CA Governance Policy Authority

Digitally signed by CA Governance Policy Authority
Date: 2021.04.26 11:57:45 +02'00'

GlobalSign

Qualified Timestamping Practice Statement

Date: April 28, 2021

Version: v1.3

Table of Contents

Document History

Version	Release Date	Status & Description
v1.0	March 31, 2019	Initial release
V1.2	October 29, 2020	Administrative update/clarifications
V1.3	April 28, 2021	Revision of OIDs Various layout and spelling updates UK eIDAS updates Clarification of collection of evidences

Acknowledgments

GlobalSign® and the GlobalSign Logo are registered trademarks of GMO GlobalSign K.K.

1.0 Introduction

1.1 Overview

This Qualified Timestamping Practice Statement (“QTSPS”) applies to the eIDAS and UK eIDAS Qualified Timestamping Services of GlobalSign NV/SA and affiliated entities (“GlobalSign”).

Among other services, GlobalSign offers timestamping services to ensure the long-term validity of digitally signed documents. The Qualified Timestamping Service is an auxiliary service, and its terms and conditions are determined by the overall GlobalSign CA Certification Practice Statement (practice statement).

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 requirements of Regulation (EU) No. 910/2014 on electronic identification and trust services for electronic transactions in the internal market) (“eIDAS”) and eIDAS (UK Legislation) and The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (“UK eIDAS”) and other relevant international standards for Timestamping Authorities. An independent conformity assessment body verifies the efficiency of these procedures on a regular basis.

Trust services for the United Kingdom are operated by and provided through GMO GlobalSign LTD., an affiliate entity of GlobalSign.

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

This QTSPS conforms to Policy and Security Requirements for Trust Service Providers issuing Electronic Timestamps (ETSI EN 319 421) and complies with the eIDAS and UK eIDAS regulations.

1.3 Scope

This document specifies policy and security requirements relating to the operation and management practices of the GlobalSign Trusted Service Authority issuing timestamps. Such timestamps can be used in support of digital signatures or for any application that requires proof that a datum existed before a particular time.

This document can be used by independent bodies as the basis for confirming that GlobalSign is trusted for issuing timestamps according to the eIDAS and UK eIDAS regulations.

This document does not specify:

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

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

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

[5] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps”

[6] ETSI EN 319 422: "Electronic Signatures and Infrastructures (ESI); Timestamping protocol and timestamp token profiles.”

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

[8] IETF RFC3161 https://www.ietf.org/rfc/rfc3161.txt

3.0 Definitions and abbreviations

3.1 Definitions

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

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.

GNSS: Global Navigation Satellite System

GPS: Global Positioning System

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

Qualified Timestamping Service: Timestamping Service issuing qualified electronic timestamp tokens as per eIDAS or UK eIDAS regulations.

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 Service: trust service for issuing timestamps

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

UK eIDAS ("UK eIDAS"): eIDAS (UK Legislation) and The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016.

3.2 Abbreviations

For the purposes of this document, the abbreviations given in ETSI EN 319 401 [4] 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

4.0 General Concepts

4.1 General Policy Requirements

This document references ETSI EN 319 401 [4] for generic policy requirements common to all classes of Trust Service Providers' service.

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

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).

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

The TSP confirms that the TSA is audited at least every 24 months by a conformity assessment body.

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

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

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

The TSP may make use of other parties to provide parts of the timestamping services. However, the TSP always maintains overall responsibility (as per clause 6.5) and ensures that the policy requirements identified in this document are met. The TSP may operate several identifiable timestamping units.

The TSP is a trust service provider as described in ETSI EN 319 401 [4] 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 CA and the entity that is contracted with GlobalSign for the use of the Timestamping Service.

4.5 Timestamp Policy and TSA Practice Statement

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

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

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

This document specifies the timestamp policy and the practice statement for the GlobalSign TSA.

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 identifier of the timestamp policies specified in this document are:

1.3.6.1.4.1.4146.1.32 - Timestamping Certificate Policy – Certificates for Qualified Timestamping (QTS) under eIDAS and UK eIDAS regulation
iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 4146 certificate-policies(1) eidas(32)

1.3.6.1.4.1.4146.2 - Policy by which the timestamping services operated by GlobalSign incorporates the time into IETF RFC 3161 responses
iso(1) iso-identified-organization(3) dod(6) internet(1) private(4) enterprises(1) 4146(4146) time-stamp-policies(2)

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)
iso(1) iso-identified-organization(3) dod(6) internet(1) private(4) enterprises(1) 4146(4146) time-stamp-policies(2) rfc3161-tst-policy-sha2(3)

1.3.6.1.4.1.4146.2.5 - Timestamping Token Policy
iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 4146 time-stamp-policies(2) qualified-timestamping-token(5)

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)

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 [6]) 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:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate management processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the certificate data and certificate management processes; and
3. 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.
4. 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.

