Valencia, July 23rd, 2018

## 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 GB" hierarchy with its Delegated Certification Authorities as detailed in Appendix A, WISeKey has:

- disclosed its Extended Validation SSL ("EV SSL") certificate lifecycle management business practices in its Certification Practice Statements as enumerated in Appendix B including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Requirement on the 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 EV SSL certificates it manages is established and protected throughout their lifecycles; and
  - EV SSL subscriber information is properly authenticated (for the registration activities performed by WISeKey)

in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.6.

## 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 – Extended Validation SSL – Version 1.6.

## 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 EV SSL certificate lifecycle management business practices, including its relevant controls over the issuance, renewal, and revocation of EV SSL certificates;
(2) selectively testing transactions executed in accordance with disclosed EV 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.

## 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

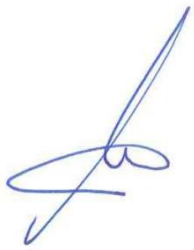
In our opinion, throughout the period May 9th, 2017 through May 8th, 2018, WISeKey management's assertion, as referred to above, is fairly stated, in all material respects, in accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL – Version 1.6.

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 – Extended Validation SSL – Version 1.6, 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 – Extended Validation SSL 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 SSL and Network Security audit

### 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 | 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=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 | 1503E4CC0000000000 09 | 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=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 | 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 |

| 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 | 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 |

| 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 | 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 |

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

# WISeKey MANAGEMENT'S ASSERTION

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

WISeKey SA ("**WISeKey**") operates the Certification Authority (CA) services known as "**OISTE WISeKey Global Root GB**" (hierarchy with its subordinated Certification Authorities as detailed in appendix A), and provides EV SSL CA services.

**WISeKey** management has assessed its disclosures of its certificate practices and controls over its EV SSL CA services. Based on that assessment, in providing its EV SSL (and non-SSL) Certification Authority (CA) services at its main and disaster recover datacentres in Switzerland, throughout the period May 9th 2017 through May 8th 2018, **WISeKey** has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in the document "OISTE WISeKey Root Certification Practice Statement as enumerated in Attachment B (combined CP & CPS documents), including its commitment to provide EV SSL certificates in conformity with the CA/Browser Forum Requirements on the **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 EV SSL certificates it manages is established and protected throughout their lifecycles; and
    - EV SSL subscriber information is properly authenticated (for the registration activities performed by **WISeKey**)

In accordance with the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL v1.6, as published at [http://www.webtrust.org/principles-and-criteria/docs/item83989.pdf].

Geneva, 23rd July 2018

Carlos Moreira
CEO

Pedro Fuentes
CSO

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

### 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 | 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=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 | 1503E4CC0000000000 09 | 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=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 | 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=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 | 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=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 | 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 |

## 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