Trustcenter of Deutsche Rentenversicherung

Trust Service Provider Deutsche Rentenversicherung Bund according to eIDAS-RE

Certificate Policy of Certificate Authority DRV QC Root CA

Document-OID: 1.3.6.1.4.1.22204.1.8.1.1.1

Version	06.02.00
Release	01.07.17
Document	TCDRV_CP_DRV-QC-Root-CA_EN
Status	Released
Classification	Unrestricted

Table of Contents

1 Introduction

1.1 Overview

The institutions of Deutsche Rentenversicherung (DRV) operate a common Trustcenter with qualified trust services according to eIDAS-RE [1]. The following trust service provider (tenants in the Trustcenter of DRV) provide qualified trust services:

(1) TSP DRV Bund provides:

- Certificate Authority DRV QC Root CA:
  Qualified trust service DRV QC Root CA for issuance of:
  - CA certificates for DRV QC Root CA, DRV QC 70 MA CA, DRV QC 13 MA CA and DRV QC 11 MA CA,
  - TSA certificates for Time Stamp Authority DRV QC Root TSA,
  - OCSP certificates for Validation Service DRV QC Root OCSP;
- Time Stamp Authority DRV QC Root TSA:
  Qualified trust service DRV QC Root TSA for issuance of:
  - qualified time stamps;
- Certificate Authority DRV QC 70 MA CA:
  Qualified trust service DRV QC 70 MA CA for issuance of:
  - Qualified EE certificates,
  - OCSP certificates for Validation Service DRV QC 70 MA OCSP;

(2) TSP DRV Rheinland provides:

- Certificate Authority DRV QC 13 MA CA:
  Qualified trust service DRV QC 13 MA CA for issuance of:
  - Qualified EE certificates,
  - OCSP certificates for Validation Service DRV QC 13 MA OCSP;

(3) TSP DRV Westfalen provides:

- Certificate Authority DRV QC 11 MA CA:
  Qualified trust service DRV QC 11 MA CA for issuance of:
  - Qualified EE certificates,
  - OCSP certificates for Validation Service DRV QC 11 MA OCSP.

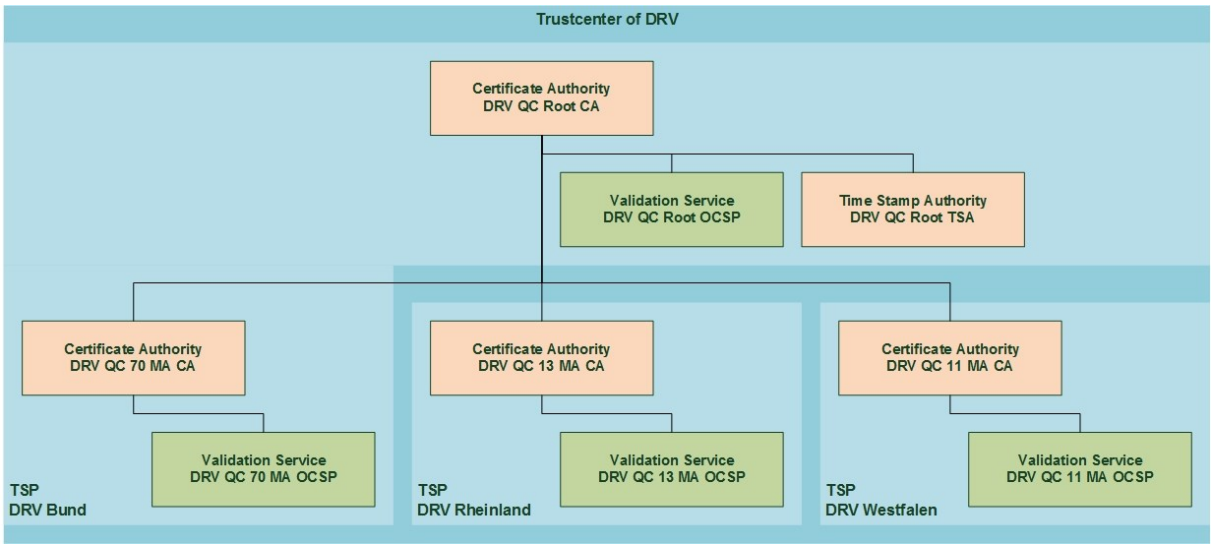

Figure 1 Qualified Trust Services in the Trustcenter of DRV

Certificate Authority DRV QC Root CA issues Root CA certificates, which are the trust anchor for the complete qualified certificate hierarchy in the Trustcenter of DRV.

Each qualified Certificate Authority uses its own QSCD for storage and usage of its private key for signing of qualified certificates.

The qualified Time Stamp Authority uses its own QSCDs for storage and usage of its private keys for signing of qualified time stamps.

The Validation Services (OCSP responder) use their own QSCDs for storage and usage of their private keys for signing of OCSP responses.

The next figure gives an overview about the relevant policy documents of the Certificate Authority DRV QC Root CA.

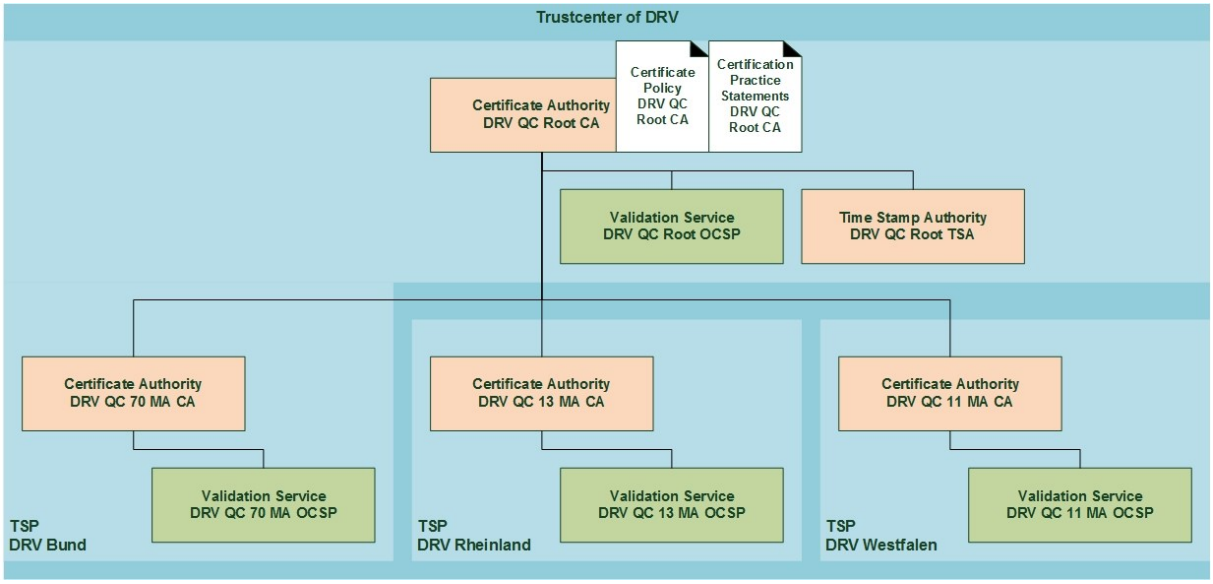

Figure 2 Policy Documents of Certificate Authority DRV QC Root CA

This document comprises the Certificate Policy for issuing qualified system certificates (CA/TSA//OCSP certificates) by Certificate Authority DRV QC Root CA as well as for issuing qualified system certificates (OCSP certificates) by Certificate Authorities of the tenants of the Trustcenter of DRV.

