

WISeKey SA ADVANCED SERVICES ISSUING CERTIFICATION AUTHORITY CERTIFICATION PRACTICE STATEMENT

**Version 1.01
Effective Date: 16 January 2007**

WISeKey S.A. © 2000-2007

WISeKey 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 WISeKey.

1	INTRODUCTION	6
1.1	OVERVIEW AND TRUST MODEL	6
1.1.1	WISeKey SA	7
1.1.2	Definitions	7
1.1.3	PKI Operational Infrastructure	7
1.1.4	Scope	7
1.2	IDENTIFICATION	7
1.2.1	X.500 Object Identifier hierarchy	7
1.3	COMMUNITY AND APPLICABILITY	8
1.3.1	OISTE and Subordinated Policy Approval Authorities	8
1.3.2	WISeKey Policy Approval Authority role for Issuing CA	8
1.3.3	OISTE WISeKey Root CA	9
1.3.4	Advanced Policy Certification Authority	9
1.3.5	Advanced Services Issuing Certification Authority	9
1.3.6	WISeKey Registration Authorities	10
1.3.7	Registration Authorities (RAs)	10
1.3.8	End Users or entity	10
1.3.9	Relying Parties	11
1.3.10	Applicability	11
1.4	CONTACT DETAILS	11
2	GENERAL PROVISIONS	12
2.1	OBLIGATIONS	12
2.1.1	Issuing CA Obligations	12
2.1.2	End User Obligations	13
2.1.3	Relying Party Obligations	14
2.2	LIABILITY LIMITS AND DISCLAIMERS	14
2.3	FINANCIAL RESPONSIBILITY	15
2.3.1	No Fiduciary relationships	15
2.4	INTERPRETATION AND ENFORCEMENT	15
2.4.1	Governing Law	15
2.4.1.1	Applicable contract structure	15
2.4.2	Severability, Survival, Merger, Notice	16
2.4.2.1	Severability	16
2.4.2.2	Survival	16
2.4.2.3	Merger	16
2.4.2.4	Notice	16
2.4.2.5	Headings and Appendices	17
2.4.2.6	Assignment	17
2.4.3	Dispute resolution procedures	17
2.4.3.1	Hierarchy of the Certification Practice Statement	17
2.4.3.2	Process	17
2.5	PUBLICATION AND REPOSITORIES	18
2.5.1	Dissemination of information on the Certification Services	18
2.5.2	Frequency of publication	18
2.5.3	Access Control	18
2.6	COMPLIANCE AUDIT	18
2.6.1	Issuing CA Compliance Audits	18
2.6.2	Topics covered by audit	19
2.6.3	Communication of results	19
2.7	CONFIDENTIALITY	19
2.7.1	Types of information to be kept confidential	19

2.7.1.1	Collection and Use of Personal Information	19
2.7.1.2	Registration information (Identification Information).....	20
2.7.2	<i>Types of information not considered confidential</i>	20
2.7.2.1	Summary Information	20
2.7.3	<i>Issuing CA Documentation</i>	20
2.7.4	<i>Disclosure of Certificate Revocation/Suspension information</i>	20
2.7.4.1	Disclosure of Certificate suspension information	20
2.7.5	<i>Release to law enforcement officials</i>	20
2.7.6	<i>Release as part of civil evidence or discovery purposes</i>	20
2.8	INTELLECTUAL PROPERTY RIGHTS	21
2.8.1	<i>General provision</i>	21
2.8.1.1	Public and private keys	21
2.8.1.2	Certificate.....	21
2.8.1.3	Distinguished names	21
2.8.1.4	Intellectual Property	21
3	OPERATIONAL REQUIREMENTS.....	22
3.1	CERTIFICATE ISSUANCE.....	22
3.1.1	<i>Certificate Issuance Process</i>	22
3.1.1.1	Corporate Email Certificate	22
3.1.2	<i>Operational periods</i>	23
3.2	CERTIFICATE ACCEPTANCE	23
3.3	CERTIFICATE SUSPENSION AND REVOCATION	23
3.3.1	<i>Circumstances for Suspension</i>	23
3.3.2	<i>Who can request a Suspension or Revocation?</i>	23
3.3.3	<i>Limits on suspension period</i>	23
3.3.4	<i>Circumstances for revocation</i>	23
3.3.5	<i>Procedure for revocation request</i>	24
3.3.5.1	Issuing CA duties	24
3.3.6	<i>Revocation request grace period</i>	24
3.3.7	<i>Certificate Validity Checking Requirements</i>	24
3.4	SECURITY AUDIT PROCEDURES	24
3.4.1	<i>Types of Event Recorded</i>	24
3.4.2	<i>Frequency of processing log</i>	25
3.4.3	<i>Retention period for audit log</i>	25
3.4.4	<i>Audit collection system</i>	25
3.4.5	<i>Notification to event-causing subject</i>	25
3.5	RECORDS ARCHIVAL	25
3.6	KEY CHANGEOVER	25
3.7	COMPROMISE AND DISASTER RECOVERY	25
4	PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS.....	26
4.1	PHYSICAL CONTROLS FOR THE ISSUING CA	26
4.2	PROCEDURAL CONTROLS	26
4.3	PERSONNEL CONTROLS	26
5	TECHNICAL SECURITY CONTROLS	27
5.1	KEY PAIR GENERATION AND INSTALLATION	27
5.1.1	<i>Key Pair Generation</i>	27
5.1.2	<i>CA Public Key Delivery to Users</i>	27
5.1.3	<i>Key Sizes</i>	27
5.1.4	<i>Public Key Parameters Checking</i>	27
5.1.5	<i>Parameter Quality Checking</i>	27
5.1.6	<i>Private Key Protection and Cryptographic Module Engineering Controls</i>	27
5.2	PRIVATE KEY PROTECTION	28
5.2.1	<i>Cryptographic Modules Standards and Controls</i>	28
5.2.2	<i>Private Key Multi-Person Control</i>	28
5.2.3	<i>CA Key Backup and Recovery</i>	28

