GlobalSign

Timestamping Practice Statement

Date: March 24, 2025

Version: v1.1

Table of Contents

Document History

Version	Release Date	Status & Description
V1.0	February 10, 2022	Initial release
V1.1	March 24, 2025	Removed references to UK eIDAS Included references to Regulation (EU) 2024/1183 (European Digital Identity Framework) Updates to timestamp policy identifiers Updates for ETSI EN 319 421 Updates for CA/B Forum ballot CSC-26

Acknowledgments

1.0 Introduction

1.1 Overview

This Timestamping Practice Statement ("TPS") applies to the services for issuing Timestamps of GlobalSign NV/SA and affiliated entities ("GlobalSign").

Timestamps can be used in support of digital signatures or for any application that requires proof that a signature was created before a particular time.

This document states only additional timestamping specific practices; in particular, the facility, management and operational controls, security measures, processes and procedures which have been implemented to satisfy the following requirements, where applicable:

- eIDAS regulation
- CA/Browser Forum Network and Certificate System Security Requirements
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates

The English version of this practice statement is the primary version. In the event of any conflict or inconsistency between the English practice statement and any localized or translated version, the provisions of the English version shall prevail.

1.2 About this document

The structure and contents of this document are based on ETSI EN 319 421 (Policy and Security Requirements for Trust Service Providers issuing Electronic Timestamps) [5].

1.3 Scope

This document specifies the policies and practices related to the operation and management of Timestamps and further extends the applicable practices of the GlobalSign CPS.

2.0 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] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"

[4] ETSI EN 319 411-2: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

[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); Timestamping protocol and timestamp token profiles."

[7] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules."

[8] IETF RFC3161

[9] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates

[10] CA/Browser Forum Network Security Guidelines

[11] FIPS PUB 140-3 (2019): "Security Requirements for Cryptographic Modules".

3.0 Definitions and abbreviations

3.1 Definitions

Authenticode: A Microsoft codesigning technology that identifies the publisher of Authenticode-signed software

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

CPS: GlobalSign's Certification Practice Statement available at http://www.globalsign.com/repository/ (as updated from time to time).

eIDAS regulation ("eIDAS"): REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, amended by Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework.

GNSS: Global Navigation Satellite System

NTP: Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable latency data networks.

Qualified Timestamp: an electronic timestamp which meets the requirements of the eIDAS regulation.

Qualified Timestamping Service: Timestamping Service issuing qualified electronic Timestamp tokens as per the eIDAS regulation.

Relying Party: recipient of a Timestamp token who relies on that Timestamp token.

Subscriber: legal or natural person to whom a Timestamp is issued and who is bound to any subscriber obligations

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

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

Timestamping Authority (TSA): TSP providing timestamping services using one or more timestamping units

Timestamping Unit (TSU): set of hardware and software which is managed as a unit and has a single Timestamp 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 Practice Statement: statement of the practices that a TSA employs in issuing Timestamps

TSA system: composition of IT products and components organized to support the provision of timestamping services

See GlobalSign CPS for additional definitions.

3.2 Abbreviations

For the purposes of this document, the abbreviations given in ETSI EN 319 401 [3] and the following apply:

BIPM	Bureau International des Poids et Mesures
CA	Certification Authority
IT	Information Technology
TSA	Timestamping Authority
TSP	Trust Service Provider
TSU	Timestamping Unit
UTC	Coordinated Universal Time

See GlobalSign CPS for additional abbreviations.

4.0 General Concepts

4.1 General Policy Requirements

This document references ETSI EN 319 401 [3] for generic policy requirements.

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

Subscribers and Relying Parties are expected to consult this practice statement to obtain further details of precisely how this Timestamp policy is implemented by the particular TSA (e.g. protocols used in providing this service).

4.2 Timestamping Services

The provision of timestamping services is broken down into the following component services for the purposes of classifying requirements:

- Timestamping provision: This service component generates Timestamps.
- Timestamping management: This service component monitors and controls the operation of the timestamping 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 timestamping provision service. This subdivision of services is only for the purposes of clarifying the requirements specified in this document and places no restrictions on any subdivision of an implementation of timestamping services.