The qualified system certificates are issued to natural person on qualified electronic signature creation devices (QSCD) according to policy QCP-N-QSCD (refer to [7]).

This policy is structured according to RFC 3647 (see [2]).

1.2 Document Name and Identification

Document Name: Certificate Policy of Certificate Authority DRV QC Root CA

Document-OID: 1.3.6.1.4.1.22204.1.8.1.1.1

PEN-DRV-Bund (1.3.6.1.4.1.22204).Trustcenter (1).Policies (8).
QC-CP (1).Productive System (1).QC-Root-CA (1)

This document Certificate Policy of Certificate Authority DRV QC Root CA considers the relevant ETSI norms:

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [5];
- ETSI EN 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements [6];
- ETSI EN 319 411-2: 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 [7].

The standard ETSI EN 319 401 defines general requirements for a trust service provider (TSP). A TSP for certification services has to consider the requirements in standard ETSI EN 319 411-1. A TSP issuing qualified certificates has in addition also to consider the requirements in standard ETSI EN 319 411-2.

1.3 PKI Participants

1.3.1 Certificate Authorities

The institutions of Deutsche Rentenversicherung are operating a common Trustcenter of DRV. The TSP DRV Bund operates the qualified Certificate Authority DRV QC Root CA for issuing of qualified CA certificates for itself (self-signed) and for the Certificate Authorities of the tenants of the Trustcenter of DRV. This service issues in addition the qualified system certificates for the Validation Service DRV QC Root OCSP and the Time Stamp Authority DRV QC Root TSA.

The qualified Certificate Authorities of the tenants of the Trustcenter of DRV are issuing amongst others qualified system certificates for their own Validation Services.

The Certificate Authorities of the Trustcenter of DRV are using together the same central certificate management system.

The certificate of the Certificate Authority DRV QC Root CA is the trusted anchor of the hierarchy of qualified certificates in the Trustcenter of DRV.

1.3.2 Registration Authorities

The security representative of DRV Bund or the manager of TSP DRV Bund perform the registration process of the subscriber of qualified system certificates.

1.3.3 Subscriber

The qualified Certificate Authorities of the Trustcenter of DRV issue qualified system certificates for natural person as certificate holder (subscriber):

(1) Manager of TSP DRV Bund is certificate holder for:
   - Certificate of Root Certificate Authority DRV QC Root CA,
   - Certificates of Certificate Authorities of the tenants.

(2) Responsible system administrator server of TSP DRV Bund is certificate holder for:
   - Certificates of Time Stamp Authority DRV QC Root TSA,
   - Certificates of Validation Service DRV QC Root OCSP,
   - Certificates of Validation Services of the tenants.

The manager of TSP DRV Bund is the certificate holder for the qualified Certificate Authority DRV QC Root CA. The manager of TSP DRV Bund is also the certificate holder for the qualified Certificate Authorities of the tenants of the Trustcenter of DRV due to administrative agreements with the appropriate tenants.

The responsible system administrator server of TSP DRV Bund is the certificate holder for the certificates of Time Stamp Authority DRV QC Root TSA as well as of Validation Services DRV QC Root OCSP, DRV QC 70 MA OCSP, DRV QC 13 MA OCSP and DRV QC 11 MA OCSP due to administrative agreements.

The applications for certificate holder of qualified system certificates are not barrier-free due to technical reasons. There are limitations for administrators in trusted roles.

1.3.4 Relying Parties

The relying parties comprise all persons and systems, who or which rely on the trustworthiness of issued certificates and therefore have to check the status of the issued certificates. Relying parties include amongst others:

- Certificate holder,
- Employees of the tenants of the Trustcenter of DRV,
- Employees of other DRV institutions, if certificates are used in business processes,
- Employees of national or international public authorities, if certificates are used in business processes.

1.3.5 Other Parties

The security representative of DRV Bund and a TSP independent auditor accompany the key ceremony of the Certificate Authority DRV QC Root CA. The tasks of these persons are described in the document Certification Practice Statements.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The qualified system certificates issued by Certificate Authority DRV QC Root CA may be used for:

- CA certificate for Certificate Authority DRV QC Root CA,
- CA certificate for Certificate Authorities of the tenants of the Trustcenter of DRV,
- OCSP certificates for Validation Service DRV QC Root OCSP,
- TSA certificates for Time Stamp Authority DRV QC Root TSA.

The qualified system certificates issued by Certificate Authorities of the tenants of the Trustcenter of DRV may be used for:

- OCSP certificates for Validation Services of the appropriate tenant.

1.4.2 Prohibited Certificate Uses

The usage of qualified system certificates is limited to the statements in chapter 1.4.1. It is not allowed to use these certificates for other purposes.

1.5 Policy Administration

1.5.1 Administering of the Document

The TSP DRV Bund is responsible to maintain this policy document.

1.5.2 Contact Person

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

The document "Certificate Policy of Certificate Authority DRV QC Root CA" will be published after formal approval according to chapter 2.2.

1.5.3 Person Determining CPS Suitability for the Policy

The policy requirements and the guidelines for practice statements are reviewed and approved by the same body (refer to chapter 1.5.2).

1.5.4 CPS Approval Procedures

An approval process is not explicitly defined. Consistency between the documents Certificate Policy and Certification Practice Statements will be reached due to the responsibility of the same body to both documents.

1.6 Definitions and Acronyms

Terms and Abbreviations are defined in chapter 10.

2 Publication and Repository Responsibilities

2.1 Repositories

The system certificates issued by Certificate Authority DRV QC Root CA and by the qualified Certificate Authorities of the tenants (CA/TSA/OCSP certificates) are published into the repository of the Trustcenter of DRV.

The appropriate OCSP responder delivers OCSP responses for the issued certificates. An OCSP responder belongs to exactly one Certificate Authority.

The issued certificates include URL's of the repository for downloading the issuer certificate. The issued certificates also include the URL of the appropriate OCSP responder to get the current certificate status. Issuer certificates and OCSP responder are publicly available.

2.1.1 Repository Service

The repository of the Trustcenter of DRV publishes the qualified system certificates (CA/TSA/OCSP certificates) issued by the qualified Certificate Authorities. These certificates are publicly available.