5.2.4	<i>Private Key Entry into or from a Cryptographic Module</i>	29
5.2.5	<i>Private Key Storage on Cryptographic Module</i>	29
5.2.6	<i>Method of Activating Private Key</i>	29
5.2.7	<i>Method of deactivating private key</i>	29
5.2.8	<i>Method of Destroying Private Key</i>	29
5.2.9	<i>Usage Periods for the Public and Private Key</i>	29
5.3	COMPUTER SECURITY CONTROLS	30
5.4	LIFE CYCLE TECHNICAL CONTROLS	30
5.4.1	<i>System Development Controls</i>	30
5.4.2	<i>Security management controls</i>	30
5.4.3	<i>Network Security Controls</i>	30
6	CERTIFICATE, CRL AND OCSP PROFILES	31
6.1	CERTIFICATE POLICY OVERVIEW	31
6.2	CERTIFICATE PROFILE	32
6.2.1	<i>Version Numbers</i>	32
6.2.2	<i>Certificate Extensions</i>	32
6.2.3	<i>Key usage</i>	32
6.2.4	<i>Certificate Policy Extensions</i>	33
	POLICY QUALIFIERS ARE GENERALLY ABSENT	33
	THIS EXTENSION'S CRITICALITY FIELD IS SET TO FALSE	33
6.2.5	<i>Subject Alternative Names</i>	33
6.2.6	<i>Issuer Alternative Name</i>	33
	THIS EXTENSION'S CRITICALITY FIELD IS SET TO FALSE	33
6.2.7	<i>Basic Constraints</i>	33
6.2.8	<i>Extended Key Usage</i>	33
6.2.9	<i>CRL Distribution Points</i>	34
6.2.10	<i>Authority Key Identifier</i>	34
	THE EXTENSION'S CRITICAL FIELD IS GENERALLY SET TO FALSE	34
6.2.11	<i>Subject Key Identifier</i>	34
	THE EXTENSION'S CRITICAL FIELD IS GENERALLY SET TO FALSE	34
6.2.12	<i>Algorithm Object Identifiers</i>	34
6.2.13	<i>Name Forms</i>	34
6.2.14	<i>Certificate Policy Object Identifier</i>	34
	WHERE THIS EXTENSION IS USED, THIS EXTENSION'S CRITICALITY FIELD IS SET TO FALSE	34
6.2.15	<i>Usage of Policy Constraints Extension</i>	34
6.2.16	<i>Processing Semantics for the Critical Certificate Policies extension</i>	34
6.3	CERTIFICATE POLICY.....	35
6.3.1	<i>Secure Email -CertifyID Advanced User</i>	35
6.3.2	<i>Secure Email -CertifyID Advanced Corporate User</i>	37
6.3.3	<i>Secure Server Certificate -CertifyID Advanced Server</i>	39
6.4	CRL PROFILE	41
6.5	OCSP PROFILE	42
7	SPECIFICATION ADMINISTRATION	43
7.1	SPECIFICATION CHANGE PROCEDURES.....	43
7.1.1	<i>Initial publication</i>	43
7.1.2	<i>Changes</i>	43
7.1.2.1	<i>Authority to Amend</i>	43
7.1.2.2	<i>Nature of Amendments and Effective Date</i>	43

7.2	PUBLICATION AND NOTIFICATION POLICIES	43
7.3	CPS APPROVAL PROCEDURES	44
8	APPENDIX - GLOSSARY	45

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 the Issuing Certification Authorities (Issuing CAs) subordinated to the OISTE WISeKey Global Root CA.

The WISeKey Certification Authority Services (WCAS) under which the operation of the Issuing CAs 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, corporate uses) 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:

- o Practices employed by the operators of Issuing CAs;
- o Use of technologies and procedures to support the underlying operational structure.

The minimum 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 clear 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 real world needs and 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 (“WISeKey”) 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 Advanced Services Issuing CA is operated by WISeKey subordinated to the OISTE/WISeKey Root Public Key Infrastructure, which is a combination of services and infrastructures implemented and managed by WISeKey in accordance with the OISTE WISeKey Root CPS available at <http://www.wisekey.com/repository/>.

1.1.4 Scope

This CPS covers the practices applied to the Advanced Services Issuing CA of 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 ‘WISeKey Advanced Services Issuing CA CPS’. The primary source of the current version of the CPS and other important WISeKey certification services documents is <http://www.wisekey.com/repository/>

1.2.1 X.500 Object Identifier hierarchy

Object Identifiers (OIDs) below this Issuing CA are assigned WISeKey and documented in a Configuration baseline.

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 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 WISEKey Policy Approval Authority (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.

1.3.2 WISEKey Policy Approval Authority role for Issuing CA

WISEKey's PAA role has been extended to review and/or approve the practices, policies and procedures for the Advanced Services Issuing CA it operates by undertaking, subject to compliance with the OISTE WISEKey Root CPS, the following functions:

- Reviewing and approving this CPS and all practices and policies ensuring compliance with the OISTE WISEKey Root CPS.
- Initiating, consulting in respect of, and approving any amendment to this CPS.
- Establishing guidelines for the dissemination of this CPS as well as similar policy documents.
- Ensuring the methods of dissemination of applicable policies to the community using the certification services of the Issuing CA.
- Taking the necessary measures to ensure ongoing compliance and enforcement of this CPS.
- Approving naming conventions in compliance with the OISTE WISEKey Root CPS.
- Investigating and deciding under which circumstances End User Certificates issued by the Issuing CA should be revoked.
- 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 Issuing CAs.
- Undertaking other functions specified in the CPS.

The WISEKey PAA may be contacted at:

<p style="text-align: center;">WISEKey Policy Approval Authority 29 Route de Pré-Bois, PO Box 885 1215 Geneva 15 Switzerland cps@wisekey.com</p>
--

1.3.3 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.

1.3.4 Advanced Policy Certification Authority

Advanced Policy CA is a certification authority whose certificate is signed by the OISTE WISEKey Root CA and issue certificates to Advanced Issuing Certification Authorities under a specific policy. Advanced Policy CA do not issue any certificates to End Users or for any other type of entities. In issuing certificates to Issuing CAs, Advanced Policy CA perform a wide variety of functions within the OISTE WISEKey Root PKI concerning the lifecycle management of certificates issued to Issuing CAs.

1.3.5 Advanced Services Issuing Certification Authority

Advanced Services Issuing CA has been issued its certificate by the Advanced Policy Certification Authority.

WISEKey uses the OISTE WISEKey Common Global Root GA (AICPA/CICA WebTrust Program for Certification Authorities compliant security provider) for its Root CA Certificates. The following high-level representation of the WISEKey PKI is used to illustrate the hierarchy utilized.

