GlobalSign
PKI Disclosure Statement

Date: April 14, 2023

Version: v2.0

Table of contents

1. Introduction

This PKI Disclosure Statement (PDS) applies to the Qualified certificates issued by GlobalSign NV/SA and affiliated entities (“GlobalSign”), acting as a Trust Service Provider. The activities of GlobalSign related to the provisioning of Qualified certificates are referred to as the “Service”.

The purpose of this document is to summarize the key points of the Service for the benefit of Subscribers and Relying Parties. This document does not replace the applicable agreements and CPS (see 10. Applicable Agreements, CPS/CP). Any terms used but not defined herein shall have the meaning ascribed to them in the CPS.

Qualified certificates are certificates issued in accordance with the eIDAS or UK eIDAS regulations (“the eIDAS Regulations”):

“eIDAS Regulation (eIDAS)” means The 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”.

Certificates issued in accordance with the eIDAS regulation are issued by GlobalSign NV/SA.

“UK eIDAS Regulations (UK eIDAS)” means The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019 and The Electronic Identification and Trust Services for Electronic Transactions Regulation 2016 (2016 No.696).

Certificates issued in accordance with the UK eIDAS regulations are issued by GMO GlobalSign LTD.

2. Contact Information

GlobalSign can be contacted at the following address:

GlobalSign NV/SA
Diestsevest 14,
3000 Leuven,
Belgium
Tel: +32 (0) 16 891900
Fax: + 32 (0) 16 891909

And

GMO GlobalSign Ltd
Springfield House,
Sandling Road, Maidstone, Kent,
ME14 2LP, United Kingdom
Tel: +44 1622 766766
Fax: +44 1622 662255

For any queries regarding this PKI Disclosure Statement or other documents related to this Service, please send an email to legal@globalsign.com .

Due to the nature of revocation requests and the need for efficiency, GlobalSign provides automated mechanisms for requesting and authenticating revocation requests. The primary method for Subscribers is through the account used to issue the Certificate that is requested to be revoked.

Anti-Malware Organizations, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may report suspected Private Key Compromise, Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates by sending email to: report-abuse@globalsign.com.

3. Certificate Types

GlobalSign offers the following Qualified certificate types:

- Qualified certificates for electronic signatures
- Qualified certificates for electronic seals
- Qualified certificates for website authentication

Certificates are offered to the general public (private companies, public entities, professionals, private persons, etc.), under the conditions published in the repository.

eIDAS

Certificates issued in accordance with the eIDAS Regulation are identified by the following policies:

OID	Description
1.3.6.1.4.1.4146.1.40.36	**eIDAS Qualified Certificates - QSCD**
1.3.6.1.4.1.4146.1.40.36.1	Qualified Certificates for Electronic Signatures
1.3.6.1.4.1.4146.1.40.36.2	Qualified Certificates for Electronic Seals
1.3.6.1.4.1.4146.1.40.37	**eIDAS Qualified Certificates – Non QSCD**
1.3.6.1.4.1.4146.1.40.37.1	Qualified Certificates for Electronic Signatures
1.3.6.1.4.1.4146.1.40.37.2	Qualified Certificates for Electronic Seals
1.3.6.1.4.1.4146.1.40.37.3	Qualified Certificates for Electronic Seals - Open Banking
1.3.6.1.4.1.4146.1.40.38	**eIDAS Qualified Certificates – Remote QSCD**
1.3.6.1.4.1.4146.1.40.38.1	Qualified Certificates for Electronic Signatures
1.3.6.1.4.1.4146.1.40.38.2	Qualified Certificates for Electronic Seals
1.3.6.1.4.1.4146.1.40.39	**Qualified Certificates for Authentication**
1.3.6.1.4.1.4146.1.40.39.1	Qualified Certificates for Authentication (Natural Persons)
1.3.6.1.4.1.4146.1.40.39.2	Qualified Certificates for Authentication (Legal Persons)
1.3.6.1.4.1.4146.1.40.39.3	Qualified Certificates for Website Authentication (QWAC)
1.3.6.1.4.1.4146.1.40.39.4	Qualified Certificates for Website Authentication (QWAC) – Open Banking
1.3.6.1.4.1.4146.1.40.41	**eIDAS Qualified Certificates – Remote Non QSCD**
1.3.6.1.4.1.4146.1.40.41.1	Qualified Certificates for Electronic Signatures
1.3.6.1.4.1.4146.1.40.41.2	Qualified Certificates for Electronic Seals

