REVENUE ON-LINE SERVICE CERTIFICATE POLICY

Document Version 1.2
Date: 15 September 2007

OID for this CP: 1.2.372.980003.1.1.1.1.1

No part of this document may be copied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written permission from the Office of the Revenue Commissioners.

Copyright © 2000 – 2007 Office of the Revenue Commissioners

REVISION HISTORY

Version	Date	Author	Comments
Ver 1.0	19 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.	Documente 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 7
2 Purpose of this Certificate Policy Statement (CP) 8
3 Conditions of Use 9
3.1 Function of the Conditions of Use 9
4 Policies for Certificates issued by the ROS CA to Approved Persons or Authorised Persons (ROS CA Policies) 9
4.1 Function of the ROS CA Polices 9
5 Appendix D Glossary 10
6 Web Site for Revenue PKI Certificate Policy and Practice Documents 10
7 Background to the Revenue CA/ROS CA 10
8 Amendment Procedure 10
3.2 Policy Approval Authority (PAA) 10
3.3 Change 11
Appendix A – Conditions of Use 12
2. Use of the Certificates 12
3. Who do the Conditions apply to 12
4. Conditions applying to the use of the Certificates 12
6. Dispute Resolution 14
Appendix B – Policies for Certificates issued to Approved Persons or Authorised Persons (ROS CA Policies) 15
1 Introduction 15
1.1 Overview 15
1.1.2 Introduction 15
1.1.3 Standards 16
1.1.4 Definitions 16
1.1.5 X500 Object Identifier Hierarchy 16
1.1.6 . Establishing the Highest Point of Trust in the Revenue PKI 16
1.2 Identification 16
1.2.1 Revenue CA OID 16
1.2.2 ROS CA OID 16
1.2.3 OID for this CP 16
1.3 Applicability 16
1.3.1 Certification Authorities 17
1.3.1.1 Revenue Certification Authority (Revenue CA) 17
1.3.1.2 ROS CA 18
1.3.2 Registration 20
1.3.3 Approved Persons or Authorised Persons 20
1.3.3.1 Approved Person or Authorised Person Functions 20
1.3.3.2 Approved Person or Authorised Person Contact Details 20
1.3.4 Applicability 20
1.3.5 Contact Details 20
2 General Provisions 21
2.1 Obligations 21
2.1.1 General Obligations 21
2.1.2 Revenue CA Obligations 21
2.1.3 ROS CA's Obligations 21
2.1.4 Approved Person or Authorised Person's Obligations 21

2.1.5 Relying Party Obligations 22
2.1.6 Repository Obligations 22
2.2 Liability 22
2.3 Financial Responsibility 22
2.3.1 Fiduciary Relationships 22
2.4 Interpretation 22
2.4.1 Governing Law 22
2.4.2 Severability, Survival, Merger, Notice 22
2.4.2.1 Severability 22
2.4.2.2 Survival (Continuing Obligations) 23
2.4.2.3 Merger 23
2.4.2.4 Notice 23
2.4.2.5 Notice Action 23
2.4.2.6 Notice Acknowledgement 23
2.4.3 Dispute Resolution Procedures 23
2.4.3.1 2.4.3.1 Hierarchy of Certificate Policy 23
2.4.3.2 Process 24
2.5 Fees 24
2.6 Publication 24
2.6.1 Publication of ROS CA Information 24
2.6.2 Frequency of Publication 24
2.6.3 Access Controls 25
2.7 Compliance Audit 25
2.7.1 Frequency of Compliance Audit 25
2.7.2 Identity/qualifications of Auditor 25
2.7.3 Auditor's Relationship to Audited Party 25
2.7.4 Topics Covered by Audit 25
2.7.5 Actions Taken as a Result of Deficiency 25
2.7.6 Communication of Results 25
2.8 Confidentiality and Privacy 26
2.8.1 Types of information to be Kept Confidential 26
2.8.1.1 Application of Government Information Privacy Principles 26
2.8.1.2 Tax Number Information 26
2.8.1.3 Registration Information 26
2.8.1.4 Certificate Information 26
2.8.2 Types of Information not Considered Confidential 26
2.8.2.1 Certificate Information 26
2.8.3 Disclosure of Certificate Revocation Information 26
2.8.4 Release to Law Enforcement Officials 27
2.8.5 Release as Part of Civil Discovery 27
2.8.6 Disclosure Upon Entity's Request 27
2.8.7 Other Information Release Circumstances 27
2.9 Intellectual Property Rights 27
2.9.1 General Provision 27
2.9.1.1 Revenue PKI 27
2.9.1.2 Public and Private Keys 28
2.9.2 Copyright 28
3 Identification and Authentication 28
3.1.1 Initial Registration 28
3.1.2 Entity User Administrators 28

3.1.3 Initial Registration 29
3.1.4 Types of Names 29
3.1.5 Need for Names to be Meaningful 29
3.1.6 Rules for Interpreting Various Name Forms 29
3.1.7 Uniqueness of Names 29
3.1.8 Name Claim Dispute Resolution Procedure 29
3.1.9 Recognition, Authentication and Role of Trademarks 29
3.1.10 Authentication of Organisation Identity 29
3.1.11 Authentication of Individual Identity (Administrator) 30
3.1.12 Authentication of Individual Identity (Other User) 30
3.1.13 Method to Prove Possession of Private Key 30
3.2 Routine Renewal of Certificates 30
3.3 Rekey After Revocation 30
4 Operational Requirements 30
4.1 Certificate Application 30
4.2 Certificate Issuance 30
4.2.1 Certificate Issue Process 31
4.2.1.1 Revenue PKI's Right to Reject Certificate Requests 31
4.2.1.2 Operational Periods 31
4.3 Certificate Acceptance 31
4.4 Certificate Revocation 31
4.4.1 Circumstances for Revocation 31
4.4.2 Who can Request Revocation 32
4.4.3 Procedure for Revocation Request 33
4.4.3.1 ROS CA Processing 33
4.4.3.2 Approved Person or Authorised Person Duties 33
4.5 Certificate Suspension 33
4.5.1 CRL Issuance Frequency 34
4.6 Audit Logs 34
4.6.1 Types of Event Recorded 34
4.6.2 Retention Period for Archive 34
4.6.2.1 Secure Maintenance of Keys 34
4.6.2.2 Secure Maintenance of Certificate 34
4.6.2.3 Term of Archive Maintenance 34
4.6.3 Protection of Archive 34
4.6.4 Archive Backup Procedures 34
4.6.5 Requirements for Time-stamping of Records 34
4.6.6 Archive Collection System 35
4.6.7 Procedures to Obtain and Verify Archive Information 35
4.7 Key Changeover 35
4.8 Compromise and Disaster Recovery 35
4.8.1 Computing Resources Software and/or Data are Corrupted 35
4.8.2 ROS CA's Public Key is Revoked 35
4.8.3 ROS CA's Private Key is Compromised 35
4.8.4 Secure Facility After a Natural or Other Type of Disaster 36
4.8.5 Contingency and Disaster Recovery Plan 36
4.9 ROS CA Termination 36
5 Physical, Procedural, and Personnel Security Controls 36
5.1 Physical Controls 36
5.2 Procedural Controls 36

5.3 Personnel Controls 36
6 Technical Security Controls 37
6.1 Key Pair Generation and Installation 37
6.1.1 Key Pair Generation for Approved Person or Authorised Person 37
6.1.2 Private Key Delivery to Approved Person or Authorised Person 37
6.1.3 Public Key Delivery to Approved Person or Authorised Person 37
6.1.4 Delivery of the ROS CA's Public Key 37
6.1.5 Key Sizes 37
6.1.6 Public Key Parameters Generation 37
6.1.7 Parameter Quality Checking 37
6.1.8 Hardware Key Generation 37
6.1.9 Key Usage Purposes 37
6.2 ROS CA's Private Key Protection 38
6.2.1 Standards for Cryptographic Module 38
6.2.2 Private Key Multi-person Control 38
6.2.3 Private Key Escrow 38
6.2.4 Private Key Backup 38
6.2.5 Private Key Archival 38
6.2.6 Private Key Entry into Cryptographic Module 38
6.2.7 Method of Activating Private Key 38
6.2.8 Method of Deactivating Private Key 38
6.2.9 Method of Destroying Private Key 38
6.3 Other Aspects of Key Pair Management 39
6.3.1 Public Key Archival 39
6.3.2 Usage Periods for the Public and Private Keys 39
6.4 Activation Data 39
6.4.1 Activation Data Generation and Installation 39
6.4.2 Activation Data Protection 39
6.5 Computer Security Controls 39
6.5.1 Specific Computer Security Technical Requirements 39
6.5.2 Computer Security Rating 39
6.6 Life Cycle Technical Controls 39
7 Certificate and CRL Profiles 39
7.1 Certificate Profile 39
7.1.1 Version Numbers 39
7.1.2 Certificate Extensions 40
7.1.3 Algorithm Object Identifiers 40
7.1.4 Name Forms 40
7.1.5 Name Constraints 41
7.1.6 Certificate Policy Object Identifier 41
7.1.7 Usage of Policy Constraints Extension 41
7.1.8 Policy Qualifiers Syntax and Semantics 41
7.1.9 Processing Semantics for the Critical Certificate Policy Extension 41
7.2 CRL Profile 41
7.2.1 Version Numbers 41
8 Specification Administration 41
Appendix C 42
Web Addresses 42
Appendix D – Glossary 43

1 Introduction

The information contained in this document is intended for personnel charged with the management and operation of Certificates issued by the Revenue On-Line Service Certification Authority (ROS CA) under the Revenue Certification Authority (Revenue CA) as part of the Revenue Public Key Infrastructure (Revenue PKI).

