Trustcenter of Deutsche Rentenversicherung

Trust Service Provider Deutsche Rentenversicherung Bund according to eIDAS-RE

TSA Policy of Time Stamp Authority DRV QC Root TSA

Document-OID: 1.3.6.1.4.1.22204.1.8.1.1.3

Version	06.02.00
Release	01.07.17
Document	TCDRV_TP_DRV-QC-Root-TSA_EN
Status	Released
Classification	Unrestricted

Table of Contents

1 Introduction

1.1 Overview

The institutions of Deutsche Rentenversicherung (DRV) operate a common Trustcenter of DRV 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.

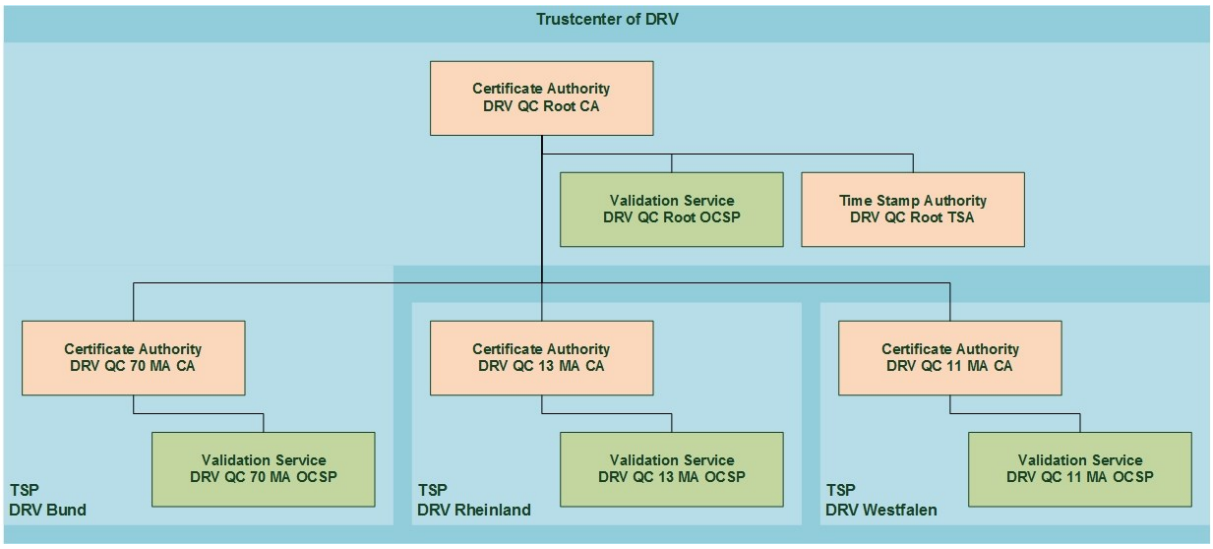

Figure 1 Qualified Trust Services in the Trustcenter of DRV

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 Time Stamp Authority DRV QC Root TSA.