OISTE WISEKey Common Global Root GA CA

→ WISEKey CertifyID Advanced G1 CA

→ WISEKey CertifyID Advanced Services CA 1

1.3.6 WISeKey Registration Authorities

WISeKey has established the necessary secure infrastructure to fully manage the lifecycle of digital certificates within its PKI. Through a network of Registration Authorities (RA), WISeKey also makes its certification authority services available to its subscribers. WISeKey RAs:

- Accept, evaluate, approve or reject the registration of certificate applications.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of application as specified in the WISeKey validation guidelines documentation.
- Use official, notarized or otherwise indicated document to evaluate a subscriber application.
- Verify the accuracy and authenticity of the information provided by the subscriber at the time of reissue or renewal as specified in the WISeKey validation guideline documentation.

Certificates issued through an RA contain an amended Certificate Profile within an issued certificate to represent the involvement of the RA in the issuance process to the Relying Party.

1.3.7 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 WISeKey.

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.

1.3.8 End Users or entity

End Users or certificate subscribers are issued certificates generated by the Advanced Services Issuing Certification Authority but the End User's certificate application may be processed by the Issuing CA or a RA, in accordance with this Certification Practice Statement. End users are required to consent to an End User Agreement which states their rights and obligations or to be subject to compliance with policies or regulations (for example, organizational security policies) that incorporate the content of an End User Agreement.

1.3.9 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. WISeKey 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 or to be subject to regulations or policies that incorporate the terms of the Relying Party Agreement.

1.3.10 Applicability

This Certification Practice Statement applies to the certification practices followed by WISeKey in the issuance and life-cycle management of certificates performed by WISeKey.

1.4 Contact Details

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

<p style="text-align: center;">WISeKey 29 Route de Pré-Bois, PO Box 885 CH-1215 Geneva 15 Switzerland Tel: +41 22 594 3000 Fax: +41 22 594 3001 cps@wisekey.com</p>
--

2 GENERAL PROVISIONS

2.1 *Obligations*

WISeKey as operator of the Advanced Services Issuing CA and any RAs operated directly by it or by third parties under this Certification Practice Statement undertakes to comply with, or contractually imposes compliance on any third party RAs (as applicable), 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:

- o Policy Approval and Maintenance: Establish and maintain the Policy Approval Authorities and the policy approval procedures as described in §1.3.3
- o 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.
- o 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 §7.1.
- o Compliance Audits: Perform and have performed compliance audits in accordance with §2.6
- o Confidential Information and Data Protection: Handle confidential information, personal data, and information disclosure in accordance with §2.7
- o Intellectual Property Rights: Acknowledge and comply with the intellectual property rights provisions in §2.8
- o Certificate Lifecycle Management: Perform the certificate application processes, certificate issuance, and certificate lifecycle management in accordance with §3.1-§3.3 and §3.6.
- o Event Logging and Audit Systems: Maintain and operate the event logging and audit systems in accordance with §3.4.
- o Records Archiving: Maintain and archive records in accordance with §3.5.
- o Dispute Resolution Procedures: Follow the dispute resolution mechanisms provided by this CPS.
- o Disaster Recovery Plan: Have in place a disaster recovery plan in accordance with §3.7.
- o Physical Procedural and Personnel Security Controls: Comply with the security controls described in §4.
- o Technical Security Controls: Comply with the security controls concerning the technical systems as described in §5.

2.1.1 Issuing CA Obligations

Upon accepting the certificates issued by the WISeKey CertifyID Advanced Policy CA, WISeKey hereby warrants that in performing the functions as an Issuing CA will comply with the obligations referred to in section 2.1 above. WISeKey further warrants and represents that:

- Private Cryptographic Key Integrity: the Issuing CA cryptographic private key it uses to operate the Issuing CA and Issuing 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 by WISEKey to be false.
- Changes Notification: immediately notify WISEKey or the third party operator that issued its certificate of any changes to the information material to the certificates issued to it and that it shall maintain all other information maintained by WISEKey or any third party operator 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 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 (e.g. third party hosting of an Issuing CA or registration authority services) are legally bound to comply with the corresponding this CPS or, in the case of third party operators, their CPS.

WISEKey further warrants and represents that the Issuing CA cryptographic private key it uses to operate the WISEKey Advanced Services Issuing CA and provide certification services has not been compromised and that the information contained in the certificates it issues is not known to be false.

As operator of the Issuing CA, WISEKey assumes no other warranties or obligations in the purview of such activities as described in this CPS.

2.1.2 End User Obligations

The Advanced Services Issuing CA ensures 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 are 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.

2.1.3 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 certificates may include a brief statement describing limitations of liability, limitations in the value of transactions to be accomplished, validation period, and intended purpose of the certificate and disclaimers of warranty that may apply. End Users must agree to WISeKey Terms & Conditions before signing-up for a certificate.

2.3 Financial responsibility

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 arising with regard to a certificate issued by the Issuing CA (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 maximum per certificate liability of WISeKey or any other entity within the OISTE WISeKey Root PKI shall be Ten Thousand Swiss Francs (CHF 10,000). 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 for the whole of the validity period of a certificate issued by the Issuing CA (unless revoked or suspended prior to its expiry) towards all persons with regard to such certificate is One Million Swiss Francs (CHF 1,000,000.-)..

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

2.3.1 No Fiduciary relationships

WISeKey is not an agent, fiduciary, trustee, or other representative of Subordinate CAs, Subordinate Registration Authorities, End Users or Relying Parties.

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 law.

2.4.1.1 Applicable contract structure

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

- Root CA-Issuing CA Agreement: This is the contractual arrangement through which the relation between WISeKey and WISeKey is regulated.

- Issuing CA – 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.
- End User Agreement: This contract establishes a contractual relationship between an Issuing CA and its certificate subscribers. As described in section 2.1.2, the terms of this agreement may be incorporated into other documents such as internal employee policy documents or goods or services purchase terms and conditions. This will state the end users' obligations when acting as a certificate subscriber and is required to be consented to as part of the certificate issuance process (whatever the form such process may take).
- Relying Party Agreement: This contract establishes a relationship between WISeKey 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 (with electronic receipt of delivery) 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
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 – Issuing CA agreement, this CPS shall prevail;
- An Issuing CA – RA Agreement, 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 International Court of Arbitration of the International Chamber of Commerce (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 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 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 Issuing CA.

2.5 Publication and Repositories

In order to ensure the full availability of this CPS and other essential public documents, WISEKey maintains a repository at the following location:

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

2.5.1 Dissemination of information on the Certification Services

The dissemination of WISEKey information relevant to the certification services operated by it is done through the above referenced domain name. Unauthorized dissemination is not recognized by WISEKey as its own and is therefore not binding upon it.