Revenue reserves the right to add to, amend, or vary the terms of this agreement by publishing notice of such changes on its web-site and the continued use of the service will signify acceptance of the changes.

The framework in which the Revenue CA operates and its possible relationships with other proposed developments are shown in Figure 1.

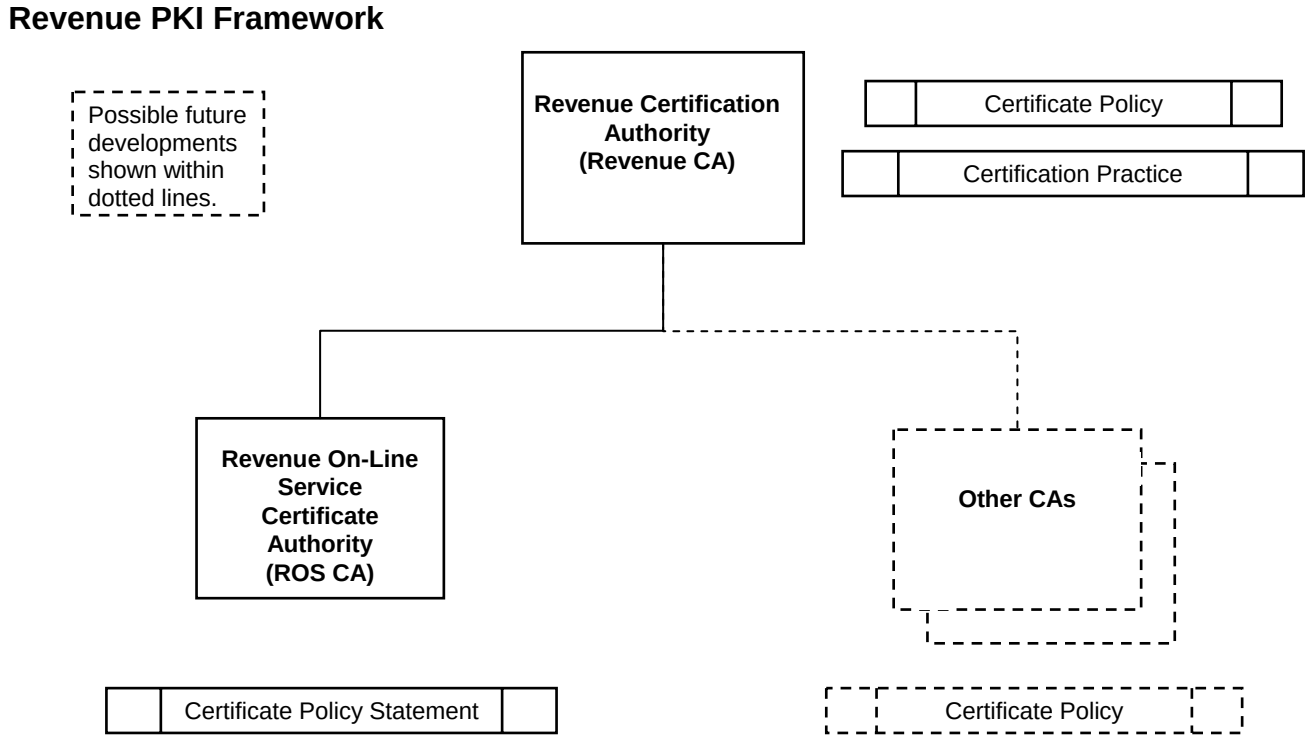

Figure 1 – Revenue PKI Framework

The Revenue PKI must ensure that it maintains the trust of those who have been issued with Certificates. The relationship between the Revenue CA and the ROS CA is shown in Figure 2 on the following page.

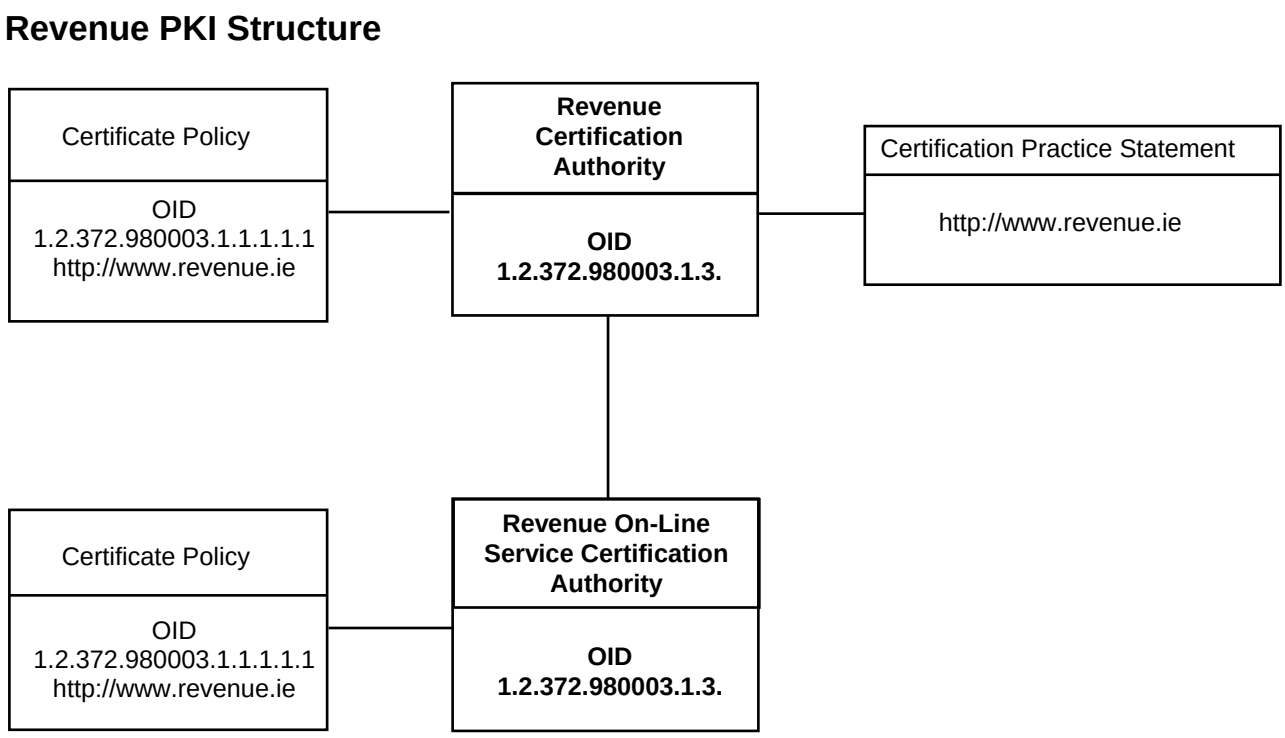

Figure 2 – Revenue PKI Structure

2 Purpose of this Certificate Policy Statement (CP)

The information contained in this CP is intended to inform those who may be issued with Certificates by the ROS CA of their rights and obligations. It also sets out how the ROS CA will discharge its obligations to those persons.

The ROS CA will issue under this CP, Certificates to individuals who have been supplied by Revenue with a ROS Access Number (RAN) and have agreed to the Conditions of Use (Appendix A) that apply to those Certificates. For the purposes of this document such individuals will be referred to as Approved Persons or Authorised Persons.

