Trust Service Provider "Trustcenter der Deutschen Rentenversicherung"

Policy of the Qualified Time Stamp Authority of "Trustcenter der Deutschen Rentenversicherung"

Version: 04.02

Release: 30.09.16

Table of Content

1 Policy of Qualified Time Stamp Service of "Trustcenter der Deutschen Rentenversicherung"

1.1 Introduction

1.1.1 Overview

The carrier of pension insurance "Deutsche Rentenversicherung" are operating a common "Trustcenter der Deutschen Rentenversicherung" to provide trust services according to "Regulation 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" (eIDAS-RE [1]).

The "Trustcenter der Deutschen Rentenversicherung" operates amongst others a qualified Time Stamp Authority to issue qualified time stamp compliant to eIDAS regulation [1] article 42.

This document comprises the policy of the qualified Time Stamp Authority of the "Trustcenter der Deutschen Rentenversicherung". Chapter 1 includes the "TSA Disclosure Statements". There is no separate document for "TSA Disclosure Statements".

This policy considers the relevant standards in current version from European Telecommunications Standards Institute (ETSI).

- "ETSI EN 319 401" [2] and
- "ETSI EN 319 421" [3].

Chapter 2 explains in detail how the requirements of these standards are fulfilled.

1.1.2 Document Identification

Document name	Policy of Qualified Time Stamp Authority of the "Trustcenter der Deutschen Rentenversicherung"
Version	04.02
OID	1.3.6.1.4.1.22204.1.8.1.1.3

1.1.3 Document Management

The carrier "Deutsche Rentenversicherung Bund" is responsible to manage this policy document.

1.1.4 Contact

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

1.2 Legal requirements of eIDAS Regulation

1.2.1 Article 42: Requirements for Qualified Electronic Time Stamps

The qualified Time Stamp Authority of the "Trustcenter der Deutschen Rentenversicherung" fulfils the requirements of eIDAS regulation [1] Article 42.

(a) The current time stamp information and the delivered data are bind together with a qualified electronic signature. The possibility of undetected data, which were changed after signature creation, can be reasonable precluded.

(b) The time stamp is based on the DCF77 radio time signal, which is derived from PTB(UTC). The accuracy of the time stamp is at least 1 second.

(c) A secure signature creation device (SSCD), which is certified according to Common Criteria EAL4+, creates the qualified electronic signature. The "Trustcenter der Deutschen Rentenversicherung" generates for each SSCD a dedicated qualified certificate by its qualified Certification Authority.

1.2.2 ANNEX I Requirements for Qualified Certificates for Electronic Signatures

The qualified Time Stamp Authority of the "Trustcenter der Deutsche Rentenversicherung" binds the delivered data (hash value of data, which shall be time stamped) and a time stamp together with a qualified electronic signature. The requirements to the qualified certificate of the qualified Time Stamp Authority service are fulfilled.

- The qualified certificates of the qualified Time Stamp Authority include the QC-statement according to the appropriate ETSI standard [5]. An application can process the QC-statement automatically.
- The qualified certificates of the qualified Time Stamp Authority include the name of the issuing qualified Certification Authority of the "Trustcenter der Deutschen Rentenversicherung" as issuer name.
- The qualified certificates of the qualified Time Stamp Authority include the public key, which can be used to validate the signature of the time stamp.
- The qualified certificates of the qualified Time Stamp Authority include the validity period of the certificate (not before date, not after date).
- The qualified certificates of the qualified Time Stamp Authority include a certificate serial number, which is in conjunction with the issuer name unique.
- The qualified certificates of the qualified Time Stamp Authority include the URL(s) to download the certificate of the issuing Certification Authority.
- The qualified certificates of the qualified Time Stamp Authority include the URL of the OCSP-Responder for validation of the certificate revocation status.
- The qualified certificates of the qualified Time Stamp Service include the OID of the corresponding Certificate Policy. The referenced policy defines the usage of a secure signature creation device (SSCD) certified for creation of qualified signatures.
- The qualified certificates of the qualified Time Stamp Service are signed from the qualified Certification Authority of "Trustcenter der Deutschen Rentenversicherung".

