Time-Stamping Authority

Policy and Practice Statement

exceet Secure Solutions GmbH

Author:	exceet Secure Solutions GmbH, J. Krumm
	exceet Secure Solutions GmbH, A. Kotte
	exceet Secure Solutions GmbH, P. Kraschinski

Document Class:	**Public**
Version:	1.7
Date:	13.10.2016
Filename:	TSA_Policy_and_Practice_Statement_exceet_1.7.docx

Document History

Version	Date	Author	Description
1.0	06.03.2016	Andreas Kotte	Layout and structure, Andreas Kotte
1.1	07.03.2016	Jörg Krumm	Content and security concept referrers, Jörg Krumm
1.2	08.03.2016	Andreas Kotte	Review, Andreas Kotte
1.3	09.03.2016	Jörg Krumm	Corrections, Jörg Krumm
1.4	23.03.2016	Jörg Krumm	Added additional information according to the observations report, version 1.0, of the conformity assessment body, TÜVIT Added a “important document information” header to the document
1.5	24.03.2016	Jörg Krumm	Added/ corrected information according to the observation report, version 1.1, of the conformity assessment body, TÜVIT
1.6	31.08.2016	Jörg Krumm	7.6.6 Added the information, that the validity of private keys never exceeds the validity of issued certificates. 7.14 b) f) added a statement, that the TSP will revoke all of its certificates in case of termination
1.7	13.10.2016	Pierre Kraschinski	Changed legal form of corporation and URL to published certificates.

Document Information

Important document information	
Class	Policy
Title	TSA Policy and Practice Statement exceet Secure Solutions GmbH
Number:	-
Author	Jörg Krumm
Responsible Auditor of the document::	Schmitz, Christian
Filename:	tsa_policy_and_practice_statement_exceet_1.7.docx
Creation started on:	2016-03-06
Last change on:	2016-10-13
Pagecount:	27
Status:	Approved
Approved on:	
Approved by:	exceet Secure Solutions GmbH Christian Schmitz, Managing Director

Table of content

Introduction

Companies, authorities and organizations of all kinds throughout the world are increasingly generating their processes electronically for purposes of optimization, cost reduction and speed. Thus, existing paper-based processes are being replaced by electronic processes and new processes made possible through the use of digital information and communication.
These new, improved processes (using electronic information) are subject to the same statutory provisions, compliance and protection requirements, as traditional paper-based processes. In order to meet these requirements, both paper-based and electronic information has to be protected, among other things, against manipulation and loss. In order to be able to assess the observation of compliance requirements in a professional environment, proof of integrity, completeness and confidentiality are often the main criteria. Electronic time stamps can deliver this proof of integrity and completeness in a way that is simple, legally secure, permanent, inexpensive and, on request, anonymous.
A time stamp is an electronic certificate, which states when certain data existed. It thus documents the "when" and "what". An electronic signature, often referred to as personal signature, documents the "who" and "what". In contrast to an electronic signature, a time stamp is not bound to people and their actions. It can thus be integrated much more simply and also fully-automatically into electronic processes.

Time stamps are easier to use than electronic signatures as their application can be fully automatic and independent of specific individuals, or anonymous.

About exceet Secure Solutions GmbH

exceet Secure Solutions GmbH is a 100% owned subsidiary of the internationally active exceet Group AG, a technology company that specializes in developing and manufacturing of intelligent, complex and secure electronics.
Started in 2000, as a specialist for securing electronic business processes with the help of qualified electronic signatures and timestamps, the company's focus today is on secure solutions in the areas of M2M (Machine-to-Machine), Multi ID - and Access Solutions (eMIS) and based on improved networking of organizations, for exam-ple through process optimization in the field of telematics. The offer is completed by Hardware Security Modules (HSM), PKI solutions and products as well as services for signatures and timestamps, including trust center operation.

About this document

The Document is structured according ETSI EN 319 421 [5]

1. Scope

The present document specifies policy and security requirements relating to the operation and management practices of the ESS Trusted Service Authority issuing time-stamps. Such time-stamps can be used in support of digital signatures or for any application requiring to prove that a datum existed before a particular time.

The present document can be used by independent bodies as the basis for confirming that ESS can be trusted for issuing time-stamps according to Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation).

