Tel: 314-889-1100
Fax: 314-889-1101
www.bdo.com

101 South Hanley Road, Suite 800
St. Louis, MO 63105

INDEPENDENT ACCOUNTANT'S REPORT

To the Management of GlobalSign NV/SA:

We have examined GlobalSign NV/SA's certification authority ("CA") operations in Japan, Singapore, and the United Kingdom, GlobalSign NV/SA's disclosure of its SSL certificate life cycle management business practices, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements in the GlobalSign NV/SA repository**,** the provision of such services in accordance with its disclosed practices, and the design of its controls over key and SSL certificate integrity, over the authenticity and confidentiality of SSL subscriber and relying party information, over continuity of key and SSL certificate life cycle management operations, and over development, maintenance, and operation of CA systems integrity, and over meeting the network and certificate system security requirements set forth by the CA/Browser Forum, throughout the period April 1, 2016 to March 31, 2017 for its root and issuing CAs enumerated in Appendix B, in scope for SSL Baseline Requirements and Network Security Requirements.

These disclosures and controls are the responsibility of GlobalSign NV/SA's management. Our responsibility is to express an opinion on the conformity of these disclosures and controls with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, Version 2.0, based on our examination.

We conducted our examination in accordance with standards for attestation engagements established by the American Institute of Certified Public Accountants and, accordingly, included:

(1) obtaining an understanding of GlobalSign NV/SA's SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates, and obtaining an understanding of GlobalSign NV/SA's network and certificate system security to meet the requirements set forth by the CA/Browser Forum;
(2) selectively testing transactions executed in accordance with disclosed SSL certificate lifecycle management practices;
(3) testing and evaluating the operating effectiveness of the controls; and
(4) performing such other procedures as we considered necessary in the circumstances.

We believe that our examination provides a reasonable basis for our opinion.

The relative effectiveness and significance of specific controls at GlobalSign NV/SA and their effect on assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations. We have performed no procedures to evaluate the effectiveness of controls at individual subscriber and relying party locations.

Because of the nature and inherent limitations of controls, GlobalSign NV/SA's ability to meet the aforementioned criteria may be affected. For example, controls may not prevent, or detect and correct, error, fraud, unauthorized access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection of any conclusions based on our findings to future periods is subject to the risk that changes may alter the validity of such conclusions.

We noted the following matters that resulted in a modification of our opinion.

Impacted WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security		**Control Deficiency Noted**
2 - 2.1	The CA maintains controls to provide reasonable assurance that certificates issued meet the minimum requirements for Certificate Content and profile as established in section 9 of the Baseline Requirements including the following: • Issuer Information (See SSL Baseline Requirements Section 9.1) • Subject Information (See SSL Baseline Requirements Section 9.2) • Certificate Policy Identification (See SSL Baseline Requirements Section 9.3) • Validity Period (See SSL Baseline Requirements Section 9.4) • Subscriber Public Key (See SSL Baseline Requirements Section 9.5) • Certificate Serial Number (See SSL Baseline Requirements Section 9.6) • Additional Technical Requirements (See SSL Baseline Requirements Section 9.7) - Appendix A - Cryptographic Algorithm and Key Requirements - Appendix B - Certificate Extensions. (See SSL Baseline Requirements Section 9)	Management discovered a bug that allowed orders that are re-issued with modified domains within the Subject Alternative Name field of the certificate to not include the Key Usage (KU) or Extended Key Usage (EKU) extensions. This occurred between August 29, 2016 and September 19, 2016. Management noted 68 Certificates were affected, 4 of these are extended validation certificates and 64 are organization validation certificates. Management was not able to revoke all certificates within 24 hours, due to customer requirements.
2 - 5.3	The CA maintains controls to provide reasonable assurance that Certificates are revoked within 24 hours if any of the following events occurs: • The Subscriber requests in writing that the CA revoke the Certificate; • The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; • The CA obtains evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has suffered a Key Compromise, or that the Certificate has otherwise been misused (also See SSL Baseline Requirements Section 13.1.5);	

