

Independent Assurance Report

To the management of GlobalSign NV/SA ("GlobalSign")

Scope

We have been engaged, in a reasonable assurance engagement, to report on GlobalSign management's assertion to destroying all copies of 19 Issuing CA (ICA) keys, as enumerated in [Appendix A](#), during multiple key ceremonies throughout the period July 28, 2020 to September 16, 2020, GlobalSign has:

- ▶ followed the CA key destruction requirements in its:
 - ▶ [Certificate Policy v6.4](#)
 - ▶ [Certification Practice Statement v9.4](#)
- ▶ included appropriate, detailed procedures and controls in its Key Destruction script(s)
- ▶ maintained effective controls to provide reasonable assurance that the GlobalSign ICA keys in scope of the key destruction ceremony were destroyed in conformity with the procedures described in its Certificate Policy (CP), Certification Practices Statement (CPS), and Key Destruction script(s)
- ▶ performed, during key destruction process, all procedures required by the Key Destruction script(s)
- ▶ destroyed the GlobalSign ICA keys in scope of the key destruction ceremony in a physically secured environment as described in its CP/CPS
- ▶ destroyed the GlobalSign ICA keys in scope of the key destruction ceremony using personnel in trusted roles under multiple person control and split knowledge

in accordance with ICA Key Destruction Criterion 4.6 of the [WebTrust Principles and Criteria for Certification Authorities, Version 2.2](#).

Certification Authority's responsibilities

GlobalSign's management is responsible for its assertion, including the fairness of its presentation, and for destroying its CA keys in accordance with the Criteria.

Our independence and quality control

We have complied with the independence and other ethical requirements of the *Code of Ethics for Professional Accountants* issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies International Standard on Quality Control 1, and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Auditor's responsibilities

Our responsibility is to express an opinion on management's assertion based on our procedures. We conducted our procedures in accordance with International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, management's assertion is fairly stated, and, accordingly, included:

1. obtaining an understanding GlobalSign's documented plan of procedures to be performed for the destruction of the GlobalSign ICA keys;
2. reviewing the detailed CA key destruction script(s) for conformance with industry standard practices;
3. testing and evaluating, during the ICA keys destruction process, the effectiveness of the controls defined in the key destruction scripts and the actual destruction of the key material;
4. observation of all procedures performed during the ICA keys destruction process to ensure that the procedures actually performed on July 28, 2020; August 3, 2020; August 26, 2020 and September 16, 2020 were in accordance with the Key Destruction script(s) for the GlobalSign ICAs and
5. performing such other procedures as we considered necessary in the circumstances.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Opinion

In our opinion, throughout the period July 28, 2020 to September 16, 2020, GlobalSign management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with CA Key Destruction Criterion 4.6 of the [WebTrust Principles and Criteria for Certification Authorities, Version 2.2](#)

This report does not include any representation as to the quality of GlobalSign's services beyond those covered by CA Key Destruction Criterion 4.6 of the [WebTrust Principles and Criteria for Certification Authorities, Version 2.2](#), nor the suitability of any GlobalSign's services for any customer's intended purpose.

EY Bedrijfsrevisoren BV
Diegem, Belgium

Christel Weymeersch, Partner*

October 16, 2020

* Acting on behalf of a BV

Appendix A - identifying information

CA hierarchy

The following table provides an overview of the CAs:

Name	Subject Key Identifier
GlobalSign Qualified Timestamping ECC CA 2020	85:a0:9d:62:2d:a1:1d:77:5a:d4:c7:4d:7f:93:a5:d1:ba:2e:e3:48
GlobalSign HV ECC DV SSL CA 2018	2b:6a:46:49:be:68:76:90:9c:be:47:9c:6c:10:48:b1:c2:ba:6d:b3
GlobalSign R6 RSA EV SSL CA 2019	db:3c:67:3c:93:76:0e:38:a5:b1:ce:f4:45:9d:0f:60:aa:16:af:0a
GlobalSign R6 Admin CA - SHA256 - G3	81:49:5c:e9:05:bf:0c:88:a0:38:96:b2:5d:41:03:5a:e9:ff:d7:87
GlobalSign RSA EV SSL CA 2019	bc:f4:83:6b:6a:53:6c:17:05:bd:d4:bf:0c:b3:16:f1:0f:63:c5:df
GlobalSign ECC EV SSL CA 2019	f9:ec:81:c9:90:a3:04:3c:7c:a4:ec:45:c9:56:a8:e2:ca:df:c9:64
GlobalSign Qualified CA 2	81:43:71:1e:bb:f9:22:bc:ac:3a:36:15:d5:b2:8e:37:54:95:b9:16
GlobalSign Qualified CA 3	a7:d2:4c:1e:f6:e6:b7:b8:6d:14:23:ae:e8:1c:aa:78:42:6a:89:d5
GlobalSign PersonalSign 2 CA - SHA256 - G4	ac:a9:d2:3e:25:5c:a3:e7:65:08:f9:57:64:e4:59:ae:0b:52:57:4e
Trafigura PTE Ltd S/MIME ICA 2020	f9:76:ab:89:d7:42:0d:ea:4c:de:38:6b:c6:3b:86:4a:9c:36:e9:66
GlobalSign Qualified Time Stamping CA 2019	71:4b:5c:ac:76:e2:a1:4d:e1:b3:e9:8c:f2:c2:f9:b7:b0:07:40:d3
MSC Trustgate.com RSA AATL CA 2019	eb:ae:6b:85:2f:70:10:16:ec:28:59:5c:a4:3d:b7:7a:74:31:a9:6e
VWFS CA for AATL	85:88:43:b4:7d:34:84:6f:c5:17:2d:b9:06:1e:56:20:70:d7:e8:13
GlobalSign PersonalSign 1 CA - G3	e9:14:6a:00:48:d0:40:24:98:72:cd:76:13:0c:59:9c:80:4a:d7:27
GlobalSign PersonalSign 2 CA - G3	64:37:95:b7:81:44:e3:5a:9d:78:2c:b2:03:51:39:9d:bd:01:c9:51
GlobalSign PersonalSign 3 CA - G3	e2:2a:f7:e1:56:13:9e:2f:91:c7:08:62:09:9e:c0:21:5f:be:6e:53
GlobalSign PersonalSign 2 ECC CA SHA 384 - G4	7a:6d:be:62:3f:a7:eb:3a:bc:d2:3d:d3:c1:bd:ad:a2:dc:4c:3c:26
GlobalSign PersonalSign 2 RSA CA SHA 384 - G4	c2:80:13:02:09:b8:8f:c8:ef:82:2d:95:a5:e7:88:34:7e:50:aa:90
GlobalSign CA for AATL on HV	3a:f3:d5:9d:10:22:e4:7d:26:92:bf:a0:35:03:8c:87:ac:85:2a:b7

GlobalSign Management's Assertion

October 15, 2020

GlobalSign NV/SA (GlobalSign) has deployed a public key infrastructure. As part of the key management lifecycle, in order to destroy all copies of 19 Issuing CA (ICA) keys listed in Appendix A, multiple key ceremonies were conducted across multiple locations throughout the period of July 28, 2020 to September 16, 2020, the purpose of which was to formally witness and document the destruction of the ICA keys.

GlobalSign's management has securely destroyed the private keys in support of its CA operations. The private keys were destroyed in accordance with procedures described in GlobalSign's Certificate Policy (CP) and Certification Practice Statement (CPS), and its ICA Key Destruction script(s), which are in accordance with Key Destruction Criterion 4.6 of the [WebTrust Principles and Criteria for Certification Authorities, Version 2.2](#).

GlobalSign's management established and maintained effective controls over the destruction of these keys. These controls were designed to provide reasonable assurance of adherence to the above-mentioned practices throughout the key destruction process.

GlobalSign's management is responsible for establishing and maintaining procedures over its CA key destructions, and over the integrity and confidentiality of all cryptographic hardware and access keys (including physical keys, tokens, and passwords) used in the destruction of the ICA keys, and for the CA environment controls relevant to the destruction of its CA keys.

GlobalSign's management has assessed the procedures and controls for the destruction of the CA keys. Based on that assessment, in management's opinion, in destroying its CA keys throughout the period of July 28, 2020 to September 16, 2020 for the ICAs as enumerated in Appendix A,

GlobalSign has

- followed the CA key destruction requirements in its:
 - [Certificate Policy v6.4](#)
 - [Certification Practice Statement v9.4](#)
- included appropriate, detailed procedures and controls in its ICA Key Destruction script(s)
- maintained effective controls to provide reasonable assurance that the cryptographic hardware related to GlobalSign ICAs were destroyed in conformity with the procedures described in its CP/CPS and its Key Destruction script(s)
- performed, during the key destruction process, all procedures required by the ICA Key Destruction script(s)
- destroyed the ICA keys in a physically secured environment as described in its CP/CPS
- destroyed the ICA keys using personnel in trusted roles under multiple person control and split knowledge



