

Independent Assurance Report

To the Management of WISEKey SA (WISEKey):

Scope

We have been engaged, in a reasonable assurance engagement, to report on WISEKey management's assertion that for its Certification Authority (CA) operations at Geneva, Switzerland, throughout the period May 9th, 2017 through May 8th, 2018 for its "OISTE WISEKey Global Root GA", "OISTE WISEKey Global Root GB" and "OISTE WISEKey Global Root GC" hierarchies with its Delegated Certification Authorities as detailed in Appendix A, WISEKey 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.
- maintained effective controls to provide reasonable assurance that:
 - WISEKey provides its services in accordance with its Certification Practice Statements
- maintained effective 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 WISEKey); and
 - subordinate CA certificate requests are accurate, authenticated, and approved.
- 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 v2.0.

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



WISeKey does not escrow its CA keys. Accordingly, our procedures did not extend to controls that would address those criteria.

Certification authority's responsibilities

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 v2.0.

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 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 WISeKey'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) selectively testing transactions executed in accordance with disclosed key and certificate lifecycle management business 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.

Relative effectiveness of controls

The relative effectiveness and significance of specific controls at 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

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

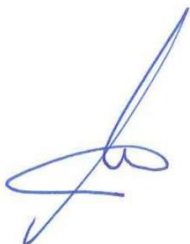
Opinion

In our opinion, throughout the period May 9th, 2017 through May 8th, 2018, 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 v2.0.

This report does not include any representation as to the quality of WISeKey's services beyond those covered by the WebTrust Principles and Criteria for Certification Authorities v2.0, nor the suitability of any of WISeKey's services for any customer's intended purpose.

Use of the WebTrust seal

WISeKey's use of the WebTrust for Certification Authorities 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 23rd, 2018



APPENDIX A: PKI Hierarchy in scope of the Webtrust audit

OISTE WISEKey Global Root GA CA

CA#	Subject	Issuer	serialNumber	Key Type	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
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	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
1.1	CN=WISEKey CertifyID Advanced G1 CA, OU=International, OU=Copyright (c) 2005 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	6191DBA10000000002	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Dec 11 17:50:47 2005 GMT	Dec 11 18:00:47 2020 GMT	50:1F:30:C0:93:92:8D:71:23:38:34:5C:B9:0A:F6:D3:2B:EB:81:45	46:A2:A3:A0:F1:1E:03:C0:3A:41:F3:E5:17:5F:D5:8B:EC:10:22:FB:81:EB:93:49:31:7E:1F:DB:A6:4C:C3:D4
1.1.1	CN=WISEKey CertifyID Advanced Services CA 2, OU=International, OU=Copyright 2011 WISEKey SA, O=WISEKey, C=CH	CN=WISEKey CertifyID Advanced G1 CA, OU=International, OU=Copyright (c) 2005 WISEKey SA, O=WISEKey, C=CH	341818F70000000001A	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Feb 9 15:37:32 2011 GMT	Dec 11 18:00:47 2020 GMT	D7:2F:2F:F3:09:F1:56:21:53:1D:E7:4C:2E:48:44:4A:DA:86:FD:98	0A:D7:41:D9:8A:84:C3:B9:C4:E7:55:2E:15:BF:F1:E3:69:B6:80:68:39:45:5D:BA:FC:AC:63:81:24:D5:F1:00

End-entity: PolicyIdentifier	Name and type
2.16.756.5.14.4.3.2.1.1	Secure Email -CertifyID Advanced User
2.16.756.5.14.4.3.2.1.3	Secure Email -CertifyID Advanced Corporate User
2.16.756.5.14.4.3.2.1.4	Secure Server Certificate -CertifyID Advanced Server
2.16.756.5.14.4.7.1	Time Stamp Certificate

1.2	CN=WISEKey CertifyID Advanced Services CA 3, OU=International, OU=Copyright (c) 2015 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	43230BA40000000006	rsaEncryption - 2048 bit	sha256WithRSAEncryption	Jul 28 15:22:20 2015 GMT	Jul 28 15:32:20 2030 GMT	6E:87:78:D6:3A:58:8A:C8:BE:60:E5:21:7E:F1:FE:6E:F0:B6:E0:75	6F:90:A5:FD:98:8F:AE:CC:EC:5B:17:E5:61:2F:F3:6D:19:9C:88:45:51:F3:94:F3:1A:AB:A4:F9:21:E4:2A:05
-----	--	--	--------------------	--------------------------	-------------------------	--------------------------	--------------------------	---	---