An individual may act as the Approved Person or Authorised Person, on behalf of an Entity that is required by taxation legislation to submit business and/or personal tax returns or declarations. Where this is the case, Revenue will accept that the Approved Person or Authorised Person has authority to transmit data to Revenue on behalf of the Entity and/or retrieve previously submitted tax information pertaining to that Entity.

This CP does the following:

1. Sets out the Conditions of Use that apply to the issue and use of Certificates issued by the ROS CA at Appendix A.

2. Describes the policies employed by the ROS CA to ensure the security and integrity of the ROS CA's operations and the Certificates at Appendix B.

3. Has at Appendix C a list of relevant web sites.

4. Has attached at Appendix D a Glossary of terms.

This CP has been produced in accordance with the general provisions of the Irish Government's policy and guidelines on the protection of information and information technology environments.

The ROS CA is operated under the Revenue PKI in accordance with the Revenue Certificate Practice Statement (CPS).

3 Conditions of Use

3.1 Function of the Conditions of Use

The Conditions of Use at Appendix A set out the conditions that apply to Certificates issued by the ROS CA to an Approved Person or Authorised Person.

The Approved Person or Authorised Person should particularly note that the use of the Certificates is limited to the purpose of the Approved Person or Authorised Person communicating with the Office of the Revenue Commissioners within the Republic of Ireland.

4 Policies for Certificates issued by the ROS CA to Approved Persons or Authorised Persons (ROS CA Policies)

4.1 Function of the ROS CA Polices

The ROS CA Policies are attached at Appendix B.

The function of those polices is to provide guidelines for the following:

1. Generation, operational use, compromise, expiry, and revocation of Certificates issued by the ROS CA for Revenue customers.

2. Security, mutual consistency, and effectiveness of the ROS CA’s operations.

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

This CP is also complemented by an annotated statement of the policy that appears in the Certificates issued by the ROS CA. That statement is known as the policy qualifier (see Appendix B section 1.3.1.2.3). This CP is also supported by a number of supporting documents that are referenced throughout Appendix B. Unless otherwise stated; those documents are publicly available from the web sites indicated. You may download and copy that material to understand your obligations under the Conditions of Use but for no other purpose.

5 Appendix D Glossary

The glossary contains definitions of the key terms used in this CP.

6 Web Site for Revenue PKI Certificate Policy and Practice Documents

There is a requirement for information about this and other Revenue PKI policy and practice documents to be available via the Internet. Documents will be published on revenue web site – www.revenue.ie.

In the remainder of this document the repository for those documents is referred to as the Revenue PKI Certificate Policy Repository**.**

7 Background to the Revenue CA/ROS CA

The ROS CA will be operated for the purpose of issuing Certificates to customers

- that have been issued with a ROS Access Number (RAN), (Approved Persons), or
- for whom a Certificate has been requested by an Approved Person, (Authorised Persons). Revenue will not have access to the private key of a Revenue customer.

Certificates issued by the ROS CA are designed for the transmission of Tax returns (e.g. VAT 3 and VAT RTD) and other related Revenue returns from Revenue customers. The use of Certificates for use by Revenue customers for viewing previously submitted returns will also be supported. Note that Revenue customers are under no obligation to submit tax returns electronically in order to view their previously submitted returns.

Certificates issued by the Revenue PKI are subject to copyright and may only be used for the purpose of communicating Revenue customer information to discharge an obligation with Revenue. If they are used for any other purpose Revenue may cancel the Certificates without further reference to the Revenue customer.

The use of Certificates in transmitting a tax return will not in itself constitute the signing of a tax return or the making of a declaration in connection with the submission of any tax return.

8 Amendment Procedure

3.2 Policy Approval Authority (PAA)

As new standards emerge, or policy matters are identified for improvement, this CP including the Appendixes will be amended.

The Revenue PAA's responsibilities are set out in Appendix B of this CP.

A document setting out the functions of the Revenue PAA (the PAA Constitution) is made available to all parties responsible for creating or amending this CP. The document is also made available to any approved person conducting a security audit.

3.3 Change

After a change to the Conditions of Use or the policy in Appendix B has been approved the Revenue PKI will do the following:

1. Publish at the Revenue PKI Certificate Policy Web Site (see Appendix C), this CP including the Conditions of Use and the CPS.

2. Publish information advising Approved Persons or Authorised Persons with Certificates as to the effect of the change and its date of effect.

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

If an existing document requires re-issue, the change process employed is the same as for initial publication, as described above. Note that the new OID issued for a new document will have a new version number

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 – Conditions of Use

Electronic Certificates Issued by the ROS CA

1. Purpose

1.1 The Entity has indicated that it wishes to use Revenue's Internet based e-commerce system. The Irish Revenue has asked the Revenue On-Line Service Certification Authority (ROS CA) to issue to the individual with authority to electronically transmit documents and/or view submitted tax returns and declarations on the Entity's behalf, (the Approved Person or Authorised Person), Public and Private Certificates (Certificates). While the Public Key is set out in the Certificate the Private Key is not disclosed to anyone except the intended Approved Person or Authorised Person.

1.2 The Certificates are issued to the Approved Person or Authorised Person subject to these Conditions of Use. The Approved Person or Authorised Person agrees to be bound by these Conditions on each occasion when the Certificates are used. These Conditions should be read in conjunction with the rest of the ROS CA's Certificate Policy Statement (**CP)** which is set out at the Revenue PKI Certificate Policy Web Site**.**

2. Use of the Certificates

2.1 No one but Revenue may rely on the digital signature created by the Certificates unless Public Keys and details of the Certificates are published in a directory of valid Certificates at the Revenue PKI Certificate Policy Web Site.

2.2 All information transmitted electronically over the Internet must be signed and encrypted using the Certificates. A description of other material that may be signed using the Certificates is located at the Revenue PKI Certificate Policy Web Site.

3. Who do the Conditions apply to

3.1. These Conditions of Use apply to the relationship between the Approved Person or Authorised Person and Revenue.

4. Conditions applying to the use of the Certificates

4.1 The Approved Person or Authorised Person agrees:

Use of the Certificates

(a) that true, complete and accurate information has been provided to Revenue when application was made for a RAN or for the Certificates. The Approved Person or Authorised Person undertakes to promptly notify the ROS CA in the event that any part of that information changes or a Private Key has been compromised;

(b) that the Approved Person or Authorised Person has full authority to use the Certificates on the Entity's behalf and if that is no longer the case the Entity will immediately request the ROS CA to revoke the Certificates;

(d) that the Approved Person or Authorised Person may not disclose the Private Keys included as part of the Certificates to any other person;

(e) as between Revenue and the Approved Person or Authorised Person and except as provided in this clause, that Revenue will at all times own the intellectual property rights in the Certificates. Revenue assigns to the Approved Person or Authorised Person any intellectual property including copyright it may have in the Private Keys issued to the Approved Person or Authorised Person but not the Public Keys. Revenue has the right

to use the Approved Person or Authorised Person's distinguished name with the Certificates;

(f) to indemnify Revenue for any loss arising from the Approved Person or Authorised Person's failure to ensure the safety and integrity of the Private Key or the use of the Certificates;

(g) that failure by the Approved Person or Authorised Person to ensure the safety and integrity of the Private Key, or other circumstances that result in the revocation of the use of Certificates by the ROS CA, will result in the Approved Person being required to reapply for a new ROS Application Number (RAN) from Revenue.

Such failure may result in the withdrawal of the Approved Person or the Authorised Person's approval to access ROS.

Role of the ROS CA

(h) that the ROS CA:

(i) oversees the use of Certificates issued through the ROS CA including the policies that promote the integrity of the infrastructure as set out in the **CP**;

(ii) reserves the right to alter these Conditions of Use and the terms and conditions of the **CP** from time to time by notice to the Entity; and

(iii) may revoke the use of the Certificates where it suspects a Private Key has been compromised, the Certificates have been misused, there has been a breach of these Conditions of Use, or it is required to do so under the **CP**.