The issuing CAs are published in the repository and on the website of FPS Economy, SMEs, Self-employed and Energy - Quality and Safety at https://tsl.belgium.be/.

UK eIDAS

Certificates issued in accordance with the UK eIDAS Regulations are identified by the following policies:

OID	Description
1.3.6.1.4.1.4146.1.44.36	**UK eIDAS Qualified Certificates – QSCD**
1.3.6.1.4.1.4146.1.44.36.1	Qualified Certificates for Electronic Signatures
1.3.6.1.4.1.4146.1.44.36.2	Qualified Certificates for Electronic Seals
1.3.6.1.4.1.4146.1.44.37	**UK eIDAS Qualified Certificates – Non QSCD**
1.3.6.1.4.1.4146.1.44.37.1	Qualified Certificates for Electronic Signatures
1.3.6.1.4.1.4146.1.44.37.2	Qualified Certificates for Electronic Seals
1.3.6.1.4.1.4146.1.44.37.3	Qualified Certificates for Electronic Seals - Open Banking
1.3.6.1.4.1.4146.1.44.38	**UK eIDAS Qualified Certificates – Remote QSCD**
1.3.6.1.4.1.4146.1.44.38.1	Qualified Certificates for Electronic Signatures
1.3.6.1.4.1.4146.1.44.38.2	Qualified Certificates for Electronic Seals
1.3.6.1.4.1.4146.1.44.39	**UK eIDAS Qualified Certificates for Authentication**
1.3.6.1.4.1.4146.1.44.39.1	Qualified Certificates for Authentication (Natural Persons)
1.3.6.1.4.1.4146.1.44.39.2	Qualified Certificates for Authentication (Legal Persons)
1.3.6.1.4.1.4146.1.44.40	**UK eIDAS Qualified Certificates for Website Authentication (QWAC)**
1.3.6.1.4.1.4146.1.44.40.1	Qualified Certificates for Website Authentication (QWAC)
1.3.6.1.4.1.4146.1.44.40.2	Qualified Certificates for Website Authentication (QWAC) – Open Banking
1.3.6.1.4.1.4146.1.44.41	**UK eIDAS Qualified Certificates – Remote Non QSCD**
1.3.6.1.4.1.4146.1.44.41.1	Qualified Certificates for Electronic Signatures
1.3.6.1.4.1.4146.1.44.41.2	Qualified Certificates for Electronic Seals

The issuing CAs are published in the repository and on the website of https://ico.org.uk/for-organisations/guide-to-eidas/uk-trusted-list/

4. Validation procedures

GlobalSign verifies by appropriate means and in accordance with national law, the identity and, if applicable, any specific attributes of the natural or legal person to whom the Qualified certificate is issued.

The identity is verified either by GlobalSign directly or by relying on a third party in accordance with national law, by the physical presence of the natural person or of an authorized representative of the legal person; or equivalent methods supported by article 24.1 of the eIDAS Regulations.

See Section 3.2 of the CPS.

5. Usage

Conditions apply to the use of Qualified certificates depending on their policy:

- QCP-n and QCP-l are aimed to support the advanced electronic signatures based on a Qualified certificate defined in articles 26 and 27 of the eIDAS Regulations.
- QCP-n-qscd and QCP-l-qscd are aimed to support qualified electronic signatures and seals such as defined in article 3 (12) and 3 (27) of the eIDAS Regulations.
- QEVCP-w are aimed to support website authentication based on a Qualified certificate defined in articles 3 (38) and 45 of the eIDAS Regulations.

