

OISTE WISEKEY ROOT CERTIFICATION PRACTICE STATEMENT

Version 1.01
Effective Date: 16 January 2007

WIS@key S.A. © 2000-2007

WIS@key hereby grants non-exclusive permission to reproduce and distribute copies of this Certification Practice Statement for non-commercial purposes, provided the full source and copyright ownership are included. Any reproduction, distribution or other use beyond the foregoing permission requires authorisation by WIS@key and to such end may contact WIS@key in accordance with § 2.5.3.

1. INTRODUCTION	5
1.1. OVERVIEW AND TRUST MODEL	5
1.1.1. WISeKey SA.....	6
1.1.2. Definitions.....	6
1.1.3. PKI Operational Infrastructure	6
1.1.4. Scope.....	6
1.2. IDENTIFICATION.....	6
1.2.1. X.500 Object Identifier hierarchy.....	6
1.3. COMMUNITY AND APPLICABILITY	7
1.3.1. OISTE WISeKey Root CA.....	7
1.3.2. OISTE and Subordinated Policy Approval Authorities.....	7
1.3.3. Policy Certification Authorities (PCAs).....	9
1.3.4. Registration Authorities (RAs).....	9
1.3.5. End Users.....	9
1.3.6. Relying Parties.....	9
1.3.7. Applicability	10
1.4. CONTACT DETAILS	10
2. GENERAL PROVISIONS	11
2.1. OBLIGATIONS.....	11
2.1.1. Root CA Obligations.....	11
2.1.2. Policy CA Obligations	12
2.1.3. End User Obligations.....	12
2.1.4. Relying Party Obligations.....	13
2.2. LIABILITY LIMITS AND DISCLAIMERS	14
2.3. FINANCIAL RESPONSIBILITY.....	15
2.3.1. No Fiduciary relationships.....	16
2.4. INTERPRETATION AND ENFORCEMENT.....	16
2.4.1. Governing Law	16
2.4.2. Severability, Survival, Merger, Notice	17
2.4.3. Dispute resolution procedures.....	18
2.5. PUBLICATION AND REPOSITORIES.....	19
2.5.1. Publication of information on the Certification Services	19
2.5.2. Frequency of publication	19
2.5.3. Access Control.....	19
2.6. COMPLIANCE AUDIT.....	20
2.6.1. OISTE WISeKey Root PKI Compliance Audits	20
2.6.2. Topics covered by audit.....	20
2.6.3. Communication of results.....	20
2.7. CONFIDENTIALITY	20
2.7.1. Types of information to be kept confidential.....	20
2.7.2. Types of information not considered confidential	21
2.7.3. WISeKey PKI Documentation.....	21
2.7.4. Disclosure of Certificate Revocation/Suspension information.....	22
2.7.5. Release to law enforcement officials	22
2.7.6. Release as part of civil evidence or discovery purposes.....	22
2.8. INTELLECTUAL PROPERTY RIGHTS	22
2.8.1. General provision.....	22

3. OPERATIONAL REQUIREMENTS	24
3.1. CERTIFICATE ISSUANCE	24
3.1.1. Certificate Issuance Process.....	24
3.1.2. Operational periods.....	24
3.2. CERTIFICATE ACCEPTANCE	24
3.3. CERTIFICATE SUSPENSION AND REVOCATION	24
3.3.1. Circumstances for Suspension	24
3.3.2. Who can request a Suspension or Revocation?	25
3.3.3. Limits on suspension period	25
3.3.4. Circumstances for revocation	25
3.3.5. Procedure for revocation request	26
3.3.6. Revocation request grace period.....	26
3.3.7. Certificate Validity Checking Requirements	26
3.4. SECURITY AUDIT PROCEDURES	27
3.4.1. Types of Event Recorded.....	27
3.4.2. Frequency of processing log	27
3.4.3. Retention period for audit log.....	27
3.4.4. Audit collection system.....	27
3.4.5. Notification to event-causing subject.....	27
3.5. RECORDS ARCHIVAL	27
3.6. KEY CHANGEOVER	28
3.7. COMPROMISE AND DISASTER RECOVERY	28
4. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS	29
4.1. PHYSICAL CONTROLS FOR ROOT CA	29
4.2. PROCEDURAL CONTROLS	29
4.3. PERSONNEL CONTROLS.....	29
5. TECHNICAL SECURITY CONTROLS	30
5.1. KEY PAIR GENERATION AND INSTALLATION	30
5.1.1. Key Pair Generation.....	30
5.1.2. Private Key Delivery to Entity.....	30
5.1.3. Public Key Delivery to Certificate Issuer	30
5.1.4. Root CA Public Key Delivery to Users	30
5.1.5. Key Sizes	30
5.1.6. Public Key Parameters Checking.....	30
5.1.7. Parameter Quality Checking	30
5.1.8. Key Usage Purposes	31
5.2. PRIVATE KEY PROTECTION	31
5.2.1. Standards for Cryptographic Module.....	31
5.2.2. Private Key (n out of m) Multipersonal Control.....	31
5.2.3. Private Key Escrow.....	31
5.2.4. Private Key Backup	31
5.2.5. Private Key Archival.....	31
5.2.6. Private Key Entry into Cryptographic Module.....	31
5.2.7. Method of Activating Private Key	31
5.2.8. Method of Deactivating Private Key	32
5.2.9. Method of Destroying Private Key	32
5.2.10. Usage Periods for the Public and Private Key	32

5.3.	ACTIVATION DATA	32
5.3.1.	Activation Data Generation and Installation.....	32
5.3.2.	Activation Data Protection.....	32
5.4.	COMPUTER SECURITY CONTROLS	32
5.5.	LIFE CYCLE TECHNICAL CONTROLS	32
5.5.1.	System Development Controls	32
5.5.2.	Security management controls.....	33
5.6.	NETWORK SECURITY CONTROLS	33
6.	SPECIFICATION ADMINISTRATION	34
6.1.	SPECIFICATION CHANGE PROCEDURES	34
6.1.1.	Initial publication.....	34
6.1.2.	Changes.....	34
6.2.	PUBLICATION AND NOTIFICATION POLICIES	35
6.3.	CPS APPROVAL PROCEDURES	35
7.	APPENDIX - GLOSSARY.....	36

1. INTRODUCTION

1.1. Overview and Trust Model

This Certification Practice Statement (CPS) describes the practices followed with regard to the management of the lifecycle of OISTE WISEKey Global Root CA by the WISEKey World Certification Authority Services.

The WISEKey Certification Authority Services (WCAS) have been designed and are operated in accordance with the broad strategic direction of international PKI (Public Key Infrastructure) standards as well as their application to concrete identity frameworks in different domains (e.g. ID cards, passports, health cards) and is intended to serve as a common services infrastructure for Certification Authorities worldwide that comply with WISEKey requirements.

The technologies, infrastructures, practices, and procedures implemented by the WISEKey Certification Authority Services have been designed with explicit standards of security in mind based on the requirements approved by the International Organization for Secure Electronic Transactions ("IOSET" or "OISTE"), a Swiss non-profit foundation established in 1998. The IOSET Foundation maintains a Policy Approval Authority (PAA) that drafts, approves and revises the policies to which WISEKey is bound to comply with under its operator contract. The OFPAA is composed of members of the community to which OISTE provides its Certification Authority Services, resulting in a virtuous cycle for trust management.

The IOSET Foundation, under Swiss law, cannot belong to any individual or company nor does it have shareholders. It is subject to annual supervision by the Swiss Federal Government and audited annually by independent auditors. Such supervision and audit require the foundation to pursue the objectives that have been set out for it, which includes the promotion of security in electronic communications worldwide.

This CPS provides factual information that describes the:

- Practices employed by WISEKey in operating the WISEKey Certification Authority Services.
- Use of technologies and procedures to support the underlying operational structure.

The practices described in this CPS, together with the technologies, policies and procedures referred to in the documents contained and incorporated into the WISEKey Repository (<http://www.wisekey.com/repository/>), illustrate the efforts made to convey trustworthiness by providing high levels of security of the WISEKey Certification Authority Services operations.

The WISEKey Certification Authority Services and this CPS undergo a regular review process, by which the reviewers involved strive to take into consideration developments in international PKI standardization initiatives, developments in technology, information security law and policy, as well as other relevant circumstances.

The structure of this CPS is broadly based on the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework¹.