The published certificates can be downloaded from the repository of the Trustcenter of DRV via HTTP and LDAP from the internet as well as from the DRV network. The appropriate URL's of the HTTP and LDAP services for downloading the issuer certificate are included in the extension "Issuer Alt Name (IAN)" of the issued certificates.

The repository of the Trustcenter of DRV is high available 24 hours per day, 7 days per week.

2.1.2 Validation Service

The status of the issued certificates can be requested from the appropriate Validation Service (OCSP responder). The OCSP response can deliver the following certificate status: "Good", "Revoked" or "Unknown". The appropriate URL of the OCSP responder is included in the extension "Authority Info Access (AIA)" of the issued certificates.

The Validation Service DRV QC Root OCSP provides OCSP responses about the status of certificates issued by Certificate Authority DRV QC Root CA. The OCSP responses will be provided until 30 years after certificate expiration. If the operation of Certificate Authority DRV QC Root CA and respectively the Validation Service DRV QC Root OCSP will be terminated, then the certificate revocation information will be provided in form of a certificate revocation list (CRL).

The Validation Service of the Trustcenter of DRV is high available 24 hours per day, 7 days per week.

2.1.3 TSL of NSB

The qualified system certificates issued by the Certificate Authority DRV QC Root CA for the qualified trust services of the Trustcenter of DRV (CA/TSA certificates) are handed over to the National Supervisory Body (NSB) according to article 17 of eIDAS-RE [1]. NSB publishes the qualified certificates of the qualified trust services in case of a positive CAR (see chapter 8) according to article 22 of eIDAS-RE in the national Trust-Service Status List (TSL) [12].

2.2 Publication of Information

This document "Certificate Policy of Certificate Authority DRV QC Root CA" will be published on the web site of TSP DRV Bund [10].

The terms and conditions of the Certificate Authority DRV QC Root CA will be published in form of "PKI Disclosure Statements" on the web site of TSP DRV Bund.

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

Document-OID: 1.3.6.1.4.1.22204.1.8.6.1.1

The document "Certification Practice Statements of Certificate Authority DRV QC Root CA" will not be published and can be requested in case of reasonable necessity from TSP DRV Bund via the known contact address (refer to chapter 1.5.2).

The certificates of the Root Certificate Authority DRV QC Root CA are published in addition on the web site of TSP DRV Bund DRV Bund and in the journal „RVaktuell“. "RVaktuell" is the official journal of DRV.

If the service of Certificate Authority DRV QC Root CA and respectively the Validation Service DRV QC Root OCSP will be terminated, then the certificate revocation information will be provided in form of a certificate revocation list (CRL). This CRL will be published on the web site of TSP DRV Bund for 30 years.

The web site of TSP DRV Bund is high available 24 hours per day, 7 days per week.

2.3 Time or Frequency of Publication

The time and frequency of the publication depends on the type of information. The next table gives an overview about the relevant information:

Table 1: Published Information

Information	Frequency of issuance	Time of publication	Target of publication
Document CP	Update if required	After approval of the document	• Web site of TSP DRV Bund
Document PKI Disclosure Statements	Update if required	After approval of the document	• Web site of TSP DRV Bund
Document CPS	Update if required	No publication	• not relevant
Certificate of Certificate Authority DRV QC Root CA (Root CA certificate)	Certificate renewal in advance of expiration of the current certificate	Directly after issuing of the certificate	• Web site of TSP DRV Bund • Journal RVaktuell • Repository • Validation Service • TSL
Certificate Revocation List of Certificate Authority DRV QC Root CA	One-time generated, if the operation of the Certificate Authority will be terminated	After generation of the CRL	• Web site of TSP DRV Bund
Certificates of Validation Service DRV QC Root OCSP	Directly after certificate renewal of the appropriate Root CA certificate	Directly after issuing of the certificates	• Validation Service
Certificates of Time Stamp Authority DRV QC Root TSA	Directly after certificate renewal of the appropriate Root CA certificate	Directly after issuing of the certificates	• Validation Service • TSL
Certificates of qualified Certificate Authorities of the tenants	Directly after certificate renewal of the appropriate Root CA certificate	Directly after issuing of the certificates	• Repository • Validation Service • TSL
Certificates of qualified Validation Services of the tenants	Directly after certificate renewal of the appropriate tenant CA certificate	Directly after issuing of the certificates	• Validation Service

2.4 Access Controls on Repositories

The access to the repositories is limited by appropriate access controls. The next table gives an overview about the access controls in place:

Table 2: Access Controls for the Repositories

Publication system	Access for	Access by	Access control
Web site of TSP DRV Bund	Create Change Delete	Web-Admin	Authentication is required
	Read	Unrestricted	Anonymous
Repository	Create Change Delete	Certificate Management System	Authentication is required
	Read	Unrestricted for system certificates	Anonymous
Validation service	Create Change Delete	Certificate Management System	Authentication is required
	OCSP request	Unrestricted	Anonymous

3 Identification and Authentication

This chapter describes identification and authentication of the subscriber of the qualified system certificates.

3.1 Naming

3.1.1 Type of Names

The qualified system certificates, issued by Certificate Authority DRV QC Root CA or by the qualified Certificate Authorities of the tenants, include the following attributes in issuer and subject name:

- Common Name,
- Organizational Unit,
- Organization,
- Country.

The attribute „Organizational Unit“ is used to distinguish different Certificate Authorities of a TSP. The attribute „Common Name“ is used to give the certificate a meaningful name. The next table gives an overview about the used names for qualified system certificates.

Table 3: Names for system certificates

Subject	Subject Name
Certificate Authority DRV QC Root CA	CN=DRV QC Root CA <JJJJ><V> OU=QC Root CA O=Deutsche Rentenversicherung C=DE
Validation Service DRV QC Root OCSP	CN=DRV QC Root OCSP <JJJJ><V> OU=QC Root CA O=Deutsche Rentenversicherung C=DE
Time Stamp Authority DRV QC Root TSA	CN=DRV QC Root TSA <JJJJ><V> OU=QC Root CA O=Deutsche Rentenversicherung C=DE
Certificate Authority DRV QC 70 MA CA	CN=DRV QC 70 MA CA <JJJJ><VV> OU=QC 70 Mitarbeiter CA O=Deutsche Rentenversicherung Bund C=DE
Validation Service DRV QC 70 MA OCSP	CN=DRV QC 70 MA OCSP <JJJJ><VV> OU=QC 70 Mitarbeiter CA O=Deutsche Rentenversicherung Bund C=DE
Certificate Authority DRV QC 13 MA CA	CN=DRV QC 13 MA CA <JJJJ><VV> OU=QC 13 Mitarbeiter CA O=Deutsche Rentenversicherung Rheinland C=DE

Subject	Subject Name
Validation Service DRV QC 13 MA OCSP	CN=DRV QC 13 MA OCSP <JJJJ><VV> OU=QC 13 Mitarbeiter CA O=Deutsche Rentenversicherung Rheinland C=DE
Certificate Authority DRV QC 11 MA CA	CN=DRV QC 11 MA CA <JJJJ><VV> OU=QC 11 Mitarbeiter CA O=Deutsche Rentenversicherung Westfalen C=DE
Validation Service DRV QC 11 MA OCSP	CN=DRV QC 11 MA OCSP <JJJJ><VV> OU=QC 11 Mitarbeiter CA O=Deutsche Rentenversicherung Westfalen C=DE

Data in angle brackets <…> are placeholder.

