Valencia, December 5th 2017

## Independent Assurance Report

To the Management of WISeKey SA (WISeKey):

## Scope

We have audited the Assertion by the management of WISeKey, for its SSL Certification Authority services at Geneva (Switzerland) through "OISTE WISeKey Global Root GC" hierarchy with its Delegated Advanced Certification Authorities as detailed in appendix 1 during the period from September 16th 2017 through December 4th 2017.

In this period, WISeKey has:

- disclosed its SSL certificate lifecycle management business practices in its:
  - OISTE WISeKey Root Certification Practice Statement - Version: 2.9
    https://cdn.wisekey.com/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.9-CLEAN.pdf

  including its commitment to provide 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 SSL certificates it manages is established and protected throughout their lifecycles; and
  - SSL subscriber information is properly authenticated (for the registration activities performed by 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

- 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

in accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2.

## 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 – SSL Baseline with Network Security v2.2.

## 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 behavior.

Auren 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 SSL certificate lifecycle management business practices including its relevant controls over the issuance, renewal, and revocation of SSL certificates and obtaining an understanding of WISeKey's network and certificate system security to meet the requirements set forth by the CA/Browser Forum
(2) evaluating the suitability of the design of the controls; and;
(3) performing such other procedures as we considered necessary in the circumstances.

We did not perform procedures to determine the operating effectiveness of controls for any period. Accordingly, we express no opinion on the operating effectiveness of any aspects of WISeKey's controls, individually or in the aggregate.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

## Suitability of controls

The suitability of the design of the 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 suitability of the design of the controls at individual subscriber and relying party locations.

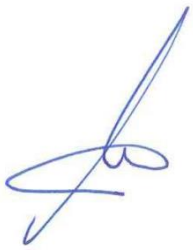
## Inherent limitations

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 from September 16th 2017 through December 4th 2017, 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 with Network Security v2.2.

This report does not include any representation as to the quality of WISeKey's services beyond those covered by the the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.2, nor the suitability of any of WISeKey's services for any customer's intended purpose.



F. Mondragon, Auditor

auren

Valencia, SPAIN

December 5th, 2017

## APPENDIX 1

# Generation C

**CN=OISTE WISeKey Global Root GC CA**
Fingerprint=E0:11:84:5E:34:DE:BE:88:81:B9:9C:F6:16:26:D1:96:1F:C3:B9:31
subject= /C=CH/O=WISeKey/OU=OISTE Foundation Endorsed/CN=OISTE WISeKey Global Root GC CA

**CN=WISeKey CertifyID Advanced GC CA 1**
Fingerprint=13:A1:8A:B2:90:58:BC:34:63:64:07:52:E7:3F:0B:58:54:81:7D:96
subject= /C=CH/O=WISeKey/CN=WISeKey CertifyID Advanced GC CA 1

WISeKey

# WISeKey MANAGEMENT'S ASSERTION

as to its Disclosure of its Business Practices and Controls over its SSL Certification Authority Operations during the period from September 16th 2017 through December 4th 2017

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

The management of **WISeKey** is responsible for establishing and maintaining effective controls over its SSL and non-SSL CA operations, including its network and certificate security system controls, its SSL CA business practices disclosure on its website [https://www.wisekey.com/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 **WISeKey's** Certification Authority operations. Furthermore, because of changes in conditions, the effectiveness of controls may vary over time.

**WISeKey** management has assessed its disclosures of its certificate practices and controls over its SSL CA services. Based on that assessment, in **WISeKey** management's opinion, in providing its SSL [and non-SSL] Certification Authority (CA) services at its main and disaster recover datacentres in Switzerland, throughout the period September 16th 2017 through December 4th 2017, **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 Version 2.9" (25 July 2017) available at the link [https://cdn.wisekey.com/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.9-CLEAN.pdf] (combined CP & CPS document), including its commitment to provide 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 SSL certificates it manages is established and protected throughout their lifecycles; and
    - SSL subscriber information is properly authenticated (for the registration activities performed by **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
- 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

In accordance with the WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security v2.0, as published at [http://www.webtrust.org/homepage-documents/item79806.pdf].

Geneva, 4 December 2017

Carlos Moreira
CEO

Pedro Fuentes
CSO

# Appendix A: PKI Hierarchy in scope of the WebTrust SSL and Network Security audit

## OISTE WISeKey Global Root GC CA

Thumbprint: E0 11 84 5E 34 DE BE 88 81 B9 9C F6 16 26 D1 96 1F C3 B9 31
Valid From: 9th May 2017 To: 9th May 2042

**Issuing CAs**

- WISeKey CertifyID Advanced GC CA 1
  Thumbprint: 13 A1 8A B2 90 58 BC 34 63 64 07 52 E7 3F 0B 58 54 81 7D 96
  Valid From: 23th August 2017 To: 9th May 2042