The present document does not specify:

- protocols used to access the ESS-TSA;
- how the requirements identified herein can be assessed by an independent body;
- Requirements for information to be made available to such independent bodies;
- Requirements on such independent bodies.

2. References

[1]	Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
[2]	ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".
[3]	ISO/IEC 15408 (parts 1 to 3): "Information technology -- Security techniques -- Evaluation criteria for IT security".
[4]	ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"
[5]	ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps"
[6]	ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".
[7]	FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".
[8]	Security Concept, TSA, Version 4.5 (non-disclosed)
[9]	Terms and Conditions for timestamping customers http://www.exceet-secure-solutions.de/en/it-security/electronic-timestamps-compliant-with-eidas/
[10]	Informationssicherheitsleitline, Version 1.2, 20.08.2014 (non-disclosed)
[11]	IETF (RFC3161) https://www.ietf.org/rfc/rfc3161.txt

3. Definitions and abbreviations

3.1. Definitions

Coordinated Universal Time (UTC): time scale based on the second as defined in Recommendation ITU-R TF.460-6 [1]

dcf-77: "DCF77 is a German longwave time signal and standard-frequency radio station. It started service as a standard-frequency station on 1 January 1959. In June 1973 date and time information was added. Its primary and backup transmitter are located at 50°0′56″N 9°00′39″E in Mainflingen, about 25 km south-east of Frankfurt am Main, Germany. The transmitter generates a nominal power of 50 kW, of which about 30 to 35 kW can be radiated via a T-antenna." *Wikipedia, 08.03.2016

ntp: "Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. In operation since before 1985, NTP is one of the oldestInternet protocols in current use. NTP was originally designed by David L. Mills of the University of Delaware, who still oversees its development." *Wikipedia, 08.03.2016

relying party: recipient of a time-stamp who relies on that time-stamp

subscriber: legal or natural person to whom a time-stamp is issued and who is bound to any subscriber obligations

time-stamp: data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time

time-stamp policy: named set of rules that indicates the applicability of a time-stamp to a particular community and/or class of application with common security requirements

Time-Stamping Authority (TSA): TSP providing time-stamping services using one or more time-stamping units

Time-stamping service: trust service for issuing time-stamps

Time-Stamping Unit (TSU): set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time **trust service:** electronic service that enhances trust and confidence in electronic transactions

Trust Service Provider (TSP): entity which provides one or more trust services

TSA Disclosure statement: set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements

TSA practice statement: statement of the practices that a TSA employs in issuing time-stamp

TSA system: composition of IT products and components organized to support the provision of time-stamping services

UTC(k): time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns.

3.2. Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 401 [4] and the following apply:

BIPM	Bureau International des Poids et Mesures
BTSP	Best practices Time-Stamp Policy
CA	Certification Authority
ESS	exceet Secure Solutions GmbH
GMT	Greenwich Mean Time
IERS	International Earth Rotation and Reference System Service
IT	Information Technology
TAI	International Atomic Time
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

4. General concepts

4.1. General policy requirements concepts

The present document references ETSI EN 319 401 [4] for generic policy requirements common to all classes of trust service providers service.

These policy requirements are based upon the use of public key cryptography, public key certificates and reliable time sources.

Subscriber and relying parties are expected to consult the TSA's practice statement to obtain further details of precisely how this time-stamp policy is implemented by the particular TSA (e.g. protocols used in providing this service).

4.2. Time-stamping services

The provision of time-stamping services is broken down in the present document into the following component services for the purposes of classifying requirements:

Time-stamping provision:
This service component generates time-stamps.

Time-stamping management:
This service component monitors and controls the operation of the time-stamping services to ensure that the service provided is as specified by the TSA. This service component has responsibility for the installation and de-installation of the time-stamping provision service. This subdivision of services is only for the purposes of clarifying the requirements specified in the present document and places no restrictions on any subdivision of an implementation of time-stamping services.

4.3. Time-Stamping Authority (TSA)

A Trust Service Provider (TSP) providing time-stamping services to the public, is called the Time-Stamping Authority (TSA).
The TSA has overall responsibility for the provision of the time-stamping services identified in clause 4.2. The TSA has responsibility for the operation of one or more TSUs which creates and signs on behalf of the TSA. The TSA responsible for issuing a time-stamp is identifiable (see clause 7.7.1, d).
ESS hereby confirms, that the TSA is audited at least every 24 month by a conformity assessment body.