4.3 Timestamping Authority (TSA)

A Trust Service Provider (TSP) providing timestamping services to the public, is called a Timestamping Authority (TSA).

GlobalSign has overall responsibility for the provision of the timestamping services identified in section 4.2. GlobalSign has responsibility for the operation of one or more TSUs which create and sign Timestamps on behalf of a GlobalSign TSA.

GlobalSign may make use of other parties to provide parts of the timestamping services. However, GlobalSign always maintains overall responsibility and ensures that the policy requirements identified in this document are met. GlobalSign may operate several identifiable timestamping units.

GlobalSign is a Trust Service Provider as described in ETSI EN 319 401 [3] which issues both digital certificates and Timestamps.

4.4 Subscriber

A Subscriber, as used herein, refers to both the subject of the certificate issued by GlobalSign and the entity that is contracted with GlobalSign for the use of the Timestamping Service.

4.5 Timestamp Policy and TSA Practice Statement

This section explains the relative roles of Timestamp policy and TSA practice statement.

A Timestamp policy is a form of trust service policy as specified in ETSI EN 319 401 [3] applicable to Trust Service Providers issuing Timestamps.

The GlobalSign Timestamping Practice Statement is a form of Trust Service Practice Statement as specified in ETSI EN 319 401 [3] applicable to Trust Service Providers issuing Timestamps.

This document specifies the Timestamp policy and the practice statement for the GlobalSign Timestamping Authority.

5.0 Timestamp Policies

5.1 General

This policy defines a set of rules adhered to by GlobalSign when issuing Timestamps, supported by public key certificates, with an accuracy of one (1) second or better against UTC.

5.2 Identification

The identifiers of the Timestamp policies specified in this document are:

Type	OID	Description
	1.3.6.1.4.1.4146.2	**Timestamp Policies Arc**
Non-Qualified	1.3.6.1.4.1.4146.2.3	Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2)
	1.3.6.1.4.1.4146.2.3.1	Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2) with R6 CA hierarchy
	1.3.6.1.4.1.4146.2.3.1.1	Trusted Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2) with R6 CA hierarchy
	1.3.6.1.4.1.4146.2.3.1.2	CodeSign Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2) with R6 CA hierarchy
	1.3.6.1.4.1.4146.2.3.2	Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2) with R45 CA hierarchy
	1.3.6.1.4.1.4146.2.3.2.1	Trusted Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2) with R45 CA hierarchy
	1.3.6.1.4.1.4146.2.3.2.2	CodeSign Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 2 (SHA2) with R45 CA hierarchy
	1.3.6.1.4.1.4146.2.4	Policy by which the time-stamping services operated by GlobalSign incorporate the time into IETF RFC 3161 responses specifically for extended validation code signing services
	1.3.6.1.4.1.4146.2.7	Timestamp Policy for JP Accredited non-AATL
Qualified	1.3.6.1.4.1.4146.2.5	Timestamp Policy for eIDAS Qualified[1]

[1] By including this object identifier in the generated timestamps, GlobalSign claims conformance to these additional timestamp policies: itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)

Legacy OIDs

The following OIDs are marked as legacy and where applicable are being replaced with a new Policy indicated in the table above.

Type	OID	Description
Non-Qualified	1.3.6.1.4.1.4146.1.31	Timestamp Policy for AATL
	1.3.6.1.4.1.4146.2.2	Timestamping policy covering Timestamp Tokens (TST) issued under IETF RFC 3161 with a Secure Hash Algorithm version 1 (SHA1)

5.3 User Community and Applicability

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

This policy may be used for public timestamping services or timestamping services used within a closed community.

6.0 Policies and Practices

6.1 Risk Assessment

GlobalSign's security program includes an annual risk assessment that:

- Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Timestamp data or Timestamp management processes.
- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the data and processes; and
- Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that GlobalSign has in place to counter such threats. Based on the risk assessment, GlobalSign develops, implements, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the risk assessment, commensurate with the sensitivity of the certificate data and certificate management processes.
- The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the certificate data and certificate management processes. The security plan also takes into account available technology and the cost of implementing the specific measures and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

6.2 Trust Service Practice Statement

GlobalSign shall ensure the quality, performance, and operation of the timestamping service through the implementation of various security policies and controls.

