address:
Deutsche Rentenversicherung Bund
Abteilung Organisation und IT-Services
Trustcenter der Deutschen Rentenversicherung
10704 Berlin

Additional information can be downloaded from the specified web site.

Web site TSP DRV Bund [4]: Provisioning of the following information:

- PKI Disclosure Statements DRV QC Root CA
- Certificate Policy DRV QC Root CA
- Certificates of der DRV QC Root CA

1.4 Subscriber of the PKI Service

Employees of DRV Bund are the subscriber of qualified EE certificates on ES-CK issued by Certificate Authority DRV QC 70 MA CA.

Employees of DRV institutions are the subscriber of qualified EE certificates on MS-CK issued by Certificate Authority DRV QC 70 MA CA.

1.5 Issued Certificates

The qualified Certificate Authority DRV QC 70 MA CA issues EE certificates:

- Qualified signature certificates on single-signature smart cards (ES-CK),
- Qualified signature certificates on mass-signature smart cards (MS-CK).

The qualified EE certificates issued by Certificate Authority DRV QC 70 MA CA may be used for business purposes.

The private key corresponding to the qualified certificate may be used for issuing qualified electronic signatures. Additional use cases are not defined.

The Validation Service DRV QC 70 MA OCSP (OCSP responder) provides certificate status information for qualified certificates issued by Certificate Authority DRV QC 70 MA CA.

If the operation of the Certificate Authority DRV QC 70 MA CA and respectively the Validation Service DRV QC 70 MA OCSP will be terminated, then the certificate revocation information will be provided in form of a certificate revocation list.

The certificate revocation information will be provided until 30 years of expiration of the appropriate certificate.

1.6 Trustworthiness of issued certificates

The cryptographic keys are created and used on ES-CK / MS-CK smart cards. These smart cards are certified according to Common Criteria EAL4+. BSI lists the smart cards as qualified electronic signature creation devices (QSCD).

The archived data concerning created qualified certificates will be preserved for 30 years after expiration of the issued certificates. Considering the certificate lifetime, the archived data will be preserved for 35 years.

1.7 Obligations of Subscriber

The subscriber are obligated to use their ES-CK / MS-CK smart card according to the defined purposes.

The subscriber of MS-CK have in addition the obligation to consider the provisions of the confirmation certificate regarding the requirements to the environment, where the MS-CK shall be used. The confirmation certificate can be downloaded from [6].

The obligation for revocation of certificates of ES-CK / MS-CK is defined in the Certificate Policy of Certificate Authority DRV QC 70 MA CA. This policy document can be downloaded from the web site of TSP DRV Bund (see chapter 1.3).

1.8 Obligations of Relying Parties

Relying parties, who rely on a qualified EE certificate, have the obligation to validate the certificates. The validation shall be done using the appropriate Validation Service (OCSP responder). If the operation of the Certificate Authority DRV QC 70 MA CA and respectively the Validation Service DRV QC 70 MA OCSP will be terminated, then certificate revocation information will be provided in form of a certificate revocation list on the web site of TSP DRV Bund. Invalid certificates shall not be used.

The URLs for downloading the issuer certificate and for getting access to the appropriate Validation Service (OCSP responder) are included in the issued qualified EE certificates.

Relying parties shall consider the restrictions for the usage of the cryptographic keys. The restrictions are included in the certificate in the extensions "Key Usage" and if existing "Extended Key Usage" (see [3] chapter 7.1).

Relying parties shall consider the restrictions for the usage of the qualified certificates. The restrictions are defined in the appropriate Certificate Policy (see [3] chapter 1.4).

The Certificate Policy [3] can be downloaded from the web site of TSP DRV Bund [4].

Relying parties shall inform the TSP DRV Bund in case of suspicion of misuse or detected misuse of the qualified certificate. The contact address defined in chapter 1.3 shall be used.

1.9 Liability of Trust Service Provider

TSP DRV Bund is liable according to general national lawful regulations according to article 13 of eIDAS-RE.

1.10 Guidelines for Certificate Authority

The provisions for issuing of qualified certificates are defined in the appropriate policy documents:

Document	Classification	Published on
Certificate Policy of Certificate Authority DRV QC Root CA	Unrestricted	Web site of TSP DRV Bund (see chapter 1.3)
Certification Practice Statements of Certificate Authority DRV QC Root CA	Restricted - for internal use only	Written request to contact address (see chapter 1.3)

1.11 Privacy Policy

TSP DRV Bund meets the requirements for private data protection according to BDSG.

The amount of the collected private data of the subscriber depends on the provisions of eIDAS-RE. The subscriber of qualified certificates on ES-CK / MS-CK are informed about the collected private data (type and amount of data, storage, and retention period).

1.12 Fees and Refund Policy

No stipulation.

1.13 Governing Law and Dispute Settlement

German law and eIDAS-RE are applicable. The eIDAS-RE is prioritised and overrides German law in case of differences.

The arbitration board of the Trustcenter of DRV executes surveys and complaints about qualified time stamps and the used qualified certificates. The arbitration board is also responsible to settle disputes.

The arbitration board can be reached as follows:

E-Mail	Trustcenter-gRV@drv-bund.de
Postal Address	Deutsche Rentenversicherung Bund 1178-81 Trustcenter / Schiedsstelle D-10704 Berlin

1.14 Compliance with Applicable Law

The Certificate Authority DRV QC 70 MA CA is operated as trust services issuing qualified certificates according to eIDAS-RE [1]. The services is operated compliant to the relevant ETSI norms [2].

The last conformity assessment took place in first quarter 2017 by the CAB TÜVIT GmbH. The CAB publishes the conformity certificate after successful assessment [5].

2 Information to the Document

2.1 Abbreviations

BDSG	Privacy Law of Federal Republic of Germany (Bundesdatenschutzgesetz)
CA	Certificate Authority
CC	Common Criteria
CP	Certificate Policy
CPS	Certification Practice Statements
DRV	Deutsche Rentenversicherung
EAL	Evaluation Assurance Level
EE	End Entity
ES-CK	Single-Signature Smart Card (Einzelsignaturchipkarte)
ETSI	European Telecommunications Standard Institute
IT	Information Technology
MA	Employee (Mitarbeiter)
MS-CK	Mass-Signature Smart Card (Massensignaturchipkarte)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PEN	Private Enterprise Number
PKI	Public Key Infrastructure
QC	Qualified Certificate
RE	Regulation
TSA	Time Stamp Authority
TSP	Trust Service Provider
URL	Unified Resource Locator
VA	Validation Authority

2.2 Document History

Version	Date	Ch.	Reason	Author
01.00.00	21.04.2017	All	Initial Document	Atos
01.01.00	10.05.2017	1.5, 1.8	Update	Atos
01.02.00	01.07.2017	1.13	Postal address for dispute resolution has been changed	Atos

2.3 References

[1] eIDAS-RE: REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, released in the Official Journal of the European Union L257/73; http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32014R0910

[2] ETSI EN 319 411-2 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/

[3] Certificate Policy of Certificate Authority DRV QC 70 MA CA

[4] Web-Site of TSP DRV Bund; http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html

[5] Web-Site of CAB TÜVIT for publication of CAR for TSP conformity assessment; https://www.tuvit.de/de/zertifikate-1265-4512.htm

[6] Confirmation Certificate "Digitale Signatur: Sichere Signaturerstellungseinheiten CardOS V5.0 with Application for QES, V1.0", published by BNetzA; https://www.bundesnetzagentur.de/SharedDocs/QESProdukte/Signaturkarten/CardOS%20V5.0.html?nn=322598