1.1.1. WISeKey SA

WISeKey SA is a “Société Anonyme” under Swiss law with headquarters in Geneva, Switzerland and subsidiaries and affiliates in different regions and countries worldwide. The company manages the WISeKey Certification Authority Services (WCAS), including the OISTE WISeKey Global Root CA, which is maintained off-line in a high-security facility in Switzerland.

WISeKey has located its headquarters in Switzerland and is simultaneously establishing affiliates in regions and countries worldwide. This enables, on the one hand, the traditional Swiss neutrality and high quality infrastructures and services and, on the other hand, the local capacity to establish infrastructures in each country and region adapted to the local needs, regulations and policies. This results in a series of links between entities that conform a chain of trust running throughout its infrastructures worldwide.

1.1.2. Definitions

Definitions used within this document are contained in the [Glossary](#) located in the Appendix.

1.1.3. PKI Operational Infrastructure

The OISTE/WISeKey Root Public Key Infrastructure is a combination of services and infrastructures implemented and managed by WISeKey.

1.1.4. Scope

This CPS covers the practices applied to the OISTE WISeKey Global Root GA (OISTE WISeKey Root CA) operated by WISeKey. The practices described in this document are applied by WISeKey to its own operations.

1.2. Identification

This CPS is referred to as the ‘OISTE WISeKey Root CPS’. The primary source of the current version of the CPS and other important WISeKey documents is <http://www.WISeKey.com/repository/>.

1.2.1. X.500 Object Identifier hierarchy

Object Identifiers (OIDs) are assigned by WISeKey and documented in a Configuration baseline. OIDs are not assigned to Certification Authorities or Registration Authorities. OIDs are assigned by the WISeKey Policy Approval Authority (WPAA) to:

- Certificate policies under which Certificates are issued by Policy CAs and
- Private extensions included in any certificates issued by Policy CAs

The corporate OID assigned to WISEKey is:

- 2.16.756.5.14

1.3. Community and Applicability

1.3.1. OISTE WISEKey Root CA

The OISTE WISEKey Root CA self-signs its own Root Certificate which has been endorsed by the OISTE Foundation. The Private Cryptographic Key of the OISTE WISEKey Root CA is maintained off-line in a high security facility in Switzerland. Certificate Revocation Lists (CRLs) are published by the OISTE WISEKey Root CA which include the certificates suspended or revoked by the OISTE WISEKey Root CA.

The OISTE WISEKey Root CA may also establish on a case by case basis agreements with other Root Certification Authorities which result in cross recognitions, cross certifications, cross validations or other forms of enabling interoperability between public key infrastructures.

1.3.2. OISTE and Subordinated Policy Approval Authorities

The OISTE Foundation PAA (OFPAA), which manages all high level policy approval issues concerning the OISTE WISEKey Root CA, supervises the activities of the WPAA and, on occasions, may issue guidelines which the WPAA must take into consideration in accordance with the operator contract WISEKey has with the OISTE Foundation. All Policy Approval Authorities subordinated to the OFPAA have a PAA Constitution document which describes its formation, procedures, membership and other relevant details.

The WPAA is managed and organised by WISEKey and has been established to approve the practices, policies and procedures under which the OISTE WISEKey Root PKI operates. Its members are chosen by WISEKey S.A. and may be subject to rejection by the OISTE Foundation PAA.

Both the OFPAA and the WPAA have a series of distinct functions. The OFPAA is a committee operating within the OISTE Foundation under policies, rules and regulations determined by the foundation itself. The OISTE Foundation PAA's mandate is limited to the OISTE WISEKey Root CA and to the supervisory role over the public key infrastructures subordinated to it.

The WPAA has been established to develop, review and/or approve the practices, policies and procedures for the entire OISTE WISEKey PKI by undertaking, subject to guidelines established or approval by the OISTE Foundation PAA, the following functions:

- Reviewing and approving this CPS and all practices and policies within the scope of the OISTE WISEKey Root PKI as well as all procedures which are relevant to the security of the OISTE WISEKey Root PKI, together with the adoption of documents changing or excluding practices with this CPS.
- Initiating, consulting in respect of, and approving any amendment to this CPS

- or request for amendment of subordinate CPSs and CPs .
- Establishing guidelines for the publication of this CPS, CPs and others subordinated to them as well as similar policy documents.
 - Instigating the drafting of practices, policies and procedures for new Policy CAs entering the PKI
 - Allocating an object identifier or “OID” to a specific CP or application.
 - Issuing guidelines for the management of the OISTE WISEKey Root PKI (and requiring the amendment of CPSs across the whole infrastructure).
 - Maintaining and updating existing practices, policies and procedures.
 - Determining compliance of Policy CAs with the policies, practices and procedures applicable to each through the mechanisms provided for in this CPS.
 - Endorsing the operations and processes undertaken in support of the practices, policies and procedures approved by the WPAA.
 - Maintaining all of the public practices, policies, and procedures applicable within the OISTE WISEKey Root PKI published and/or available to the appropriate community of interest.
 - Delegating WPAA responsibilities as required.
 - Liaising with external policy creation and approval authorities on issues of common concern.
 - Approving naming conventions used by the Root CAs and Policy CAs.
 - Undertaking a full assessment (including on compliance, complementarity and viability) of cross-certification, cross validation, recognition or other forms of interoperability with Certification Authorities or Public Key Infrastructures outside the OISTE WISEKey Root PKI community.
 - Investigating and deciding whether Policy CA Certificates issued as part of the OISTE WISEKey Root PKI should be revoked.
 - Ordering the Revocation of Certificates issued by the OISTE WISEKey Root PKI.
 - Assessing the smooth function of the disaster recovery and business continuity procedures, including in dealings with holders of Shares under their cryptographic key shareholder agreements.
 - Supervising the resolution of deficiencies identified in an audit; setting rules on the access to logs in respect of security audit procedures.
 - Establishing a procedure to verify archived information.
 - Establishing procedures for key changeovers for Policy CAs.
 - Recommending key sizes used by Certificate Subscribers.
 - Establishing Certificate Profiles.
 - Undertaking other functions specified in the CPS.

The WPAA itself and/or the guidelines established by the OISTE Foundation PAA may add to, modify, or remove functions from the WPAA.

The WPAA may be contacted at:

WISeKey Policy Approval Authority

29, route de Pré-Bois

Case postale 885

CH-1215 Geneva 15

Switzerland

cps@wisekey.com

1.3.3. Policy Certification Authorities (PCAs)

Policy CAs are certification authorities whose certificates are signed by the OISTE WISeKey Root CA and issue certificates to Issuing Certification Authorities under a specific policy. Policy CAs do not issue any certificates to End Users or for any other type of entities. In issuing certificates to Issuing CAs, Policy CAs perform a wide variety of functions within the OISTE WISeKey Root PKI concerning the lifecycle management of certificates issued to Issuing CAs. In the event that new policies are created by the WPAA which do not fit within the scope of the Policy CAs regulated in this CPS, new Policy CAs may be created, such as a Time-stamping policy authority and will be subject to comply with a separate Certificate Policy in addition to this CPS.

1.3.4. Registration Authorities (RAs)

Registration Authorities are systems (which may or may not be separate legal entities) that process the issuance, suspension and revocation of certificates on behalf of OISTE WISeKey Root PKI.

RAs are bound to comply with the Certification Practices Statement under which they process the certificates and, when they are not part of the same legal entity as the Certification Authority for which it provides RA certification services, it shall be bound by contract to do so.

As part of its operations, a Registration Authority may:

- Determine the certificate policies it will support from those available through the Certification Authorities it provides services to;
- Provide RA services to one or more Certification Authorities;
- Designate registration officers who will provide the RA services.

The specific functions and obligations of a Registration Authority are provided in the applicable CPS and Certificate Policies under which it provides RA certification services.

1.3.5. End Users

The OISTE WISeKey Root CA and subordinated Policy CAs do not issue digital certificates to end users.

1.3.6. Relying Parties

Relying parties are individuals or legal entities that rely on a digital signature, certificate, certificate revocation list or information upon which reliance can be placed in accordance with this CPS. The OISTE WISeKey Root PKI is contractually bound directly or indirectly

(through contract chains) to all entities to which it provides services directly or indirectly, including end users and relying parties. In order to become a part of such a closed community and to place reliance on such services, relying parties are required to consent to a Relying Party Agreement within the OISTE WISeKey Root PKI.

1.3.7. **Applicability**

This Certification Practice Statement applies to the certification practices followed by WISeKey in the issuance and life-cycle management of certificates performed directly by WISeKey. The certification services provided by third parties within the OISTE WISeKey Root PKI are bound to their own CPS and policies, through which they undertake to comply with the minimum practices and policies of this CPS.