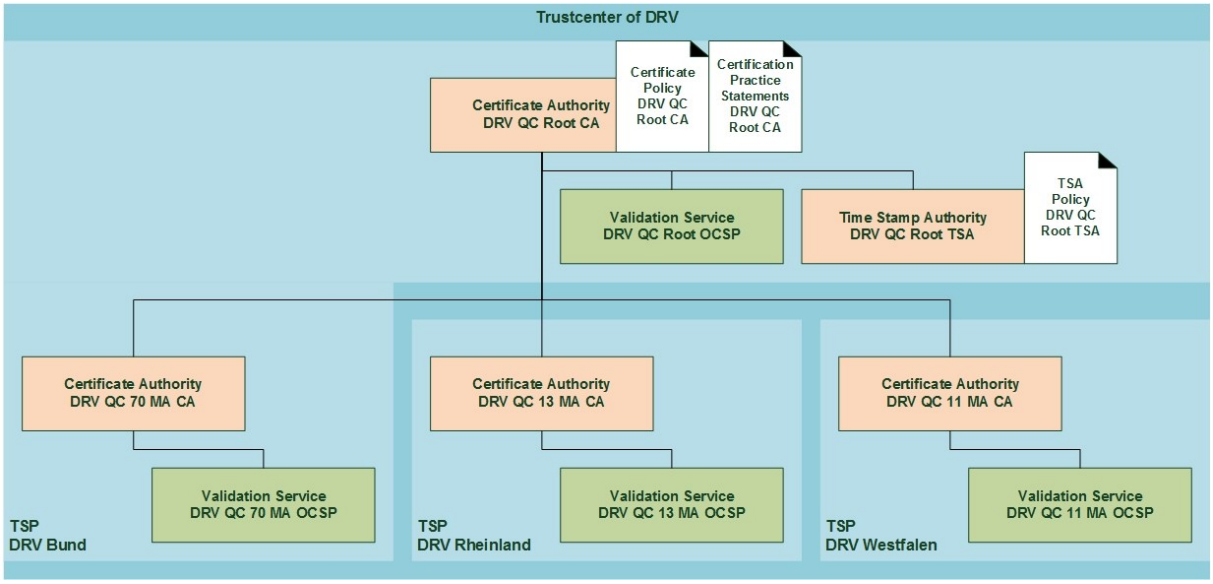

Figure 2 Policy Documents of Time Stamp Authority DRV QC Root TSA

There is no separate document TSA Practice Statements of the Time Stamp Authority DRV QC Root TSA. The relevant operational, environmental and security provisions are defined in the document Certification Practice Statements of Certificate Authority DRV QC Root CA.

The TSA certificates of the qualified Time Stamp Authority DRV QC Root TSA are issued and managed according to Certificate Policy [7] and to Certification Practice Statements [8] of the Certificate Authority DRV QC Root CA.

This document comprises the policy for issuance of qualified time stamps by the Time Stamp Authority DRV QC Root TSA.

The Time Stamp Authority DRV QC Root TSA issues qualified time stamps for authorized subscriber (Refer to chapter 1.3.3).

Qualified time stamps are issued according to Best Practice Time Stamp Policy (BTSP, see [5]).

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

1.2 Document Name and Identification

Document Name: Policy of Time Stamp Authority DRV QC Root TSA

Document-OID: 1.3.6.1.4.1.22204.1.8.1.1.3

PEN-DRV-Bund (1.3.6.1.4.1.22204).Trustcenter (1). Policies (8). QC-CP (1). Productive System (1). QC-Root-TSA (3)

This policy of the Time Stamp Authority DRV QC Root TSA considers the relevant ETSI norms:

- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [4];
- ETSI EN 319 421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps [5];
- ETSI EN 319 422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles [6].

The standard ETSI EN 319 401 defines general requirements for a trust service provider (TSP). A TSP for time stamp services has to consider the requirements in standards ETSI EN 319 421 and ETSI EN 319 422.

1.3 Participants of Time Stamp Service

1.3.1 Certificate Authority

The institution of Deutsche Rentenversicherung are operating a common Trustcenter of DRV. The Trustcenter of DRV provides amongst other services the Time Stamp Authority DRV QC Root TSA for issuing of qualified time stamps according to article 42 of eIDAS-RE.

TSP DRV Bund operates also the qualified Certificate Authority DRV QC Root CA, which issues amongst other certificates the qualified TSA certificates for the Time Stamp Authority DRV QC Root TSA.

TSP DRV Bund operates in addition the non-qualified Certificate Authority DRV NQ Root CA and a couple of non-qualified sub-CAs for issuing of authentication and encryption certificates. One of the non-qualified Certificate Authorities issues non-qualified authentication certificates for authorized subscriber of the Time Stamp Authority.

The application of Time Stamp Authority of TSP DRV Bund is barrier-free. There are no known limitations for persons with disabilities.

1.3.2 Time Stamp Authority

TSP DRV Bund operates the qualified trust service DRV QC Root TSA for issuing of qualified time stamps according to article 42 of eIDAS-RE.

1.3.3 Subscriber

Subscriber of the Time Stamp Authority DRV QC Root TSA are natural persons or responsible persons for systems, who or which may request qualified time stamps.

The usage of the qualified Time Stamp Authority DRV QC Root TSA is based on an administrative agreement between TSP DRV Bund and the institution, which is using the time stamp service.

1.3.4 Relying Parties

The relying parties are not limited. The status of the TSA certificate, which belongs to the signature key used for time stamp generation, can be verified over the internet as well as over the DRV network.

1.3.5 Other Participants

No stipulation.

1.4 Time Stamp Usage

1.4.1 Appropriate Use Cases

The Time Stamp Authority DRV QC Root TSA issues qualified time stamps according to article 42 of eIDAS-RE. Authorized subscriber may request qualified time stamps. The qualified time stamps may be used in applications of authorized subscriber.

1.4.2 Prohibited Use Cases

The usage of qualified time stamps is limited to the use cases defined in chapter 1.4.1. Any other use case is not allowed.

