



Post.Trust Certificate Authority

Certification Practice Statement

CA Policy and Procedures Document

Issue date: 25 January 2005
Version: 2.7.1 Release

Contents

DEFINITIONS.....	6
LIST OF ABBREVIATIONS.....	7
Executive Summary	8
1 INTRODUCTION	9
1.1 OVERVIEW	9
1.2 IDENTIFICATION.....	9
1.3 COMMUNITY AND APPLICABILITY	9
1.4 CONTACT DETAILS	10
1.4.1 ADMINISTRATION ORGANISATION.....	10
2. GENERAL PROVISIONS	11
2.1 OBLIGATIONS.....	11
2.1.1 Post.Trust Certificate Authority (CA) Obligations.....	11
2.1.2 Post.Trust Registration Authority (RA) Obligations	11
2.1.3 Subscriber Obligations.....	11
2.1.4 Relying Party Obligations.....	12
2.1.5 Repository Obligations	12
2.2 LEGAL PROVISIONS	12
2.2.1 Warranty	12
2.2.2 Limited Liability	12
2.2.3 Privacy	13
2.2.4 Force Majeure	13
2.2.5 Certificate Revocation	13
2.2.6 Record Keeping	13
2.2.7 Certificate Content.....	13
2.2.8 Relying Parties.....	13
2.2.9 Governing Law	14
2.2.10 Dispute Resolution Process.....	14
2.2.11 Fiduciary	14
2.2.12 Chained CA Certificate Practices and Liability.....	14
2.2.13 General.....	14
2.3 PUBLICATION AND REPOSITORY.....	15
2.3.1 Publication of CA information.....	15
2.3.2 Frequency of CRL publication.....	15
2.3.3 Access controls	15
2.3.4 Repositories – LDAP Directory.....	15
2.4 COMPLIANCE AUDIT	15
2.5 CONFIDENTIALITY.....	15
2.5.1 Types of Information to be kept Confidential.....	16
2.5.2 Types of Information not considered Confidential.....	16
2.5.3 Disclosure of Certificate Revocation Information.....	16
2.6 INTELLECTUAL PROPERTY RIGHTS	16
3. IDENTIFICATION AND AUTHENTICATION.....	17
3.1 REGISTRATION	17
3.1.1 Types of names	17
3.1.2 Need for names to be meaningful	18

3.1.3 Uniqueness of names	18
3.1.4 Name claim dispute resolution procedure.....	18
3.1.5 Recognition, authentication and role of trademarks	18
3.1.6 Authentication of organisation identity	18
3.1.7 Authentication of individual identity	18
3.2 ROUTINE CERTIFICATE ROLLOVER	19
3.3 REKEY AFTER REVOCATION.....	19
3.4 REVOCATION REQUEST.....	19
4. OPERATIONAL REQUIREMENTS.....	20
4.1 CERTIFICATE REGISTRATION PROCESS.....	20
4.2 CERTIFICATE ISSUANCE/DISTRIBUTION PROCESS	20
4.3 CERTIFICATE ACCEPTANCE.....	20
4.4 CERTIFICATE REVOCATION	21
4.4.1 Circumstances for Revocation	22
4.4.2 Who Can Request Revocation	22
4.4.3 Procedure for Revocation Request.....	22
4.4.4 CRL Issuance Frequency	22
4.4.5 CRL Checking Requirements	23
4.4.6 Online Revocation/Status Checking Availability	23
4.5 DATA TO BE AUDITED WITHIN THE POST.TRUST PKI	23
4.5.1 Types of Data to be recorded	23
4.5.2 Retention Period for Archived Audit Data	25
4.5.3 Vulnerability Assessments.....	25
4.5.4 Protection of Archived Audit Records.....	25
4.5.5 Requirement for Time-Stamping of Records.....	25
4.6 KEY CHANGEOVER.....	25
4.7 COMPROMISE AND DISASTER RECOVERY	25
4.7.1 If Computing Resources, Software and/or Data become corrupted	26
4.7.2 Post.Trust CA Certificate Lifespan.....	26
4.8 CA TERMINATION	26
4.8.1 Private Key Destruction Procedures	26
5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS.....	27
5.1 PHYSICAL SECURITY CONTROLS	27
5.1.1 Site Location and Construction.....	27
5.1.2 Physical Access.....	27
5.1.3 Power and Air Conditioning	27
5.1.4 Fire Prevention and Protection.....	27
5.1.4 Off-site Backup & Recovery Procedures.....	27
5.2 PROCEDURAL CONTROLS.....	28
5.2.1 Trusted Roles	28
5.2.2 Number of Persons Required per Task	31
5.2.3 Identification and Authentication for Each Role	31
5.3 PERSONNEL SECURITY CONTROLS	31
5.3.1 Background, Qualifications, Experience, and Clearance Requirements	31
5.3.2 Background Check Procedures	31
6. TECHNICAL SECURITY CONTROLS	32