1.4. *Contact Details*

This CPS is administered by WISeKey. Enquiries or other communications about this document should be addressed to:

<p>WISeKey SA 29, route de Pré-Bois PO Box 885 CH-1215 Geneva 15 Switzerland Tel: +41 22 594 3000 Fax: +41 22 594 3001</p>
--

2. GENERAL PROVISIONS

2.1. *Obligations*

WISeKey as OISTE WISeKey Root PKI operator and under this Certification Practice Statement undertakes compliance with a series of requirements outlined in this CPS, which cover the following topics and, where applicable, are detailed in the sections referenced under each topic:

- Policy Approval and Maintenance: Establish and maintain the Policy Approval Authorities and the policy approval procedures as described in §1.3.2
- Compliance with Local Law and Agreements: Comply with the law applicable to it for the provision of certification services including data protection or privacy legislation as well as with the agreements it has executed with WISeKey or any third party (e.g. outsourced registration authorities, end users, relying parties, other ancillary service providers) for the provision of certification services.
- Publication of CPS and other documents: Publish the CPS and other relevant public information applicable to its certification services in accordance with §2.5 and §6.1.
- Compliance Audits: Perform and have performed compliance audits in accordance with §2.6
- Confidential Information and Data Protection: Handle confidential information, personal data, and information disclosure in accordance with §2.7
- Intellectual Property Rights: Acknowledge and comply with the intellectual property rights provisions in §2.8
- Certificate Lifecycle Management: Perform the certificate application processes, certificate issuance, and certificate lifecycle management in accordance with §3.1-§3.4 and §3.7.
- Event Logging and Audit Systems: Maintain and operate the event logging and audit systems in accordance with §3.4.
- Records Archiving: Maintain and archive records in accordance with §3.5.
- Dispute Resolution Procedures: Follow the dispute resolution mechanisms provided by this CPS.
- Disaster Recovery Plan: Have in place a disaster recovery plan in accordance with §3.7.
- Physical Procedural and Personnel Security Controls: Comply with the security controls described in §4.
- Technical Security Controls: Comply with the security controls concerning the technical systems as described in §5.

2.1.1. **Root CA Obligations**

WISeKey hereby warrants that in performing its functions as a Root CA it will comply with the obligations referred to in section 2.1 above. WISeKey further warrants and represents that the Root CA cryptographic private key it uses to operate the OISTE WISeKey Root CA and provide Root certification services has not been compromised and that the

information contained in the certificates it issues is not known by WISEKey to be false. As operator of the OISTE WISEKey Root CA, WISEKey assumes no other warranties or obligations in the purview of such activities as described in this CPS.

2.1.2. Policy CA Obligations

Upon accepting the certificates issued by the OISTE WISEKey Root CA, WISEKey providing certification services as a Policy CA in accordance with this CPS hereby warrant that in performing the functions as a Policy CA will comply with the obligations referred to in section 2.1 above. WISEKey or any third party acting as Policy CA further warrant and represent that:

- Private Cryptographic Key Integrity: the Policy CA cryptographic private key it uses to operate any Policy CAs and provide Policy CA certification services has not been compromised.
- Truthfulness and Accuracy: that the information supplied by it during the certificate application process is truthful and that the data published in the certificate pertaining to it is accurate;
- Accuracy of Information in Certificate: that the information contained in the certificates it issues is not known at any time during the certificates' validity period to be false.
- Changes Notification: in the case of Policy CAs operated by third parties, immediately notify WISEKey of any changes to the information material to the certificates issued to it and that it shall maintain all other information maintained by WISEKey with regard to it up to date.
- Avoidance of Damages to PKI: not to interfere with or damage, or attempt to interfere with or damage, any component of the OISTE WISEKey Root PKI, as well as to promptly notify WISEKey of any such incident it becomes aware of.
- Compliance by Outsourcers: ensure that any certification services provided under its authority but outsourced to third parties are legally bound to comply with the corresponding this CPS or, in the case of third party operators, their CPS.

Additional or different obligations may apply to new types of Policy CAs operated by WISEKey and created after the Effective Date of this CPS. Such additional or different obligations shall be described in separate Certificate Policies. Future versions of this CPS may incorporate any new types of Policy CAs, including through the integration of such Certificate Policies into such future versions of this CPS.

2.1.3. End User Obligations

The OISTE WISEKey Root PKI does not issue digital certificates to end users but any entities that issue certificates to end users under the OISTE WISEKey Root PKI shall be required to have end users subscribe an end user agreement or consent to terms through other mechanisms (e.g. internal corporate certificate use policy) that include the issues referenced in this section. The final form of the end user agreement, policy or other similar document would be subject to approval by WISEKey.

Upon applying for certificate end users shall:

- comply with the certificate application process;
- provide the certification authority with accurate and complete information for the

relevant type and/or class of certificate;

- generate or have generated its cryptographic keys in a way that complies with the requirements of the type and/or class of certificate;

The foregoing would not apply in the cases in which the end user does not apply for certificate but is issued a certificate (e.g. an employer issues a certificate to its employees using the human resources database).

In all cases, upon accepting or receiving the certificate issued to it, an end user warrants that:

- the data contained in the certificate is accurate;
- the private cryptographic key associated with the public key contained in the certificate has not been compromised;
- it shall only use the cryptographic key pair and certificates in accordance with the authorised uses for the corresponding type and/or class;
- it shall exercise reasonable care to avoid unauthorized use of the private cryptographic key associated with the public key contained in the certificate;
- it shall notify the issuer of the certificate or other certification services provider (e.g. authorised Registration Authority) that processed its certificate issuance if, prior to the expiration of the certificate:
 - the private key has been lost, stolen, or potentially compromised;
 - control over its private key has been lost due to compromise of the password or other reasons;
 - inaccuracy or changes to the certificate content; and/or
 - the end user wishes to suspend or revoke a certificate for any reason it considers appropriate.

When an end user is issued a certificate as part of the procedure for joining an organization (e.g. employment), community (e.g. club) or for using a product or service, the organization or community compulsory policies or the terms for the product purchase or service subscription will integrate the end user obligations mentioned above.

2.1.4. Relying Party Obligations

All entities that wish to rely on the OISTE WISeKey Root PKI certificates, certificate revocation lists, certificate chains, this Certification Practice Statement, Certificate Policies or any other information published by WISeKey or other certification services providers within the OISTE WISeKey Root PKI are required to consent to the Relying Party Agreement or other document (employee policy, subscription or purchase agreement) incorporating the key terms of the Relying Party Agreement.

Upon consenting to the Relying Party Agreement or other document incorporating the terms of the Relying Party Agreement, a Relying Party undertakes to observe the following obligations:

- verify the validity, suspension or revocation of the certificate using current revocation status information.
- take account of any limitations on the usage and liability limits of the certificate;
- Only rely on digital signatures and certificates when such reliance is deemed

reasonable. In considering the reasonableness of reliance, the aspects to be considered shall include whether:

- the digital signature was created during the validity period of the certificate;
- the digital signature can be verified successfully;
- all of the public key hashes (thumbprints) on the certificates within the corresponding certificate chain are verified successfully;
- the certificates in the certificate chain have not expired;
- the certificate and certificate chain are successfully validated;
- there are no additional circumstances that may affect the reliability of the digital signature, certificate, certificate chain or certificate revocation list.

2.2. Liability Limits and Disclaimers

WISeKey's approach to the use of public key infrastructures, certificates and digital signatures is to allow small and large organizations as well as individuals to benefit from these technologies in the least burdensome and most useful manner. In pursuance of this, WISeKey provides its certification services as described in this CPS.

In sections 2.1, 2.2 and 2.3 of this CPS are the warranties provided by WISeKey which cover the security and procedural regulations that are designed to provide varying levels of security and risk management (from low to high).

WISeKey follows the procedures described in the warranties referred to and in doing so does not pretend to provide the impossible full proof security with the provision of these certification services. In doing so, WISeKey simply seeks to increase the overall level of security for those using its services. Therefore, WISeKey assumes liability for its compliance with the procedures and security measures described in the warranties, but not, where allowed by applicable law, for example, for any warranties that are implied by the law or by any other regulation.

