GlobalSign

Qualified Signing Service

Practice Statement

Date: April 14th, 2023

Version: 1.0

Document history

Version	Release Date	Status & Description
1.0	14/04/2023	Initial release

Table of Contents

1. Introduction

1.1. Overview

This Qualified Signing Service Practice Statement ("QSSPS") applies to the Qualified Signing Service (“QSS” or “Service”) of GlobalSign NV/SA and affiliated entities ("GlobalSign") for remote signatures based on Qualified Certificates in accordance with the eIDAS and UK eIDAS Regulations.

This document describes GlobalSign’s delivery of signing services and management of the lifecycle of private keys on behalf of Subscribers and aims to comply with the requirements of:

- eIDAS Regulation: Regulation (EU) No 910/2014
- UK eIDAS Regulations: eIDAS (UK Legislation) and The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016
- ETSI TS 119 431-1

This document is binding between GlobalSign and the Subscriber and/or the Relying Party, who uses, relies upon, or attempts to rely upon signing services referring to this document.

For Subscribers, this document becomes effective and binding by accepting the terms and conditions of the Service.

For Relying Parties, this document becomes binding by relying upon a Signature or Certificate from the Service.

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

1.2. Document Name and Identification

This document is the GlobalSign Qualified Signing Service Practice Statement and is identified by the Object Identifier 1.3.6.1.4.1.4146.3.3.

It aims to comply with the EUSCP policy of ETSI TS 119 431-1:

EU SSASC Policy: itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd (3).

Certificates that include the EUSCP Policy OID are governed by this policy.

1.3. PKI Participants

1.3.1. Certification authorities

GlobalSign is a Certification Authority that issues Certificates and performs functions related to Certificate lifecycle management such as Subscriber registration, Certificate issuance, Certificate renewal, Certificate distribution and Certificate revocation.

The GlobalSign CPS governs the Certificates issued for Subscribers of the Qualified Signing Service.

1.3.2. Registration authorities

GlobalSign acts as a Registration Authority for Certificates of the Qualified Signing Service.

GlobalSign may also delegate the identity proofing of both the Organization and the Individual to a Registration Authority under the condition that this Registration Authority meets the identity proofing requirements set by the eIDAS or UK eIDAS Regulations.

See Section 1.3.2 of the CPS.

1.3.3. Subscribers

See definition of "Subscriber" in Section 1.6.1 Definitions.

1.3.4. Relying parties

See definition of "Relying Party" in Section 1.6.1 Definitions.

1.3.5. Other participants

No Stipulation

1.4. Certificate Usage

The GlobalSign CPS governs the Certificates issued for Subscribers of the Qualified Signing Service.

See Section 1.4 of the CPS.

1.5. Policy Administration

1.5.1. Organization Administering the Document

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

1.5.2. Contact Person

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

1.5.3. Person Determining Practice Statement Suitability for the Policy

PACOM1 – CA Governance determines the suitability and applicability of the Policy and the conformance of this practice statement based on the results and recommendations received from a Qualified Auditor.

In an effort to maintain credibility and promote trust in this practice statement and better correspond to accreditation and legal requirements, the PACOM1 – CA Governance shall review this practice statement at least annually and may make revisions and updates to policies as it sees fit or as required by other circumstances.

1.5.4. Practice statement Approval Procedures

PACOM1 – CA Governance reviews and approves any changes to this practice statement. Upon approval of updates by PACOM1 – CA Governance, the new version is published in the GlobalSign Repository at https://www.globalsign.com/repository.

The updated version is binding upon all Subscribers of the Service, including the Subscribers and Relying Parties for the Services provided under a previous version of the practice statement.

1.6. Definitions and Acronyms

1.6.1. Definitions

Certificate: An electronic document that uses a Digital Signature to bind a Public Key and an identity.

Certification Practice Statement: A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying Certificates.

Data To Be Signed Representation: Data formatted which is used to compute the digital signature value (e.g. hash value)

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.

Electronic Seal: Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity and is applied in the name of a legal entity.

Electronic Signature: Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity and is applied in the name of an Individual.

Hardware Security Module: A type of secure crypto processor targeted at managing digital keys, accelerating crypto processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications.

Qualified Certificate: A Certificate that meets the qualification requirements defined by the eIDAS/UK eIDAS Regulation.

