Valencia, April 30th, 2019

Independent Assurance Report

To the Management of 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, as of April 1st, 2019 for its CAs as enumerated in Appendix A, OISTE has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its Certification Practice Statements as enumerated in Appendix B.
  - "OGTM Certification Practice Statement Version 3.0" – 25 February 2019
  - "CP for Personal Certificates Version 1.1" – 21 March 2019
  - "CP for SSL Certificates Version 1.0" – 25 February 2019
  - "CP for Device Certificates Version 1.0" – 25 February 2019

- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - OISTE's Certification Practice Statement is consistent with its Certificate Policies
  - OISTE provides its services in accordance with its Certificate Policies and Certification Practice Statement

- suitably designed, and placed into operation, controls to provide reasonable assurance that:
  - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
  - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
  - subscriber information is properly authenticated (for the registration activities performed by OISTE); and
  - subordinate CA certificate requests are accurate, authenticated, and approved.

- suitably designed, and placed into operation, 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.1.

OISTE makes use of external registration authorities for specific subscriber registration activities as disclosed in OISTE's business practices. Our procedures did not extend to the controls exercised by these external registration authorities.

OISTE does not escrow its CA keys, does not provide subscriber key generation services, and does not provide certificate suspension services. Accordingly, our procedures did not extend to controls that would address those criteria.

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 v2.1.

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 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 of OISTE's key and certificate lifecycle management business practices and its controls over key and certificate integrity, over the authenticity and confidentiality of subscriber and relying party information, over the continuity of key and certificate lifecycle management operations and over development, maintenance and operation of systems integrity;
(2) evaluating the suitability of the design of the controls; and;
(3) performing such other procedures as we considered necessary in the circumstances.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of OISTE's controls, individually or in the aggregate

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

Suitability of controls

The suitability of the design of the 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 suitability of the design of the controls at individual subscriber and relying party locations.

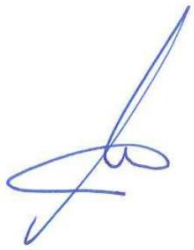
Inherent limitations

Because of the nature and inherent limitations of controls, OISTE'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.

Opinion

In our opinion, as of April 1st, 2019, 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 v2.1.

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 v2.1, nor the suitability of any of OISTE's services for any customer's intended purpose.



F. Mondragon, Auditor

auren

Valencia, SPAIN

April 30th, 2019

APPENDIX A List of CAs in scope

Root CAs
1. OISTE WISeKey Global Root GA CA
2. OISTE WISeKey Global Root GB CA
3. OISTE WISeKey Global Root GC CA

APPENDIX A: PKI Hierarchy in scope of the Webtrust audit

CA #	Cert #	Subject	Issuer	serialNumber	Key Algorithm	Key Size	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
1	1	CN=OISTE WISeKey Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WISeKey, C=CH	413D72C7F46B1F81437DF1D22854DF9A	rsaEncryption	2048 bit	sha1WithRSAEncryption	Dec 11 16:03:44 2005 GMT	Dec 11 16:09:51 2037 GMT	B3:03:7E:AE:36:BC:B0:79:D1:DC:94:26:B6:11:BE:21:B2:69:86:94	41C923866AB4CAD6B7AD578081582E020797A6CBDF4FFF78CE8396B38937D7F5
2	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	76B1205274F0858746B3F8231AF6C2C0	rsaEncryption	2048 bit	sha256WithRSAEncryption	Dec 1 15:00:32 2014 GMT	Dec 1 15:10:31 2039 GMT	35:0F:C8:36:63:5E:E2:A3:EC:F9:3B:66:15:CE:51:52:E3:91:9A:3D	6B9C08E86EB0F767CFAD65CD98B62149E5494A67F5845E7BD1ED019F27B86BD6
3	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	212A560CAEDA0CAB4045BF2BA22D3AEA	id-ecPublicKey	384 bit	ecdsa-with-SHA384	May 9 09:48:34 2017 GMT	May 9 09:58:33 2042 GMT	48:87:14:AC:E3:C3:9E:90:60:3A:D7:CA:89:EE:D3:AD:8C:B4:50:66	8560F91C3624DABA9570B5FEA0DBE36FF11A8323BE9486854FB3F34A5571198D

OISTE MANAGEMENT'S ASSERTION

as to its Disclosure of its Business Practices and Controls over its Certification Authority Operations as of April 1st 2019

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 appendix A, and provides the following CA services:

- Subscriber registration
- Certificate renewal
- Certificate rekey
- Certificate issuance
- Certificate distribution
- Certificate revocation
- Certificate suspension
- Certificate validation
- Subscriber key generation and management
- Subordinate CA certification
- Timestamp services

The management of **OISTE** is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website [https://www.oiste.org/repository], CA business practices management, CA environmental controls, CA key lifecycle management controls, subscriber key lifecycle management controls, certificate lifecycle management controls, and subordinate CA 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.