6.1 KEY GENERATION.....	32
6.1.1 Key pair generation.....	32
6.1.2 Post.Trust CA Private Key Distribution Service	32
6.1.3 Certificate delivery to certificate requester.....	32
6.1.4 Access to Post.Trust CA Certificate to End Users.....	32
6.1.5 Key sizes	32
6.1.6 Hardware/Software Key Generation.....	33
6.2 PRIVATE KEY PROTECTION.....	33
6.2.1 Standards for Cryptographic Module.....	33
6.2.2 Private Key Escrow.....	33
6.2.3 Method of Activating Private Key.....	33
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT.....	33
6.3.1 Usage periods for the public and private keys.....	33
6.4 LIFE CYCLE TECHNICAL SECURITY CONTROLS.....	34
6.4.2 Security management controls.....	34
6.5 NETWORK SECURITY CONTROLS	34
7. CERTIFICATE AND CRL PROFILES	35
7.1 CERTIFICATE PROFILE.....	35
7.2 CRL PROFILE	35
8. SPECIFICATION ADMINISTRATION	36
8.1 SPECIFICATION CHANGE PROCEDURES	36
8.1.1 Items that can change without notification	36
8.1.3 Items whose change requires a new policy.....	36
8.2 CPS APPROVAL PROCEDURES	36
APPENDIX A - REGISTRATION, CERTIFICATION AND DELIVERY.....	37
Certificate CATEGORY: Post.Trust Server SSL Certificates.....	37
Certificate CATEGORY: Post.Trust Employee Class A Certificates	39
Certificate CATEGORY: Post.Trust Client Signing, Encryption and Authentication Qualified Certificates	41
Certificate CATEGORY: Post.Trust Qualified Document Signing Certificates.....	44
Certificate CATEGORY: Post.Trust Client SSL Authentication Certificates.....	47
APPENDIX B - DIGITAL CERTIFICATE PROFILE DETAILS	49
Post.Trust Server SSL Certificate Profile Details.....	49
Limited Liability	49
Post.Trust Employee Class A Profile Details	51
Limited Liability	51
Post.Trust Client Authentication SSL Certificate Profile Details.....	52
Limited Liability	52
Post.Trust Qualified Encryption Certificate Profile Details	53
Limited Liability	53
Post.Trust Qualified Signing Certificate Profile Details.....	54
Limited Liability	54
Post.Trust Qualified Authentication Certificate Profile Details	55
Limited Liability	55
Post.Trust Qualified Document Signing Certificate Profile Details.....	56
Limited Liability	56

APPENDIX C - POST.TRUST CA PROFILE DETAILS	57
Post.Trust Root CA Certificate Profile Details.....	57
Post.Trust Operational CA Certificate Profile Details.....	57
REFERENCES	59

DEFINITIONS

Certification: The process of creating a public key certificate for an entity binding the entity's identity to its public key.

Certification Authority (CA): An entity trusted by one or more entities to create, assign or revoke public key certificates.

Certification Practice Statement (CPS): A statement of the practices, which a certification authority employs in issuing certificates.

Registration Authority (RA): An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a RA is delegated certain tasks on behalf of a CA).

Relying Party: A recipient who acts in reliance on a certificate and digital signature.

Subscriber: An applicant for and/or a holder of a Post.Trust digital certificate, including without limitation, organisations, individuals and/or hardware and/or software devices.