Qualified Certificate for Electronic Seals: A Certificate for Electronic Seals, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III of eIDAS/UK eIDAS Regulation.

Qualified Certificate for Electronic Signature: A Certificate for Electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of eIDAS/UK eIDAS Regulation.

Qualified Electronic Seals: An advanced Electronic Seal, which is created by a Qualified Electronic Seal Creation Device, and that is based on a Qualified Certificate for Electronic Seal.

Qualified Electronic Signature: An advanced Electronic Signature that is created by a Qualified Electronic Signature Creation Device, and which is based on a Qualified Certificate for Electronic Signatures.

Qualified Electronic Signature/Seal Creation Device: An electronic signature/seal creation device that meets the requirements as stipulated within Annex II of eIDAS Regulation.

Relying Party: Any natural or legal person that relies on a Certificate.

Service: See QSS

Signature: An Electronic Signature or Electronic Seal.

Signer: An Individual who applies a Signature acting as the Subject if the Subject is a natural person or on behalf of the Subject if the Subject is a legal person.

Subject: The natural or legal person identified in a Certificate as the Subject.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

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

Any capitalized terms used but not otherwise defined herein shall have the meaning set forth in the GlobalSign CPS.

1.6.2. Acronyms

CPS	Certification Practice Statement
DTBS/R	Data To Be Signed Representation
eID	Electronic identification
HSM	Hardware Security Module
OTP	One Time Password
QSCD	Qualified Signature Creation Device
QSS	Qualified Signing Service
SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SIC	Signer's Interaction Component
SSASP	Server Signing Application Service Provider

2. Publication and Repository Responsibilities

2.1. Repositories

This document, the GlobalSign CP, CPS and Subscriber Agreement are published on the public repositories: https://www.globalsign.com/repository and https://www.globalsign.com/en/company/corporate-policies.

GlobalSign refrains from making sensitive and/or confidential documentation including security controls, operating procedures, and internal security policies publicly available. These documents are, however, made available to Qualified Auditors as required during any WebTrust or ETSI audit performed on GlobalSign.

In the event of any inconsistency, the English language version shall prevail.

2.2. Publication of Certificate Information

Certificate information is published in accordance with the GlobalSign CPS.

See Section 2.2 of the CPS for additional information.

2.3. Time or Frequency of Publication

GlobalSign reviews this practice statement at least annually and makes appropriate changes so that GlobalSign operation remains accurate, transparent and complies with external requirements listed in section 1.1 of this document.

New or modified versions of the practice statement are published within seven days after approval.

2.4. Access Controls on Repositories

GlobalSign makes its Repository publicly available in a read-only manner.

Logical and physical security measures are implemented to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3. Service practices

3.1. Introduction

The Qualified Signing Service enables the creation of Qualified Electronic Signatures (for natural persons) and Qualified Electronic Seals (for legal persons) based on Qualified Certificates in accordance with the eIDAS and UK eIDAS Regulations (where applicable).

The Private Keys supporting the Service are stored on a Qualified Signature and Seal Creation Device (QSCD) at GlobalSign, on behalf of the Signer.

During a signing session, the Signature Activation Protocol (SAP) will require data to authorize the signing request using Signature Activation Data (SAD) that takes the data to be signed as Data To Be Signed Representation (DTBS/R) and create a digital signature under signer control.

To ensure (sole) control of the Signer over the Private Key, a mobile application is provided by GlobalSign during enrolment. This mobile application is required to authorize the signatures and generate the Signature Activation Data.

3.2. Signing key initialization

3.2.1. Signing key generation

Subscriber Private Keys are generated and used within the following Qualified Signature Creation Device (QSCD) during the lifecycle of the keys:

Supplier:	Ascertia Ltd.
Name:	ADSS Server SAM Appliance v6.0
Reference:	https://ocsi.isticom.it/documenti/accertamenti/ascertia/ac_rda_eidas_adss_sam_60_v1.0.pdf

The QSCD is initialized with technical mechanisms that require at least two operators and operated in accordance with the operating conditions described in the certification documentation.

Time of generation

A Signer's signing key is generated prior to Certificate generation, but as part of the Certificate generation process.