Additionally, for compliance to ETSI EN 319 421 the following measures have been implemented:

6.2.1 Timestamp Format

The issued timestamp tokens by GlobalSign are compliant to RFC 3161 timestamps. The service issues RSA2048 encrypted timestamps that accept one of the following hash algorithms:

- SHA256
- SHA384
- SHA512

6.2.2 Accuracy of the Time

The timestamping service is located in the UK where a time signal is provided from GNSS using a 72-parallel channel GNSS receiver with a crystal oscillator, providing an accuracy of 400x10^-6 over 24 hours (10^-9 per second), and which is GPS time traceable to UTC(USNO). The timestamping service uses this time signal together with an NTP Time Monitor for monitoring time.offset and time.drift from a set of UTC(k) laboratory NTP servers. With that setup the timestamping service reaches an accuracy of the time well under +/-1s 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

Subscriber may not exceed the permitted number of Timestamps purchased.

Subscriber shall be responsible for applying the Timestamps into the documents or code using the GlobalSign provided URL.

Subscriber shall not share the URL or its access credentials for the Service or permit use of the Service by third parties.

Subscriber shall not request more than five (5) Timestamps per second unless Subscriber has purchased a higher rate limit.

6.2.5 Obligations of Relying Parties

Before placing any reliance on a timestamp, a relying party must:

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 until the time of the verification. GlobalSign provides several ways to do so. See clause 6.2.6.
b) take into account any limitations on the usage of the timestamp indicated by this practice statement
c) take into account any other precautions prescribed in agreements or elsewhere

For qualified timestamps, ETSI EN 319 421 states: "The relying party is expected to use a Trusted List to establish whether the timestamp unit and the timestamp are qualified. If the public key of the TSU is listed in 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."

During the TSU certificate validity period, the status of the certificate can be checked using the relevant OCSP as stated within the AIA extension of the certificate.

Relying parties should rely on DNS services that respect the TTL value of the A record when accessing the timestamp services and certificate status services.

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.

6.2.6 Verification of the Timestamp

Timestamp verification includes the following:

6.2.6.1 Verification of the timestamp issuer

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

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

6.2.6.2 Verification of the timestamp revocation status

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

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

- Redundant setup of IT Systems, including HSM 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

6.3.1 Trust Service Policy being Applied

This document represents the applied trust service policy. See chapter 5 for further information.

6.3.2 Period of Time During which TSP Event Logs are Retained

GlobalSign retains any audit logs generated for at least ten years. GlobalSign makes these audit logs available to Qualified Auditors (as such term is defined in the GlobalSign CPS) upon request.

6.4 Information Security Policy

GlobalSign has implemented 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 the changes to the information security policy.

7.0 TSA Management and Operation

7.1 Introduction

GlobalSign has implemented information security policies and operational procedures to maintain the security of the service.

7.2 Internal Organization

For the proper operations of the timestamping service, GlobalSign maintains non-disclosed documentation, that specifies all operational controls concerning personnel security, access controls, risk assessment etc. These internal documents are used by independent bodies to confirm compliance of the service against ETSI EN 319 421.

a) Legal entity: The TSA is provided by GlobalSign nv/sa.
b) Information security management and quality management of the service is carried out within the security concept of the service.
c) GlobalSign operates its TSU from an ISO27001-compliant data center located in the UK which provides the basic infrastructure (Internet access, electricity, physical security, etc.) of the trust service. Only GlobalSign personnel have access to GlobalSign premises within the data center.

7.3 Personnel Security

7.3.1 Qualifications, Experience, and Clearance Requirements

Prior to the engagement of any person in the certificate management process, whether as an employee, agent, or an independent contractor, GlobalSign verifies the identity and trustworthiness of such person.

GlobalSign employs a sufficient number of personnel that possess the expert knowledge, experience and qualifications necessary for the offered services, as appropriate to the job function.

GlobalSign personnel fulfil the requirement through expert knowledge, experience and qualifications with formal training and education, actual experience, or a combination of the two.

Trusted roles and responsibilities are documented in job descriptions.

GlobalSign personnel (both temporary and permanent) have job descriptions defined from the viewpoint of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.
GlobalSign personnel are formally appointed to trusted roles.

7.3.2 Background Check Procedures

All GlobalSign personnel in trusted roles are free from conflict of interests that might prejudice the impartiality of the CA operations.

GlobalSign does not appoint any person to a trusted role who is known to have a conviction for a serious crime or another offence if such conviction affects his/her suitability for the position.

Personnel do not have access to the trusted functions until any necessary checks are completed and results analyzed, provided such checks are permitted by the jurisdiction in which the person will be employed.