The security policies and controls are reviewed regularly by an independent body, whilst trained trustworthy personnel check the adherence of the security controls to the policies.

6.2.1 Timestamp Format

The service issues Timestamps signed using one of the following digest algorithms:

- SHA-256
- SHA-384
- SHA-512

6.2.2 Accuracy of the Time

The timestamping service time signal is provided from GNSS, together with an NTP Time Monitor for monitoring time.offset and time.drift from a set of Stratum 1, 2 or 3 UTC(k) laboratory NTP servers.

The timestamping service ensures an accuracy of 1 second with respect to UTC.

Note that the time of timestamping is not the timestamping request acceptance moment, but the timestamping system processing moment.

6.2.3 Limitations of the Service

No stipulation.

6.2.4 Obligations of the Subscriber

Subscribers must inform Relying Parties of this practice statement (in particular the obligations in section 6.2.5) and the GlobalSign CPS.

6.2.5 Obligations of Relying Parties

Before relying on a timestamp, the Relying Party shall:

a) Verify that the Timestamp has been correctly signed, that the certificate used to sign the Timestamp was valid at the time indicated within the Timestamp and that the private key used to sign the Timestamp has not been compromised before the time of the verification. See section 6.2.6 of this practice statement and section 9.6.4 of the GlobalSign CPS.

b) Consider any limitations on the usage of the Timestamp indicated by this practice statement.

c) Consider any other precautions prescribed in agreements or elsewhere.

For Qualified Timestamps, if this verification takes place after the end of the validity period of the certificate, the Relying Party should follow the guidance denoted in Annex D of ETSI EN 319 421 [5].

6.2.6 Verification of the Timestamp

Timestamp verification includes the following:

6.2.6.1 Verification of the Timestamp issuer

TSU and issuing CA certificates are published to allow Relying Parties to verify that Timestamps are issued by a TSU operated by GlobalSign.

The certificates can be found on the GlobalSign support site: https://support.globalsign.com.

For Qualified Timestamps, GlobalSign employs certificate chaining and has added CA certificates to the EU Trusted List, Therefore Relying Parties are expected to check that the TSUs certificate was signed by a key listed on the Trusted List and the service it represents is a Qualified Timestamping Service, then the Timestamps issued by this TSU can be considered as qualified.

TSU certificates for Qualified Timestamps should be issued under ETSI EN 319 411-2 [4] certificate policy.

6.2.6.2 Verification of the Timestamp revocation status

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

6.2.7 Applicable law

This practice statement is governed, construed, and interpreted in accordance with the laws of Belgium. This choice of law is made to ensure uniform interpretation of this practice statement, regardless of the place of residence or place of use of GlobalSign Certificates or other products and services. The law of Belgium applies also to all GlobalSign commercial or contractual relationships in which this practice statement may apply or quoted implicitly or explicitly in relation to GlobalSign products and services where GlobalSign acts as a provider, supplier, beneficiary receiver or otherwise.

Each party, including GlobalSign partners, Subscribers and Relying Parties, irrevocably submit to the jurisdiction of the district courts of Leuven, Belgium.

6.2.8 Service availability

GlobalSign implements the following measures to ensure availability of the service:

- Redundant setup of IT Systems, including Timestamp issuing infrastructure, in order to avoid single points of failure
- Redundant high-speed internet connections in order to avoid loss of service
- Use of uninterruptable power supplies

Although those measures ensure service availability, GlobalSign does not guarantee an annual availability of 100%. GlobalSign aims to provide 99% service availability per year while reaching an average availability of 99.95% per year.

6.3 Terms and Conditions

This document represents the applied trust service policy.

For Subscribers, please refer to the obligations in section 6.2.4. Service specific agreements may apply.

For Relying Parties, please refer to the obligations in section 6.2.5.

6.4 Information Security Policy

GlobalSign implements an information security policy which all employees must adhere to. The information security policy is reviewed on a regular basis and when significant changes occur. The "GlobalSign PASEC1 - Information Security Governance Policy Authority" approves changes to the information security policy.

6.5 TSA obligations

6.5.1 General

No stipulation.

