CERTIFICATION PRACTICE STATEMENT

Document version: 1.2
Date: 15 September 2007

OID for this CPS: None

Information in this document is subject to change without notice.

REVISION HISTORY

Version	Date	Author	Comments
Ver 1.0	29 March 2004	Beth A. MacMonigle, RSA Security Inc.	Final document for Revenue Commissioners approval
Ver 1.1	7 April 2004	Beth A. MacMonigle, RSA Security Inc.	Documented updated for final publication.
Ver 1.2	20 August 2007	Tony Egan	Document updated to take account of certs to be used by DoE and possibly other Gov Depts in the future

Contents

1 Introduction

The information contained in this document is intended for personnel charged with the management and operation of the Office of the Revenue Commissioners Public Key Infrastructure (Revenue PKI) including the Revenue Certification Authority (Revenue CA) and Revenue On-Line Service Certification Authority (ROS CA).

The Revenue PKI must ensure that it maintains the trust of those who have been issued with Certificates.

The Revenue CA creates and signs its own Certificate. It also signs the Certificate created by the ROS CA and acts as the highest point of trust in the Revenue PKI. The ROS CA issues certificates to Approved or Authorized users, in accordance with the relevant certificate policy.

The practices associated with the management of the Revenue PKI are documented in the attached Revenue Certification Practice Statement (CPS).

2 Purpose of this Certification Practice Statement

The purpose of this document is to provide factual information describing the Certification practices employed by the Revenue CA in relation to the following:

1. Management of its Public Key Infrastructure (PKI).

2. Administration of the Revenue PKI under the Certificate Policy Statement (CP) as issued by the Revenue CA.

3. Certificate life cycle within its PKI.

These practices are detailed in the formal statement attached as Appendix A - Certification Practice Statement (CPS).

The Revenue CA is a self-signing Certification Authority.

It should be noted that the Revenue CA and other Certification Authorities may issue multiple Certificate Policy Statements (CP) mapped to this Certification Practice Statement. In each case, the corresponding CP within this CPS will be nominated.

3 Certification Practice Statement (CPS)

The CPS discussed in this introductory statement is attached as Appendix A.

3.1 Function of CPS

The function of this CPS is to provide factual information that identifies and details, as appropriate, the standard operating practices that support Certificates issued by the Revenue CA under Certificate Policy Statements. These Certification practices cover the following:

1. Generation, operational use, compromise, expiry, suspension and revocation of nominated Certificates issued by the Revenue CA and other Revenue Certification Authorities.

2. Security mutual consistency and effectiveness of the Revenue PKI's operations.

3. Maintenance of the logical and physical elements of the Revenue PKI.

4 Availability of Revenue PKI Certificate Policy and Certification Practice Documents

There is a requirement for this and other Revenue PKI policy and practice documents to be available for inspection by interested parties. For information about how to obtain access to these documents see Appendix D.

In the remainder of this document the repository for the Revenue PKI policy and practice documents and the instructions above are referred to as the Revenue PKI Certificate Policy Web Site**.**

5 Amendment Procedure

5.1 Policy Approval Authority (PAA)

As new standards emerge, or policy and practices are identified for improvement, this document shall be amended.

The responsibility for amending and approval of this document rests with the Revenue PKI Policy Approval Authority (PAA).

The PAA is responsible for setting Certificate Policy direction for Revenue's overall Public Key Infrastructure and includes representatives from the Offices of the Revenue Commissioners and other bodies, as defined within the PAA Constitution.

5.2 Change

After changes to this CPS have been approved the Revenue PKI will:

1. Publish at the Revenue PKI Certificate Policy Web Site (see Attachment D), this CPS.

2. Advise Approved or Authorised Persons with Keys and Certificates by email as to the effect of the change and its date of effect. The email address used will be that supplied as part of the initial registration process.

3. Cancel Keys and Certificates where the Approved or Authorised Person indicates that they no longer wish to abide by the new arrangements.

If there is a requirement to amend an existing document, the change process employed is the same as for initial publication, as described above.

The naming convention for amendment notices shall be:

YYYY Indicating the year the amendment was issued

XXX Where XXX represents a sequential number beginning with 000

Appendix A – Revenue PKI Certification Practice Statement

1 Introduction

1.1 Overview

1.1.1 Introduction

This Certification Practice Statement (CPS) is written for use within the Revenue Public Key Infrastructure (PKI). At the highest level the Revenue PKI consists of the Revenue Certification Authority (Revenue CA) and the Revenue On-Line Service Certification Authority (ROS CA). The Revenue CA is the highest point of trust in the Revenue PKI.

The Revenue PKI supports the creation and use of Keys and Certificates by Revenue and its customers. Keys and Certificates are used for the security of transactions carried out between Revenue and its customers by providing the following functions:

1. Authentication.
2. Integrity.
3. Confidentiality.
4. Non-repudiation.
5. Other functions as may be approved by the Revenue PKI from time to time under a particular CP.

This CPS provides factual information that describes the:

1. Practices employed within the Revenue PKI to support the use of Certificates issued by the Revenue Certification Authority.
2. Attendant use of technologies and processes to support the underlying operational infrastructure.

The practices described in this CPS, together with the technologies and processes referred to in other documents, illustrate the trustworthiness and integrity of Revenue PKI's operations from Certificate generation and signing to expiry.

PKI Certificate Services

The Certificates and associated CPs supported under this CPS cover signatory functions and other services required for communication between Revenue and its customers.

Certificate Types Issued

This CPS supports the operation of the following:

1. Certificates and supporting CPs as may be approved by the Revenue PAA.

These include:

- Certificates required for Officers of the Revenue in their communication with Approved or Authorised Persons.

- Other Certificates required for Approved or Authorised Persons in their communication with Government

Certificate Policies supported by this CPS are listed in ***Appendix B - CP Supported under this CPS*** and are published at the Revenue PKI Certificate Policy Web Site. See Appendix D.

Approved Policy Qualifiers

The following Policy Qualifiers have been approved for use in Certificates issued by the Revenue CA and ROS CA for the operation of the Revenue PKI. Other Policy Qualifiers are set out in the relevant CP.

Revenue CA Policy Qualifier

The Revenue CA creates and signs its own certificate and signs the ROS CA certificate. The ROS CA issues certificates to its PKI subordinate elements and to Approved or Authorised Persons who may use them only to communicate with the Office of the Revenue Commissioners.

ROS CA Policy Qualifier

Certificates issued under this CP are qualified certificates under the Electronic Commerce Act 2000 for use by Approved and Authorised Persons only to communicate with the Revenue Commissioners, and other Government Departments where ROS certificates may be used for authentication purposes.

Revisions

This CPS will undergo a regular review process as prescribed by the Revenue PAA.

Revisions of this document are identified through a configuration baseline schema and numbering convention.

1.1.2 Standards

This CPS is referred to as the "Revenue CPS".

The structure of this CPS is based on RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,, for more information see Section ***1.1.2 Standards*** in a relevant CP.

This CPS differs from the RFC 3647 standard only to the degree necessary to adequately describe the operational practices used within the Revenue PKI.

1.1.3 Definitions

This CPS assumes that the reader is familiar with basic PKI concepts, including:

1. The use of digital signatures for authentication, integrity and non-repudiation.
2. The use of encryption for confidentiality.
3. The principles of asymmetric encryption, Keys and Certificates and key pairs.
4. The role of Certification Authorities.

Definitions used within this document are contained in Appendix B - Glossary.

These definitions are based on the following:

1. ISO Glossary of IT Security Technology.

It should be noted that not all terms or acronyms have been used in this document. However the list as presented is consistent across the Revenue PKI documentation suite.

1.1.4 X.500 Object Identifier Hierarchy

Object Identifiers (OID) have been assigned by the Revenue PKI and documented in the Revenue PKI configuration baseline.

OIDs are assigned to the Revenue CA, ROS CA, and each subordinate element of the ROS CA and each CP. An OID is not assigned to this CPS.

All OIDs are to be recorded in:

- An appropriate CP:
  - The Revenue CA's OID is recorded in this CPS
  - A CP OID is recorded in the relevant CP

1.1.5 Certificate Management Life Cycle

The Revenue certificate management life cycle (CMLC) is illustrated in Figure 1.1 below. The CMLC applies to all Certificates issued within the Revenue PKI.

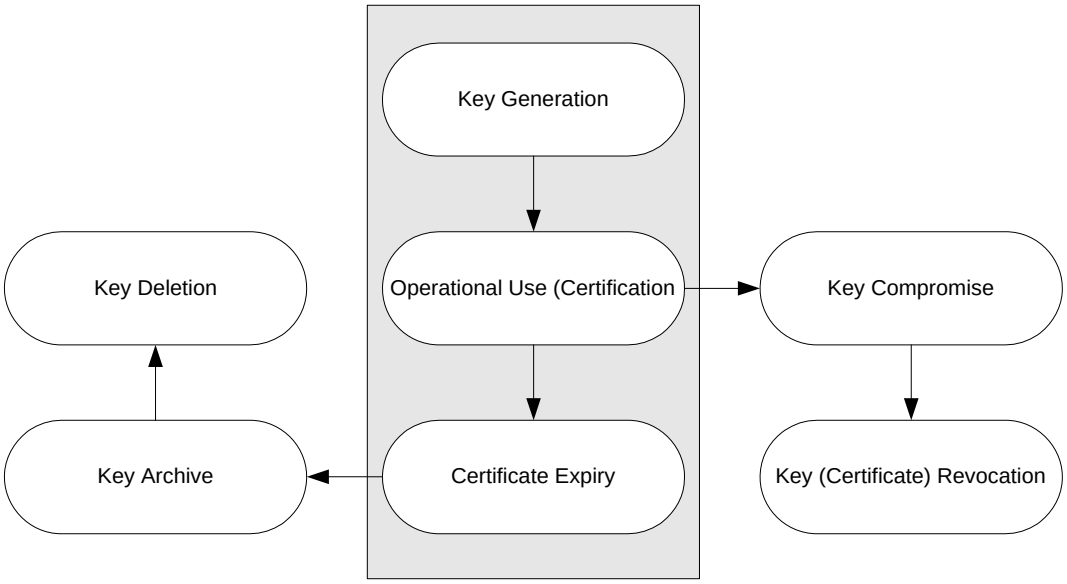

Figure 1. Certificate Management Life Cycle

The CMLC represents the high-level Certificate management process within the Revenue PKI. It consists of primary and secondary Certificate states. The primary states are:

1. Generation.
2. Operational use.
3. Expiry.

All Certificate types issued pass through these three primary states as part of their life cycle.

