TRUSTCENTER
a company of CHOSENSECURITY

TC TrustCenter GmbH
Time-Stamp Practice and Disclosure Statement

Version 1.0.2 of November 17, 2008

NOTE: The information contained in this document is the property of TC TrustCenter GmbH.

This document may not be copied, distributed, used, stored or transmitted in any form or by any means, whether in part or as a whole, without the prior written consent of TC TrustCenter GmbH.

TC TrustCenter
Time-Stamp Practice and Disclosure Statement

Version 1.0.2 of November 17, 2008

TC TrustCenter
Time-Stamp Practice and Disclosure Statement

Version 1.0.2 of November 17, 2008

1 Overview

TC TrustCenter issues Time Stamps in compliance with the ETSI standard ETSI TS 102023. This compliance is confirmed by an independent third party certification body thorough an ETSI certificate which can be downloaded from TC TrustCenter's website.

TC TrustCenter establishes the general rules concerning the operation of TC TrustCenter's Time-stamping Authority in its Time-Stamp Policy. This document, TC TrustCenter's Time-Stamp Practice Statement, in combination with TC TrustCenter's CPS defines how TC TrustCenter meets the technical, organizational, and procedural requirements identified in TC TrustCenter's Time-Stamp Policy.

TC TrustCenter's public documents (Certification Practice Statement, General Terms and Conditions, Time-Stamp Policy, and this Time-Stamp Practice and Disclosure Statement) may be found at TC TrustCenter's website (http://www.trustcenter.de).

TC TrustCenter is accredited by the German authorities as an issuer of qualified certificates and qualified time-stamps in conformance with the German Signature Act [GSA] and the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [EUDIR].

TC TrustCenter conducts regular risk assessments to evaluate threats and to determine the necessary security controls and operational procedures.

TC TrustCenter's Policies and Practices Board (PPB) consisting of TC TrustCenter's executives has the responsibility for maintaining and approving TC TrustCenter's policies and practices according to the terms of section 8 "Specific Administration" of TC TrustCenter's CPS [TC-CPS].

2 Identification

TC TrustCenter issues several types of time-stamps. Currently these are:

- Qualified time-stamps
- Advanced time-stamps
- Advanced time-stamps for Adobe Certified Document Services.

To distinguish between different time-stamps TC TrustCenter's Time-Stamp Policy specifies for each type of time-stamp a separate OID:

The object-identifier for support of qualified time-stamps is:

> iso(1) member-body(2) de(276) din-certco(0) trustcenter(44) Basis policies(1) time-stamp-policies(2) SigG(1).

The object-identifier for support of advanced time-stamps is:

> iso(1) member-body(2) de(276) din-certco(0) trustcenter(44) Basis policies(1) time-stamp-policies(2) Advanced(3).

The object-identifier for support for Adobe Systems Incorporated: CDS Certificate Policy is:

> OID=1.2.840.113583.1.2.1.

TC TrustCenter includes the appropriate OID in each time-stamp object issued.

3 TSA obligations

3.1 General

TC TrustCenter implements all requirements specified in its Time-Stamp Policy ([TC-TSP]).

TC TrustCenter ensures conformance with the procedures prescribed its Time-Stamp Policy.

All TSA functionality is undertaken by TC TrustCenter; long-term archival is undertaken by TC TrustCenter and, in addition, by a sub-contractor.

TC TrustCenter will adhere to any additional obligations indicated in time-stamps either directly or incorporated by reference.

3.2 TSA obligations towards subscribers and relying parties

TC TrustCenter provides permanent access to the time-stamping service except during maintenance intervals and except during periods where a reliable time source is not available or other events that do not lie in TC TrustCenter's sphere of influence (force majeure, war, strike, governmental restrictions, etc.).

Planned maintenance windows may be contractually agreed upon with subscribers; they may also be announced on TC TrustCenter's website.

