Valencia, July 19, 2024

Independent Assurance Report

To the Management of the OISTE Foundation (OISTE):

Scope

We have been engaged, in a reasonable assurance engagement, to report on OISTE management's assertion that for its Certification Authority (CA) operations at Geneva, Switzerland, throughout the period May 9, 2023 through May 8, 2024 for its CAs as enumerated in Appendix A, OISTE has:

- disclosed its SSL certificate lifecycle management business practices in its Certification Practice Statements as enumerated in Appendix B including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirement on the OISTE website 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 OISTE)

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.7.

Certification authority's responsibilities

OISTE's management is responsible for its assertion, including the fairness of its presentation, and the provision of its described services in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.7.

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 behaviour.

The firm applies International Standard on Quality Management (ISQM) 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements* 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.

Practitioner'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 of OISTE'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 OISTE'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 the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

The relative effectiveness and significance of specific controls at OISTE 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.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. For example, because of their nature, controls may not prevent, or detect unauthorised access to systems and information, or failure to comply with internal and external policies or requirements. Also, the projection to the future of any conclusions based on our findings is subject to the risk that controls may become ineffective.

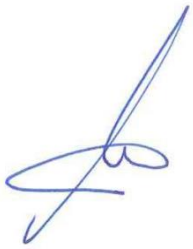
Opinion

In our opinion, throughout the period May 9, 2023 through May 8, 2024, OISTE management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.7.

This report does not include any representation as to the quality of OISTE's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.7, nor the suitability of any of OISTE's services for any customer's intended purpose.

Use of the WebTrust seal

OISTE's use of the WebTrust for Certification Authorities – SSL Baseline with Network Security Seal constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.



F. Mondragon, Auditor

auren

Valencia, SPAIN
July 19, 2024

APPENDIX A: List of CAs in Scope

Root Cas
1. OISTE WISeKey Global Root GB CA
2. OISTE WISeKey Global Root GC CA
3. OISTE Server Root RSA G1
4. OISTE Server Root ECC G1

CA Identifying Information for in Scope Cas

CA#	Cert #	Subject	Issuer	serialNumber	notBefore	NotAfter	SHA256 Fingerprint
1	1	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	76B1205274F0858746B3F8231AF6C2C0	Dec 1 15:00:32 2014 GMT	Dec 1 15:10:31 2039 GMT	6B9C08E86EB0F767CFAD65CD98B62149E5494A67F5845E7BD1ED019F27B86BD6
2	1	CN=OISTE WISeKey Global Root GC CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GC CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	212A560CAEDA0CAB4045BF2BA22D3AEA	May 9 09:48:34 2017 GMT	May 9 09:58:33 2042 GMT	8560F91C3624DABA9570B5FEA0DBE36FF11A8323BE9486854FB3F34A5571198D
3	1	CN=OISTE Server Root RSA G1, O=OISTE Foundation, C=CH	CN=OISTE Server Root RSA G1, O=OISTE Foundation, C=CH	55A5D9679428C6ED0CFA27DD5B014D18	May 31 14:37:16 2023 GMT	May 24 14:37:15 2048 GMT	9AE36232A5189FFDDB353DFD26520C015395D22777DAC59DB57B98C089A651E6
4	1	CN=OISTE Server Root ECC G1, O=OISTE Foundation, C=CH	CN=OISTE Server Root ECC G1, O=OISTE Foundation, C=CH	23F9C3D635AF8F284B1FF054EA7E979D	May 31 14:42:28 2023 GMT	May 24 14:42:27 2048 GMT	EEC997C0C30F216F7E3B8B307D2BAE42412D753FC8219DAFD1520B2572850F49

APPENDIX B: LIST OF CERTIFICATION PRACTICE STATEMENTS

- **OISTE CERTIFICATION PRACTICES STATEMENT**

Version	Date	Changes
3.4	29/Sep/22	Annual review
3.5	15/Aug/23	Integration of S/MIME BR and minor reviews

- **OISTE CERTIFICATE POLICY FOR SSL/TLS CERTIFICATES**

Version	Date	Changes
1.4	30/Jan/23	Annual review. No changes
1.5	24/Jan/24	Annual review. No significant changes

APPENDIX C: LIST OF REPORTS TO CA/B FORUM

No incidents reported by client in the audit period.