Qualified Certificate: A certificate whose primary purpose is to identify a person with a high level of assurance, where the certificate meets the qualification requirements defined by the applicable legal framework of the European Directive on Electronic Signature, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, 1999.

LIST OF ABBREVIATIONS

CA Certification Authority
CPS Certification Practice Statement
CRL Certificate Revocation List
DN Distinguished Name
FIPS Federal Information Processing Standard
LDAP Lightweight Directory Access Protocol
PIN Personal Identification Number
PKI Public Key Infrastructure
PKIX Public Key Infrastructure (X.509) (IETF Working Group)
RA Registration Authority
RAA Registration Authority Administrator
RAO Registration Authority Operator

Executive Summary

The Post.Trust Certification Practice Statement (“Post.Trust CPS document” or this “CPS”) represents the manner in which Post.Trust Limited will operate its certification authority business (“Post.Trust”) in the provision of digital certificates (the “Post.Trust Service”). The implementation of a Public Key Infrastructure (PKI) is a complex undertaking involving tight and stringent business process and IT controls, which this document details. The Post.Trust CPS document details the ways in which Post.Trust will create a registration authority, accept registrations, verify details, issue digital certificates and manage digital certificates as part of providing PKI solutions to our customers.

The Post.Trust CPS document outlines the roles and responsibilities of all parties involved in the generation and use of digital certificates and covers the operation of the following aspects of the Post.Trust Service:

- The operation of all Certificate Authority (CA) services.
- The operation of all Registration Authority (RA) services.
- The operation of all Registration Authority Operators (RAO) services.
- Customer agreements.
- Post.Trust certificate policies.
- Post.Trust certificate applications.

In addition, this CPS indicates the types of application that the Post.Trust digital certificates may be used for. The types of applications include, but are not limited to, e-mail; transmission of documents; signature of electronic forms; and authentication of network components such as Web servers and firewalls.

1 INTRODUCTION

This CPS is the certificate practice statement under which the Post.Trust Certification Authority (CA) operates. This CPS covers the practices and procedures employed by Post.Trust to operate the Post.Trust Service. Information contained within this CPS outlines the various certificate policies that have been adopted by Post.Trust and how digital certificates are to be issued to the end user. This CPS also sets out details of the security procedures that have been put into place for subscribers, relying parties and the system architecture. Please refer to the table of contents to view the precise contents of this CPS.

The services that are offered by the Post.Trust Services include;

- Identification and authentication of individuals/organisations and servers
- Certificate holder key pair generated by Post.Trust
- Certificate generation (Qualified and non-Qualified)
- Certificate signing
- Certificate issuance and publication
- Certificate revocation
- LDAP directory service
- Bespoke software development

1.1 OVERVIEW

This CPS is applicable to digital certificates issued by Post.Trust binding the identity of individuals and organisations to a public key for digital signature and non-repudiation.

The purpose of this document is to describe the procedures employed by Post.Trust to undertake the Post.Trust Services and to provide evidence of the methods used to manage tasks associated with authentication and digital certificate generation.

Certificate holders can consult this CPS to obtain details of precisely how the certificate policies are implemented by the Post.Trust CA for any particular digital certificate.

1.2 IDENTIFICATION

Post.Trust provides identification and authentication services for certificate holders, servers, PC or network devices. The registration procedures set out in this CPS and in Appendix A define the credentials necessary to establish the identity of an individual or entity. For Qualified Certificates, all identification processes for individuals require applicants to present themselves for face-to-face verification.

1.3 COMMUNITY AND APPLICABILITY

Within the Post.Trust CA hierarchy there is one Root CA entity that represents the source of all trust within the Post.Trust PKI. In addition to this, there is initially one operational CA and one operational RA module that are responsible for the certification process. Digital certificates are issued on both an individual and an organisational basis.

The suitable applications are as follows: secure electronic mail (s/mime), retail transactions (banking applications), IPSEC applications, secure SSL/TLS applications, contracts signing applications, custom e-Commerce applications etc. Post.Trust digital certificates comply with the latest in Internet Standards (x509 v.3) as set out in RFC 2459.