GlobalSign
GMO INTERNET GROUP

in accordance with CA Key Destruction Criterion 4.6 of the [WebTrust Principles and Criteria for Certification Authorities, Version 2.2.](#)

GlobalSign NV/SA
Leuven, Belgium

Signed by: Arvid Vermote
Function: Chief Information Security Officer
October 15, 2020



GlobalSign

GMO INTERNET GROUP

Appendix A – identifying information

CA hierarchy

The following table provides an overview of the CAs:

Name	Subject Key Identifier
GlobalSign Qualified Timestamping ECC CA 2020	85:a0:9d:62:2d:a1:1d:77:5a:d4:c7:4d:7f:93:a5:d1:ba:2e:e3:48
GlobalSign HV ECC DV SSL CA 2018	2b:6a:46:49:be:68:76:90:9c:be:47:9c:6c:10:48:b1:c2:ba:6d:b3
GlobalSign R6 RSA EV SSL CA 2019	db:3c:67:3c:93:76:0e:38:a5:b1:ce:f4:45:9d:0f:60:aa:16:af:0a
GlobalSign R6 Admin CA - SHA256 - G3	81:49:5c:e9:05:bf:0c:88:a0:38:96:b2:5d:41:03:5a:e9:ff:d7:87
GlobalSign RSA EV SSL CA 2019	bc:f4:83:6b:6a:53:6c:17:05:bd:d4:bf:0c:b3:16:f1:0f:63:c5:df
GlobalSign ECC EV SSL CA 2019	f9:ec:81:c9:90:a3:04:3c:7c:a4:ec:45:c9:56:a8:e2:ca:df:c9:64
GlobalSign Qualified CA 2	81:43:71:1e:bb:f9:22:bc:ac:3a:36:15:d5:b2:8e:37:54:95:b9:16
GlobalSign Qualified CA 3	a7:d2:4c:1e:f6:e6:b7:b8:6d:14:23:ae:e8:1c:aa:78:42:6a:89:d5
GlobalSign PersonalSign 2 CA - SHA256 - G4	ac:a9:d2:3e:25:5c:a3:e7:65:08:f9:57:64:e4:59:ae:0b:52:57:4e
Trafigura PTE Ltd S/MIME ICA 2020	f9:76:ab:89:d7:42:0d:ea:4c:de:38:6b:c6:3b:86:4a:9c:36:e9:66
GlobalSign Qualified Time Stamping CA 2019	71:4b:5c:ac:76:e2:a1:4d:e1:b3:e9:8c:f2:c2:f9:b7:b0:07:40:d3
MSC Trustgate.com RSA AATL CA 2019	eb:ae:6b:85:2f:70:10:16:ec:28:59:5c:a4:3d:b7:7a:74:31:a9:6e
VWFS CA for AATL	85:88:43:b4:7d:34:84:6f:c5:17:2d:b9:06:1e:56:20:70:d7:e8:13
GlobalSign PersonalSign 1 CA - G3	e9:14:6a:00:48:d0:40:24:98:72:cd:76:13:0c:59:9c:80:4a:d7:27
GlobalSign PersonalSign 2 CA - G3	64:37:95:b7:81:44:e3:5a:9d:78:2c:b2:03:51:39:9d:bd:01:c9:51
GlobalSign PersonalSign 3 CA - G3	e2:2a:f7:e1:56:13:9e:2f:91:c7:08:62:09:9e:c0:21:5f:be:6e:53
GlobalSign PersonalSign 2 ECC CA SHA 384 - G4	7a:6d:be:62:3f:a7:eb:3a:bc:d2:3d:d3:c1:bd:ad:a2:dc:4c:3c:26
GlobalSign PersonalSign 2 RSA CA SHA 384 - G4	c2:80:13:02:09:b8:8f:c8:ef:82:2d:95:a5:e7:88:34:7e:50:aa:90
GlobalSign CA for AATL on HV	3a:f3:d5:9d:10:22:e4:7d:26:92:bf:a0:35:03:8c:87:ac:85:2a:b7

GlobalSign NV/SA

Martelarenlaan 38 3010 Leuven Belgium

Main: +32 16 89 19 00 | Fax: +32 16 89 19 09

Web: www.globalsign.com | Email: sales@globalsign.com