DICT - GOVERNMENT OF SEYCHELLES
STANDARD ISSUING CERTIFICATION AUTHORITY
CERTIFICATION PRACTICE STATEMENT
Version 2.0
Effective Date: 20th July 2011

1. INTRODUCTION

Definitions used within this document are contained in the Glossary located in the Appendix.
This CPS covers the practices applied to the Issuing CA of DICT - GOVERNMENT OF SEYCHELLES, hereafter referred to as the **ISSUING CA OPERATOR**. The practices described in this document are applied by the **ISSUING CA OPERATOR** to its own operations.

DICT - GOVERNMENT OF SEYCHELLES
PO BOX 737
SEYCHELLES
DNO@ICT.GOV.SC

The DICT is the Department of Information Communications and Technology in the Ministry of National Development, Government of Seychelles.

The Issuing CA is operated by the **ISSUING CA OPERATOR**, and is a subordinate Issuing CA within 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**
In order to ensure the full availability of this CPS and other essential public documents, the **ISSUING CA OPERATOR** maintains a repository at the following location: **http://www.egov.sc/pki/repository**.

1.1. OISTE WISeKey Root CA

The OISTE WISeKey Root CA self-signs its own Root Certificate which has been endorsed by the OISTE Foundation. **WISeKey SA** is the operator of the OISTE WISeKey Root CA.

1.2. Policy Certification Authorities (PCAs)

Policy CAs are certification authorities whose certificates are signed by the OISTE WISeKey Root CA and issue certificates to Issuing Certification Authorities under a specific policy.

1.3. Issuing Certification Authorities (Issuing CA)

STANDARD ISSUING CAs are certification authorities whose certificates are signed and issued by the WISeKey Standard Policy CA and issue certificates for end-entities only.

1.4. Seychelles Government Standard G1 CA3 Certification Authority

This certification authority's certificate has been signed by the WISekey Standard Policy CA and the **ISSUING CA OPERATOR** operates this Issuing CA, in accordance with the OISTE WISeKey Root CA and Subordinate CA CPS.

1.5. ISSUING CA OPERATOR Policy Approval Authority

The **ISSUING CA OPERATOR** PAA has been established to review and/or approve the practices, policies and procedures for the Issuing CA it operates by undertaking, subject to compliance with the OISTE WISeKey Root CPS.
The **ISSUING CA OPERATOR** PAA may be contacted at:

DICT - GOVERNMENT OF SEYCHELLES
Policy Approval Authority
PO BOX 737
SEYCHELLES
DNO@ICT.GOV.SC

1.6. End Users

End Users or certificate subscribers are issued certificates generated by an Issuing Certification Authority and the End User's certificate application is processed by an Issuing CA or an 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 (e.g., organizational security policies) that incorporate the content of an End User Agreement.

1.7. Relying Parties

Relying parties are individuals or legal entities that rely on a digital signature, certificate, certificate revocation list or information upon which reliance can be placed in accordance with this CPS. The **ISSUING CA OPERATOR** 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.
Relying parties should refer to an accept the CertifyID Relying Party Agreement, a copy of which can be obtained from the WISeKey repository: **http://www.wisekey.com/repository**.

2. GENERAL PROVISIONS

2.1. Obligations

The **ISSUING CA OPERATOR** as operator of the Issuing CA under this Certification Practice Statement undertakes compliance with a series of requirements outlined in this CPS, which cover the following topics and, where applicable, are detailed in the sections referenced under each topic:

- Establish & maintain the Policy Approval Authorities
- Compliance with Local Law and Agreements
- Publish the CPS and other relevant public information
- Perform and have performed compliance audits
- Handle confidential information, personal data, and information disclosure
- Intellectual Property Rights: Acknowledge and comply with the intellectual property rights provisions
- Perform the certificate application processes, certificate issuance and lifecycle management
- Maintain and operate the event logging and audit systems
- Maintain and archive records
- Follow the dispute resolution mechanisms provided by this CPS
- Have in place a disaster recovery plan
- Comply with the security controls & concerning the technical systems described

2.1.1. Issuing CA Obligations

Upon accepting the certificates issued by the WISeKey CertifyID Standard Policy CA, the **ISSUING CA OPERATOR** hereby warrants that in performing the functions as an Issuing CA it will comply with the obligations referred to in section 2.1 above. The **ISSUING CA OPERATOR** 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 **ISSUING CA OPERATOR** 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.