1.4 CONTACT DETAILS

1.4.1 ADMINISTRATION ORGANISATION

The authority responsible for the registration, maintenance and interpretation of this CSP is Post.Trust's elected committee. In the event that individuals have any queries regarding any aspect of the Post.Trust Service, the following email address and telephone number should be used to submit these:

Email Address: info@post.trust.ie

Telephone: 18 90 6 17 17 1

2. GENERAL PROVISIONS

This section contains provisions relating to the respective obligations of the Post.Trust CA, Post.Trust RA, subscribers and relying parties, as well as other issues pertaining to law and dispute resolution.

2.1 OBLIGATIONS

2.1.1 Post.Trust Certificate Authority (CA) Obligations

The Post.Trust CA obligations include the following:

- Issuance of digital certificates to subscribers, in accordance with this CPS;
- Notification of issuance of a digital certificate to the subscriber (and others) and other relying parties. In the case of issuing company employee certificates the management will also be made aware of the employee receiving their certificate;
- Notification of revocation of a digital certificate to the subscriber and others;
- Timely publishing of revoked digital certificates in a publicly accessible repository in the form of CRLs v 2 (Certificate Revocation Lists);
- Protection of Post.Trust's private key against key compromise;
- Distribution of Post.Trust's public key;

2.1.2 Post.Trust Registration Authority (RA) Obligations

The Post.Trust RA obligations include the following:

- Protection of its private key against key compromise;
- Authentication of subscriber's identification information, which is necessary to issue a digital certificate, to the CA;
- Notification of authenticated digital certificate request to the CA;
- Verification that the information provided by the subscriber for the digital certificate application has been accurately transcribed to the digital certificate;
- Acceptance and verification of digital certificate revocation requests and notification of the verified requests to the CA.

2.1.3 Subscriber Obligations

A subscriber is solely responsible for the protection of their private keys. Subscribers shall notify Post.Trust immediately if they believe a private key has or may have been compromised in any way. A Subscriber shall be liable to Post.Trust and third parties for any misrepresentations they make to Post.Trust, as well as for direct and indirect consequences of those misrepresentations. Subscribers to Post.Trust Services acknowledge that they have been advised to obtain proper training in the use of a public key infrastructure prior to requesting or relying upon a digital certificate. Post.Trust offers different classes of digital certificate. Post.Trust makes no endorsement or recommendation in relation to these of any particular class of digital certificate for any particular application or purpose.

Subscribers must independently assess and determine the appropriateness of each class of digital certificate for any particular application or purpose.

2.1.4 Relying Party Obligations

Relying parties shall be responsible for reviewing this CPS to ensure the use of digital certificates for an appropriate purpose. Relying parties shall also be responsible for verifying certificate validity, including revocation checking before using the digital certificate. A relying party acknowledges and agrees to all applicable liability caps and warranties in a digital certificate before relying on that digital certificate. Post.Trust offers different classes of digital certificate. Post.Trust makes no endorsement or recommendation in relation to these of any particular class of digital certificate for any particular application or purpose. Relying parties must independently assess and determine the appropriateness of each class of digital certificate for any particular application or purpose.

2.1.5 Repository Obligations

Post.Trust will host a repository in the form of an LDAP directory for the purpose of

- Storing and making available all X.509 v 3 certificates issued under the Post.Trust CA, facilitating public access to download these digital certificates for subscriber and relying party requirements.
- Receiving (from the Post.Trust CA), storing and making publicly available regularly updated CRL v 2 information, for the purpose of digital certificate validation.

2.2 LEGAL PROVISIONS

2.2.1 Warranty

Post.Trust hereby warrants (a) it has taken reasonable steps to verify that the information contained in any digital certificate is accurate at the time of issue (b) digital certificates shall be revoked if Post.Trust believes or is notified that the contents of the digital certificate are no longer accurate, or that the key associated with a digital certificate has been compromised in any way. The nature of the steps Post.Trust takes to verify the information contained in a digital certificate vary according to the digital certificate fee charged, the nature and identity of the subscriber, and the applications for which the digital certificate will be marked as trusted. Post.Trust makes no other warranties, and all warranties, express or implied, statutory or otherwise, are excluded to the greatest extent permissible by applicable law, including without limitation all warranties as to merchantability or fitness for a particular purpose.