The secondary states are:

1. Compromise.
2. Revocation.
3. Archive.

Because these secondary states represent exception situations, it is expected that:

1. Most Certificates issued to Approved or Authorised Persons will pass through only the primary states during their life cycle.

2. A small number of Certificates issued to Approved or Authorised Persons may pass through one or more of the secondary states.

The Revenue PKI supports the CMLC Certificate states in the delivery of all of its Keys and Certificates. It should be noted that some Keys and Certificate states may be supported on a procedural basis only.

The CMLC does not support a provisional Certificate state. Certificates are issued after a Certificate application has been submitted and approved, and are deemed to be in operational use in accordance with the relevant CP.

Key Pairs

Key pairs are bound to Certificates and the Keys are rendered useless by the expiry of the Certificate.

Expired key pairs are not re-assigned or otherwise re-used.

1.1.5.1 Generation

The relevant Certification Authority within the Revenue PKI generates Certificates upon receipt of an authorised and validated request for:

1. New Certificates.

2. Certificate renewal.

Generation involves:

1. Receipt of an approved and verified Certificate request from a Revenue customer through the Revenue web site (www.revenue.ie) and associated Revenue registration processes.

2. Generating a certificate request and Key Pair at the Approved or Authorised Person's environment.

3. Creating a new Certificate.

4. Binding the Key Pair associated with the Certificate to an Approved or Authorised person.

5. Issuing the Certificate and the associated Public Key for operational use under both of the following:

    - A Distinguished Name associated with the Approved or Authorised person and the Entity that they represent

    - A relevant CP

Generation of keys for use within the Revenue CA is performed within a hardware security module (HSM) in a physically secure facility, on the receipt of a properly authorised request for a Certificate. This will be put in place under procedures approved

by the relevant Certification Authority within the Revenue PKI and documented in the relevant CP.

Generation of keys for use by Approved or Authorised Persons within the ROS CA will be performed at the Approved or Authorised person's computer, using digitally signed code supplied to the Approved or Authorised person by Revenue. Such code will be subject to independent review, by a trusted third party appointed by the Revenue PAA.

Entity names are unique and comply with the X.500 standard for Distinguished Names.

1.1.5.2 Operational Use

A set of Certificates come into operational use at the time of issue, and remain in operational use until they do one of the following:

1. Expire.

2. Are compromised or revoked.

Certificate Lifetimes

Keys and Certificates have a fixed operational lifetime that is determined by the relevant CP.

1.1.5.3 Expiry

Certificates expire automatically upon reaching the designated expiry date, at which time the Certificate is archived.

Note that:

1. The life of a Certificate can not be and is not extended.

2. Expired Certificates can not be and are not re-issued.

1.1.5.4 Archive

Expired Certificates are archived for a minimum period of ten (10) years from the date of expiry, unless another period is specified in the relevant CP.

1.1.5.5 Compromise

Certificates in operational use that become compromised are revoked in accordance with a defined procedure. Certificates are deemed to be compromised when the integrity of the Private Key associated with the Keys and Certificates is in doubt.

Consistent with the relevant CP, Keys and Certificates suspected to be compromised remain in the compromised state for only such time as it takes to arrange for revocation.

1.1.5.6 Revocation

Certificate revocation permanently invalidates any trusted use of a certificate and the associated private signing key.

Keys and Certificates are revoked when:

1. There is a compromise of the Approved or Authorised Person's Private Key.

2. There is a misrepresentation or errors in a Certificate.

3. The Entity ceases to exist, for example through death, liquidation or by dissolution of a partnership.

4. The Keys and Certificates are no longer required, because the Approved or Authorised person no longer represents the Entity, and so on.

Revoked Certificates are added to the Revenue X.500 Directory Certificate Revocation List (CRL). Note that this directory is subject to the requirements of the Data Protection Act (1998). See the relevant CP for details.

1.1.5.7 Operational Compliance

All Certificate operations comply with:

1. The policy requirements of:

    - The Revenue On-Line Certificate Policy
    - This CPS
    - Published and internal privacy policies and practices including the Data Protection Act (1998)
    - Internal security policies and operational procedures

2. The technology requirements of:

    - Relevant internal guidelines for the physical protection of technology assets
    - X.500 Directory services
    - X.509 Certificate format
    - X.509 CRL format
    - X.500 Distinguished name standards
    - PKCS#7 format for Digital Encryption and Digital Signatures
    - PKCS#10 Certificate Request format

- PKCS#12 Personal Information Exchange format
- Recognised PKI conventions and standards

3. Appropriate international and domestic standards relevant to PKI operations.

1.1.6 PKI Operational Infrastructure

The Revenue PKI operational infrastructure uses approved products from a PKI hosting service provider. These products automate Key and Certificate management functions.

RA Service Domain

The RA service domain consists of the RAs that operate under the Revenue PKI. These RAs are responsible for supplying user registration functions and facilitating key generation requests from entities. Unless otherwise stated in a CP, Revenue performs the RA function for the Revenue PKI.

Note that within the ROS CA environment, the Revenue On-Line Service application itself provides some of the RA functionality, initiating user registration and facilitating the key generation process at the Approved or Authorised Person's computer environment.

User Service Domain

The User service domain includes entities, who use or rely on Certificates for authentication, integrity non-repudiation and confidentiality.

1.1.7 Scope

The practices described in this CPS are binding upon all parties within the Revenue PKI, through the inter-linking contractual responsibilities, obligations and duties between the Revenue PKI and Approved or Authorised Persons.

This CPS incorporates information from other documents regarding practices involved in the issue, use and validation of Certificates, and in the operational maintenance of the PKI infrastructure. The CPS includes, but is not limited to the:

1. Certificate categories that may be created.
2. Establishment of the Revenue CA and ROS CA.
3. Functions and obligations of the Revenue CA and the ROS CA.
4. Registration of Approved or Authorised Persons.
5. Functions and obligations of Approved or Authorised Persons.
6. Process of approving new Certificate categories and Certificate policy.

1.1.8 Security Philosophy

In all cases, the Revenue PKI operates to:

1. Securely generate Keys and Certificates and take appropriate precautions to protect against their compromise, modification, disclosure, loss or unauthorised use.

2. Be able to detect and record unauthorised events and actions.

These procedures extend to the Revenue PKI, which must ensure that only an Approved or Authorised Person is made aware of the Private Keys and any associated Pass-phrase values.

1.1.9 Staffing Arrangements

The Revenue PKI has adopted and employs personnel and management practices to ensure the trustworthiness, integrity and professional conduct of all staff and agents involved in its operation.

The following personnel standards are applied:

1. All Revenue staff are recruited in line with Irish Government recruitment procedures.

2. All Revenue staff and staff engaged by agents have taken an oath of secrecy in accordance with the Official Secrets Act (1963).

3. All Revenue PKI operations staff are provided with appropriate training, including:

    - Basic PKI concepts

    - For pertinent CA staff, how to explain to RA Certificate applicants the responsibilities adhering to the possession, use and operation of their key pairs

    - How to explain to Approved or Authorised Persons the responsibilities adhering to the possession, use and operation of their Keys and Certificates

    - The meaning and effect of the Conditions of Use that applies to the Keys and Certificates

1.1.10 Right of Inquiry

The Revenue PKI reserves the right to make all reasonable inquiries in accordance with its published terms and conditions to determine the validity of a revocation request.

1.2 Identification

This CPS is referred to as the "Revenue CPS".

1.3 Community and Applicability

This CPS supports:

1. All CA and RA services that operate under the Revenue PKI, and are within the Revenue "chain of trust".

2. All types of Certificates issued under the Revenue PKI.

As a consequence, the practices described in this document allow for a wide range and variety of:

1. Certificate types, supporting individual and non-individual transactions that have differing levels of information sensitivity and financial value.

2. End Entities, who include:

   - Individuals
   - Organisations, companies, trusts and partnerships
   - Government departments, agencies or authorities
   - Individuals employed by the above

The practices in this CPS must:

1. Accommodate the diversity of the community and the scope of applicability within the Revenue PKI's chain of trust.

2. Adhere to the primary purpose of the CPS, of ensuring the uniformity and efficiency of practices throughout the PKI.

In keeping with their primary purpose, the practices in this document:

1. Are the minimum requirements necessary to ensure that Approved or Authorised Persons have the highest possible level of assurance, and that critical functions are provided at appropriate levels of trust.

2. Apply to all Revenue PKI stakeholders, for the generation, issue, use and management of all Certificates.

1.3.0 Policy Authorities

1.3.0.1 Revenue Policy Approval Authority (PAA)

The PAA is responsible for the creation of policy unique to the operation of the Revenue PKI. The PAA is responsible for setting, implementing and administering policy decisions throughout the Revenue PKI.

The PAA will include representatives from the Office of the Revenue Commissioners and other parties, as defined within the PAA Constitution.

1.3.0.1.1 PAA Functions

The PAA performs the following functions:

1. Formulate new policy and policy changes.
2. Approve new policy and policy changes, as appropriate.
3. Ensure that this CPS and the CPs are implemented.

1.3.0.1.2 PAA Contact Details

The PAA may be contacted through the Office of the Revenue Commissioners.

1.3.1 Certification Authorities

1.3.1.1 Revenue Certification Authority

The primary purpose of the Revenue CA to sign its own Certificate and operate under the Revenue PKI hierarchy is to provide a trust anchor and certificate management services (generation, operational use, compromise, revocation and expiry) for intermediate certificate authorities operated on behalf the Revenue On-Line Service (ROS) Certificate Authority within their respective policy domains.

1.3.1.1.1 Functions of the Revenue CA

The Revenue CA performs the following functions:

1. Generate its own keys and will issue a self signed Certificate, publishing the Public Key of the Revenue CA with the hash which establishes the Revenue CA as the highest point of trust in the Revenue PKI.
2. Publish each CP under which it issues Certificates, and this CPS within the Revenue PKI Certificate Policy Web Site (see Appendix D).
3. Certify the Public Key of the ROS CA.
4. Operate the Revenue PKI in an efficient and trustworthy manner and in accordance with:
    - The Revenue Concept of Operations
    - The CP that they issue Certificates under
    - This CPS
    - The System Security Policy for the Revenue PKI
    - Documented internal operational procedures

5. Issue Certificates in accordance with the Revenue CA CP.

6. Revoke Certificates it has issued on receipt of authenticated revocation requests, or when they have been compromised.

7. Post revoked Certificates in the directory services CRL.

8. Conduct regular audits and facilitate external audits.

1.3.1.1.2 Revenue CA Contact Details

Revenue On – Line Service

Trident House

Blackrock

County Dublin

Tel: 1890 201106

E-Mail:roshelp@revenue.ie

The contact details for the Revenue CA are published in each CP that they issue Certificates under or the CP may advise a web site address or other location where the contact details may be found.