TC TrustCenter implements and operates a reliable and trustworthy infrastructure for information exchange and communication. This is regularly verified by independent third party audits. These external audits include audits pursuant to the standards

- the German Signature Act,
- TC TrustCenter acting as a CSP for Identrust Level One Participants,
- MBA/SISAC (Secure Identity Services Accreditation Corporation, a subsidiary of the Mortgage Bankers Association of America),
- ETSI TS 101 456,
- ETSI TS 102 042, and
- ETSI TS 102 023.

ETSI TS 102 042 is in many cases accepted as an equivalent to the WebTrust™ program for Certification Authorities. ETSI TS 101 456 is a standard for compliance with European regulations for issuing qualified certificates and qualified time-stamps. ETSI TS 102 023 is recognized by many authorities and institutions. It defines policy requirements for time-stamping authorities

All of these audits require demonstration of a maximum level of security and conformity to documented policies and practices. The respective provisions supplement one another and serve to enhance the overall security controls, which are audited regularly by independent third parties.

TC TrustCenter respects the role of trademarks and intellectual property.

TC TrustCenter uses at least one independent external time source (two for qualified time-stamps) and at least one internal time source which are permanently compared to guarantee a deviation from German Legal Time of less than one second. At least one of the external time sources is the official German Legal Time provided by Physikalisch-Technische Bundesanstalt (http://www.ptb.de).

TC TrustCenter
Time-Stamp Practice and Disclosure Statement

Version 1.0.2 of November 17, 2008

TC TrustCenter provides subscribers and relying parties with the necessary information about the terms and conditions regarding the use of TC TrustCenter’s time-stamping service as specified in section 4: TSA Disclosure Statement.

4 TSA Disclosure Statement

TC TrustCenter’s Time-Stamping Authority Disclosure Statement (this section of this document) discloses to all subscribers and potential relying parties the terms and conditions regarding the use of TC TrustCenter’s time-stamping services.

4.1 Contact details

4.1.1 Specification administration organization

This Time-stamp Policy and Time-stamp Practice Statement is administered by TC TrustCenter’s Policies and Practices Board.

4.1.2 Contact person

Certification Practice Administrator
TC TrustCenter GmbH
Sonninstrasse 24-28
20097 Hamburg
Germany
Phone:+49 (0)40 808026-0
Fax: +49 (0)40 808026-126
E-Mail: certificate@trustcenter.de

4.1.3 Person determining Time-Stamp Policy and Time-Stamp Practice Statement suitability

TC TrustCenter’s Policies and Practices Board consisting of TC TrustCenter executives determines the suitability of this Time-Stamp Policy and Time-Stamp Practice Statement.

4.2 Time-Stamp Policy applied

TC TrustCenter’s Time-Stamp Policy can be found at http(s)://www.trustcenter.de/repository.

4.3 Hash algorithm for time-stamps

The cryptographic algorithms and key lengths used by TC TrustCenter’s TSA comply with ETSI TS 101.861, Time Stamping Profile. Currently TC TrustCenter’s TSA uses:

- Hash: SHA-1 or SHA-256

- Signature: sha1WithRSAEncryption or sha256WithRSAEncryption, 2048 bit key.

For qualified time-stamps SHA-256 will be used.

ETSI TS 101.861, V 1.2.1 has been published in the year 2002. It does not reflect recent developments and technical progress made since 2002. Meanwhile SHA-1 is no longer deemed suitable by the German authorities and issuers of qualified certificates and qualified time-stamps may no longer use SHA-1 in connection with qualified certificates and qualified time-stamps. TC TrustCenter upgraded to SHA-256 for the issuance of qualified time-stamps.

4.4 Life-time of time-stamps

The expected life-time of the qualified signatures used to sign qualified time-stamp tokens using the algorithms mentioned in section 4.3 is determined by the German authorities (http://www.bundesnetzagentur.de/enid/36c6764238b9744d2363b4cd60bca53c,0/Publications_and_Notifications/Suitable_Algorithms_z8.html). Currently the algorithms are declared to be suitable at least until end of 2014.