5. Liability

5.1. The parties agree:

(a) that the liability of any party for breach of these Conditions of Use or for any other common law or statutory cause of action arising out of the use of the Certificates or the operation of the ROS CA, shall be determined under the relevant law in Ireland that is recognised, and would be applied by the Irish courts;

(b) that the Approved Person or Authorised Person will be liable for any loss that may result from the use of the Certificates for any purpose other than for communicating with Revenue;

(c) that the Approved Person or Authorised Person will not be liable to Revenue for the use of the Certificates after it has received notification from the ROS CA that the Keys or Certificates have been revoked. The Approved Person or Authorised Person understands that any such notice may be sent electronically to the address on the RAN application or the address on the application by an Approved Person for a Certificate for an Authorised Person;

(d) that no implied or express warranties are given by any person who may be involved in issuing or managing the Certificates and that all statutory warranties are to the fullest extent permitted by law expressly excluded;

(e) Revenue shall not be liable to the Approved Person nor the Authorised Person nor any Third party for any special, consequential, incidental or indirect damages, including but not limited to loss of profits, damage to data arising out of the use of Keys and Certificates, the services provided by ROS, whether or not Revenue have been advised of the possibility of such damages;

(f) if the Approved Person or Authorised Person breaches these Conditions of Use Revenue may commence proceedings to protect their interests; and

(g) the Approved Person or Authorised Person understands that it is not liable where the Keys or Certificates have

been compromised by the fraudulent or negligent conduct of Revenue.

6. Dispute Resolution

6.1 Subject to the provisions of Chapter 6 of Part 38 of the Taxes Consolidation Act 1997 and without prejudice to its provisions, the **CP** sets out how disputes between the persons referred to in these Conditions of Use are to be resolved and the parties agree that those requirements apply to the extent that the dispute concerns the use of the Certificates.

7. Interpretation

7.1 These Conditions are governed by, and are to be construed in accordance with, the laws from time to time in force in the Republic of Ireland.

7.2 The terms that commence with capital letters will unless there is a contrary intention, for example to indicate the start of a new sentence, have the meaning applied to them in the Glossary to the **CP.**

The Revenue PKI Certificate Policy is available from the Revenue Web Site at www.revenue.ie

Appendix B – Policies for Certificates issued to Approved Persons or Authorised Persons (ROS CA Policies)

1 Introduction

1.1 Overview

1.1.2 Introduction

The Revenue CA is a self signing Certification Authority primarily established to facilitate secure, electronic communication between Revenue customers who have registered for and received a Revenue On-Line Service Access Number (RAN), or have had a certificate application made for them by an Approved Person, and Revenue.

The Revenue CA uses 2048 bit Keys to sign the ROS CA's Certificate and the ROS CA issues 1024 bit Keys to entities under this CP. The Certificates issued under this CP may be issued to an Entity where that Entity has:

(a) appointed an individual (the Approved Person or Authorised Person) to use Certificates to sign documents on the Entity's behalf; and

(b) the Approved Person or Authorised Person has agreed to be bound by this CP including the Conditions of Use at Appendix A and these Revenue CA and ROS CA Policies.

The Revenue PKI may also issue certificates to officers of Revenue who are required to communicate with Approved Persons or Authorised Persons and perform other functions for Revenue.

The infrastructure supporting this CP is made up of the ROS CA and related facilities. Registration Authority (RA) functions are performed by Revenue and based upon Revenue's normal requirements for the establishment of a Revenue customer's identity.

Certificates provided by the Revenue PKI have one type of key pair that is used for both Authentication and Data Integrity purposes by a Customer.

The key pair consists of a Private Key and a Public Key.

For Authentication purposes, the Private Key is used to digitally sign a challenge message and the Public Key is used by the recipient (the ROS application) to verify the attached digital signature.

For Data Integrity purposes, the message to be exchanged is digitally signed by the Private Key and the Public Key is used by the recipient (the ROS application) to verify the attached digital signature.

1.1.3 Standards

This CP is largely based on RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework; see Appendix C for web site details.

Where that document does not provide for sufficient detail this CP will differ in so far as it is necessary for clarity. Requirements relating to the obligations of the Approved Person or Authorised Person have been included in the Conditions of Use at Appendix A.

1.1.4 Definitions

The definitions used within this document are contained in Appendix D - Glossary. These definitions are based on:

1. ISO Glossary of IT Security Technology.

2. Glossary of Terms.

1.1.5 X500 Object Identifier Hierarchy

The authority for all objects identified originates from the Revenue CA.

Specified elements under this CP have been assigned an X.500 Object Identifier (OID).

1.1.6 . Establishing the Highest Point of Trust in the Revenue PKI

Revenue will use the hash of the authentication certificate for the Revenue CA within the ROS application (the Relying Party for the ROS CA) to provide a mechanism by which the validity of digital signatures originating from a customer may be checked by the ROS application.

In operational use, the Revenue PKI entities will also use the hash of the Revenue CA to validate certificates originating from the Revenue PKI.

1.2 Identification

1.2.1 Revenue CA OID

The OID for the Revenue CA is: 1.2.372.980003.1.3.1

1.2.2 ROS CA OID

The OID for the ROS CA is: 1.2.372.980003.1.3.2

1.2.3 OID for this CP

The OID for this CP is: 1.2.372.980003.1.1.1.1.1

1.3 Applicability

This CP is applicable to:

1. ROS CA.

2. Approved Persons and Authorised Persons.

3. Policy Authorities

Details may be found in Section 1.3.0 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Repository (Appendix C).

1.3.1 Certification Authorities

1.3.1.1 Revenue Certification Authority (Revenue CA)

1.3.1.1.1 Revenue CA Functions

Details may be found in Section 1.3.1.1.1 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Repository (Appendix C).

1.3.1.1.2 Revenue CA Contact Details

Details may be found in Section 1.3.1.1.2 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Repository (Appendix C).

1.3.1.1.3 Revenue CA Certificate Root Certificate:

The Revenue CA will be a self signed root certificate. The Revenue CA certificate will contain:

Field	Value
Version	"2" (representing X.509 V3)
Serial Number	An integer that acts as a unique identifier, generated by the CA
Signature Algorithm	MD5,RSA, md5WithRSAEncryption algorithm
Issuer	C=IE, O=Revenue Commissioners, OU=Revenue On-Line Service, CN=Revenue CA
Validity (From)	The date the certificate is valid from. (*date of issue*)
Validity (To)	The date the certificate is valid until. (*Max 10 years*)
Subject	Distinguished Name of CA: C=IE, O=Revenue Commissioners, OU=Revenue On-Line Service, CN=Revenue CA
Subject Public Key Info	RSA Encryption with SHA-1 Key size is 2048
Authority Key Identifier (AKI)	MD5 Hash of Revenue CA public key.
Subject key identifier (SKI)	MD5 hash of Revenue CA public key.
Basic constraints	1
Key Usage	Key Cert Sign, Digital signature; CRL Signature
Certificate Policies	Certificate Policy OID: 1.2.372.980003.1.1.1.1.1 CP URL**:** www.revenue.ie Policy Qualifier in certificates: The Revenue CA creates and signs its own certificate and signs the ROS CA certificate.

1.3.1.1.4 Revenue CA Certificates Issued to ROS CA

The Revenue CA certificate issued to the ROS CA will contain:

Field	Value
Version	"2" (representing X.509 V3)
Serial Number	An integer that acts as a unique identifier, generated by the ROS CA
Signature Algorithm	MD5,RSA, md5WithRSAEncryption algorithm
Issuer	C=IE, O= Revenue Commissioners, OU=Revenue On-Line Service, CN=Revenue CA
Validity (From)	The date the certificate is valid from. (*date of issue*)
Validity (To)	The date the certificate is valid until. (*Max 6 years)*
Subject	Distinguished Name of CA c=IE, o=Revenue Commissioners, ou=Revenue On-Line Service, cn=ROS CA
Subject Public Key Info	RSA Encryption with SHA-1 Key size is 2048
1.3.1.1.4.1 Authority Key Identifier (AKI)	MD5 Hash of Revenue CA public key.
Subject key identifier (SKI)	MD5 hash of ROS CA certificate.
Basic constraints	0
Key Usage	Key Cert Sign, Digital signature; CRL Signing
Certificate Policies	Certificate Policy OID: 1.2.372.980003.1.1.1.1.1 CP URL**:** www.revenue.ie Policy Qualifier in certificates: 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.

1.3.1.2 ROS CA

1.3.1.2.1 ROS CA Functions

Details may be found in Section 1.3.1.2.1 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Repository (Appendix C).

1.3.1.2.2 ROS CA Contact Details

Details may be found in Section 1.3.1.2.2 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Repository (Appendix C).

1.3.1.2.3 ROS CA Certificates Issued to Revenue customers

The ROS CA will issue Certificates to Approved Persons or Authorised Persons with the following details under this CP:

- Certificates are qualified certificates under the Irish Electronic Commerce Act 2000. They are specifically used for communicating with the 'The Office of the Revenue Commissioners'.