6.5.2 TSA Obligations towards Subscribers

The present document places no specific obligations on the Subscriber beyond any TSA specific requirements stated in the section 6.3.

6.6 Information for relying parties

Please refer to the obligations of Relying Parties in section 6.2.5.

7.0 TSA Management and Operation

7.1 Introduction

GlobalSign applies various policies and procedures to ensure the trustworthiness of the timestamping service.

Note: The provision of a Timestamp token in response to a request is at the discretion of GlobalSign.

7.2 Internal Organization

The TSA is provided by Globalsign NV/SA and affiliated entities. GlobalSign implements information security practices, including personnel security, access controls, risk assessment, as appropriate for the timestamping services.

7.3 Personnel Security

GlobalSign implements personnel security policies and procedures to ensure that employees and contractors support the trustworthiness of the TSP's operations.

In particular:

- GlobalSign employs staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding security and personal data protection rules as appropriate for the offered services and the job function.
- Trusted roles, on which the security of the operations depends, are clearly identified.

  Personnel exercises administrative and management procedures and processes that are in line with information security management procedures.

7.4 Asset Management

GlobalSign implements asset management policies and procedures (including media handling) to ensure an appropriate level of protection of its assets including information assets.

An asset inventory is maintained, which includes all information assets and classification based on risk assessment.

7.5 Access Control

GlobalSign implements access control management policies and procedures to ensure TSP system access shall be limited to authorized individuals.

Different security layers with respect to physical access and logical access ensure a secure operation of the timestamping service:

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

7.6 Cryptographic Controls

Security controls are in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle.

In particular:

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 section 7.8) by personnel in trusted roles (as per section 7.3) under at least dual control.

b) The personnel authorized to carry out this function is limited to those required to do so under GlobalSign's practices.

c) The generation of the TSU's signing key(s) is carried out within a cryptographic module which is conformant to FIPS PUB 140-2 [7], level 3 or FIPS PUB 140-3 [11], level 3.

d) The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing Timestamps key are specified by GlobalSign's Policy Authority.

e) Effective April 15, 2025, GlobalSign will generate and protect Private Keys associated with its Root CA certificates and new Subordinate CA certificates used for signing TSU keys for CodeSigning with a validity period of greater than 72 months containing the id-kp-timeStamping KeyPurposeId in the extKeyUsage extension in a Hardware Crypto Module conforming to the requirements of section 7.6.1.1.

7.6.1.1 Code-Signing specific requirements

The Hardware Crypto Module must be validated as meeting at least FIPS 140-2 level 3, FIPS 140-3 level 3, or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats, and maintained in a High Security Zone and in an offline state or air-gapped from all other networks.

7.6.2 TSU private key protection

The TSU private signing key is held and used within a cryptographic module which meets the requirements identified in FIPS PUB 140-2 [7], level 3 or FIPS PUB 140-3 [11], level 3.

Each TSU private signing key is always associated with only one TSU certificate. A TSU is connected to exactly one hardware security module ensuring that only one private key per TSU is used.

TSU private keys are not backed up.

Timestamp Certificates for CodeSigning issued on or after April 15, 2025, issued by a Timestamp Authority Subordinate CA with a validity period greater than 72 months, will be signed by a Private Key generated and protected in a Hardware Crypto Module conforming to the requirements of section 7.6.1.1.

7.6.3 Public key certificate

GlobalSign 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 publicly available certificates. The certificates can be found on the GlobalSign Support Site: https://support.globalsign.com.

b) The TSU does not issue a Timestamp before its signature verification (public key) certificate is loaded into the TSU or its cryptographic device. When obtaining a signature verification (public key) certificate, GlobalSign verifies that this certificate has been correctly signed (including verification of the certificate chain to its trusted certification authority).

7.6.4 Rekeying TSU's key

The lifetime of the TSU's certificate shall not be longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose (see section 7.6.1 d)).

Once a year or when significant changes occur, GlobalSign's Policy Authority verifies any cryptographic algorithms used within the TSU against the algorithms recognized as suitable as in clause 7.6.1 d).

If an algorithm becomes compromised or is not suitable anymore, GlobalSign will rekey any affected private keys.