2.5.2 Frequency of publication

Newly approved versions of this CPS 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 WISEKey PKI, 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. The CRLs of the Issuing CA shall be public and free of charge.

2.6 Compliance Audit

2.6.1 Issuing CA Compliance Audits

The Advances Services Issuing CA is audited annually by WISEKey internal audit or an independent third party authorised by OISTE/WISEKey with specialist knowledge in the auditing of Certification services and Public Key Infrastructures.

Where non-compliance is found, the necessary corrections will be made to restore compliance. Where substantial non-compliance is found or where a false declaration of

compliance is discovered, the measures may involve the immediate suspension or revocation of the Issuing CA certificate and, as a result, the loss of the right to operate within the OISTE WISeKey PKI or the imposition of restrictions on their operations, depending on the circumstances of each case. Where such non-compliance is substantial and is detected during the certification authority's certificate renewal process, the certificate will be refused and may or may not be renewed regardless of whether compliance can be met.

A special auditing regime may be established for each Certification Authority to allow for their progressive commencement of operations and provision of certification services.

2.6.2 Topics covered by audit

The topics covered by a compliance audit include:

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

2.6.3 Communication of results

Audit results are considered to be sensitive information. Unless otherwise stipulated by contract, they will be protected as confidential information in accordance with § 2.7.1 of this CPS.

Copies of the audit logs and reports will be made available to WISeKey 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 Switzerland 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.

The details of how WISeKey collects, processes and stores personal data is contained in the WISeKey Privacy Policy available at the 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 by the Advanced Services Issuing CA might be publicly disclosed.

2.7.3 Issuing CA Documentation

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

1. This CPS
2. The WISeKey Privacy Policy
3. Relying Party Agreement
4. Other documents approved by WISeKey

2.7.4 Disclosure of Certificate Revocation/Suspension information

The reason(s) for the suspension or revocation of a Certificate may be disseminated, in accordance with applicable law or in the sole and absolute discretion of WISeKey.

2.7.4.1 Disclosure of Certificate suspension information

The reasons for certification suspension may be 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:

- o A properly constituted warrant or request is produced,
- o the law enforcement official is properly identified, and
- o 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:

- o A properly constituted request (i.e. that has complied with all legal procedures) for the production of the information is produced; and

- o 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 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 WISeKey identification numbers vest with WISeKey unless otherwise specified in a 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 Advanced Services issuing CA will only issue digital certificates for End Entities, users and servers.

3.1.1 Certificate Issuance Process

Certificate issuance to End Users entails verifying and validating Identity data such as name, date of birth, nationality, etc. With regard to legal entities, they are required to provide relevant incorporation and legal representative documentation. Verification of devices or other type of entity or object is done with substantially equivalent data. The verification procedure requires face to face or direct verification procedures and can also be done through databases of identity data that are well-maintained and were created based on face to face or direct verification.

The identity verification procedure of an end user who is a legal person or who represents a legal person extends to both the individual authorized to represent the legal person and to the legal person itself.

The individuals representing a legal person applying for a certificate are subject to the aforementioned verification levels in addition to the requirement to provide sufficient proof of the person's authority within the legal entity that is applying for a certificate to apply for and use the e-ID (e.g. share-holders meeting resolutions, board-meeting minutes, authorization to apply for a certificate, and/or official letter or publication by a public entity).

When issuing server certificates, additional verification will be performed links to FQDN (fully qualified domain name) ownership or right to use.

3.1.1.1 Corporate Email Certificate

Corporate versions of Secure Email Certificates are only available through the CertifyID MPKI manager and will only be issued to email addresses within approved domain names. The CertifyID MPKI manager account holder must first submit a domain name to WISEKey and appropriate domain name ownership, or right to use a domain name, validation takes place in accordance with this CPS.

Upon successful validation of a submitted domain name WISEKey allows the CertifyID MPKI manager account holder to utilize email addresses within the domain name.

The CertifyID MPKI manager nominated administrator applies for corporate versions of the Secure Email Certificate. The administrator will submit the secure email certificate end-entity information on behalf of the end-entity. An email is then delivered to the end-entity containing unique login details to online certificate generation and collection facilities hosted by WISEKey.

Once logged into the online certificate generation and collection facilities, the end-entity's browser creates a public and private key pair. The public key is submitted to WISEKey

who will issue a corporate version Secure Email Certificate containing the public key. WISeKey then validate using an automated cryptographic challenge that the applicant holds the private key associated with the public key submitted during this automated application process. If the automated challenge is successful, WISeKey will release the digital certificate to the end-entity subscriber.

3.1.2 Operational periods

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

3.2 Certificate Acceptance

Certificate acceptance shall take place as part of or as a result of the End User certificate issuance procedure.

3.3 Certificate Suspension and Revocation

Suspension of certificates issued by WISeKey Advanced Services Issuing CA may precede revocation and where so it shall be done in accordance with the specific procedures described in this section.

3.3.1 Circumstances for Suspension

The suspension or revocation of certificates issued by the WISeKey Advanced Services Issuing CA shall occur at the discretion of WISeKey and may include the circumstances in which there are indications or suspicion that:

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

3.3.2 Who can request a Suspension or Revocation?

Suspension or revocation may be requested by a representative of WISeKey explicitly given authority to perform suspension or revocation requests.

Suspension or revocation of certificates may also be requested by the WISeKey PAA.

3.3.3 Limits on suspension period

Certificates issued by the Issuing 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 Issuing CA shall be revoked in all cases through a certificate revocation request issued by the a person authorized by WISeKey PAA or by the WISeKey PAA itself, and only 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;

3.3.5 Procedure for revocation request

In processing a revocation request, the Issuing CA will:

- Revoke the certificate on the Issuing CA, record the reason for the revocation, and maintain relevant documentation.
- Generate immediately a CRL (Certificate Revocation List) from the Issuing CA
- Withdraw the certificate from any certificate directory.
- Issue a notice containing the Certificate details and the date and time of revocation to the certificate subscriber.

3.3.5.1 Issuing CA duties

The Issuing CA 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 WISEKey PAA.

3.3.6 Revocation request grace period

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

3.3.7 Certificate Validity Checking Requirements

All entities relying on the certificates issued by or under 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 Issuing CA such certificate may be validated using the validation services offered by such Issuing Certification Authority (i.e. Certificate Revocation Lists or OCSP Validations).

However WISEKey does not accept any responsibility for the proper reliance checking of certificates, as this is outside of our control.