- Certificates to the authorised representative of an Entity such as:

  the public officer of a company or other incorporated body,
  a sole proprietor,
  a partner,
  a trustee,
  a corporate trustee,
  a trustee of a superannuation fund, or
  a government department or agency

  who has authority to transmit documents to Revenue on behalf of that Entity,

- Certificates to an individual who is a Revenue customer, and

- Certificates to the authorised representative of an Entity such as the public officer of a company, a sole proprietor or a partner who transmits information to Revenue on behalf of clients of that Entity.

The entity certificate will contain:

Field	**Value**
Version	"2" (representing X.509 V3)
Serial Number	An integer that acts as a unique identifier, generated by the ROS CA
Signature Algorithm	MD5,RSA, md5WithRSAEncryption algorithm (OID: 1.2.840.113529.1.1.5), as defined within PKCS#1
Issuer	C=IE, O=Revenue Commissioners, OU=Revenue On-Line Service, CN=ROS CA
Validity (From)	The date the certificate is valid from. (*date of issue*)
Validity (To)	The date the certificate is valid until. *(Max 2 Years)*
Subject	Distinguished Name of Approved Person or Authorised Person *(John Citizen)* for example, c=IE, o=XYZ Company, ou=RAN, cn=John Citizen
Subject Public Key Info	RSA Encryption with SHA-1 Key size is 1024
Authority Key Identifier (AKI)	MD5 Hash of ROS CA public key.
Subject key identifier (SKI)	MD5 hash of user certificate.
Certificate Policies	Certificate Policy OID: 1.2.372.980003.1.1.1.1.1 CP URL: www.revenue.ie Policy Qualifier in certificates: Certificates issued under this CP are qualified certificates under the Electronic Commerce Act 2000 for use by Approved or Authorised persons only to communicate with the Revenue Commissioners, and other Government Departments where ROS certificates may be used for authentication purposes.

The Keys and Certificates will be in accordance with the international X.509 v3 standard in RFC 3280 – 'Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile'. Keys and Certificates carry with them a 'policy qualifier', which is used to bring out the major points of this CP. The purpose of the policy qualifier is to provide the person relying upon the Keys

and Certificates with an abbreviated message signifying a policy issue that the Relying Party must be aware of:

Certificates issued under this CP are given to Approved Persons or Authorised Persons who may use them only to communicate with the Office of the Revenue Commissioners, and other Government Departments where ROS certificates may be used for authentication purposes.

1.3.2 Registration

The ROS CA will establish the identity of the Approved Person or Authorised Person by reference to information and procedures administered by the Office of the Revenue Commissioners.

1.3.3 Approved Persons or Authorised Persons

The key length of an Approved Person or Authorised Person's Authentication keys as issued by the ROS CA are fully compliant with the requirements of Revenue.

Approved Person's or Authorised Person's Certificates will be generated by the ROS CA in a way so that only the Approved Person or Authorised Person will have access to the Private Key.

1.3.3.1 Approved Person or Authorised Person Functions

Approved Person or Authorised Person functions are defined in Attachment A, Conditions of Use.

1.3.3.2 Approved Person or Authorised Person Contact Details

The following Approved Person or Authorised Person contact details may be published upon a confidential directory in an Approved Person or Authorised Person's Public Key Certificate in compliance with X.509 standards:

1. Entity name and Approved Person or Authorised Person's name in the End Entity's Distinguished Name in the Organization "O" and Common Name "CN" fields. Note that for an Approved Person or Authorised Person acting on their own behalf, the Organization and Common Name fields will both contain the name of the Approved Person or Authorised Person.

2. The ROS Access Number (RAN) in the End Entity's Distinguished Name in the Organizational Unit "OU" field.

Entity and Approved Person or Authorised Person contact information is maintained confidentially by Revenue as taxpayer information.

1.3.4 Applicability

Certificates issued by the ROS CA are used to support the secure exchange of information between the Revenue customer and Revenue.

1.3.5 Contact Details

The contact information for the ROS PKI Services Manager is at:

Revenue On-Line Service
Trident House

Blackrock
County Dublin

Tel: (1) 890 201106

E-Mail: roshelp@revenue.ie

2 General Provisions

2.1 Obligations

This section covers the obligations of the Revenue and the Revenue PKI to all entities relying on Certificates issued by the ROS CA to Approved Persons or Authorised Persons.

2.1.1 General Obligations

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

2.1.2 Revenue CA Obligations

Details of the Revenue CA's obligations may be found in Section 2.1.2.1 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Web Site (Appendix C).

2.1.3 ROS CA's Obligations

The ROS CA shall:

- Receive and verify requests for certificate issuance in accordance with this CP
- Issue certificates to Entities
- Issue Certificates to Revenue Customers (Approved Persons or Authorised Persons)
- Comply, and ensure that its employees and contractors comply with the conditions set out in this CP and the practices set out in the Revenue CPS
- Maintain Certificate information in a designated Revenue X.500 Directory, including posting CRLs as required
- Revoke certificates that are issued by the CA in accordance with the policies set out in this CP and the practices in the CPS

2.1.4 Approved Person or Authorised Person's Obligations

Approved Person or Authorised Person's obligations are set out in the Conditions of Use set out in the terms and conditions that are provided to and signed prior to issuing revenue certificates.

2.1.5 Relying Party Obligations

The primary Relying Party for the Revenue PKI is the Revenue On-Line Service application.

- Relying Party obligations are set out in the Conditions of Use at Appendix A.
- The Relying Party is obligated to use the ROS certificates exclusively for legal and authorised purposes in accordance with the Conditions of Use at Appendix A and applicable laws.

2.1.6 Repository Obligations

The Revenue Repository function is performed by the Revenue X.500 Directory. This repository is restricted to access by Revenue personnel.

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

2.2 Liability

The Conditions of Use (Appendix A) sets out the liability of the parties.

Further details may be found in Section 2.2 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Repository (Appendix C).

2.3 Financial Responsibility

2.3.1 Fiduciary Relationships

Issuing Certificates in accordance with this CP does not make an Approved Person or Authorized Person an agent, fiduciary, trustee, or other representative of the Revenue or the Entity that they represent.

NOTE – The Revenue On-Line Service application is the primary Relying Party for the Revenue PKI.

2.4 Interpretation

2.4.1 Governing Law

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

2.4.2 Severability, Survival, Merger, Notice

2.4.2.1 Severability

In the event that any one or more of the provisions of the CP shall for any reason be held to be invalid, illegal, or unenforceable at law, such unenforceability shall not affect any other provision, but this CP shall then be construed as if such unenforceable provision or provisions had never been contained herein, and in so far as possible, construed to maintain the original intent of this CP.

2.4.2.2 Survival (Continuing Obligations)

Not applicable.

2.4.2.3 Merger

Not applicable.

2.4.2.4 Notice

A notice or any other communication required to be provided under this CP will be published on or made available via the Revenue PKI Certificate Web Site (Appendix C).

2.4.2.5 Notice Action

Notices will be issued by the ROS CA for the following events:

- Establishment of a new CP that replaces this CP
- Change or alteration of existing CP

2.4.2.6 Notice Acknowledgement

Not applicable.

2.4.3 Dispute Resolution Procedures

The dispute resolution provisions shall be taken to cover any area covered by this CP. This includes but is not limited to:

- Contractual matters supported by this CP including the Conditions of Use
- Privacy policy and practice impacted by or on this CP

The disputes relating to taxation legislation and its administration should be dealt with in accordance with the normal requirements of the law including the administrative law and practice.

2.4.3.1 2.4.3.1 Hierarchy of Certificate Policy

Subject to the provisions of Chapter 6 of Part 38 of the Taxes Consolidation Act 1997 and without prejudice to its provisions, in the event that a relevant dispute arises between Revenue PKI and an Approved Person or Authorised Person the following precedence will apply: where the subject of the dispute is covered within the Conditions of Use and any other part of this CP the Conditions of Use shall prevail.

This CP does not support third party reliance, for example between this CP and any other body and the Revenue PKI.

2.4.3.2 Process

If a dispute arises in connection with this CP, the parties undertake in good faith to use all reasonable endeavours to settle the dispute by negotiation or mediation.

If the parties are not able to resolve a dispute within 28 days from the date the dispute first arose, then the parties shall agree to jointly appoint an independent mediator, having appropriate qualifications and practical experience ("mediator"), for the purpose of resolving the dispute and agree to be bound by the decision of that mediator.

If the parties are not able to agree on a mediator within 56 days from the date the dispute first arose, then the parties agree to appoint the person nominated by the President for the time being of the Irish Institute of Arbitrators. Either party may request the President of the Irish Institute of Arbitrators to make such a nomination.

