Valencia, July 09, 2025

Independent Assurance Report

To the Management of OISTE/WISeKey Global Trust Model (composed of OISTE Foundation (OISTE) and WISeKey SA (WISeKey):

Scope

We have been engaged, in a reasonable assurance engagement, to report on OISTE/WISeKey management's assertion that for its Certification Authority (CA) operations at Geneva, Switzerland, throughout the period May 9, 2024 through May 8, 2025 for its CAs as enumerated in Appendix A in scope for S/MIME Baseline Requirements, OISTE/WISeKey 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/WISeKey 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/WISeKey)

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.3. (https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/01618-ms_24-3464_webtrust-for-ca-smime-certificates-v1-0-3_final.pdf)

Certification authority’s responsibilities

OISTE/WISeKey’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 v1.0.3.

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/WISeKey’s S/MIME certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of S/MIME certificates,
(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/WISeKey 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, 2024, through May 8, 2025, OISTE/WISeKey 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 v1.0.3.

This report does not include any representation as to the quality of OISTE/WISeKey’s services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – S/MIME Certificates v1.0.3, nor the suitability of any of OISTE/WISeKey’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 09, 2025

APPENDIX A: List of CAs in Scope

Root CAs
1. OISTE WISeKey Global Root GA CA
3. OISTE WISeKey Global Root GB CA
6. OISTE WISeKey Global Root GC CA
8. OISTE_Client_Root_RSA_G1
10. OISTE_Client_Root_ECC_G1
S/MIME Issuing CAs
2. WISeKey CertifyID Advanced Services CA 4
4. WISeKey CertifyID Personal GB CA 3
5. WISeKey CertifyID Personal GB CA 4
7. WISeKey CertifyID Advanced GC CA 1
9. WISeKey CertifyID Client RSA CA 1
11. WISeKey CertifyID Client ECC CA 1

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=WISeKey CertifyID Advanced Services CA 4, OU=International, OU=Copyright (c) 2016 WISeKey SA, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WISeKey, C=CH	39FB381700000000000D	Feb 10 16:53:24 2016 GMT	Dec 11 16:09:51 2037 GMT	41144BD4174C3152E1CA526F77D9F9CE89DEBC4EBA6C778F815C21164B5101D3
3.	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
4.	1	CN=WISeKey CertifyID Personal GB CA 3, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	330000001B8161C85F062B5BCE00000000001B	Jul 4 15:12:21 2020 GMT	Dec 1 15:10:31 2039 GMT	E5937790AA6915755C9A532B10C9610A07C9877C7C60E1B819A294207A3786F5
5.	1	CN=WISeKey CertifyID Personal GB CA 4, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	330000001CCD876BC9754EA7CB00000000001C	Jul 4 15:20:26 2020 GMT	Jul 4 15:30:26 2035 GMT	8D45BF32C041A7EE46325F06AE604FAF7142DD99373DDB1EB74C70488A56FFB8
6.	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
7.	1	CN=WISeKey CertifyID Advanced GC CA 1, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GC CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	1F00000007C30FBC43144D3B82000000000007	Aug 23 14:13:58 2017 GMT	May 9 09:58:33 2042 GMT	387D496B92202D4C443CD94FF42DA17DF2F1E68E244C2FBBA7E294DBDD11357B
8.	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
9.	1	CN=WISeKey CertifyID Client RSA CA 1, O=WISeKey, C=CH	CN=OISTE Client Root RSA G1, O=OISTE Foundation, C=CH	232FE4EDC8215E881E94FB0CD2F88DB9	Feb 20 16:06:44 2024 GMT	Feb 16 16:06:43 2039 GMT	41F8755AEE782FF08D8EBB579ABC33C93E9E5613FC146F86A86E012860B54ADA
10.	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	D9A32485A8CCA85539CEF12FFFFF711378A17851D73DA2732AB4302D763BD62B
11.	1	CN=WISeKey CertifyID Client ECC CA 1, O=WISeKey, C=CH	CN=OISTE Client Root ECC G1, O=OISTE Foundation, C=CH	38FD425E2EC6E92BED8870D3AD09691F	Feb 20 16:19:04 2024 GMT	Feb 16 16:19:03 2039 GMT	1F5233119B894DB95B4A3737397366457B566308CF8E30C4D2935EA7049013D0

