



xyzmo Timestamping Authority Practice Statement

v1.0

Content

- 1 Document History 3
 - 1.1 v1.0 3
- 2 Overview 4
 - 2.1 xyzmo Software GmbH 4
- 3 Time Stamping Authority (TSA) 5
 - 3.1 Time Synchronization 5
 - 3.2 Verification and Validity of a Timestamp..... 5
- 4 Certificates 6
 - 4.1 xyzmo Timestamp Root CA 2007..... 6
 - 4.2 Timestamp Signing Certificates 6
 - 4.2.1 xyzmo Timestamping Service 5 R 6
 - 4.2.2 xyzmo Timestamping Service 4 R 6
 - 4.2.3 xyzmo Timestamping Service 3 6
 - 4.2.4 xyzmo Timestamping Service 2 7
- 5 Liability Limitations 8
- 6 Key Management 9
 - 6.1 Keys and Certificates 9
 - 6.2 Algorithms 9
 - 6.3 Storage, Backup and Recovery of Private Keys 9
 - 6.4 Publication of the Public Keys 9
 - 6.5 Use of the Keys 9
 - 6.6 Changing the Keys 9
 - 6.7 End of the Life Cycle for a Key Pair 10
 - 6.8 Life Cycle of the TSA 10
- 7 Physical, Organizational and Personnel Security Measures 11
 - 7.1 Security Management 11
 - 7.2 Personal Security 11
 - 7.3 Physical Security 12
 - 7.4 Organizational Security Measures 13
 - 7.5 Access Authorization and Protection from Unauthorized Access 13
 - 7.6 Trustworthy Systems 13
 - 7.7 Compromise 14
 - 7.8 Cessation of Operation 14
 - 7.9 Conformity with Legal Requirements 14
 - 7.10 Documentation and Archiving 15
 - 7.11 Organizational 15
 - 7.12 Administration of this Policy 16



1 Document History

1.1 v1.0

- This is the first version of this document and valid from 2009-08-01.

2 Overview

This document describes the policy the xyzmo Time-Stamping Authority (further referred as "TSA") is operated with. This includes operational security, maximum time deviation, availability and the timestamp signing certificates.

With this TSA and a appropriate signing software any electronic document or file can be equipped with a timestamp (refer to http://en.wikipedia.org/wiki/Trusted_timestamping). For the creation of a timestamp a hash value of the document is sent to the TSA. The user (requester) of a timestamp is solely responsible for the content of the document itself. The xyzmo Software GmbH as operator of the TSA only warrants for the validity and accuracy of the time in the timestamp according to this policy.

This service is provided by xyzmo Software GmbH completely voluntarily and free of charge; it may be modified or cancelled at any time. The user acquires no title or right regarding this service in connection with his license.

2.1 xyzmo Software GmbH

The xyzmo Software GmbH (further referred as "xyzmo") is a private company based in Ansfelden, Austria with international offices in the United States and Germany. xyzmo is an internationally leading supplier of comprehensive electronic signature solutions for the safeguarding and optimization of business processes. Originating from an almost 100-years tradition in stamps and signature signing, we possess the competency to carry these processes over to the digital world in a user-friendly manner.

xyzmo Software GmbH

FN 250152 x / ATU58043726

Haiderstraße 23

4052 Ansfelden, Austria

Phone: +43 (0) 7229 88060-0

Fax: +43 (0) 7229 88060-720

Email: office@xyzmo.com

Managing Director: DI Dr. Gerald Cäsar MBA

3 Time Stamping Authority (TSA)

The time specified in the timestamp is synchronized by xyzmo with Universal Time Coordinated (UTC), with a deviation of a maximum of 1 minute.

If xyzmo ascertains that the internal clock of a TSA deviates from UTC by more than 1 minute, or if synchronization with the time servers used takes so long that accuracy within 1 minute cannot be warranted, then no timestamp will be generated by this TSA until the fault has been remedied.

Each timestamp is signed by a TSA with a key, which is used exclusively for timestamping. It does correspond to the format specified in RFC 3161.

3.1 Time Synchronization

xyzmo ensures that the internal clock of the TSA deviates by no more than 1 minute from Universal Time Coordinated (UTC). When the hardware for the TSA is selected, it is made sure that it has an internal clock which does not deviate by more than one second per day.