All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation where permitted by law.

Any use of information revealed by background checks by GlobalSign shall be in compliance with applicable laws of the jurisdiction where the person is employed.

7.3.3 Training Requirements

GlobalSign provides all personnel with skills training that covers basic public key infrastructure (PKI) knowledge, policies and procedures (including this document) and common threats (including phishing and other social engineering tactics).

GlobalSign maintains records of such training and ensures that all personnel maintain a skill level that enables them to perform their duties satisfactorily.

7.3.4 Retraining Frequency and Requirements

All personnel in trusted roles maintain skill levels consistent with GlobalSign's training and performance programs.

Individuals in trusted roles are aware of changes in GlobalSign operations, as applicable. Any significant change to the operations has a training (awareness) plan, and the execution of such plan is documented.

GlobalSign provides information security and privacy training at least once a year to all employees.

7.3.5 Job Rotation Frequency and Sequence

GlobalSign ensures that any change in the staff will not affect the operational effectiveness of the service or the security of the system.

7.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary sanctions are applied to personnel violating provisions and policies or CA related operational procedures.

7.3.7 Independent Contractor Requirements

All contractor personnel employed for GlobalSign operations are subject to the same process, procedures, assessments, security controls and training as permanent CA personnel.

7.3.8 Documentation Supplied to Personnel

GlobalSign makes available to its personnel all relevant statutes, policies and contracts. Other technical, operational and administrative documents (e.g., administrator manuals, user manuals, etc.) are provided in order for the personnel in trusted roles to perform their duties.

7.4 Asset Management

All IT systems used within the service are clearly identified, categorized and filed.

7.4.1 Media Handling

All media is handled securely.
GlobalSign CA ensures that all media used for the storage of information is declassified or destroyed in a generally accepted manner before being released for disposal.

7.5 Access Control

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

For instance:

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

Any personnel changing roles within GlobalSign will have all security tokens reviewed and withdrawn where necessary.

Any personnel who leave GlobalSign will have all security tokens withdrawn.

7.6 Cryptographic Controls

GlobalSign uses several private keys to fulfil its service. One private key pair is used to issue the public key timestamp certificates which are used within the TSUs. One or more private key pair is or are used within the TSU to issue the timestamp.

All private keys are stored in a FIPS 140-2 Level 3 hardware security module (HSM).

7.6.1 TSU key generation

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

b) The generation of the TSU's signing key(s) is carried out within a cryptographic module which is conformant to FIPS PUB 140-2 [i.9], level 3

c) The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing timestamps key is recognized by any national supervisory body.

7.6.2 TSU private key protection

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

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.

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 clause 7.7.1c).

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 7.6.1c).

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

All hardware will be inspected during the commissioning process to ensure conformity to supply and no evidence of tampering found.

Hardware and software procured are purchased in a fashion which reduces the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).

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 practically impossible to recover them.

7.6.6 End of TSU Key Life Cycle

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

After expiration of the private keys, the private keys within the cryptographic hardware are destroyed in a manner such that the private keys cannot be retrieved or used anymore. The GlobalSign Key Manager defines key validity periods in accordance to clause 7.6.1c.

7.7 Timestamp Issuance

The GlobalSign Qualified Timestamping Service issues qualified timestamps which conform to the timestamp profile defined in ETSI EN 319 422 [5].
The provision of a timestamp token in response to a request is at the discretion of GlobalSign.

7.7.1 Clock Synchronization with UTC

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

Specifically, the following topics are covered:

- 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 maintains physical and environmental security policies for systems used for timestamping services which 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, and disaster recovery. Controls should be implemented to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities.

7.8.1 Site Location and Construction

GlobalSign's Qualified Timestamping Services are located within a secure data center. The data center is a purpose-built facility made of concrete and steel construction.

7.8.2 Physical Access

GlobalSign's Qualified Timestamping Services operate within a secure data center that provides premise security with biometric scanners and card access systems. A 24x7 Closed Circuit TV (CCTV) monitoring system as well as digital recording is provided. Qualified security guards secure the physical premises and only security-cleared and authorized personnel are allowed into the premises.

7.8.3 Power and Air Conditioning

GlobalSign's Qualified Timestamping Services operate within a secure data center that is equipped with redundant power and cooling system. UPS and failover to power generator are in place in the unlikely event of power outage.

7.8.4 Water Exposures

GlobalSign's Qualified Timestamping Services are protected against water. It is located above ground and on a higher floor with raised flooring. In addition, a water detection alarm system is in place and on-site data center operations staff are ready to respond to any unlikely water exposure.

7.8.5 Fire Prevention and Protection

GlobalSign's Qualified Timestamping Services operate within a secure data center that is equipped with a fire detection and suppression system.