The expected life-time of advanced time-stamps is determined by the validity period of the certificate used for issuing time-stamps. Currently time-stamp certificates have a validity of at least 7 years.

TC TrustCenter offers the option to time-stamp issued time-stamps before the end of their life-time. The new time-stamp will use algorithms which are considered secure when the new time-stamp is issued such that the old time-stamp remains valid.

4.5 Accuracy of the time in the time-stamp tokens with respect to UTC

TC TrustCenter's TSA assures time with ±1 second of a trusted UTC time source and will not issue time-stamps outside this declared accuracy.

4.6 Limitations on the use of the time-stamping service

TC TrustCenter does not set reliance limits for time-stamp services beyond those outlined in the Time-Stamp Policy section 6.3 "Relying Party Obligations". TC TrustCenter as well as the German authorities (Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Federal Network Agency, http://www.bundesnetzagentur.de) will post public notice on their websites if it is determined that cryptographic algorithms and key lengths used in TC TrustCenter's time-stamps are no longer considered secure.

4.7 Subscriber and Relying Party obligations

The subscriber's obligations are defined in section 6.2 of the Time-Stamp Policy.

The relying party's obligations are defined in section 6.3 of the Time-Stamp Policy.

Section 6.3 also contains information on how to verify the time-stamp token such that the relying party may "reasonably rely" on the time-stamp token.

4.8 Retention period for event logs

Event logs for time-stamps will be archived as long as described in 7.12.

4.9 Applicable law

The applicable legal system is the law of the Federal Republic of Germany, expressly excluding international private law and the UN Treaty on International Sale of Goods.

4.10 Limitations of liability

TC TrustCenter will not be liable for matters that lie outside its sphere of influence and responsibility.

TC TrustCenter makes no express or implied representations or warranties relating to the availability or accuracy of TC TrustCenter's time-stamping service for advanced time-stamps.

TC TrustCenter will be liable only for damage to subscribers and relying parties in relationship to valid qualified digital certificates and valid qualified time-stamps relied upon in accordance with the German Signature Act. The liabilities for qualified time-stamps are specified in §11 of the German Signature Act.

4.11 Complaints and dispute settlement

It is in the interest of TC TrustCenter as a Time-Stamping Authority and trusted third party to resolve any dispute promptly and efficiently. Therefore, any party intending to make claims should contact TC TrustCenter first, regardless of the nature of the claim.

Dispute resolution procedures relating to disputes between TC TrustCenter and Customers are set for the in the agreements between the parties. Dispute resolution procedures relating to disputes between TC TrustCenter and Subscribers can be set forth in contractual agreements with Subscribers.

In any case of dispute, claim, or controversy in connection with or relating to this TS-PDS or any certificate or time-stamp issued by TC TrustCenter TC TrustCenter can be contacted by e-mail to dispute@trustcenter.de.

Disputes may also be reported to:

TC TrustCenter GmbH
CA Administration
Sonninstrasse 24-28
20097 Hamburg
Germany

5 Key management life cycle

5.1 TSA key generation

Any private key used for issuing time-stamps is generated on a hardware security module (HSM) evaluated as “E4 high” according to ITSEC criteria (or equivalent) e.g. a Smart Card, or using a FIPS 140-1 Level 3-compliant HSM, which is tested for proper operation before commencing the key generation procedure.

Private keys used for issuing qualified time-stamps are always generated on a smart card evaluated as “E4 high” according to ITSEC criteria (or equivalent) and confirmed to be compliant with the requirements identified in CEN Workshop Agreement 14167-2 [CEN]. Furthermore, these smart cards meet the requirements of the German Signature Act, which is confirmed by an independent third party and the relevant German supervisory authority for qualified signatures and qualified time-stamps (Federal Network Agency).

Key generation takes place in a physically secured environment by personnel in trusted roles under, at least, dual control. The personnel authorized to carry out this function is limited to those assigned to the specific roles under TC TrustCenter’s role concept.