The TSA is coordinated with the Simple Network Time Protocol (SNTP) and time servers available on the Internet. The verification mechanisms provided in NTP are used to ensure the accuracy of the time. When selecting the time server, which xyzmo uses to synchronize the clock of the TSA, it is ascertained that the time for each time server is derived directly or indirectly from at least one of the UTC laboratories of the Bureau International des Poids et Mesures (BIPM).

3.2 Verification and Validity of a Timestamp

The timestamps are issued according to the standard RFC 3161.

The verification software has to go back in time to check if the timestamping certificate of a certain timestamp was valid at the time when the timestamp was issued.

The timestamp certificates validity itself is given when the whole certificate chain was valid at the time of issuing the certificate. Validity checks have to be performed via CRL (see chapter Certificates).

4 Certificates

The following chapter lists the certificates which are in used for signing timestamps.

4.1 xyzmo Timestamp Root CA 2007

This is the certificate of the xyzmo Root CA which issued the timestamp service certificates.

- **DN:** CN = xyzmo Timestamp Root CA 2007, O = xyzmo Software GmbH, C = AT
- **Validity:** 12.1.2007 – 12.1.2022
- **Thumbprint:** 64 14 fb 12 0d 30 a4 6e b2 e1 1f 5a 75 f8 bc ef 25 19 06 80
- **CRL:** http://crl.xyzmo.com/xyzmo_timestamp_root_ca_2007.crl

4.2 Timestamp Signing Certificates

4.2.1 xyzmo Timestamping Service 5 R

- **DN:** CN=xyzmo Timestamping Service 5 R, O=xyzmo Software GmbH, C=AT
- **Validity:** 16.7.2009 - 16.7.2019
- **Key Size:** 2048 bit
- **Hash Algorithm:** SHA1
- **Thumbprint:** 70 3a 23 81 cd 77 df 7b 56 83 a2 82 9e 1b 2c 22 41 55 53 f1
- **Note:** This timestamp certificate is used to issue RFC3161 conformant timestamps only.

4.2.2 xyzmo Timestamping Service 4 R

- **DN:** CN=xyzmo Timestamping Service 4 R, O=xyzmo Software GmbH, C=AT
- **Validity:** 16.7.2009 - 16.7.2019
- **Key Size:** 2048 bit
- **Hash Algorithm:** SHA1
- **Thumbprint:** f1 c3 fe fa 6c cd 10 e8 0e 9d 69 4c 35 4d ba ed f1 7d 4d bf

4.2.3 xyzmo Timestamping Service 3

- **DN:** CN = xyzmo Timestamping Service 3, O = xyzmo Software GmbH, C = AT
- **Validity:** 6.11.2008 – 6.11.2018
- **Key Size:** 2048 bit
- **Hash Algorithm:** SHA1
- **Thumbprint:** d8 cc 40 01 38 ec 80 91 40 6a 6a a8 bd 55 d9 4d 17 ed 38 0d

4.2.4 xyzmo Timestamping Service 2

- **DN:** CN = xyzmo Timestamping Service 2, O = xyzmo Software GmbH, C = AT
- **Validity:** 18.1.2007 - 18.1.2017
- **Key Size:** 2048 bit
- **Hash Algorithm:** SHA1
- **Thumbprint:** 30 84 d9 a0 b4 c5 aa 80 32 3f 1b fe a0 0d f3 88 66 57 91 ac



5 Liability Limitations

xyzmo only warrants for the validity and accuracy of the time in the timestamp according to this policy. It does not know the content of a particular document but only the hash value of it. The requester of the timestamp is responsible for the document's content.

As this service is provided completely voluntarily and free of charge, xyzmo, as far as legally permissible, does not assume any warranty or any liability for any damages caused by the use of this service.

6 Key Management

6.1 Keys and Certificates

The keys and certificates used by the TSA to create signatures for timestamps are generated in a controlled and physically secured environment. Two people must be present for the generation of the keys in order to comply with the 'four-eyes principle'. These people have been entrusted by the management of xyzmo with the task of "security officer". Only a limited number of trustworthy and technically competent personnel are entrusted with these tasks.