1.2.3 ANNEX II Requirements for Qualified Electronic Signature Creation Devices

The qualified Time Stamp Service of "Trustcenter der Deutschen Rentenversicherung" binds delivered data (hash value of data, which shall be time stamped) and a time stamp together with a qualified electronic signature. The requirements to the qualified secure signature creation device (SSCD) are fulfilled.

- Confidentiality: The private signature key is created inside the secure 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 algorithm catalog [9]. The impossibility of derivation is ensured until end of 2022.
- Appropriation: The signature key will only be used by the qualified Time Stamp Authority service 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 secure signature creation device (SSCD). The SSCD does not alter the hash value. It is not foreseen to display the toBeSigned data structure in automatic operation.
- "Trustcenter der Deutschen Rentenversicherung" creates and manages the secure signature creation devices (SSCD) of the qualified Time Stamp Authority.
- The signature keys of qualified Time Stamp Service are not saved or archived. This feature is technically not supported.

1.3 Participants

1.3.1 Trust Service Provider "Trustcenter der Deutschen Rentenversicherung"

The carrier of pension insurance "Deutsche Rentenversicherung" are operating a common "Trustcenter der Deutschen Rentenversicherung".

The trustcenter provides amongst others a qualified Time Stamp Authority service. This service issues time stamps compliant to eIDAS regulation article 42.

The "Trustcenter der Deutschen Rentenversicherung" operates a qualified Certification Authority service, which issues amongst others the qualified certificates for the qualified Time Stamp Authority.

The "Trustcenter der Deutschen Rentenversicherung" operates also an advanced Certification Authority, which issues amongst others end-entity user certificates for authentication of users, who may use the qualified Time Stamp Authority service.

1.3.2 Qualified Time Stamp Service

The "Trustcenter der Deutschen Rentenversicherung" operates as Trusted Service Provider the qualified Time Stamp Authority compliant to eIDAS regulation article 42.

1.3.3 Subscriber

Subscriber of qualified Time Stamp Service are individuals or sponsors of systems, who may request qualified time stamps from the "Trustcenter der Deutschen Rentenversicherung".

Subscriber are limited to carrier of pension insurance, carrier of social insurance and other public-law bodies of Germany. Trustcenter administrators of "Deutsche Rentenversicherung Bund" manage the subscriber of the qualified Time Stamp Authority. The usage of the qualified Time Stamp Authority service is based on an administrative agreement between the "Trustcenter der Deutschen Rentenversicherung" and the institution of the subscriber.

1.3.4 Relaying Parties

The affiliation to relying parties is not limited. The status of qualified certificates belonging to a qualified time stamp signature can be verified over the internet.

1.4 Applicability

1.4.1 Types of Time Stamps and Utilisation

The qualified Time Stamp Authority service of the "Trustcenter der Deutschen Rentenversicherung" creates qualified time stamps according to eIDAS regulation article 42.

Only persons or systems may request a qualified time stamp, who are authenticated by an authentication certificate of the "Trustcenter der Deutschen Rentenversicherung" in advance. Authentication is processed by a TLS-Proxy in front of the qualified Time Stamp Authority.

These user authentication certificates are stored and configured inside the Time Stamp Authority as trusted user certificates. Only subscriber may get such an authentication certificate, who belong to an institution, which has signed the administrative agreement mentioned in chapter 1.3.3).

The qualified Time Stamp Authority uses at least six smart cards as secure signature creation devices (SSCD) to create the signatures for qualified time stamps:

- Each of the two Time Stamp Authorities in the main datacenter gets at least one SSCD,
- One replacement SSCD for the main datacenter,
- Each of the two Time Stamp Authorities in the backup datacenter gets at least one SSCD,
- One replacement SSCD for the backup datacenter.

Each SSCD includes an individual key pair. The "Trustcenter der Deutschen Rentenversicherung" generates for each SSCD a qualified certificate. Qualified time stamps can be verified with the public key of the Time Stamp Authority certificate, the public key is part of the certificate delivered in the qualified time stamp.

