

## Independent Auditors Report

To the Management of WISEKey SA:

We have audited the assertion by the WISEKey SA Management, (hereinafter, WISEKey) according its services as issuer of digital certificates, for the Root Certification Authority "OISTE WISEKey Global Root GA", and as a Delegated Certification Authority linked to the above mentioned Root Certification Authority through "WISEKey CertifyID Standard G1 CA", "WISEKey CertifyID Advanced G1 CA" and "WISEKey CertifyID Qualified G1 CA" and its issuing CAs "WISEKey CertifyID Standard Services CA 1", "WISEKey CertifyID Advanced Services CA 1", "WISEKey CertifyID Qualified Services CA 1", "WISEKey CertifyID Advanced Services CA 2", "WISEKey CertifyID Standard Services CA 2" and "WISEKey CertifyID Qualified Services CA 2" during the period from May 27<sup>th</sup> 2014 through May 26<sup>th</sup> 2015.

In this period, WISEKey has:

- Disclosed its certificate and key life cycles management business and information privacy practices as provided such (WISEKey's CPS published at <https://www.wisekey.com/repository>)
- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly authenticated;
  - The integrity of keys and certificates it managed was established and protected throughout their life cycles;
  - Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
  - The continuity of key and certificate life cycle management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

based on the AICPA/CPA Canada WebTrust for Certification Authorities Criteria (Principles and Criteria for Certification Authorities 2.0).

WISEKey's Management is responsible for its assertion. Our responsibility is to express an opinion on management's assertions based on our audit.

WISEKey makes use of external registration authorities for specific subscriber registration activities as disclosed in WISEKey's business practice disclosures. Our audit did not extend to the controls of external registration authorities

The audit was conducted in accordance with standards for assurance engagements of WebTrust Criteria for Certification Authorities, established by the



organizations competent in this matter, namely the AICPA/CPA Canada. Our audit included:

- Obtaining an understanding of WISeKey's key and certificate life cycle management business and information privacy practices and its controls over key and certificate integrity, over the continuity of key and certificate life cycle management operations, over the authenticity and privacy of subscriber and relying party information and over development, maintenance and operation of systems integrity;
- Selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business and information privacy practices;
- Testing and evaluating the operating effectiveness of the controls; and
- Performing such other procedures as we considered necessary in the circumstances.

We believe that our audit provides a reasonable basis for our opinion.

### **Auditor's Opinion**

In our opinion, for the period May 27<sup>th</sup> 2014 through May 26<sup>th</sup> 2015, WISeKey's Management Assertions regarding its Certification Authority Practices, are properly formulated in all material matters, in accordance with the AICPA/CPC Canada WebTrust Program for Certification Authorities criteria.

### **Inherent limitations**

Because of inherent limitations control systems themselves, there may be undetected errors or instances of fraud. Furthermore, the projection of any conclusions based in our findings, to future periods subsequent to the date of our report, is subject to the risk that there may be:

- (1) changes made to the system or controls;
- (2) changes in processing requirements;
- (3) changes required because of the passage of time; or
- (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

### **Exclusions**

The relative effectiveness and significance of specific controls at WISeKey and their effect on the assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls and other factors present in the sites of subscribers and the relying parties. We have performed no procedures to evaluate the effectiveness of controls at external registration authorities and individual subscriber and relying party locations.



This report does not include any professional opinion regarding the quality of WISeKey's services, beyond those covered by the Webtrust for Certification Authorities Criteria, nor the suitability of any of WISeKey's services for any customer's intended purposes.

A handwritten signature in blue ink, appearing to be "F. Mondragon".

F. Mondragon, Auditor

**auren**



Management Assertion as to its Disclosure of its Business Practices and Controls over its Certification  
Authority Operations during the period from May 27<sup>th</sup> 2014 through May 26<sup>th</sup> 2015

June 1<sup>st</sup>, 2015

WIS@key SA operates as a Root Certification Authority (CA) through "OISTE WIS@key Global Root GA", and as a Delegated Certification Authority linked to the above mentioned Root Certification Authority through "WIS@key CertifyID Standard G1 CA", "WIS@key CertifyID Advanced G1 CA" and "WIS@key CertifyID Qualified G1 CA" and its issuing CAs "WIS@key CertifyID Standard Services CA 1", "WIS@key CertifyID Advanced Services CA 1", "WIS@key CertifyID Qualified Services CA 1", "WIS@key CertifyID Advanced Services CA 2", "WIS@key CertifyID Standard Services CA 2" and "WIS@key CertifyID Qualified Services CA 2", and provides the following Certification Authorities Services:

- Subscriber registration
- Certificate issuance
- Certificate renewal
- Certificate distribution
- Certificate revocation
- Certificate suspension
- Certificate status information processing

In order to provide the certification service, WIS@key SA makes use of Registry Authorities for the identification of applicants for certificates, in line with the regulations of the Certification Practices Statement (CPS).