The private keys used on the TSA are protected from unauthorized access by appropriate, state-of-the-art security measures. A hardware security module is not used at present.

6.2 Algorithms

RSA is used as the algorithm with a key length of at least 2048 bit.

The following hash algorithms are accepted: SHA1, SHA256, SHA384, SHA512, RipeMD160

6.3 Storage, Backup and Recovery of Private Keys

The private keys are stored in an encrypted format and are protected from unauthorized access by appropriate, state-of-the-art security measures. A hardware security module is not used at present.

In compliance with the 'four-eyes principle' two people, who are entrusted by the management of xyzmo with the tasks of a "security officer" ensure that two backups of the private keys are created, which are saved on CD/DVD and stored in a sealed envelope. A backup is locked in a safe on xyzmo's premises, which can only be opened by a member of management accompanied by two security officers. The other backup copy is deposited with a notary and it can only be accessed by a member of management accompanied by two security officers.

6.4 Publication of the Public Keys

X.509 certificates are issued for the public key of every TSA, whereby xyzmo either issues a self-signed certificate or issues a server certificate for another certification provider. The certificates of the individual TSAs are published in this document.

6.5 Use of the Keys

xyzmo's cryptographic keys, which are described in this chapter, are used exclusively for the TSA service in the manner described. The keys are used exclusively in a secured environment.

6.6 Changing the Keys

The keys used for the TSA can be changed at any time. In any case, xyzmo will change the keys if the algorithm used or the key length used are no longer deemed as sufficiently secure

according to Austrian law in the sense of § 3 (2) of the Signature Ordinance and/or its appendix.

6.7 End of the Life Cycle for a Key Pair

xyzmo ensures that private keys are no longer used after the end of their life cycle. If the certificate of a TSA expires, or if a key pair needs to be changed then a new key pair is generated and the TSA is configured to use this key pair.

6.8 Life Cycle of the TSA

A TSA is operated under xyzmo's control for the entire duration of its lifespan. The server is protected from unauthorized access by appropriate, state-of-the-art measures. The key pairs are generated with adherence to the 'four-eyes principle'. If a TSA or hardware component (hard disk in particular) is decommissioned, then it is ensured that it does not contain any keys.

7 Physical, Organizational and Personnel Security Measures

7.1 Security Management

xyzmo ensures that the security management system complies with state-of-the-art technology.

xyzmo bears the ultimate responsibility for time stamp service in accordance with this policy, immaterial whether individual activities are outsourced to service providers. The responsibility of service providers used is clearly defined by xyzmo and it is ensured that the service providers implement all of the measures demanded by xyzmo through appropriate contractual obligations.

The responsibility for the security management system is incumbent on a security team arranged within xyzmo, which is made up of the management of xyzmo and two other people, who have been entrusted with the role of a "security officer". The security team's decisions regarding questions of security management and any changes of the security specifications are communicated to all employees of xyzmo or the service providers used.

Security measures and operating regulations concerning the timestamp service are documented, implemented and maintained by the security team.

7.2 Personal Security

The person involved with the TSA - regardless of whether they are employed by xyzmo or other companies, and regardless of whether they are concerned with the service on a long-term basis or for individual tasks on short notice - must have the specialized knowledge that is necessary for the respective tasks as well as the necessary experience.

The following roles are defined for the security-relevant tasks. The roles are assigned by management to the respective person and documented in the job description. The decisions made by the management concerning security management are to be taken into account for the realization of the assigned tasks.

Persons in prominent positions must have sufficient knowledge of the technology used for the electronic signature and time stamp, time synchronization, IT security and risk analysis. Technical personnel must have sufficient expertise in the areas specified in §10 (5) SigV (general EDP training, security technology, cryptography, electronic signatures, PKI, technical standards, hardware and software).

The following are defined as roles in the sense of this chapter:

Management

The overall responsibility for the entire security management concept is incumbent on the management of xyzmo. The management ensures that decisions concerning security management are communicated to all employees of xyzmo or appointed service providers. The management assigns employees with the roles described in this chapter.