The qualified Certification Authority of Trust Service Provider "Deutsche Rentenversicherung" generates the qualified certificates for qualified Time Stamp Authority. The qualified certificates of qualified Time Stamp Authority have all the same subject name. They differentiate from the others in certificate serial number and in the included public key.

- Issuer [May 2016]:
  OU=QC Root CA, O=Deutsche Rentenversicherung, C=DE
- Subject [May 2016]:
  CN=QC Root TSP, OU=QC Root CA, O=Deutsche Rentenversicherung, C=DE

The certificate of the issuing CA can be downloaded from public directory service of the "Trustcenter der Deutschen Rentenversicherung". This certificate of the issuing CA can also be requested directly in the time stamp request. The certificate of the issuing CA can verified using the appropriate OCSP-Responder (refer to policy of qualified Certification Authority of "Deutsche Rentenversicherung" [6]).

Authorized persons or systems under control of authorized sponsors may request qualified time stamps using the following URL:

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

The formats of requests and responses are compliant to standards RFC 3161 [7] and ETSI 319422 [4]. The request includes amongst others the hash value of the data, which shall be time stamped. The qualified Time Stamp Authority supports the hash algorithm SHA2-256 and SHA2-512.[1]

The lifetime of qualified time stamps is not limited. The qualified Time Stamp Authority logs the creation of qualified time stamps in a log file for audit purposes. The retention period of the log files is defined in chapter 1.4.2.

The "Trustcenter der Deutschen Rentenversicherung" ensures the validation of the signature of qualified time stamps at least 30 years after the end of validity of the certificate of the qualified Time Stamp Authority, which is used for validation.

1.4.2 Accuracy of time stamps, Logging features

The qualified Time Stamp Authority generates time stamps with an accuracy of at least 1 second. The qualified Time Stamp Authority uses the internal system clock as time base. The internal system clock is synchronized with the official German time source once every 12 hours.

The internal system clock is compared against the official German time source every 10 seconds. The difference between these two times must not exceed 1 second. If a time difference greater than 1 second is detected then will the qualified Time Stamp Authority immediately be stopped.

The DCF77 radio time signal provides the official German time source. The radio time signal is based on high-precise time sources of the German time lab UTC(PTB).

The qualified Time Stamp Authority logs all generated time stamps into a log file. The log file is incorporated into daily log rotation and log backup procedures. The retention period of the log files is 5 years.

1.4.3 Certifications

The software of Time Stamp Authority is certified according to ITSEC level E2. This certification is compliant to Common Criteria level EAL3. This software is operated in the secured environment of the "Trustcenter der Deutschen Rentenversicherung".

The secure signature creation devices (SSCD) are certified according Common criteria level EAL4+. The SSCD are initialised, personalised and operated in the secured environment of the "Trustcenter der Deutschen Rentenversicherung".

The "Trustcenter der Deutsche Rentenversicherung" operates the qualified Time Stamp Authority according to eIDAS regulation article 42. The operation of qualified Time Stamp Authority is registered at the German supervising administration according to eIDAS regulation article 17.

[1] The notation SHA2-256 and SHA2-512 is derived from notation of the new hash algorithm of SHA3 group.

1.5 Rights and Obligations

1.5.1 Rights of Subscriber

The rights of the subscriber are regulated in the administrative agreement between the "Trustcenter der Deutschen Rentenversicherung" and the institution of the subscriber (refer to chapter 1.3.3).

1.5.2 Obligations of Subscriber and Relaying Parties

Subscriber and relying parties have the obligation to validate the time stamps issued by the qualified Time Stamp Authority of the "Trustcenter der Deutschen Rentenversicherung" according to the specifications of the appropriate CP/CPS policy document (refer to [6]).

1.5.3 Liability of Trust Service Provider

The "Trustcenter der Deutsche Rentenversicherung" is liable according to general lawful regulations. The liability for qualified signature certificates is regulated in the appropriate CP/CPS policy document (refer to [6]).