Cryptographic algorithms and key lengths

GlobalSign supports the following cryptographic algorithms and key lengths:

- Cryptographic algorithm: RSA
- Key length: 2048 bit
- Hashing algorithm: SHA256

Algorithm parameters

Algorithm parameters for signature creation are chosen that are currently resistant and will remain resistant during the lifetime of the Subject's Certificate.

Key protection

Private keys are stored in an encrypted manner, ensuring confidentiality and integrity, in a database outside the QSCD.

3.2.2. Electronic identification means linking

GlobalSign provides a mobile application as electronic identification means to the Signer upon successful enrollment.

The electronic identification means contains an internal reference. This reference is used by the Service to ensure that the person identification data linked to the eID means is the same as the one linked to the Subject of the associated Certificate. The eID also establishes a unique link to the Signer’s private key.

GlobalSign does not delegate the provisioning of the eID or authentication to a third party.

3.2.3. Certificate linking

The link between Signer’s signing keys and public key Certificate is verified before Certificate issuance.

The integrity of the link is protected and the signing key cannot be used by the Signer before the public key Certificate is linked.

3.2.4. Electronic identification means provision

The mobile application provided as eID means requires activation using two OTPs:

- SMS to the Signer’s mobile phone number
- Email to the Signer’s email address

3.3. Signing key life-cycle operational requirements

3.3.1. Signature activation

Identification and authentication

The Service requires successful identification and authentication of the Subject before allowing any actions that can impact the sole control of any signing key.

Two OTPs will be submitted to the Subject as part of enrolment of the mobile device for two factor authentication.

Upon provisioning of the mobile application, biometric approval or PIN will need to be set for future authorization of signatures.

Protection against attacks

The Service provides protection of signing data while in transit, ensuring both confidentiality and integrity.

Access controls to avoid other Signer’s key access.

The QSCD ensures sole control of the Signer over the signing key. It ensures integrity and confidentiality of the signing key and the link between the Signer and the signing key.

DTBS only signed by signing key belonging to Signer.

The Signer, using the mobile application, communicates with the Service to submit the signature activation data (SAD). The SAD binds together the Signer authentication with the signing key and the data to be signed, i.e., DTBS/R.

Present SAD to SAM for authentication and activating signing key.

The Service requires the Signer to provide the SAD through the signature activation protocol (SAP) for authentication to activate the signing key.

Controls based on risk assessment for threats.

The Service implements measures, based on risk assessment, to protect against threats to the SAD.

DTBS linked by SAP with signing key.

The QSCD ensures that the activated signing key can only be used to sign the DTBS/R received as part of the signature activation protocol.

Certificate validity

The validity of the public key Certificate is verified before using the corresponding signing key.

Signing key requires Signer's consent.

The Signer shall confirm the signing action within the mobile application using biometric or device PIN authentication.

3.3.2. Signing key deletion

GlobalSign will destroy the Subject private key if:

- The Certificate linked to the private key expires; or
- Subject requests deletion of the account.

The link between the signing key and the Signer is maintained after signing operations.

3.3.3. Signing key backup and recovery

All private keys are securely stored during the entire lifecycle. Subscriber signing keys are generated in the HSM of the QSCD and encrypted with a key held in the HSM. The encrypted material is then backed up securely to the database, which is replicated for availability purposes.

Encryption of private keys relies only on cryptographic algorithms, and algorithm parameters of equivalent or higher strength.

Backup, storage, and recovery of private keys is only performed by authorized personnel. Keys used to protect both Subscriber and operational keys are backed up, stored and reloaded under at least dual control. Keys are only held outside the QSCD in protected form.

The number of duplicated datasets is limited to the minimum needed to ensure continuity of the Service.

3.4. EU specific requirements

3.4.1. SSASP as a Qualified TSP

For the status of GlobalSign as a Qualified Trust Service Provider, please refer to the eIDAS and UK eIDAS trusted lists.

3.4.2. Policy name and identification

GlobalSign aims to comply with the EUSCP: EU SSASC Policy, which itself includes all requirements of the NSCP: Normalized SSASC Policy.

3.4.3. General requirements

See Section 3 for the certification of the Qualified Signature Creation Device.

3.4.4. Signing key generation

Signer's signing keys are generated in a QSCD, which is operated in accordance with the operating conditions.

3.4.5. Signature activation

Signer's signing keys are used in a QSCD, which is operated in the configuration as described in the certification guidance documentation or in an equivalent configuration which achieves the same security objective.