1.5 Policy Administration

1.5.1 Administration 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 "TSA Policy of Time Stamp Authority DRV QC Root TSA" will be published after formal approval according to chapter 2.2.

1.5.3 Person Determining TPS Suitability for the Policy

The TSA Policy and the Certification Practice Statements of Certificate Authority DRV QC Root CA are reviewed and approved by the same body (refer to 1.5.2).

1.5.4 TPS Approval Procedures

An approval process is not explicitly defined. Consistency between the documents TSA Policy and Certification Practice Statements of Certificate Authority DRV QC Root CA 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 certificates issued by Certificate Authority DRV QC Root CA (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 (amongst others TSA certificates). The OCSP responses will be provided until 30 years after certificate expiration. If the service of Certificate Authority DRV QC Root CA will be terminated, then the operation of the Validation Service DRV QC Root OCSP will also be terminated. In this case 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) [13].

2.2 Publication of Information

This document "Policy of Time Stamp Authority DRV QC Root TSA" will be published on the web site of TSP DRV Bund [11].

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

Document Name: TSA Disclosure Statements of Time Stamp Authority DRV QC Root TSA

Document-OID: 1.3.6.1.4.1.22204.1.8.6.1.3

A separate document for "TSA Practice Statements" is not planned. The provisions made in the document Certification Practice Statements of the Certificate Authority DRV QC Root CA [8] are also valid for the Time Stamp Authority DRV QC Root TSA. This belongs especially to the chapters 5 and 6 concerning the security preventive measures in the Trustcenter of DRV.

If the service of Certificate Authority DRV QC Root CA will be terminated, then the operation of the Validation Service DRV QC Root OCSP will also be terminated. In this case 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 TSA Policy	Update if required	After approval of the document	• Web site of TSP DRV Bund
Document TSA Disclosure Statements	Update if required	After approval of the document	• Web site of TSP DRV Bund

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 required
	Read	Unrestricted	Anonym

3 Identification and Authentication

This chapter describes identification and authentication of the subscriber of the qualified Time Stamp Authority.

3.1 Naming

Not applicable.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Not applicable.

3.2.2 Authentication of Organization Identity

Subscriber of the Time Stamp Authority DRV QC Root TSA authenticate himself or herself against a TSL proxy server via TLS client authentication. The TLS proxy server is located in front of the Time Stamp Authority DRV QC Root TSA. TSP DRV Bund issues the appropriate client certificates for authentication of the organization of the subscriber.

An institution, which wants to use the Time Stamp Authority DRV QC Root TSA, has to close an administrative agreement with TSP DRV Bund in advance.

3.2.3 Authentication of Individual Identity

Not applicable.

3.2.4 Non-Verified Subscriber Information

No stipulation.

3.2.5 Validation of Authority

No stipulation.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Renewal Requests

The administrative agreement defines the usage period for the Time Stamp Authority for one (1) year. The usage period will be automatically prolonged for one year if neither the TSP DRV Bund nor the subscriber resign the agreement in time.

3.4 Identification and Authentication for Revocation Request

Electronic time stamps cannot be revoked.

4 Time Stamp Life-Cycle Operational Requirements

4.1 Time Stamp Request

Authorized subscriber can use the Time Stamp Authority DRV QC Root TSA via the following URL:

https://tsp.tc.deutsche-rentenversicherung.de

The formats of the time stamp request as well as the time stamp response are compliant to the appropriate standards RFC 3161 [3] and ETSI 319 422 [6]. The time stamp request includes the hash value of the data, which shall be time stamped. Supported hash algorithms are SHA-256 und SHA-512.

4.2 Time Stamp Application Processing

Only subscriber or systems, which are operated under the control of a subscriber, can request a qualified time stamp from the Time Stamp Authority DRV QC Root TSA. The subscriber possess an authentication certificate from TSP DRV Bund. The subscriber has to authenticate himself or herself on a TLS proxy server via TLS client authentication in front of the Time Stamp Service.

The authentication certificates will be stored and authorized in the Time Stamp Authority DRV QC Root TSA. Authorized subscriber, who has signed the administrative agreement (see chapter 1.3.3), get such an authentication certificate from TSP DRV Bund.

The time stamp request shall be handed over in "Request Format" according to RFC 3161 [3]. The time stamp service supports amongst others the following fields:

- Version (mandatory);
- MessageImprint (hash value of the data, which shall be time stamped; mandatory);
- Nonce (random number against replay attacks; optional);
- CertReq (request of certificate chain of the time stamp unit; optional).