End-entity: PolicyIdentifier	Name and type
2.16.756.5.14.4.3.2.1.4	Secure Server Certificate - CertifyID Advanced Server

1.3	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	39FB38170000000000D	rsaEncryption - 2048 bit	sha256WithRSAEncryption	Feb 10 16:53:24 2016 GMT	Dec 11 16:09:51 2037 GMT	F4:E4:9B:57:D2:AE:C2:9E:88:4D:00:BA:2B:AF:65:C9:63:A9:87:9B	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
-----	--	--	---------------------	--------------------------	-------------------------	--------------------------	--------------------------	---	---

End-entity: PolicyIdentifier	Name and type
2.16.756.5.14.4.3.2.1.4	Secure Server Certificate -CertifyID Advanced Server



1.4	CN=WiSeKey CertifyID Policy GA CA 1, O=WiSeKey, C=CH	CN=OISTE WiSeKey Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WiSeKey, C=CH	1824B8690000000000B	rsaEncryption - 2048 bit	sha256WithRSAEncryption	Dec 16 10:08:51 2015 GMT	Dec 11 16:09:51 2013 GMT	0D:B0:C5:0B:8D:34:F7:C5:54:59:C5:23:F5:7A:43:75:AB:E0:8E:0F	05:74:6C:EA:C8:30:B3:84:40:5A:B7:3C:D6:23:9D:E4:2C:E9:F4:87:55:3E:F3:FA:8B:0A:06:4E:57:92:68:3C
1.5	CN=WiSeKey CertifyID Qualified G1 CA, OU=International, OU=Copyright (c) 2006 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	6106E07600000000004	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Oct 17 15:48:05 2006 GMT	Oct 17 15:58:05 2021 GMT	B8:B5:F8:53:D2:72:3D:73:F6:BB:64:67:A7:E5:64:EB:12:EA:73:62	68:C1:82:C8:FE:37:4D:5C:09:4E:63:25:95:59:F2:F0:76:4A:58:97:43:58:3F:4A:03:E3:F6:3B:74:D7:AE:EA
1.5.1	CN=WiSeKey Qualified Services CA 2, OU=International, OU=Copyright (c) 2013 WiSeKey SA, O=WiSeKey, C=CH	CN=WiSeKey CertifyID Qualified G1 CA, OU=International, OU=Copyright (c) 2006 WiSeKey SA, O=WiSeKey, C=CH	7C4416CE000000000007	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Oct 24 15:10:19 2013 GMT	Oct 17 15:58:05 2021 GMT	B6:74:71:9D:74:EA:AA:C1:71:62:97:D0:78:86:2B:A0:C5:54:EC:11	30:0E:B3:21:90:57:8B:9A:C5:78:E1:A1:D2:80:04:21:91:45:69:8C:E3:B6:3F:29:DF:21:EE:4C:54:2C:08:85

End-entity: PolicyIdentifier	Name and type
2.16.756.5.14.4.4.2.1.3	CertifyID Qualified Individual for Adobe
2.16.756.5.14.4.4.2.1.4	CertifyID Qualified Corporate for Adobe

1.6	CN=WiSeKey CertifyID Standard G1 CA, OU=International, OU=Copyright (c) 2005 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	610D977400000000003	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Dec 23 10:45:32 2005 GMT	Dec 23 10:55:32 2020 GMT	FA:D8:71:32:3C:DC:EA:D2:35:7E:5F:D8:64:E2:F1:FF:1C:66:AB:6D	AE:DA:9E:12:9E:5F:BA:12:53:CA:79:11:6A:ED:99:0D:DF:AA:AB:24:BD:48:A1:CC:BD:99:A7:E0:3C:9D:DB:96
1.6.1	CN=WiSeKey CertifyID Standard Services CA 2, OU=International, OU=Copyright (c) 2012 WiSeKey SA, O=WiSeKey, C=CH	CN=WiSeKey CertifyID Standard G1 CA, OU=International, OU=Copyright (c) 2005 WiSeKey SA, O=WiSeKey, C=CH	12E3815300000000001D	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Jan 23 15:32:20 2012 GMT	Dec 23 10:55:32 2020 GMT	BB:F5:CE:AE:5B:28:21:4B:DC:02:B4:4D:4D:8F:B3:4A:E2:B4:E1:93	13:4A:96:99:68:C7:0E:47:65:13:B3:7B:01:3D:8C:13:8C:21:10:46:69:B5:AD:62:D4:D5:FA:B1:68:69:B9:EA