Management of WIS@key SA is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental 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 provide only 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.

Management has assessed the controls over its CA operations. Based on that assessment, in WIS@key SA Management's opinion, in providing its Certification Authority (CA) services, during the period from May 27<sup>th</sup> 2014 through May 26<sup>th</sup> 2015:

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly authenticated by the Registration Authority, WIS@key SA itself;
  - The integrity of keys and certificates it managed was established and protected throughout their life cycles;

- Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
- The continuity of key and certificate life cycle management operations was maintained; and
- CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

All of it based on the AICPA/CICA [WebTrust for Certification Authorities Criteria](#) including the following:

#### CA Business Practices Disclosure

##### Service integrity

##### **Key Life Cycle Management Controls:**

- Certificate Key Generation
- Certificate Key Storage, Backup, and Recovery
- Certificate Public Key Distribution
- Certificate Key Usage
- Certificate Key Destruction
- Certificate Key Archival
- Certificate Cryptographic Hardware Life Cycle Management

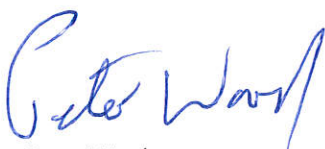
##### **Controls in Certificate Life Cycle Management:**

- Subscriber Registration
- Certificate Renewal
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Status Information Processing

##### CA Environmental Controls:

- Certification Practice Statement Management
- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Event Journaling

WISeKey, SA



Peter Ward  
Chief Financial Officer



Kevin Blackman  
Chief Technical Officer

## Independent Auditors Report

To the Management of WISeKey SA:

We have audited the assertion by the WISeKey SA Management, (hereinafter, WISeKey) according its services as issuer of digital certificates, for the Root Certification Authority through "OISTE WISeKey Global Root GB CA" (created on December 1<sup>st</sup> 2014), and as a Delegated Certification Authority linked to the above mentioned Root Certification Authority through "WISeKey CertifyID Policy GB CA 1" (created on May 13<sup>th</sup> 2015), and its issuing CAs "WISeKey CertifyID Advanced GB CA 2", "WISeKey CertifyID Standard GB CA 2" and "WISeKey CertifyID Qualified GB CA 2" (created on May 27<sup>th</sup> 2015) during the period December 1<sup>st</sup> 2014 through June 4<sup>th</sup>, 2015.

In our opinion, during this period, WISeKey has:

- Disclosed its certificate and key life cycles management business and information privacy practices an provided such (WISeKey's CPS published at <https://www.wisekey.com/repository>)
- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly authenticated;
  - The integrity of keys and certificates it managed was established and protected throughout their life cycles;
  - Subscriber and relying party information was restricted to authorized individuals and protected from uses not specified in the CA's business practices disclosure;
  - The continuity of key and certificate life cycle management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

based on the AICPA/CPA Canada WebTrust for Certification Authorities Criteria (Principles and Criteria for Certification Authorities 2.0).

WISeKey's Management is responsible for its assertion. Our responsibility is to express an opinion on management's assertions based on our audit.

WISeKey makes use of external registration authorities for specific subscriber registration activities as disclosed in WISeKey's business practice disclosures. Our audit did not extend to the controls of external registration authorities

The audit was conducted in accordance with standards for assurance engagements of WebTrust Criteria for Certification Authorities, established by the organizations competent in this matter, namely the AICPA/CPA Canada. Our audit included:





- Obtaining an understanding of WISeKey's key and certificate life cycle management business and information privacy practices and its controls over key and certificate integrity, over the continuity of key and certificate life cycle management operations, over the authenticity and privacy of subscriber and relying party information and over development, maintenance and operation of systems integrity;
- Selectively testing transactions executed in accordance with disclosed key and certificate life cycle management business and information privacy practices;
- Testing and evaluating the operating effectiveness of the controls; and
- Performing such other procedures as we considered necessary in the circumstances.

We believe that our audit provides a reasonable basis for our opinion.

### **Auditor's Opinion**

In our opinion, during the period December 1<sup>st</sup> 2014 through June 4<sup>th</sup>, 2015, WISeKey's Management Assertions regarding its Certification Authority Practices, are properly formulated in all material matters, in accordance with the AICPA/CPA Canada WebTrust Program for Certification Authorities criteria.