Other warranties (implied by law or otherwise) that are excluded where allowed by applicable law include any warranties:

- to achieve a specific result,
- of merchantability or fitness for a particular purpose,
- with regard to the accuracy or reliability of information contained in certificates that is not provided by and/or verified by WISeKey,
- that are not related to the issues covered in this CPS;
- on the commercial or financial reliability or stability of third parties providing certification services under their own authority or using or relying on the certification services;
- on the legal validity, the ability to satisfy formal requirements or the evidentiary status of digital signatures, certificates or cryptographic keys, and
- with regard to matters outside WISeKey's reasonable control or the reasonable control of third parties providing certification services under OISTE WISeKey Root PKI.

If WISEKey is liable for its non-compliance with the warranties or for any other reason, we seek to avoid paying the excessive damages that are being awarded in certain jurisdictions of the world and for activities that are not directly related to the provision of certification services (in much the same way that a public authority cannot be responsible for what a person does with their official identity card). WISEKey therefore requires the members of the OISTE WISEKey Root PKI community to consent to the fact that WISEKey does not assume liability for any type of damages arising from the circumstances described below (including special, consequential, incidental, indirect or punitive damages), regardless of whether it has been notified of them (or their potential) or not, or whether they are reasonably foreseeable or not.

- underlying transactions between end users and third parties, including relying parties;
- third party products and/or services (including hardware and software) that interact or use the certification services, certificates, digital signatures, etc.;
- if there is a delay, mutilation, loss or other errors in relation to data or documents while they are being created, stored or communicated;
- unreasonable reliance on a certificate, a digital signature, a cryptographic key or key pair, or the certification services to which this CPS refers;
- non-compliance by third parties (including members of the OISTE WISEKey Root PKI community) with local Data Protection or privacy legislation, consumer protection legislation, or any other legislative or regulatory compliance required in local jurisdiction; or
- any indirect or consequential loss or damage, loss of profits, loss of goodwill, loss of anticipated savings, loss of revenue, loss of business, business interruption; or loss of information.

In order to further manage the risks relating to the provision of certification services and to ensure the long term stability of the OISTE WISEKey Root PKI, the amount of any damages awarded are also limited under the terms described in section 2.7.

2.3. Financial responsibility

WISEKey's liability limits towards Subordinate PKI Entities are regulated through contractual agreements with such entities. This CPS and other relevant documents are incorporated by reference into such contracts.

Unless otherwise explicitly agreed or explicitly provided for in a Certificate Policy approved by the WISEKey Policy Approval Authority, WISEKey's liability to End users, Relying Parties and any other entities that are not Subordinate PKI Entities, is limited against claims of any kind, including those of contractual, tortious, extracontractual and delictual nature, on a per certificate basis regardless of the number of transactions, digital signatures, or causes of action arising out of or related to such certificate or any services provided in respect of such certificate and on a cumulative basis.

Any and all claims within the OISTE WISEKey Root PKI arising with regard to a certificate (regardless of the entity causing the damages or the entity that issued a certificate or provided certification services) shall be subject to the liability limitations applicable to it as per this CPS, the Subordinate PKI Entity's CPS and the corresponding Certificate Policy

(where applicable).

The maximum per certificate liability of the OISTE WISeKey Root PKI or any other entity within the OISTE WISeKey Root PKI shall be established in the applicable Certificate Policy. Such per certificate liability limit shall apply regardless of the number of transactions, digital signatures, or causes of action arising out of or related to such certificate or any services provided in respect of such certificate and on a cumulative basis.

Subject to the foregoing limitations, WISeKey's aggregate liability limit towards all End users, Relying Parties and any other entities that are not Subordinate PKI Entities for the whole of the validity period of a certificate issued by the WISeKey Root CA (unless revoked or suspended prior to its expiry) towards all persons with regard to such certificate is CHF 5,000,000.00 (Five Million Swiss Francs), with a maximum aggregate per year liability on such certificates of CHF 500,000.00 (Five Hundred and Thousand Swiss Francs).

In no event shall WISeKey's liability exceed the aforementioned limits.

2.3.1. No Fiduciary relationships

The OISTE WISeKey Root CA is not an agent, fiduciary, trustee, or other representative of Subordinate CAs, Subordinate Registration Authorities, Subordinate Registration Organisations other parties within the OISTE WISeKey Root PKI, End Users or Relying Parties.

Subordinate PKI entities, End Users and Relying Parties are not agents, fiduciaries, trustees or other representatives of WISeKey and shall therefore not bind, make any warranty or representation, act for or in representation of WISeKey, nor undertake or assume any obligation or responsibility on its behalf.

2.4. Interpretation and Enforcement

2.4.1. Governing Law

WISeKey operates out of Switzerland and its certification services are therefore governed and construed in accordance with Swiss laws.

The certification services provided under the authority of third parties may be subject to the laws of other jurisdictions as is indicated in their CPS and/or Certificate Policy.

2.4.1.1. Applicable contract structure

The contractual structure that underpins the OISTE WISeKey Root PKI as a whole includes:

- Root CA-PCA Agreement: This is the contractual arrangement through which the relation between WISeKey and a third party operating a Policy CA is regulated and by which such third party is authorised to operate as such.
- Root CA or PCA – RA Agreement: This is the contractual arrangement by which

- the provision of registration authority services by a third party legal entity is regulated and by which such entity is authorised to operate as such.
- Relying Party Agreement: This contract establishes a relationship between WISeKey or other entity providing certification services within the OISTE WISeKey Root PKI and persons relying on them. This agreement must be consented to prior to reliance and may be incorporated into other documents such as internal employee policy documents or goods or services terms and conditions.

2.4.2. Severability, Survival, Merger, Notice

2.4.2.1. Severability

In the event that any one or more of the provisions of this CPS is for any reason held to be null, invalid, unconstitutional, illegal, or unenforceable at law, such nullity, invalidity, unconstitutionality, illegality or unenforceability shall not affect any other provision, but this CPS shall then be construed as if such provision or provisions had never been contained herein, and insofar as possible, construed to maintain the original intent of the CPS.

2.4.2.2. Survival

This section and the provisions of sections **1.4 (Contact Details)**, **2.1 (Obligations)**, **2.2 (Liability Limits and Disclaimers)**, **2.3 (Financial Responsibility)**, **2.4 (Interpretation and Enforcement)**, **2.6 (Compliance Audit)**, **2.7 (Confidentiality)**, and **2.8 (Intellectual Property Rights)** shall survive the termination of any agreement which this Certification Practice Statement forms a part of.

2.4.2.3. Merger

The provisions of this as well as any rights and obligations corresponding to WISeKey and any third parties, including end users, relying parties or any other entities, may not be amended, waived or terminated by oral, written or other means not compliant with the corresponding procedures, except as expressly provided for herein.

2.4.2.4. Notice

Unless otherwise explicitly provided for in this CPS, notices must be done either in a digitally signed message that can be verified with a certificate capable of being validated within the OISTE WISeKey Root PKI or sent by registered mail or similar courier services that provide a receipt indicating delivery. In either case, the notice will be effective from the moment a digitally signed acknowledgement of receipt or the regular mail delivery receipt is received by the person or entity sending the notice. If it is not received within 5 working days after the moment it was purported to have been received by WISeKey, the notice should be considered as not having been received by WISeKey.

Notices in accordance with the previous paragraph must be delivered to the following email address or postal address:

WISeKey, SA
29, route de Pré-Bois
PO Box 885
CH-1215 Geneva 15
Switzerland
Email: cps@wisekey.com

2.4.2.5. Headings and Appendices

The headings in this CPS are included for convenience purposes only and should not be used to interpret, construe or enforce any of the provisions of the CPS.

The Glossary is an integral part of this CPS but in the event that a contradiction arises between the provisions of this CPS and the Glossary, the former will prevail over the latter.

2.4.2.6. Assignment

The contracts subscribed for the provision of certification services may not be assigned or transferred to other parties without explicit approval by WISeKey. The contracts subscribed by end users or relying parties may not be transferred or assigned under any circumstances.

2.4.3. Dispute resolution procedures

2.4.3.1. Hierarchy of the Certification Practice Statement

In the event of a conflict between this CPS and other policies, plans, agreements, contracts or procedures, where the subject of the conflict is between this CPS and:

- A Root CA - CA agreement, this CPS shall prevail;
- Any agreement between any certification service providers subordinated to the OISTE WISeKey Root PKI, this CPS shall prevail;
- A Certificate Policy, the Certificate Policy shall prevail;
- The CPS and the CPS of a Certification Authority operated under the authority of a third party, this CPS shall prevail.
- An End User agreement or Relying Party agreement, the End User Agreement or Relying Party Agreement shall prevail;
- Any policy, plan, procedures or any other operational or practices documentation whatsoever, this CPS shall prevail.