The assessment report is submitted within 3 working days to the national supervisory body.

Where the supervisory body requires the TSA to remedy any failure to fulfil requirements, the TSA will act accordingly and in a timely fashion.

The supervisory body will be informed of any change in the provision of the TSA.

ESS may make use of other parties to provide parts of the time-stamping services. However, the TSA always maintains overall responsibility (as per clause 6.5) and ensures that the policy requirements identified in the present document are met.

ESS may operate several identifiable time-stamping units.

ESS is a trust service provider as described in ETSI EN 319 401 [4] which issues time-stamps.

4.4. Subscriber

When the subscriber is an organization, it comprises several end-users or an individual end-user and some of the obligations that apply to that organization will have to apply as well to the end-users. In any case the organization will be held responsible if the obligations from the end-users are not correctly fulfilled and therefore such an organization is expected to suitably inform its end users.

When the subscriber is an end-user, the end-user will be held directly responsible if its obligations are not correctly fulfilled.

4.5. Time-stamp policy and TSA practice statement

This clause explains the relative roles of time-stamp policy and TSA practice statement. It places no restriction on the form of a time-stamp policy or practice statement specification.

A time-stamp policy is a form of Trust Service Policy as specified in ETSI EN 319 401 [4] applicable to trust service providers issuing time-stamps.

TSA Practice Statement is a form of Trust Service Practice Statement as specified in ETSI EN 319 401 [4] applicable to trust service providers issuing time-stamps.

The present document specifies the time-stamp policy and the practice statement for the ESS TSA.

5. Time-stamp policies

5.1. General

This policy defines a set of rules adhered by ESS issuing time-stamps, supported by public key certificates, with an accuracy of 100 milliseconds or better.

5.2. Identification

The identifier of the time-stamp policy specified in the present document is: **1.3.6.1.4.1.12655.3.2**

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) exceet-secure-solutions(12655) tsa(3) EU-Regulation 910(2)}

By including this object identifier in the generated time-stamps, ESS claims conformance to this time-stamp policy.

5.3. User community and applicability

This policy is aimed at meeting the requirements of time-stamp for long term validity (e.g. as defined in ETSI EN 319 122 [6]) but is generally applicable to any use which has a requirement for equivalent quality.

This policy may be used for public time-stamping services or time-stamping services used within a closed community.

6. Policies and practices

6.1. Risk assessment

ESS performs risk assessments on a regular basis to ensure the quality and reliability of the time-stamping services. Security Controls that are defined in a security concept of the time-stamping services are controlled every three months in order to ensure the efficiency of the controls.

Detailed explanation regarding this topic is described in the *security concept [8]*: Chapter 9 “Bedrohungsanalyse und Maßnahmenauswahl” and chapter 18 “Restrisikoanalyse”.

6.2. Trust Service Practice Statement

Quality Assurance is one of the most important values of ESS. Therefore, a variety of security controls have been implemented at ESS that shall ensure the quality, performance and operation of the time-stamping service.

The security controls are documented in a security concept that is reviewed regulary by an independent body, trained trustworthy personal check the adherence of the security controls.

Additionally to be compliant to ETSI TS 119 421 the following measures have been applied, respectively the following information applies to the service:

6.2.1. Time-stamp format

The issued time-stamp token by ESS are compliant to RFC 3161 time-stamps. The service issues RSA2048 encrypted time-stamps that accept one of the following hash algorithm:

- SHA256
- SHA384
- SHA512

6.2.2. Accuracy of the time

The time-stamping service is located in Germany where a time signal is provided via *dcf-77*. The time-stamping service uses this time signal and a set of *ntp* servers as time sources. With that setup the time-stamping service reaches an accuracy of the time of +/-100ms or better with respect to *UTC*.

6.2.3. Limitations of the service

The time stamp service of ESS may only be used in connection with legal transactions/confirmations, the value of which at the time of their use in legal and business transactions does not exceed Euro 2,500,000.- in the individual case and a total of Euro 10,000,000.- per calendar year.

6.2.4. Obligations of the subscriber

Please see “Terms and conditions for timestamp customers [9]” for detailed information.

6.2.5. Obligations of relying parties

Please see “Terms and conditions for timestamp customers [9]” for detailed information.