### **Inherent limitations**

Because of inherent limitations control systems themselves, there may be undetected errors or instances of fraud. Furthermore, the projection of any conclusions based in our findings, to future periods subsequent to the date of our report, is subject to the risk that there may be:

- (1) changes made to the system or controls;
- (2) changes in processing requirements;
- (3) changes required because of the passage of time; or
- (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

### **Exclusions**

The relative effectiveness and significance of specific controls at WISeKey and their effect on the assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls and other factors present in the sites of subscribers and the relying parties. We have performed no procedures to evaluate the effectiveness of controls at external registration authorities and individual subscriber and relying party locations.

This report does not include any professional opinion regarding the quality of WISeKey's services, beyond those covered by the Webtrust for Certification



Authorities Criteria, nor the suitability of any of WISeKey's services for any customer's intended purposes.

A handwritten signature in blue ink, appearing to be "F. Mondragon".

F. Mondragon, Auditor

**auren**





Management Assertion as to its Disclosure of its Business Practices and Controls over its Certification  
Authority Operations during the period December 1<sup>st</sup> 2014 through June 4<sup>th</sup>, 2015

June 4<sup>th</sup>, 2015

WIS@key SA operates as a Root Certification Authority (CA) through "OISTE WIS@key Global Root GB CA" (created on December 1<sup>st</sup> 2014), and as a Delegated Certification Authority linked to the above mentioned Root Certification Authority through "WIS@key CertifyID Policy GB CA 1" (created on May 13<sup>th</sup> 2015), and its issuing CAs "WIS@key CertifyID Advanced GB CA 2", "WIS@key CertifyID Standard GB CA 2" and "WIS@key CertifyID Qualified GB CA 2" (created on May 27<sup>th</sup> 2015), and provides the following Certification Authorities Services:

- Subscriber registration
- Certificate issuance
- Certificate renewal
- Certificate distribution
- Certificate revocation
- Certificate suspension
- Certificate status information processing

In order to provide the certification service, WIS@key SA makes use of Registry Authorities for the identification of applicants for certificates, in line with the regulations of the Certification Practices Statement (CPS).

Management of WIS@key SA is responsible for establishing and maintaining effective controls over its CA operations, including CA business practices disclosure, service integrity (including key and certificate life cycle management controls), and CA environmental 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 provide only 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.

Management has assessed the controls over its CA operations. Based on that assessment, in WIS@key SA Management's opinion, in providing its Certification Authority (CA) services, during the period December 1<sup>st</sup> 2014 through June 4<sup>th</sup>, 2015:

- Disclosed its key and certificate life cycle management business and information privacy practices and provided such services in accordance with its disclosed practices
- Maintained effective controls to provide reasonable assurance that:
  - Subscriber information was properly authenticated by the Registration Authority, WIS@key SA itself;
  - The integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - Subscriber and relying party information was restricted to authorized individuals and

A handwritten signature in blue ink, consisting of a stylized 'W' followed by a large, flowing 'S'.

- protected from uses not specified in the CA's business practices disclosure;
- The continuity of key and certificate life cycle management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

All of it based on the AICPA/CICA [WebTrust for Certification Authorities Criteria](#) including the following:

#### CA Business Practices Disclosure

##### Service integrity

###### **Key Life Cycle Management Controls:**

- Certificate Key Generation
- Certificate Key Storage, Backup, and Recovery
- Certificate Public Key Distribution
- Certificate Key Usage
- Certificate Key Destruction
- Certificate Key Archival
- Certificate Cryptographic Hardware Life Cycle Management

###### **Controls in Certificate Life Cycle Management:**

- Subscriber Registration
- Certificate Renewal
- Certificate Issuance
- Certificate Distribution
- Certificate Revocation
- Certificate Suspension
- Certificate Status Information Processing

##### CA Environmental Controls:

- Certification Practice Statement Management
- Security Management
- Asset Classification and Management
- Personnel Security
- Physical and Environmental Security
- Operations Management
- System Access Management
- Systems Development and Maintenance
- Business Continuity Management
- Monitoring and Compliance
- Event Journaling

WISeKey, SA



Peter Ward  
Chief Financial Officer



Kevin Blackman  
Chief Technical Officer

## Independent Auditors Report

To the Management of WISeKey SA:

We have audited the Assertion by the management of WISeKey SA, (hereinafter WISeKey) as of June 4<sup>th</sup> 2015 for its SSL Certification Authority services at Geneva (Switzerland) through its subordinate "WISeKey CertifyID Advanced Services CA 2" for its "OISTE WISeKey Global Root GA CA" hierarchy and through its subordinate "WISeKey CertifyID Advanced GB CA 2" for its "OISTE WISeKey Global Root GB CA" hierarchy.