OISTE management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in **OISTE** management's opinion, in providing its Certification Authority (CA) services at its main and disaster recover datacentres in Switzerland, as of April 1st 2019, **OISTE** has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the documents:
    - "OGTM Certification Practice Statement Version 3.0" – 25 February 2019, available at the link [https://oiste.org/wp-content/uploads/OGTM-OISTE-Foundation-CPS.v3.0.pdf]
    - "CP for Personal Certificates Version 1.1" – 21 March 2019, available at [https://oiste.org/wp-content/uploads/OGTM-CP-Personal-Certificates.v1.1.pdf]
    - "CP for SSL Certificates Version 1.0" – 25 February 2019, available at [https://oiste.org/wp-content/uploads/OGTM-CP-SSL-Certificates.v1.0.pdf]
    - "CP for Device Certificates Version 1.0" – 25 February 2019", available at [https://oiste.org/wp-content/uploads/OGTM-CP-Device-Certificates.v1.0.pdf]
- suitably designed, and placed into operation, controls to provide reasonable assurance that **OISTE** provides its services in accordance with its Certification Practice Statement

- suitably designed, and placed into operation, controls to provide reasonable assurance that:
    - the integrity of keys and certificates it manages is established and protected throughout their lifecycles;
    - the integrity of subscriber keys and certificates it manages is established and protected throughout their lifecycles;
    - subscriber information is properly authenticated (for the registration activities performed by **OISTE**); and
    - subordinate CA certificate requests are accurate, authenticated, and approved
- suitably designed, and placed into operation, 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities v2.0 [http://www.webtrust.org/homepage-documents/item54279.pdf], including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)

CA Business Practices Management

- Certificate Policy Management
- Certification Practice Statement Management
- CP and CPS Consistency

CA Environmental Controls

- Security Management
- Asset Classification and Management
- Personnel Security
- Physical & Environmental Security
- Operations Management
- System Access Management
- System Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Audit Logging

CA Key Lifecycle Management Controls

- CA Key Generation
- CA Key Storage, Backup, and Recovery
- CA Public Key Distribution
- CA Key Usage
- CA Key Archival and Destruction
- CA Key Compromise
- CA Cryptographic Hardware Lifecycle Management
- CA Key Escrow

Subscriber Key Lifecycle Management Controls

- CA-Provided Subscriber Key Generation Services

- CA-Provided Subscriber Key Storage and Recovery Services
- Integrated Circuit Card (ICC) Lifecycle Management
- Requirements for Subscriber Key Management

Certificate Lifecycle Management Controls

- Subscriber Registration
- Certificate Renewal
- Certificate Rekey
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Validation

Subordinate CA Certificate Lifecycle Management Controls

- Subordinate CA Certificate Lifecycle Management

Geneva, April 1st 2019

Dourgam Kummer
OISTE Administrator

Philippe Doubre
OISTE President

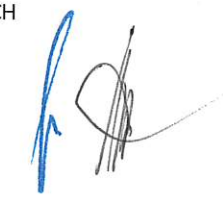
Appendix A: PKI Hierarchy in scope of the WebTrust audit

OISTE WISeKey Global Root GA CA

Subject Name: CN=OISTE WISeKey Global Root GC CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WISeKey, C=CH
Thumbprint: 41 C9 23 86 6A B4 CA D6 B7 AD 57 80 81 58 2E 02 07 97 A6 CB DF 4F FF 78 CE 83 96 B3 89 37 D7 F5
Valid From: 11th December 2005 To: 11th December 2037

OISTE WISeKey Global Root GB CA

Subject Name: CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH
Thumbprint: 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
Valid From: 1st December 2014 To: 1st December 2039

OISTE WISeKey Global Root GC CA

Subject Name: CN=OISTE WISeKey Global Root GC CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH
Thumbprint: E0 11 84 5E 34 DE BE 88 81 B9 9C F6 16 26 D1 96 1F C3 B9 31
Valid From: 9th May 2017 To: 9th May 2042