2.4.3.2. Process

Should a dispute arise out of or in connection with these practices and/or related contracts, prior to resorting to arbitration or legal proceedings, the parties to the dispute shall attempt to settle such dispute or differences by negotiations between them in good faith. In doing so, they shall promptly notify WISeKey of such dispute in accordance with the notification mechanisms provided for under section 2.4 of this CPS. Within a period of 10 days following such notification, WISeKey shall contact the parties to obtain the necessary information and shall appoint a mediator or shall have one appointed by the

Chamber of Commerce and Industry of Geneva, Switzerland (the latter only in the event that WISEKey is a party to the dispute).

If the parties are not able to resolve the dispute through negotiation within twenty (20) days from the date the dispute first arose, then the parties agree to enter into binding arbitration in accordance with the Rules of Conciliation and Arbitration of the International Chamber of Commerce, to jointly appoint an independent arbitrator, having appropriate qualifications and practical experience ("Arbitrator"), for the purpose of resolving the dispute, and agree to be bound by the decision of that arbitrator. The Arbitral Tribunal shall be conducted in English and have its seat in Geneva, Switzerland. The parties will promptly furnish to the Arbitrator (imposing appropriate obligations of confidence) all information reasonably requested by the Arbitrator relating to the dispute. The Arbitrator shall apply the laws of the Canton of Geneva, Switzerland and will use all reasonable endeavours to render the Arbitrator's decision within 30 days following receipt of the information requested or if this is not possible, as soon as practical thereafter. The parties must co-operate fully with the Arbitrator to achieve this objective.

Regardless of the measures taken by the parties to resolve the dispute in accordance with this CPS, WISEKey shall retain its right to seek injunctive relief in the event of alleged or effective material breach of this CPS or any other circumstance related to the dispute which may affect partially or wholly the security of the OISTE WISEKey Root PKI.

2.5. Publication and Repositories

In order to ensure the full availability of this CPS and other essential public documents, WISEKey maintains a repository within its Web site at

<http://www.wisekey.com/repository/>.

2.5.1. Publication of information on the Certification Services

The publication of WISEKey information relevant to the certification services operated by it is done through its Web site. Unauthorized publications or media are not recognized by WISEKey as its own and are therefore not binding upon it.

This document and others describing WISEKey's certification services are on the WISEKey Web site at <http://www.wisekey.com/repository/>.

2.5.2. Frequency of publication

Newly approved versions of a CPS, Certification Authority Certification Practice Statements, Certificate Policies, and any other relevant documents are published in accordance with the amendment and notification procedures in § 6 and any other relevant provisions in the corresponding documents..

2.5.3. Access Control

Access to the OISTE WISEKey Root PKI CPS, public Certificate Policies and other similar documents pertaining to WISEKey's operation of certification services, shall be publicly available.

All CRLs for the OISTE WISeKey Root PKI will be accessible publicly and for free.

2.6. Compliance Audit

2.6.1. OISTE WISeKey Root PKI Compliance Audits

Root CA and Policy CA Audit Level: In the case of the OISTE WISeKey Root CA and the Policy CAs, WISeKey or any third party operators are audited annually by the OISTE Foundation or by a third party authorized by the OISTE Foundation with specialist knowledge in the auditing of Certification services and Public Key Infrastructures. The OISTE Foundation may also, directly or indirectly, at any moment and with the frequency it considers appropriate, perform comprehensive or partial audits to determine whether the OISTE WISeKey Root Cryptographic Key management is compliant with the OISTE Foundation's guidelines (if any). The OISTE Foundation may request that such audits be undertaken by a duly qualified third party.

2.6.2. Topics covered by audit

The topics covered by a compliance audit include:

- Physical Security
- Technology Evaluation
- CA Services Administration
- Personnel Vetting
- CPS and other policies
- Contracts
- Data Protection and Privacy Considerations
- Disaster Recovery Planning

2.6.3. Communication of results

Audit results are considered to be sensitive commercial information. Unless otherwise stipulated by contract, they will be protected as confidential information in accordance with § 2.11 of this CPS.

Copies of the audit logs and reports will be made available to the OISTE Foundation or any independent auditors for the purposes of the audit itself.

2.7. Confidentiality

2.7.1. Types of information to be kept confidential

2.7.1.1. Collection and Use of Personal Information

All personal information collected or used by WISEKey is done in compliance with Swiss Data Protection legislation and based on the distinction provided in this CPS (see glossary) between “Summary Information” and “Identification Information”. Personal information collected and used by certification service providers operated under the authority of third parties shall be required to comply with the applicable data protection legislation. In the absence of any local legislation, the certification services provider shall comply with the minimum standard provided by this CPS and the WISEKey Privacy Policy. In the case of certification services being provided under the authority of a third party to the general public (and not to a closed community) and it ceases to provide certification services, as part of the termination procedure it is required to transfer the personal and other data corresponding to its provision of certification services to another local certification services provider serving the general public or other entity designated by WISEKey or the competent authorities. In all cases, the storage and availability of such data for the purpose of maintaining the provision of certification services to the corresponding end users shall be sought.

The details of how WISEKey collects, processes and stores personal data is contained in the WISEKey Privacy Policy available at the WISEKey repository (<http://www.wisekey.com/repository>).

2.7.1.2. Registration information (Identification Information)

Identification Information is the information obtained or presented to positively identify an entity and provide the certification services requested by it.

Identification information shall be treated as confidential information unless consent is explicitly given otherwise by the entity to which the information refers.

2.7.2. Types of information not considered confidential

2.7.2.1. Summary Information

All certificates issued within the OISTE WISEKey Root PKI for public use may be publicly disclosed. All certificates issued by WISEKey in its direct provision of certification services to third parties may also be publicly disclosed.

2.7.3. WISEKey PKI Documentation

The following WISEKey documents are publicly available and are not considered to be confidential information:

1. This CPS
2. Approved Public Certificate Policies
3. The WISEKey Privacy Policy
4. WISEKey Relying Party Agreement
5. Other documents approved for publication by WISEKey

2.7.4. Disclosure of Certificate Revocation/Suspension information

The reason(s) for the suspension or revocation of a Certificate may be made public, in accordance with applicable law or in the sole and absolute discretion of WISEKey or the Certification Authority that issued the certificate which was suspended or revoked.

2.7.4.1. Disclosure of Certificate suspension information

The reasons for certification suspension are not disclosed.

2.7.5. Release to law enforcement officials

No document or record retained by WISEKey is released to law enforcement agencies or officials except where:

- A properly constituted warrant or request is produced,
- the law enforcement official is properly identified, and
- other applicable legal procedures are complied with.

The documents retained by certification services operating under the authority of third parties shall be treated similarly, but in accordance with the corresponding CPS and applicable law.

2.7.6. Release as part of civil evidence or discovery purposes

As a general principal, no confidential document or record stored by WISEKey is released to any person except where:

- A properly constituted request (i.e. that has complied with all legal procedures) for the production of the information is produced; and
- The person requiring production is a person authorised to do so and is properly identified.

Certification services provided under the authority of third parties may be required to release information for civil evidence or discovery purposes regarding the OISTE WISEKey Root PKI in any jurisdiction where the appropriate legal procedures have been followed.

2.8. Intellectual Property rights

2.8.1. General provision

Except for components which may be the intellectual property of third parties, all intellectual property rights including copyright in all certificates, certificate revocation lists, certificate directories and, unless otherwise explicitly provided for, all practices, policy, operational and security documents concerning the OISTE WISEKey Root PKI (electronic or otherwise) as well as agreements, belong to and will remain the property of WISEKey.

Through the corresponding contracts for the provision of certification services, WISEKey grants a license to third parties for the use of certificates, certificate revocation lists, and

other authorised practices and policy documents as may be required for the provision of certification services in accordance with this CPS.

2.8.1.1. Public and private keys

All intellectual property rights in the public and private keys generated shall vest in the entity by which or for which such keys were generated or the entity designated by it. Certification services operated under the authority of third parties and end users shall not obtain any rights whatsoever in relation to the certificates, their content, format or structure.

2.8.1.2. Certificate

WISeKey reserves the right at any time to suspend or revoke any certificate in accordance with the procedures and policies set out in this Certification Practice Statement and any applicable Certificate Policy. WISeKey hereby grants a non-exclusive and irrevocable license to all Certification Authorities, Relying Parties and other entities to reproduce, and distribute copies of the certificates issued within the OISTE WISeKey Root PKI for the purposes of providing, using and/or relying on the certificates and certification services in accordance with the provisions of this CPS.