In this point of time, WISeKey has:

- Disclosed its Certificate practices and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines (WISeKey's CPS published at <https://www.wisekey.com/repository>)
- Designed effective controls to provide reasonable assurance that:
  - The Certificate Policy and/or Certificate Practice Statement are available on a 24x7 basis and updated annually
  - Subscriber information is properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - The integrity of keys and certificates it manages are established and protected throughout their life cycles;
  - Logical and physical access to CA systems and data are restricted to authorized individuals;
  - The continuity of key and certificate management operations are maintained; and
  - CA systems development, maintenance and operations are properly authorized and performed to maintain CA systems integrity.

based on the AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security.

WISeKey's Management is responsible for its assertion. Our responsibility is to express an opinion on management's assertions based on our audit.

WISeKey makes use of external registration authorities for specific subscriber registration activities as disclosed in WISeKey's business practice disclosures. Our audit did not extend to the controls of external registration authorities

Our audit was conducted in accordance with standards for assurance engagements established by the AICPA/CPA Canada and, accordingly, included:



- Obtaining an understanding of WISeKey's SSL certificate life cycle management practices and procedures, including its relevant controls over the issuance, renewal and revocation of SSL certificates;
- Evaluating the suitability of the design of the controls; and
- Performing such other procedures as we considered necessary in the circumstances.

We believe that our audit provides a reasonable basis for our opinion.

### **Auditor's Opinion**

In our opinion, as of June 4<sup>th</sup> 2015, 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.

### **Inherent limitations**

Because of inherent limitations control systems themselves, there may be undetected errors or instances of fraud. Furthermore, the projection of any conclusions based in our findings, to future periods subsequent to the date of our report, is subject to the risk that there may be:

- (1) changes made to the system or controls;
- (2) changes in processing requirements;
- (3) changes required because of the passage of time; or
- (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

### **Exclusions**

The relative effectiveness and significance of specific controls at WISeKey and their effect on the assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls and other factors present in the sites of subscribers and the relying parties. We have performed no procedures to evaluate the effectiveness of controls at external registration authorities and individual subscriber and relying party locations.

This report does not include any professional opinion regarding the quality of WISeKey's services, beyond those covered by the WebTrust Principles and



Criteria for Certification Authorities – SSL Baseline with Network Security, nor the suitability of any of WISEKey's services for any customer's intended purposes.

A handwritten signature in blue ink, appearing to be "F. Mondragon". The signature is stylized with a large, sweeping initial "F" and a cursive "Mondragon".

F. Mondragon, Auditor

**auren**





Assertion by Management of WIS@key SA Regarding Its Disclosure of its Certificate Practices and its Controls Over its SSL Certification Authority Services as of June 4<sup>th</sup>, 2015

June 4<sup>th</sup> 2015

The Management of WIS@key SA has assessed the disclosure of its certificate practices and its controls over its SSL-CA services. Based on that assessment, in WIS@key's Management's opinion, WIS@key SA has designed, implemented and manage controls over its SSL-CA services in Geneva (Switzerland), as of June 4<sup>th</sup> 2015 through its subordinate "WIS@key CertifyID Advanced Services CA 2" for its "OISTE WIS@key Global Root GA CA" hierarchy and through its subordinate "WIS@key CertifyID Advanced GB CA 2" for its "OISTE WIS@key Global Root GB CA" hierarchy.

In this point-of-time, WIS@key SA has:

- a) Disclosed its Certificate practices and its commitment to provide SSL Certificates in conformity with the applicable CA/Browser Forum Guidelines
- b) Designed effective controls to provide reasonable assurance that:
  - The Certificate Policy and/or Certificate Practice Statement are available on a 24x7 basis and updated annually;
  - Subscriber information was properly collected, authenticated (for the registration activities performed by the CA, Registration Authority (RA) and subcontractor) and verified;
  - The integrity of keys and certificates it manages was established and protected throughout their life cycles;
  - Logical and physical access to CA systems and data was restricted to authorized individuals;
  - The continuity of key and certificate management operations was maintained; and
  - CA systems development, maintenance and operations were properly authorized and performed to maintain CA systems integrity.

All of it in accordance with the AICPA/CPA Canada [WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security](#).