4.3 Time Stamp Issuance

4.3.1 Time Stamp Units

The Trustcenter of DRV operates the Time Stamp Authority DRV QC Root TSA. The term Time Stamp Authority (TSA) comprises the whole Time Stamp Service. The term Time Stamp Unit (TSU) defines a single TSA instance, which generates time stamps with dedicated qualified signature creation devices (QSCD). The Time Stamp Authority DRV QC Root TSA comprises two active instances in the productive main system and two stand-by instances in the productive backup system.

A Time Stamp Unit instance is logically divided into functional blocks (e.g. monitoring of the signature creation devices, time monitoring, time synchronisation, signature creation).

4.3.2 Time Stamp Unit Signature Key

The Time Stamp Authority DRV QC Root TSA binds the delivered data (hash value of the data, which shall be time stamped) and a time stamp together with a qualified electronic signature.

The Time Stamp Authority DRV QC Root TSA fulfils the requirements regarding the usage of qualified signature creation devices (QSCD).

- Confidentiality: The private signature key is created inside the qualified signature creation device and cannot be exported.
- Uniqueness: The private and public keys are created based on the smart card internal physical random number generator. The generated key pair is as far as possible unique.
- Impossibility of derivation: The signature key pair uses the RSA algorithm with key length 2048 bit. This algorithm is approved in the current national algorithm catalogue [12]. The impossibility of derivation is approved until end of 2022.
- Appropriation: The signature key will only be used by the qualified Time Stamp Authority DRV QC Root TSA to sign time stamps. The appropriation is defined in the qualified certificate.
- The qualified Time Stamp Authority creates the toBeSigned data structure, calculates its hash value and hands this hash value over to the qualified signature creation device (QSCD). The QSCD does not alter the hash value. It is not foreseen to display the toBeSigned data structure in automatic operation.
- The Certificate Authority DRV QC Root CA creates and manages the QSCD of the qualified Time Stamp Authority DRV QC Root TSA.
- The signature keys of qualified Time Stamp Service DRV QC Root TSA are not saved or archived. This feature is technically not supported.

The Time Stamp Service DRV QC Root TSA possess at least six (6) qualified signature creation devices (QSCD) for signature creation of the electronic time stamps.

- Each of the TSA instances in main system gets at least one (1) QSCD,
- One (1) replacement QSCD for the main system,
- Each of the TSA instances in backup system gets at least one (1) QSCD,
- One (1) replacement QSCD for the backup system.

Each of the QSCD includes an individual signature key. The signature of the created time stamps can be verified with the appropriate public key. This public key is part of the certificate of the Time Stamp Unit. This TSA certificate will be delivered to the subscriber as part of the time stamp response.

4.3.3 Time Stamp Unit Signature Certificate

The Time Stamp Authority DRV QC Root TSA fulfils the requirements regarding qualified certificates.

- The qualified certificates of the Time Stamp Authority DRV QC Root TSA include the QC statement with the attributes QcsCompliance and QcsQcSSCD.
- The qualified certificates of the Time Stamp Authority DRV QC Root TSA include the name of the Certificate Authority DRV QC Root CA as issuer name.
- The qualified certificates of the Time Stamp Authority DRV QC Root TSA include the public key of the Time Stamp Unit, which can be used to validate the signature of the time stamp.
- The qualified certificates of the Time Stamp Authority DRV QC Root TSA include the validity period of the certificate (not before date, not after date).
- The qualified certificates of the Time Stamp Authority DRV QC Root TSA include a certificate serial number, which is in conjunction with the issuer name unique.
- The qualified certificates of the Time Stamp Authority DRV QC Root TSA include the URL(s) to download the certificate of the issuing Certificate Authority.
- The qualified certificates of the Time Stamp Authority DRV QC Root TSA include the URL of the OCSP responder for validation of the certificate revocation status.
- The qualified certificates of the Time Stamp Authority DRV QC Root TSA include the OID of the corresponding Certificate Policy [7]. The referenced policy defines the usage of a qualified signature creation device (QSCD) certified for creation of qualified signatures.
- The qualified certificates of the Time Stamp Authority DRV QC Root TSA include a qualified electronic signature of the Certificate Authority DRV QC Root CA.

The certificates of the Time Stamp Authority DRV QC Root TSA are issued by the Certificate Authority DRV QC Root CA. The certificates include all the same name as subject name. The certificates differentiate in the certificate serial number. Provisions for the certificate profile are defined in the Certificate Policy of the Certificate Authority DRV QC Root CA [7].