1.5.4 Privacy

The qualified Time Stamp Authority 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 Certification Authority, which has issued the certificate of the Time Stamp Authority.

Both qualified certificates include a pseudonym of the certificate holder. The qualified certificate of the Certificate Authority is available on the internet site of "Deutsche Rentenversicherung Bund" (refer to [8]).

The generated time stamps are stored in log files by the Time Stamp Authority. The arbitration board can use these log files by to settle differences. The retention period of the log files is regulated in chapter 1.4.2.

The subscriber of qualified Time Stamp Authority services have to authenticate himself or herself to a TLS-Proxy server in front of the Time Stamp Authority. This authentication is based on TLS client certificates. These client certificates include the name of the organisation of the subscriber. These client certificates are stored in log files for charging and analysis purposes. The retention period of the log files is regulated in chapter 1.4.2.

1.5.5 Applicable Law

The law applicable to this policy is generally German law. In case of differences between German law and eIDAS regulation, the eIDAS regulation is prioritised and overrides German law. The place of jurisdiction is regulated in the law.

1.5.6 Arbitration Board

The arbitration board of the "Trustcenter der Deutschen Rentenversicherung" 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 1170-05 Trustcenter / Schiedsstelle D-10704 Berlin

2 References to ETSI EN 319 401 / ETSI EN 319 421

This policy of qualified Time Stamp Authority of the "Trustcenter der Deutschen Rentenversicherung" is oriented on the appropriate standards:

- ETSI EN 319401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [2]
- ETSI EN 319421: Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps [3]

Standard ETSI EN 319401 defines general requirements to the policy of trusted service provider. Standard ETSI EN 319421 defines the requirements for Time Stamp Authorities in detail. The following chapter figure out how the requirements of these standards are fulfilled by the qualified Time Stamp Authority.

2.1 Scope

This policy belongs to the qualified Time Stamp Authority service provided by the "Trustcenter der Deutschen Rentenversicherung".

2.2 References

The relevant references are listed in chapter 3.4.

2.3 Abbreviations and Definitions

Document specific abbreviations and definitions are defined in chapter 3.2 and 3.3.

2.4 General Concepts

2.4.1 General Policy Requirements Concepts

The qualified Time Stamp Authority generates qualified time stamps for authorized subscriber of carrier of pension insurance, carrier of social insurance and other public-law bodies of Germany.

2.4.2 Software of Time Stamp Authority

The qualified Time Stamp Authority is one software component, which cannot be divided. This software provides logical different services like time drift monitoring, time synchronisation, monitoring of the secure signature creation devices and generation of qualified time stamps.

2.4.3 Service of Time Stamp Authority

The "Trustcenter der Deutschen Rentenversicherung" operates a qualified Time Stamp Authority in a high-availability configuration. At least six secure signature creation devices are used for signature generation. The technology is figured out in chapter 1.4.

2.4.4 Subscriber

The subscriber are figured out in chapter 1.3.

2.4.5 TSA Policy and TSA Practice Statements

The policy of the qualified Time Stamp Authority (TSA) is subject of this document.

A separate document for "TSA Practice Statements" is not foreseen. The Security Concept and the Operational Manual include the relevant definitions and regulations for the qualified Time Stamp Authority and the belonging qualified Certification Authority. Both documents are confidential and not publicly available.

The public available information regarding the qualified Time Stamp Authority is included in this policy document. The public available information regarding the qualified Certification Authority is included in appropriate policy document [6].

The usage of qualified Time Stamp Authority service is based on an administrative agreement between the "Trustcenter der Deutschen Rentenversicherung" and the institution of the subscriber. This agreement includes additional information for authorized subscriber.

2.5 Introduction to Time Stamp Policy and General Requirements

2.5.1 General

The qualified Time Stamp Authority is operated according to "Best Practices Time Stamp Policy (BTSP)". This policy is defined for time stamp services working with Public Key Certificates (PKC) and an accuracy of at least one second.