Cryptographic strength

The SAP provides mechanisms with sufficient cryptographic strength to protect the authentication factors against compromise by the protocol threats as well as trusted third-party impersonation attacks.

To authorize the signature, the Signer must authenticate to the mobile device to access the authorization key held in the mobile device's secure storage. The user authenticates to the mobile device using biometric techniques or the mobile device passcode.

Threat mitigation

The SAP is protected against replay, bypass, and forgery attack, using a salt, a validity period and the authorization signature of the Signer.

Environment protection

The SAM is integrated in the QSCD and is a trustworthy system assured to EAL 4 in accordance with ISO/IEC 15408 and Common Criteria certified to protection profile "prEN 419 221-5, v015, 29 November 2016".

Protection against tampering

The SAP is designed such that the SAD is reliably protected against duplication, tampering and replay attacks, through a cryptographic key stored in the mobile device secure storage.

Protection against attacker

The SAP ensures that the Signer can reliably protect the signing key activation by the SAD against an attacker with high attack potential.

3.4.6. Signature activation data management

Signature activation data format

The signed SAD value cryptographically binds together at least the following attributes:

- The Signer's identity and authentication (via the signature on the SAD value);
- The hash of the data to be signed remotely (DTBS/R);
- Random salt information to prevent replay attacks; and
- The Signer's signing key.

Signature activation data collection and generation

The SAD is generated in the Signer's environment by the Signer's Interaction Component (SIC) under control of the Signer.

The mobile application is the Signer's Interaction Component. It is used locally by the Signer to communicate with the SAM. The mobile application authorizes the remote signing actions by digitally signing authorization responses using an authorization key pair held securely in the mobile device's secure storage.

Signature activation data parameters

The SAD links with a high level of confidence at least the following parameters:

- A given DTBS/R or a set of DTBS/R;
- Items to identify the authenticated Signer; and
- The selected signing key.

Signature activation data usage

The SAD is used to activate the signing key only if Signer authentication succeeds by computing SAD after successful authentication.

Signature activation data destination

The Signature Activation Data (SAD) is passed to the Signature Activation Module (SAM) via the Signature Activation Protocol (SAP).

Natural person: signature activation data collection and protection

The creation of the electronic signature or electronic seal is always initiated by a natural person.

The SAD:

- Is collected in a way that is under the control of the Signer with a high level of confidence;
- Is protected so that any keys held within devices are secure; and
- Protects any secret (either single-use or long-term) against replay, bypass and forgery attack between Signer and the remote QSCD.

To be able to authorize a remote signature, the mobile application is first registered with the QSCD against the Signer's account. The signing authorization is in accordance with EN 419 241-1.

During a remote signing operation, the Signer will be asked to launch the mobile application to download the authorization request for the Signer to view and authorize.

Natural person: signature activation data submission under sole control

For the mobile application to sign the authorization response, the Signer must authenticate to the mobile device to access the authorization key held in the mobile device's secure storage. The Signer authenticates to the mobile device using biometric techniques or the mobile device passcode.

Signature activation data protection after activation

The SAD is verified such that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication for signature activation.

4. Facility, management, and operational controls

4.1. General

GlobalSign maintains a security program, including risk assessment covering the risks related to the Qualified Signing Service.

Based on this assessment, GlobalSign develops, implements, and maintains a security plan with security procedures, measures, and products to manage and control the risks identified during the risk assessment, commensurate with the sensitivity of the Qualified Signing Service processes.

GlobalSign also implements controls to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities.

See Section 5.0 of the CPS for additional information.

4.2. Physical security controls

GlobalSign maintains physical and environmental security policies for systems supporting the Service 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.

See Section 5.1 of the CPS for additional information.

4.3. Procedural controls

Access to systems supporting the Service is restricted in accordance with the access control policy.

GlobalSign administers user access of the systems, including user account management and timely removal of access.

See Section 5.2 of the CPS for additional information.

4.4. Personnel controls

GlobalSign ensures that employees and contractors support the trustworthiness of the operations through a combination of training, experience and qualification requirements and background checks.

See Section 5.3 of the CPS for additional information.