Data in square brackets […] are optional.

Table 4: Explanation of placeholder

Placeholder	Explanation	Range (examples)
<JJJJ>	Year of creation	2017, 2018, …
<V>	Version of certificates of first level	a, b, …
<VV>	Version of certificates of second level, the first letter is copied from the issuer	aa, ab, … ba, bb, …

Remarks:

- The version of CA certificates of second level includes as the first letter the version of the issuing Root CA certificate.
- The version of TSA certificate is identical with the version of the issuing Root CA certificate.
- The version of OCSP certificates are identical with the version of the issuing CA certificate.

3.1.2 Need for Names to be Meaningful

The attribute "Common Name" gives each qualified system certificate a meaningful name.

3.1.3 Anonymity or Pseudonymity of Subscribers

The qualified system certificates (CA/OCSP/TSA certificates) are issued for natural persons identified by pseudonyms. The assignment of pseudonyms to natural persons is realized by organizational means. The pseudonym is included in the issued certificates in the extension "Subject Directory Attributes":

Table 5: Pseudonyms in qualified system certificates

Service	Subject Name	Pseudonym for Certificate Holder
Certificate Authority	DRV QC Root CA	Zertifikatsdienst DRV QC Root CA <NN>:PN
	DRV QC 70 MA CA	Zertifikatsdienst DRV QC 70 MA CA <NN>:PN
	DRV QC 13 MA CA	Zertifikatsdienst DRV QC 13 MA CA <NN>:PN
	DRV QC 11 MA CA	Zertifikatsdienst DRV QC 11 MA CA <NN>:PN
Validation Service	DRV QC Root OCSP	Validierungsdienst DRV QC Root OCSP <S><NN>:PN
	DRV QC 70 MA OCSP	Validierungsdienst DRV QC 70 MA OCSP <S><NN>:PN
	DRV QC 13 MA OCSP	Validierungsdienst DRV QC 13 MA OCSP <S><NN>:PN
	DRV QC 11 MA OCSP	Validierungsdienst DRV QC 11 MA OCSP <S><NN>:PN
Time Stamp Authority	DRV QC Root TSA	Zeitstempeldienst DRV QC Root TSA <S><NN>:PN

Table 6: Explanation of the placeholder

Placeholder	Explanation	Range (examples)
<S>	Abbreviation of the location, where the service is operated	B for Berlin, W for Wurzburg
<NN>	Sequential 2-digit number	01, 02, …

3.1.4 Rules for Interpreting Various Name Forms

Various name forms does not exist.

3.1.5 Uniqueness of Names

The used names are unique by definition.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Private keys are generated on qualified signature creation devices (QSCD) in the protected environment of the Trustcenter of DRV.

The proof of possession of private CA keys is implicitly processed by the certificate management system during certificate issuance process.

The proof of possession of private TSA/OCSP keys is processed explicitly via signature validation of the PKCS#10 certificate request by the certificate management system.

3.2.2 Authentication of Organization Identity

The organization of natural person will be authenticated in a secure way using their employee ID card. The key ceremony protocol includes amongst others the following data of the certificate holder or the auditor:

- Personnel number.

3.2.3 Authentication of Individual Identity

Natural person will be authenticated in a secure way using their identity card or passport. The key ceremony protocol contains amongst others the following data of the certificate holder:

- Name, surname(s), title,
- Date of birth, place of birth, citizenship,
- Type, number and validity of the official identity document.

3.2.4 Non-Verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

Subscriber get the authorization for holding qualified system certificates through administrative agreements or the role description for system administrator server. The manager of TSP DRV Bund or his deputies will perform the verification of authorization of the system administrator server.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Renewal Requests

3.3.1 Identification and Authentication for Routine Renewal

The identity validation for renewal of system certificates will be processed in the same way like for initial system certificate issuance.

3.3.2 Identification and Authentication for Renewal after Revocation

The identity validation after revocation of system certificates will be processed in the same way like for system initial certificate issuance.

3.4 Identification and Authentication for Revocation Request

Only authorized persons have the right to request the revocation of qualified system certificates. The following person are authorized to revoke qualified system certificates:

- Employees of NSB (BNetzA),
- Manager of TSP DRV Bund or his deputies,
- Manager of TSP DRV Rheinland or his deputy,
- Manager of TSP DRV Westfalen or his deputy.

The authorized persons are informed in written form about the identification of the requestor and the authorization of revocation requests.

The process of certificate revocation will be described in the document Certification Practice Statements.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

The provisions will be defined in the document Certification Practice Statements.

4.2 Certificate Application Processing

The provisions will be defined in the document Certification Practice Statements.

4.3 Certificate Issuance

The provisions will be defined in the document Certification Practice Statements.

4.4 Certificate Acceptance

The provisions will be defined in the document Certification Practice Statements.

4.5 Key Pair and Certificate Usage

The provisions will be defined in the document Certification Practice Statements.

4.6 Certificate Renewal

The provisions will be defined in the document Certification Practice Statements.

4.7 Certificate Renewal with Re-Key

The provisions will be defined in the document Certification Practice Statements.

4.8 Certificate Modification

The provisions will be defined in the document Certification Practice Statements.

4.9 Certificate Revocation and Suspension

The reasons for certificate revocation are defined in the next sub-chapter. The provisions for the revocation procedure will be defined in the document Certification Practice Statements.

4.9.1 Circumstances for Revocation

Reasons for certificate revocation are:

- Certificate holder (subscriber) leaves the organization,
- Loss, defect or theft of the appropriate system smart card,
- Wrong information in issued certificates,
- Necessary changes in certificate attributes,
- System smart cards are no longer approved for use as QSCD,
- Suspicion of misuse of the private key,
- Compromise of the private key of the issuing CA,
- Certificate is no longer used (e.g. in case of termination of operation),
- Irregularities in the processes registration, initialization, key generation or certificate issuance.

4.10 Certificate Status Services (OCSP)

The provisions will be defined in the document Certification Practice Statements.

4.11 End of Subscription

The provisions will be defined in the document Certification Practice Statements.

4.12 Key Escrow and Recovery

The provisions will be defined in the document Certification Practice Statements.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

Physical security controls will be defined in the document Certification Practice Statements.

5.2 Procedural Controls (Organization)

Procedural security controls will be defined in the document Certification Practice Statements.

5.3 Personnel Controls

Personnel security controls will be defined in the document Certification Practice Statements.

5.4 Audit Logging Procedure

Provisions for monitoring and audit logging will be defined in the document Certification Practice Statements.

5.5 Records Archival

Provisions for data archiving will be defined in the document Certification Practice Statements.