	• The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber or Terms of Use Agreement; • The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name); • The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name; • The CA is made aware of a material change in the information contained in the Certificate; • The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement; • The CA determines that any of the information appearing in the Certificate is inaccurate or misleading; • The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; • The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository; • The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate; • Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or • The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time). (See SSL Baseline Requirements Section 13.1.5)	
3-4	The CA develops, implements, and maintains a Business Continuity Plan that includes at a minimum: • the conditions for activating the plan; • emergency procedures;	The following points were noted during our review:

	• fall-back procedures; • resumption procedures; • a maintenance schedule for the plan; • awareness and education requirements; • the responsibilities of the individuals; • recovery time objective (RTO); • regular testing of contingency plans; • the CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes; • a requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • what constitutes an acceptable system outage and recovery time; • how frequently backup copies of essential business information and software are taken; • the distance of recovery facilities to the CA's main site; and • 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. The Business Continuity Plan is tested at least annually, reviewed, and updated. (See SSL Baseline Requirements Section 16.4)	• a backup plan does not define the frequency of copies of essential information to be taken from the Japan and Singapore locations; • backup jobs were failing to complete successfully for the RA Production Server and GCC Production Server; • no backup was conducted for the system log server; • sufficient documentation was not retained for the annual test of the business continuity plan for the Japan location.

This caused the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security Criterion outlined above to not be met.

In our opinion, except for the effect of the matters discussed in the preceding paragraph, throughout the period April 1, 2016 to March 31, 2017, in all material respects, GlobalSign NV/SA has:

- disclosed its SSL certificate lifecycle management business practices the applicable version of its Certification Practice Statement and Certificate Policy enumerated in Appendix A, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the GlobalSign NV/SA repository, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated for the registration activities performed by GlobalSign NV/SA

- maintained effective controls to provide reasonable assurance that:
    - logical and physical access to CA systems and data is restricted to authorized individuals;
    - the continuity of key and certificate management operations is maintained; and
    - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, Version 2.0.

This report does not include any representation as to the quality of GlobalSign NV/SA's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security, Version 2.0, nor the suitability of any of GlobalSign NV/SA's services for any customer's intended purpose.

BDO USA, LLP

Certified Public Accountants
St. Louis, Missouri
July 26, 2017

Assertion of Management as to its Disclosure of its Business Practices and its Controls Over its Certification Authority Operations during the period of April 1, 2016 through March 31, 2017

July 26, 2017

Our Commitment to Security, Controls and Integrity:

GlobalSign NV/SA is committed to providing the highest level of security, controls, and integrity to provide SSL certificates with its disclosed practices described in the Certification Practice Statement, enumerated in Appendix A. To that end, we have subjected our certification authority business practices to the WebTrust for Certification Authorities – SSL Baseline with Network Security Requirements Audit Criteria.

Our Assertion with Respect to SSL Baseline with Network Security

GlobalSign NV/SA operates the Certification Authority (CA) services for its root and issuing CAs enumerated in Appendix B in scope for SSL Baseline Requirements and Network Security Requirements and provides SSL CA services.

GlobalSign NV/SA management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in providing its SSL and non-SSL CA services in Japan, Singapore, the United Kingdom, throughout the period April 1, 2016 through March 31, 2017, GlobalSign NV/SA has:

- disclosed its SSL certificate lifecycle management business practices in the applicable versions of the Certificate Practice Statement and Certificate Policy, as enumerated in Appendix A, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements in the GlobalSign NV/SA's repository, and provided such services in accordance with its disclosed practices

- maintained effective controls to provide reasonable assurance that:
  - the integrity of keys and SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated, for the registration activities performed by GlobalSign NV/SA

- maintained effective controls to provide reasonable assurance that:
  - logical and physical access to CA systems and data is restricted to authorized individuals;
  - the continuity of key and certificate management operations is maintained; and
  - CA systems development, maintenance, and operations are properly authorized and performed to maintain CA systems integrity