2.2.2 Limited Liability

Post.Trust shall be liable to subscribers or relying parties for the direct loss arising from any breach of this CPS or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to an aggregated maximum limit specified in Appendices B in respect of the relevant class of digital certificate for any one event or series of related events (in any one twelve month period). Post.Trust shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of this CPS, wasted management or other staff time,

losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term “loss” means a partial loss or reduction in value as well as a complete or total loss.

2.2.3 Privacy

The contents of digital certificates issued by Post.Trust are public information. Post.Trust hereby guarantees that it will not divulge any additional subscriber information to any third party for any reason, unless compelled to do so by law or competent regulatory authority.

2.2.4 Force Majeure

Post.Trust accepts no liability for any breach of warranty, delay or failure in performance that results from events beyond its control such as acts of God, acts of war, acts of terrorism, epidemics, power or telecommunication services failure, fire, and other natural disasters.

2.2.5 Certificate Revocation

Post.Trust shall revoke digital certificates at its sole discretion, and shall publish the list of revoked digital certificates in a publicly accessible Certificate Revocation List.

2.2.6 Record Keeping

Post.Trust shall keep records material to the issue of digital certificates for a minimum of 5 years.

2.2.7 Certificate Content

A Post.Trust digital certificate purports to certify only the information contained therein. A relying party shall make no assumptions about information that does not appear in a digital certificate. Each digital certificate includes a brief statement detailing limitations of liability and disclaimers of warranty, with a reference to the full text of such warnings, limitations and disclaimers in this CPS. In accepting a digital certificate, subscribers and relying parties are acknowledging and agreeing to all such limitations and disclaimers.

2.2.8 Relying Parties

It is unreasonable for any party to rely on a digital certificate issued by Post.Trust if the party has actual or constructive notice of the compromise of the digital certificate or its associated private key. Such notice includes but is not limited to the contents of the digital certificate and information incorporated in the digital certificate by reference, as well as the contents of this CPS and the current set of revoked digital certificates published by Post.Trust.

2.2.9 Governing Law

In order to ensure uniform procedures and interpretation of all subscribers and relying parties, irrespective of their country of residence or nationality, the laws of Ireland shall govern the enforceability, construction, interpretation and validity of this CSP.

2.2.10 Dispute Resolution Process

In the event of any dispute or claim arising from the issue of a Post.Trust digital certificate, the complainant undertakes to notify Post.Trust in writing of the exact nature of the dispute and to follow the Post.Trust complaint processing and dispute resolution policy and procedure available for examination and download at [http://www.post.trust.ie/Downloads/DisputeResolutionProcedures\(DISRES\).pdf](http://www.post.trust.ie/Downloads/DisputeResolutionProcedures(DISRES).pdf) .

2.2.11 Fiduciary

Post.Trust is not the agent, fiduciary or other representative of any subscriber and/or certificate holder and must not be represented by the subscriber and/or certificate holder to be so. Subscribers and/or certificate holders have no authority to bind Post.Trust by contract or otherwise, to any obligation.

2.2.12 Chained CA Certificate Practices and Liability

Post.Trust may delegate trust to other certificate authorities (CA's) ("Chained CA's") through certificate chaining or cross-certification. Post.Trust requires that a Chained CA verify the content of a digital certificate with processes that are at least as conservative and stringent as those employed by Post.Trust. Post.Trust hereby agrees to be liable to third parties for digital certificates issued by Chained CA's in compliance with this CPS, as if Post.Trust in fact issued those digital certificates.