3.4 Security Audit procedures

WISEKey is required to undertake audits of internal operations. 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 Issuing CA system.

3.4.2 Frequency of processing log

Audit logs take place whenever an operation is performed on the Issuing CA.

3.4.3 Retention period for audit log

Audit logs are retained for a minimum of 10 years.

3.4.4 Audit collection system

The WISeKey audit collection system is a combination of automated and manual processes performed by the Issuing CA operating systems 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.

3.5 *Records Archival*

All RA's records concerning the operation of its certification services are archived and are retained for a minimum period of ten (10) years. The time source for the RA is independently verified periodically and all 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 RA. The archival 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.

Key changeover of the end users certificates is instigated at least thirty (30) days 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 Issuing CA. 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 the Issuing CA*

- The hardware and software for the Issuing CA is maintained on-line in a secured facility with perimeter security and enforced internal access controls. Physical controls are documented in our Security Policy.

4.2 *Procedural Controls*

- No member of staff is allowed to gain physical access or operate any component of the Issuing CA 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 Issuing CA. 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 Issuing CA is subjected to background checks and vetting according to WISeKey internal security policies.
- Personnel involved in the control and operation of the Issuing CA 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 Advanced Services Issuing CA are generated in a hardware security module (HSM) which have gone through the WISeKey certification procedure, and meet at least FIPS 140-2 Level 2 Accredited.
- The CA key pairs are generated within the HSM using the RSA Algorithm.
- The Advanced Services Issuing CA key was generated as recorded in the relevant CA Key Generation Ceremony document. The activities that were performed and the personnel that were involved in the ceremony are available for audit review.

5.1.2 CA Public Key Delivery to Users

- The entire Certificate Chain, including the Root CA and Subordinate CAs is generally distributed to End Users for Certificate path validation purposes.
- The certificate hash (thumbprint) and the Certificate of the WISeKey CA certificates are available on the WISeKey Web site (www.WISeKey.com/repository/). Relying parties must confirm the validity of the Root CA certificate using this thumbprint.

5.1.3 Key Sizes

- The modulus of the WISeKey Advanced Services Issuing CA is 2048 bits in length and uses the RSA algorithm.
- End User Key Pairs are recommended to be at least 1024 bits in length and use the RSA algorithm.
- End User key sizes and algorithms are defined in the applicable Certificate Policy.

5.1.4 Public Key Parameters Checking

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

5.1.5 Parameter Quality Checking

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

5.1.6 Private Key Protection and Cryptographic Module Engineering Controls

- The combination of procedural, physical and logical controls that are used to protect the WISeKey CA described in this CPS.

In addition all subscribers are required to adopt suitable precautions to protect their Private Key, and to avoid its disclosure, modification, loss, or unauthorised use.

5.2 Private Key Protection

5.2.1 Cryptographic Modules Standards and Controls

WISeKey uses hardware security modules that are accredited and certified for use by WISeKey, or modules that are certified FIPS 140-2 Level 2 or higher for all Issuing CAs.

5.2.2 Private Key Multi-Person Control

- The WPAA has implemented security procedures and technical measures so that all sensitive CA cryptographic operations require the presence and active involvement of multiple Trusted Persons. The activation of the CA private signing key is performed using multiparty control.
- If necessary, based on a risk assessment, the activation of the CA private signing key is performed using multi-factor authentication (for example, a combination of smart card and password, biometric and password).

5.2.3 CA Key Backup and Recovery

- The Issuing CA Private Cryptographic Key is only backed up for disaster recovery purposes.
- As part of standard operation procedure encrypted backup copies of CA Private Keys, that require the participation of multiple Trusted Persons before reconstruction in a secure cryptographic device, are kept onsite and offsite for business continuity and disaster recovery.
- All hardware cryptographic modules used for CA Private Key activation, storage and protection must meet the requirements defined in this CPS.
- The CA Private Key is backed up, stored, and recovered by authorised personnel using multiparty control in a physically secured environment. If the CA's private signing key is backed up, backup copies of the CA Private Keys should be subject to the equivalent or greater level of security controls as keys currently in use.
- If the CA Private Key is exported from a secure cryptographic module and moved to secure storage for purposes of offline processing or backup and recovery, then the Private Key is exported in a secure key management scheme including any of the following:
 - a. As ciphertext protected using multiple control,
 - b. As encrypted key fragments using multiple control and split knowledge/ownership
 - c. In another secure cryptographic module such as a key transportation device using multiple control
- End Users may, under their sole and absolute responsibility, backup their Private Keys in the event the key storage device allows it, which shall be explicitly determined in the applicable policy.

-

5.2.4 Private Key Entry into or from a Cryptographic Module

- CA key pair generation always takes place within a hardware cryptographic module. Keys stored outside of a module are always in encrypted form, whether for transport between modules, or backup/disaster recovery purposes, as defined in this CPS.

5.2.5 Private Key Storage on Cryptographic Module

- Recovery and storage of the CA Private Key is conducted in the same secure schema used in the backup process, using multiple controls as defined in this CPS.
- The private key may be cloned to multiple cryptographic module(s) complying with the requirements in this CPS, where additional cryptographic performance is required.

5.2.6 Method of Activating Private Key

- The Issuing CA Private key activation requires multi-party control compliant with specified security parameters.
- Private Key activation data for all Entities in the Infrastructure, including Certificate Subscribers, and CA, is be protected in an affordable and reasonable manner that avoids loss, theft, unauthorised use and disclosure.

5.2.7 Method of deactivating private key

- The PKI Services and CA private keys are used in a secure environment using a Hardware Security Module that manages activation and deactivation in accordance with strict role separation and security procedures.
- End Users control the use and deactivation of private keys and the secure storage devices on which they are stored, and must comply with the applicable Certificate Policy.

5.2.8 Method of Destroying Private Key

- The Issuing 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 Issuing CA will be physically destroyed prior to disposal.
- Destruction of End User private keys shall be in accordance with the relevant certificate policy, provided such measures are sufficiently secure to avoid misuse or compromise.

5.2.9 Usage Periods for the Public and Private Key

- The CA key pair and certificate expires 10 years from the moment of their generation.
- The usage period of the key pair and certificates for End Users will be defined in the applicable Certificate Policy.