See Section 1.4 of the CPS.

6. Reliance Limits

See Section 9.8 of the CPS.

7. Subscriber's Obligations

The certificate subscriber (and if applicable, Subject) must:

- Provide GlobalSign with accurate and complete information during the certificate request, particularly with regards to registration;
- Only use the key pair in accordance with any limitations notified to Subscriber and;
- Use private keys only for electronic signatures or electronic seals, depending on the certificate policy;
- Adopt suitable measures to prevent unauthorized use of the private key;
- When the Subject is a natural person: maintain the private key under the Subject's sole control;
- When the Subject is a legal person: maintain the private key under the Subject's control;
- Notify GlobalSign without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:
    - The private key has been lost, stolen, potentially compromised;
    - Control over the Subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons;
    - any information contained in its certificate is inaccurate or no longer valid: Inaccuracy or changes to the certificate content, as notified to the Subscriber or to the Subject;
- Following compromise of the Subject's private key, to immediately and permanently discontinue the use of this key, except for key decipherment;
- In the case of being informed that the Subject's certificate has been revoked, or that the issuing CA has been compromised, to ensure that the private key is no longer used by the Subject;
- If Subscriber or Subject generates the Subject's keys, follow the recommendations of ETSI TS 119 312 for the key length and key generation algorithm for the uses of the certified key as identified in the CPS during the validity time of the certificate; and
- If Subscriber or Subject generates the Subject's keys and the certificate policy requires a QSCD, generate and store private keys and create signatures within a certified QSCD, which has either been supplied or approved in writing by GlobalSign.

For more information, please refer to the Subscriber Agreement and Section 9.6.3 of the CPS.

8. Certificate Status Checking Obligations of Relying Parties

Any natural person, legal person or entity relying on a certificate must:

- Verify the validity or revocation of the certificate using current revocation status information. Such verification can be performed by consulting the list of revoked certificates (CRL) published by the CA or by querying the OCSP service provided by the CA, at the addresses (URLs) contained within the certificate;
- Take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or the terms and conditions supplied; and
- Take any other precautions prescribed in agreements or elsewhere.

As a condition for a certificate to be relied upon as an EU or UK Qualified Certificate, the trust anchor for the validation of the certificate shall be as identified in a service digital identifier of an appropriate EU or UK trusted list entry for a QTSP (see ETSI TS 119 612).

9. Limited Warranty and Disclaimer/Limitation of Liability

GlobalSign's liability is limited in accordance Article 13 of the eIDAS or UK eIDAS Regulations.

See Sections 9.6 and 9.8 of the CPS.

10. Applicable Agreements, CPS/CP

The agreements and conditions applicable to the Service are published in the repository:

- GlobalSign Certificate Policy (CP)
- GlobalSign Certification Practice Statement (CPS)
- Subscriber Agreement
- Privacy Policy

11. Privacy Policy

GlobalSign complies with EU Regulation No. 679/2016 and UK Data Protection Act 2018, and with the recommendations and provisions of the Belgian Data Protection Authority and ICO (Information Commissioner's Office). GlobalSign protects personal information in accordance with its Privacy Policy published in the repository.

Audit records of registration information, acceptance of the terms and conditions and events related to the life cycle of the certificate are retained for 10 years.

12. Refund Policy

If a subscriber is not completely satisfied with the issued certificate, the subscriber may request a refund within 7 days of the certificate being issued. Any refunds will be net of any fees incurred by GlobalSign.

13. Applicable Laws, Complaints and Dispute Resolution

The Service is governed, construed, and interpreted in accordance with the laws of the country set forth in the Subscriber Agreement.

14. TSP and Repository Licenses, Trust Marks, and Audit

The Service is subject to conformity assessment, according to European norms ETSI EN 319 411-1 and ETSI 319 411-2, by an independent, qualified, and accredited auditor, as required by both the eIDAS Regulation and UK eIDAS Regulations.