2.5.2 Identification

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

The object identifier (OID) of BTSP:

```
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)
```

2.5.3 User Community and Applicability

The qualified Time Stamp Authority of the "Trustcenter der Deutschen Rentenversicherung" is not public available. Subscriber are limited to carrier of pension insurance, carrier of social insurance and other public-law bodies of Germany (refer to chapter 1.3.3). The validation of qualified time stamps by relying parties is public available via CRL download or OCSP requests.

2.6 Policy und Practices

2.6.1 Risk Assessment

The collection and assessment of risks as well as the derivation of countermeasures to mitigate risks are subject of the security concepts of the qualified Time Stamp Authority and the qualified Certification Authority of the "Trustcenter der Deutschen Rentenversicherung". These documents are classified as confidential and not public available. The security concepts are periodically (normally once a year) reviewed and updated if required.

2.6.2 TSA Practice Statement

It is mentioned in chapter 2.4.5 that a separate document "TSA Practice Statements" is not planned. The guidelines for management and operation of the qualified Time Stamp Authority are defined in the appropriate security concepts of the qualified Time Stamp Authority and the qualified Certification Authority of the "Trustcenter der Deutschen Rentenversicherung". These documents are classified as confidential and not public available.

2.6.3 Terms and Conditions

The rights and obligations of subscriber and relying parties are defined in chapter 1.5. Additional terms of use for subscribers are defined as part of the administrative agreement between the "Trustcenter der Deutschen Rentenversicherung" and the institution of the subscriber (refer to chapter 1.3.3).

2.6.4 Information Security Policy

The guidelines for management and operation of the qualified Time Stamp Authority are defined in the appropriate security concepts of the qualified Time Stamp Authority and the qualified Certification Authority of the "Trustcenter der Deutschen Rentenversicherung". These documents are classified as confidential and not public available.

2.6.5 TSA Obligations

The obligations are defined in chapter 1.5.

2.6.6 Information for Relaying Parties

The term relying parties comprises all user, who want verify a qualified time stamp. The verification includes checks of confidence of the appropriate authorities as well as the used signatures.

The response of the qualified Time Stamp Authority includes the certificates of the qualified Time Stamp Authority and of the qualified Root Certification Authority, which has issued the certificated of the qualified Time Stamp Authority. These certificates includes the URL of the appropriate OCSP responder to verify the certificate revocation status.

The certificate of the qualified Root Certification Authority is published on and can be downloaded from the web site of "Deutsche Rentenversicherung Bund" [8]. It is also published in the official journal of "Deutschen Rentenversicherung Bund" „RVaktuell“.

2.7 TSA Management and Operation

2.7.1 Introduction

No stipulation.

2.7.2 Organisation

The carrier of pension insurance "Deutsche Rentenversicherung Bund" operates the qualified Time Stamp Authority. The security concepts for qualified Time Stamp Authority and for qualified Certification Authority define the requirements for the organisation of the "Trustcenter der Deutschen Rentenversicherung". The organisational concept defines the practical organisation in the trustcenter. The assignment of employees to the defined trustcenter roles is documented in appropriate trustcenter protocols.

2.7.3 Personal Security

The security concepts for qualified Time Stamp Authority and for qualified Certification Authority define the requirements for the staff managing and operating the "Trustcenter der Deutschen Rentenversicherung".

2.7.4 Asset Management

The administrative staff of the "Trustcenter der Deutschen Rentenversicherung" manages all assets belonging to the trustcenter. The appropriate procedures for management, operation and business continuity are defined in the operational manual. The Operational manual is periodically (normally once a year) reviewed and updated if required.

The generated time stamps are stored in log files by the Time Stamp Authority. The arbitration board can use these log files by to settle differences. The operational manual defines the procedures for log file backups.

2.7.5 Physical Access Control

The qualified Time Stamp Authority is operated on dedicated server. These server are located in the datacenter of the "Trustcenter der Deutschen Rentenversicherung". The datacenter as well as the appropriate racks are physically secured. Only authorized trustcenter staff can get the required access token.