5.3 Computer Security Controls

- The Advanced Services CA comply with WISeKey technical documentation stipulating the required computer security technical controls.
- All CA software, data files, and operations are maintained on trustworthy systems that meet a minimum level of security as specified in the WISeKey security policy. Unauthorized access to these servers are prohibited, and unauthorized access attempts are logged. Only trusted persons having valid business reasons are permitted to use these servers.
- Firewalls are employed where necessary to segregate and protect the CA Services Infrastructure network from other network elements, and prevent intrusion attempts.

5.4 Life Cycle Technical Controls

5.4.1 System Development Controls

- The CA software used by the Issuing CA for certificate issuance and lifecycle management has been developed in accordance with the requirements of ITSEC (Information Technology Security Evaluation Criteria). Common Criteria EAL 3 or higher.
- The applications used within the CA Infrastructure are expected to be developed, implemented and maintained in line with appropriate development methodology and change management standards.
- Software developed for the CA Infrastructure is checked to ensure that the appropriate version is being used, and that its integrity is intact, before being deployed on the platform.

5.4.2 Security management controls

WISeKey implements monitoring and configuration control policies for the CA Infrastructure systems where necessary.

5.4.3 Network Security Controls

- In order to prevent unauthorised access and malicious activity, all CA and Certificate management functions are performed over secured networks in accordance with the WISeKey Security Policy. Furthermore, highly sensitive information is protected using encryption channels, and authentication performing using digital signatures where required.
- The Issuing CA is maintained on-line and uses firewalls for connections to un-trusted networks including the Internet. The configuration and access control to these network security devices is strictly controlled and limited to authorised personnel only.

6 Certificate, CRL and OCSP Profiles

6.1 Certificate Policy Overview

Applicant	Certificate Type	Channels Available	Validation Level	Suggested Usage
Individual	Secure Email Certificate for Individual – CertifyID Advanced User	WISeKey web site, WISeKey appointed Registration Authority	Applicant must present a signed application form, and accompanying identity documentation. Ownership of email address must also be confirmed through an email challenge or other method. Email uniqueness among the group of Individual advanced user certificate holders will be checked.	Allows certificate owner to digitally sign email messages, documents, and files. Allows relying parties to verify digital signed emails, documents and files, and to send encrypted email to the certificate subscriber. Also allows secure authentication to web sites.
Individual on behalf of- Company	Secure Email Certificate - Corporate	WISeKey web site, WISeKey appointed Registration Authority	<p>Applicant must present a signed application form, and accompanying documentation indicating their position in the company . The right to use the business name must be proven through documentation or third party databases. Ownership of email address must be confirmed through an email challenge, or other method.</p> <p>In addition, when delivered via an MPKI account, the corporate must prove right to use the domain names that will be restricted to its use. These domain names will be checked to be distinguished within the MPKI account application.</p>	Allows certificate owner to digitally sign email messages, documents, and files proving corporate authorship. Allows relying parties to verify digital signed emails, documents and files, and to send encrypted email to the certificate subscriber. Also allows secure authentication to web sites.
Individual or Company	Server Certificate – SSL Certificate	WISeKey Web Site WISeKey appointed Registration Authority	The application must provide documentation proving their right to use the domain name. The right to use the business name must be proven via documentation or third party databases.	<p>Secure web, mail and other servers by allowing the establishment of an SSL/TLS session between the server in which the Server Certificate is installed and the requesting client.</p> <p>The certificate allows the authentication of the server to the client, and establishment of a secure TLS/SSL session.</p>

6.2 Certificate Profile

The WISEKey PAA may establish several Certificate Profiles to accommodate the different types of Certificates issued by the WISEKey PKI. In all cases, such Certificates are compliant with the WISEKey Certificate Services technical specifications and should be documented in an internal Certificate Profile framework.

Issuing CA shall issue certificates having the profile and contain the fields specified in the related policy framework document. The Certificates shall conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and, where not superseded by the preceding standards (b) Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.

The end entity Certificates issued by the issuing CA shall contain the following fields:

- o Version—Set to v3
- o Key usage
- o Serial number—Unique values for each Certificate in the CA domain i.e. unique values for the issuer DN
- o Signature algorithm identifier
- o Object identifier of the algorithm used by the CA to sign the Certificate
- o Issuer DN — Certificate issuer's distinguished name, identification of the Certificate issuer
- o Valid From — Greenwich Mean Time (Zulu) time base. Synchronised to a trusted time source.
- o Valid To — Greenwich Mean Time (Zulu) time base. Synchronised to a trusted time source.
- o Subject DN — Certificate subject's distinguished name
- o Subject Public Key —A single Public Key algorithm (RSA) is supported for the subject Public Key. Public key information: algorithm identifier (that is, RSA with SHA-1) and Public Key encoded in accordance with the WISEKey Certificate Standards.

6.2.1 Version Numbers

All Certificates shall be X.509 Version 3 Certificates. The WISEKey Certificate Services Infrastructure shall issue Version 3 CA Certificates and X.509 Version 3 Certificate Subscriber Certificates.

6.2.2 Certificate Extensions

The WISEKey Certificate Services Infrastructure shall populate X.509 Version 3 Certificates with the extensions required by the internal Certificate Policy framework.

6.2.3 Key usage

The criticality field of this extension is generally set to FALSE.

End entity certificates key usages should follow the key usage extensions stipulated in the WISEKey internal Certificate Profile framework.

WISEKey certificates use the key usage extension fields to specify the purposes for which

the key can be used, and to technically limit how the keys can be used when using compliant software. However the reliance on these extensions to limit key usage is entirely outside the control of WISeKey.

6.2.4 Certificate Policy Extensions

WISeKey Certificate Services Infrastructure Certificates may use the Certificate Policies extension.

If the Certificate Policies extension is populated, then it should contain the applicable object identifier for the WISeKey CP in accordance with the internal Certificate Profile framework.

The Certificate Policies extension may also contain the applicable object identifier for the WISeKey Certificate Services Certificate Policy to which this certificate is mapped.

Policy qualifiers are generally absent.

This extension's criticality field is set to FALSE.

6.2.5 Subject Alternative Names

The subject alternative name may be present in Certificates in the WISeKey Certificate Services PKI. This field should generally be encoded as an RFC822 string. This extension's criticality field is set to FALSE.

6.2.6 Issuer Alternative Name

The issuer alternative name may be present in Certificates in the WISeKey Certificate Services PKI and if so then it should be a copy of the subject alternative name from the issuer's Certificate. This field should generally be encoded as an RFC822 string.

This extension's criticality field is set to FALSE.