4.3.4 Time Stamp service

The Time Stamp Authority DRV QC Root TSA creates electronic time stamps compliant to the norm ETSI EN 319 422 [6] and the requirements of eIDAS-RE.

- The current time will be linked to the delivered data through a qualified electronic signature. Undiscovered changes of the electronic time stamp are not possible according to current judgement.
- The time of the Time Stamp Authority is synchronized with the radio time signal DCF77. The accuracy of the time stamp is at least one (1) second.
- The qualified electronic signature is created by a certified (Common Criteria EAL4+) qualified signature creation device (QSCD). The Certificate Authority DRV QC Root CA issues a separate qualified certificate for each time stamp unit.

Qualified electronic time stamps are created in "Response Format" according to RFC 3161 [3]. The following fields are supported amongst others:

- Version (mandatory);
- Policy (BTSP; mandatory);
- MessageImprint (hash value of the data, which shall be time stamped; mandatory);
- SerialNumber (hash value derived from process PID and current time; mandatory);
- GenTime (time of generation of the time stamp, mandatory);
- Accuracy (accuracy of the time stamp, optional);
- Nonce (random number, copy from the time stamp request; optional);
- TSAName (Name of the Time Stamp Authority, optional);
- Certificates (certificate chain of the Time Stamp Unit; optional).

4.3.5 Time Synchronisation

The Time Stamp Authority DRV QC Root TSA creates electronic time stamps with an accuracy of at least 1 second based on the official German time source. The synchronisation of the system clock of the Time Stamp Units occurs one time per day.

The system clock of the Time Stamp Authority instance will be compared every 10 seconds against the external time source. The plausibility of the comparison will be checked. The difference between the system clock and the external time source DCF77 shall not exceed the value of one (1) second. If there is a difference greater than one (1) second, then Time Stamp Authority instance will be automatically terminated.

The exception of leap seconds will be handled by the Time Stamp Authority in a proper way and does not lead to a system unavailability. The detection of leap seconds happens via the time telegram of the radio time signal DCF77 (refer to [15]). The log file of the Time Stamp Authority instances store leap second events.

The radio time signal DCF77 is used as the external time source providing the official German time. The radio time sender DCF77 is based on the time of the German time lab UTC(PTB) (refer to [16]).

4.4 Time Stamp Acceptance

The qualified electronic time stamps are valid at the time of delivery. The validation of an electronic time stamp requires the following checks:

- verification of the signature of the electronic time stamp;
- verification of the signature certificate of the time stamp unit, which has signed the electronic time stamp (certificate is included in the time stamp response);
- verification of the CA certificate, which has issued the time stamp unit certificate (certificate is included in the time stamp response).

4.5 Time Stamp Usage

The time stamp response includes the certificate chain of the appropriate time stamp unit. The certificates include amongst others the URL of the Validation Service (OCSP responder) DRV QC Root OCSP, which delivers OCSP responses for the relevant certificates.

4.6 Time Stamp Renewal

Not applicable.

4.7 Time Stamp Renewal with Re-Key

Not applicable.

4.8 Time Stamp Modification

Not applicable.

4.9 Time Stamp Revocation

Not applicable.

4.10 Certificate Status Services (OCSP)

4.10.1 Operational Characteristics

The Validation Service (OCSP responder) is implemented with two (2) instances in the productive main system and with two (2) instances in the productive backup system. Either the main system or the backup system is active. The two instances of a location are load balanced.

4.10.2 Service Availability

The Validation Service (OCSP responder) is operated in high-availability mode. The availability shall reach 99.5% per year.

4.10.3 Operational Features

No stipulation.

4.11 End of Subscription

If the contractual relationship between TSP DRV Bund and the subscriber of the Time Stamp Authority DRV QC Root TSA shall be terminated, then the administrative agreement (see chapter 1.3.3) must by resigned by at least one party.

4.12 Key Escrow and Recovery

Key escrow for private keys belonging to qualified certificates is not foreseen.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

The Time Stamp Authority DRV QC Root TSA is operated on dedicated server. These server are located in the datacenter of the Trustcenter of DRV. The datacenter as well as the server racks are physically protected. Only authorized staff has physical access to the server.

The logical access to the server is protected via firewalls. The network access from the internet and from the DRV network is limited to request qualified electronic time stamps and to get the appropriate time stamp responses.

The security measures are described in detail in the document Certification Practice Statements of the Certificate Authority DRV QC Root CA [8].