1.3.1.2 Revenue On-Line Service Certification Authority

1.3.1.2.1 ROS CA Functions

The ROS CA has the following functions:

1. Publish the CP for Keys and Certificate issued by the ROS CA.

2. Issues Certificates to Approved or Authorised Persons in accordance with the relevant CP. Note that for Revenue customers the key generation process will be performed within the customer computer environment itself.

3. Maintains an X.500 Directory for the internal use of the Revenue PKI to which it will post Certificate information. (see section 2.6.3).

4. Monitor compliance with the relevant CP.

1.3.1.2.2 ROS CA Contact Details

Revenue On – Line Service

Trident House

Blackrock

County Dublin

Tel: 1890 201106

E-Mail:roshelp@revenue.ie

1.3.2 Registration Authorities

The Revenue PKI establishes the identity of Approved or Authorised Persons who it has issued Keys and/or Certificates by reference to information and procedures administered by the Office of the Revenue Commissioners. That information may not be provided to any other person in any circumstances.

1.3.3 Entities and Approved and Authorised Persons

The term Entity includes the following:

- Individuals
- Organisations
- Companies
- Trusts
- Partnerships
- Other Revenue customers
- Other person(s) defined within the relevant CP

The term Approved person is defined as an individual person who has been issued with a Certificate in accordance with the provisions within the appropriate Certificate Policy or Policies and who represents an Entity with respect to communications with Revenue through the Revenue On-Line Service.

The term Authorised Person is defined as an individual person who has been issued with a Certificate under the terms of this CPS on application by an Approved Person.

Key pairs will be generated by the Revenue PKI in such a way that only the Approved or Authorised Person will have access to the relevant Private Key.

Approved and Authorised Persons are required to take reasonable security measures to ensure the protection of their Private Keys against compromise.

1.3.3.1 Approved and Authorised Persons Functions

The Approved or Authorised Person's functions are defined in the Revenue's Conditions of Use or other relevant CP.

1.3.3.2 Approved person Contact Details (Approved or Authorised Person)

The following Approved or Authorised Person contact details may be published in a Approved or Authorised Person Public Key Certificate in compliance with X.509 standards:

1. Entity name and Approved or Authorised Person's name in the End Entity's Distinguished Name in the Organization "O" and Common Name "CN" fields.
2. The ROS Access Number (RAN) in the End Entity's Distinguished Name in the Organizational Unit "OU" field.

Approved or Authorised Person contact information is maintained confidentially by the Revenue.

1.3.4 Applicability

Certificates issued by the Revenue PKI are used to support secure exchange of information as required for the purposes of the legislation administered by Revenue. Later Revenue may permit the use of Revenue issued Keys and/or Certificates for broader electronic commerce purposes and the secure exchange of information between Approved and Authorised Persons and Government.

The Revenue PKI user community may regard the practices described in this CPS as:

1. Ensuring standard operating procedures and uniform quality of service delivery across the PKI.

2. Fostering and promoting high levels of trust and integrity across the Revenue PKI.

1.3.4.1 Restricted Certificate Usage

Specific restrictions on the use of Keys and Certificates are contained in the CP under which the Certificates are issued. These restrictions may limit or prescribe the:

1. Community of interest.

2. Conditions which must be satisfied before a Certificate is used.

3. Actual usage of the Certificate.

4. Processing steps or other actions which are to be performed after a Certificate has been used.

Approved and Authorised Persons who receive Certificates from the Revenue PKI are to use those Certificates only in the manner, and for the purposes prescribed in a relevant CP. Any use of a Certificate in a manner or for a purpose not in accordance with a relevant CP is not recognised nor supported by this CPS.

1.4 Contact Details

1.4.1 Specification Administration Organisation

This CPS is administered by the Revenue PKI.

1.4.2 Contact Person

Inquiries or other communications about this document should be addressed to the Revenue CA, see section 1.3.1.1.2.

2 General Provisions

2.1 Obligations

2.1.1 General Obligations

The ROS CA shall provide a secure message infrastructure that enables the operation of Keys and Certificates using Public Key cryptographic methods. The Revenue CA will be the highest point of trust within the Revenue PKI.

Approved or Authorised Persons are:

1. Advised through the CP of their duties and obligations to ensure the safety, protection and integrity of their Private Keys.

2. Required for specific classes of Keys and Certificates to comply with the Conditions of Use.

3. Not to interfere with or damage, or attempt to interfere with or damage, the operational infrastructure of the Revenue PKI. The Revenue PKI has:

    - Been structured and is operated in such a manner as to minimise the risk of compromise or wilful damage by a Approved or Authorised Person

    - Defined a security policy that provides for the early detection of an attempt to damage the infrastructure and to collect sufficient evidence for a prosecution

2.1.2 Revenue PKI Obligations

Changes to this CPS can only be made at the direction of the Revenue PAA. Factors that will normally result in change requests include, but are not limited to:

1. A mandated change to Irish Government requirements.

2. A change in the technology supporting the PKI.

3. A change required for compliance with published International, European and Irish standards.

2.1.2.1 PAA Obligations

The PAA may advise the Revenue PKI of any changes that need to be made to this CPS. The PAA's general obligations in regard to approving CP and maintaining the Revenue PKI policy infrastructure are detailed in a relevant CP.

2.1.2.2 Revenue CA's Obligations

The Revenue CA is a combination of software, hardware, and procedures. RSA Security’s Keon Certification Authority (KCA) software is used to perform certificate issuance and management for the Revenue CA. The processes and procedures for

certificate issuance and management are carried out by the Revenue PKI staff and associated hosting service. The Revenue CA obligations are:

- Issue Certificates to itself
- Receive and verify requests for Certificates in accordance with the relevant CP
- Issue Certificates to the ROS CA
- Comply, and ensure that its employees and contractors comply with the conditions set out the relevant CP and the practices set out in this CPS
- Maintain Certificate information in a designated Revenue X.500 Directory
- Issue and publish a certificate revocation list (CRL), as required
- Receive revocation requests and revoke certificates that are issued by the CA in accordance with the relevant CP; and,
- Issue new Certificates in accordance with the relevant CP.

The Revenue CA discharges its obligations under this CPS by:

1. Providing CA, RA and other PKI services.
2. Making reasonable efforts to ensure it conducts an efficient and trustworthy operation. "Reasonable efforts" includes but does not limit the Revenue CA to operating in compliance with:
    - Documented internal operational procedures
    - This CPS
    - Within applicable law
3. Maintaining this CPS and enforcing the practices described within it.
4. Issuing Certificates that are factually correct from the information known to it at the time of issue, and that are free from data entry errors.

2.1.2.3 ROS CA Operated Under the Revenue CA

The ROS CA is a combination of software, hardware, and procedures. The RSA Security Keon Certification Authority (CA) software is used to provide certificate issuance and management for the ROS CA. The processes and procedures for certificate issuance and management are carried out by the Revenue PKI staff and associated hosting service.

The ROS CA obligations are:

- Receive and verify requests for and certificates in accordance with the relevant CP
- Issue certificates to the ROS CA

- Comply, and ensure that its employees and contractors comply with the conditions set out the relevant CP and the practices set out in this CPS
- Maintain certificate information in a designated Revenue X.500 Directory
- Ensure that its certificate signing private key is used only to sign certificates and CRLs.
- Issue and publish a certificate revocation list (CRL) at least every 24 hours.
- Receive revocation requests and revoke certificates that are issued by the CA in accordance with the relevant CP; and,
- Issue new Certificates in accordance with the relevant CP.

2.1.2.4 RA Obligations

Registration Authorities (RAs) operating under the Revenue PKI shall comply, and ensure that RA operational staff comply with relevant CPs.

RAs operating under the Revenue PKI shall:

- comply, and ensure that the RA operational staff comply with this CPS; and,
- identify Approved and Authorised Persons to the Revenue CAs, using processes specified by the Revenue; and,
- verify the integrity and possession of Approved and Authorised Person's generated keys presented for certification;
- make certification requests on behalf of Approved Persons to the Revenue CAs; and,
- receive issued Approved or Authorised Person certificates from the Revenue CAs;
- may make revocation requests;
- receive revocation requests; and
- generate new keys for, or accept new Approved or Authorised Person generated keys from, Approved and Authorised Persons who suspect their keys or Certificates may have become compromised, or in the event that the keys or Certificates have become compromised, after checking the Approved and Authorised Person's identity.

The Revenue On-Line Service will act as part of the Registration Authority for the ROS CA within the Revenue PKI.

2.1.3 Entity and Approved and Authorised Persons Obligations

Approved and Authorised Persons are required by the relevant CPs to:

1. Provide the Revenue PKI with true and correct information at all times.

2. Provide sufficient proof of material required in order to meet user registration or Certificate renewal requirements.

3. Have their Public Keys and Certificates published in the Revenue X.500 directory.

4. Immediately notify the Revenue PKI of any error or defect in their Certificates, or of any subsequent changes in the Certificate information.

5. Read the applicable CP and this CPS before using their Keys and Certificates.

6. Use their Keys and Certificates only in accordance with a relevant CP.

7. Ensure the safety and integrity of their Private Keys, including:

   - Controlling access to the computer media containing their Private Keys

   - Protecting the access control mechanism used to access their Private Keys (e.g. the use of a Passphrase value)

8. Immediately notify the Revenue PKI of any instance in which a key pair is compromised or in which they have reason to believe a key pair may have become compromised.

9. Exercise due diligence and reasonable judgement before deciding to rely on a digital signature, including whether to check on the status of the relevant Certificate.

2.1.4 Relying Party Obligations

Relying parties have no Certificate Practice obligations under this CPS. Where specific obligations do exist, these will be published within the appropriate CP.

Note that the ROS application is a Relying Party within the ROS CA .

2.1.5 Repository Obligations

The Revenue Repository functions are performed by the Revenue X.500 Directory. This repository is restricted to access by Revenue and its appointed agents.

The Revenue PKI provides and maintains the operational infrastructure for the Revenue X.500 Directory.

2.2 Liability

The Revenue CA has introduced a number of measures to reduce or limit their liabilities in the event that the safeguards in place to protect its resources fail to:

1. Inhibit misuse of those resources by authorised personnel.

2. Prohibit access to those resources by unauthorised individuals.

These measures include but are not limited to:

1. Identifying contingency events and appropriate recovery actions in a Business Continuity Plan.

2. Performing regular system data backups.

3. Performing a backup of the current operating software and certain software configuration files.

4. Storing all backups in secure local and offsite storage.

5. Maintaining secure offsite storage of other material needed for disaster recovery.

6. Periodically testing local and offsite backups to ensure that the information is retrievable in the event of a failure.