2.8.1.3. Distinguished names

Intellectual property rights in distinguished names and customer identification numbers vest with WISeKey unless otherwise specified in a CP, contract or other agreement.

2.8.1.4. Intellectual Property

The intellectual property in this CPS is the exclusive property of WISeKey.

3. OPERATIONAL REQUIREMENTS

3.1. *Certificate Issuance*

The OISTE WISeKey Root PKI will only issue digital certificates for Policy CAs.

3.1.1. **Certificate Issuance Process**

Certificate issuance to a Policy CA entails the following:

1. WISeKey will undertake a CA Creation Ceremony for the Policy CA which shall be witnessed by an auditor designated by WISeKey.
2. The Policy CA will generate its key pairs in an approved hardware security module in accordance with § 5 of this CPS and will generate a PKCS#10 certificate request.
3. The certificate request will be securely transported to the WISeKey Root CA on computer readable media, where WISeKey operating staff will verify the request and then generate the Policy CA certificate and create the Policy CA.
4. The Policy CA certificate will then be taken from the Root CA on computer readable media for incorporation into the Policy CA system and dissemination as required.
5. All valid certificates issued to Policy Certification Authorities shall be published on the WISeKey Web site.

3.1.2. **Operational periods**

All Certificates begin their operational period on the date of issue. The operational period of a Policy CA certificate will be determined at the date of issuance and in no case shall it exceed the expiration date of the Root CA certificate.

3.2. *Certificate Acceptance*

Certificate acceptance shall take place as part of or as a result of the Policy CA Creation Ceremony and will occur at the moment WISeKey and the appointed auditor approve compliance with the ceremony.

3.3. *Certificate Suspension and Revocation*

Suspension of certificates issued by WISeKey usually precedes revocation and where such revocation proceeds, it shall be done in accordance with the specific procedures described in this section.

3.3.1. **Circumstances for Suspension**

The suspension of certificates issued by the WISeKey Root CA may occur immediately or

after an investigation has taken place.

The WPAA will have an ongoing function of investigating any circumstances that may constitute sufficient grounds to suspend or revoke certificates issued by the WISEKey Root. Such investigations will be initiated upon the WPAA receiving information which indicates or raises suspicion that:

- the private key corresponding to the public key in the certificate has been lost, disclosed without authorisation, stolen or compromised in any way.
- the security, trustworthiness or integrity of the OISTE WISEKey Root PKI is materially affected due to the Policy CA's activities.
- there has been an improper or faulty issuance of a certificate due to:
 - A material prerequisite to the issuance of the Certificate not being satisfied;
 - A material fact in the Certificate is known, or reasonably believed, to be false.
- any other material circumstance that requires investigation to ensure the security, integrity or trustworthiness of the OISTE WISEKey Root PKI.

The result of the investigation will be either the order by the WPAA to produce a suspension request or a decision not to proceed with the suspension.

3.3.2. Who can request a Suspension or Revocation?

Suspension or revocation may be requested by the following entities:

- A representative of OISTE explicitly given authority to perform suspension or revocation requests.
- A representative of WISEKey explicitly given authority to perform suspension or revocation requests.
- Swiss court decision by which a decision of a foreign court or public authority requesting the suspension or revocation of the certificate issued by WISEKey is declared executable (*executoire*) in Switzerland.

A valid suspension or revocation request received from any of the aforementioned entities shall result in immediate suspension and the initiation of a post-suspension investigation on whether revocation should follow or the suspension should be lifted.

Suspension or revocation of certificates may also be requested by the WPAA. A suspension request from the WPAA will result in the immediate suspension of the certificate and the initiation of a post-suspension investigation. A revocation request by the WISEKey PAA will result in immediate revocation.

3.3.3. Limits on suspension period

Certificates issued by the WISEKey Root CA shall only remain suspended for a maximum period of twenty (20) days. Upon termination or prior to termination, WISEKey shall determine whether it should be revoked or reinstated as valid.

3.3.4. Circumstances for revocation

A certificate issued by the WISEKey Root CA shall be revoked in all cases through a certificate revocation request issued by the WPAA and only in the following cases:

- when, after going through suspension procedures, it is determined that revocation is required due to material circumstances being ascertained in the post-suspension investigation that merit certificate revocation; and
- when the WPAA requests the revocation of a certificate, regardless of whether the post-suspension investigation has taken place.

3.3.5. Procedure for revocation request

In processing a revocation request, the Root CA will:

- Revoke the certificate on the Root CA, record the reason for the revocation, and maintain relevant documentation.
- Generate immediately a CRL (Certificate Revocation List) from the Root CA
- Withdraw the certificate from the WISeKey Web site and place a prominent revocation notice in its place.
- Issue a notice containing the Certificate details and the date and time of revocation to the certificate subscriber.
- Notify the PCA that it is required to follow the necessary rules and procedures applicable to it under its own CPS, its contracts with its PKI subordinate entities, and any applicable law and licensing/accreditation scheme with regard to the revocation of its certificate.

3.3.5.1. Policy CA duties

The Policy CA of a revoked Certificate shall:

- Continue to safeguard the private key associated with the revoked Certificate, until the date of Certificate expiry, at which time it should be securely destroyed or
- Securely destroy the private key associated with the revoked Certificate in accordance with a procedure approved by the WPAA.
- Actively and promptly notify its Subordinate PKI Entities of the revocation of its certificate.

3.3.6. Revocation request grace period

Revocation requests shall be processed within 24 hours of having a definitive decision by the WPAA to revoke the certificate in accordance with the WPAA operational procedures.

3.3.7. Certificate Validity Checking Requirements

All entities relying on the certificates issued by the OISTE WISeKey Root PKI are required to check the validity status of the certificates in the certificate chain leading up to the OISTE WISeKey Root CA certificate each time a OISTE WISeKey Root PKI certificate is relied upon. Where a Relying Party chooses to rely on certificates issued by a Policy Certification Authority such certificate may be validated using the validation services offered by such Policy Certification Authority (i.e. Certificate Revocation Lists or OCSP Validations).

3.4. Security Audit procedures

WISeKey undertakes comprehensive audits of internal operations and may submit to periodic third party audits. Audit procedures are documented in internal procedures, including information from audit documents.

Access to audit logs is strictly controlled by WISeKey.

3.4.1. Types of Event Recorded

The minimum audit records to be kept include all:

- Certificate application records, including records relating to rejected applications;
- Certificate generation requests, whether or not Certificate generation was successful;
- Certificate issuance, suspension and revocation records, including CRLs;
- Audit records, including security related events;
- Access records to the WISeKey secure off-line facilities.

3.4.2. Frequency of processing log

Audit logs take place whenever an operation is performed on the WISeKey Root CA, otherwise the WISeKey Root CA remains offline.

3.4.3. Retention period for audit log

Audit logs are retained for a minimum of 20 years.

3.4.4. Audit collection system

The WISeKey audit collection system is a combination of automated and manual processes performed by the OISTE WISeKey Root CA and Policy CA operating systems, the OISTE WISeKey Root CA and Policy CA applications, and by operational personnel. The system is therefore maintained through access control mechanisms and role separations with regard to the software and hardware that handle the automated collections and through confidential documented operational procedures known and followed by WISeKey personnel with regard to manual collection.

3.4.5. Notification to event-causing subject

Operations personnel notify their security administrator when a process or action causes a critical security event or discrepancy. Subordinate PKI Entities are also required to notify any event that may cause a critical security event or discrepancy. In all cases, the WPAA shall decide what steps should be taken.

3.5. Records Archival

All OISTE WISeKey Root PKI records concerning the operation of its certification services are archived and are retained for a minimum period of twenty (20) years. The time source for the WISeKey Root CA is independently verified periodically and all electronic automated Root CA records are associated with the time and date of their occurrence. Archives of records are maintained under closed access control and are subject to inspection by auditors.

All physical records and Identification Information shall be archived by the entity that directly provides certification services to a Subordinate PKI Entity. WISeKey shall require the entity to archive such records and information for a period of 10 years from the date of certificate expiry and shall use its best endeavours to have such entities maintain compliance with their archival obligations. Such period may be extended with regard to specific records and information upon request of special archiving services. In all cases, the records may be archived in paper or electronic form.

3.6. Key changeover

Key changeover is not automatic. Keys expire at the same time as their associated Certificates.

Policy CAs are required to instigate key changeover at least sixty-six (66) months before the expiration of their certificates.