Security officer

Comprehensive responsibility for the conversion of this policy is bestowed upon a person who has been entrusted with this role. Security officers are particularly entrusted with tasks concerning the cryptographic key used by the TSA.

System administrator

A person, who has been assigned this role, is authorized to install, configure, create and maintain running backups of trustworthy systems or to supervise any maintenance work that is conducted by a third party. A four-eyes principle is not designated. The system administrators have access to the trustworthy systems and know the administrator passwords for these servers.

Computer centre personnel

Employees of the appointed computer centre are responsible for the particular activities regarding ongoing support of the trustworthy systems, in particular the provision of the uninterruptible power supply and the network connection. The computer centre employees do not know the administrator passwords. A four-eyes principle is not designated. The roles are not assigned by the management of xyzmo, but by the appointed computer centre, which must ensure the necessary reliability and expertise.

Any person appointed one of the aforementioned roles should not be involved in any conflict of interest that affects their impartiality.

The following incompatibilities exist between the individual roles

Employees assigned the role of "computer centre personnel" and/or "registration office personnel" are supervised by the roles commanded by the "security officer", "system administrator" and/or the "registration office representative" and therefore cannot be entrusted with one of these roles at the same time. There is no incompatibility between the roles of "management", "security officer" and "system administrator". For some tasks conducted by the "security officer" a four-eyes principle is assumed, especially in connection with cryptographic keys, for other tasks it is not.

7.3 Physical Security

The following facilities are protected by physical security measures: The trustworthy systems are located in a locked rack in an appointed computer centre.

In addition, the business premises of xyzmo and the registration offices, as well as areas in which backups of the cryptographic keys are kept are protected.

Access to the appointed computer centre is monitored and recorded by computer centre personnel. The locked rack, in which the trustworthy systems are located, can only be opened by the system administrators. Other personnel (e.g. maintenance personnel) only have access when accompanied and supervised by a system administrator. The computer centre has a 24x7x365 access control system, extinguishing gas systems, fail-safe power supply with UPS and backup generators, redundant climatic control and cooling systems and redundant GBit Internet connections with several carriers.

Only personnel employed by xyzmo and its appointed service providers have access to the office premises. Any other person, who is not in an area expressly designated for visitors, must be appropriately supervised by xyzmo's and/or its appointed service provider's personnel.

The safes, in which backups of the cryptographic keys are stored, are located in areas that are only accessible to authorized personnel.

7.4 Organizational Security Measures

All of xyzmo's systems, particularly the trustworthy systems and computers used for software development, are protected from unauthorized access as well as against viruses and other harmful software. All security-relevant incidents and malfunctions are to be notified to a security officer immediately if no special measures have been specified for the incident.

All data carriers, which are used in connection with TSA, are protected against damage, theft and unauthorized access. Any data carriers that are no longer needed are destroyed in a secure manner.

7.5 Access Authorization and Protection from Unauthorized Access

xyzmo ensures that only authorized personnel have access to the systems that are used for TSA.

The trustworthy systems and the internal network in the business premises of xyzmo are protected from unauthorized access by firewalls (including unauthorized access by customers, registration offices and other service providers).

The firewalls are configured in such a way that all protocols and access possibilities, which are not essential for xyzmo's operations, are blocked.

The software requesting a timestamp from a TSA has to authenticate via HTTP authentication to get access. This is also done for accounting reasons.

A security officer oversees the allocation of access authorization to the trustworthy systems particularly with regard to the access authorisation afforded to the system administrators, and ensures that access authorization is detracted and/or the password changed if a person is removed from his/her role.

It is necessary for all relevant personnel to be appropriately authenticated for admission and access to all trustworthy systems.

The member of personnel is responsible for his/her own activities. For security-relevant events protocols are kept.

7.6 Trustworthy Systems

The following systems are regarded as particularly worthy of protection: the computers, on which the server software for TSA is operated (TSA), the corresponding firewall computers and network components (routers, switches).

The trustworthy systems are located in a computer centre and protected from unauthorized access by a lockable rack. Furthermore, the systems are protected by organizational measures and a limited allocation of access authorization. Only the system administrators have admission and access authorization to the trustworthy systems (particularly with regard to knowledge of the administrator passwords).

The installation of new versions of the software, changes to configuration and the installation of patches are logged.