7. Periodically reviewing its Business Continuity Plan, including the identification, analysis, evaluation and prioritisation of risks.

8. Periodically testing uninterrupted power supplies.

Specific matters relating to liability are set out in the CPs.

2.2.1 Entity Liability

Please refer to the relevant CP.

2.3 Financial Responsibility

Please refer to the relevant CP.

2.3.1 Indemnification by Relying Parties

Please refer to the relevant CP.

2.3.2 Fiduciary Relationships

Please refer to the relevant CP.

2.3.3 Administrative Processes

Please refer to the relevant CP.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

This CPS is governed by the laws in force in the Republic of Ireland.

2.4.2 Severability, Survival, Merger, Notice

2.4.2.1 Severability

Please refer to the relevant CP.

2.4.2.2 Survival (Continuing Obligations)

Please refer to the relevant CP.

2.4.2.3 Merger

Please refer to the relevant CP.

2.4.2.4 Notice

Please refer to the relevant CP.

2.4.2.5 Notice Action

Please refer to the relevant CP.

2.4.2.6 Notice Acknowledgment

Please refer to the relevant CP.

2.4.3 Dispute Resolution Procedures

Each CP includes a statement on dispute resolution.

2.5 Fees

Please refer to the relevant CP.

2.6 Publication and Repository

2.6.1 Publication of Revenue PKI Information

This CPS is available in both electronic (PDF) and printed formats from the Revenue PKI Certificate Policy Web Site (see Appendix D for access details).

2.6.2 Frequency of Publication

Newly approved versions of this CPS and relevant CP are published promptly.

2.6.3 Access Controls

There are no access controls on the reading of this CPS or of relevant CP on the web sites nominated for publication.

Access to Certificate information (including CRLs) within the Revenue X.500 Directory is limited in the case of Certificates issued to Approved and Authorised Persons to a single named search enquiry by officers within the Revenue.

Appropriate Access Controls are used to ensure that only authorised personnel have the ability to write to or modify entries in the Revenue X.500 Directory.

2.6.4 Repositories

The Repository for the Revenue PKI is provided through the Revenue X.500 Directory. This directory contains Certificate information for all Certificates issued by Certification Authorities within the Revenue PKI.

The Revenue X.500 Directory does not contain any information about any Private Keys of any kind.

The Directory does not contain any information of a confidential nature

2.7 Compliance Audit

2.7.1 Frequency of Entity Compliance Audit

Revenue shall conduct a comprehensive compliance audit of the practices documented in the Revenue PKI:

1. Within one year of the commencement of operations of the Revenue CA.

2. At any other time that it deems warranted.

2.7.2 Identity/qualifications of Auditor

The PAA will identify and appoint an Auditor.

2.7.3 Auditor's Relationship to Audited Party

External audits will be conducted by persons appointed by the Revenue Commissioners.

2.7.4 Topics Covered by Audit

The topics covered by a compliance audit include those covered within the policies and procedures associated with the Revenue PKI.

2.7.5 Actions Taken as a Result of Deficiency

Copies of the Audit report are submitted to:

- Revenue Commissioners
- The PAA

When irregularities are found, the ROS Strategy Manager, Revenue On-Line Service shall promptly oversee or implement an appropriate corrective action.

2.7.6 Communication of Results

Audit results are considered to be sensitive commercial information. Unless otherwise specified, they are protected in accordance with section 2.9.

2.8 Confidentiality and Privacy

2.8.1 Types of Information to be Kept Confidential

2.8.1.1 Application of Government Information Privacy Principles

Personal Information, as defined in the Data Protection Act 1988 (The Act) provided to or by or on behalf of the Republic of Ireland is covered by the Data Protection Principles as set out in the Act. The Revenue PKI is required to operate fully within the requirements of the Act.

2.8.1.2 Tax Number Information

While Tax Number information may be used to establish the identity of the Entity and the Approved or Authorised Person, that information will not be disclosed or used in the Keys and Certificates.

The term Tax Number Information is used to indicate one or more numbers or other identifiers, allocated by Revenue for the purpose of identification during business communications between entities and Revenue. For example, the VAT numbers and the Tax Advisors Identification Number (TAIN).

The ROS Access Number (RAN) is not included within the definition of Tax Number Information and is disclosed in a Certificate as part of the Distinguished Name.

2.8.1.3 Registration Information

Information collected or held by Revenue may only be released to a third party in accordance with the Official Secrets Act (1963) and the Freedom of Information Act (1998).

2.8.1.4 Certificate Information

At the time of registration the information collected by Revenue may include Personal Information.

Some of this information will, pursuant to the *ITU -T Recommendation X.500 (1993) ISO/IEC 9594 -1:1993, Information technology -Open Systems Interconnection -The Directory: Overview of Concepts, Models and Services*, and in accordance with the Distinguished Name conventions approved by the PAA, be included in the Certificate.

Information embodied in a Certificate and in accordance with the previous paragraph, is not considered to be confidential, for example, the name of an Approved or Authorised Person, to the Revenue PKI.

All other information obtained during the registration process by Revenue is considered confidential.

2.8.1.5 Revenue PKI Documentation

Some of the documentation required for the operation of the Revenue PKI contains information that may not be released.

2.8.2 Types of Information not Considered Confidential

2.8.2.1 Certificate Information

Revenue is required to inform potential Approved and Authorised Persons and other Approved and Authorised Persons that the information included on the Certificate that identifies the Approved or Authorised Person is not treated as confidential and is deemed to be Public knowledge where the Certificate is used in its intended fashion.

2.8.2.2 Revenue Documentation

The following Revenue documents are public documents and are not considered to be confidential information:

1. CPs issued by the Revenue CA or ROS CA.
2. This CPS.
3. Privacy Policy (Public).

2.8.3 Disclosure of Certificate Revocation/information

Information leading to a decision to revoke Keys and Certificates may not be released to a third party.

2.8.4 Release to Law Enforcement Officials

As a general principle, no document or record belonging to or held within the Revenue PKI shall be released to law enforcement agencies or officials except where:

1. A properly constituted warrant is produced or the information is otherwise legally required to be disclosed.
2. The law enforcement official is properly identified.

Despite any thing above Revenue will not hold a copy of Approved and Authorised Persons' Private Keys and accordingly will not be able to make them available to any law enforcement agency.

2.8.5 Release as Part of Civil Discovery

As a general principle, no document or record belonging to or held by the Revenue PKI shall be released to any person except where a properly constituted instrument that has emanated from a court having jurisdiction or an authority having legal jurisdiction requiring production of the information is produced.

If officers of the Revenue want to obtain access to similar information they will have to document the reason for access to the satisfaction of the PAA.

2.8.6 Disclosure Upon Owner's Request

An Approved or Authorised Person shall have full access to any information that it has provided to the Revenue CA, and shall be empowered to authorise release of that information to another person in accordance with the normal arrangements approved by the Revenue Commissioners or under the Freedom of Information Act (1998). However an Approved or Authorised Person will not have access to any other person's registration record unless formal authorisation has been given by the relevant person.

This authorisation may take two forms:

- A properly constituted electronic request providing that the request is electronically signed by a valid set of Keys and Certificates
- By application in writing

No release of information is permitted without authorisation in accordance with this section.

2.8.7 Other Information Release Circumstances

No other release of information is permitted unless authorised by the person subject of the information, or unless required by law.

2.9 Intellectual Property Rights

Please refer the relevant CP.

3 Identification and Authentication

3.0 General

3.0.1 Initial Registration

A fundamental concept underpinning the operation of the Revenue PKI and the Revenue CA is trust. Trust must be realised in each and every aspect of the service operation.

3.0.2 Initial Registration

Entities making their initial application for a Certificate under a relevant CP are to be provided with the following information as part of the registration process:

1. Advice of the information required in order for them to register with the Revenue On-Line Service.

2. A copy of the appropriate Conditions of Use.

The detailed procedures are set out in the relevant CP.

3.1 Initial Registration

3.1.1 Types of Names

All subjects require a distinguished name that is in compliance with the X.500 standard for Distinguished Names.

The Revenue CA approves naming conventions for the creation of distinguished names for Certificate applicants. Different naming conventions may be used in different policy domains.

3.1.2 Need for Names to be Meaningful

Distinguished names must be meaningful. Pseudonymous names may not be used.

3.1.3 Rules for Interpreting Various Name Forms

The normal operation of some types of Certificate generation requires the insertion of an organisation name as part of the distinguished name.

3.1.4 Uniqueness of Names

Distinguished names are to be unambiguous and unique.

3.1.5 Name Claim Dispute Resolution Procedure

Any dispute regarding a Distinguished Name is resolved under the terms of the relevant CP.

3.1.6 Recognition, Authentication and Role of Trademarks

Recognition, Authentication and the role of trademarks is a commercial issue. Nothing in this CPS shall prevent the use of a trademark in a Distinguished Name.

3.1.7 Authentication of Organisation Identity

An Organisation’s identity is to be authenticated by reference to the records of Revenue.

Refer to the appropriate CP for further details of the authentication process.

3.1.8 Authentication of Individual Identity

An individual's identity is to be authenticated by reference to the records of Revenue.

Refer to the appropriate CP for further details of the authentication process.

3.2 Routine Renewal of Keys and Certificates

Approved Persons and other subjects may request that the Revenue PKI renew their Keys and Certificates at the end of the life provided that:

1. The request is made prior to the expiry of the current Keys and Certificates.
2. Material Certificate information has not changed.
3. The current Keys and Certificates have not been revoked.

If any of these conditions are not met, the subject must apply for a new Certificate, and agree to be bound by the relevant Conditions of Use.

Certificate renewal is governed by the relevant CP.

3.3 Rekey after Revocation

Rekey is not permitted after Certificate revocation. An Approved person or other subject requiring a replacement Certificate after revocation must:

1. Apply for new Certificates.
2. Comply with all initial registration and requirements, as documented within the relevant CP and this CPS..

4 Operational Requirements

4.1 Certificate Application

It is the responsibility of the customer requiring Certificates to make that request to the Revenue PKI in accordance with the requirements of the relevant CP.

4.2 Certificate Issuance

The Revenue PKI is to take reasonable care in accepting and processing Certificate applications. They are to comply with the practices described in this CPS and with any requirements imposed by the relevant CP under which the Certificates are issued.

4.2.1 Certificate Issue Process

The Certificate issuing process is governed by the relevant CP.