7.6.5 Life Cycle Management of Signing Cryptographic Hardware

Hardware is protected during the lifecycle to ensure prevent tampering during shipment, when and while stored.

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

TSU private signing keys stored on TSU cryptographic module shall be erased upon device retirement in a way that it is impossible to recover them.

7.6.6 End of TSU Key Life Cycle

The validity of TSU private keys never exceed the validity of the associated public key certificate.

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.

Operational or technical procedures shall be in place to ensure that a new key is put in place when a TSU's key expires.

The GlobalSign Key Manager defines key validity periods in accordance with clause 7.6.1 d) with a maximum validity period as specified in the CPS.

Private Keys associated with Qualified Timestamp Certificates issued shall be removed from the Hardware Crypto Module protecting the Private Key within 5 years after issuance of the Timestamp Certificate.

Effective April 15, 2025, Private Keys associated with Codesigning Timestamp Certificates issued for greater than 15 months shall be removed from the Hardware Crypto Module protecting the Private Key within 18 months after issuance of the Timestamp Certificate.

For Timestamp Certificates for CodeSigning and Qualified issued on or after June 1, 2024, GlobalSign shall log the removal of the Private Key from the Hardware Crypto Module through means of a key deletion ceremony performed by the CA and witnessed and signed-off by at least two Trusted Role members. GlobalSign may also perform a key destruction ceremony, meaning that all copies of that private key are unequivocally/securely destroyed (i.e. without a way to recover the key), including any instance of the key as part of a backup, to satisfy this requirement.

7.7 Timestamping

7.7.1 Timestamp Issuance

The following types of Timestamps are provided:

7.7.1.1 Qualified Timestamps

Qualified Timestamps are tokens issued in compliance with:

- RFC 3161 [8]
- ETSI EN 319 422 [6]
- the eIDAS regulation

7.7.1.2 Non-Qualified Timestamps

Non-Qualified Timestamps are tokens that meet the requirements of RFC 3161 [8].

7.7.1.3 Authenticode Timestamps

Authenticode Timestamps are tokens intended for Authenticode Digital Signatures.

7.7.2 Clock Synchronization with UTC

The TSU clock is synchronized with UTC [1] within an accuracy of 1 second or better traceable to at least one real time value distributed by a UTC(k) laboratory.

Clock synchronization shall be maintained when a leap second occurs as notified by the appropriate body. Any change to take account of the leap second shall occur during the last minute of the day when the leap second is scheduled to occur. A record shall be maintained of the exact time (within the declared accuracy) when this change occurred.

For Qualified Timestamps, in case where the TSU clock drifts out of accuracy, no Timestamp will be issued until re-synchronization of the clock.

GlobalSign maintains policies and procedures to ensure:

- Continuous calibration of the TSU clock
- Monitoring of the accuracy of the TSU clock
- Threat analysis against attacks on time-signals
- Behavior while skipping/adding leap seconds

GlobalSign logs all records concerning the following clock synchronization related events:

- All events relating to synchronization of a TSU's clock to UTC shall be logged (including re-calibration or synchronization of clocks used in timestamping).
- All events relating to detection of loss of synchronization shall be logged.

7.8 Physical and Environmental Security

GlobalSign implements physical and environmental security policies and procedures for systems used for timestamping services to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities.

These policies and procedures cover 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 & entering.

The following additional controls apply to timestamping management:

- The timestamping 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 non-authorized person shall be accompanied by an authorized person whilst in the secure area. Every entry and exist shall be logged.
- Physical protection is achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the timestamping management. Any parts of the premises shared with other organizations are outside this perimeter.
- Physical and environmental security controls protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation.
- Controls protect against equipment, information, media and software relating to the timestamping services being taken off-site without authorization.

Other functions may be supported within the same secured area provided that the access is limited to authorized personnel.

7.9 Operation Security

GlobalSign implements a set of system and security controls to ensure service quality and availability.