6.2.7 Basic Constraints

In general, End Entity, or Certificate Subscriber Certificates should not contain the BasicConstraints extension. If they do contain the Basic Constraints extension then the value of cA should be set to FALSE.

Advanced Issuing CA Certificates has a "pathLenConstraint" field value of "0" indicating that only end entity certificates may follow this Certificate in the certification path.

WISeKey cannot guarantee that the basic constraints extension will be respected, as it is totally dependent on use of compliant software.

6.2.8 Extended Key Usage

The Certificates in the WISeKey Certificate Services Infrastructure may use extended key usage fields as specified in the internal Certificate Policy framework.

End entity certificates can only be issued with a subset of the Extended Key Usage Constraints that are present in the Issuing CA certificate.

6.2.9 CRL Distribution Points

The WISeKey Certificate Service Infrastructure certificates include the cRLDistributionPoints extension.

6.2.10 Authority Key Identifier

WISeKey Certificate Services Infrastructure Certificates are generally populated with the Authority Key Identifier extension of X.509 Version 3 and all Root CA, Policy CA, Issuing CA and End Entity Certificates should contain this extension. When present in a Certificate, the Authority Key Identifier extension should contain the 160-bit SHA-1 hash of the Public Key of the CA issuing the Certificate.

The extension's critical field is generally set to FALSE.

6.2.11 Subject Key Identifier

The keyIdentifier is calculated based on the Public Key of the Subject of the Certificate whenever the a Certificate is populated with the subjectKeyIdentifier extension.

The extension's critical field is generally set to FALSE.

6.2.12 Algorithm Object Identifiers

Certificates are signed with sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) or md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) in accordance with the governing CPS and Certificate Policy framework.

6.2.13 Name Forms

The WISeKey Certificate Services Infrastructure respects the name forms outlined in the IETF PKIX X.509 V3 Standard. In particular:

- o For Root CA, Policy CA, and all other CA Certificates the Subject Distinguished Name should always be present.
- o For Root CA, Policy CA, and Issuing CA Certificates, the Subject Distinguished Name must contain at least the CN attribute, other attributes are optional. The Organisation attribute should be present and should clearly and uniquely identify the CA operator.

6.2.14 Certificate Policy Object Identifier

The Certificate Policies extension MAY be used, and Certificates can possess the object identifier of the Certificate Policy corresponding to the Certificate Type as specified in the governing CPS and within the Certificate Policy Framework.

Where this extension is used, this extension's criticality field is set to FALSE.

6.2.15 Usage of Policy Constraints Extension

Policy constraints are generally not used and their use is discouraged.

6.2.16 Processing Semantics for the Critical Certificate Policies extension

Not used.

Authority Key Identifier	Extension marked non-critical.
Key Identifier	KeyID=6a ae 5e a8 be 9e 5a 59 a5 ab 59 c4 2a 2e 53 f1 2f 30 97 2a
Subject Key Identifier	Extension marked non-critical
Key Identifier	The Subject Key Identifier of the Subject of this certificate.
SMIME Capabilities	<p>[1]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80</p> <p>[2]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 00 80</p> <p>[3]SMIME Capability Object ID=1.3.14.3.2.7</p> <p>[4]SMIME Capability Object ID=1.2.840.113549.3.7</p>
CRL Distribution Point	Extension marked non-critical.
Fullname	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://public.wisekey.com/crl/wcidasca1.crl</p>
Authority Information Access	Extension marked non-critical.
	<p>[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://public.wisekey.com/crt/wcidasca1.crt</p>
Key Usage	Extension marked critical.
	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
Enhanced Key Usage	<p>Document Signing (1.3.6.1.4.1.311.10.3.12) Smart Card Logon (1.3.6.1.4.1.311.20.2.2) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)</p>

--	--

6.3.2 Secure Email -CertifyID Advanced Corporate User

Version	2 (i.e. X.509 version 3)	
Serial Number	Unique serial numbers are assigned by the CA	
Signature Algorithm	Sha1RSA	f
Issuer Distinguished Name		
Common Name (CN)	WISeKey CertifyID Advanced Services CA 1	f
Organisational Unit (OU)	International	f
Organisational Unit (OU)	Copyright (c) 2006 WISeKey SA	
Organisation (O)	WISeKey	f
Country (C)	CH	f
Validity		
Not Before	Time of issue	
Not After	1 – 3 years	f
Subject		
Email (E)	<Subscriber email>	o/e
Common Name (CN)	<Subscriber common name>	m/e
Locality (L)	<Subscriber locality>	o/e
State or Province Name (ST)	<Subscriber state>	o/e
Organisational Unit (OU)	Copyright (c) 2006 WISeKey SA	o/e
Organisational Unit (OU)	CertifyID Advanced User	m/f
Organisational Unit (OU)	Validated by [Appointed RA] – CertifyID RA Issued via [Client MPKI subscriber name]	o/f
Organisational Unit (OU)	<Subscriber organisational unit>	
Organisation (O)	<Subscriber organisation name - reserved>	m/e
Country (C)	<Subscriber country code>	m/e
Subject Public Key Info	1024 bit RSA	f

X.509 Extensions

Authority Key Identifier	Extension marked non-critical.
Key Identifier	KeyID=6a ae 5e a8 be 9e 5a 59 a5 ab 59 c4 2a 2e 53 f1 2f 30 97 2a
Subject Key Identifier	Extension marked non-critical
Key Identifier	The Subject Key Identifier of the Subject of this certificate.
SMIME Capabilities	<p>[1]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80</p> <p>[2]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 00 80</p> <p>[3]SMIME Capability Object ID=1.3.14.3.2.7</p> <p>[4]SMIME Capability Object ID=1.2.840.113549.3.7</p>
CRL Distribution Point	Extension marked non-critical.
Fullname	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://public.wisekey.com/crl/wcidasca1.crl</p>
Authority Information Access	Extension marked non-critical.
	<p>[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://public.wisekey.com/crt/wcidasca1.crt</p>
Key Usage	Extension marked critical.
	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
Allowed Enhanced Key Usages	<p>Document Signing (1.3.6.1.4.1.311.10.3.12) Smart Card Logon (1.3.6.1.4.1.311.20.2.2) Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)</p>