6.2.6. Verification of the timestamp

Timestamp verification includes the following tasks

Task I: Verification of the timestamp issuer

A timestamping authority that uses appropriate electronic certificates issues the timestamp. The public keys of the used certificates, including the TSU and CA certificates, are published to enable a verification that the timestamp has been signed correctly by the TSA.

The certificates can be found at: http://www.exceet-secure-solutions.de/en/it-security/electronic-timestamps-compliant-with-eidas/

Task II: Verification of the timestamp revocation status

An OCSP responder service is available in order to check the revocation status of the used certificates in the timestamp.

The OCSP responder can be reached at:

http://ocsp.exceet.cloud/ocsp

Task III: Verification of the integrity of the timestamp

The cryptographic integrity of the timestamp, for example the correct ASN.1 structure, and the belonging datum (the data that has been timestamped) can be verified at a webservice form ESS, that is offered free of charge at:

https://www.signature-check.com

6.2.7. Applicable law

Please see “Terms and conditions for timestamp customers [9]” for detailed information.

6.2.8. Service availability

ESS has implemented the following measures to ensure availability of the service:

- Redundant setup of IT Systems, including HSM infrastructure, in order to avoid single point of failures
- Redundant high speed internet connections in order to avoid loss of service
- Use of uninterruptable power supplies

Although those measures ensure service availability ESS cannot guaranty an annual availability of 100%. ESS aims to provide 99% service availability per year while reaching an average availability of 99,95% per year.

6.3. Terms and conditions

Within the published document “Terms and conditions for timestamp customers [9]” information about e.g. limitation of the service, subscribers obligations, information for relying parties or limitations of liability can be found.

Additionally the following information apply:

6.3.1. Trust service policy being applied

The present document represents the applied trust service policy, see chapter 5 for further information.

6.3.2. Period of time during which TSP event logs are retained.

Event logs are retained for at least three month. Timestamp protocols, meaning every issued timestamp, are kept for at least 10 years.

6.4. Information security policy

ESS has implemented an information security policy [10] throughout the company. All employees must adhere to the regulations stated in that policy and derived security concepts.

The information security policy is reviewed on a regular basis and when significant changes occur.

The senior management body of ESS approves the changes of the information security policy.

6.5. TSA obligations

The conformance with the procedures that are stated in the present document is ensured by ESS. An independent supervisory body verifies the efficiency of the procedures on a regular basis.

6.5.1. TSA obligations towards subscribers

The present document places no specific obligations on the subscriber beyond any TSA specific requirements stated in the clause 6.3, Terms and conditions.

6.6. Information for relying parties

The obligations of a Subscriber (see clause 6.5.1) are valid for relying parties too. In addition the relying party shall do the following.

a) verify that the time-stamp has been correctly signed and that the private key used to sign the time-stamp has not been compromised until the time of the verification. ESS provides several ways to do so, see clause 6.2.6.

b) take into account any limitations on the usage of the timestamp indicated by the timestamp policy

c) take into account any other precautions prescribed in agreements or elsewhere

7. TSA management and operation

7.1. Introduction

ESS has implemented an information security management system to maintain the security of the service.

7.2. Internal organization

For proper operations of the time-stamping service, ESS maintains a non-disclosed document, security concept [8], that specifies all operational controls concerning personnel security, access controls, risk assessment…etc. That internal document is used by independent bodies to confirm compliance of the service against ETSI TS 119 421.

a) Legal entity
   The TSA is provided by exceet Secure Solutions GmbH (ESS). ESS is a 100% owned subsidiary of the internationally active exceet Group AG, a technology company that specializes in developing and manufacturing of intelligent, complex and secure electronics:
   exceet Secure Solutions GmbH
   Rethelstrasse 47
   40237 Düsseldorf/ Germany
   HRB Düsseldorf 78770
b) Information Security management and quality management of the service is carried out within the security concept [8] of the service.

7.3. Personnel security

ESS has understood that talented and motivated employees are a key factor for business success. Therefore, the hiring practices is a very important process at ESS.

Only well-educated, with respect to their job role, and trustworthy personnel fulfil operations in the time-stamping service.

A role concept enforces the segregation of duties to ensure that entitled personnel only do important operational tasks.

Before personnel is appointed in trusted roles, the TSP verifies that the necessary knowledge exists or is transferred via trainings and that all background-screening tasks are completed.

TSP personnel is free from conflict of interests that might prejudice the impartiality of the TSP operations.