At no point during the generation process does the private key leave the HSM in unencrypted form, and no unencrypted private key material leaks out.

5.2 TSU private key protection

TC TrustCenter keeps its private keys in Hardware Security Modules evaluated as “E4 high” according to ITSEC criteria (or equivalent) e.g. a Smart Card, or using a FIPS 140-1 Level 3-

compliant HSM. The computer system the HSMs are connected to are kept in a secure physical facility. Access to both the facility and the private keys is protected by access control mechanisms. The private keys can only be activated by two persons and are, once decrypted using the proper authorization, never written to any permanent or magnetic storage media.

The use of FIPS 140-1 Level 3 or ITSEC “E4 high” certified cryptographic modules prevents that private keys can be exported from the modules in clear.

No copy of any private key is kept on magnetic media in unencrypted form.

Private keys used for time-stamping are backed up, copied, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment. (see [TC-TSP] section 7.4.4). The personnel authorized to carry out this function is limited to those assigned to the specific roles under TC TrustCenter’s role concept.

Private keys for qualified time-stamps are generated and stored on smart cards compliant with “CEN Workshop Agreement 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations” and “E4 high” according to ITSEC criteria (or equivalent). These private keys can not be exported from the smart cards. Back-up, copying, external storage, and recovery does not apply to such smart cards.

5.3 TSU public key Distribution

TC TrustCenter’s time-stamping public key certificates are published on TC TrustCenter’s website.

This enables relying parties to verify the integrity and authenticity of time-stamp tokens issued by TC TrustCenter.

5.4 Rekeying TSU's Key

TC TrustCenter’s TSU's certificate will not be used beyond the period of time that the chosen algorithm and key length is recognized as being suitable fit for the chosen purpose.

5.4.1 End of TSU key life cycle

TC TrustCenter’s TSU private signing keys are not used beyond the end of their life cycle.

TC TrustCenter has operational and technical procedures in place to initiate a key-rollover before private keys expire.

The TSU private signing keys, or any key part, including any copies will be destroyed such that the private keys cannot be retrieved.

The time-stamp issuing system rejects any attempt to issue time-stamps if the signing private key has expired.

5.4.2 Life cycle management of cryptographic module used to sign time-stamps

Cryptographic hardware life-cycle controls are specified in TC TrustCenter’s CPS ([TC-CPS]) in section 6.6.

6 Time-stamping

6.1 Time-stamp token

Time-stamps issued by TC TrustCenter include the correct official German legal time and a unique identifier (serial number).

The time values used by the time-stamping unit are provided by Physikalisch-Technische Bundesanstalt (http://www.ptb.de).

The PTB is one of the official authorities (UTC(k)) responsible for time dissemination services (see http://www.bipm.org/en/scientific/tai/time_server.html).

Each time-stamp issued by TC TrustCenter includes the hash value of the data being time-stamped and is signed using a key generated exclusively for the purpose of time-stamping.

The certificate of the time-stamp unit used for signing time-stamps includes

- an identifier for the unit which issues the time-stamps,
- the name of the TSA, and
- an identifier for the country in which the TSA is established.

6.2 Clock Synchronization with UTC

TC TrustCenter's clocks are located in TC TrustCenter's high security area. This area is strictly access controlled. Therefore, the clocks are protected against unauthorized access and unauthorized manipulation.

For qualified time-stamps (OID 1.2.276.0.44.1.2.1) TC TrustCenter permanently compares this official time signal form the PTB to two other, independent time sources.

If these time sources differ more than the time period specified in section 4.5 TC TrustCenter's TSA will stop issuing time-stamps until all clocks are re-synchronized.

For advanced time-stamps (OID 1.2.276.0.44.1.2.3) and for time-stamps issued for Adobe Certified Document Signing (OID 1.2.840.113583.1.2.1) TC TrustCenter receives time information from the PTB and calibrates the system clock of the TSU-system accordingly.