5.6 Key Changeover

Provisions for the key ceremony of Certificate Authorities will be defined in the document Certification Practice Statements.

5.7 Compromise and Disaster Recovery

Provisions for activities after compromising technical systems or cryptographic keys as well as measures for the recovery of services after a disaster will be defined in the document Certification Practice Statements.

5.8 Termination of Service

The qualified Certificate Authority DRV QC Root CA issues certificates for the following trust services:

- Qualified Time Stamp Authority DRV QC Root TSA,
- Qualified Certificate Authority DRV QC 70 MA CA,
- Qualified Certificate Authority DRV QC 13 MA CA and
- Qualified Certificate Authority DRV QC 11 MA CA.

The manager of TSP DRV Bund decides in collaboration with the directorate of DRV Bund about the termination of the qualified trust service DRV QC Root CA. The manager of TSP DRV Rheinland and TSP DRV Westfalen are involved in the decision process.

The qualified trust service DRV QC Root CA can only be terminated, if all subordinated trust services are terminated.

The following provisions shall be met in the termination process of the qualified trust service DRV QC Root CA:

- Handover of obligations, tasks and documentation:

  Obligations, tasks and documentation shall not be handed over to another trust service provider. The Certificate Authority service shall not be continued.

  All valid certificates of the Certificate Authority DRV QC Root CA will be revoked. One of the last tasks of the Certificate Authority DRV QC Root CA will be the creation of a complete certificate revocation list (CRL).

  The certificates of the Certificate Authority DRV QC Root CA as well as the complete CRL of this service will be published on the web site of TSP DRV Bund (see chapter 2.2).

  The concepts and the documentation of the trust service DRV QC Root CA will be archived by the TSP DRV Bund. The archived data concerning created qualified certificates will be preserved for the legally required time period. The documents can be requested for inspection in authorized cases.

- Informational obligations

  The TSP DRV Bund informs the subscriber directly about the termination of the qualified trust service DRV QC Root CA and the depending subordinated trust services.

  The TSP DRV Bund informs the NSB according to eIDAS-RE about the planned termination of the qualified trust service DRV QC Root CA in advance.

  The TSP DRV Bund informs the relying parties about the termination of the qualified trust service DRV QC Root CA on the web-site of TSP DRV Bund.

- Coordinated demolition:

  The private key of the qualified Certificate Authority DRV QC Root CA will be destroyed. Afterwards, it is not possible to create any certificate with this Certificate Authority.

The procedures for the termination of the qualified trust service DRV QC Root CA are described in detail in the termination plan of the Trustcenter of DRV [9].

6 Technical Security Controls

6.1 Key Pair Generation and Installation

Technical security controls regarding key generation and key installation will be defined in the document Certification Practice Statements.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Technical security controls regarding protection of private keys will be defined in the document Certification Practice Statements.

6.3 Other Aspects of Key Pair Management

Technical security controls regarding key management will be defined in the document Certification Practice Statements.

6.4 Activation Data

Technical security controls regarding the management of activation data will be defined in the document Certification Practice Statements.

6.5 Computer Security Controls

Technical security controls regarding security of computer systems will be defined in the document Certification Practice Statements.

6.6 Life Cycle Technical Controls

Technical security controls for the operation of the Trustcenter of DRV will be defined in the document Certification Practice Statements.

6.7 Network Security Controls

Technical security controls regarding network will be defined in the document Certification Practice Statements.

6.8 Time-Stamping

Technical security controls regarding time synchronization will be defined in the document Certification Practice Statements.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

TSP DRV Bund issues qualified system certificates according to RFC 5280 [3].

7.1.1 Version Number(s)

TSP DRV Bund issues X.509 certificates version 3 according to RFC 5280 [3].

7.1.2 Certificate Extensions

The qualified system certificates of trusted services include certificate extensions according to RFC 5280 [3]. The following certificate extensions shall be used:

Table 7: Certificate extensions for qualified system certificates

Extension	Explanation	Used for			
		QC Root CA	QC Root OCSP QC Root TSA	QC 70 MA CA QC 13 MA CA QC 11 MA CA	QC 70 MA OCSP QC 13 MA OCSP QC 11 MA OCSP
Authority Key Identifier	Hash value of the public issuer key		x	x	x
Subject Key Identifier	Hash value of the public subject key	x		x	
Certificate Policies	OID & URL of the policy of DRV; OID & URL of the policy QCP-N-QSCD	x	x	x	x
Subject Directory - Attributes	Pseudonym of the certificate holder	x	x	x	x
Authority Info Access	URL of Validation Service (OCSP responder) for certificate status checking		x	x	x
Issuer Alt Names	URL(s) for download of the issuer certificate		x	x	x
QC Statements	Attribute QcsCompliance and QcsQcSSCD according to [8]	x	x	x	x
Key Usage; critical	Allowed usage of the cryptographic key	keyCertSign crlSign [1]	nonRepudiation	keyCertSign crlSign [2]	nonRepudiation
Extended Key Usage; critical	Allowed extended usage of the cryptographic key		OCSPSigning timeStamping [3]		OCSPSigning
Basic Constraints; critical	Restrictions for certificate usage (CA or EE certificate)	x	x	x	x

[1] CRL will be generated in case of termination of services.
[2] CRL will be generated in case of termination of services.
[3] OCSP certificates include the attribute OCSPSigning, TSA certificates the attribute timeStamping.

7.1.3 Algorithm Object Identifiers (OID)

The Certificate Authority DRV QC Root CA as well as the qualified Certificate Authorities of the tenants issue qualified system certificates with signature algorithm sha256withRSAEncryption.

The signature algorithm RSASSA-PSS can be used alternatively.

The provisions of the national algorithm catalogue [11] shall be considered.

Table 8: Signature algorithm for qualified system certificates

Signature algorithm	Explanation	OID
sha256withRSAEncryption	SHA2-256 hash value, PKCS#1 v1.5 Padding, RSA encryption	1.2.840.113549.1.1.11

RSASSA-PSS	rsaPSS_Parameter Sequence {
	hashAlgorithm = { id-sha256, NULL }
	maskGenAlgorithm = { id-pkcs1-mgf,
	{ id-sha256, NULL } }
	saltLength = 32
	}
		1.2.840.113549.1.1.10

The qualified Validation Services create OCSP responses with signature algorithm sha256withRSAEncryption.

The signature algorithm RSASSA-PSS can be used alternatively.

The provisions of the national algorithm catalogue [11] shall be considered.

Table 9: Signature algorithm for OCSP responses

Signature algorithm	Explanation	OID
sha256withRSAEncryption	SHA2-256 hash value, PKCS#1 v1.5 Padding, RSA encryption	1.2.840.113549.1.1.11

RSASSA-PSS	rsaPSS_Parameter Sequence {
	hashAlgorithm = { id-sha256, NULL }
	maskGenAlgorithm = { id-pkcs1-mgf,
	{ id-sha256, NULL } }
	saltLength = 32
	}
		1.2.840.113549.1.1.10

7.1.4 Name Forms

The allowed names are defined in chapter 3.1.1.

