GlobalSign
PKI Disclosure Statement

Date: December 7th, 2018

Version: v1.1

Introduction

This document is the PKI Disclosure Statement, as required by European standard ETSI EN 319 411-1, related to the certification service offered by the Trust Service Provider **GlobalSign NV/SA.**, a Belgian company with VAT number BE0459.134.256.

In the following, the certification service is also referred to by "CA service" (Certification Authority). 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" is referred to by "eIDAS Regulation."

The purpose of this document is to summarise the key points of the CA service for the benefit of Subscribers and Relying Parties. This document does not substitute or replace the Terms and Conditions of the CA service nor the Certification Practice Statement (CPS) published on the CA website (see further on).

CA Contact Information

The CA can be contacted at the following address:

GlobalSign NV
Martelarenlaan 38,
3010 Leuven,
Belgium
Tel: +32 (0) 16 891900
Fax: + 32 (0) 16 891909

For any queries regarding this PKI Disclosure Statement or other documents of GlobalSign's CA 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 is through the GCC account used to issue the Certificate that is requested to be revoked. Alternative out of band methods may be used, such as receipt of a fax/letter/phone call, the origins of which must be authenticated using shared secrets from the GCC account. Alternatively, where GCC accounts are not provided, methods may be used which rely on a demonstration of control of one or more elements of the Subject DN of the Certificate.

Certificate Types, Validation Procedures and Usage

GlobalSign issues **qualified certificates** according to European standard ETSI EN 319 411 and other related standards. Certificates are offered to the general public (private companies, public entities, professionals, private persons, etc.), at the conditions published on the CA website.

All certificates are signed with at minimum a hashing function of SHA-256. For further information on the supported certificate policies (e.g. their respective OIDs and other features) see the documentation published on the CA website at https://www.globalsign.com/repository/.

The certificates of GlobalSign issuing CAs are published on the CA website and on the website of FPS Economy, SMEs, Self-employed and Energy - Quality and Safety at https://tsl.belgium.be/ (see the "Trusted List").

To allow validation of certificates, GlobalSign offers an on-line status checking service based on the OCSP standard and may offer Certificate Revocations List (CRL). The relevant URLs will be included in each certificate, respectively in either/both the AuthorityInformationAccess and CRLDistributionPoints extensions.

Reliance Limits

Certificates are issued for qualified electronic signatures and electronic seals.

All records pertaining to the life-cycle of certificates, as well as all the CA service audit logs, are retained by GlobalSign for at least 10 years.

Subscriber's Obligations

The certificate subscriber must:

- provide complete, accurate and truthful information to the CA at the time of certificate request;
- use its private keys only for the purposes and in the ways allowed by the CPS;
- adopt suitable measures to prevent any non-authorized use of its private keys;
- (for certificates that require use of a signature device) if it generates its private key by itself, generate it within a signature device approved by the CA;
- up to the date of certificate expiration, promptly inform the CA in the following cases:
    - any loss, theft or damage of its signature device;
    - any loss of the exclusive control of its private key, e.g. because of compromise of the activation data (e.g. PIN) of its signature device;
    - any information contained in its certificate is inaccurate or no longer valid:
- in the case of compromise of its private key (e.g. because the PIN of its signature device gets lost or disclosed to non-authorized people), immediately cease any use of such private key and make sure that it will no longer be used.
- should subscriber re-use a hardware token they must ensure it is both qualified (QSCD) and seek approval for its use in advance from GlobalSign

For further information, please refer to the GlobalSign CPS.

Certificate Status Checking Obligations of Relying Parties

Any natural person, legal person or entity replying on the information contained in certificates (in short, "Relying Parties") must verify that certificates are not suspended or revoked. 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 themselves.

Limited Warranty and Disclaimer/Limitation of Liability

For warranty and liability limitations, please refer to the Terms and Conditions of the Qualified CA service published on the GlobalSign website at https://www.globalsign.com/repository/.

Applicable Agreements, CPS/CP

The agreements and conditions applying to the CA service are found in the following documents, published on the GlobalSign website at https://www.globalsign.com/repository/:

- GlobalSign Certification Practice Statement (CPS)
- Subscriber Agreement
- Enterprise PKI Service Agreement
- Agreement for Issuance of Qualified Certificate
- Relying Party Agreement
- Warranty Policy
- Privacy Policy
- GlobalSign Certificate Center Terms & Conditions
- GlobalSign Payment Terms
- GlobalSign Refund & Cancellation Policy

The supported Certificate Policies (CP) are described in the CPS; see also section 3 above.

Privacy Policy

GlobalSign complies with EU Regulation No. 679/2016, and with the recommendations and provisions of the Belgian Data Protection Authority. GlobalSign protects personal information in accordance with its Privacy Policy published on GlobalSign CA's web site at https://www.globalsign.com/repository.

All records relating to qualified certificates issued by GlobalSign (e.g. evidence of the identity of subscribers; certificate issuance requests, including acceptance of the Terms and Conditions; certificate revocation requests; etc.) are retained by GlobalSign for 10 years.

Refund Policy

For the refund policy, please refer to the GlobalSign Refund & Cancellation Policy service published on the GlobalSign website at https://www.globalsign.com/repository/.

Applicable Laws, Complaints and Dispute Resolution

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

TSP and Repository Licenses, Trust Marks, and Audit

GlobalSign is a Certification Service Provider (Certification Authority) active since 1999. The GlobalSign CA service is subject to conformity assessment every two years, according to European norms ETSI EN 319 411-1 and ETSI 319 411-2, by an independent, qualified and accredited auditor, as required by the eIDAS Regulation.