4.2.1.2 Revenue PKI's Right to Reject Certificate Requests

Certificates are issued at the discretion of the Revenue PKI. If a Certificate request is rejected, the Revenue CA is to promptly inform the applicant. The Revenue PKI is under no obligation to disclose the reason for the rejection of any Certificate request, except where required by the CP under which the Certificate was to have been issued, or by law or government regulation.

4.2.2.2 Operational Periods

All Certificates begin their operational period on the date of issue unless otherwise stated on the Certificate. The operational period of a Certificate is governed by the CP.

The expiry date of issued Certificates must not result in an operational period greater than that permitted by the above instruments. In the event that a Certificate is issued with a greater than permitted operational period, the Certificate is to be revoked.

4.3 Certificate Acceptance

An Approved or Authorised Person or other subject's receipt of Certificates, and their subsequent use constitutes Certificate acceptance.

By accepting the Certificates, the Approved or Authorised person or other subject agrees to be bound by the continuing responsibilities, obligations and duties imposed on them by the Conditions of Use, and the relevant CP.

4.4 Certificate Revocation

4.4.1 Circumstances for Revocation

Revocation can be described as no longer being able to use a Certificate. Certificates are revoked, for example, when:

1. The Keys or Certificates are compromised.
2. Media holding the Private Key is compromised.
3. The Approved or Authorised Person ceases to represent the Entity.
4. The Entity ceases to exist. For example through death, liquidation or dissolution of partnership.
5. Improper or faulty issue of the Certificates.
6. When the Certificate information becomes inaccurate.

7. The Revenue CA or ROS CA ceases to operate.

8. Upon receipt by the Revenue PKI of request from an authorised representative of an Entity, the Approved or Authorised Person or other subject.

4.4.2 Who can Request Revocation

Certificate revocation can be initiated in accordance with the requirements of the relevant CP by:

1. The Revenue PKI.

2. The Approved or Authorised Person or other subject who is named in the Certificate.

3. The Entity named in the Certificate.

4. Authorised third parties.

Note that the Revenue On-Line Service supports the concept of an Approved person within an Entity being nominated for the role of Administrator. The Administrator may request the generation and/or revocation of Private Keys and Certificates for other users within the same Entity (Authorised Persons).

4.4.3 Procedure for Revocation Request

The procedure as set out in the relevant CP shall apply to revocation requests.

4.5 Security Audit Procedures

The Revenue PKI is required to maintain adequate records and archives of information pertaining to the operation of the Revenue CA or the ROS CA.

4.5.1 Types of Event Recorded

Details of the minimum events to be recorded within the Revenue PKI are documented within a separate Auditing and Archiving Policy document, details of which may be obtained from the PAA.

4.5.2 Frequency of Processing Log

Audit logs are processed on a daily, weekly, monthly and annual basis.

4.5.3 Retention Period for Audit Log

Audit logs shall be maintained 'on site' for a minimum period of three months and a maximum period of twelve months. All audit logs shall then be retained in secure archives for a minimum period of 10 years, unless another period is specified in the relevant CP.

4.5.4 Protection of Audit Log

Audit logs are protected by a special user account and password known only to the officer carrying out audit duties. The integrity of the audit logs is protected. The audit logs configuration and procedures will be implemented to ensure that:

- Only authorised people have access to the audit logs;
- Only authorised people may archive audit logs; and
- Audit logs are not modified.

4.5.5 Audit Log Backup Procedures

The Revenue PKI is to establish and maintain a backup procedure for audit logs. Audit logs will be backed up and stored locally for a period of time, and then sent to a secure off-site storage facility. Further details of the backup procedures are in the Audit and Archive Policy document.

4.5.6 Audit Collection System

The Revenue PKI audit collection system is a combination of automated and manual processes performed by the CA or operating system, the CA application, the ROS application, and by operational personnel.

Further details of this collection system are documented in the separate Operations Procedures document.

4.5.7 Notification to Certain Events

Revenue PKI operations personnel notify the Revenue PKI security officer when a process or action causes a critical security event or discrepancy.

4.5.8 Vulnerability Assessments

A Security Risk Review (SRR) has been completed for the entire revenue PKI. This SRR covers the overarching risks and threats that may impact on the Revenue PKI.

4.6 Records Archival

The Revenue PKI maintains an archive of relevant records described in this CPS.

4.6.1 Types of Event Recorded

Details of the minimum events to be archived within the Revenue PKI are documented within a separate Operations Procedures document.

4.6.2 Retention Period for Archive

4.6.2.1 Secure Maintenance of Keys

Approved or Authorised Persons' Private Keys are never held within the Revenue PKI or by Revenue.

Only the Revenue CA and ROS CA private signing keys are archived. The period for archiving the Revenue PKI's private signing keys shall be a minimum period of ten (10) years from the date when they expire or such other time as required to meet requirements of the Revenue Commissioners. At the completion of that term, the private signing keys are archived in a secure facility approved by the PAA. The ROS CA's private keys shall be archived securely.

4.6.2.2 Secure Maintenance of Certificate

Certificates are archived for a minimum period of ten years from the date of expiry, unless another period is specified in the relevant CP.

4.6.2.3 Term of Archive Maintenance

Audit trail information is kept for a minimum period of ten (10) years from the date of expiration, unless another period is specifically required under the relevant CP.

4.6.3 Protection of Archive

Archive media is protected either by physical security, or a combination of physical security and cryptographic protection. It is also protected from environmental factors such as temperature, humidity, and magnetism.

4.6.4 Archive Backup Procedures

The Revenue PKI has established archive back up procedures to ensure and enable complete restoration of current service in the event of a disaster situation as set out in the relevant CP.

4.6.5 Requirements for Time-stamping of Records

Trusted third party time stamping is not supported, but nothing in this CPS will operate to prevent a third party from offering that service outside of the Revenue PKI structure.

4.6.6 Archive Collection System

The Revenue PKI has established an archive collection system that meets the requirements of this CPS. Details of the archive collection system are in the Revenue PKI Operations Procedures.

4.6.7 Procedures to Obtain and Verify Archive Information

The integrity of the Revenue PKI's archives are verified:

1. Annually at the time of a programmed Security Audit.

2. At any other time when a full security audit is required.

3. At the time the archive is prepared.

4.7 Key Changeover

Key changeover is not automatic. Keys expire at the same time as their associated Certificates and, with the exception of the Revenue CA which issues a new Certificate and new keys to itself. All parties within the Revenue PKI are to obtain new keys by making an application for Certificate renewal a minimum of one week prior to Certificate expiry in accordance with the requirements under the relevant CP.

The Revenue PKI needs to:

1. Ensure that key changeover causes minimal disruption to Approved or Authorised users and other subjects in their chain of trust.

2. Provide Approved or Authorised users and other subjects with a minimum of three months' notice of planned key changeover.

3. Revoke and archive the old CA private signing key.

4.8 Compromise and Disaster Recovery

The Revenue PKI:

1. Has established and maintains detailed documentation covering its:

    - Contingency and Disaster Recovery Plan, including key compromise, hardware, software and communications failures, and natural disasters such as fire and flood

    - PKI Configuration Baseline, including operating software, and PKI specific application programs

    - Backup, archiving and offsite storage procedures.

2. Provides the above documentation on the request of:

    - Persons conducting a security or compliance audit

3. Provides appropriate training to all relevant staff in contingency and disaster recovery procedures.

    - At least annually tests its Contingency & Disaster Recovery Plan.

4.8.1 Computing Resources, Software, and/or Data are Corrupted

The Revenue PKI has established a configuration baseline plan, and back-up, archiving and response plan to provide data for identifying component failure and subsequent service restoration.

4.8.2 Revenue CA's Public Key is Revoked

The Revenue PKI will have a Contingency and Disaster Recovery Plan that addresses the actions to be taken in the event that the Revenue CA's or the ROS CA's Public Key is revoked or compromised.

4.8.3 Revenue CA's Public Key is Compromised

The Revenue PKI will have a Contingency and Disaster Recovery Plan that addresses the actions to be taken in the event that the Revenue CA's or the ROS CA's Public Key is revoked or compromised.

4.8.4 Secure Facility After a Natural or Other Type of Disaster

The Revenue PKI has an alternative secure facility to house the CA operations in the event of a natural or other disaster renders the primary facility unable to continue CA operations. This alternative facility is named in the Contingency and Disaster Recovery Plan.

Normal CA operations will be covered by the Contingency and Disaster Recovery Plan to provide a smooth transition to the disaster recovery site. These plans include procedures for repatriating the CA operations back to the primary facility when the disaster has concluded and the primary facility is ready to host CA operations.

4.9 Revenue PKI Termination

If the operation of the Revenue CA or the ROS CA is terminated for any reason Revenue will endeavour to give Entities, Approved or Authorised Persons and other subjects as much warning as possible and put in place alternative arrangements.

All Approved or Authorised user certificates will be revoked. The Revenue PKI will make appropriate arrangements for the continued retention of the CA's archived information to include certificates, revoked keys, audit logs, and all related information in accordance with Section 4.6.

The Revenue PKI is committed to providing a secure process that will enable Entities, Approved or Authorised Persons and other subjects to discharge their obligations in a cost effective and efficient manner.

5 Physical Procedural, and Personnel Security Controls

5.1 Physical Controls

This section outlines the physical, procedural, and personnel security controls required by the Revenue PKI to protect its operations.

5.1.1 Site Location and Construction

The site location of the Revenue CA and ROS CA shall be in a secure environment at a secure hosting facility.. The Revenue PKI operates within a secure physical environment within a secure building.

5.1.2 Physical Access

The Revenue PKI shall permit entry to their secure operating area only to authorised personnel, and to visitors under the constant supervision of an authorised person. The facility is automatically monitored for unauthorized access. The number of personnel authorised to enter the area is kept to a minimum and a log is maintained of all accesses.

5.1.3 Power and Air Conditioning

The Revenue PKI secure operating areas is connected to a standard power supply. All critical components are connected to uninterrupted power supply (UPS) units, to prevent abnormal shutdown in the event of a power failure.

The area has an air conditioning system to control the heat and humidity.

5.1.4 Water Exposures

The Revenue PKI is operated in a facility that is protected from water exposure by …...

5.1.5 Fire Prevention and Protection

Suitable fire suppression systems are maintained in the Revenue PKI operating facility, to provide protection from fire damage.

5.1.6 Media Storage

All magnetic media containing Revenue PKI information, including backup media, are stored in containers, cabinets or safes with fire protection capabilities and are located either within the service operations area or in a secure off-site storage areas.