Logical access control is provided by firewalls to the DRV network as well as to the internet. Network access is limited to requests for qualified time stamps.

Relying parties can verify the certificate revocation status via OCSP responder. Access to the qualified Time Stamp Authority is not required as part of verification process.

Authorized administrators can manage the qualified Time Stamp Authority using the local server console.

2.7.6 Cryptographic Controls

2.7.6.1 General

The crypto manager of the "Trustcenter der Deutschen Rentenversicherung" regularly reviews the used cryptographic algorithm. The report of approved cryptographic (refer to [9]) algorithms issued by the supervisory body of Germany according to eIDAS regulation [1] article 17 is the basement for the review.

The term "Time Stamp Authority" (TSA) identifies the time stamp service as a whole. The term "Time Stamp Unit" (TSU) identifies a single instance of the TSA processing time stamp requests and generating time stamp responses with a dedicated secure signature creation device (SSCD). The TSA comprises two active TSU's in the main datacenter and two hot standby TSU's in the backup datacenter.

2.7.6.2 TSU Key Generation

A qualified Time Stamp Unit uses a smartcard as secure signature creation device (SSCD), which is certified according to Common Criteria with EAL 4+. The key generation as well as the signature creation is processed on the smartcard in the secure environment of the "Trustcenter der Deutschen Rentenversicherung". The smartcard uses RSA keys with key length 2048 bit.

2.7.6.3 TSU Private Key Protection

The private signature key of the qualified Time Stamp Unit is protected by the physical key store, the smartcard. The export of the private signature key from the smartcard is impossible by design. The key generation is processed directly on the smartcard based on the chip random number generator (RNG). The RNG and the prime number check algorithm are the basement for probabilistic generated prime numbers and as far as possible derived unique keys.

An administrator must enter the signature PIN in advance of private key usage for signature purposes. The entering of the signature PIN is processed once at start of the qualified Time Stamp Unit. Only authorized trustcenter administrators have access to the smartcard signature PIN.

2.7.6.4 TSU Public Key Certificate

The qualified Root Certification Authority issues the public key certificate for the qualified Time Stamp Unit. The time stamp response includes the certificates of the qualified Time Stamp Unit and of the qualified Root Certification Authority.

The certificate of the qualified Root Certification Authority is published on and can be downloaded from the web site of "Deutsche Rentenversicherung Bund" [8]. It is also published in the official journal of "Deutschen Rentenversicherung Bund" „RVaktuell".

These certificates includes the URL of the appropriate OCSP responder to verify the certificate revocation status.

2.7.6.5 Re-Keying TSU Key

The usage period of the Time Stamp Unit public key certificate is defined in the certificate profile policy document of the "Trustcenter der Deutschen Rentenversicherung". The TSU key pair is not longer valid than the appropriate key pair. The validity period is currently defined with 7 years at a maximum.

A re-keying process, i.e. creation of a new certificate with an already used key, is not allowed.

2.7.6.6 Life Cycle Management of Signing Cryptographic Hardware

The provider of the smartcards delivers the smartcards for Time Stamp Units (TSU) in manufacturing state to the "Trustcenter der Deutschen Rentenversicherung". The manufacturing state can be identified by challenge-response-procedure using the so-called manufacturing key. The manufacturing key is a secret key and not public known.

The initialisation of the TSU smartcards as well as the generation of the TSU key pair is processed in the datacenter of the "Trustcenter der Deutsche Rentenversicherung". The initialisation will detect, if the smartcards do not carry the right manufacturing key. In this case, the smartcard will not be used for TSU's.

2.7.6.7 End of TSU Key Life Cycle

The Time Stamp Unit can use the secure signature creation device (SSCD) with its signature key as long as (a) the certificate is valid, which certifies the appropriate public key, or the SSCD is replaced by new one with new signature key and new public key certificate.

If a SSCD is replaced by a new one, then the old one will be physically destroyed. This process makes it impossible to use the old signature key any longer.