--	--

6.3.3 Secure Server Certificate -CertifyID Advanced Server

Version	2 (i.e. X.509 version 3)	
Serial Number	Unique serial numbers are assigned by the CA	
Signature Algorithm	Sha1RSA	f
Issuer Distinguished Name		
Common Name (CN)	WISeKey CertifyID Advanced Services CA 1	f
Organisational Unit (OU)	International	f
Organisational Unit (OU)	Copyright (c) 2006 WISeKey SA	
Organisation (O)	WISeKey	f
Country (C)	CH	f
Validity		
Not Before	Time of issue	
Not After	1 – 3 years	f
Subject		
Common Name (CN)	<Subscriber common name>	m/e
Organisational Unit (OU)	Copyright (c) 2006 WISeKey SA	m/f
Organisational Unit (OU)	CertifyID Advanced Server	m/f
Organisational Unit (OU)	Validated by [Appointed RA] – CertifyID RA Issued via [Client MPKI subscriber name]	m/e
Organisation (O)	<Subscriber organisational affiliation>	m/e
Locality (L)	<Subscriber locality>	o/e
State or Province Name (ST)	<Subscriber state>	o/e
Country (C)	<Subscriber country code>	m/e
Subject Public Key Info	1024 bit RSA	f

X.509 Extensions

Authority Key Identifier	Extension marked non-critical.
Key Identifier	KeyID=6a ae 5e a8 be 9e 5a 59 a5 ab 59 c4 2a 2e 53 f1 2f 30 97 2a
Subject Key Identifier	Extension marked non-critical

Key Identifier	The Subject Key Identifier of the Subject of this certificate.
SMIME Capabilities	<p>[1]SMIME Capability Object ID=1.2.840.113549.3.2 Parameters=02 02 00 80</p> <p>[2]SMIME Capability Object ID=1.2.840.113549.3.4 Parameters=02 02 00 80</p> <p>[3]SMIME Capability Object ID=1.3.14.3.2.7</p> <p>[4]SMIME Capability Object ID=1.2.840.113549.3.7</p>
CRL Distribution Point	Extension marked non-critical.
Fullname	<p>[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://public.wisekey.com/crl/wcidasca1.crl</p>
Authority Information Access	Extension marked non-critical.
	<p>[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://public.wisekey.com/crt/wcidasca1.crt</p>
Key Usage	Extension marked critical.
	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
Allowed Enhanced Key Usages	Server Authentication (1.3.6.1.5.5.7.3.1)

6.4 CRL Profile

The Root CA has established a CRL profile for CRLs issued by the Root and Subordinate CAs in the network. In all cases, such CRL profiles are compliant with the WISEKey Certificate Services technical specifications and are documented in an internal Certificate Profile framework. The CRL follows the RFC 2459 standard.

WISEKey Certificate Service CRLs generally contain the following fields:

- o Version — v2
- o CRLNumber – this extension field must be present in the CRL. The number is a monotonically increasing integer value that uniquely identifies an instance of the CRL.
- o AuthorityKeyIdentifier — this extension field must be present in the CRL. When the Certificate issuer contains the Subject Key Identifier extension, the Authority Key Identifier matches Subject Key Identifier of the CA issuing the Certificate.
- o Signature Algorithm — Identifies algorithm used to sign CRL. Allowed signature algorithms are sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) or md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) in accordance with the WISEKey Certificate Services Technical Standards.
- o Issuer — directoryName of issuer Entity who has signed and issued the CRL. The CRL Issuer Name is in accordance with the Issuer Distinguished Name requirements specified in the CPS and Certificate Policy framework.
- o This update — Date and Time of CRL issue. Encoded as G Greenwich Mean Time (Zulu) time. WISEKey Certificate Service Infrastructure CRLs are effective upon issue.
- o Revoked Certificates — Listing of revoked Certificates, including the Serial Number of the revoked. CRL Entry extensions are permitted in compliance with Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.
- o Next update— Date by which the next CRL will be issued. This field is generally not included, however it may be included. If included the frequency of CRL issuance will be governed by the Certificate Policy.

The profile of the CA CRL is as follows:

Version	<i>1 (i.e. X.509 version 2 CRL)</i>
Serial Number	<i>Unique serial numbers are assigned by the CA</i>
Signature Algorithm	SHA1RSA
Issuer Distinguished Name	
Common Name (CN)	WISEKey CertifyID Advanced Services CA 1
Organisational Unit (OU)	International
Organisational Unit (OU)	Copyright (c) 2006 WISEKey SA
Organisation (O)	WISEKey
Country (C)	CH

This update	Date/Time of issue
Next update	1 day after time of issue
Revoked certificates	
Serial number	<Subscriber certificate serial number>
Revocation date	<Time/date certificate marked revoked>
CRL reason code	<In accordance with RFC3280>
CRL number	Unique number for each CRL issued by CA Extension marked non-critical.
Authority Key Identifier	Extension marked non-critical.
Key Identifier	KeyID=6a ae 5e a8 be 9e 5a 59 a5 ab 59 c4 2a 2e 53 f1 2f 30 97 2a

6.5 OCSP Profile

The WISeKey Services Infrastructure supports the use online Certificate status and revocation checking services based on the RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

7 Specification Administration

The WISEKey Policy Approval Authority is responsible for setting certification practices and certificate policy direction overall for the Issuing CA.

7.1 Specification change procedures

7.1.1 Initial publication

The WISEKey Root CPS shall be published at the WISEKey Web site at <http://www.wisekey.com/repository/>.

The Issuing CA CPS shall be disseminated to WISEKey web site <http://www.wisekey.com/repository/>.

7.1.2 Changes

7.1.2.1 Authority to Amend

WISEKey, through its PAA, shall have the right to amend this CPS.

WISEKey shall also be entitled to require WISEKey to comply with the guidelines it issues in order to ensure compliance with the OISTE WISEKey Root PKI CPS.

7.1.2.2 Nature of Amendments and Effective Date

Amendments to the Issuing CA CPS shall not be retroactive, shall override any previous versions of this CPS and conflicting provisions of the amended CPS. The amendments made to this CPS may be of three types:

- o Substantial Amendments: these are the amendments which, in the judgment of WISEKey and WISEKey, are of such significance that they require being subject to a consultation by WISEKey prior to their becoming effective.
- o Immediately Effective Substantial Amendments: these are amendments which, in the judgment of WISEKey and 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 Issuing CA or the OISTE WISEKey Root PKI.
- o Insubstantial Amendments: these are amendments that are, in the judgment of WISEKey and WISEKey, of little significance and are therefore not subject to any consultation. Unless otherwise explicitly provided for, these amendments shall have effect upon publication.

7.2 Publication and Notification Policies

All amendments undertaken in accordance with the foregoing sections shall be published 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.

7.3 CPS approval procedures

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

8 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.