Valencia, July 09, 2025

Independent Assurance Report

To the Management of the 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, OISTE/WISeKey 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/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 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/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 – SSL Baseline v2.8. (https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/01618-ms_24-3464_webtrust-for-ca-ssl-baseline-v2-8_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 – SSL Baseline v2.8.

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 SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of SSL certificates,
(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/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 – SSL Baseline v2.8.

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 – SSL Baseline v2.8, nor the suitability of any of OISTE/Wisekey's services for any customer's intended purpose.

Use of the WebTrust seal

OISTE/Wisekey's use of the WebTrust for Certification Authorities – SSL Baseline 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 GB CA
5. OISTE WISeKey Global Root GC CA
8. OISTE_Server_Root_RSA_G1
10. OISTE_Server_Root_ECC_G1
OV SSL Issuing Cas
2. WISeKey CertifyID SSL GB CA 2
3. TuringSign RSA Secure CA
4. TuringSign ECC Secure CA
6. WISeKey CertifyID Advanced GC CA 1
7. WISeKey CertifyID SSL GC CA 1
9. WISeKey CertifyID Server RSA CA 1
11. WISeKey CertifyID Server ECC CA 1
EV SSL Issuing Cas
2. WISeKey CertifyID SSL GB CA 2
3. TuringSign RSA Secure CA
4. TuringSign ECC Secure CA
6. WISeKey CertifyID Advanced GC CA 1
9. WISeKey CertifyID Server RSA CA 1
11. WISeKey CertifyID Server ECC CA 1

CA Identifying Information for 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=WISeKey CertifyID SSL GB CA 2, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	330000001D6C1C9E01D66B39B900000000001D	Jul 4 15:25:26 2020 GMT	Jul 4 15:35:26 2035 GMT	C8A610BA9417770D2C02DE22BCA8C56A428AF75E8E354EFA36C568221DDB7CFC
3.	1	CN=TuringSign RSA Secure CA, O=Turing Crypto GmbH, C=DE	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	330000001F6998AF8A69E2E4CC00000000001F	Jun 21 11:43:07 2021 GMT	Jun 21 11:53:07 2026 GMT	12976558B68E8E1EAA79A629A8E4D17EDEF93F5AC30DE6DFB0CDEE389D56D156
4.	1	CN=TuringSign ECC Secure CA, O=Turing Crypto GmbH, C=DE	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	3300000020738162853491282D000000000020	Jun 21 11:45:10 2021 GMT	Jun 21 11:55:10 2026 GMT	1937B9BF662FB578407B77AB87D8D662B16327CF923340D0F72D951952B19C80
5.	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
6.	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
7.	1	CN=WISeKey CertifyID SSL GC CA 1, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GC CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	30EF3ECCDA882A63379BF35F66DF835C74959B	Feb 20 15:56:56 2024 GMT	Feb 16 15:56:55 2039 GMT	B05E05CFCBF81813EC30FA3F74920AA23FED367E147CC81E1121F64698449D0F
8.	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
9.	1	CN=WISeKey CertifyID Server RSA CA 1, O=WISeKey, C=CH	CN=OISTE Server Root RSA G1, O=OISTE Foundation, C=CH	328F33BCBD426EB9CD896D524A77E308	Feb 20 16:15:20 2024 GMT	Feb 16 16:15:19 2039 GMT	AE70FF8A3E11C7F95C3BAB3C8FB55EF4CB06EB4559469E9B90ED6EF7FC6DDE4E
10.	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
11.	1	CN=WISeKey CertifyID Server ECC CA 1, O=WISeKey, C=CH	CN=OISTE Server Root ECC G1, O=OISTE Foundation, C=CH	47C8782ECC023DF7C7247F7D6A997B60	Feb 20 16:12:02 2024 GMT	Feb 16 16:12:01 2039 GMT	042FCAA086492C92FB02A82AC957489E5C61E47B6E9A6901BBB548A8AC88A380

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 SSL/TLS CERTIFICATES**

Version	Date	Changes
1.6	18 July 2024	Annual review. No significant changes
1.5	24 January 2024	Annual review. No changes.