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

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

2.2. Financial responsibility

the **ISSUING CA OPERATOR**'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 the **ISSUING CA OPERATOR** or any other entity within the OISTE WISeKey Root PKI shall be SLR 1.00 (ONE SEYCHELLES RUPEE). 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, the ISSUING CA OPERATOR'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) with regard to such certificate is SLR 1.00 (ONE SEYCHELLES RUPEE), with a maximum aggregate per year liability on all certificates of SLR 1,000.00 (ONE THOUSAND SEYCHELLES RUPEES.

In no event shall the **ISSUING CA OPERATOR**'s liability exceed the aforementioned limits.

2.3. Interpretation and Enforcement

2.3.1. Governing Law

The **ISSUING CA OPERATOR** operates out of REPUBLIC OF SEYCHELLES and its certification services are governed and construed in accordance with REPUBLIC OF SEYCHELLES laws.

2.3.2. Severability, Survival, Merger, Notice

2.3.2.1. 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.

2.3.2.2. 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.

2.3.2.3. Merger

The provisions of this as well as any rights and obligations corresponding to the **ISSUING CA OPERATOR**, 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.

2.3.2.4. Notice

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

DICT - GOVERNMENT OF SEYCHELLES
P.O. BOX 737
SEYCHELLES
Email: DNO@ICT.GOV.SC

2.3.2.5. Assignment

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

2.3.3. Dissemination of information on the Certification Services

Repository location: http://www.egov.sc/pki/repository

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

2.3.4. 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.

2.4. Compliance Audit

2.4.1. Issuing CA Compliance Audits

The Issuing CA is audited by OISTE, WISeKey, or an appointed 3rd party designated by WISeKey or OISTE.

2.5. Confidentiality

For confidentiality and privacy commitments and obligations please refer to the CertifyID Privacy Policy located in the WISeKey repository: ***http://www.wisekey.com/repository***, and to the privacy and confidentiality policies published by the **ISSUING CA OPERATOR** in its repository, or otherwise disseminated to its end entities.

2.6. Intellectual Property rights

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

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

3. OPERATIONAL REQUIREMENTS

3.1. Certificate Issuance

The STANDARD ISSUING CA only issues digital certificates for End Users only.

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 representative documentation. Verification of devices or other type of entity or object is done with substantially equivalent data. The verification procedure should 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).

The identity verification of the legal person itself includes reviewing the originals, certified copies or other reliable sources of the following, where applicable:

- the full legal name and postal address of the entity
- the certificate of incorporation of the legal entity or other similarly reliable document;
- the memorandum and articles of association of the legal entity;
- the number of registration (in the trade registry or other similar register) of the legal entity; and
- if a governmental or public entity, an official letter by the superior governmental entity under which the Applicant operates indicating its support and the authority of the Applicant to apply for a certificate.

3.1.2. Key changeover

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

Issuing CAs should instigate key changeover of the end users certificates at least thirty (30) days before the expiration of their certificates.

3.1.3. 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 the **ISSUING CA OPERATOR**'s Issuing CA usually precedes revocation and where such revocation proceeds, it shall be done in accordance with the specific procedures described in this section.

3.3.1. Circumstances for Suspension

The suspension of certificates issued by the **ISSUING CA OPERATOR**'s Issuing CA shall occur at the discretion of the **ISSUING CA OPERATOR** and may include the circumstances in which there are indications or suspicion that:

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

3.3.2. Circumstances for revocation

A certificate issued by the Issuing CA shall be revoked in all cases through a certificate revocation request issued by the **ISSUING CA OPERATOR** PAA or a person authorized by it and in the following cases:

when, after going through suspension procedures, it is determined that revocation is required due to material circumstances being ascertained in the post-suspension investigation that merit certificate revocation.

3.3.3. 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.

3.3.3.1. 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 may be securely destroyed or
- Securely destroy the private key associated with the revoked Certificate in accordance with a procedure approved by the **ISSUING CA OPERATOR** PAA.

3.3.4. 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 an 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 CA (i.e. Certificate Revocation Lists or OCSP Validations).

3.4. Compromise and Disaster Recovery

The **ISSUING CA OPERATOR** 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.

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 **ISSUING CA OPERATOR** staff involved in the operation of the Issuing CA is subjected to background checks and vetting according to **ISSUING CA OPERATOR** 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, Installation & Protection

Key pairs for the Issuing CA are generated in a hardware security module (HSM) which has gone through the WISeKey certification procedure.

The CA Key pair should be a minimum size of 2048 bit RSA and its certificate should utilize SHA-1, SHA-256 or equivalent hash algorithms. The CA Certificate must NOT use MD2, MD4, or MD5 algorithms.

Key delivery to the end user may be provided by the Issuing CA.