End-entity: PolicyIdentifier	Name and type
2.16.756.5.14.4.4.1.1	Secure Email -CertifyID Standard User



OISTE WISeKey Global Root GB CA

CA#	Subject	Issuer	serialNumber	Key Type	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
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	sha256WithRSANcrypton	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	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
2.1	CN=WISeKey CertifyID Policy GB CA 1, O=WISeKey, C=CH, O=WISeKey, C=CH	CN=OISTE WISeKey Global Root GB CA, OU=OISTE Foundation Endorsed, O=WISeKey, C=CH	1503E4CC0000000009	rsaEncryption - 2048 bit	sha256WithRSANcrypton	May 13 15:09:04 2015 GMT	Dec 1 15:10:31 2039 GMT	D1:E6:0B:82:25:74:25:2C:55:91:D5:03:18:7B:BF:C1:EE:AF:1D:80	59:15:9F:BC:93:49:71:93:FC:1A:20:CA:6E:CF:A5:97:A0:00:18:A1:05:11:2A:60:04:B7:9C:32:92:49:47:60
2.1.1	CN=WISeKey CertifyID Advanced GB CA 2, O=WISeKey, C=CH	CN=WISeKey CertifyID Policy GB CA 1, O=WISeKey, C=CH	098BADEE59C7FAB9	rsaEncryption - 2048 bit	sha256WithRSANcrypton	May 27 15:22:04 2015 GMT	Dec 1 15:10:31 2039 GMT	A0:1C:B2:3F:3F:6A:4A:A0:BF:83:BB:FC:79:C3:AA:CB:1D:DF:DE:75	68:E6:29:2F:D4:AA:38:4D:63:A5:F4:FA:8B:D8:85:BD:16:56:E3:50:9B:A4:20:66:73:E0:66:0A:16:9F:E7:01

End-entity: PolicyIdentifier	Name and type
2.16.756.5.14.7.4.2	CertifyID Advanced Personal Certificate
2.16.756.5.14.7.4.6	CertifyID Standard SSL Certificate
2.16.756.5.14.7.4.7	CertifyID Advanced OV SSL Certificate
2.16.756.5.14.7.4.8	CertifyID Advanced EV SSL Certificate

2.1.2	CN=WISeKey CertifyID Qualified GB CA 2, O=WISeKey, C=CH	CN=WISeKey CertifyID Policy GB CA 1, O=WISeKey, C=CH	5863A1D7E83FB060	rsaEncryption - 2048 bit	sha256WithRSANcrypton	May 27 16:02:04 2015 GMT	Dec 1 15:10:31 2039 GMT	06:93:7D:BD:69:39:52:72:D7:8B:B5:FB:3F:C2:CB:CC:9C:6B:05:C3	04:AB:EE:21:CF:8C:B7:74:F0:F7:AB:14:8F:19:7B:5E:14:C2:70:6E:68:69:90:2F:B9:9D:09:48:70:94:C8:F6
-------	---	--	------------------	--------------------------	-----------------------	--------------------------	-------------------------	---	---

End-entity: PolicyIdentifier	Name and type
2.16.756.5.14.7.4.4	CertifyID Qualified Personal Certificate
2.16.756.5.14.7.4.5	CertifyID Qualified Corporate Certificate
2.16.756.5.14.7.4.9	CertifyID Code Signing Certificate
2.16.756.5.14.7.4.10	CertifyID EV Code Signing Certificate