2.2.13 General

Any waiver of any provision of this CPS must be in writing and signed by Post.Trust to be valid. A waiver of any provision hereunder shall not operate as a waiver of any other provision, or a continuing waiver of the same provision in the future. If any court or competent jurisdiction finds any provision of this CPS to be void or unenforceable for any reason, then such provision shall be ineffective to the extent of the courts finding without affecting the validity and enforceability of the remaining provisions, and the parties thereby affected agree to substitute the void or unenforceable provision with a valid and enforceable provision which achieves to the greatest extent possible the legal, commercial and economic objectives of the parties. This CPS, the subscriber agreement and any limitations and exclusions contained in a digital certificate represent the entire understanding and agreement between Post.Trust and each subscriber and relying party relating to the Post.Trust Service, and the issue, acceptance and use of all digital certificates issued by Post.Trust and supersede any and all previous statements, understandings or agreements whether oral or written, and shall not be modified except in writing and signed by Post.Trust.

2.3 PUBLICATION AND REPOSITORY

2.3.1 Publication of CA information

Any changes that shall be made to this CPS such as practices for certificate registration process, the version of digital certificates that are issued shall be published within the most reasonable time frame possible.

2.3.2 Frequency of CRL publication

Publication of the Post.Trust Certificate Revocation List will be configured to be issued once per hour. In addition to this configuration, the CA will automatically publish a CRL to the dedicated directory every time a digital certificate has been revoked. This measure ensures that the directory makes available CRLs that include all revoked digital certificates under the Post.Trust CA at any given time.

2.3.3 Access controls

Public access to CA published information objects such as certificate policy definitions, this CPS, issued digital certificates and digital certificate status shall be unrestricted. All information relating to issued digital certificates and digital certificate status will be published to the dedicated Post.Trust directory server.

2.3.4 Repositories – LDAP Directory

All digital certificate information shall be published to the dedicated Post.Trust LDAP directory server. Each time the Post.Trust CA issues a digital certificate a copy of this digital certificate will automatically be published to the directory server via the LDAP v 3 protocol. The directory server is publicly available in the Post.Trust repository.

2.4 COMPLIANCE AUDIT

An independent external auditor shall audit services of the Post.Trust CA and any designated authorised agents on an annual basis. Any failure to comply with the specified requirements of this CSP shall be addressed by the Post.Trust CA or its authorised agent as soon as is operationally possible. Post.Trust reserves the right to appoint this independent external auditor.

2.5 CONFIDENTIALITY

The Post.Trust CA and subscribers, relying parties and all others using or accessing any personal data in connection with matters dealt with this CPS shall comply with the Data Protection Acts 1988 and 2003, and Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and any amending and/or implementing legislation enacted from time to time, and any other relevant legislation relating to data protection, and any equivalent legislation or regulations in any relevant jurisdiction. In the course of accepting a digital certificate, all subscribers have agreed to allow their personal data submitted in the course of registration to be processed by and on behalf of the Post.Trust CA,

and used as explained in the registration process. They have also been given an opportunity to decline from having their personal data used for particular purposes. They have also agreed to let certain personal data to appear in publicly accessible directories and be communicated to others.

2.5.1 Types of Information to be kept Confidential

All information other than that going into the digital certificate or held in publicly available repositories will be kept strictly confidential.

2.5.2 Types of Information not considered Confidential

All information going into the digital certificate or held in publicly available repositories will not be kept confidential.

2.5.3 Disclosure of Certificate Revocation Information

Access to information relating to the revocation of digital certificates shall be published to the Post.Trust public directory service and access to this directory will be unrestricted. In addition, real-time on-line revocation information is available for digital certificates that are secured by Arcot Wallets that can be issued by Post.Trust to secure private keys. For further information on Arcot technology see www.arcot.com.

2.6 INTELLECTUAL PROPERTY RIGHTS

All Intellectual Property Rights in the Post.Trust Service and any associated documentation (including any and all functional and performance specifications (the “Specifications”)) shall vest in Post.Trust Limited and/or its licensors. For the purposes of this CPS, “Intellectual Property Rights” shall mean all patents, copyrights (including copyright in computer software), design rights, trade marks, trade names, service marks, know-how, trade secrets and technical data, together with all goodwill attaching or relating thereto and all other industrial or intellectual property rights of whatever nature arising anywhere in the world, (and whether any such rights are registered or unregistered, including any application for registration in respect of any such rights).