APPENDIX B: LIST OF CERTIFICATION PRACTICE STATEMENTS

- **OISTE & WISEKEY CERTIFICATION PRACTICES STATEMENT**

Version	Date	Changes
4.0.2	21 March 2025	Minor changes
4.0.1	13 January 2025	Minor changes
4.0	09 December 2024	First consolidated CP/CPS

- **OISTE CERTIFICATION PRACTICES STATEMENT**

Version	Date	Changes
3.6	18 July 2024	Annual review.
3.5	15 August 2023	Updated for new S/MIME BR

- **OISTE WISeKey Root Certification Practice Statement**

Version	Date	Changes
3.9	15 March 2024	Updated to add new Issuing CAs

- **OISTE CERTIFICATE POLICY FOR PERSONAL CERTIFICATES**

Version	Date	Changes
1.5	18 July 2024	Annual review. No relevant changes.
1.4	15 August 2023	Updated for new S/MIME BR

APPENDIX C: LIST OF REPORTS TO CA/B FORUM

	Matter topic	Matter description
1	Pre-certificates revoked with certificateHold reason	Error caused by a bug in EJBCA, that was revoking "orphan" pre-certificates with certificateHold reason. ACTION: We strengthen the controls before applying new EJBCA versions and patches. https://bugzilla.mozilla.org/show_bug.cgi?id=1824257
2	S/MIME certificate issuance without proper validation	A bug in the Free Certificate Request Form allowed potential attackers to obtain certificates for a mailbox different from the one validated. The issue was detected by an independent researcher and reported to WISeKey. ACTION: Development and testing workflows were reinforced to include systematic peer reviews. https://bugzilla.mozilla.org/show_bug.cgi?id=1949755

OISTE/WISeKey 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 9th 2024 through May 8th 2025

The International Organization for the Security of Electronic Transactions ("**OISTE**") operates the Certification Authority (CA) services known as "**OISTE/WISeKey Global Trust Model**" hierarchy with its Root Certification Authorities as detailed in Attachment A, and provides S/MIME CA services.

The management of OISTE/WISeKey is responsible for establishing and maintaining effective controls over its S/MIME CA services, including its S/MIME CA business practices disclosure on its website https://github.com/OISTE/repository/tree/main, 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/Wisekey's Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

OISTE/WISeKey management has assessed its disclosures of its certificate practices and controls over its S/MIME CA services. Based on that assessment, in providing its S/MIME Certification Authority (CA) services at Switzerland, throughout the period May 9th 2024 through May 8th 2025, OISTE/WISeKey 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/WISeKey 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/WISeKey)
- 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

In accordance with the WebTrust Principles and Criteria for Certification Authorities – S/MIME v1.0.3, as published at [https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/01618-ms_24-3464_webtrust-for-ca-smime-certificates-v1-0-3_final.pdf]

Geneva, 7th July 2025

Philippe Doubre
OISTE President

Carlos Moreira
CEO

Appendix A: PKI Hierarchy in scope of the WebTrust audit

OISTE WISeKey Global Root GA CA

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
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	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	
2.	CN=WISeKey CertifyID Advanced Services CA 4, OU=International, OU=Copyright (c) 2016 WISeKey SA, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WISeKey, C=CH	41:14:4B:D4:17:4C:31:52:E1:CA:52:6F:77:D9:F9:CE:89:DE:BC:4E:BA:6C:77:8F:81:5C:21:16:4B:51:01:D3	Issuing CA	ACTIVE	Previously allowed also for SSL Certificates