More information regarding personnel security is described in the *security concept*: Chapter 6 “Personalmanagement”.

7.4. Asset management

All IT systems used within the service are clearly identified, categorized and filed in an asset management database.

a) Media Handling

All media is handled securely.

Data from disposed media is securely deleted, either by an electronic erase of the data or by physically destroying the disposed media.

7.5. Access control

Different security layers with respect to physical access and logical access ensure a secure operation of the time-stamping service.

For instance:

- Secured physical environment
- Segregation of network segments
- Segregation of duties
- Firewalls
- Network and Service Monitoring
- Hardening of IT Systems

In case a person, which carries out operations in the TSP, changes the role or leaves the TSP, all security tokens for the TSP are withdrawn from that person or are changed.

7.6. Cryptographic controls

The TSA uses several private keys to fulfill its service. One private key pair is used to issue the public-key timestamp certificates, that are used within the TSUs. One or more private key pair is or are used within the TSU to issue the timestamp.

All private keys are stored in a FIPS 140-2 Level 3 Hardware Security Modul.

All regulations that are described within the *security concept*: Chapter 13 “Kryptographische Aspekte” shall apply.

7.6.1. TSU key generation

a) The generation of the TSU's signing key(s) is undertaken in a physically secured environment (as per clause 7.8) by personnel in trusted roles (as per clause 7.3) under, at least, dual control. The personnel authorized to carry out this function is limited to those required to do so under the TSA's practices.

b) The generation of the TSU's signing key(s) is carried out within a cryptographic module which is conformant to FIPS PUB 140-2 [i.9], level 3
c) The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time-stamps key is recognized by any national supervisory body, or in accordance with existing current state of art, as being fit for the purposes of time-stamps as issued by the TSA.

7.6.2. TSU private key protection

The TSU private signing key is held and used within a cryptographic module which is conformant to FIPS PUB 140-2 [i.9], level 3.

TSU private keys are not backed up, only the CA private key is backed up only by personnel in trusted roles using, at least, dual control in a physically secured environment. Time-stamping

7.6.3. Public key certificate

The TSA guarantees the integrity and authenticity of the TSU signature verification (public) keys as follows:

a) TSU signature verification (public) keys are available to relying parties in a public key certificate. The certificates are published at: http://www.exceet-secure-solutions.de/it-security/governance-risk-compliance/
b) The TSU does not issue a time-stamp before its signature verification (public key) certificate is loaded into the TSU or its cryptographic device. When obtaining a signature verification (public key) certificate, the TSA verifies that this certificate has been correctly signed (including verification of the certificate chain to a trusted certification authority).

7.6.4. Rekeying TSU's key

The life-time of TSU's certificate is not longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose (see clause 7.6.1c).

Once a year or when significant changes occur, the person who holds the role “Kryptografiebeauftragter” verifies all cryptographic algorithm used in the TSA against the algorithm recognized as suitable as in clause 7.6.1c).

If an algorithm becomes compromised or is not suitable anymore, the person will instruct the TSA to rekey any affected private keys.

7.6.5. Life cycle management of signing cryptographic hardware

The used cryptographic hardware is inspected by trustworthy personnel in dual control during shipment and storing. Specifically the hardware is checked for

a) any damages of security seals
b) any damages of the case of the hardware (e.g. scratches, bumps…)

c) any damages of the packing of the hardware

The inspection is protocolled.

Additionally the following applies:

c) The Installation, activation and duplication of TSU's signing keys in cryptographic hardware is done only by personnel in trusted roles using, at least, dual control in a physically secured environment.

d) TSU private signing keys stored on TSU cryptographic module are erased upon device retirement in a way that it is practically impossible to recover them.

7.6.6. End of TSU key life cycle

The validity of all used private keys never exceeds the validity of certificates issued with help of those private keys.

After expiration of the private keys, the private keys within the cryptographic hardware are destroyed in a manner such that the private keys cannot be retrieved or used anymore.

The job role “Kryptografiebeauftragter” defines the key validity in accordance to 7.6.1c)

7.6.7. Root Certification Authority

The TSP operates an own Public Key Infrastructure consisting of an offline “Root Certification Authority” and an OCSP Responder service.