The CA can only issue subordinate or end-entity with 2048-bit RSA key modulus or greater, or ECC equivalent.
The CA does NOT issue MD2, MD4 or MD5 certificates.
The CA issues certificates using SHA-1, SHA-256 or equivalent hash algorithms.
The key pairs may be generated by the end user and they may submit a certificate request with the public key using the provided web interface or other approved mechanism.
The Certificate of the Root CA is distributed to End Users for Certificate path validation purposes.
The certificate hash (thumbprint) and the Certificate of the WISeKey Root CA certificate and WISeKey Policy CAs are available on the WISeKey repository (**http://www.wisekey.com/repository**). Relying parties must confirm the validity of their copy of the Root CA and Policy CAs certificate using this thumbprint.
The modulus of the **ISSUING CA OPERATOR**'s Issuing CA is at least 2048 bits in length and uses the RSA algorithm.
The parameters used in the generation of public keys are in accordance with the requirements of FIPS 140-1.
Parameter quality checking is in accordance with FIPS 140-1 level 2.
The Issuing CA Cryptographic Keys may be used for:

- Issuance of certificates to End entity
- Issuance of Certificate Revocation Lists

The key usage purposes of Issuing CAs are limited to their activities as Subordinate PKI Entities and may therefore not be used for any other purposes. Key usage is also defined by the CA level (Standard, Advanced or Qualified).
The End User key usage purposes are defined in the applicable certificate policy.

5.2. Private Key Protection

5.2.1.Standards for Cryptographic Module

The cryptographic module used by the Issuing CA is certified to meet the requirements of FIPS 140-1 level 2.

5.2.2.Private Key (m out of n) Multi-personnel Control

The Issuing CA Cryptographic Key can only be exported from the hardware security module when split into multiple parts and requires the presence and participation of several authorized **ISSUING CA OPERATOR** officers to reconstruct.

5.2.3.Private Key Escrow

ISSUING CA OPERATOR may decide to implement Private Key Escrow at the Issuing CA level. Implementation of such functionality should be properly communicated to end users.
Key Escrow operation requires the presence and participation of several authorized **ISSUING CA OPERATOR** officers and should be properly documented.

5.2.4.Private Key Backup

The Issuing CA Private Cryptographic Key should only backed-up for disaster recovery purposes.
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.

5.2.5.Method of Activating Private Key

The Issuing CA's Private key activation requires entry and validation of a PIN/passphrase compliant with specified security parameters.

5.2.6.Method of deactivating private key

The Issuing CA's private keys must be deactivated when not in use. The private key secure storage device is required to be stored securely when not in use.
End Users control the use and deactivation of private keys and the secure storage devices on which they are stored.

5.2.7.Method of Destroying Private Key

The Issuing CA Private Key in the HSM may be destroyed by returning the HSM to its factory initialized 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 **ISSUING CA OPERATOR** internal policies, provided such measures are sufficiently secure to avoid misuse or compromise.

5.2.8.Usage Periods for the Public and Private Key

The Issuing CA key pair and certificate will expire after a maximum 10 years from the moment of their generation, or as otherwise determined by the OISTE WISeKey PAA.
The usage period of the key pair and certificates for End Users will be defined in the applicable certificate policy.

6. Specification Administration

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

6.1. Specification change procedures

6.1.1. Initial publication

The Issuing CA CPS is disseminated at http://www.egov.sc/pki/repository.
The WISeKey Root CPS is published at the WISeKey Web site at **http://www.wisekey.com/repository/**.

6.1.2. Changes

6.1.2.1. Authority to Amend

ISSUING CA OPERATOR, through its PAA, shall have the right to amend this CPS.
WISeKey shall also be entitled to require the **ISSUING CA OPERATOR** to comply with the guidelines it issues in order to ensure compliance with the OISTE WISeKey Root PKI CPS.

6.1.2.2. 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:

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

7. Appendix – Glossary

Access Control
The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner.
[ISO 7498-2: 1989]

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

Asymmetric Key Pair
A pair of related keys where the private key defines the private transformation and the public key defines the public transformation.
[ISO/IEC 9798-1 (2nd edition): 1997] [2nd DIS ISO/IEC 11770-3 (08/1997)]

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

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

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

Audit Record
The discrete unit of data recorded in the audit trail on the occurrence of a recorded event. An audit record consists of a set of audit descriptions, each of which has a set of audit attributes associated with it. Every audit record always has an audit description for the record' s header, and usually has additional audit descriptions describing the entity(ies) and object(s) involved in the event.
[ISO/IEC POSIX Security]

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

Certificate
It is a data structure, using the CCITT ITU X.509 standard, containing the public key of an entity, together with associated information, and rendered un-forgeable 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.