

Independent Assurance Report

To the Management of WISEKey SA (WISEKey):

Scope

We have examined the assertion by the WISEKey Management, according its services as issuer of digital certificates at Geneva (Switzerland), for the Root Certification Authority "OISTE WISEKey Global Root GC" hierarchy with its Delegated Certification Authorities as detailed in appendix 1 as of the point in time September 15th 2017.

In this point in time, WISEKey has:

- disclosed its business, key lifecycle management, certificate lifecycle management, and CA environment control practices in its:
 - OISTE WISEKey Root Certification Practice Statement - Version: 2.8
<https://cdn.wisekey.com/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.8-CLEAN1.pdf>
- suitably designed, and placed into operation, controls to provide reasonable assurance that:
 - WISEKey provides its services in accordance with its Certification Practice Statement
- suitably designed, and placed into operation 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
- suitably designed, and placed into operation 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.

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 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 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) 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, as of September 15th, 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.



F. Mondragon, Auditor

auren

Valencia, SPAIN

September 15th, 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

WIS@key MANAGEMENT'S ASSERTION

as to its Disclosure of its Business Practices and Controls over its Certification Authority Operations as of September 13th 2017

WIS@key SA (“WIS@key”) operates the Certification Authority (CA) services known as “OISTE WIS@key Global Root GC” hierarchy with its Delegated Advanced 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.

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, as of September 13th 2017, 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 Version 2.8” (19 June 2017) available at the link [<https://cdn.wisekey.com/uploads/images/WKPKI.DE001-OWGTM-PKI-CPS.v2.8-CLEAN1.pdf>] (combined CP & CPS document)
- suitably designed, and placed into operation, controls to provide reasonable assurance that WIS@key provides its services in accordance with its Certification Practice Statement
- suitably designed, and placed into operation, 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
- suitably designed, and placed into operation, 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)

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

Geneva, 13 September 2017



Peter Ward
CFO



Pedro Fuentes
CSO

Appendix A: PKI Hierarchy in scope of the WebTrust audit

OISTE WIS@key 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

- WIS@key 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: 23rd August 2017 To: 9th May 2042