2.1.3	CN=WISeKey CertifyID Standard GB CA 2, O=WISeKey, C=CH	CN=WISeKey CertifyID Policy GB CA 1, O=WISeKey, C=CH	6B0549F708B200BE	rsaEncryption - 2048 bit	sha256WithRSANcrypton	May 27 15:44:36 2015 GMT	Dec 1 15:10:31 2039 GMT	50:BE:94:10:8E:4E:59:2B:B4:06:70:91:49:2A:9B:57:39:7C:83:AE	33:16:AF:F1:FD:EB:87:E3:72:26:8A:A5:B6:91:82:0A:25:4C:8D:24:BB:09:B1:25:A2:8A:0A:C8:F4:22:F0:F4
-------	--	--	------------------	--------------------------	-----------------------	--------------------------	-------------------------	---	---

End-entity: PolicyIdentifier	Name and type
2.16.756.5.14.7.4.1	CertifyID Standard Personal Certificate



OISTE WISeKey Global Root GC CA

CA#	Subject	Issuer	serialNumber	Key Type	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
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	212A560CA EDA0CAB40 45BF2BA22 D3AEA	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	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
3.1	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	1F0000000 7C30FBC43 144D3B820 000000000 07	id-ecPublicKey - 384 bit	ecdsa-with-SHA384	Aug 23 14:13:58 2017 GMT	May 9 09:58:33 2042 GMT	38:0C:44:5F:AA:4A:8B:7E:C6:5B:ED:0F:AC:A8:D1:58:4F:31:7E:C2	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

End-entity: PolicyIdentifier	Name and type
2.16.756.5.14.8.2.1	CertifyID Device Certificate
2.16.756.5.14.9.4.2	CertifyID Corporate Advanced Certificate
2.16.756.5.14.9.4.7	CertifyID Advanced OV SSL Certificate

APPENDIX B: LIST OF CERTIFICATION PRACTICE STATEMENTS

Version	Date	Changes
2.6	12/11/2016	Minor changes to add support to special OIDs
2.8	19/6/2017	Inclusion of new GC Root Minor changes to adapt to latest BR Minor edits on document change management procedures Minor edits on certificate templates.
2.9	25/7/2017	Minor changes after Webtrust assessment
2.10	18/4/2018	Modified to limit issuance of SSL certificates to 2 years (825 days for acceptance of previous identity validation) Minor changes to adapt to latest BR
2.11	23/5/2018	Minor changes to improve BR compliance Corrected a typo in Fingerprint of GC Root



WIS@key MANAGEMENT'S ASSERTION

as to its Disclosure of its Business Practices and Controls over its Certification Authority Operations during the period from May 9th 2017 through May 8th 2018

WIS@key SA (“**WIS@key**”) operates the Certification Authority (CA) services known as “**OISTE WIS@key Global Root GA**”, “**OISTE WIS@key Global Root GB**” and “**OISTE WIS@key Global Root GC**” (hierarchies with its subordinated 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 **WIS@key** is responsible for establishing and maintaining effective controls over its CA operations, including its CA business practices disclosure on its website [<https://www.wisekey.com/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 **WIS@key's** Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

WIS@key management has assessed its disclosures of its certificate practices and controls over its CA services. Based on that assessment, in **WIS@key** management's opinion, in providing its Certification Authority (CA) services at its main and disaster recover datacentres in Switzerland, throughout the period May 9th 2017 through May 8th 2018, **WIS@key** has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the document “OISTE WIS@key Root Certification Practice Statement” as enumerated in Attachment B (combined CP & CPS documents)
- maintained effective controls to provide reasonable assurance that **WIS@key** provides its services in accordance with its Certificate Policy(ies) and Certification Practice Statement
- maintained effective 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 **WIS@key**); and
- subordinate CA certificate requests are accurate, authenticated, and approved
- 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 v2.0 [<http://www.webtrust.org/homepage-documents/item54279.pdf>], including the following:

CA Business Practices Disclosure

- Certification Practice Statement (CPS)
- Certificate Policy (CP, embedded in CPS document)

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

WiSeKey does not escrow its CA keys. Accordingly, our assertion does not extend to controls that would address those criteria.