5.1.7 Waste Disposal

Paper documents and magnetic media containing the Revenue PKI sensitive information or confidential information are securely disposed of by:

1. In the case of magnetic media:

    - Physical damage to, or complete destruction of the asset

    - The use of an approved utility to wipe or overwrite magnetic media

2. In the case of printed material, shredding, or destruction by an approved devise or service.

5.1.8 Off Site Backup

The off-site storage is used for the storage and retention of archive software and data. The off site storage:

1. Is available to authorised personnel 24 hours per day seven days per week for the purpose of retrieving software and data.

2. Has appropriate levels of physical security in place.

5.2 Procedural Controls

5.2.1 Trusted Roles

In general the Revenue PKI supports the separation of duties for critical CA functions to prevent one person from maliciously using the CA system without detection or circumventing the security features.

At a minimum, the following roles are established for the Revenue PKI:

1. Security Officer

2. CA System Administrator.

3. Registrar (ROS CA).

4. Security Administrator.

Separate individuals fill each of the roles described above. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over system operation. However:

1. A single individual may assume the roles of the System Administrator and Registrar.

2. The Security Administrator must always remain separate from the System Administrator in order to provide an independent review of the audit log.

3. Any task requiring the creation, backup or importation into a database of the Revenue CA's Private Key must involve two trusted persons, one performing the function and the second fulfilling a security monitoring role.

5.2.2 Number of Persons Required Per Task

Each of the operations that require dual control by two personnel within the Revenue PKI shall not be carried out by one person. Each person in a dual control shall be responsible for the integrity of the process they are performing. They will not disclose to the other person any parts of a password.

The following tasks require two or more persons:

1. Generating the CA private signing key;
2. Resigning the CA certificate; and
3. Setting the HSM security policy for access control to the CA private signing keys.

5.2.3 Identification and Authentication for Each Role

All Revenue staff are recruited in line with Irish Government recruitment procedures. All PKI personnel shall have their identity and authorization verified before they are:

1. included in the access list for the secure facility;
2. included in the access list for physical access to the CA system;
3. given a certificate for the performance of their CA administration role; or
4. given an account on the CA system for system administration role.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

The Revenue PKI shall require that all personnel performing duties with respect to the operation of the CA, to include trusted roles, shall have sufficient qualification and experience in PKI. All personnel shall meet organisational personnel security requirements.

5.3.2 Background Check Procedures

Background checks are conducted on all persons selected to take up a trusted role in accordance with the designated security screening procedure, prior to the commencement of their duties.

5.3.3 Training Requirements

All Revenue PKI services staff are provided with appropriate training, including:

- Basic PKI concepts

- For pertinent CA staff, how to explain to RA Certificate applicants the responsibilities adhering to the possession, use and operation of their key pairs
- How to explain to users, for example Approved or Authorised Persons, the responsibilities adhering to the possession, use and operation of their Keys and Certificates
- The meaning and effect of the Conditions of Use that applies to the Keys and Certificates

Note that additional software product specific training will be provided to Revenue PKI services staff, as and when deemed appropriate.

5.3.4 Retraining Frequency and Requirements

Revenue PKI services personnel will receive a security briefing update at least once a year.

Training in the use and operation of the CA and RA's software is provided when new versions of the software are installed.

Remedial training is completed when recommended by audit comments.

5.3.5 Job Rotation Frequency and Sequence

The Revenue PKI may implement formal job rotation practices (for example through formal relief). Where formal job rotation is not implemented, cross-training activities are conducted to ensure operations continuity.

5.3.6 Sanctions for Unauthorised Actions

Unauthorised actions by Revenue PKI services personnel staff are submitted to appropriate authorities including, but not limited to, the Security Administrator.

5.3.7 Contracting Personnel Requirements

Revenue PKI services personnel may be contractors who are appointed in writing and given written notification of the terms and conditions of their position. They are normally assigned full-time to their responsibilities.

5.3.8 Documentation Supplied to Personnel

Revenue PKI services personnel shall have access to their relevant:

1. Hardware and software documentation.
2. Policy documents, including this CPS.
3. Operational practice and procedural documents, including a relevant CP.

Help Desk personnel will receive appropriate procedural guidelines and appropriate training to enable them to provide assistance to Approved or Authorised users.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The Revenue CA and ROS CA key pairs will be generated upon initial configuration of the CA application. Both Revenue and ROS CA signature keys are generated in a hardware security module (HSM) that is rated to FIPS 140-1 Level 3.

Approved or Authorised user key pairs will be generated by the Revenue PKI application in such a way that only the Approved or Authorised users will have access to the relevant Private Key.

6.1.2 Private Key Delivery

Private Keys are delivered to Approved or Authorised users through the Revenue On Line secure client application..

6.1.3 Public Key Delivery

Public Keys will be delivered to approved or authorized users through the Revenue On Line secure client application. Certificates will be distributed over the Internet, using a protected session (128 bit SSL).

6.1.4 Revenue PKI Public Key Delivery to Entities

The ROS CA public key is delivered to approve or authorized users through the Revenue On Line secure client application. It is also available from the ROS Web site (see Appendix C).

6.1.5 Key Sizes

The Revenue PKI key lengths are determined by the relevant CP. They are typically a minimum of 2048 bits for CA keys and 1024 bits for end user keys. Below is a table showing the key lengths and algorithms used within the Revenue PKI.

Key Pair	Key Size	Algorithm
Revenue CA	2048	RSA / SHA-1
ROS CA	2048	RSA / SHA-1
End Entities	1024	RSA / SHA-1
Approved and Authorised Persons	1024	RSA / SHA-1

6.1.6 Public Key Parameters Generation

The parameters used to create Public Keys are generated by the hardware security module (HSM) for the CA keys and the Revenue ROS client application for the Entities and Approved or Authorised Persons.

6.1.7 Parameter Quality Checking

The quality of Public Key parameters is automatically checked by the Revenue PKI software.

6.1.8 Hardware/software Key Generation

Revenue CA and ROS CA key generation is performed in an HSM that is rated to FIPS 140-1 Level 3. All other key pairs are generated in software within the ROS application.

Revenue does not have access to Approved or Authorised Persons or other subjects' Private Keys.

6.1.9 Key Usage Purposes

Entities Keys may be used for the purposes and in the manner described in section 1.3.4 Applicability.

The certificate KeyUsage field shall be used within the Revenue CA and ROS CA certificates only. The key usage values shall be set for the CA certificates only:

KeyCertSign

cRLSign

DigitalSignature

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

Cryptographic modules that are used as part of the operations of the Revenue PKI are compliant with FIPS 140-1 Level 3. Keys used by the Revenue CA and the ROS CA are generated and stored in hardware security modules evaluated to FIPS 140-1 Level 3.

6.2.2 Private Key Multi-person Control

The Private Keys of the Revenue CA and ROS CA shall be under multi-person control.

There shall be multiple person control for CA key operations. A minimum of m of n persons shall participate or be present where m must exceed n/2. An m of n person control means there is a minimum "m" persons present out of a total "n" persons (i.e. 3 of 5 persons). The Revenue and ROS CA both require multi-person control for management of the CA's private signing key

6.2.3 Private Key Escrow

Private Key escrow is not supported by the Revenue PKI.

6.2.4 Private Key Backup

The Revenue CA and ROS CA's Private Keys are stored securely in accordance with the relevant CP.

Revenue does not hold copies of Private Keys issued to Approved or Authorised Persons or other subjects.

6.2.5 Private Key Archival

See section 4.6.2.1 Secure Maintenance of Keys.

6.2.6 Private Key Entry into Cryptographic Module

The Revenue and ROS CA private signing keys are generated and stored in a hardware security module (HSM). Approved or Authorised Persons signing keys are generated in software.

Where a cryptographic module is used, the Private Key must be generated in it and remain there in both encrypted and decrypted forms, and be decrypted only at the time at which it is being used.

6.2.7 Method of Activating Private Key

The CA private keys are activated by the use of a token and passphrase in the HSM. Private keys are activated by the ROS application, following the successful completion of a login process that requests and validates an authorised user passphrase value.

6.2.8 Method of Deactivating Private Key

Private keys shall be deactivated when the associated CA (e.g. Revenue CA and/or ROS CA) software application is deactivated.

6.2.9 Method of Destroying Private Key

The software supplied to an Approved and Authorised person or other subject by Revenue is designed to ensure that the Private Keys are destroyed in memory by overwriting it with zeros when the software shuts down.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The Revenue PKI shall archive the signature verification public keys for the period of at least ten (10) years.

6.3.2 Usage Periods for the Public and Private Keys

The usage period for the Revenue CA private and public key shall be ten (10) years. The usage period for other keys issued by the Revenue PKI shall be as set out in the relevant CP.

The Revenue CA's private signing key used to issue certificates shall be valid for no more than ten (10) years. The certificate issued for the ROS CA public signature verification key shall be valid for at least 7 years, which is the period required for retention in archive of CA information

For CA Administrators, Entities, and Authorized and Approved persons the private signing key shall be valid for no longer than 2 years. Authorized and Approved person's public keys (certificates) will be available for validation up to ten (10) years after issuance.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

No activation data other than Access Control mechanisms is required to operate cryptographic software supplied to an Entity.

6.4.2 Activation Data Protection

No activation data other than access control mechanisms, for example a passphrase value, is required to operate cryptographic modules. Activation data, e.g., passphrases will not be stored on magnetic media, computer files. All passphrases that are written down shall be protected from unauthorized using tamper evident envelopes and being stored in a secure container under access control.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The Revenue PKI has established a System Security Policy that incorporates computer security technical requirements for the operation of the Revenue PKI.

6.5.2 Computer Security Rating

The Revenue PKI has established a System Security Policy that incorporates computer security ratings for the operation of the Revenue PKI, where applicable.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The Revenue PKI operational software has been developed in a controlled environment employing appropriate quality controls.

6.6.2 Security Management Controls

System security management is controlled by the privileges assigned to operating system accounts, and by the trusted roles described in section 5.2.1 Trusted roles.

6.6.3 Life Cycle Security Ratings

The Revenue PKI has established a Security Risk Review that identifies and addresses all high or significant life cycle security threats.

6.7 Network Security Controls

The Revenue PKI has established a Security Risk Review that identifies and addresses all high or significant network security threats.

6.8 Cryptographic Module Engineering Controls

The Revenue PKI has established a Security Risk Review that identifies and addresses all high or significant cryptographic module engineering security threats.

7 Certificate and CRL Profiles

7.1 Certificate Profile

7.1.1 Version Numbers

The Revenue PKI supports and uses X.509 Version 3 Certificates, which contain v.3 (integer value 2) in the version field.