2.7.7 Time Stamp

2.7.7.1 Time Stamp Issuance

The qualified Time Stamp Authority creates time stamps compliant to the standard ETSI EN 319422 [4]. The Time source has an accuracy of 1 second and is derived from German time laboratory UTC(PTB) (refer to chapter 1.4.2).

2.7.7.2 Clock Synchronisation with UTC

Time synchronisation is based on German time laboratory UTC(PTB) via the DCF77 radio time signal (refer to chapter 1.4.2).

2.7.8 Physical and Environmental Security

The collection and assessment of risks as well as the derivation of countermeasures to mitigate risks are subject of the security concepts of the qualified Time Stamp Authority and the qualified Certification Authority of the "Trustcenter der Deutschen Rentenversicherung". This includes physical and environmental security risks.

2.7.9 Operation Security

The product of the qualified Time Stamp Authority is certified according to ITSEC evaluation level E2. Changes of the installation are processed (a) as part of a project based in a predefined change request process or (b) as a patch in case of an incidents. All changes will be documented in the appropriate installation & configuration documentation.

At first patches and updates will be installed and tested in a quality assurance environment. After test approval by a responsible person of the trustcenter, the software will be installed and operated in the operational environment.

The operational and management processes are defined in the operational manual.

The collection and assessment of risks as well as the derivation of countermeasures to mitigate risks are subject of the security concepts of the qualified Time Stamp Authority and the qualified Certification Authority of the "Trustcenter der Deutschen Rentenversicherung". This includes operational security risks.

2.7.10 Network Security

The network of the qualified Time Stamp Authority has the following requirements:

- The qualified Time Stamp Units are operated on dedicated server. The server are located in the trustcenter datacenter. The server are logically separated from the DRV network and from the internet via firewalls.
- The network access to the Time Stamp Unit server is limited to dedicated network services (interface/protocol/port) required for requesting time stamps.
- The network access to the Time Stamp Unit server is limited to authorized subscriber.
- The Time Stamp Unit server do not communicate with the other application server in the "Trustcenter der Deutschen Rentenversicherung".

The network configuration is defined in the network concept of "Deutsche Rentenversicherung Bund".

The collection and assessment of risks as well as the derivation of countermeasures to mitigate risks are subject of the network security concept.

2.7.11 Incident Management

A central monitoring system supervises the platform and the service of the qualified Time Stamp Authority. The qualified Time Stamp Authority service writes all activities in its log files. The monitoring system evaluates also the error messages in these log files.

In case of a platform failure, the trustcenter administrators can initiate a failover procedure to switch the Time Stamp Authority service from the main to the backup datacenter. The failover process is described in the operational manual.

In case of a software product failure, the trustcenter administrator can initiate an incident in a ticket system. Service level 2 by the system integrator and service level 3 by the product vendor will then work to solve the issue. Appropriate service contracts are closed.

2.7.12 Collection of Evidence

The qualified Time Stamp Authority service writes all activities in its log files. The log files will be archived. The log files include amongst other information:

- Requests and responses of qualified time stamps,
- Time synchronisation based on DCF77 radio time signal,
- Lost of DCF77 radio time signal,
- Error in time drift (deviation greater than 1 second between server time and DCF radio time signal).

The log files will be archived. The retention period is defined in chapter 1.4.2. Due to technical reasons, there is not time unit in the time stamp responses. This information is not required for evidences to settle differences (refer to chapter 1.5.6).

2.7.13 Business Continuity Management

The recovery of a qualified Time Stamp Unit or the whole qualified Time Stamp Authority service is defined in the business continuity plan. The business continuity plan is part of the operational manual of the "Trustcenter der Deutschen Rentenversicherung".

2.7.14 TSA Termination and Termination Plans

The termination of the qualified Time Stamp Authority follows the rules for termination of trusted service provider. The termination plan of the qualified Time Stamp Authority is part of the operational manual.

Subscribers of the qualified Time Stamp Authority will be informed according to the agreement between the "Trustcenter der Deutsche Rentenversicherung" and the institution of the subscriber. Relying parties will not be informed.