5.2 Procedural Controls

The staff of the TSP DRV Bund operate the Time Stamp Authority DRV QC Root TSA. The requirements concerning the TSP organization are described in the security concept of the Certificate Authority DRV QC Root CA. The organization of the TSP DRV Bund is described in the organization concept of TSP DRV Bund. The assignment of employees to the defined trusted roles is electronically documented in a database of TSP DRV Bund.

The security measures are described in detail in the document Certification Practice Statements of the Certificate Authority DRV QC Root CA [8].

5.3 Personnel Controls

The TSP DRV Bund maintain a repository of the relevant documentation as part of the asset management:

- The current documentation including the version is maintained in Trustcenter specific database.

The security measures are described in detail in the document Certification Practice Statements of the Certificate Authority DRV QC Root CA [8].

5.4 Audit Logging Procedure

All activities of the Time Stamp Authority DRV QC Root TSA are logged in appropriate log files and later on archived. The log files include amongst other information:

- Requests for and creation of qualified electronic time stamps,
- Time synchronisation based on the radio time signal DCF77,
- Loss of the time signal from the radio time sender,
- Loss of time synchronisation (deviation greater than 1 second).

The log files are saved and later on archived.

The security measures are described in detail in the document Certification Practice Statements of the Certificate Authority DRV QC Root CA [8].

5.5 Records Archival

The created qualified electronic time stamps are stored in log files for evidence purposes. The log files will be archived. The subscriber of the Time Stamp Authority DRV QC Root TSA authenticate himself or herself on a TLS proxy server in front of the time stamp service via TLS client authentication. The client certificates for authentication include the organization name of the subscriber. These client certificates for authentication will be stored in log files and later on archived for monitoring, clearing and evidence purposes by the TLS proxy server. The archived data will be preserved for 5 years.

5.6 Key Changeover

The security measures are described in detail in the document Certification Practice Statements of the Certificate Authority DRV QC Root CA [8].

5.7 Compromise and Disaster Recovery

The recovery of a Time Stamp Authority instance or of the whole Time Stamp Authority DRV QC Root TSA after a disaster is described in the recovery plan. The recovery plan is part of the operational concept of the TSP DRV Bund in the Trustcenter of DRV.

The security measures are described in detail in the document Certification Practice Statements of the Certificate Authority DRV QC Root CA [8].

5.8 Termination of Service

The qualified Time Stamp Authority DRV QC Root TSA is used by:

- Institutions with an appropriate administrative agreement with TSP DRV Bund for the usage of the qualified Time Stamp Service.

The manager of TSP DRV Bund decides in collaboration with the directorate of DRV Bund about the termination of the qualified Time Stamp Authority DRV QC Root TSA.

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

- Handover of obligations, tasks and documentation:

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

  All valid certificates of the Time Stamp Authority DRV QC Root TSA will be revoked. The Validation Service DRV QC Root OCSP provides the appropriate certificate status information online. If the operation of the Certificate Authority DRV QC Root CA and respectively the Validation Service DRV QC Root 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.

  The concepts and the documentation of the trust service DRV QC Root TSA 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 about the planned termination of the qualified trust service DRV QC Root TSA in advanced based on the administrative agreement.

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

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

- Coordinated demolition:

  All private keys of the Time Stamp Authority DRV QC Root TSA will be destroyed. Afterwards, it is not possible to create any time stamp with this Time Stamp Authority.

The procedures for termination of the Time Stamp Authority DRV QC Root TSA are described in the termination plan [10] of the Trustcenter of DRV.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

The key generation process is described in detail in the document Certification Practice Statements of the Certificate Authority DRV QC Root CA [8].

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The measures for private key protection are described in detail in the document Certification Practice Statements of the Certificate Authority DRV QC Root CA [8].

6.3 Other Aspects of Key Pair Management

Additional aspects of key management are described in detail in the document Certification Practice Statements of the Certificate Authority DRV QC Root CA [8].

6.4 Activation Data

The handling of activation data is described in detail in the document Certification Practice Statements of the Certificate Authority DRV QC Root CA [8].

6.5 Computer Security Controls

The computer security measures for private key protection are described in detail in the document Certification Practice Statements of the Certificate Authority DRV QC Root CA [8].

6.6 Life Cycle Technical Controls

The Time Stamp Authority DRV QC Root TSA is based on a certified software product compliant to ITSEC evaluation strength E2. Changes on the installed product are implemented (a) regularly based on software improvements following the implemented change request process or (b) event-driven in case of incidents in form of software patches. All changes are documented. Changes in the installation are documented in the so called installation & configuration documentation.