7.8.6 Media Storage

Storage of backup media is off-site, physically secured and protected from fire and water damage.

7.8.7 Waste Disposal

GlobalSign ensures that all media used for the storage of information is declassified or destroyed in a generally accepted manner before being released for disposal.

7.8.8 Off-Site Backup

GlobalSign performs regular off-site backup of critical data. The backed-up data is stored at a physically secured off-site location.

7.9 Operation Security

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

In particular, these controls are:

a) An analysis of security requirements is carried out at the design and requirements specification stage of any systems development project undertaken by GlobalSign or on behalf of GlobalSign to ensure that security is built into information technology systems.

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

c) 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.

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

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

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

g) 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.

7.10 Network Security

GlobalSign protects its network and systems from attack.

In particular:

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

b) GlobalSign restricts access and communications between zones. Non-required connections and services are explicitly forbidden or deactivated. The established rule set is reviewed quarterly.

c) All GlobalSign critical systems (e.g. Root CA systems, TSU) are kept in a secured zone.

d) A dedicated network for administration of IT systems that is separated from the operational network is established. Systems used for administration will not be used for non-administrative purposes.

e) Test and production platforms are separated from other environments not concerned with live operations (e.g. development).

f) Communication between distinct trustworthy systems can only be established through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

g) The external network connection to the internet is redundant to ensure availability of the services in case of a single failure.

h) 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

An incident management process has been implemented in order to react quickly to incidents. System activities concerning access to IT systems, user of IT systems, and service requests are monitored.

In particular:

a) Monitoring activities take account of the sensitivity of any information collected or analyzed.

b) Abnormal system activities that indicate a potential security violation, including intrusion into GlobalSign network, are detected and reported as alarms.

c) GlobalSign IT systems monitor the following events:

a) Start-up and shutdown of the logging functions;

b) Availability and utilization of needed services within GlobalSign network.

c) 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.

d) 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.

e) The national supervisory body is informed within 24h after discovery of a critical security breach.

f) Audit logs are monitored or reviewed regularly, at least quarterly, to identify evidence of malicious activity.

g) 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.

h) Incident reporting and response procedures are employed in such a way that damage from security incidents and malfunctions are minimized.

7.12 Collection of Evidence

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

GlobalSign records and keeps accessible for an appropriate period, including after the activities of 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:

a) The confidentiality and integrity of current and archived records concerning operation of services is maintained.

b) Records concerning the operation of services are completely and confidentially archived in accordance with disclosed business practices.

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

d) The precise time of significant TSP environmental, key management and clock synchronization events are recorded. The time used to record events as required in the audit log is synchronized with UTC continuously.

e) Records concerning services are held for a period after the expiration of the validity of the signing keys or any trust service token as appropriate for providing necessary legal evidence according to this document.

f) The events are logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.

g) Accountability of personnel: All activities accomplished by system administrators are logged in a central log server. System administrators always identify themselves with named accounts, so administration activities can be mapped to persons at all times.

h) Records concerning all events relating to the life-cycle of TSU keys and certificates are logged.

i) 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 time-stamping.

j) Records concerning all events relating to detection of loss of synchronization are logged.

7.13 Business Continuity Management

GlobalSign does not disclose business continuity plans to Subscribers or Relying Parties but will provide business continuity plan and security plans to GlobalSign's auditors upon request. GlobalSign annually tests, reviews, and updates these procedures. The business continuity plan includes:

1. The conditions for activating the plan;
2. Emergency procedures;
3. Fall-back procedures;
4. Resumption procedures;
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans;
10. GlobalSign's plan to maintain or restore the CA business operations in a timely manner following interruption to or failure of critical business processes;
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time;
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA's main site; and
15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.
16. Any loss of calibration or compromising of a TSU clock is covered in clause 7.7.1 of this document.

7.14 TSA Termination and Termination Plans

In the event 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.
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.

7.15 Compliance

GlobalSign ensures compliance with applicable law at all times.

Specifically, the GlobalSign TSA is compliant to:

a) 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
b) The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019)
c) The Electronic Identification and Trust Services for Electronic Transactions Regulation 2016 (2016 No.696))
d) ETSI EN 319 401, ETSI EN 319 421, ETSI EN 319 422
e) IETF RFC 3161

GlobalSign maintains its compliance with the requirements identified above via a Qualified Auditor on a bi-annual (eIDAS/UK eIDAS) and contiguous basis.

For eIDAS, 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.

For UK eIDAS, the audit is performed by a conformity assessment body accredited on the basis of EN ISO/IEC 17065 as profiled by ETSI EN 319 403 and in particular against the requirements defined in the UK eIDAS Regulation (eIDAS (UK Legislation) and The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016).

8.0 Contact

GlobalSign NV
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.