Geneva, 23rd July 2018

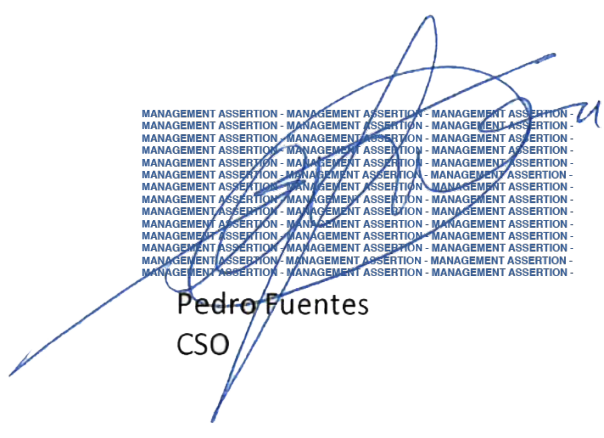
MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -

Carlos Moreira
CEO



MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -
 MANAGEMENT ASSERTION - MANAGEMENT ASSERTION - MANAGEMENT ASSERTION -

Pedro Fuentes
CSO



Appendix A: PKI Hierarchy in scope of the WebTrust audit

OISTE WIS@key Global Root GA CA

CA#	Subject	Issuer	serialNumber	Key Type	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
1	CN=OISTE WIS@key Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WIS@key, C=CH	CN=OISTE WIS@key Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WIS@key, 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	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
1.1	CN=WIS@key CertifyID Advanced G1 CA, OU=International, OU=Copyright (c) 2005 WIS@key SA, O=WIS@key, C=CH	CN=OISTE WIS@key Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WIS@key, C=CH	6191DBA10000000002	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Dec 11 17:50:47 2005 GMT	Dec 11 18:00:47 2020 GMT	50:1F:30:C0:93:92:8D:71:23:38:34:5C:B9:0A:F6:D3:2B:EB:81:45	46:A2:A3:A0:F1:1E:03:C0:3A:41:F3:E5:17:5F:D5:8B:EC:10:22:FB:81:EB:93:49:31:7E:1F:DB:A6:4C:C3:D4
1.1.2	CN=WIS@key CertifyID Advanced Services CA 2, OU=International, OU=Copyright 2011 WIS@key SA, O=WIS@key, C=CH	CN=WIS@key CertifyID Advanced G1 CA, OU=International, OU=Copyright (c) 2005 WIS@key SA, O=WIS@key, C=CH	341818F70000000001A	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Feb 9 15:37:32 2011 GMT	Dec 11 18:00:47 2020 GMT	D7:2F:2F:F3:09:F1:56:21:53:1D:E7:4C:2E:48:44:4A:DA:86:FD:98	0A:D7:41:D9:8A:84:C3:B9:C4:E7:55:2E:15:BF:F1:E3:69:B6:80:68:39:45:5D:BA:FC:AC:63:81:24:D5:F1:00
1.2	CN=WIS@key CertifyID Advanced Services CA 3, OU=International, OU=Copyright (c) 2015 WIS@key SA, O=WIS@key, C=CH	CN=OISTE WIS@key Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WIS@key, C=CH	43230BA400000000006	rsaEncryption - 2048 bit	sha256WithRSAEncryption	Jul 28 15:22:20 2015 GMT	Jul 28 15:32:20 2030 GMT	6E:87:78:D6:3A:58:8A:C8:BE:60:E5:21:7E:F1:FE:6E:F0:B6:E0:75	6F:90:A5:FD:98:8F:AE:CC:EC:5B:17:E5:61:2F:F3:6D:19:9C:88:45:51:F3:94:F3:1A:AB:A4:F9:21:E4:2A:05
1.3	CN=WIS@key CertifyID Advanced Services CA 4, OU=International, OU=Copyright (c) 2016 WIS@key SA, O=WIS@key, C=CH	CN=OISTE WIS@key Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WIS@key, C=CH	39FB38170000000000D	rsaEncryption - 2048 bit	sha256WithRSAEncryption	Feb 10 16:53:24 2016 GMT	Dec 11 16:09:51 2037 GMT	F4:E4:9B:57:D2:AE:C2:9E:88:4D:00:BA:2B:AF:65:C9:63:A9:87:9B	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