The operation of the systems of the Trustcenter of DRV is monitored. In case of an error an incident-call will be opened. The staff of TSP DRV Bund supports and coordinates the error correction process. Relevant software patches will be implemented in time. Subscribers will be informed in suitable manner if they are concerned.

The incident and patch management processes are described in detail in the document Certification Practice Statements of the Certificate Authority DRV QC Root CA [8].

The analysis, evaluation and definition of countermeasures of operational risks are subject of the security concept of TSP DRV Bund. The requirements for the operation of the Time Stamp Authority DRV QC Root TSA are described in detail in the security concept of the Time Stamp Authority DRV QC Root TSA. The requirements for generation and management of cryptographic keys and public key certificates are described in the security concept of the Certificate Authority DRV QC Root CA. These documents are classified as "confidential" and publicly not available.

TSP DRV Bund maintains a repository of the current configuration of the technical systems operated under the control of TSP DRV Bund as part of the asset management:

- The operated technical systems including hardware components and software applications are documented based on a software application.

The measures concerning security management are defined in the security concept [9]. The security concept shall be reviewed regularly and updated if required.

6.7 Network Security Controls

The network security measures for private key protection are described in detail in the document Certification Practice Statements of the Certificate Authority DRV QC Root CA [8].

6.8 Time-Stamping

Each technical system in the Trustcenter of DRV is time synchronized in a proper way.

The server of the Validation Service (OCSP responder) and of the qualified Time Stamp Service are synchronized once a day by the Time Stamp Authority DRV QC Root TSA based on the radio time signal DCF77. The time of DCF77 is based on the German UTC time lab UTC(PTB) operated by Physical-Technical Federal Agency Braunschweig.

All other server of the Trustcenter of DRV are time synchronized with the NTP server of DRV Bund.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

The document Certificate Policy of Certificate Authority DRV QC Root CA [7] defines the provisions for the certificate profile of the Time Stamp Authority DRV QC Root TSA.

7.2 CRL Profile

The provisions for issuing certificate revocation lists (CRL) by Certificate Authority DRV QC Root CA are defined in the appropriate Certificate Policy (refer to [7]).

7.3 OCSP Profile

The Certificate Policy of Certificate Authority DRV QC Root CA [7] defines the OCSP profile of the Validation Service DRV QC Root OCSP.

7.4 TSA Profile

7.4.1 Signature Algorithm

The Time Stamp Authority DRV QC Root TSA creates qualified electronic time stamps with signature algorithm sha256withRSAEncryption or RSASSA-PSS.

The provisions of the national algorithm catalogue [12] shall be considered.

Table 3: Signature algorithm for qualified electronic time stamps

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

7.4.2 TSA Policy

The Time Stamp Authority DRV QC Root TSA creates qualified electronic time stamps according to "Best Practices Time Stamp Policy (BTSP)". This policy is used for time stamp services, which generates electronic time stamps based on public key certificates with an accuracy of one (1) second.

The identifier of the policy "Best Practices Time-Stamp Policy (BTSP)" is included in the time stamp response in ASN.1 format.

The OID of the policy BTSP is defined as:

```
0.4.0.2023.1.1
itu-t(0).identified-organization(4).
etsi(0).time-stamp-policy(2023).policy-identifiers(1).
best-practices-ts-policy(1)
```

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. The CAB decides together with NSB 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 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 Time Stamp Authority DRV QC Root TSA instances 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 [14].

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 institution, which uses the time stamp service.

9.1.2 Certificate Access Fees

The fees are matter of the administrative agreement between TSP DRV Bund and the institution, which uses the time stamp service.

9.1.3 Revocation or Status Information Access Fees

The fees are matter of the administrative agreement between TSP DRV Bund and the institution, which uses the time stamp service.

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 Time Stamp Authority DRV QC Root TSA to cover damages according to article 13 of eIDAS-RE.

9.2.2 Other Assets

DRV Bund provides the technical systems of Time Stamp Authority DRV QC Root TSA.

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 of the security concept (including risk analysis, counter measures) are classified as "confidential". The information regarding the operation of the Time Stamp Authority DRV QC Root TSA (Certification Practice Statements [8], 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 qualified Time Stamp Authority DRV QC Root TSA does not use person related data to create qualified time stamps. The time stamp request does not include person related data. The generated response includes beside the qualified time stamp also the certificate chain auf the qualified time stamp. The certificate chain comprises a qualified certificate of the Time Stamp Authority and a qualified certificate of the Certificate Authority, which has issued the certificate of the Time Stamp Authority.