The subscriber and each relying party shall ensure that in using the Post.Trust Services it will do nothing illegal or infringe upon any third party rights and in particular will ensure that any material that it supplies or transmits is not illegal, libelous, and does not infringe upon any Intellectual Property Right of Post.Trust or any third party.

The subscriber and relying parties are given a non-exclusive, non-transferable, royalty free, limited license to use the Intellectual Property Rights in the Post.Trust Service only to the extent and solely for the purpose of availing of the Post.Trust Service. The granting of this limited licence is conditional on the subscriber’s and relying party’s agreement to and compliance with all of the terms and conditions of this CPS.

Nothing in this CPS shall be taken or inferred as any endorsement by Post.Trust of the subscriber, its business, goods or services.

3. IDENTIFICATION AND AUTHENTICATION

This section serves as an overview of the requirements to be followed in identifying and authenticating individuals and organisations requesting certification under the Post.Trust CA. As the Post.Trust CA will be involved in certifying a variety of certificate types, the identification and authentication process may vary in each particular case. Therefore refer to Appendix A for a detailed description of the identification and authentication procedure for each certificate type.

3.1 REGISTRATION

Post.Trust will implement rigorous authentication requirements, to ensure that the identity of the subscriber is proven. This may include face-to-face identity verification at the beginning of the certificate request procedure or at some point prior to digital certificate delivery to the subscriber. The registration procedure will depend on the type of digital certificate that is being applied for. See Appendix A for the various procedures.

3.1.1 Types of names

The naming convention used by Post.Trust to identify certificate holders uniquely is ISO/IEC 9594 (X.500) Distinguished Name (DN).

The Post.Trust X500 Distinguished Name will comprise of a number of the following components:

Dname Attributes	Examples
Common Name (CN=)	<ul style="list-style-type: none"> • Individual Digital Certificate: The digital certificate holders given name • Role based Digital Certificate: The digital certificate holders organisational role (e.g. general manager) • Server Digital Certificate: The DNS server name () • Company Digital Certificate: The organisation name
Organisation (O=)	Registered business name of organization
Country (C=)	Ireland
Organisation Unit (OU=)	<ul style="list-style-type: none"> • Internal organisation department (e.g. Sales and Marketing) • Job description • Certificate description
Locality (L=)	Town/ City of certificate holder or organisation
Email(E=)	Email address of the certificate holder
Phone Number(Phone=)	Contact number of the certificate holder

3.1.2 Need for names to be meaningful

All subject names must be meaningful¹. The names provided on the digital certificate must be as accurate as possible when describing the person or organisation or role within the organisation. Digital certificates will not be issued for names that are not to be deemed meaningful by Post.Trust.

3.1.3 Uniqueness of names

All names must be unique within the Post.Trust domain. Each digital certificate request must contain a unique set of Dname attributes. These attributes include a collection of the persons/companies name, organisation unit, common name, and postal address. Any digital certificate requests which are not unique will be automatically rejected by the Post.Trust CA. Subscribers who have been rejected by the CA on the grounds that their name is not unique will be notified as promptly as is operationally possible.

3.1.4 Name claim dispute resolution procedure

Name allocation will be subject to availability, although the likelihood of two subscribers wanting to use the same Dname values is unlikely to happen frequently.

3.1.5 Recognition, authentication and role of trademarks

Subscribers represent and warrant that all information supplied in the digital certificate application process is accurate and does not infringe or violate in any way the trademarks, service marks, trade name, company name, or any other Intellectual Property Rights of any third party. Subscribers also warrant that any material they supply or transmit is not libelous and does not constitute malicious falsehood or disparagement of goods or services, is not otherwise defamatory, is not immoral, obscene, pornographic, is not illegal and does not advocate illegal activity, does not constitute a violation of privacy and does not infringe any Intellectual Property Rights of Post.Trust or a third party.

3.1.6 Authentication of organisation identity

As the authentication process is dependent on the class of digital certificate being issued, this procedure will differ accordingly. Please refer to Appendix A for a detailed account of the various authentication processes Post.Trust will carry out.

3.1.7 Authentication of individual identity

The authentication process may include a face to face identity verification process, prior to key material or digital certificate distribution.