3.7. Compromise and Disaster Recovery

WISeKey has established a Disaster Recovery plan for the event of a compromise or other disaster that might threaten the OISTE WISeKey Root PKI. The Disaster Recovery plan is reviewed periodically in light of changes to the risk environment.

The Disaster Recovery plan addresses:

- Failure/corruption of computing resources;
- Key compromise
- Natural disasters and CA Termination

4. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

4.1. *Physical Controls for Root CA*

The hardware and software for the WISEKey Root CA is maintained off-line in a high security facility with comprehensive perimeter security and enforced internal access controls. Sophisticated intruder detection systems are deployed to notify security personnel of any violation of access controls.

4.2. *Procedural Controls*

No member of staff is allowed to gain physical access or operate any component of the OISTE WISEKey Root PKI without the presence of other designated members of staff who have the skills required to confirm that no unauthorized or inappropriate actions are conducted.

Procedures are defined and documented for all operations upon the OISTE WISEKey Root PKI. Operating procedures are regularly reviewed in the light of new operational requirements.

4.3. *Personnel Controls*

All WISEKey staff involved in the operation of the OISTE WISEKey Root PKI is subjected to background checks and vetting. Character references are thoroughly investigated for all operational personnel.

All operation of the OISTE WISEKey Root PKI is under the direct responsibility of WISEKey Executive Officers.

Personnel involved in the control and operation of the OISTE WISEKey Root PKI shall be sufficiently trained to comply with the functions allocated to their role and shall be provided with ongoing training to ensure the appropriate levels of awareness of the security policies and procedures.

5. TECHNICAL SECURITY CONTROLS

5.1. *Key Pair Generation and Installation*

5.1.1. **Key Pair Generation**

Key pairs for the OISTE WISeKey Root CA and Policy CAs are generated in a hardware security module (HSM) certified to meet the requirements of FIPS 140-1 level 3 or higher.

5.1.2. **Private Key Delivery to Entity**

Key delivery to Policy CAs will not be provided as each PCA will generate its own cryptographic key pairs.

5.1.3. **Public Key Delivery to Certificate Issuer**

Policy CAs' Public keys are delivered to the Root CA as a PKCS#10 certificate request. The signature on the PKCS#10 request is verified to confirm that the Policy CA is in possession of the private key associated with each public key delivered.

5.1.4. **Root CA Public Key Delivery to Users**

The Certificate of the Root CA is made publicly available for Certificate path validation purposes.

The certificate hash (thumbprint) and the certificates of the OISTE WISeKey Root PKI are available on the WISeKey Web site (www.wisekey.com/repository/). Relying parties must confirm the validity of their copy of the OISTE WISeKey Root PKI certificates using these thumbprints.

5.1.5. **Key Sizes**

The modulus of the WISeKey Root CA and the keys of Policy CAs are all at least 2048 bits in length and use the RSA algorithm.

5.1.6. **Public Key Parameters Checking**

The parameters used in the generation of public keys are in accordance with the requirements of FIPS 140-1.

5.1.7. **Parameter Quality Checking**

Parameter quality checking is in accordance with FIPS 140-1.

5.1.8. Key Usage Purposes

The Root Cryptographic Key may be used for:

- The issuance of certificates to Policy Certification Authorities.
- Protocol functions for the operation of the Root CA
- Issuance of Certificate Revocation Lists
- Cross-certification, as approved by the WPAA and the OISTE Foundation.

5.2. Private Key Protection

5.2.1. Standards for Cryptographic Module

The cryptographic module used by the OISTE WISeKey Root PKI is certified to meet the requirements of FIPS 140-1 level 3. In the case of the WISeKey Root CA, such cryptographic module is maintained offline.

5.2.2. Private Key (n out of m) Multipersonal Control

The Root Cryptographic Key can only be exported from the hardware security module when split into multiple parts and requires the presence and participation of several authorised WISeKey officers to reconstruct.

5.2.3. Private Key Escrow

The WISeKey Root CA does not provide this service.

5.2.4. Private Key Backup

The Root Private Cryptographic Key is only backed up for disaster recovery purposes.

5.2.5. Private Key Archival

The Root Private Cryptographic Key will not be archived.

5.2.6. Private Key Entry into Cryptographic Module

Private keys for the Root CA and Policy CAs are generated in Hardware Security Modules. Where there is a requirement for a private key to be loaded or unloaded from a cryptographic module (HSM), the private key is never available in plain text whilst outside a secure environment.

5.2.7. Method of Activating Private Key

Root CA and Policy CA Private key activation requires entry and validation of a PIN/passphrase compliant with specified security parameters

5.2.8. Method of Deactivating Private Key

The Root CA Private Key is automatically deactivated after each use.

5.2.9. Method of Destroying Private Key

The Root CA and Policy CA Private Key in the HSM may be destroyed by returning the HSM to its factory initialised state. Smartcards and other cryptographic tokens used by the Root CA and Policy CA will be physically destroyed prior to disposal.

5.2.10. Usage Periods for the Public and Private Key

The WISeKey Root CA key pair and certificate will expire after 32 years from the moment of their generation.

The Policy CA key pair and certificates will expire 15 years from the moment of their generation.

5.3. Activation Data

5.3.1. Activation Data Generation and Installation

All activation data generation and installation complies with FIPS 140-1, level 2 or higher.

5.3.2. Activation Data Protection

Activation data protection complies with FIPS 140-1, level 2 or higher.

5.4. Computer Security Controls

WISeKey has established and documented all computer security technical controls implemented for the OISTE WISeKey Root PKI,

5.5. Life Cycle Technical Controls

5.5.1. System Development Controls

The CA software used by the OISTE WISeKey Root PKI for certificate issuance and lifecycle management has been developed in accordance with the requirements of ITSEC (Information Technology Security Evaluation Criteria) Level E3.

The HSM used by the WISeKey Root CA and Policy CAs has been certified to meet the requirements of FIPS 140-1 level 3.

5.5.2. **Security management controls**

Security management controls are enforced by rigid separation of operator roles to meet the requirements of the established security policy.

5.6. Network Security Controls

The WISeKey Root CA is maintained off-line and is not networked with any external components.

6. Specification Administration

The WPAA is responsible for setting certification practices and certificate policy direction overall for the PKI. Contact details for the WPAA appear in this CPS under section 1.3.2. The WPAA is required to follow the guidelines (if any) established by the OISTE Foundation, which is the legal entity that owns the Root Cryptographic Key managed by WISeKey.

6.1. Specification change procedures

6.1.1. Initial publication

The WISeKey Root CPS shall be published upon approval by the WPAA. Publication shall take place at the WISeKey Web site at <http://www.wisekey.com/repository/>.

6.1.2. Changes

6.1.2.1. Authority to Amend

WISeKey, through the WPAA, shall have the right to amend this CPS.

The OISTE Foundation PAA shall also be entitled to require WISeKey to comply with the guidelines it issues for the management of the Root Cryptographic Key which may entail the amendment of this CPS.

6.1.2.2. Nature of Amendments and Effective Date

Amendments to the Root CPS shall not be retroactive, shall override any previous versions of the WISeKey CPS and conflicting provisions of the amended CPS, and shall apply to the OISTE WISeKey Root PKI. The amendments made to the Root CPS may be of three types:

- Substantial Amendments: these are the amendments which, in the judgment of WISeKey, are of such significance that they require being subject to a consultation by OISTE prior to their becoming effective.
- Immediately Effective Substantial Amendments: these are amendments which, in the judgment of WISeKey, are of similar significance to the Substantial Amendments but require immediate effectiveness to impede the total or partial loss of integrity, security or trustworthiness to the OISTE WISeKey Root PKI.
- Insubstantial Amendments: these are amendments that are, in the sole judgment of WISeKey, of little significance and are therefore not subject to any consultation. Unless otherwise explicitly provided for in WISeKey's sole discretion, these amendments shall have effect upon publication.

6.2. Publication and Notification Policies

All amendments undertaken in accordance with the foregoing sections shall be published at the WISEKey Repository at <http://www.wisekey.com/repository/>. Unless otherwise explicitly provided for, such publication shall be deemed sufficient notice for the purposes of the effectiveness date of the amendments, the consent to the amendments, as well as any other relevant purposes regarding such published documents.

6.3. CPS approval procedures

Certification Practice Statements for use under the OISTE WISEKey Root PKI must be approved by the WPAA.

7. Appendix - Glossary

Access Control

The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner.