- maintained effective controls to provide reasonable assurance that it meets the Network and Certificate System Security Requirements as set forth by the CA/Browser Forum

based on Principle 4 of the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.0, except for the effects of the matters noted below:

Impacted WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security		Control Deficiency Noted	GlobalSign Management Response
2 - 2.1	The CA maintains controls to provide reasonable assurance that certificates issued meet the minimum requirements for Certificate Content and profile as established in section 9 of the Baseline Requirements including the following: • Issuer Information (See SSL Baseline Requirements Section 9.1) • Subject Information (See SSL Baseline Requirements Section 9.2) • Certificate Policy Identification (See SSL Baseline Requirements Section 9.3) • Validity Period (See SSL Baseline Requirements Section 9.4) • Subscriber Public Key (See SSL Baseline Requirements Section 9.5) • Certificate Serial Number (See SSL Baseline Requirements Section 9.6) • Additional Technical Requirements (See SSL Baseline Requirements Section 9.7) - Appendix A -	Management discovered a bug that allowed orders that are re-issued with modified domains within the Subject Alternative Name field of the certificate to not include the Key Usage (KU) or Extended Key Usage (EKU) extensions. This occurred between August 29, 2016 and September 19, 2016. Management noted 68 Certificates were affected, 4 of these are extended validation certificates and 64 are organization validation certificates. Management was not able to revoke all certificates within 24 hours, due to customer requirements.	Management noted that GlobalSign informed the CA/B Forum and browsers of this issue as soon as it was discovered in line with baseline and root program requirements.

	Cryptographic Algorithm and Key Requirements - Appendix B - Certificate Extensions. (See SSL Baseline Requirements Section 9)		
2 – 5.3	The CA maintains controls to provide reasonable assurance that Certificates are revoked within 24 hours if any of the following events occurs: • The Subscriber requests in writing that the CA revoke the Certificate; • The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization; • The CA obtains evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has suffered a Key Compromise, or that the Certificate has otherwise been misused (also See SSL Baseline Requirements Section 13.1.5); • The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber or Terms of Use Agreement;		

	• The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name); • The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name; • The CA is made aware of a material change in the information contained in the Certificate; • The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement; • The CA determines that any of the information appearing in the Certificate is		

	inaccurate or misleading; • The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate; • The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository; • The CA is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate; • Revocation is required by the CA's Certificate Policy and/or Certification Practice Statement; or • The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and		

	replaced by CAs within a given period of time). (See SSL Baseline Requirements Section 13.1.5)		
3-4	The CA develops, implements, and maintains a Business Continuity Plan that includes at a minimum: • the conditions for activating the plan; • emergency procedures; • fall-back procedures; • resumption procedures; • a maintenance schedule for the plan; • awareness and education requirements; • the responsibilities of the individuals; • recovery time objective (RTO); • regular testing of contingency plans; • the CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes; • a requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location; • what constitutes an acceptable system outage and recovery time;	Management noted the following points based on the auditors review: • a backup plan does not define the frequency of copies of essential information to be taken from the Japan and Singapore locations; • backup jobs were failing to complete successfully for the RA Production Server and GCC Production Server;; • no backup was conducted for the system log server; • sufficient documentation was not retained for the annual test of the business continuity plan for the Japan location.	Whereas backups were configured in the systems, we failed to document all the in-scope systems' backup specifications. GlobalSign will be enhancing the backup specification document for full coverage of systems in scope for Baseline Requirements. There were some backup failures in RA and GCC, but these have since been resolved and root cause identified for future availability. GlobalSign will also be including syslog server into the scope of backup in line with other in-scope servers. For above-mentioned issues, this data has been retained as per the retention period as

	• how frequently backup copies of essential business information and software are taken; • the distance of recovery facilities to the CA's main site; and • 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. The Business Continuity Plan is tested at least annually, reviewed, and updated. (See SSL Baseline Requirements Section 16.4)		defined in CPS and no data has been lost due to these events. Disaster recovery testing was conducted, but the report lacked the level of required detail. GlobalSign will be enhancing the BCP drill procedure.