7.1.2 Certificate Extensions

The Revenue PKI supports and uses X.509 Version 3 Certificate extensions that are identified in the Revenue PKI Certificate Policy. The Revenue and ROS CA support the following certificate extensions:

1. key identifiers (subject key identifier and authentication key identifier)

2. certificate policies

7.1.3 Algorithms Used

The following hashing/digest algorithms are supported:

1. Secure Hash Algorithm-1 (SHA-1).

2. Message Digest 5 (MD5).

The following padding algorithms are supported:

1. ISO 9796.

2. PKCS#1.

The following encryption algorithms are supported:

1. RSA.

2. Triple DES

3. DES.

The use of multiple algorithms within the same hierarchy is supported.

7.1.4 Name Forms

Certificates issued by the Revenue PKI contain the full X.500 distinguished name of the Certificate issuer and Certificate subject in the issuer name and subject name fields.

7.1.5 Name Constraints

Anonymous or pseudonymous names are not supported.

7.1.6 Certificate Policy Object Identifier

The OID of the relevant CP is carried in the certificatePolicies extension field of X.509 Certificates and is published in the CP.

7.1.7 Usage of Policy Constraints Extension

The Revenue PKI supports the use of the Policy Constraints extension.

7.1.8 Policy Qualifiers

The Revenue PKI supports the use of policy qualifiers within certificate extensions.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

See section 1.3.1.2 of the relevant CP.

7.2 CRL Profile

7.2.1 Version Numbers

The Revenue PKI supports and uses X.509 Version 2 CRLs for CRL's that are publicly available under the relevant CP.

7.2.2 CRL and CRL Entry Extensions

The Revenue PKI supports and uses X.509 Version 2 CRL entry extensions for CRL's that are publicly available under the relevant CP.

8 Specification Administration

The Revenue PKI operates a Policy Approval Authority (PAA) which is responsible for setting Certificate Policy direction for the Revenue PKI. Contact details for the Revenue PAA appear in each CP.

8.1 Specification Change Procedures

8.1.1 Initial Publication

The responsible authority for changes to the CPs used in conjunction with the Revenue PKI is the PAA.

The relevant CA (Revenue CA or ROS CA) will request formal endorsement and allocation of an OID.

After the OID has been granted, the CA will publish details of the CP on the Revenue PKI Certificate Policy Web Site (see Attachment D).

The CA will then be responsible for:

1. Advising all subordinate elements of the CP and its applicability;

8.1.2 Change

Two forms of CP change are contemplated:

1. Issue of a new CP;

2. Change or alteration of an existing CP.

In the event that the CP requires re-issue, then the change process employed will be as for initial publication (as above).

Appendix B – Glossary

Term or Acronym	Explanatory notes
Access	Obtaining knowledge or possession of classified material, or Access to a designated secure area.
Access Control	The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner.
Administrator	An Administrator within the ROS environment is an Approved person who is able to register and/or revoke Authorised Persons within the same Entity.
Approved person	Defined in S917G of the Taxes Consolidated Act 1997. An individual who applies for a Digital Certificate for their own use or on behalf of an Entity, and who applies for digital certificates for Authorised Persons.
Asymmetric cryptographic technique*	A cryptographic technique that uses two related transformations, a Public private transformation (defined by the Private Key). The two transformations have the property that, given the Public transformation, it is computationally infeasible to derive the private transformation. NOTE – A system based on asymmetric cryptographic techniques can either be an encipherment system, a signature system, a combined encipherment and signature system, or a key agreement system. With asymmetric cryptographic techniques there are four elementary trans formations: sign and verify for signature schemes, encipher and decipher for encipherment systems. The signature and decipherment transformation are kept private by the owning entity, whereas the corresponding verification and encipherment transformation are published. There exist asymmetric cryptosystems (e.g. for example RSA) where the four elementary functions may be achieved by only two transformations: one private transformation suffices for both signing and decrypting messages, and one Public transformation suffices for both verifying and encrypting messages. However, since this is not the general case, throughout this International Standard the four elementary transformations and the corresponding keys are kept separate.
Asymmetric encipherment system	A system based on asymmetric techniques whose Public transformation is used for encipherment and whose private transformation is used for decipherment.
Asymmetric key pair	A pair of related keys where the Private Key defines the private transformation and the Public Key defines the Public transformation.
Asymmetric signature system	A system based on asymmetric techniques whose private transformation is used for signing and whose Public transformation is used for verification.

Term or Acronym	Explanatory notes
Authentication	The process whereby a service provider satisfies him/her self to an appropriate level of confidence that a service requestor is entitled to the service sought.
Authentication Private Key	The key used to digitally sign a message.
Authentication Public Key	The key used to verify a digital signature.
Authentication	The provision of assurance of the claimed identity of an entity.
Authenticity	The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information.
Authorised Person	Defined in S917G of the Taxes Consolidated Act 1997. An individual who receives a Digital Certificate applied for on their behalf by an Approved Person.
CA	Certification Authority. Within this CPS the term CA may apply to the Revenue CA and the ROS CA.
Certificate	An electronic document generated by the CA, which is signed with the CA's private key and which contains a public key and details of the Entity and Approved or Authorised Person.
Certificate Policy Statement (CP)	Means a set of procedures to be followed by the CA when Certificates are issued to an Entity.
Certification Practice Statement (CPS)	A statement of the practices that the Revenue CA employs in issuing Certificates.
Certificate Revocation List (CRL)	The process of retracting the guarantees associated with a Public Key pair. In particular the guarantee that the entity and the Public Key pair are mutually identified bound.
Certificate serial number	An integer value, unique within the issuing CA (certification authority), which is unambiguously associated with a Certificate issued by that CA.
Certificate	An entity's data rendered unforgeable with the private or secret key of a certification authority.
Certification authority (CA)	(i) A centre trusted to create and assign Public Key Certificates. Optionally, the certification authority may create and assign keys to the entities. (ii) An authority trusted by one or more users to create and assign Certificates. Optionally the certification authority may create the user's keys. (iii) A trusted entity that verifies the identity of a user, allocates a Distinguished Name to that user, and verifies the correctness of information concerning that user by signing the data which constitutes the digital signature for that user.4
Certification chain	See Certification path

Term or Acronym	Explanatory notes
Certification path	An ordered sequence of Certificates of objects in the DIT (directory information tree) which, together with the Public Key of the initial object in the path, can be processed to obtain that of the final object in the path
Certification Request	Means an electronic document containing the details of the Certificates which are to be created by the CA, completed and digitally signed by the RA, and sent by the RA to the CA.
Communications Security (COMSEC)	All measures applied to the protection of telecommunications from unauthorised interception and exploitation. Communications Security includes: (a) Crypto security - That component of communications security which results from the provision of technically sound cryptosystems and their proper use: (b) Physical security - That element of communications security which results from all physical measures necessary to safeguard classified equipment, material and documents from Access or observation by unauthorised people; and (c) Transmission Security - That component of communication security which results from all measures designed to protect transmissions from unauthorised interception, traffic analysis and imitative deception (the latter term relates to attempts to introduce bogus transmissions into a communications system).
Concept Of Operations (CONOPS)	A high level description of the services offered by the Revenue CAs including the management and security arrangements.
Conditions of Use	Conditions of Use at Appendix A to the CP
Confidentiality Private Key	The key used to encipher or encode the contents of a message.
Confidentiality Public Key	The key used to decipher or decode the contents of a message.
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes
CONOPS	See Concept of Operations.
CP	See Certificate Policy Statement.
CPS	See Certification Practice Statement.
CRL	Certificate Revocation List

Term or Acronym	Explanatory notes
Cryptographic algorithm	A cryptographic algorithm is defined as an algorithm which transforms data in order to hide or reveal its information content and which uses at least one secret parameter. This definition includes both symmetric algorithms (for example DES and FEAL) and asymmetric algorithms (for example RSA and Rabin). In the case of a symmetric algorithm the data is hidden and revealed using a secret parameter. In the case of an asymmetric algorithm the data is hidden using a Public parameter and revealed using a secret parameter.
Cryptographic Information	Information, including crypto-material, significantly descriptive of cryptographic techniques and processes, or of cryptosystems and equipment or their functions and capabilities, the disclosure of which would assist the cryptanalytic solution of an encrypted text or a crypto-system.
Cryptographic key; key	A parameter used in conjunction with an algorithm for the purpose of validation, Authentication, encipherment or decipherment.
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.
DAP	Directory Access Protocol
DEA	Data Encryption Algorithm
Decrypt	Practice of recovering an encrypted message by reverting from cipher text to plain language.
DES	Data Encryption Standard
Digest	The result from the application of a hashing algorithm to message text to a defined data. It is just a quotient.
Digital signature	Data appended to, or a cryptographic transformation (see cryptography) 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 for example by the recipient
Document	Anything on which information is recorded by any means, including words, symbols, images or electromagnetic impressions.
DSA	Digital Signature Algorithm. Directory Service Agent.
Encrypt	Practice of converting plain language to cipher text
Entity	For the Revenue PKI, the term Entity is used to describer a Revenue customer. For example, an Entity may be a company, trust, partnership, sole trader or individual taxpayer who is an employee of a company and pays tax through PAYE. NOTE – The term “entity” is also sometimes used in this glossary as a generic term to describe an Approved or Authorised Person and/or relying party within a PKI.

Term or Acronym	Explanatory notes
Entity Authentication	The corroboration that an entity is the one claimed.
Evaluation authority	A body which implements the criteria for a specific community by means of an evaluation scheme and thereby sets the standards and monitors the quality of evaluations conducted by bodies within that community.
Evaluation scheme	The administrative and regulatory framework under which the criteria are applied by an evaluation authority within a specific community.
Hash	A computed number. A hash is used to compare versions of a calculated piece of data. If the hash results match, an assurance can be drawn that the data has not been tampered with.
Hash field	Field of the intermediate string which conveys the hash-code.
Hash function	(i) A (mathematical) function which maps values from a (possibly very large) domain into a smaller range. A "good" hash function is such that the results of applying the function to a (large) set of values in the domain will be evenly distributed (and apparently at random) over the range. (ii) A function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - it is computationally infeasible to find for a given output an input which maps to this output. - it is computationally infeasible to find for a given input a second input which maps to the same output. [ISO/IEC 10118-1:1994] [FCD ISO/IEC 14888-1 (12/1997)] The following notes are contained in ISO/IEC 10118-1. The second note is also contained in ISO/IEC 14888-1. NOTES 1. The literature of the subject contains a variety of terms which have the same or similar meaning as hash function. Compressed encoding and condensing function are some examples. 2. Computational feasibility depends on the user's specific security requirements and environment.
Hash-code	The string of bits which is the output of a hash-function.
Hierarchy	See Revenue PKI Hierarchy
LSO	International Organisation for Standardisation
ITSEC	Information Technology Security Evaluation Criteria
Key establishment	The process of making available a shared secret key to one or more entities. Key establishment includes key agreement and key transport.
Key generating function	A function which takes as input a number of parameters, at least one of which shall be secret, and which gives as output keys appropriate for the intended algorithm and application. The function shall have the property that it shall be computationally infeasible to deduce the output without prior knowledge of the secret input.