OISTE MANAGEMENT'S ASSERTION

as to its Disclosure of its Business Practices and Controls over its SSL Certification Authority Operations during the period from May 9th 2023 through May 8th 2024

The International Organization for the Security of Electronic Transactions ("**OISTE**") operates the Certification Authority (CA) services known as "**OISTE Global Trust Model**" hierarchy with its Root Certification Authorities as detailed in attachment A, and provides the following CA services, and Network Security Requirements and provides SSL and non-SSL CA services.

The management of **OISTE** is responsible for establishing and maintaining effective controls over its SSL (and non-SSL) CA operations, including its network and certificate security system controls, its SSL CA business practices disclosure on its website [https://www.oiste.org/repository], SSL key lifecycle management controls, and SSL certificate lifecycle management controls. These controls contain monitoring mechanisms, and actions are taken to correct deficiencies identified.

There are inherent limitations in any controls, including the possibility of human error, and the circumvention or overriding of controls. Accordingly, even effective controls can only provide reasonable assurance with respect to **OISTE's** Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

OISTE 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) Certification Authority (CA) services at Switzerland, throughout the period May 9th 2023 through May 8th 2024, **OISTE** has:

- disclosed its SSL certificate lifecycle, practices in the document "OISTE Root Certification Practice Statement as enumerated in Attachment B, including its commitment to provide SSL certificates in conformity with the CA/Browser Forum Requirements on the **OISTE** website, 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 **OISTE**)
- 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

In accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.7.

Geneva, 17th July 2024

Philippe Doubre
OISTE President

Carlos Moreira
CEO

Appendix A: PKI Hierarchy in scope of the WebTrust audit

OISTE WISeKey Global Root GB CA

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
2.	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	6B:9C:08:E8:6E:B0:F7:67:CF:AD:65:CD:98:B6:21:49:E5:49:4A:67:F5:84:5E:7B:D1:ED:01:9F:27:B8:6B:D6	Issuing CA	ACTIVE	

OISTE WISeKey Global Root GC CA

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
3.	CN=OISTE WISeKey Global Root GC CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GC CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	85:60:F9:1C:36:24:DA:BA:95:70:B5:FE:A0:DB:E3:6F:F1:1A:83:23:BE:94:86:85:4F:B3:F3:4A:55:71:19:8D	Issuing CA	ACTIVE	

OISTE Server Root RSA G1

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
6.	CN=OISTE Server Root RSA G1, O=OISTE Foundation, C=CH	CN=OISTE Server Root RSA G1, O=OISTE Foundation, C=CH	9A:E3:62:32:A5:18:9F:FD:DB:35:3D:FD:26:52:0C:01:53:95:D2:27:77:DA:C5:9D:B5:7B:98:C0:89:A6:51:E6	Issuing CA	ACTIVE	

OISTE Server Root ECC G1

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
7.	CN=OISTE Server Root ECC G1, O=OISTE Foundation, C=CH	CN=OISTE Server Root ECC G1, O=OISTE Foundation, C=CH	EE:C9:97:C0:C3:0F:21:6F:7E:3B:8B:30:7D:2B:AE:42:41:2D:75:3F:C8:21:9D:AF:D1:52:0B:25:72:85:0F:49	Issuing CA	ACTIVE	

Appendix B: CP/CPS documents in scope of the WebTrust audit

CP Documents

CP for SSL Certificates

Version	Date	URL
1.4	30/Jan/23	https://cdn.wisekey.com/osite/uploads/20230130092159/OGTM-CP-SSL-Certificates.v1.4.pdf
1.5	24/Jan/24	https://cdn.wisekey.com/osite/uploads/20240125074343/OGTM-CP-SSL-Certificates.v1.5.pdf

CPS Documents

Version	Date	URL
3.4	29/Sep/22	https://cdn.wisekey.com/osite/uploads/20220929143146/OGTM-OISTE-Foundation-CPS.v3.4-CLEAN.pdf
3.5	15/Aug/23	https://cdn.wisekey.com/osite/uploads/20240125074336/OGTM-OISTE-Foundation-CPS.v3.5-CLEAN-1.pdf

Appendix C: Disclosure of incidents during the period

No incidents in the audit period