GlobalSign
Leuven, Belgium

Koji Takenobu
Board Member

Appendix A - Certification Practice Statements and Certificate Policies in Scope

Certification Practice Statement	Begin Effective Date	End Effective Date
Version 8.0	August 20, 2015	May 1, 2016
Version 8.1	May 2, 2016	June 15, 2016
Version 8.2	June 16, 2016	August 21, 2017
Version 8.3	August 22, 2016	February 1, 2017
Version 8.4	February 2, 2017	Current

Certification Policy	Begin Effective Date	End Effective Date
Version 5.0	August 20, 2015	May 1, 2016
Version 5.1	May 2, 2016	June 15, 2016
Version 5.2	June 16, 2016	August 21, 2017
Version 5.3	August 22, 2016	February 1, 2017
Version 5.4	February 2, 2017	Current

Appendix B – In-Scope CAs

Root Cas	Serial Number	SHA1 Thumbprint
CN = GlobalSign Root CA OU = Root CA O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 15 4b 5a c3 94	b1 bc 96 8b d4 f4 9d 62 2a a8 9a 81 f2 15 01 52 a4 1d 82 9c
CN = GlobalSign O = GlobalSign OU = GlobalSign Root CA - R2 *	04 00 00 00 00 01 0f 86 26 e6 0d	75 e0 ab b6 13 85 12 27 1c 04 f8 5f dd de 38 e4 b7 24 2e fe
CN = GlobalSign O = GlobalSign OU = GlobalSign Root CA - R3	04 00 00 00 00 01 21 58 53 08 a2	d6 9b 56 11 48 f0 1c 77 c5 45 78 c1 09 26 df 5b 85 69 76 ad
CN = GlobalSign O = GlobalSign OU = GlobalSign ECC Root CA - R4 *	2a 38 a4 1c 96 0a 04 de 42 b2 28 a5 0b e8 34 98 02	69 69 56 2e 40 80 f4 24 a1 e7 19 9f 14 ba f3 ee 58 ab 6a bb
CN = GlobalSign O = GlobalSign OU = GlobalSign ECC Root CA - R5	60 59 49 e0 26 2e bb 55 f9 0a 77 8a 71 f9 4a d8 6c	1f 24 c6 30 cd a4 18 ef 20 69 ff ad 4f dd 5f 46 3a 1b 69 aa
CN = GlobalSign O = GlobalSign OU = GlobalSign Root CA - R6	45 e6 bb 03 83 33 c3 85 65 48 e6 ff 45 51	80 94 64 0e b5 a7 a1 ca 11 9c 1f dd d5 9f 81 02 63 a7 fb d1
CN = GlobalSign Root CA - R7 OU = Root CA O = GlobalSign nv-sa C = BE	48 1b 6a 06 a6 23 3b 90 a6 29 e6 d7 22 d5	c0 f6 29 8e 78 38 ca 4b f6 71 7c ef 2d de eb 57 e3 56 61 fc
CN = GlobalSign Root CA - R8 OU = Root CA O = GlobalSign nv-sa C = BE	48 1b 6a 09 f4 f9 60 71 3a fe 81 cc 86 dd	62 01 ff ce 4f 09 cd c7 e0 2f e1 10 f4 fd 67 f0 37 1a 2f 2a

* - Google Inc. assumed operations of the GlobalSign Root CA - R2 and GlobalSign ECC Root CA - R4 roots on August 11, 2016. GlobalSign NV/SA operated these roots prior to August 11, 2016 and was responsible for the key generation for these roots.

