

## 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, throughout the period May 9, 2023 through May 8, 2024 for its CAs as enumerated in Appendix A in scope for S/MIME Baseline Requirements and Network Security Requirements, OISTE has:

- disclosed its S/MIME certificate lifecycle management business practices in its Certification Practice Statements as enumerated in Appendix B including its commitment to provide S/MIME 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 S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME 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 that are incorporated by reference



in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.0.

### **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 – S/MIME Certificates v1.0.0.

### **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 S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME 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 S/MIME 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 – S/MIME Certificates v1.0.0.

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 – S/MIME Certificates v1.0.0, 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 – S/MIME 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

S/MIME Issuing CAs	
1.	OISTE WISeKey Global Root GA CA
2.	OISTE WISeKey Global Root GB CA
3.	OISTE WISeKey Global Root GC CA
4.	OISTE Client Root RSA G1
5.	OISTE Client 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 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	Dec 11 16:03:44 2005 GMT	Dec 11 16:09:51 2037 GMT	41C923866AB4CAD6B7AD578081582E020797A6CBDF4FFF78CE8396B38937D7F5
2	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
3	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
4	1	CN=OISTE Client Root RSA G1, O=OISTE Foundation, C=CH	CN=OISTE Client Root RSA G1, O=OISTE Foundation, C=CH	34176F5901881BAAA5DDC848BBB43B73	May 31 14:23:29 2023 GMT	May 24 14:23:28 2048 GMT	D02A0F994A868C66395F2E7A880DF509BD0C29C96DE16015A0FD501EDA4F96A9
5	1	CN=OISTE Client Root ECC G1, O=OISTE Foundation, C=CH	CN=OISTE Client Root ECC G1, O=OISTE Foundation, C=CH	54EC97D68BB4C40B216E0EB2D053C87A	May 31 14:31:40 2023 GMT	May 24 14:31:39 2048 GMT	D9A32485A8CCA85539CEF12FFFFFF711378A17851D73DA2732AB4302D763BD62B

## 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 PERSONAL CERTIFICATES**

Version	Date	Changes
1.3	30/Jan/23	Annual review. No changes
1.4	15/Aug/23	Inclusion of S/MIME BR and minor edits



## **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  
S/MIME Certification Authority Operations during  
the period from May 9<sup>th</sup> 2023 through May 8<sup>th</sup> 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 S/MIME CA services.

The management of **OISTE** is responsible for establishing and maintaining effective controls over its S/MIME CA services, including its network and certificate security system controls, its S/MIME CA business practices disclosure on its website [<https://www.oiste.org/repository>], S/MIME key lifecycle management controls, and S/MIME 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 EV S/MIME CA services. Based on that assessment, in providing its S/MIME Certification Authority (CA) services at Switzerland, throughout the period May 9<sup>th</sup> 2023 through May 8<sup>th</sup> 2024, **OISTE** has:

- disclosed its S/MIME, certificate lifecycle management business practices in its "OISTE WISEKey Root Certification Practice Statement as enumerated in Attachment B (combined CP & CPS documents), including its commitment to provide S/MIME 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 S/MIME certificates it manages is established and protected throughout their lifecycles; and
  - S/MIME 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 that are incorporated by reference.

In accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME v1.0.0, as published at [[https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/smime-certificates\\_100\\_final\\_aoda-compliant.pdf](https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/smime-certificates_100_final_aoda-compliant.pdf)]



Geneva, 06<sup>th</sup> July 2024



Philippe Doubre  
OISTE President



Carlos Moreira  
CEO

## Appendix A: PKI Hierarchy in scope of the WebTrust audit

### OISTE WIS@key Global Root GA CA

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
1.	CN=OISTE WIS@key Global Root GA CA, OU=OISTE Foundation Endorsed, O=WIS@key, C=CH	CN=OISTE WIS@key Global Root GA CA, OU=OISTE Foundation Endorsed, O=WIS@key, C=CH	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	Issuing CA	ACTIVE	

### OISTE WIS@key Global Root GB CA

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
2.	CN=OISTE WIS@key Global Root GB CA, OU=OISTE Foundation Endorsed, O=WIS@key, C=CH	CN=OISTE WIS@key Global Root GB CA, OU=OISTE Foundation Endorsed, O=WIS@key, 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 WIS@key Global Root GC CA

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
3.	CN=OISTE WIS@key Global Root GC CA, OU=OISTE Foundation Endorsed, O=WIS@key, C=CH	CN=OISTE WIS@key Global Root GC CA, OU=OISTE Foundation Endorsed, O=WIS@key, 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	This Root has been requested to be removed for S/MIME from all Root Programs

### OISTE Client Root RSA G1

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
4.	CN=OISTE Client Root RSA G1, O=OISTE Foundation, C=CH	CN=OISTE Client Root RSA G1, O=OISTE Foundation, C=CH	D0:2A:0F:99:4A:86:8C:66:39:5F:2E:7A:88:0D:F5:09:BD:0C:29:C9:6D:E1:60:15:A0:FD:50:1E:DA:4F:96:A9	Issuing CA	ACTIVE	

### OISTE Client Root ECC G1

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
5.	CN=OISTE Client Root ECC G1, O=OISTE Foundation, C=CH	CN=OISTE Client Root ECC G1, O=OISTE Foundation, C=CH	D9:A3:24:85:A8:CC:A8:55:39:CE:F1:2F:FF:FF:71:13:78:A1:78:51:D7:3D:A2:73:2A:B4:30:2D:76:3B:D6:2B	Issuing CA	ACTIVE	

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

### CP Documents

CP for S/MIME Certificates

Version	Date	URL
1.3	30/Jan/23	<a href="https://cdn.wisekey.com/osite/uploads/20230130092201/OGTM-CP-Personal-Certificates.v1.3.pdf">https://cdn.wisekey.com/osite/uploads/20230130092201/OGTM-CP-Personal-Certificates.v1.3.pdf</a>
1.4	15/Aug/23	<a href="https://cdn.wisekey.com/osite/uploads/20230816074406/OGTM-CP-Personal-Certificates.v1.4.pdf">https://cdn.wisekey.com/osite/uploads/20230816074406/OGTM-CP-Personal-Certificates.v1.4.pdf</a>

### CPS Documents

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

## **Appendix C: Disclosure of incidents during the period**

No incidents in the audit period.