7.1.5 Name Constraints

The allowed names are defined in chapter 3.1.1.

The certificate extension "Name Constraints" shall not be used.

7.1.6 Certificate Policy Object Identifier (OID)

The Certificate Authority DRV QC Root CA as well as the qualified Certificate Authorities of the tenants issue qualified system certificates according to the following policies.

Table 10: Policies for qualified system certificates

Policy	Explanation	OID
CP DRV Bund	Policy of TSP DRV Bund for Certificate Authority DRV QC Root CA	1.3.6.1.4.1.22204.1.8.1.1.1
QCP-N-QSCD	Policy of EU for qualified certificates issued for natural person on qualified signature creation devices according to [8]	0.4.0.194112.1.2

7.1.7 Usage of Policy Constraints Extension

The certificate extensions "Policy Mappings", "Policy Constraints" and "Inhibit Any Policy" shall not be used.

7.1.8 Policy Qualifiers Syntax and Semantics

The Certificate Authority DRV QC Root CA as well as the qualified Certificate Authorities of the tenants issue qualified system certificates with the following policy qualifier.

Table 11: Policy Qualifier for qualified system certificates

Attribute	Explanation	Value
Policy URL	URL DRV Bund Policy	http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html
	URL Norm ETSI EN 319411-2	http://www.etsi.org/deliver/etsi_en/319400_319499/31941102/

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The certificate extension "Certificate Policies" shall net be set critical.

7.2 CRL Profile

7.2.1 Version Number(s)

The TSP DRV Bund does not generate certificate revocation lists (CRL) for the Certificate Authority DRV QC Root CA in normal operation mode.

If the Certificate Authority DRV QC Root CA shall be terminated, then the TSP DRV Bund generates a final certificate revocation version 2 according to RFC 5280 [3] for this Certificate Authority.

7.2.2 CRL and CRL Entry Extensions

The TSP DRV Bund does not generate certificate revocation lists (CRL) for the Certificate Authority DRV QC Root CA in normal operation mode.

If the operation of the Certificate Authority DRV QC Root CA shall be terminated, then the TSP DRV Bund will generate a final certificate revocation list (CRL) for this Certificate Authority. The CRL shall include information about all revoked certificates of the Certificate Authority DRV QC Root CA. The following extensions shall be used according to RFC 5280:

Table 12: CRL extensions for qualified certificates

Extension	Explanation
Authority Key Identifier	Hash value of the public issuer key
Issuer Alt Names	URL(s) for downloading of the issuer certificate
CRL Number	Number of the (final) certificate revocation list

7.3 OCSP Profil

7.3.1 Version Number(s)

The Validation Services (OCSP responder) in the Trustcenter of DRV issue OCSP responses version 1 according to RFC 6960 [4] for all issued qualified certificates.

7.3.2 OCSP Extensions

The Validation Services in the Trustcenter of DRV operate as "Authorized Responder" according to RFC 6960 [4]. The OCSP responses include the certificate of the OCSP responder and the certificate of the qualified Certificate Authority, which has signed the OCSP certificate.

The OCSP response includes the following extensions.

Table 13: Extensions for OCSP responses

Extension	Explanation	Value
OcspNonce	Random number against replay attacks; delivered in OCSP request by the OCSP client	Repetition of the value delivered in OCSP request
OcspArchiveCutoff	The OCSP responder calculates the date.	13.09.1978 00:00:00 GMT [4]

[4] Example

8 Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

A complete conformity assessment occurs regular every two (2) years according to article 20 of eIDAS-RE [1].

One year after the complete assessment a review audit is foreseen. This audit is mainly focused on the found vulnerabilities from the last assessment.

If there are main changes regarding the technology basement or the processes then the CAB shall be informed. After clearance of open questions the CAB decides if an extraordinary conformity assessment is required.

8.2 Identity and Qualifications of Assessor

The conformity assessment will be done by a CAB, which is accredited by the NAB and authorized by NSB according to article 17 eIDAS-RE [1] with conformity assessment for an eIDAS compliant TSP.

8.3 Assessor's Relationship to Assessed Entity

There is no business relationship between TSP DRV Bund and CAB beside the conformity assessment.

8.4 Topics Covered by Assessment

The conformity assessment comprises the qualified Certificate Authorities for issuing qualified system certificates in the productive main system and in the productive backup system.

8.5 Actions Taken as a Result of Deficiency

The staff of TSP DRV Bund eliminate or correct the findings, which have been outcome during the conformity assessment according to the guidelines of the CAB.

8.6 Communications of Results

The CAB publishes the conformity certificate if conformity assessment was successful [13].

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

The fees are matter of the administrative agreement between TSP DRV Bund and the tenants of the Trustcenter of DRV.

9.1.2 Certificate Access Fees

The fees are matter of the administrative agreement between TSP DRV Bund and the tenants of the Trustcenter of DRV.

9.1.3 Revocation or Status Information Access Fees

The fees are matter of the administrative agreement between TSP DRV Bund and the tenants of the Trustcenter of DRV.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

TSP DRV Bund possesses an appropriate liability insurance according to article 24 of eIDAS-RE [1] for the qualified Certificate Authority DRV QC Root CA to cover damages according to article 13 of eIDAS-RE.

9.2.2 Other Assets

DRV Bund provides the central technical systems of qualified Certificate Authorities in the Trustcenter of DRV.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The information in the security concept (including risk analysis, counter measures, etc.) are classified as "confidential". The information regarding the operation of the qualified Certificate Authorities (Certification Practice Statements, Operational Concept, etc.) are classified as "Restricted - for internal use only".

9.3.2 Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

The system administrator server of the Trustcenter of DRV and the staff of TSP DRV Bund are responsible to protect confidential information, which is gathered, used and stored under their control.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

The TSP DRV Bund meets the legal provisions for protection of privacy data according to BDSG.

The amount of collected data depends on the provisions of eIDAS-RE. The subscriber of qualified system certificates are informed about the collected data (which data, where stored, retention period).

9.4.2 Information Treated as Private

The identification information of the subscriber of qualified system certificates collected in the key ceremony protocol shall be treated as private.

9.4.3 Information Not Deemed Private

No stipulation.

9.4.4 Responsibility to Protect Private Information

The system administrator server of the Trustcenter of DRV and the staff of TSP DRV Bund are responsible to protect private information, which is gathered, used and stored under their control.

9.4.5 Notice and Consent to Use Private Information

The subscriber of qualified system certificates shall agree in the key ceremony protocol, that the TSP DRV Bund creates certificates on behalf of them.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Private data can be disclosed, if there exists a well-grounded business or legal reason. The contact address in chapter 1.5.2 shall be used in this case.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property rights

No stipulation.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The obligations of TSP DRV Bund shall comply with the provision in the relevant ETSI norms [5], [6] and [7]. In particular, TSP DRV Bund has the obligation to provide revocation information about issued qualified certificates. The revocation information will be provided until 30 years after expiration of the appropriate certificate.