Other Cas	Serial Number	SHA1 Thumbprint
CN = AlphaSSL CA - G2 O = AlphaSSL	04 00 00 00 00 01 2f 4e e1 37 02	58 24 cf 32 c3 cc 2a 47 44 3d b1 0a 33 bb e3 ac 8d e5 24 e1
CN = AlphaSSL CA - SHA256 - G2 O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 44 4e f0 36 31	4c 27 43 17 17 56 5a 3a 07 f3 e6 d0 03 2c 42 58 94 9c f9 ec
CN = AlphaSSL CA - SHA256 - G2 O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 44 4e f0 3a 38	92 80 01 ce 96 78 a6 87 9b 50 23 18 b7 7c 73 98 10 ce 75 77
CN = AlphaSSL CA - SHA256 - G3 O = GlobalSign nv-sa C = BE	47 07 b1 00 4c 72 89 07 cd 35 47 55 f7 22	c3 dd f3 b3 c8 10 10 41 70 4a c2 d3 d6 52 9a f8 4b 65 33 7c
CN = GlobalSign CloudSSL CA - SHA1 - G3	46 f0 8c da b0 f0 81 59 59 3b b3 36 d8 dc	a0 04 2b 9e dc 56 09 65 c8 21 6c 9d 61 78 0b db

O = GlobalSign nv-sa C = BE		de 2b de 0a
CN = GlobalSign CloudSSL CA - SHA256 - G3 O = GlobalSign nv-sa C = BE	46 f0 8c db cf 2c 54 66 ef 33 01 dd 5f 34	b4 18 b3 2d b3 b8 cf 9f df a1 9c c3 12 16 85 2f cc 82 86 e3
CN = GlobalSign CodeSigning CA - G2 O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 2f 4e e1 35 5c	90 00 40 17 77 dd 2b 43 39 3d 7b 59 4d 2f f4 cb a4 51 6b 38
CN = GlobalSign CodeSigning CA - G3 O = GlobalSign nv-sa C = BE	47 c3 0f fe fc 22 bb 28 0f 96 fe a7 52 51	f1 e7 b6 c0 c1 0d a9 43 6e cc 04 ff 5f c3 b6 91 6b 46 cf 4c
CN = GlobalSign Domain Validation CA - G2 O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 2f 4e e1 41 43	2a 3c f4 bd dc 74 cc aa 48 05 58 f9 d8 d1 d2 a0 84 f3 4b 31
CN = GlobalSign Domain Validation CA - G2 O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 31 89 e5 59 25	59 aa d2 4a 09 9d 25 d4 0d 41 bc d0 c3 00 a2 bd b0 44 12 44
CN = GlobalSign Domain Validation CA - G2 O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 2f 4e e1 3f 11	04 81 c8 ca 31 be 0f a9 40 c7 e0 cc d5 72 37 4e ad f5 2b 73
CN = GlobalSign Domain Validation CA - SHA256 - G2 O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 44 4e f0 3e 20	73 6a 4d c6 79 d6 82 da 32 15 63 64 7c 60 f6 99 f0 df c2 68
CN = GlobalSign Domain Validation CA - SHA256 - G3 O = GlobalSign nv-sa C = BE	47 07 b1 00 f4 18 22 43 4e c0 5b 8c 7b 7f	2b 74 91 52 1f b3 40 04 ab ae 31 94 19 a3 dc 79 1f 63 95 5e
CN = GlobalSign Organization Validation CA - G2 O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 2f 4e e1 45 0c	b9 ee 85 a1 0f d4 95 d9 94 ed 63 48 8a b7 4a 18 cb 8e 6b fa
CN = GlobalSign Organization Validation CA - G2 O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 31 89 e5 5b f4	bf f1 25 8f 5e 1e 79 b6 0f 47 01 ff 26 5c 42 71 39 d9 8c 88
CN = GlobalSign Organization Validation CA - G2 O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 2f 4e e1 42 f9	04 00 00 00 00 01 2f 4e e1 42 f9
CN = GlobalSign Organization Validation CA - SHA256 - G2 O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 44 4e f0 42 47	90 2e f2 de eb 3c 5b 13 ea 4c 3d 51 93 62 93 09 e2 31 ae 55
CN = SignTrust Domain Verification CA - G2	04 00 00 00 00 01 2f 4e e1 39 16	4a 8c 78 cb c8 02 d9 9c 21 dc 14 ef 54 ff 92 df a1