9.4.2 Information Treated as Private

The identification information of the subscriber of Time Stamp Authority DRV QC Root TSA 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 the Time Stamp Authority DRV QC Root TSA agree in an administrative agreement, that the TSP DRV Bund creates a certificate for their organisation. The subscriber also agree, that this certificate can be logged by the Time Stamp Service for evidence and evaluation purposes.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

No stipulation.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property rights

No stipulation.

9.6 Representations and Warranties

9.6.1 TSP Representations and Warranties

The obligations of TSP DRV Bund are regulated in the Certificate Policy of Certificate Authority DRV QC Root CA [7]. In particular, TSP DRV Bund has the obligation to provide revocation information about issued qualified TSA certificates. The revocation information will be provided until 30 years after expiration of the appropriate certificate.

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 TSA Representations and Warranties

The obligations of Time Stamp Authority DRV QC Root TSA are regulated in the administrative agreement, which is a prerequisites for using the Time Stamp Service.

9.6.3 Subscriber Representations and Warranties

The rights and obligations of subscriber are regulated in the administrative agreement between the TSP DRV Bund and the institution of the subscriber (refer to chapter 1.3.3).

9.6.4 Relying Party Representations and Warranties

Relying parties, who rely on a qualified time stamp issued by DRV QC Root TSA, have the obligation to validate the time stamps issued by the qualified Time Stamp Authority. Especially the signature shall be validated according to the specifications of the appropriate document Certificate Policy of DRV QC Root CA (refer to [7]).

Relying parties, who rely on qualified TSA 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 operation of the Validation Service DRV QC Root OCSP will be terminated, then 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. Invalid certificates shall not 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 general lawful regulations. The liability for qualified signature certificates of the Time Stamp Authority DRV QC Root TSA is regulated in the appropriate document Certificate Policy of DRV QC Root CA (refer to [7]).

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 Time Stamp Service DRV QC Root TSA.

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 time stamp 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). An individual notice to subscribers of the Time Stamp Authority DRV QC Root TSA takes place according to the provisions in the administrative agreement.

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 decides in cases of updates or modifications of the document, if there are significant changes for the security of the time stamp service, for the confidence into the issued time stamps, for rights and obligations of participating parties and for applicability of the issued time stamps. 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 the Time Stamp Authority DRV QC Root TSA in an appropriate way.

If there are only minor changes (e.g. error corrections, additional remarks) than the information to subscriber of the Time Stamp Authority DRV QC Root TSA 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 used 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

Time Stamp Authority DRV QC Root TSA is operated as trust service issuing qualified time stamps according to article 42 of eIDAS-RE [1] and to the relevant ETSI norms [4], [5] und [6]

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

No stipulation.

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
RE	Regulation
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)
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 has to follow 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 und 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 und 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 und 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
01.00.00	27.06.2006	All	Initial Document	DRV Bund
02.00.00	10.08.2007	All	Migration to stronger cryptographic algorithm	DRV Bund
03.00.00	23.01.2007	All	CRL was stopped for qualified CA services	DRV Bund
04.00.00	12.05.2016	All	Adaption to standards ETSI EN 319401, ETSI EN 319421, regulation 910/2014 of EU (eIDAS-RE)	DRV Bund
04.01.00	03.06.2016	All	Retention period for log files is defined to 5 years	Atos
04.02.00	30.09.2016	All	Dispute Resolution Body was defined	Atos
05.00.00	---	---	Change due to formal reasons	---
06.00.00	21.04.2017	All	Adaption to RFC3647	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 3161: Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP) http://www.faqs.org/rfcs/rfc3161.html

[4] ETSI EN 319 401 V2.1.1 (2016-02); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers http://www.etsi.org/deliver/etsi_en/319400_319499/319401/

[5] ETSI EN 319421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps http://www.etsi.org/deliver/etsi_en/319400_319499/319421/

[6] ETSI EN 319422: Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles http://www.etsi.org/deliver/etsi_en/319400_319499/319422/

[7] Certificate Policy of Certificate Authority DRV QC Root CA http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html

[8] Certification Practice Statements of Certificate Authority DRV QC Root CA

[9] Security Concept of TSP DRV Bund

[10] Termination Plan of Trustcenter of DRV

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

[12] 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

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

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

[15] Web site of PTB, working group 4.41 leap seconds, https://www.ptb.de/cms/de/ptb/fachabteilungen/abt4/fb-44/ag-441/darstellung-der-gesetzlichen-zeit/schaltsekunden.html

[16] Web site of PTB, working group 4.42 time transmission, https://www.ptb.de/cms/ptb/fachabteilungen/abt4/fb-44/ag-442.html