Term or Acronym	Explanatory notes
Key generator	A type of cryptographic equipment used for generating cryptographic keys and, where needed, initialisation vectors.
Key management	The administration and use of the generation, registration, certification de-registration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy.
Key pair	Means a complementary pair of encryption keys generated by the CA and formatted into a private key and public key. The public key is distributed within a certificate issued by the CA.
Key token	Key management message sent from one entity to another entity during the execution of a key management mechanism
Key transport	The process of transferring a key from one entity to another entity, suitably protected
Key	(i) A sequence of symbols that controls the operation of a cryptographic transformation (for example encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification). (ii) A sequence of symbols that controls the operation of a cryptographic transformation (for example encipherment, decipherment).
Message	(i) String of bits of limited length. (ii) A string of bits of any length. (iii) String of bits of any length, possibly empty.
Message Authentication code (MAC)	(i) A code in a message between a sender and a receiver used to validate the source and part or all of the text of a message. The code is the result of an agreed calculation. (ii) A data item derived from a message using symmetric cryptographic techniques and a secret key. It is used to check the integrity and origin of the message by any entity holding the secret key.
Non-repudiation exchange	A sequence of one or more transfers of non-repudiation information (NRI) for the purpose of non-repudiation.
Non-repudiation information	A set of information that may consist of the information about an event or action for which evidence is to be generated and validated, the evidence itself, and the non-repudiation policy in effect.
Non-repudiation policy	A set of criteria for the provision of non-repudiation services. More specifically, a set of rules to be applied for the generation and verification of evidence and for adjudication.
OECD	Organisation for Economic Co-operation and Development.
OID	Object Identifier
PAA	The Policy Approval Authority established by Revenue, responsible for the policies that govern the management and operation of the Revenue PKI.

Term or Acronym	Explanatory notes
Passphrase	See Personal Identification Code.
Personal Identification Code	An Access Control mechanism used during key transport to import Private Keys into an End Entity application. Within the ROS CA the term Passphrase refers to the access control mechanism protecting locally stored private keys within the End Entity computer environment.
Personnel Security	The protective measures used to ensure that only suitable people are given Access, remain suitable for Access and are made aware of their security responsibilities.
Physical Security	(i) That part of protective security concerned with physical measures designed to prevent unauthorised Access to resources, and to safeguard them against espionage, deliberate damage, alteration or theft (for example locks, alarms, safes, and so on). (ii) The measures used to provide physical protection of resources against deliberate and accidental threats.
PIC	See Personal Identification Code.
PKAF	Public Key Authentication Framework - A framework that, if followed, allows for the establishment of a trusted Public Key system. This system will allow any entity to determine the trust and validity of a digital signature claimed to be associated with another entity.
PKI	Public Key Infrastructure.
PKI Entity	A system module component or built-in role within the PKI that has a cryptographic relationship with the CA. In the Revenue PKI the RA, RAO and CAO are all examples of PKI Entities.
Privacy	The right of individuals to control or influence what information related to them may be collected and stored and to whom that information may be disclosed. NOTE - Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.
Private Key	Means that part of a key pair which is held by a logical or legal entity in an authentication system, protected by a password, and not made available to anyone else.
Private signature key	Private Key which defines the private signature transformation. NOTE - This is sometimes referred to as a secret signature key.
Protective Security	The total concept of administrative, personnel, physical, technical, computer and communication security.

Term or Acronym	Explanatory notes
Public Key	(i) Public part, key or mathematical construct from a pair of keys which together form the basis of Public Key Technologies. (See Private Key). The key of an entity's asymmetric key pair which can be made Public. In the case of an asymmetric signature system, the Public Key and the associated algorithms define the verification transformation. [ISO/IEC 13888] ii) (In a Public Key cryptosystem) that key of a user's key pair which is Publicly known. [ISO/IEC 9594-8:1990] [CCITT X.509: 1988] (iii) That key of an entity's asymmetric key pair which can be made Public. [ISO/IEC 9798-1 (2nd edition): 1997] [ISO/IEC 11770-1: 1997] [2nd DIS ISO/IEC 11770-3 (08/1997)] The following note is contained in ISO/IEC 9798-1 and in ISO/IEC 11770-3: NOTE - In the case of an asymmetric signature system the Public Key defines the verification transformation. In the case of an asymmetric encipherment system the Public Key defines the encipherment transformation. A key that is 'Publicly known' is not necessarily globally available. The key may only be available to all members of a pre-specified group.
Public Key derivation function	A Public function, which maps strings of bits to positive integers, which is used to transform an entity's identification data to its verification key, and which satisfies the following two properties: - It is computationally infeasible to find any two distinct inputs which map to the same output. - Either the probability that a randomly chosen value Y is in the range of the function is negligibly small, or it is computationally infeasible to find for a given output an input which maps to this output. NOTE – Negligibility and computational infeasibility depend on the user's specific security requirements and environment.
Public Key information	(i) Information specific to a single entity and which contains at least the entity's distinguishing identifier and at least one Public Key for this entity. There may be other information regarding the certification authority, the entity, the Public Key included in the Public Key information, such as the validity period of the Public Key, the validity period of the associated Private Key, or the identifier of the involved algorithms. (ii) Information containing at least the entity's distinguished identifier and Public Key. The Public Key information is limited to data regarding one entity, and one Public Key for this entity. There may be other static information regarding the certification authority, the entity, the Public Key, or the involved algorithms, included in the Public Key information.

Term or Acronym	Explanatory notes
Public verification key	Public Key which defines the Public verification transformation.
RA	Registration Authority.
RAN	ROS Access Number. A unique number allocated to each potential Approved or Authorised Person to the ROS CA as part of the registration process. The RAN forms part of the Distinguished Name on the Approved or Authorised Person's Certificate and may not be re-used.
RCA	Root Certification Authority. Within the Revenue PKI this would be the Revenue CA.
Registration	The process of recording and validating information about the Entities and Approved or Authorised Persons, as specified by the Policy that the certificates are to be issued under.
Registration Authority	Registration Authority - An entity which establishes the identities of users and registers their certification requirements with a Certification Authority.
Relying Party	Is an Approved or Authorised Person who relies upon the Public Keys and Certificates of another's Public Keys to decrypt and/or authenticate a message, transaction or other electronic file. Within the ROS CA environment, the ROS application is the Relying Party.
Repudiation	Denial by one of the entities involved in a communication of having participated in all or part of the communication
Revenue	Within this document, this term refers to the Office of the Revenue Commissioners for the Republic of Ireland.
Revenue CA	Office of the Revenue Commissioners Certification Authority. The Revenue CA is the highest level of trust within the Revenue PKI.
Revenue CA software	Software used for the operations of the Revenue CA, including RSA Security's Keon Certificate Authority (KCA)
Revenue On-Line Service	The Revenue On-Line Service provides the technical, cryptographic and procedural support for the electronic filing of tax returns to Revenue.
Revenue PKI	Means the public key infrastructure established by Revenue.
Root CA	Refer to RCA.
ROS	The Revenue On-Line Service.
ROS CA	The Certification Authority supporting the ROS application. The ROS CA is a sub CA from the Revenue CA within the Revenue PKI.
RSA	A highly secure cryptography method created by Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. RSA uses a two-part key. The owner keeps the private key; the public key is published. Data that is encrypted using the recipient's public key can only be decrypted by the recipient's private key, and vice-versa.

Term or Acronym	Explanatory notes
Signature key	A secret data item specific to an entity and useable only by this entity in the signature process.
SRR	Security Risk Review
Sub CA	A sub CA is a certification authority operating under a set of cryptographic keys and associated certificates issued by a Root CA. Within the Revenue PKI, the ROS CA is a sub CA of the Revenue CA.
Symmetric cryptographic technique	A cryptographic technique that uses the same secret key for both the originator's and the recipient's transformation. Without knowledge of the secret key, it is computationally infeasible to compute either the originator's or the recipient's transformation.
System integrity	The property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorised manipulation of the system.
TOE	Trusted Operating Environment. For the Revenue PKI this will include the software and hardware components comprising the PKI. For example, the Keon software and HSMs.
Token	A message consisting of data fields relevant to a particular communication and which contains information that has been transformed using a cryptographic technique.
User	Any entity (human or machine) outside the TOE that interacts with the TOE.
Validation	The process of checking the integrity of a message, or selected parts of a message.
Verification Authentication information (verification AI)	Information used by a verifier to verify an identity claimed through exchange AI.
Verification key	(i) A value required to verify a cryptographic check value. (ii) A data item which is mathematically related to an entity's signature key and which is used by the verifier m the verification process.
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.
Vetting	The process of acquiring information to assess a person's suitability for Access to classified and/or sensitive material or to a designated secure area.

NOTE: Some of the definitions have been adopted from ISO Standards.

Appendix C – Policies Supported Under This CPS

Revenue On-Line Service Certificate Policy – OID 1.2.372.980003.1.1.1.1.1

The certificates supported by this CPS are:

- Revenue CA's self signed Certificate.
- ROS CA certificate signed by the Revenue CA.
- Certificates for the Revenue PKI's subordinate elements issued by the ROS CA.

Appendix D – Web Addresses

Web Site for Revenue Certificate Authority Policy and Practice Documents

There is a requirement for this and other Revenue PKI policy and practice documents to be available via the Internet. To access these documents do the following:

Go to: http://www.revenue.ie/

In this document the repository for these Revenue PKI policy and practice documents and the instructions above are referred to as the **Revenue PKI Certificate Policy Web Site.**

This repository includes both paper-based documents available on request from the Revenue to *bone fide* applicants and the **Revenue PKI Certificate Policy Web Site** containing electronic (PDF) versions of public documents**.**

Web Sites for Further Information about PKI:

- http://www.pki-page.org/ provides a link to some general information about PKI and Certificate Authorities. This is an external site and the Revenue Commissioners has no responsibility for its contents.

- http://www.ietf.org/rfc/rfc3647.txt/ provides a link to the Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. This is an external site and the Revenue Commissioners has no responsibility for its contents.