7.7 Compromise

The following are regarded as incidents of the security of TSA being compromised: the loss of control of the private key for a TSA or the suspicion that such a key can, or could be, used abusively by unauthorized persons, together with the suspicion that the clock of a TSA deviates by more than 1 minute of the actual time, resulting in inaccurate time stamps being generated.

In the event of a compromise xyzmo will verify to what extent the damage can be limited and determine the signatures that are affected, and it will issue an appropriate publication and/or communication regarding the security problem to inform the confidants in the security of TSA, the customers and/or signatories and other contracting parties concerned. Furthermore, the affected TSA will be switched off in the event of a compromise and it will not generate any new timestamps until the problem has been remedied.

7.8 Cessation of Operation

xyzmo reserves the right to discontinue the operation of TSA. The cessation of operation means that from this time onwards no new timestamps can be generated. The TSA signing certificates will be revoked.

All signatories that hold contracts with xyzmo will be informed via e-mail of the circumstances of cessation before operation stops. Further information will be available on the website at <http://www.xyzmo.com>.

All private keys and any backups shall be destroyed as soon as they are no longer needed. This will ensure that the private keys cannot be regenerated at any time.

A revocation of the key certificates for the TSA in the form of a revocation list is published on http://crl.xyzmo.com/xyzmo_timestamp_root_ca_2007.crl

7.9 Conformity with Legal Requirements

The TSA service is operated in conformity with the requirements of Austrian law. It does not provide qualified timestamps according to § 10 SigG.

No personal data of customers is processed in connection with TSA.

If the TSA is not used in conjunction with a xyzmo software product but with a 3rd party software the personal data of the customer is required for accounting purposes.

7.10 Documentation and Archiving

xyzmo archives information regarding security-relevant events (e.g. the lifecycle of the cryptographic keys used and the certificates issued for these keys, important configuration alterations made to the TSA and malfunctions) for a period of at least seven years after cessation of the TSA service. If this information relates to particular TSA, it will be kept for at least seven years after the server has been decommissioned.

The authenticity of a timestamp generated by TSA can be verified by every RFC3161 compatible software such as Acrobat Reader.

Time data is used in the supported protocols that are generated, whose accuracy corresponds to the accuracy of the time stamp service specified. If protocols have not been generated by a TSA, then the clock of the respective server is synchronized with a TSA or a comparable accurate time source.

The supported protocols that are generated and the electronically archived data are stored in such a way that they cannot be altered or destroyed easily.

The following are supported protocols that are generated by xyzmo:

- Protocols for every individual TSA that is generated with, among other things, information regarding the account, the hash value of the document and the time.
- Log files for the time synchronization of the TSA, particularly regarding losses during the synchronization process.

The following documents are archived by xyzmo in paper or electronic format:

- Protocols for security-relevant incidents, especially for the lifecycle of the cryptographic keys used for the TSA and the certificates issued, for the configuration of the trustworthy systems and for configuration alterations, for system malfunctions and failures and particularly for malfunctions of the time synchronization process.
- Contracts held with registration offices, the computer centre and other service providers, documents concerning xyzmo's employees (personnel records).

7.11 Organizational

xyzmo ensures the trustworthiness of xyzmo and TSA via the following measures: Policies, security concepts and organizational measures for TSA are non-discriminatory. The TSA service is at the disposal of all customers who commit themselves to the license conditions.

xyzmo Software GmbH is an incorporated enterprise in accordance with Austrian law.

xyzmo employs sufficient personnel who have the appropriate education, training, technical knowledge and experience to operate TSA in accordance with this policy.

If any activities are outsourced by xyzmo to service providers, this will be regulated by properly documented contracts.

7.12 Administration of this Policy

The security team within xyzmo has the task of verifying this policy on a continual basis, to decide whether any alterations or amendments are necessary, as well as advising on possible improvements and their effects on security. Any alterations to this policy shall be decided by the security team.

An alteration of the version number and date of the document is connected with each alteration of this policy. The time each alteration came into effect is also specified. The substantial changes made are specified in the version history at the beginning of the document.

The different versions of this policy are published on the website at <http://www.xyzmo.com> which also specifies which version was used at what time.