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

OISTE/WISeKey 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 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 SSL and non-SSL CA services.

The management of OISTE/WISeKey is responsible for establishing and maintaining effective controls over its SSL (and non-SSL) CA operations, including its SSL CA business practices disclosure on its website: [https://github.com/OISTE/repository/tree/main], [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/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 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 2024 through May 8th 2025, OISTE/WISeKey has:

- disclosed its SSL certificate lifecycle, practices in the document “OISTE/WISeKey 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/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 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/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 – SSL Baseline v2.8 (https://www.cpacanada.ca/-/media/site/operational/ms-member-services/docs/webtrust/01618-ms_24-3464_webtrust-for-ca-ssl-baseline-v2-8_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 SSL GB CA 2, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	C8:A6:10:BA:94:17:77:0D:2C:02:DE:22:BC:A8:C5:6A:42:8A:F7:5E:8E:35:4E:FA:36:C5:68:22:1D:DB:7C:FC	Issuing CA	ACTIVE	Constrained by EKU extension Enabled for EV SSL Certificates
5.	CN= TuringSign RSA Secure CA, O=Turing Crypto GmbH, C=DE	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	12:97:65:58:B6:8E:8E:1E:AA:79:A6:29:A8:E4:D1:7E:DE:F9:3F:5A:C3:0D:E6:DF:B0:CD:EE:38:9D:56:D1:56	Issuing CA	ACTIVE	Constrained by EKU extension Enabled for EV SSL Certificates
6.	CN= TuringSign ECC Secure CA, O=Turing Crypto GmbH, C=DE	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	19:37:B9:BF:66:2F:B5:78:40:7B:77:AB:87:D8:D6:62:B1:63:27:CF:92:33:40:D0:F7:2D:95:19:52:B1:9C:80	Issuing CA	ACTIVE	Constrained by EKU extension Enabled for EV SSL Certificates

OISTE WISeKey Global Root GC CA

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
7.	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	
8.	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
9.	CN=WISeKey CertifyID SSL GC CA 1, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GC CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	B0:5E:05:CF:CB:F8:18:13:EC:30:FA:3F:74:92:0A:A2:3F:ED:36:7E:14:7C:C8:1E:11:21:F6:46:98:44:9D:0F	Issuing CA	ACTIVE	Constrained by EKU extension Enabled for EV SSL Certificates

OISTE Server Root RSA G1

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
10.	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	

11.	CN=WISeKey CertifyID Server RSA CA 1, O=WISeKey, C=CH	CN=OISTE Server Root RSA G1, O=OISTE Foundation, C=CH	AE:70:FF:8A:3E:11:C7:F9:5C:3B:AB:3C:8F:B5:5E:F4:CB:06:EB:45:59:46:9E:9B:90:ED:6E:F7:FC:6D:DE:4E	Issuing CA	ACTIVE	Constrained by EKU extension Enabled for EV SSL Certificates

OISTE Server Root ECC G1

CA#	Subject Name	Issuer Name	Fingerprint	CA Type	Status	Comments
12.	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	
13.	CN=WISeKey CertifyID Server ECC CA 1, O=WISeKey, C=CH	CN=OISTE Server Root ECC G1, O=OISTE Foundation, C=CH	04:2F:CA:A0:86:49:2C:92:FB:02:A8:2A:C9:57:48:9E:5C:61:E4:7B:6E:9A:69:01:BB:B5:48:A8:AC:88:A3:80	Issuing CA	ACTIVE	Constrained by EKU extension Enabled for EV SSL Certificates

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

CP Documents

CP for SSL Certificates

Version	Date	Changes
1.6	18 July 2024	Annual review. No significant changes
1.5	24 January 2024	Annual review. No changes.

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