WIS@key, SA

Peter Ward  
Chief Financial Officer

Kevin Blackman  
Chief Technical Officer

## Independent Auditors Report

To the Management of WISeKey SA:

We have audited the Assertion by the management of WISeKey SA, (hereinafter WISeKey) as of June 4<sup>th</sup> 2015 for its Extended Validation SSL Certification Authority services at Geneva (Switzerland) through its subordinate "WISeKey CertifyID Advanced GB CA 2" for its "OISTE WISeKey Global Root GB CA" hierarchy.

In this point of time, WISeKey has:

- Disclosed its Certificate practices and its commitment to provide Extended Validation SSL Certificates in conformity with the applicable CA/Browser Forum Extended Validation Guidelines. (WISeKey's CPS published at <https://www.wisekey.com/repository>)
- Designed effective controls to provide reasonable assurance that:
  - Extended Validation Subscriber information is properly collected, reviewed and verified ; and
  - The integrity of the keys and Extended Validation certificates administered by WISeKey are established and protected through their life cycles.

based on the AICPA/CPA Canada WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL.

WISeKey Management is responsible for its Statements. Our responsibility is to express an opinion on WISeKey's assertions, based on our audit.

WISeKey makes use of external registration authorities for specific subscriber registration activities as disclosed in WISeKey's business practice disclosures. Our audit did not extend to the controls of external registration authorities

Our audit was conducted in accordance with standards for assurance engagements established by the AICPA/CPA Canada and, accordingly, included:

- Obtaining an understanding of WISeKey's Extended Validation SSL certificate life cycle management practices and procedures, including its relevant controls over the issuance, renewal and revocation of Extended Validation SSL certificates;
- Evaluating the suitability of the design of the controls; and
- Performing such other procedures as we considered necessary in the circumstances.

We believe that our audit provides a reasonable basis for our opinion.





### **Auditor's Opinion**

In our opinion, as of June 4<sup>th</sup> 2015, 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.

### **Inherent limitations**

Because of inherent limitations control systems themselves, there may be undetected errors or instances of fraud. Furthermore, the projection of any conclusions based in our findings, to future periods subsequent to the date of our report, is subject to the risk that there may be:

- (1) changes made to the system or controls;
- (2) changes in processing requirements;
- (3) changes required because of the passage of time; or
- (4) degree of compliance with the policies or procedures may alter the validity of such conclusions.

### **Exclusions**

The relative effectiveness and significance of specific controls at WISeKey and their effect on the assessments of control risk for subscribers and relying parties are dependent on their interaction with the controls and other factors present in the sites of subscribers and the relying parties. We have performed no procedures to evaluate the effectiveness of controls at external registration authorities and individual subscriber and relying party locations.

This report does not include any professional opinion regarding the quality of WISeKey's services, beyond those covered by the WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL, nor the suitability of any of WISeKey's services for any customer's intended purposes.

A handwritten signature in blue ink, appearing to be "F. Mondragon". The signature is stylized with a large, sweeping "F" and a cursive "Mondragon".

F. Mondragon, Auditor

**auren**



Assertion by Management of WIS@Key regarding its Disclosure of its Certificate Practices and Controls over its Extended Validation Certification Operations as of June 4<sup>th</sup>, 2015

June 4<sup>th</sup>, 2015

The management of WIS@Key SA has assessed the disclosure of its certificate practices and its controls over its SSL - CA services located at Geneva (Switzerland). Based on that assessment, in WIS@Key's opinion, in providing its EV - CA services, the controls have been properly designed, implemented and managed over its Extended Validation Certification Services as of June 4<sup>th</sup>, 2015 through its subordinate "WIS@Key CertifyID Advanced GB CA 2" for its "OISTE WIS@Key Global Root GB CA" hierarchy.

WIS@Key SA has:

- Disclosed its Extended Validation certificate and key life cycles management practices and procedures, including its commitment to provide EV certificates in conformity with the CA/Browser Forum Guidelines for Extended Validation (EV) and provided such services in accordance with its disclosed practices Certification Practices Statement.
- Designed effective controls to provide reasonable assurance that:
  - Extended Validation Subscriber information is properly collected, reviewed and verified; and
  - The integrity of the keys and Extended Validation certificates administered by WIS@Key SA is established and protected through their life cycles.

All of it in accordance with the AICPA/CPA Canada [WebTrust Principles and Criteria for Certification Authorities – Extended Validation SSL](#).

WIS@Key, SA

Peter Ward  
Chief Financial Officer

Kevin Blackman  
Chief Technical Officer