In particular:

- An analysis of security requirements is carried out at the design and requirements specification stage of any systems development project undertaken by GlobalSign or on behalf of GlobalSign to ensure that security is built into information technology systems.
- Change control procedures are applied for releases, modifications, and emergency software fixes of any operational software.
- The integrity of GlobalSign systems and information is protected against viruses, malicious and unauthorized software. All systems are hardened in conformance to the relevant hardening policy of GlobalSign.
- Media used within GlobalSign systems is securely handled to protect media from damage, theft, unauthorized access, and obsolescence.
- Media management procedures protect against obsolescence and deterioration of media within the period of time that records are required to be retained.
- Procedures are established and implemented for all trusted and administrative roles that have an impact on the provisioning of services.
- GlobalSign has specified and applied procedures for ensuring security patches are applied within a reasonable time after they become 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.
- Capacity demands are monitored and projections of future capacity requirements are made to ensure that adequate processing power and storage are available.

7.10 Network Security

GlobalSign implements network security policies and procedures to protects its network and systems from attack.

In particular:

- The network is segmented into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services.

- Accounts, applications, services, protocols, and ports that are not used in the TSA's operations are removed or disabled.
- Access and communication is restricted between zones. Non-required connections and services are explicitly forbidden or deactivated. The established rule set is reviewed quarterly.
- Critical systems (e.g. Root CA systems, TSU) are kept in a secured zone.
- 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.
- Test and production platforms are separated from other environments not concerned with live operations (e.g. development).
- 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.
- The external network connection to the internet is redundant to ensure availability of the services in case of a single failure.
- GlobalSign also performs regular vulnerability assessment and penetration testing covering all GlobalSign assets related to certificate issuance, products, and services. Assessments focus on internal and external threats that could result in unauthorized access, tampering, modification, alteration, or destruction of the certificate issuance process

7.11 Incident Management

GlobalSign implements an incident management process in order to react appropriately to incidents.

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

In particular:

- Monitoring activities take account of the sensitivity of any information collected or analyzed.
- Abnormal system activities that indicate a potential security violation, including intrusion into the network, are detected and reported as alarms.
- IT systems monitor the following events:
    - Start-up and shutdown of the logging functions;
    - Availability and utilization of needed services within GlobalSign network.
- GlobalSign acts in a timely and coordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. GlobalSign appoints trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with GlobalSign's procedures.
- GlobalSign 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.
- The national supervisory body is informed within 24h after discovery of a critical security breach.

- Audit logs are monitored or reviewed regularly, at least quarterly, to identify evidence of malicious activity.
- GlobalSign will resolve critical vulnerabilities within a reasonable period after the discovery. If this is not possible, GlobalSign will create and implement a plan to mitigate the critical vulnerability or GlobalSign will document the factual basis for GlobalSign's determination that the vulnerability does not require remediation.
- 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

GlobalSign records and keeps accessible for at least ten years, including after the activities of the timestamping services by GlobalSign have ceased, all relevant information concerning data issued and received by GlobalSign, in particular, for providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

In particular:

- The confidentiality and integrity of current and archived records concerning operation of services is maintained.
- Records concerning the operation of services are completely and confidentially archived in accordance with disclosed business practices.
- 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.
- 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.
- 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 this document.
- 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.
- Records concerning all events relating to the life-cycle of TSU keys and certificates are logged.
- Records concerning all events relating to synchronization of a TSU's clock to UTC are logged. This includes information concerning normal re-calibration or synchronization of clocks used in timestamping.
- Records concerning all events relating to detection of loss of synchronization are logged.

7.13 Audit Logging Procedures

GlobalSign records events related to the security of its Timestamping Systems, actions taken to process a timestamp request and to issue a timestamp, including all information generated and documentation received in connection with the timestamp request

The GlobalSign Timestamp Authority logs the following information and makes these records available to its Qualified Auditor as proof of the Timestamp Authority’s compliance with these Requirements:

1. Physical or remote access to a timestamp server, including the time of the access and the identity of the individual accessing the server,
2. History of the timestamp server configuration,

3. Any attempt to delete or modify timestamp logs,
4. Security events, including:
    1. Successful and unsuccessful Timestamp Authority access attempts;
    2. Timestamp Authority server actions performed;
    3. Security profile changes;
    4. System crashes and other anomalies; and
    5. Firewall and router activities;
5. Revocation of a timestamp certificate,
6. Major changes to the timestamp server's time, and
7. System startup and shutdown.