The official German time provided by the PTB automatically contains information about the occurrence of leap seconds. TC TrustCenter's TSA systems automatically adjust their clocks and maintain clock synchronization when a leap second occurs. TC TrustCenter records the exact time (within the declared accuracy) when this change has occurred.

7 TSA management and operation

7.1 Availability

TC TrustCenter's time-stamping service is available on a 24x7 basis except during maintenance intervals and except during periods where a reliable time source is not available or other events that do not lie in TC TrustCenter's sphere of influence (force majeure, war, strike, governmental restrictions, etc.).
Planned maintenance windows will be contractually agreed upon with subscribers or they will be announced on TC TrustCenter's website.

7.2 Security management

TC TrustCenter retains responsibility for all aspects of the provision of time-stamping services within the scope of this time-stamp policy, whether or not functions are outsourced to subcontractors. If TC TrustCenter makes use of sub-contractors their responsibilities are clearly defined by TC TrustCenter in contractual agreements and appropriate arrangements are made to ensure that third parties are bound to implement any controls required by TC TrustCenter's TSA. TC TrustCenter is responsible for the disclosure of relevant practices of all parties.

TC TrustCenter's management provides direction on information security through its Policies and Practices Board (PPB) and its IT-Security management. Both of them are responsible for defining TC TrustCenter's information security policies. TC TrustCenter publishes and communicates relevant policies to all employees who are impacted by them.

TC TrustCenter maintains its information security infrastructure at all times. Any changes that have impact on the level of security provided must be approved by TC TrustCenter's management forum before the changes are implemented.

The security controls and operating procedures for TC TrustCenter 's TSA facilities, systems and information assets providing the time-stamping services are documented, implemented and maintained.

7.3 Asset classification and management

All of TC TrustCenter's assets receive an appropriate level of protection.

TC TrustCenter maintains an inventory of all assets and has assigned a classification for the protection requirements to the assets consistent with the risk analysis.

7.4 Personnel security

TC TrustCenter's personnel possess the expert knowledge, experience and qualifications necessary for the offered services and appropriate for the job function.

Security roles and responsibilities are specified in the TC TrustCenter's security policy and role concept. Trusted roles, on which the security of TC TrustCenter's TSA operation depends, are clearly identified in the above mentioned documents.

TC TrustCenter's role concept defines job descriptions including skills and experience requirements. The role concept enforces separation of duties and least privilege. Each position's sensitivity is based on the respective duties and access levels, background screening and employee training and awareness. Where appropriate, job descriptions differentiate between general functions and TSA specific functions.

The following additional controls shall be applied to time-stamping management:

All of TC TrustCenter's system administrators, system operators, and managerial personnel possess knowledge of time-stamping technology and digital signature technology. Furthermore, they possess knowledge about calibration or synchronization of TC TrustCenter's clocks.

TC TrustCenter's staff in managerial position is familiar with security procedures for personnel with security responsibilities and has practical experience with information security and risk assessment.

All TSA personnel in trusted roles is held free from conflict of interest that might prejudice the impartiality of the TSA operations.

Trusted roles include roles that involve the following responsibilities:

- Security Officers: Overall responsibility for administering the implementation of the security practices.
- System Administrators: Authorized to install, configure and maintain the TSA trustworthy systems for time-stamping management.
- System Operators: Responsible for operating the TSA trustworthy systems on a day-to-day basis. Authorized to perform system backup and recovery.
- System Auditors: Authorized to view archives and audit logs of the TSA trustworthy systems.

All of TC TrustCenter's personnel is formally appointed its roles by senior management responsible for security.

TC TrustCenter's TSA does not employ any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position. No employee has access to a trusted function until all necessary checks are completed.

7.5 Physical and environmental security

Physical and environmental security measures are specified in TC TrustCenter's CPS ([TC-CPS]), section 5.1.

7.6 Operations management

TC TrustCenter's TSA system components are secure and correctly operated, with minimal risk of failure.

TSA system components are protected against viruses, malicious, and unauthorized software.