1.4	CN=WIS@key CertifyID Policy GA CA 1, O=WIS@key, C=CH	CN=OISTE WIS@key Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WIS@key, C=CH	1824B8690000000000B	rsaEncryption - 2048 bit	sha256WithRSAEncryption	Dec 16 10:08:51 2015 GMT	Dec 11 16:09:51 2037 GMT	0D:B0:C5:0B:8D:34:F7:C5:54:59:C5:23:F5:7A:43:75:AB:E0:8E:0F	05:74:6C:EA:C8:30:B3:84:40:5A:B7:3C:D6:23:9D:E4:2C:EB:F4:87:55:3E:F3:FA:8B:0A:06:4E:57:92:68:3C
1.5	CN=WIS@key CertifyID Qualified G1 CA, OU=International, OU=Copyright (c) 2006 WIS@key SA, O=WIS@key, C=CH	CN=OISTE WIS@key Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WIS@key, C=CH	6106E07600000000004	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Oct 17 15:48:05 2006 GMT	Oct 17 15:58:05 2021 GMT	B8:B5:F8:53:D2:72:3D:73:F6:BB:64:67:A7:E5:64:EB:12:EA:73:62	68:C1:82:C8:FE:37:4D:5C:09:4E:63:25:95:59:F2:F0:76:4A:58:97:43:58:3F:4A:03:E3:F6:3B:74:D7:AE:EA
1.5.2	CN=WIS@key Qualified Services CA 2, OU=International, OU=Copyright (c) 2013 WIS@key SA, O=WIS@key, C=CH	CN=WIS@key CertifyID Qualified G1 CA, OU=International, OU=Copyright (c) 2006 WIS@key SA, O=WIS@key, C=CH	7C4416CE00000000007	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Oct 24 15:10:19 2013 GMT	Oct 17 15:58:05 2021 GMT	B6:74:71:9D:74:EA:AA:C1:71:62:97:D0:78:86:2B:A0:C5:54:EC:11	30:0E:B3:21:90:57:8B:9A:C5:78:E1:A1:D2:80:04:21:91:45:69:8C:E3:B6:3F:29:DF:21:EE:4C:54:2C:08:85
1.6	CN=WIS@key CertifyID Standard G1 CA, OU=International, OU=Copyright (c) 2005 WIS@key SA, O=WIS@key, C=CH	CN=OISTE WIS@key Global Root GA CA, OU=OISTE Foundation Endorsed, OU=Copyright (c) 2005, O=WIS@key, C=CH	610D977400000000003	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Dec 23 10:45:32 2005 GMT	Dec 23 10:55:32 2020 GMT	FA:D8:71:32:3C:DC:EA:D2:35:7E:5F:D8:64:E2:F1:FF:1C:66:AB:6D	AE:DA:9E:12:9E:5F:BA:12:53:CA:79:11:6A:ED:99:0D:DF:AA:AB:24:BD:48:A1:CC:BD:99:A7:E0:3C:9D:DB:96
1.6.2	CN=WIS@key CertifyID Standard Services CA 2, OU=International, OU=Copyright (c) 2012 WIS@key SA, O=WIS@key, C=CH	CN=WIS@key CertifyID Standard G1 CA, OU=International, OU=Copyright (c) 2005 WIS@key SA, O=WIS@key, C=CH	12E3815300000000001D	rsaEncryption - 2048 bit	sha1WithRSAEncryption	Jan 23 15:32:20 2012 GMT	Dec 23 10:55:32 2020 GMT	BB:F5:CE:AE:5B:28:21:4B:DC:02:B4:4D:4D:8F:B3:4A:E2:B4:E1:93	13:4A:96:99:68:C7:0E:47:65:13:B3:7B:01:3D:8C:13:8C:21:10:46:69:B5:AD:62:D4:D5:FA:B1:68:69:B9:EA