7.14 Retention Period for Audit Log

GlobalSign Timestamp Authorities retain, for at least two (2) years:

1. Timestamp Authority data records (as set forth in Section 7.13) after the revocation or renewal of the Timestamp Certificate Private Key
2. Timestamp Authority security event records set forth in Section 7.13(3)) after the event occurred

7.15 Business Continuity Management

GlobalSign's disaster recovery plan defines the steps to be taken in case of (suspected) compromise of a TSU's private signing key or loss of calibration of a TSU clock.

For Qualified Timestamps, if it is detected that the time that would be indicated in a timestamp, drifts or jumps out of synchronization with UTC, the TSU shall stop Timestamp issuance. In case of compromise, The TSU shall not issue Timestamps until steps are taken to recover from the compromise.

In case of compromise of the operations, (suspected) compromise or loss of calibration, GlobalSign will make available, as appropriate, a description of compromise that occurred to Subscribers and Relying Parties.

In case of major compromise of the operations or loss of calibration, GlobalSign will make available, as appropriate, to Subscribers and Relying Parties, information which can be used to identify the Timestamps which may have been affected, unless this breaches the privacy of the TSAs users or the security of the TSA services.

7.16 TSA Termination and Termination Plans

In the event GlobalSign terminates its timestamping operations, it will notify the applicable Supervisory Bodies prior to termination.

GlobalSign will ensure that prompt notification of termination is provided to Subscribers and other relevant stakeholders in GlobalSign timestamping services.

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

In addition, the following applies:

1) GlobalSign maintains an up-to-date termination plan.

2) Before GlobalSign terminates its services at least the following procedures shall be applied:

    a) GlobalSign will inform the following of the termination: all Subscribers and other entities with which GlobalSign has agreements or other form of established relations. In addition, this information will be made available to other relying parties.

b) GlobalSign will terminate authorization of all subcontractors acting on behalf of GlobalSign in carrying out any functions relating to the process of issuing trust service tokens.

c) GlobalSign will transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of GlobalSign for a reasonable period.

d) GlobalSign private keys, including any backup copies, will be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.

e) Where possible, GlobalSign will try to make arrangements to transfer the provision of trust services for its existing customers to another TSP.

f) GlobalSign will revoke all of its TSU certificates.

g) GlobalSign will ensure that the terminated TSU shall not be allocated or generated new private and public key pair and shall not issue any new time-stamp tokens.

3) GlobalSign has an arrangement to cover the costs to fulfil these minimum requirements in case it 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.

4) GlobalSign 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.

7.17 Compliance

GlobalSign ensures compliance with applicable law at all times.

The GlobalSign TSA is compliant with ETSI EN 319 401 and CA/Browser Forum Network and Certificate System Security Requirements and maintains its compliance with these requirements via an auditor on an annual (WebTrust) and bi-annual (eIDAS) and contiguous basis.

The audit is performed by a conformity assessment body accredited by a European Union member state national accreditation body on the basis of EN ISO/IEC 17065 as profiled by ETSI EN 319 403 and in particular against the requirements defined in the eIDAS Regulation (EU) No 910/2014.

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

The Supervisory Body will be informed of any significant change in the provision of the TSA.

Additionally, following specific requirements apply:

7.17.1 Qualified Timestamps

- eIDAS regulation
- ETSI EN 319 421, ETSI EN 319 422
- RFC 3161

7.17.2 Non-Qualified Timestamps

- RFC 3161
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates (Timestamp Policy for Code Signing).

7.17.3 Authenticode Timestamps

No additional requirements apply.

8.0 Contact

8.1.1 Organization Administering the Document

Requests for information related to this practice statement should be addressed to:

PACOM1 - CA Governance GlobalSign
Diestsevest 14,
3000 Leuven, Belgium
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909
Email: policy-authority@globalsign.com

8.1.2 General Inquiries

GlobalSign NV/SA
attn. Legal Practices,
Diestsevest 14,
3000 Leuven, Belgium
Tel: + 32 (0)16 891900
Fax: + 32 (0) 16 891909
Email: legal@globalsign.com
URL: www.globalsign.com

In case of complaints or dispute settlement, please reach out to GlobalSign using the above contact details.