The offline root CA is operated in the same facility and network segments as the TSP. All regulations that apply to the TSU private keys apply to the CA private keys as well, specifically:

a) CA key generation equals clause 7.6.1 TSU key generation
b) CA key protection equals clause 7.6.2 TSU private key protection
c) CA Public key certificate equals clause 7.6.3 Public key certificate
d) Rekeying CA's key equals clause 7.6.4 Rekeying TSU's key
e) End of CA key life cycle equals clause 7.6.6 End of TSU key life cycle
f) The validity of the private keys is not longer than the end of the validity of the related certificate.

7.7. Time-stamp issuance

The ESS time-stamping service issues Time-stamps conform to the time-stamp profile as defined in ETSI EN 319 422 [5].

7.7.1. Clock synchronization with UTC

The TSA clock is synchronized with UTC [1] within an accuracy of +/-500ms or better. In the case, the TSA clock, drifts out of accuracy, no timestamp will be issued until synchronization of the clock.

Detailed explanation regarding this topic is described in the *security concept*: Chapter 8.1.5 “Funktionsbeschreibung”.

Specifically, the following topics are covered:

- Continuous calibration of the TSU clock
- Monitoring of the accuracy of the TSU clock
- Threadanalysis against attacks on time-signals
- Behaviour while skipping/adding leap seconds
- Behaviour while drifting larger that 1s from UTC

7.8. Physical and environmental security

This time-stamping service has been compliant with the German signature law since 2001. Therefore, a highly secured physical environment is necessary. This physically secured environment houses the TSA.

All requirements identified in ETSI EN 319 401 [4], clause 7.6 apply.

The time-stamping management facilities are operated in an environment which physically and logically protects the services from compromise through unauthorized access to systems or data.

Every entry to the physically secure area is subject to independent oversight and an authorised person whilst in the secure area accompanies non-authorized person. Every entry and exist is logged.

Physical protection is achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the time-stamping management.

Physical and environmental security controls protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation.

The TSA's physical and environmental security policy for systems concerned with time-stamping management addresses the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.

Physical and organizational controls protect against equipment, information, media and software relating to the time-stamping services being taken off-site without authorization.

7.9. Operation security

ESS has implemented a mature system of system and security controls to ensure service quality and availability. In particular these controls are:

a) An analysis of security requirements is carried out at the design and requirements specification stage of any systems development project undertaken by the TSP or on behalf of the TSP to ensure that security is built into Information Technology's systems.

b) Change control procedures are applied for releases, modifications and emergency software fixes of any operational software.

c) The integrity of TSP systems and information is protected against viruses, malicious and unauthorized software. All systems are hardened in conformance to a hardening policy of ESS.

d) Media used within the TSP systems is securely handled to protect media from damage, theft, unauthorized access and obsolescence.

e) Media management procedures protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

f) Procedures are established and implemented for all trusted and administrative roles that have an impact on the provisioning of services.

g) The TSP has specified and applied procedures for ensuring security patches are applied within a reasonable time after they come available.

A security patch need not be applied if it would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch. The reason for not applying any security patches is documented.

7.10. Network security

The TSP protects its network and systems from attack.

In particular:

a) The TSP network is segmented into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services.
b) The TSP restricts access and communications between zones to those necessary for the operation of the TSP. Not needed connections and services are explicitly forbidden or deactivated. The established rule set is reviewed on a regular basis.
c) Any elements of the TSPs critical systems (e.g. Root CA systems, TSU) are kept in a secured zone.
d) A dedicated network for administration of IT systems that is separated from the operational network is established. Systems used for administration will not be used for non-administrative purposes.

e) Test platform and production platform are separated from other environments not concerned with live operations (e.g. development).
f) Communication between distinct trustworthy systems can only be established through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.
g) The external network connection to the internet is redundant to ensure availability of the services in case of a single failure.
h) The TSP performs a regular vulnerability scan on public and private IP addresses identified by the TSP and record evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.
i) The TSP performs a penetration test on the TSP's systems at set up and after infrastructure or application upgrades or modifications that the TSP determines are significant. The TSP records evidence that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

7.11. Incident management

Detailed explanation regarding this topic is described in the *security concept*: Chapter 17 “Vorgehensweise bei Vorkommnissen”.

System activities concerning access to IT systems, user of IT systems, and service requests are monitored.