OISTE WIS@key Global Root GB CA

CA#	Subject	Issuer	serialNumber	Key Type	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
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	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	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
2.1	CN=WIS@key CertifyID Policy GB CA 1, O=WIS@key, C=CH, O=WIS@key, C=CH	CN=OISTE WIS@key Global Root GB CA, OU=OISTE Foundation Endorsed, O=WIS@key, C=CH	1503E4CC0000000009	rsaEncryption - 2048 bit	sha256WithRSAEncryption	May 13 15:09:04 2015 GMT	Dec 1 15:10:31 2039 GMT	D1:E6:0B:82:25:74:25:2C:55:91:D5:03:18:7B:BF:C1:EE:AF:1D:80	59:15:9F:BC:93:49:71:93:FC:1A:20:CA:6E:CF:A5:97:A0:00:18:A1:05:11:2A:60:04:B7:9C:32:92:49:47:60
2.1.1	CN=WIS@key CertifyID Advanced GB CA 2, O=WIS@key, C=CH	CN=WIS@key CertifyID Policy GB CA 1, O=WIS@key, C=CH	098BADEE59C7FAB9	rsaEncryption - 2048 bit	sha256WithRSAEncryption	May 27 15:22:04 2015 GMT	Dec 1 15:10:31 2039 GMT	A0:1C:B2:3F:3F:6A:4A:A0:BF:83:BB:FC:79:C3:AA:CB:1D:DF:DE:75	68:E6:29:2F:D4:AA:38:4D:63:A5:F4:FA:8B:D8:85:BD:16:56:E3:50:9B:A4:20:66:73:E0:66:0A:16:9F:E7:01
2.1.2	CN=WIS@key CertifyID Qualified GB CA 2, O=WIS@key, C=CH	CN=WIS@key CertifyID Policy GB CA 1, O=WIS@key, C=CH	5863A1D7E83FB060	rsaEncryption - 2048 bit	sha256WithRSAEncryption	May 27 16:02:04 2015 GMT	Dec 1 15:10:31 2039 GMT	06:93:7D:BD:69:39:52:72:D7:8B:B5:FB:3F:C2:CB:CC:9C:6B:05:C3	04:AB:EE:21:CF:8C:B7:74:F0:F7:AB:14:8F:19:7B:5E:14:C2:70:6E:68:69:90:2F:B9:9D:09:48:70:94:C8:F6
2.1.3	CN=WIS@key CertifyID Standard GB CA 2, O=WIS@key, C=CH	CN=WIS@key CertifyID Policy GB CA 1, O=WIS@key, C=CH	6B0549F708B200BE	rsaEncryption - 2048 bit	sha256WithRSAEncryption	May 27 15:44:36 2015 GMT	Dec 1 15:10:31 2039 GMT	50:BE:94:10:8E:4E:59:2B:B4:06:70:91:49:2A:9B:57:39:7C:83:AE	33:16:AF:F1:FD:EB:87:E3:72:26:8A:A5:B6:91:82:0A:25:4C:8D:24:BB:09:B1:25:A2:8A:0A:C8:F4:22:F0:F4

OISTE WIS@key Global Root GC CA

CA#	Subject	Issuer	serialNumber	Key Type	Sig Algorithm	notBefore	NotAfter	SKI	SHA256 Fingerprint
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	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	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
3.1	CN=WIS@key CertifyID Advanced GC CA 1, O=WIS@key, C=CH	CN=OISTE WIS@key Global Root GC CA, OU=OISTE Foundation Endorsed, O=WIS@key, C=CH	1F00000007C30FBC43144D3B820000000007	id-ecPublicKey - 384 bit	ecdsa-with-SHA384	Aug 23 14:13:58 2017 GMT	May 9 09:58:33 2042 GMT	38:0C:44:5F:AA:4A:8B:7E:C6:5B:ED:0F:AC:A8:D1:58:4F:31:7E:C2	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

Appendix B: CPS documents in scope of the WebTrust audit

Version	Date	URL
2.6	12/Nov/16	https://cdn.wisekey.com/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.6-CLEAN.pdf
2.8	19/June/17	https://cdn.wisekey.com/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.8-CLEAN.pdf
2.9	25/July/17	https://cdn.wisekey.com/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.9-CLEAN.pdf
2.10	18/April/18	https://cdn.wisekey.com/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.10-CLEAN.pdf
2.11	23/May/18	https://cdn.wisekey.com/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.11-CLEAN.pdf

Notes:

- Version 2.7 was not publicly released but just an internal working version