[ISO 7498-2: 1989]

Applicant

The entity that has applied to be issued a certificate within the WISEKey PKI. The verification processes vary in accordance with the nature and, where applicable, the operational role within the PKI corresponding to the certificate the entity is applying.

Asymmetric Key Pair

A pair of related keys where the private key defines the private transformation and the public key defines the public transformation.

[ISO/IEC 9798-1 (2nd edition): 1997] [2nd DIS ISO/IEC 11770-3 (08/1997)]

Audit

Audit is defined as a review and examination of system records and activities to assess the adequacy and effectiveness of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Event

An action, detected internally by the system which may generate an audit record. If an event causes an audit record to be generated [for recording in the audit trail], it is a "recorded event". Otherwise, it is an "unrecorded event". The system decides, as each event is detected, whether to generate an audit record by the audit pre-selection algorithm. The set of audit events is based upon a system's security policy.

[ISO/IEC POSIX Security]

Audit Level

A series of requirements and regulations associated with Policy Types as provided in this CPS against which a specific certification services providers are audited.

Audit Record

The discrete unit of data recorded in the audit trail on the occurrence of a recorded event. An audit record consists of a set of audit descriptions, each of which has a set of audit

attributes associated with it. Every audit record always has an audit description for the record's header, and usually has additional audit descriptions describing the entity(ies) and object(s) involved in the event.

[ISO/IEC POSIX Security]

Availability

The property of information being accessible and usable upon demand by an authorised entity or process.

Certificate

It is a data structure, using the CCITT ITU X.509 standard, containing the public key of an entity, together with associated information, and rendered un-forgable by being digitally signed by the Certification Authority which issued it.

Certification Authority

An authority trusted by one or more users to create, issue and manage the life-cycle of certificates.

Certificate Chain

A chain of multiple certificates needed to validate a certificate. Certificate chains are built by linking and verifying the digital signature on a certificate with a public key on a certificate issued by the WISEKey Root Certification Authority.

Certificate Generation

Certificate generation is the process of creating a certificate from inputs specific to the application and the user.

Certificate Policy (CP)

A named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of mobile communication transactions for the trading of goods within a given price range.

Certification Practice Statement

A statement of the practices which a certification authority employs in issuing certificates and managing the life-cycle of such certificates.

Certificate Request

Authenticated request by an entity for its parent authority to issue a certificate which binds the identity of that entity to its public key.

Certificate Revocation

Certificate revocation is the process of changing the status of a certificate from valid or suspended to revoked. The status of a certificate as revoked means that it should not longer be relied upon by any entity for whatever purpose.

Certificate Revocation List (CRL)

A signed list of the certificates which have been revoked by the WISeKey Root CA.

Certification Services

Any of the services that can be provided in relation to the lifecycle management of certificates at any level of the PKI hierarchy, including ancillary services such as OCSP services, time-stamping services, identity verification services, CRL hosting, etc.

Compliance Audit

A review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures.

Confidentiality

The property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

[ISO 7498-2: 1989] [TR 13335-1: 1996]

Cryptographic Key

A parameter used in conjunction with an algorithm for the purpose of validation, authentication, encipherment or decipherment.

[ISO 8732: 1988]

Cryptographic Token

The medium in which a key is stored (e.g. smart card, cryptographic key).

Cryptography

The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use.

[ISO 7498-2: 1989] [ISO 8732: 1988]

Data Integrity

The quality or condition of being accurate, complete and valid, and not altered or destroyed in an unauthorised manner.

Digital Signature

Data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient.

[ISO 7498-2: 1989]

Encryption

The process by which plain text data are transformed to conceal their meaning. Encryption is a reversible process effected by using a cryptographic algorithm and key.

End User

These are entities (legal, natural, mechanical or electronic) that have been issued certificates within the WISeKey PKI but are not subordinate PKI entities.

Entity

Any person (legal or natural) or system (mechanical or electronic).

Evaluation

Assessment against defined criteria in order to give a measure of confidence it meets the corresponding requirements.

Identification information

The information obtained or presented to positively identify an entity and provide the certification services requested by it.

Interoperability

Interoperability implies that equipment and procedures in use by two or more entities are compatible, and hence that it is possible to undertake common or related activities.

Key

A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification).

[ISO/IEC 9798-1 (2nd edition): 1997] [ISO/IEC 11770-1: 1997]

Key Archiving

Key archiving is the process of storing used key or their ID, and/or certificates as a record in long term storage for future retrieval.

Key Destruction

Key destruction is the process of removing all copies of a key throughout the key management system.

Key Generation

Key generation is the process by which cryptographic keys are created. It is the function of generating variables required to meet particular key attributes.

Key Management

The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.

[ISO/IEC 11770-1: 1997]

Key Pair

The keys in an asymmetric cryptosystem having the property that one of the pair will decrypt what the other encrypts.

OCSP (On-Line Certificate Status Protocol)

A protocol which is used to provide real-time validation of a certificate's status. An OCSP responder is used to respond to certificate status requests and can issue one of three responses: Valid, Invalid, Unknown.

An OCSP responder replies to certificate status requests on the basis of CRLs (Certificate Revocation Lists) provided to it by certification authorities.

Operational Infrastructure

The technological infrastructure by which the certification services are provided. This infrastructure does not necessarily coincide with the legal infrastructure or relationships that exist or that develop between entities that form part of the WISEKey PKI or that use the WISEKey PKI certification services in any way.

Physical Security

The measures used to provide physical protection of resources against deliberate and accidental threats.

[ISO 7498-2: 1989]

Policy Certification Authority

A Certification Authority that has been issued its CA certificate by the WISEKey Root Certification Authority.

Post-Suspension Investigation

Investigation performed by the WPAA after a certificate has been suspended in order to determine whether such certificate should be revoked or reinstated as valid.

Private Key

The key of an entity's asymmetric key pair which shall normally only be known by that entity.

[2nd DIS ISO/IEC 11770-3 (08/1997)]

Public Key

The key of an entity's asymmetric key pair which can be made public, although not necessarily available to the public in general, as it may be restricted to a pre-determined group.

Public Key Certificate

A digital certificate that binds unforgeably the public key of an entity to the entity's distinguishing identifier, and which indicates a specific validity period.

Public Key Infrastructure

The infrastructure needed to generate, distribute, manage and archive keys, certificates and certificate revocation lists, and OCSP responders.

[2nd DIS ISO/IEC 11770-3 (08/1997)]

Recipient

The entity that gets (receives or retrieves) a message.

Rekey

The act of replacing an expired Certificate by providing a new set of keys.

Registration Authority

An entity whose purpose is to provide local support to a set of Subordinate PKI Entities or End Users that are physically far from their immediate superior certification authority. A Registration Authority performs a subset of the functions available to a certification authority administrator responsible for directly managing a set of Subordinate PKI Entities and End Users. The functions of Registration Authorities within the WISEKey PKI are provided for under § 1.3 of this CSP and under the corresponding CPS of its parent

ACA.

Relying Party

Any entity relying on a certificate that: (1) has agreed to a Relying Party Agreement within the WISEKey PKI or other similar agreement containing Relying Party provisions within the WISEKey PKI or (2) is designated as such by an approved Certificate Policy, despite not having signed a Relying Party agreement.

Revocation

To change the status of a valid or suspended certificate to “revoked” from a specified time and forward.

Subordinate PKI Entity

Any entity that has the authority to operate or provide certification services under the OISTE WISEKey Root PKI. Natural persons may not be Subordinate PKI Entities under the WISEKey Root CA.

Summary Information

The basic information required for the production of a public key certificate, for the verification of a digital signature, for the validation of a certificate’s status as well as the information produced as a result of such verification and validation.

Validation

The process of checking the validity of a Certificate in terms of its status (i.e. suspended or revoked).

Verification Process

A process which takes as input the signed message, the verification key and the domain parameters, and which gives as output the result of the signature verification: valid or invalid.

[FCD ISO/IEC 14888-1 (12/1997)]

OISTE WISEKey Root CA (OWRCA)

It is the apex of the PKI hierarchy which is provided by the OISTE WISEKey Root within the OISTE WISEKey Root PKI.

OISTE WISEKey Root PKI

It is the public key infrastructure made up of the OISTE WISEKey Root CA and the Policy CAs subordinated to it.

ⁱ Chokhani, S. and Ford, W., INTERNET X.509 PUBLIC KEY INFRASTRUCTURE CERTIFICATE POLICY AND CERTIFICATION PRACTICES FRAMEWORK, Internet Society, Network Working Group, Information Request for Comments No. 2527, March 1999.