The parties will promptly furnish to the mediator (imposing appropriate obligations of confidence) al1 information reasonably requested by the mediator relating to the dispute.

The mediator will use all reasonable endeavours to render a decision within 30 days following receipt of the information or if this is not possible, as soon as practical thereafter, and the parties agree to co-operate fully with the mediator to achieve this objective.

The parties will share equally the fees and expenses of the mediator.

If a Party does not think that the process described above is appropriate, the Parties can agree a different process that is more suitable to the circumstances of the dispute.

Disputes between the Revenue PKI and other Government agencies will be resolved in accordance with arrangements between the relevant parties.

2.5 Fees

No Fees will be payable for the initial issue of Certificates by the Revenue PKI. Fees may be payable by an Approved Person or Authorised Person in respect to the further issue, renewal, or revocation of Certificates and other services.

The Revenue PKI will inform Approved Persons or Authorised Persons prior to the imposition of any fees.

2.6 Publication

2.6.1 Publication of ROS CA Information

This CP is available in both electronic (PDF) and printed formats from the Revenue PKI Certificate Policy Web Site (see Appendix C).

A copy of the Revenue CA hash value will also be stored within the Revenue PKI Certificate Policy Web Site (see Appendix C).

2.6.2 Frequency of Publication

Newly approved versions of this CP will be published promptly.

2.6.3 Access Controls

This CP must be published. There are no Access Controls on the reading of this CP. Revenue CA will publish this CP at the Revenue PKI Policy Certificate Web Site (see Appendix C).

Further details may be found in Section 2.6.3 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Web Site (Appendix C).

2.7 Compliance Audit

2.7.1 Frequency of Compliance Audit

The Revenue PKI will be audited from time to time to ensure compliance with the policies documented in this CP.

2.7.2 Identity/qualifications of Auditor

Any person engaged to perform an audit on the Revenue PKI will have sufficient experience in the application of PKI and cryptographic technologies.

2.7.3 Auditor's Relationship to Audited Party

Aside from the audit function, the auditor and audited party shall not have any current or planned financial, legal or other relationship that could result in a conflict of interest.

2.7.4 Topics Covered by Audit

The evaluation criteria include an audit of:

1. Physical security.
2. Documentation and process.
3. Vetting of operations personnel.
4. Technology.
5. Privacy, including compliance with Irish Government Information Privacy Principles as outlined in the Data Protection Act (1988).

2.7.5 Actions Taken as a Result of Deficiency

Copies of the audit report must be submitted in confidence to the Revenue Commissioners.

When irregularities are found, the PAA shall promptly oversee or implement an appropriate corrective action and report publicly on matters as appropriate to ensure that trust in the operation of the Revenue PKI is maintained.

2.7.6 Communication of Results

While most aspects of the audit results will be made public in the usual way, some material may need to be treated as commercial-in-confidence. The amount of that material will be reduced as much as possible. Of course the normal restrictions upon the release of Revenue customer information will apply as appropriate.

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 Information Privacy 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 Approved Person or Authorised Person, that information will not be disclosed or used in the Certificates.

NOTE - The ROS Access Number (RAN) is not included within the definition of Tax Number Information and is disclosed in a Certificate issued to an Approved Person or Authorised Person as part of a 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).

The requirements for the confidentiality and privacy of registration information are dealt with at section 3.1 of this CP.

2.8.1.4 Certificate Information

The requirements for the confidentiality and privacy of Certificate Information are dealt with at section 4 of these ROS CA Policies.

Further details may be found in Section 2.8.1.4 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Web Site (Appendix C).

2.8.2 Types of Information not Considered Confidential

2.8.2.1 Certificate Information

Revenue will inform potential Approved Persons or Authorised Persons that the information included on the Certificates that identifies the Approved Person or Authorised Person will be treated as confidential by the Revenue PKI.

2.8.3 Disclosure of Certificate Revocation Information

Certificate revocation information relating to Approved Person or Authorised Persons will only be made available within Revenue.

Note that information leading to a decision to revoke shall remain confidential.

2.8.4 Release to Law Enforcement Officials

Further details may be found in Section 2.8.4 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Web Site (Appendix C).

Despite anything above the Revenue PKI will not hold a copy of an Approved Person or Authorised Person's Private Keys and accordingly it will not be able to make them available to any officer of Revenue or law enforcement agency.

The Revenue PKI will operate in full compliance with the requirements of the Electronic Commerce Act (2000), especially the provisions on confidentiality as specified within Section 27.

2.8.5 Release as Part of Civil Discovery

Further details may be found in Section 2.8.5 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Web Site (Appendix C).

Despite anything above the Revenue PKI will not hold a copy of an Approved Person or Authorised Person's Private Keys and accordingly it will not be able to make them available to any officer of Revenue or as part of any civil discovery process or for any other purpose.

The Revenue PKI will operate in full compliance with the requirements of the Electronic Commerce Act (2000), especially the provisions on confidentiality as specified within Section 27.

2.8.6 Disclosure Upon Entity's Request

Further details may be found in Section 2.8.6 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Repository (Appendix C).

2.8.7 Other Information Release Circumstances

No other release of information is permitted unless authorised by the person, the subject of the information, or unless required by law, for example, under the Freedom of Information Act, 1997.

2.9 Intellectual Property Rights

2.9.1 General Provision

The Revenue PKI warrants that it is in possession of, or holds licences to grant Certificates to Approved Persons or Authorised Persons and for the use of hardware and software in support of this CP.

The use of the IETF RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework Guideline for drafting this CP is acknowledged.

2.9.1.1 Revenue PKI

Unless stated otherwise in any contract between Revenue and RSA Security Ireland Limited, all intellectual property rights including all copyright in all software documents created by RSA Security Ireland Limited (electronic or otherwise) belongs to and will remain the property of RSA

Security. Revenue has licences to use the software and documentation required in order to operate the Revenue PKI.

2.9.1.2 Public and Private Keys

The Revenue PKI does support the use of Public and Private Key pairs generated by the Approved Person or Authorised Person, as part of the Revenue On-Line Service registration process.

Intellectual property rights in the Certificates issued to an Approved Person or Authorised Person are dealt with in the Conditions of Use.

2.9.2 Copyright

Revenue holds the copyright in this CP. Copyright in the Object Identifiers (OID) for this CP vest in Revenue.

3 Identification and Authentication

3.1.1 Initial Registration

Information relevant to the initial registration of an Approved Person or Authorised Person is contained in the requirements for the registration of a ROS Access Number (RAN). The identity of the Approved Person or Authorised Person is confirmed by Revenue by reference to tax file number information and other Revenue information.

Those requirements are described at the Revenue PKI Certificate Policy Web Site (see Appendix C). Once the Entity has been issued with a RAN and indicated a desire to participate in Revenue's Internet e-commerce system, Revenue will confirm the Approved Person or Authorised Person's identity, issue the Approved Person or Authorised Person with the required software and issue the appropriate Certificate.

Information relevant to the registration by ROS CA is contained in the CPS.

Entities making their initial application for a Certificate under this CP are to be provided with access to the following information:

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

2. A copy of the Conditions of Use.

3.1.2 Entity User Administrators

The Revenue On-Line Service application supports the specification of one Approved Person within an Entity as an Administrator.

An Administrator may request additional certificates for other users within the same Entity (Authorised Persons). For example, an Administrator may decide to delegate certain routine functions to other members of staff within the same company.

Users registered through this process will each be allocated a unique RAN but will not be required to apply directly for a Certificate through the Revenue web site.

Note that should Revenue receive a valid request to revoke the Keys and Certificate associated with an Administrator then all other users within the same Entity will be suspended within the ROS application until a new Administrator is defined for that Entity.

3.1.3 Initial Registration

The application shall involve both functions as listed below:

1. Application for a RAN and initial password by an Approved Person through the ROS application and by an Approved Person on behalf of an Authorised Person. This process will authenticate Certificate applicants through knowledge of tax numbers and other information shared between the Approved Person and Revenue.

2. Acceptance by the Approved Person or Authorised Person of the Conditions of Use.

3.1.4 Types of Names

All Approved Person or Authorised Persons require a distinguished name that is in compliance with the X.500 standard for Distinguished Names.

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

3.1.5 Need for Names to be Meaningful

Distinguished Names for Certificates must be meaningful. Pseudonymous names may not be used. Anonymous Certificates are not supported.

3.1.6 Rules for Interpreting Various Name Forms

The normal operation of Certificate generation requires the insertion of the Approved Person or Authorised Person's name as part of the Distinguished Name.