2.7.15 Compliance

The qualified Time Stamp Authority is operated according to the requirements of eIDAS regulations article 42. The appropriate security concepts are provided to the German supervisory body for qualified Time Stamp Authorities according to eIDAS regulation article 17.

2.8 Additional Requirements for Qualified Time Stamp Authority

2.8.1 TSU Public Key Certificate

The public key certificates for the qualified Time Stamp Units are issued by the qualified Root Certification Authority service of the "Trustcenter der Deutschen Rentenversicherung". The public key certificate of the qualified Time Stamp Unit includes a QC compliance statement [5].

2.8.2 TSA Issuing Non-Qualified and Qualified Electronic Time Stamps

The qualified Time Stamp Authority of the "Trustcenter der Deutschen Rentenversicherung" creates only qualified time stamps.

3 Lists and References

3.1 Document History

Version	Release	Reason
01.00	27.06.2006	Initial version
02.00	10.08.2007	Migration of cryptographic algorithm
03.00	23.01.2009	Validation of Time Stamp Service via CRL was withdrawn
04.00	12.05.2016	Adaption to standards ETSI EN 319401, ETSI EN 319421, Regulation No. 910/2014 of EU (eIDAS)
04.01	03.06.2016	Archiving of audit logs was redefined to 5 years
04.02	30.09.2016	Arbitration board added

3.2 Document-specific Abbreviations

BIPM	Bureau International des Poids et Mesures
BNetzA	Bundesnetzagentur (Supervisory body of Germany according to [1])
CC	Common Criteria
CEN	European Committee for Standardization
EAL	Evaluation Assurance Level (EAL1 - EAL7)
eIDAS	Electronic Identification and Trust Services for Electronic Transactions in the European Market
ESCD	Electronic Signature Creation Device
ETSI	European Telecommunications Standards Institute
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union
OID	Object Identifier
PBS	Production-Backup-System
PHS	Production-Main-System
PTB	German UTC Laboratory (Physikalisch-Technische Bundesanstalt)
QA	Quality Assurance
QC	Qualified Certificate
SSCD	Secure Signature Creation Device
SSL	Secure Socket Layer
TAI	International Atomic Time
TLS	Transport Layer Security
TSA	Time Stamp Authority
TSP	Time Stamp Protocol
TSP	Trust Service Provider
TSS	Time Stamp Service
TSU	Time Stamp Unit
UTC	Universal Time Coordinated

3.3 Document-specific Definitions

DCF77 DCF77 is a longwave radio time signal and standard-frequency radio station of Germany. DCF77 is controlled by PTB (Physikalisch-Technische Bundesanstalt). PTB operates 4 high-precise Caesium-based clocks for the national time reference UTC (PTB).

Time Stamp Authority Service for creation of electronic time stamps

Time Stamp Unit System comprising hard- and software, which is manage das one unit. Each Time Stamp Unit uses its own signature key to sign time stamps.

3.4 References

[1] eIDAS-RE: REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Official Journal of the European Union L 257/73
http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32014R0910

[2] ETSI EN 319401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
http://www.etsi.org/deliver/etsi_en/319400_319499/319401/

[3] 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/

[4] 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/

[5] ETSI TS 101862: Qualified Certificate Profile
http://www.etsi.org/deliver/etsi_ts/101800_101899/101862/

[6] Certificate Policy und Certification Practice Statement of Trust Service Provider "Root Certification Authority of Deutschen Rentenversicherung"
http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html

[7] RFC 3161: Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)
http://www.faqs.org/rfcs/rfc3161.html

[8] Web-Site of Trust Service Provider "Trustcenter der Deutschen Rentenversicherung"
http://www.deutsche-rentenversicherung-bund.de/static/trustcenter/policy.html

[9] Web-Site of Supervisory body of Germany for publication of approved cryptographic algorithm
http://www.bundesnetzagentur.de/cln_1432/DE/Service-Funktionen/QualifizierteelektronischeSignatur/WelcheAufgabenhatdieBundesnetzagentur/GeeigneteAlgorithmenfestlegen/geeignetealgorithmenfestlegen_node.html