4.5. Audit logging procedures

The following events are logged:

- Changes relating to the security policy;
- System start-up and shutdown;
- System crashes and hardware failures;
- Firewall and router activities and SSASC system access attempts;
- Significant QSCD environmental, key management events (generation, usage, and destruction);
- Signer signing events (e.g., successful signing with a Signer’s signing key and DTBS/R request management);
- Signer authentication during SAP;
- Signer’s SAD management by QSCD;

- Start up and shut down of the audit data generation function;
- Changes of the audit parameters; and
- Access attempts to the QSCD.

Signing events include data to associate the Certificate to the signing key.

All audit records contain the following parameters:

- Date and time of event;
- Type of event;
- Identity of the entity (e.g., user, administrator, process) responsible for the action; and
- Success or failure of the audited event.

If the Service is unable to pass audit information to external storage the failure of the operation is recorded in the logs and an administrative alert is generated and sent to specified system operators.

Authorized personnel will act upon the event of failing to pass audit information to external storage to investigate and resolve the issue.

Audit data is written using an append only mechanism and stored with integrity protection controls.

Access to audit records is limited to authorized personnel in trusted roles.

See Section 5.4 of the CPS for additional information.

4.6. Records archival

To ensure time accuracy of audited events, a time source suitably synchronized with a standard time source is used.

See Section 5.5 of the CPS for additional information.

4.7. Key changeover

See Section 5.6 of the CPS for additional information.

4.8. Compromise and disaster recovery

See Section 5.7 of the CPS for additional information.

4.9. SSASP service termination

When it is necessary to terminate SSASP activities, the impact of the termination will be minimized as much as possible considering the prevailing circumstances and is Subject to the applicable Service Agreements.

GlobalSign has a procedure in place that it will follow when terminating all or a portion of its remote signing operations. The procedure must, at a minimum:

- Ensure that any disruption caused by the termination of SSASP activities is minimized as much as possible;
- Ensure that archived records of the service are retained;
- Ensure that prompt notification of termination is provided to Subscribers and other relevant stakeholders;

- Ensure Certificate status information services are provided and maintained for the applicable period after termination, including, if applicable, transferring Certificate status information services to another GMO Internet Group entity;

- Ensure that a process for destroying all private keys used for signing at the time of termination is maintained;

- Notify all auditors, including the eIDAS/UK eIDAS Conformity Assessment Bodies;

- Notify the Belgian eIDAS supervisory body (FPS Economy, SMEs, Self-employed and Energy - Quality and Safety);

- Notify the United Kingdom eIDAS supervisory body (Information Commissioner's Office); and

- Notify other relevant Government and Certification bodies under applicable laws and related regulations.

5. Technical security controls

5.1. Systems and security management

GlobalSign ensures that all operators and administrators act in the capacity of a trusted role. Trusted roles are such that no conflict of interest is possible, and the roles are distributed such that no single person can circumvent the security of the signing system.

Trusted roles include:

- **Security Officers:** have overall responsibility for administering the implementation of the security policies, practices and have access to security related information.

- **System Administrators (Infra Engineers)**: are authorized to install, configure and maintain the QSCD but with controlled access to security-related information.

- **System Operators (Infra Operators)**: are responsible for operating the QSCD on a day-to-day basis and are authorized to perform system backup and recovery.

- **System Auditors (Auditors)**: are authorized to view archives and audit logs of the QSCD for the purposes of auditing the operations of the system in line with security policy.

GlobalSign enforces role separation either by the CA equipment (logically) or procedurally or a combination of both means. Individual CA personnel are specifically assigned to the roles defined above.

5.1.1. Privileged and non-privileged roles

Security officers and system administrators are privileged system users. System operators and system auditors have privileged roles but are not able to administer or configure the QSCD.

Measures:

- A privileged user is not able to take on all the privileged roles.

- Users shall not be associated with both privileged and non-privileged roles

- Individuals that are part of a group of privileged system users are named and trained persons.

- Only privileged users have physical access to the hardware and can administer the QSCD.

- Only privileged users have extensive privileges to administer the QSCD through all relevant applications and interfaces.

The Service supports the following non-privileged roles:

- **Signer:** authorized to use the QSCD by passing the SAD as part of the SAP to sign the DTBS/R.
- **Business application:** authorized to send the DTBS/R request to the QSCD in order to be signed by a Signer.
- **RA:** authorized to send the public key Certificate to the QSCD in response to a Certificate signing request.