In particular:

a) Monitoring activities take account the sensitivity of any information collected or analyzed.
b) Abnormal system activities that indicate a potential security violation, including intrusion into the TSP network, are detected and reported as alarms.
c) The TSP IT systems monitors the following events:
Start-up and shutdown of the logging functions;
Availability and utilization of needed services with the TSP network.
d) The TSP acts in a timely and coordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. The TSP appoints trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSP's procedures.
e) The TSP notifies the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein.
f) The national supervisory body is informed within 24h after discovery of a critical security breach via e-mail at: TSP-Incidents@bnetza.de

g) Audit logs are monitored or reviewed regularly to identify evidence of malicious activity.
h) The TSP will resolve critical vulnerabilities within a reasonable period after the discovery. If this is not possible, the TSP will create and implement a plan to mitigate the critical vulnerability or the TSP will document the factual basis for the TSP's determination that the vulnerability does not require remediation.
i) Incident reporting and response procedures are employed in such a way that damage from security incidents and malfunctions are minimized.

7.12. Collection of evidence

At the point in time when a security incident has been detected, it might be not obvious, if that security incident is subject of further investigations. Therefore, it is important, that any proof, status of IT system or information is securely saved before they become unusable or are destroyed.

The TSP records and keeps accessible for an appropriate period, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

In particular:

a) The confidentiality and integrity of current and archived records concerning operation of services is maintained.
b) Records concerning the operation of services are completely and confidentially archived in accordance with disclosed business practices.
c) Records concerning the operation of services are made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.
d) The precise time of significant TSP environmental, key management and clock synchronization events are recorded. The time used to record events as required in the audit log is synchronized with UTC continuously.
e) Records concerning services are held for a period after the expiration of the validity of the signing keys or any trust service token as appropriate for providing necessary legal evidence according to the present document.
f) The events are logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.

7.13. Business continuity management

All IT systems involved in the time-stamping service offer a minimum N+1 redundancy.

The time-stamping service itself is located in a physical secured environment that minimizes the risk of natural disasters (e.g. fire).

The private keys of the TSU are securely stored in a FIPS 140-2 Level 3 HSM, that also provides a N+1 redundancy.

In case the private keys do become compromised, the archive of saved timestamps helps to differentiate between correct and false timestamps in an audit trail.

The HSM in question would be isolated from the network immediately and corrective measures as follows would be taken:

- Notify CISO (role ITSB in the security concept) to coordinate all further action
- Start a security audit of the remaining HSMs holding further private keys (integrity checks, log file analysis)
- Notify relying parties that are concerned of the compromise
- Start the replace procedure in order to return to a N+1 redundancy

In case natural disasters (e.g. fire, earthquake, storm) happens that causes a loss of the facility, the time-stamping service would suspend its operation until it has been rebuild and reevaluated by an independent body in a new facility.

The loss of calibration or compromising of a TSU clock is covered in clause 7.7.1 of this document.

7.14. TSA termination and termination plans

In the event the TSA terminates its operations for any reason whatsoever, it will notify its national supervisory body prior to termination.

A timely notice will be provided for all relying parties in order to minimize any disruptions that are caused because of the termination of the services.

Further, in collaboration with the supervisory body the TSP will coordinate steps in order to ensure retention of all relevant archived records prior to termination of the service.

In addition, the following applies:

a) The TSP maintains an up-to-date termination plan.

b) Before the TSP terminates its services at least the following procedures apply:
    a. The TSP will inform the following of the termination: all subscribers and other entities with which the TSP has agreements or other form of established

relations, among which relying parties and TSP. In addition, this information will be made available to other relying parties;

b. TSP will terminate authorization of all subcontractors to act on behalf of the TSP in carrying out any functions relating to the process of issuing trust service tokens;
c. The TSP will transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period, unless it can be demonstrated that the TSP does not hold any such information;
d. The TSP private keys, including backup copies, will be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.
e. Where possible TSP tries to make arrangements to transfer provision of trust services for its existing customers to another TSP.
f. the TSP will revoke all of its certificates

c) The TSP has an arrangement to cover the costs to fulfil these minimum requirements in case the TSP becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.
d) The TSP will maintain or transfer to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period.

7.15. Compliance

The TSA ensures compliance with applicable law at all times.

Specifically, the TSA is compliant to:

a) Regulation (EU) N°910/2014
b) ETSI TS 119 421
c) IETF (RFC 3161)

Whenever possible, the TSP makes its services available to persons with disabilities.