Media handling and security

All media is handled securely in accordance with requirements of the information classification scheme (see [TC-TSP], section 7.4.2). Media containing sensitive data will be securely erased or physically destroyed when no longer required.

System Planning

Capacity demands are monitored and projections of future capacity requirements are made to ensure that adequate processing power and storage are available.

Incident reporting and response

TC TrustCenter has incident reporting and response procedures in place that minimize damage from security incidents and malfunctions.

All incidents are reported as soon as possible after the incident.

Operations procedures and responsibilities

The operation of TC TrustCenter's time-stamping service is independent from the operation of other services provided by TC TrustCenter.

Nevertheless, the security operations' responsibilities

- operational procedures and responsibilities;
- secure systems planning and acceptance;

- protection from malicious software;
- housekeeping;
- network management;
- active monitoring of audit journals, event analysis and follow-up;
- media handling and security;
- data and software exchange

apply to all of TC TrustCenter's operations and are regularly audited by independent third parties to prove compliance with various standards (compare [TC-TSP], section 5.4 "Conformance").

7.7 System Access Management

TC TrustCenter maintains appropriate physical and logical access controls for all affected facilities, hardware, systems, and information.

This includes:

- appropriate firewalls to protect TC TrustCenter's internal networks from unauthorized access including access by subscribers and third parties,
- appropriate user administration to maintain system security, including user account management, auditing, and timely modification or removal of access,
- appropriate restriction of access to information and application system functions in accordance with the access control policy and in accordance with the requirements of separation of trusted roles,
- appropriate identification and authentication of TSA personnel before granting access to critical applications related to time-stamping,
- appropriate accounting of all activities, for example by retaining event logs.

In addition, local network components (e.g. routers, switches) are kept in a physically secure environment and their configurations are periodically audited for compliance with the standards mentioned in section 7.6.

TC TrustCenter maintains continuous monitoring and alarm facilities to detect, register, and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

7.8 Trustworthy Systems Deployment and Maintenance

TC TrustCenter's TSA uses trustworthy systems and products that are protected against modification.

The application software of TC TrustCenter's TSA systems has been developed based on an analysis of security requirements by the TC TrustCenter's TSA to ensure that necessary security is built into systems.

Change control procedures exist and are followed for releases, modifications, and emergency software fixes of any operational software.

Keys and certificates for the time-stamping service are generated in accordance with section 5.1.

7.9 Compromise of TSA Services

In the event of compromise of a TSU private key, TC TrustCenter will follow the procedures outlined in section 5.7 Compromise and Disaster Recovery of TC TrustCenter's CPS. This includes revoking the certificate and adding it to the relevant CRL. The TSU will not issue time-stamps if its private key is not valid.

TC TrustCenter will not issue time-stamps if its clock is outside the declared accuracy from the official German time, until steps are taken to re-synchronize and/or re-calibrate the clocks.

In the case of a compromise, or suspected compromise, or loss of correct time TC TrustCenter will make available to all subscribers and relying parties a description of the compromise that occurred.

In case of compromise of the TSA's operation or loss of correct time, wherever possible, TC TrustCenter will make available to all subscribers and relying parties information which may be used to identify the time-stamps which may have been affected, unless this publication breaches the privacy of the TSAs users or the security of the TSA services.

7.10 TSA termination

TC TrustCenter's TSA can only be terminated by the Board of Directors of the TC TrustCenter. TC TrustCenter will inform subscribers about TSA termination. Subscribers will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought.

TC TrustCenter will make a reasonable effort to archive the records of the TSA and transfer them to a specified custodian, and to establish an acceptable procedure for subscribers and relying parties for switching to a different provider of time-stamping services, in order to minimize the effects of TC TrustCenter ceasing to provide these services by itself.

TC TrustCenter will make a reasonable effort to transfer to a reliable party its obligations to make available its public TSA keys and its TSA certificates and to continue maintenance of information required to verify the correctness of time-stamp tokens.
In case of termination TC TrustCenter will revoke its TSU certificates and destroy its private TSA keys (including backup copies) in a manner such that the private keys cannot be retrieved.