5.2. Systems and operations

GlobalSign operates the signature creation systems in accordance with the operating conditions to ensure the QSCD is:

- Correctly and securely operated;
- Deployed in such a way that the risk of systems failure is minimized; and
- Protected against viruses and malicious software to ensure the integrity of the systems and the information the systems process.

The systems are synchronized with NTP in accordance with manufacturer’s documentation.

5.3. Computer security controls

Access to GlobalSign systems is limited to authorized individuals through a combination of logical access and network-based access controls.

Notification and alerting is enabled to notify in a timely manner about unusual events which can have impact on the ability of the systems supporting the signing service to meet their security requirements.

See Section 6.5 of the CPS for additional information.

5.4. Life cycle security controls

GlobalSign uses trustworthy systems and products that are protected against modification. Technical security and reliability of the processes is ensured through systems development, security management and lifecycle security controls.

See Section 6.6 of the CPS for additional information.

5.5. Network security controls

All GlobalSign systems implement appropriate security measures to ensure they are guarded against denial of service and intrusion attacks.

See Section 6.7 of the CPS for additional information.

6. Compliance audit and other assessment

Full details on GlobalSign’s compliance assessments, including assessment frequencies and auditor details and qualifications are covered in Section 8 of the CPS.

7. Other business and legal matters

7.1. Fees

GlobalSign charges fees for its services in line with Section 9.1 of the CPS.

7.2. Financial responsibility

GlobalSign maintains commercial general liability insurance with policy limits. See Section 9.2 of the CPS for more details.

7.3. Confidentiality of business information

Full details on the confidentiality of business information can be found in Section 9.3 of the CPS.

7.4. Privacy of personal information

GlobalSign protects personal information in accordance with its Privacy Policy published on GlobalSign’s website at https://www.globalsign.com/repository.

7.5. Intellectual property rights

See Section 9.5 of the CPS.

7.6. Representations and warranties

Please refer to the CPS for the practices of the Certificates supporting the Qualified Signing Service.

See Section 9.6 of the CPS.

7.7. Disclaimers of warranties

See Section 9.7 of the CPS.

7.8. Limitations of liability

The liability of GlobalSign is limited in accordance with article 13 of the eIDAS or UK eIDAS Regulations.

See Section 9.8 of the CPS for additional information.

7.9. Indemnities

See Section 9.9 of the CPS.

7.10. Term and termination

See Section 9.10 of the CPS.

Changes to this practice statement become effective immediately upon publication.

7.11. Individual notices and communications with participants

See Section 9.11 of the CPS.

7.12. Amendments

See Section 9.12 of the CPS.

Changes to this practice statement become effective immediately upon publication.

7.13. Dispute resolution procedure

See Section 9.13 of the CPS.

7.14. Governing law

See Section 9.14 of the CPS.

7.15. Compliance with applicable law

For details on applicable laws and their coverage by GlobalSign, see Section 9.15 of the CPS.

7.16. Miscellaneous provisions

See Section 9.16 of the CPS.

8. Other provisions

8.1. Organizational

The Service is operated in a nondiscriminatory manner.

In providing the Qualified Signing Service, GlobalSign:

- Operates the services in a non-discriminatorily manner;
- Makes its services accessible to all applicants that agree to abide by their obligations as specified in the terms and conditions;
- Maintains sufficient financial resources and/or obtain appropriate liability insurance, in accordance with applicable law, to cover liabilities arising from its operations and/or activities (see the CPS, Section 9.2 for full details);
- Has the financial stability and resources required to operate in conformity with this policy (see the CPS, Section 9.2 for full details).
- Has policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters (see the CPS, Section 9.13 for additional information).
- Has a documented agreement and contractual relationship in place where the provisioning of any services herein involves subcontracting, outsourcing or other third-party arrangements.

8.2. Additional testing

GlobalSign provides test profiles to customers for testing the GlobalSign Qualified Signing Service.

Test profiles can be recognized through the inclusion of “testing” in the Certificate Common Name or Organizational Unit field.

8.3. Disabilities

No stipulation.

8.4. Terms and conditions

Terms and conditions for Subscribers of the GlobalSign Qualified Signing Service are available separately.

Relying Party terms and conditions are covered in this practice statement.