OISTE WISeKey Global Root GB CA

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
3.	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	
4.	CN= WISeKey CertifyID Personal GB CA 3, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	E5:93:77:90:AA:69:15:75:5C:9A:53:2B:10:C9:61:0A:07:C9:87:7C:7C:60:E1:B8:19:A2:94:20:7A:37:86:F5	Issuing CA	ACTIVE	Constrained by EKU extension Enabled for S/MIME Certificates
5.	CN= WISeKey CertifyID Personal GB CA 4, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	8D:45:BF:32:C0:41:A7:EE:46:32:5F:06:AE:60:4F:AF:71:42:DD:99:37:3D:DB:1E:B7:4C:70:48:8A:56:FF:B8	Issuing CA	ACTIVE	Constrained by EKU extension Enabled for S/MIME Certificates

OISTE WISeKey Global Root GC CA

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
6.	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	
7.	CN=WISeKey CertifyID Advanced GC CA 1, O=WISeKey, C=CH	CN= OISTE WISeKey Global Root GC CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	38:7D:49:6B:92:20:2D:4C:44:3C:D9:4F:F4:2D:A1:7D:F2:F1:E6:8E:24:4C:2F:BB:A7:E2:94:DB:DD:11:35:7B	Issuing CA	INACTIVE	Disabled in PKI platform

OISTE Client Root RSA G1

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
8.	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	
9.	CN=WISeKey CertifyID Client RSA CA 1, O=WISeKey, C=CH	CN=OISTE Client Root RSA G1, O=OISTE Foundation, C=CH	41:F8:75:5A:EE:78:2F:F0:8D:8E:BB:57:9A:BC:33:C9:3E:9E:56:13:FC:14:6F:86:A8:6E:01:28:60:B5:4A:DA	Issuing CA	ACTIVE	Constrained by EKU extension Enabled for S/MIME Certificates

OISTE Client Root ECC G1

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
10.	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	
11.	CN=WISeKey CertifyID Client ECC CA 1, O=WISeKey, C=CH	CN=OISTE Client Root ECC G1, O=OISTE Foundation, C=CH	1F:52:33:11:9B:89:4D:B9:5B:4A:37:37:39:73:66:45:7B:56:63:08:CF:8E:30:C4:D2:93:5E:A7:04:90:13:D0	Issuing CA	ACTIVE	Constrained by EKU extension Enabled for S/MIME Certificates

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

CP Documents

CP for Personal Certificates

Version	Date	Changes
1.5	18 July 2024	Annual review. No relevant changes.
1.4	15 August 2023	Updated for new S/MIME BR

Notes:

- The CP are defined by the OISTE Foundation, and WISeKey adheres to it as subordinate CA, under the OISTE Roots

CPS Documents

OISTE & WISEKEY CERTIFICATION PRACTICES STATEMENT

Version	Date	Changes
4.0.2	21 March 2025	Minor changes
4.0.1	13 January 2025	Minor changes
4.0	09 December 2024	First consolidated CP/CPS

OISTE CERTIFICATION PRACTICES STATEMENT

Version	Date	Changes
3.6	18 July 2024	Annual review
3.5	15 August 2023	Updated for new S/MIME BR

OISTE WISeKey Root Certification Practice Statement

Version	Date	Changes
3.9	15 March 2024	Updated to add new Issuing CAs

Appendix C: Disclosure of incidents during the period

	Matter topic	Matter description
1.	Pre-certificates revoked with certificateHold reason	Error caused by a bug in EJBCA, that was revoking “orphan” pre-certificates with certificateHold reason. ACTION: We strengthen the controls before applying new EJBCA versions and patches. https://bugzilla.mozilla.org/show_bug.cgi?id=1824257
2.	S/MIME certificate issuance without proper validation	A bug in the Free Certificate Request Form allowed potential attackers to obtain certificates for a mailbox different from the one validated. The issue was detected by an independent researcher and reported to WISeKey. ACTION: Development and testing workflows were reinforced to include systematic peer reviews. https://bugzilla.mozilla.org/show_bug.cgi?id=1949755