To cover all financial expenses in case of termination TC TrustCenter has made appropriate provisions in form of a Letter of Comfort (a special kind of a letter of credit). It is the intention of such a letter that TC TrustCenter's mother company guarantees that it will be responsible for the debts or duties set out in the letter.

7.11 Compliance with Legal Requirements

a. TC TrustCenter's complies with applicable legal requirements e.g. with the requirements of the European data protection Directive [EU-PROT] and with the requirements of German data protection laws.

7.12 Recording of information concerning operation of time-stamping service

TC TrustCenter maintains records of all relevant information concerning the operation of its TSA for a period of at least 5 years after the expiration of the validity of the TSU's signing keys. Records are time-stamped to protect data integrity and moved to a protected site for storage and subsequent archiving.

TC TrustCenter's TSA maintains records, including precise time, of:

- time-stamp requests and created time-stamps
- events related to TSA administration (including certificate management, key management, and clock synchronisation).

Records are treated as confidential. Records are automatically written on WORM-media, such that they cannot be easily deleted or destroyed within the period of time that they are required to be held.

Records concerning the operation of time-stamping services are made available if required for the purposes of providing evidence of the correct operation of the time-stamping services for the purpose of legal proceedings.

Any information recorded about subscribers is be kept confidential except as where agreement is obtained from the subscriber for its wider publication.

Furthermore, TC TrustCenter logs

- records concerning all events relating to the life-cycle of TSU keys,
- records concerning all events relating to the life-cycle of TSU certificates,
- records concerning events relating to synchronization of clocks. (This includes information concerning normal synchronization of clocks used in time-stamping.)
- records concerning events relating to detection of loss of synchronization.

8 Organizational

TC TrustCenter implements and operates a reliable and trustworthy infrastructure for information exchange and communication. This is regularly verified by independent third party audits. These external audits include audits pursuant to the following standards:

- the German Signature Act,
- TC TrustCenter acting as a CSP for Identrust Level One Participants,
- MBA/SISAC (Secure Identity Services Accreditation Corporation, a subsidiary of the Mortgage Bankers Association of America),
- ETSI TS 101 456,
- ETSI TS 102 042, and
- ETSI TS 102 023.

All these audits require demonstration of a maximum level of security and conformity to documented policies and practices. The respective provisions supplement one another and serve to enhance the overall security controls, which are audited regularly by independent third parties.

9 References

[CEN] CEN Workshop Agreement 14167-2: "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)".

[ETSI] ETSI TS 102 023, V1.2.1 (2003-01), Policy Requirements for time-stamping authorities

[ETSI-TS] ETSI TS 101.861, V1.2.1 (2002-03), Time Stamping Profile

[EU-DIR] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

EU-PROT Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[FIPS] FIPS PUB 140-1 (1994): "Security Requirements for Cryptographic Modules".

[GSA] Law Governing Framework Conditions for Electronic Signatures of 16 May 2001 (Federal Law Gazette I, p. 876), last amended by Art. 1 of the
First Act Amending the Signature Law (First Signature Amendment Act - 1. SigÄndG) of 4 January 2005 (Federal Law Gazette I, p. 2)
(http://www.bundesnetzagentur.de/media/archive/3612.pdf)

[GDSO] Ordinance on electronic Signatures (Signaturverordnung, SigV)
http://www.bundesnetzagentur.de/media/archive/3613.pdf

[ISO] ISO/IEC 15408 (1999) (parts 1 to 3): "Information technology - Security techniques - Evaluation
criteria for IT security".

[TC-CPS] TC TrustCenter GmbH, Certification Practice Statement
Version 1.6, July 5, 2007
http://www.trustcenter.de/cps

[TC-TSP] TC TrustCenter GmbH, Time-Stamp Policy
Version 1.1, January 21, 2008
http://www.trustcenter.de/repository