O = SignTrust OU = SignTrust Domain Verification CA - G2		46 e6 87
CN = GlobalSign Extended Validation CA - G2 O = GlobalSign nv-sa C = BE **	04 00 00 00 00 01 2f 4e e1 5b 63	06 45 6b 2c 4c 26 f3 7c 95 26 67 93 bb ed ff 61 e6 37 3d c2
CN = GlobalSign Extended Validation CA - SHA256 - G2 O = GlobalSign nv-sa C = BE **	04 00 00 00 00 01 44 4e f0 4a 55	65 be 10 2b e2 69 28 65 0e 0e f5 4d c8 f4 f1 5a f5 f9 8e 8b
CN = AlphaSSL CA - SHA256 - G2 O = AlphaSSL	04 00 00 00 00 01 31 89 c6 39 dc	ae bf 32 c3 c8 32 c7 d7 bc 55 99 b1 aa 05 fb 6c f4 d9 29 4c
CN = Beame.io CA 1 O = Beame.io Ltd L = Tel Aviv-Jaffa S = Tel Aviv C = IL	48 44 dc c1 dc 5e 09 85 5f 10 92 9a f2 63	31 31 8e 66 12 6a a2 ed 9e ff d1 8b bb 54 e5 a5 b2 36 7a 72
CN = Beame.io CA 2 O = Beame.io Ltd L = Tel Aviv-Jaffa S = Tel Aviv C = IL	48 44 dc d5 5b d0 28 0e 0b 6f 6a 11 68 81	41 9e b2 f2 96 ef 2f ad b4 76 31 a6 16 16 86 2f 00 8b 9f 29
CN = GlobalSign CloudSSL CA - SHA256 - G3 O = GlobalSign nv-sa C = BE	48 ca 81 7a c6 dc 7f 56 b6 80 bb 43 36 25	fd 13 16 3b 2c d6 1a b3 82 e1 7e 73 c4 06 99 43 3f 9b eb 77
CN = GlobalSign CloudSSL CA - SHA256 - G3 O = GlobalSign nv-sa C = BE	48 ca 81 7a c6 dc 7f 56 b6 80 bb 43 36 25	fd 13 16 3b 2c d6 1a b3 82 e1 7e 73 c4 06 99 43 3f 9b eb 77
CN = GlobalSign CodeSigning CA - SHA256 - G2 O = GlobalSign nv-sa C = BE	47 2c cb a9 49 bb 94 24 e9 8f 41 6f ad 41	90 5f 59 6a ae 77 14 15 56 43 60 6e aa 5c 83 0b 0b 1b 43 9a
CN = GlobalSign Domain Validation CA - SHA256 - G2 O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 31 89 c6 42 58	ba 60 74 c3 a2 5f 99 0b 9d 7a 11 a6 59 c4 f7 82 1c 92 ff 10
CN = GlobalSign Extended Validation CA - SHA256 - G2 O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 31 89 c6 49 2e	ce 26 9f db 77 e3 88 4c 35 d5 97 fb dd 07 fc 3e ec e9 c6 22
CN = GlobalSign Extended Validation CA - SHA256 - G3 O = GlobalSign nv-sa C = BE	48 a4 02 dd 27 92 0d a2 08 34 9d d1 99 7b	60 23 19 2f e7 b5 9d 27 89 13 0a 9f e4 09 4f 9b 55 70 d4 a2
CN = GlobalSign Extended Validation CodeSigning CA - SHA256 - G2 O = GlobalSign nv-sa	04 00 00 00 00 01 31 89 c6 4d e1	4f 5e a6 a9 e4 ba 30 a4 57 5d ea d4 e4 e9 d3 b2 da 66 ea 7b