The quality assurance system can issue certificates for test purposes. Test certificates indicate in subject name that they shall be used for test purposes.

TSP DRV Bund informs the National Supervisory Body and additional involved bodies about every security incident and every loss of integrity within 24 hours according to article 19 of eIDAS-RE. If the incident can have an adverse effect on certificate holder, these persons will be informed immediately in suitable manner.

9.6.2 RA Representations and Warranties

The security representative of DRV Bund or the manager of TSP DRV Bund perform the registration process of the subscriber of qualified system certificates. The required registration data shall be correctly taken over from the presented official identification documents of the subscriber. Any change is not allowed.

9.6.3 Subscriber Representations and Warranties

The rights and obligations of subscriber shall comply with the provisions in the relevant ETSI norms [5], [6] and [7] as well as with the provisions in the administrative agreements between TSP DRV Bund and the tenants of the Trustcenter of DRV. The subscriber are obligated to make true declarations regarding their own person in the registration process.

The subscriber hand over their system smart cards to the system administrator server for operation of the appropriate services. The system administrator server are obligated to use the system smart cards according to the intended purposes.

The subscriber shall inform the manager of TSP DRV Bund in case of any request for revocation of a qualified system certificate. The reasons for certificate revocation are defined in chapter 4.9.1.

9.6.4 Relying Party Representations and Warranties

Relying parties, who rely on qualified system certificates, have the obligation to validate the certificates issued by the qualified Certificate Authorities. The validation shall be done using the appropriate Validation Service (OCSP responder). If the operation of the Certificate Authority DRV QC Root CA and respectively the Validation Service DRV QC Root OCSP will be terminated, then the certificate revocation information will be provided in form of a certificate revocation list (CRL). The CRL will be published on the web site of TSP DRV Bund (see chapter 2.2). Invalid certificates shall not be used.

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

Relying parties shall consider the restrictions for the usage of the qualified certificates. The restrictions are defined in chapter 1.4.

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 1.5.2 shall be used.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

TSP DRV Bund is liable according to the concluded administrative agreements and the general national lawful regulations according to article 13 of eIDAS-RE [1].

9.8 Limitations of Liability

TSP DRV Bund is liable according to general lawful regulations.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This document is valid with the day its publication. The validity of the documents ends with the termination of the Certificate Authority DRV QC Root CA.

9.10.2 Termination

The validity of the documents ends premature with the publication of a new document version.

9.10.3 Effect of Termination and Survival

In the case, the validity of this policy ends; it is not allowed to issue any new certificate according to this policy.

9.11 Individual Notices and Communications with Participants

This policy will be published on the web site of TSP DRV Bund (see chapter 2.2). The manager of TSP DRV Bund or his deputies will handle individual notice to the subscribers if required.

9.12 Amendments

9.12.1 Procedure for Amendment

TSP DRV Bund keeps the right to change the current policy document. Changes can be necessary due to new or changed technical or legal circumstances or requirements.

TSP DRV Bund checks in cases of updates or modifications of the document, if there are significant changes for the security of the qualified certification services, for the confidence into the certification services, for rights and obligations of participating parties or for applicability of the issued certificates. If one of the conditions is valid than the major version number of the document will be increased.

9.12.2 Notification Mechanism and Period

If there are major changes in the policy document (see chapter 9.12.1) than TSP DRV Bund will inform the subscriber of qualified system certificates in an appropriate way.

If there are only minor changes (e.g. error corrections, additional remarks) than the information to subscriber can be omitted.

The current policy document in written format replaces all preceding policy documents. Verbally announcements are not foreseen.

9.12.3 Circumstances under which OID must be changed

The policy OID will be changed, if the scope of the policy document regarding the trust services will be changed.

9.13 Dispute Resolution Provisions

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

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

9.14 Governing Law

The law applicable to this policy is generally German law. In case of differences between German law and eIDAS-RE, the eIDAS-RE is prioritised and overrides German law.

9.15 Compliance with Applicable Law

Certificate Authority DRV QC Root CA and the Certificate Authorities of the tenants of Trustcenter of DRV are operated as trust service issuing qualified certificates according to eIDAS-RE [1] and to the relevant ETSI norms [5], [6] and [7]

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If any part of this agreement is declared unenforceable or invalid, the remainder will continue to be valid and enforceable.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

The place of jurisdiction is regulated in the law.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

TSP DRV Bund operates all central systems of the Trustcenter of DRV on behalf of the tenants. TSP DRV Bund closes administrative agreements with all of the tenants of the Trustcenter of DRV. The operation of central systems on behalf of the tenants is regulated in administrative agreements.

10 Abbreviations and Terms

10.1 Abbreviations

AD	OCSP Validation Service (Auskunftsdienst)
APC	Workplace PC (Arbeitsplatz-PC)
BDSG	Privacy Law of Federal Republic of Germany (Bundesdatenschutzgesetz)
BNetzA	Bundesnetzagentur
BSI	Federal Agency for IT Security [of Germany] (Bundesamt für Sicherheit in der Informationstechnik)
C	Country
CA	Certificate Authority
CAB	Conformity Assessment Body
CAR	Conformity Assessment Report
CC	Common Criteria (ISO/IEC 15408)
CERTSN	Certificate Serial Number
CK	Smart Card (Chipkarte)
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statements
CRL	Certificate Revocation List
DMS	Document Management System
DN	Distinguished Name
DNS	Domain Name Service
DRV	German Pension Fund (Deutsche Rentenversicherung)
DRV BB	Deutsche Rentenversicherung Berlin-Brandenburg
DRV RL	Deutsche Rentenversicherung Rheinland
DRV WF	Deutsche Rentenversicherung Westfalen
DSRV	Body for data exchange between DRV institutions and partners (Datenstelle der Träger der Rentenversicherung)
EAL	Evaluation Assurance Level
EE	End Entity
eIDAS	Electronic Identification and Trust Services for Electronic Transactions in the European Market
eIDAS-RE	eIDAS-Regulation
EN	European Norm
ES-CK	Single Signature Smart Card (Einzelsignaturchipkarte)
ETSI	European Telecommunications Standard Institute

EU	European Union
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
HSM-SCK	HSM System Smart Card (HSM System Chipkarte)
HTTP	Hyper Text Transfer Protocol
HW	Hardware
ID	Identification
IETF	Internet Engineering Task Force
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MA	Employee (Mitarbeiter)
MA-CK	Employee ID Card (Mitarbeiterchipkarte)
MA-Tool	Employee ID Card Tool (Mitarbeiter-Tool)
MS-CK	Mass Signature Smart Card (Massensignaturchipkarte)
NAB	National Accreditation Body
Nonce	Number used once
NSB	National Supervisory Body
NTP	Network Time Protocol
O	Organization
OCSP	Online Certificate Status Protocol
OCSPR	OCSP Responder (Software des AD)
OID	Object Identifier
OU	Organizational Unit
PBS	Productive Backup System
PC	Personal Computer
PEN	Private Enterprise Number
PHS	Productive Main System (Produktiv Haupt System)
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PN	Pseudonym
PP	Protection Profile
PSE	Personal Security Environment
PTB	Physical-Technical Federal Agency Braunschweig (Physikalisch-technische Bundesanstalt Braunschweig)