3.1.7 Uniqueness of Names

Distinguished Names shall be unambiguous and unique.

3.1.8 Name Claim Dispute Resolution Procedure

Any dispute regarding a Distinguished Name will be resolved in terms of section 2.4.3.2.

3.1.9 Recognition, Authentication and Role of Trademarks

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

3.1.10 Authentication of Organisation Identity

An Entity's identity is to be authenticated by reference to the register of ROS Application Numbers and to the records of Revenue.

3.1.11 Authentication of Individual Identity (Administrator)

An Approved Person's identity will be authenticated by reference to the records of Revenue where the Approved Person is either the only Approved Person acting on behalf of that Entity, or where they have been nominated as the individual performing the Administrator role on behalf of that Entity.

3.1.12 Authentication of Individual Identity (Other User)

The initial registration authentication of other Users within an Entity applying for a Certificate will be performed on their behalf by the Approved Person who has been nominated for the role of Administrator within the same Entity. All applications for additional RANs and associated passwords from such an Administrator will be considered already authenticated by Revenue.

3.1.13 Method to Prove Possession of Private Key

The ROS CA is required to satisfy itself that the Private Key in the possession of the Approved Person or Authorised Person does in fact correspond to the Public Key in respect of that Approved Person or Authorised Person.

The method to be employed to do this will be detailed in the ROS CA operating procedures, but should, at the minimum involve signing and verifying a message. This should be done for all keys.

3.2 Routine Renewal of Certificates

The ROS CA does not support the routine renewal of Certificates.

3.3 Rekey After Revocation

Rekey is not permitted after Certificate revocation. An Approved Person requiring Certificates after revocation must apply for a new RAN as though this was a new certificate application through the Revenue web site.

4 Operational Requirements

4.1 Certificate Application

An application for registration by the Approved Person will be taken as an application for an approved Certificate issued in accordance with this CP.

4.2 Certificate Issuance

A Certificate shall be issued to the Approved Person or Authorised Person only after completion of the registration process. See section 3.1.

On completion of issuance the Approved Person or Authorised Person will be issued with the certificates. A private signing key shall have a maximum validity period of 2 years. The associated public certificate shall have a validity of 2 years. The expiry date shall be calculated as two years after the date on which the ROS CA generated the Certificate.

4.2.1 Certificate Issue Process

The Keys for an Approved Person or Authorised Person are generated on the Approved Person or Authorised Person's own computer environment by a signed applet supplied by Revenue as part of the "Certificate Retrieval" option from the ROS application main web page.

The key generation process will securely store the generated keys within the Approved Person or Authorised Person's computer environment, and subsequently generate a request for a new Certificate to the ROS CA.

Certificates will be requested and distributed over the Internet, using a protected session (128 bit SSL).

Certificates will also be stored within the Revenue X.500 directory.

4.2.1.1 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 PKI 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 law or government regulation.

4.2.1.2 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 this 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

Generation of Keys and/or receipt of Certificates, and their subsequent use shall constitute acceptance of the Conditions of Use and the other requirements of this CP.

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

4.4 Certificate Revocation

The ROS CA will revoke Certificates used in accordance with this CP if any of the events listed in section 4.4.1 occur.

4.4.1 Circumstances for Revocation

Certificates shall be revoked by the Revenue PKI where:

1. The Keys or Certificates are compromised.

2. Media holding the Private Key is compromised.

3. The Entity that the Approved Person or Authorised Person represents ceases to trade. For example through death, liquidation, receivership or dissolution of a partnership.

4. The Approved Person or Authorised Person ceases to represent the Entity.

5. There has been improper or faulty issue of the Certificates.

6. There has been improper use of the Certificates by the Approved Person or Authorised Person.

7. The Certificate information becomes inaccurate.

8. The Revenue CA and/or ROS CA cease to operate.

9. The ROS CA receives a request in accordance with Section 4.4.3,

4.4.2 Who can Request Revocation

Certificate revocation may be initiated by:

1. The Revenue PKI.

2. The Approved Person or Authorised Person who is named in the Certificate Common Name or Organization fields.

3. The Entity who is named in the Certificate Organization field.

4. An Approved Person nominated within the ROS application as the Administrator for Certificates within the same Entity.

5. Authorised third parties (see further down page).

The ROS CA may initiate revocation where:

1. It is in receipt of a properly formatted request to revoke.

2. It has reason to believe that the Certificates and/or Keys have been compromised.

3. It has reason to believe that the Approved Person or Authorised Person has been compromised.

4. It has reason to believe that the Entity that the Approved Person or Authorised Person(s) represent has been compromised.

5. Its own Keys or Certificates have been compromised.

6. The Revenue CA and/or ROS CA cease operation.

7. Revenue believes that the Entity that the Approved Person or Authorised Person represents has ceased to exist, for example through death, liquidation or dissolution of a partnership.

8. Revenue believes that the Approved Person or Authorised Person has misused the Certificates.

The Approved Person or Authorised Person and the Entity that they represent may initiate revocation at any time.

Authorised third parties may request Certificate revocation through the ROS CA. Such authorised parties include, but are not limited to:

1. Third parties with Power of Attorney from the Entity or the Approved Person or Authorised Person, in which case the ROS CA must verify the Power of Attorney and the identity of the relevant person.

2. A Tax Agent with written authority to act on behalf of the Entity.

3. An Irish court with jurisdiction to require that the ROS CA take such action, in which case the Revenue CA must confirm the validity of the court order.

Note that a court order for Certificate revocation may be served directly on the ROS CA.

4.4.3 Procedure for Revocation Request

4.4.3.1 ROS CA Processing

To process a revocation request, ROS CA must do all of the following:

- Receive and authenticate the signed request
- Revoke the certificate
- Add the Certificate to its CRL
- Issue a notice confirming the revocation of the Keys and Certificate and the date and time that Certificate is revoked to the Entity and/or the Approved Person or Authorised Person. The notice need not to include the reason for revocation

Note that:

- Revoked Certificates are not deleted from the Revenue X.500 Directory until they are archived in accordance with this CP.
- ROS CA shall publish notice of revoked Certificates in the Revenue X.500 Directory CRL for use within Revenue.

4.4.3.2 Approved Person or Authorised Person Duties

The Approved Person or Authorised Person who has had Certificates revoked should securely destroy the Private Key associated with the revoked certificate.

4.5 Certificate Suspension

Certificate suspension is not supported.

4.5.1 CRL Issuance Frequency

The Revenue PKI will issue a certificate revocation list (CRL) at least daily.

4.6 Audit Logs

Details may be found in Section 4.5 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Web Site (Appendix C).

4.6.1 Types of Event Recorded

Details of the minimum events to be archived within the Revenue PKI are documented within a separate Auditing and Archiving Policy document.

4.6.2 Retention Period for Archive

4.6.2.1 Secure Maintenance of Keys

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

4.6.2.2 Secure Maintenance of Certificate

Certificates issued by the ROS CA under this CP shall be archived for a minimum period of ten years from the date when they expire, unless another period is specifically agreed by the PAA in accordance with the requirements of the Revenue Commissioners.

4.6.2.3 Term of Archive Maintenance

Audit trail information shall be kept for a minimum period of ten years from the date of generation, unless a longer period is specifically agreed by the PAA in accordance with the requirements of the Revenue Commissioners.

4.6.3 Protection of Archive

Archive media shall be 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

Archive back-up procedures have been established by the Revenue PKI to ensure complete restoration of current service or verification. Details of the policies to be adhered to by these procedures within the Revenue PKI are documented within a separate Auditing and Archiving Policy document.

4.6.5 Requirements for Time-stamping of Records

Trusted third party time stamping is not supported under this CP.

4.6.6 Archive Collection System

Archiving shall be done by the ROS CA. Detailed procedures for back-ups, archiving and storage have been set out in a separate Auditing and Archiving Policy.

4.6.7 Procedures to Obtain and Verify Archive Information

The integrity of the archives shall be verified in accordance with the criteria set out in the Revenue PKI Auditing and Archiving Policy:

1. Annually at the time of the programmed security audit.
2. At any time when a full security audit is required.
3. At the time that the archive has been prepared.

4.7 Key Changeover

Details may be found in Section 4.7 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Web Site (Appendix C).

4.8 Compromise and Disaster Recovery

The Revenue PKI shall maintain detailed documentation covering:

1. Contingency planning and disaster recovery
2. Configuration baseline of the ROS CA
3. Back-up, archiving and offsite storage

In accordance with the requirements in the Revenue PKI Certification Practice Statement (CPS).