C = BE		
CN = GlobalSign Extended Validation CodeSigning CA - SHA256 - G3 O = GlobalSign nv-sa C = BE	48 1b 6a 07 a9 42 4c 1e aa fe f3 cd f1 0f	87 a6 3d 9a db 62 7d 77 78 36 15 3c 68 0a 3d fc f2 7d e9 0c
CN = GlobalSign Organization Validation CA - SHA256 - G2 O = GlobalSign nv-sa C = BE	04 00 00 00 00 01 31 89 c6 44 c9	ef 90 b2 b8 6f 47 56 eb e7 d3 6f f3 01 5d 63 52 3a 00 76 e9
CN = ICPEdu O = Rede Nacional de Ensino e Pesquisa - RNP OU = Gerencia de Servicos (GSer) L = Rio de Janeiro S = Rio de Janeiro C = BR	57 b0 9e ef 61 56 10 87 44 91 e9 2c 54 62 f4 61 96	47 31 fc 3e 37 f4 f4 99 49 73 9a cd 83 1f 56 2d d8 bc ab dc
CN = SignTrust Domain Verification CA - SHA256 - G2 O = SignTrust OU = SignTrust Domain Verification CA - SHA256 - G2	04 00 00 00 00 01 31 89 c6 3c 2e	45 8c cd 4f 97 ba dc a6 c7 cc 50 ad c6 8b bf 50 bc 7d f0 a9
CN = Soluti CA - DV O = SOLUTI - SOLUCOES EM NEGOCIOS INTELIGENTES S/A L = Goiânia S = Goiás C = BR	47 c3 0f fc d4 02 01 81 25 ba 9f b6 e8 c9	f3 17 e9 44 62 4a 4a 10 bd 5b d4 5c e8 8d 21 6b 87 be 68 2b
CN = Soluti CA - EV O = SOLUTI - SOLUCOES EM NEGOCIOS INTELIGENTES S/A L = Goiânia S = Goiás C = BR	47 c3 0f fd e9 ca 70 68 4b 88 7a 57 0d df	e0 29 5f a6 39 fe 2b 26 4d 37 6a c6 79 a9 e7 00 1d 3b 3f eb
CN = Soluti CA - OV O = SOLUTI - SOLUCOES EM NEGOCIOS INTELIGENTES S/A L = Goiânia S = Goiás C = BR	47 c3 0f fd 59 d2 76 81 f6 6e f9 c5 a0 75	27 c0 69 9b 0b 19 14 61 3e 06 06 c0 22 d0 44 b1 99 28 b2 2f
CN = Trusted Root CA SHA256 G2 O = GlobalSign nv-sa OU = Trusted Root C = BE	04 00 00 00 00 01 36 e9 82 39 5d	9a bb 55 a2 6f 9c 06 d5 00 c4 59 91 f0 2c 15 b5 5d 00 a7 02
CN = GlobalSign ECC384 EV SSL CA - G3 O = GlobalSign nv-sa C = BE	46 74 37 78 16 26 1d 0e 7a db e2 cc b5 fc	a7 9e f0 d5 2e da 08 de fa b9 7e 2d 7c e1 68 45 f9 75 0e 19
CN = GlobalSign ECC384 SSL CA - G3 O = GlobalSign nv-sa C = BE	46 74 37 77 92 09 73 fa 48 2f e2 8d 94 62	30 57 5e 16 60 48 bd 86 4e f8 76 68 25 e7 56 fe 0d fd 8b 80

** - On October 31, 2016, GlobalSign EV Certificate issuance was changed from GlobalSign Extended Validation CA - SHA256 - G2 CAs under GlobalSign Root CA - R2 to new CAs under GlobalSign Root CA - R3. Under the root sale agreement, between GlobalSign NV/SA and Google Inc., GlobalSign NV/SA was permitted to continue using the GlobalSign Extended Validation CA - SHA256 - G2 CAs under GlobalSign Root CA - R2 through the end of 2016.