PUK	Personal Unblocking Key
QC	Qualified Certificate
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trust Service Provider
RFC	Request for Comments - Internet Standards der IETF
RSA	Asymmetric cryptographic algorithm developed by Rivest, Shamir and Adleman
RV	Pension Fund (Rentenversicherung)
SHA	Secure Hash Algorithm
SigG	Signature Law (Signaturgesetz)
SW	Software
SYS-CK	System Smart Card (Systemchipkarte)
TC	Trustcenter
TCDRV	Trustcenter of DRV (Trustcenter der Deutschen Rentenversicherung)
TSA	Time Stamp Authority
TSL	Trust Service Status List
TSP	Trust Service Provider
UHD	User Help Desk
URL	Unified Resource Locator
UTC	Universal Time Coordinated
VD	LDAP-Repository (Verzeichnisdienst)
RE	Regulation
WAN	Wide Area Network
X.509	ITU-Standard for certificates and CRL's

10.2 Terms

Certificate Policy (CP)	The term „Certificate Policy“ comprises rules and guidelines for the usability of the managed certificates The term Certificate Policy is defined in RFC 3647. Amongst other information a Certificate Policy shall define, • Requirements for creation of keys and certificates in registration, application and publication processes, • Requirements for usage of certificates, keys and if appropriate signature creation devices, • Meaning of certificates and their usage.
Certification Practice Statements (CPS)	Certification Practice Statements (CPS) - statements of the practices that a Certificate Authority employs in issuing, managing, revoking, and renewing or re-keying certificates. The term Certificate Practice Statements is defined in RFC 3647. The CPS document defines guidelines for the operation of a Certificate Authority.
DCF77	The time signal sender DCF77 of Federal Republic of Germany is operated in Mainflingen by PTB. The PTB operates 4 high-precise Caesium clocks, used as reference time source UTC(PTB). UTC(PTB) is one of the time sources for the international atom clock TAI of BIPM. The well-known time scale of BIPM is the world time UTC.
EE-Certificate	End Entity Certificate
eIDAS-Regulation	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
Tenant in Trustcenter of DRV	The Trustcenter of DRV operates the qualified and non-qualified trust services of three tenants of DRV institutions: DRV Bund, DRV Rheinland and DRV Westfalen.
Qualified EE-Certificate in the Trustcenter of DRV	Qualified certificates for: • Employees of DRV Rheinland or DRV Westfalen on MA-CK, • Employees of DRV Bund on ES-CK, • Employees of all DRV institutions on MS-CK.
Qualified system certificates in the Trustcenter of DRV	Qualified certificates for the operation of: • Certificate Authorities DRV QC Root CA, DRV QC 70 MA CA, DRV QC 13 MA CA and DRV QC 11 MA CA, • Time Stamp Authority DRV QC Root TSA, • OCSP services DRV QC Root OCSP, DRV QC 70 MA OCSP, DRV QC 13 MA OCSP and DRV QC 11 MA OCSP
Qualified Validation Services of tenants in the Trustcenter of DRV	OCSP services for qualified Certificate Authorities of the tenants: • DRV QC 70 MA OCSP • DRV QC 13 MA OCSP • DRV QC 11 MA OCSP
Qualified trust services in the Trustcenter of DRV	Qualified trust services in context of TCDRV are: • Certificate Authorities for issuance and management of qualified certificates, • Time Stamp Authority for issuance of qualified time stamps.

Qualified Certificate Authorities of tenants in the Trustcenter of DRV	Qualified Certificate Authorities of the tenants are: • DRV QC 70 MA CA • DRV QC 13 MA CA • DRV QC 11 MA CA
Qualified Trust Service Provider	Qualified Trust Service Provider means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body.
System Smart Card	QSCD for qualified system certificates
Validation Service	OCSP services providing certificate status information
Trust Service Provider	Trust Service Provider means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider.
Time Stamp Authority DRV QC Root TSA	Qualified trust service of TSP DRV Bund for issuance of: • Qualified time stamps.
Certificate Authority DRV QC 11 MA CA	Qualified trust service of TSP DRV Westfalen for issuance of: • qualified EE-certificates, • OCSP certificates of Validation Service DRV QC 11 MA OCSP.
Certificate Authority DRV QC 13 MA CA	Qualified trust service of TSP DRV Rheinland for issuance of: • qualified EE-certificates, • OCSP certificates of Validation Service DRV QC 13 MA OCSP.
Certificate Authority DRV QC 70 MA CA	Qualified trust service of TSP DRV Bund for issuance of: • qualified EE-certificates, • OCSP certificates of Validation Service DRV QC 70 MA OCSP.
Certificate Authority DRV QC Root CA	Qualified trust service of TSP DRV Bund for issuance of: • CA certificates for Certificate Authorities DRV QC Root CA, DRV QC 70 MA CA, DRV QC 13 MA CA and DRV QC 11 MA CA, • TSA certificates for Time Stamp Authority DRV QC Root TSA, • OCSP certificates of Validation Service DRV QC Root OCSP.

11 Information to the Document

11.1 Document History

Version	Date	Ch.	Reason	Author
05.00.00	28.11.2011			DRV Bund
05.01.00	08.09.2014	All	New: NQ DRV MA SIG CA	Atos
06.00.00	21.04.2017	All	Adaption to eIDAS-RE / RFC 3647	Atos
06.01.00	10.05.2017	2.x, 5.8, 7.2, 9.6	Update	Atos
06.02.00	01.07.2017	9.13	Postal address for dispute resolution has been changed	Atos

11.2 Table of Figures

11.3 Table of Tables

11.4 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] RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework; Release November 2003; http://www.faqs.org/rfcs/rfc3647.html

[3] RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Release Mai 2008; http://www.faqs.org/rfcs/rfc5280.html

[4] RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, Release June 2013; http://www.faqs.org/rfcs/rfc6960.html

[5] ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

[6] ETSI EN 319 411-1 V1.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

[7] 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

[8] ETSI EN 319 412-5 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QC Statements

[9] Termination Plan of the Trustcenter of DRV

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

[11] Web site of NSB BNetzA for publication of suitable cryptographic algorithm; https://www.bundesnetzagentur.de/cln_1412/DE/Service-Funktionen/ElektronischeVertrauensdienste/QES/WelcheAufgabenhatdieBundesnetzagentur/GeeigneteAlgorithmenfestlegen/geeignetealgorithmenfestlegen_node.html

[12] Web site of NSB BNetzA for publication of national TSL; https://www.nrca-ds.de

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