These plans will be made available to those persons responsible for conducting a security audit of the Revenue PKI and to persons responsible for conducting these tasks on a need to know basis.

4.8.1 Computing Resources Software and/or Data are Corrupted

The Configuration Baseline, Auditing and Archiving Policy, and Business Continuity plan shall provide direction for identifying component failure, and subsequent service restoration.

4.8.2 ROS CA's Public Key is Revoked

The ROS CA shall have a key and user compromise plan that addresses the actions to be taken in the event that the ROS CA Public Key is revoked.

4.8.3 ROS CA's Private Key is Compromised

The ROS CA shall have procedures that address the actions to be taken in the event that the ROS CA Private Key is compromised.

4.8.4 Secure Facility After a Natural or Other Type of Disaster

Backup, archive and offsite storage shall be managed in accordance with the configuration baseline and associated back-up, archiving and offsite storage plan.

4.8.5 Contingency and Disaster Recovery Plan

The Revenue PKI has a Business Continuity plan that addresses, in accordance with the outline in the CPS, the actions to be taken in order to restore core business operations as quickly as practicable when systems operations have been significantly and adversely impacted by fire, strikes, and so on.

4.9 ROS CA Termination

If the operation of the ROS CA is terminated for any reason the Revenue PKI will endeavour to give Approved Persons or Authorised Persons as much warning as possible.

Arrangements will be made for the continued retention of the CA's archived information to include, certificates, keys and all related information in accordance with Section 4.6.

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

5 Physical, Procedural, and Personnel Security Controls

5.1 Physical Controls

Details may be found in Section 5.1 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Web Site (Appendix C).

5.2 Procedural Controls

Details may be found in Section 5.2 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Web Site (Appendix C).

5.3 Personnel Controls

Details may be found in Section 5.3 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Web Site (Appendix C).

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation for Approved Person or Authorised Person

See section 4.2.1 of this document.

6.1.2 Private Key Delivery to Approved Person or Authorised Person

See section 4.2.1 of this document.

6.1.3 Public Key Delivery to Approved Person or Authorised Person

See section 4.2.1 of this document.

6.1.4 Delivery of the ROS CA's Public Key

The ROS CA's Public Key will be available from the Revenue PKI Certificate Policy Web Site (see Appendix C).

Keys for Approved Persons or Authorised Persons will be made available in accordance with the requirements at section 4.2.1.

6.1.5 Key Sizes

The Revenue CA and ROS CA private signing keys will be a minimum of 2048 bits. End entity keys will be a minimum of 1024 bits for Approved or Authorised persons.

6.1.6 Public Key Parameters Generation

The parameters used to create Public Keys shall be generated by the ROS CA.

6.1.7 Parameter Quality Checking

The quality of Public Key parameters shall be automatically checked by the CA software operated by the ROS CA.

6.1.8 Hardware Key Generation

ROS CA key generation shall be performed in hardware as prescribed by security policy. All CA Signature keys shall be generated and stored in a hardware cryptographic module that is rated to at least FIPS 140-1 Level 3.

6.1.9 Key Usage Purposes

Approved Person or Authorised Persons' Keys may be used for the purposes and in the manner described in section 1.3.4.

6.2 ROS CA's Private Key Protection

6.2.1 Standards for Cryptographic Module

Cryptographic modules that may be in use as part of the operations of the Revenue PKI comply with industry standards, such as FIPS 140-1 Level 3.

Keys used by the ROS CA are generated and stored in hardware security module (HSM) that is validated to FIPS 140-1 Level 3. .

6.2.2 Private Key Multi-person Control

The ROS CA's Private Keys shall be under multi-person control.

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 backed up and stored in a secure manner.

The Revenue PKI does not hold copies of Private Keys issued to Approved Persons or Authorised Persons. The Revenue PKI operates in full compliance with the confidentiality requirements defined within the Electronic Commerce Act (2000), Section 27.

6.2.5 Private Key Archival

See section 4.6.2.1. of this document.

6.2.6 Private Key Entry into Cryptographic Module

The Private Key used by an Approved Person or Authorised Person to the ROS CA shall be generated in the cryptographic software within the ROS client application.

6.2.7 Method of Activating Private Key

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 ROS CA or Revenue CA software application is deactivated.

6.2.9 Method of Destroying Private Key

The software supplied to an Approved Person or Authorised Person is designed to ensure that the Private Keys in memory are destroyed by overwriting them with zeros when the software shuts down.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The ROS CA shall archive its Public Key.

6.3.2 Usage Periods for the Public and Private Keys

The usage period for the ROS CA Private Key shall be six (6) years. The usage period for the Approved Person or Authorised Person is two (2) years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

No activation data other than the correct pass-phrase value shall be required to operate the cryptographic software supplied to an Approved Person or Authorised Person.

6.4.2 Activation Data Protection

No activation data other than the correct passphrase value shall be required to operate the cryptographic software supplied to an Approved Person or Authorised Person.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

6.5.2 Computer Security Rating

Not applicable.

6.6 Life Cycle Technical Controls

Details may be found in Section 6.6 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Web Site (Appendix C).

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 in the version field.

7.1.2 Certificate Extensions

The Revenue PKI supports and uses X.509 Version 3 Certificate extensions. The Certificate issued to the Approved Person or Authorised Person uses the following Standard Extensions:

Extension	Status	Usage
Certificate Policies	non-critical	Provides: OID for Certificate Policy; URL for Certification Practice Statement and policy qualifier text

The ROS CA does not support the use of Private extensions to the Certificates issued to Approved Persons or Authorised Persons. The status assigned to an extension determines how the Certificate is treated by an application validating the Certificate.

- If the validating process does not recognise an extension designated as **critical**, the Certificate will be rejected
- If the validating process does not recognise an extension designated as **non-critical**, the extension may be ignored

7.1.3 Algorithm Object Identifiers

OIDs may be allocated to algorithms supported and used within the Revenue PKI.

The following hashing/digest algorithms will be supported:

1. Secure Hash Algorithm-1 (SHA-1)
2. Message Digest 5 (MD5)

The following padding algorithms will be supported:

1. ISO 9796
2. PKCS#1

The following encryption algorithms will be supported:

1. RSA
2. Triple DES
3. DES

The use of multiple algorithms within the same hierarchy will be supported.

7.1.4 Name Forms

Certificates issued by the ROS CA contain the full X.500 distinguished name of the ROS CA and Approved Person or Authorised Person.

7.1.5 Name Constraints

Anonymous or Pseudonymous names will be not supported.

7.1.6 Certificate Policy Object Identifier

The OID of this CP shall be carried in the certificatePolicy extension field of X.509 Certificates and is published in this CP.

7.1.7 Usage of Policy Constraints Extension

The ROS PKI will use the Policy Constraints extension.

7.1.8 Policy Qualifiers Syntax and Semantics

The ROS CA supports the use of syntax and semantics policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

See the extensions used by Certificates issued by the ROS CA section 1.3.1.2.3.

7.2 CRL Profile

7.2.1 Version Numbers

The Revenue PKI supports and uses X.509 Version 2 CRL entry extensions for CRLs that are publicly available.

8 Specification Administration

Details may be found in Section 8 of the Revenue Certification Practice Statement (Revenue CPS), available from the Revenue PKI Certificate Web Site (Appendix C).

Appendix C

Web Addresses

1 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:

1. 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**.**

2 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.

Appendix D – 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 transformations: 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.
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.

Term or Acronym	Explanatory notes
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 Person 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
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

Term or Acronym	Explanatory notes
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
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.

Term or Acronym	Explanatory notes
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 a subscriber and/or relying party within a PKI.
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.

Term or Acronym	Explanatory notes
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.
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

Term or Acronym	Explanatory notes
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.
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.

Term or Acronym	Explanatory notes
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.
Public verification key	Public Key which defines the Public verification transformation.
RA	Registration Authority.

Term or Acronym	Explanatory notes
RAN	ROS Access Number. A unique number allocated to each potential subscriber to the ROS CA as part of the registration process. The RAN forms part of the Distinguished Name on the ROS Customer 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 Person 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	A Subscriber who relies upon the Public 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,
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 the three founders of RSA Security: Professors Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. RSA uses a two-part key. The private key is kept by the owner; 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.
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.

Term or Acronym	Explanatory notes
Subscriber	Means a person who has been issued with a set of Private Keys and a Certificate issued and used under the terms of this Certificate Policy Statement. Within the ROS CA environment, a Subscriber might be an individual Approved Person or Authorised Person or a PKI Entity.
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 certificate authority software and hardware security modules (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.