¹ As per IETF PKIX-4 definition where the term “meaningful” means that the name form has commonly understood semantics to determine identity of the individual and/or organisation.

Acceptable documentation for face-to-face identity verification shall at least include the following pieces of information:

- Individual's name,
- Individual's photograph,
- Individual's signature,
- Individual's postal address,
- Individual's passport or driving licence,

3.2 ROUTINE CERTIFICATE ROLLOVER

The validity period associated with a digital certificate will be dependent on the digital certificate class in question. The Post.Trust CA will provide a facility to reissue digital certificates that are just about to expire. The frequency at which digital certificates are reissued/rolled over is dependent on the class of digital certificates in question. See Appendix B for rollover details of the various digital certificate classes.

3.3 REKEY AFTER REVOCATION

Once a digital certificate has been revoked, for whatever reason, the subscriber will be required to begin the request process from the very beginning if they require a new digital certificate. All previous certificate information will be deemed unusable.

3.4 REVOCATION REQUEST

The revocation request may be provided via the Post.Trust Help Desk or directly by the subscriber or end user. The subscriber may be required to provide a revocation pass phrase in order to handle the revocation request. Revocation requests for of digital certificates will only be fulfilled following adequate authentication of the originator of the request.

4. OPERATIONAL REQUIREMENTS

This section describes the operating requirements imposed by this CSP on the Post.Trust CA, Post.Trust RA, and end entities. It includes handling of digital certificate revocations, audit logs, and transaction archives.

4.1 CERTIFICATE REGISTRATION PROCESS

The procedure for digital certificate application/registration is dependent on the class of digital certificate being applied for. Please see Appendix A for a detailed description of the application/registration procedure for each class of digital certificate.

4.2 CERTIFICATE ISSUANCE/DISTRIBUTION PROCESS

The procedure for digital certificate issuance/distribution is dependent on the class of digital certificate being applied for. Please see Appendix A for a detailed account of the issuance/distribution procedure for each class of digital certificate.

4.3 CERTIFICATE ACCEPTANCE

The procedure for digital certificate acceptance is dependent on the class of digital certificate being applied for. Please see Appendix A for a detailed account of the acceptance procedure for each class of digital certificate.

In the event that a subscriber requires both a private and public key from the Post.Trust CA service, the subscriber will be supplied with a secure encrypted container file, which contains both the public and private key components. This file may be formatted according to the PKCS#12 standard or using a proprietary encrypted format (Such as Arcot Wallet technology. See www.Arcot.com).

A PKCS#12 file is encrypted using a 12 to 16 digit Personal Authentication Code (PAC) generated during the registration process. Arcot wallet files are secured using a six character PIN that requires real-time on-line authentication.

In the event that a subscriber requires only a digital certificate (as the private and public keys have been generated outside the Post.Trust Service) the subscriber will be supplied with a digital certificate in various formats. For a detailed description of the digital certificate distribution/acceptance process refer to Appendix A.

By accepting a digital certificate issued by the Post.Trust CA from the Post.Trust Web site, the subscriber expressly agrees with Post.Trust and to all who reasonably rely on the information contained in the digital certificate that at the time of acceptance and throughout the operational period of the digital certificate, until notified otherwise by the subscriber that,

- no unauthorised person has ever had access to the subscriber's private key;
- all representations made by the subscriber to Post.Trust regarding the information contained in the digital certificate are true;
- all information contained in the digital certificate is true to the extent that the subscriber had knowledge or notice of such information, and does not promptly notify Post.Trust of any material inaccuracies in such information;
- the digital certificate is being used exclusively for authorised and legal purposes, consistent with this CPS, and

BY ACCEPTING A DIGITAL CERTIFICATE, THE SUBSCRIBER ACKNOWLEDGES THAT IT AGREES TO THE TERMS AND CONDITIONS CONTAINED IN THIS CPS AND THE APPLICABLE SUBSCRIBER AGREEMENT –

BY ACCEPTING A DIGITAL CERTIFICATE, THE SUBSCRIBER ASSUMES A DUTY TO RETAIN CONTROL OF THE SUBSCRIBER'S PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM AND TO TAKE REASONABLE PRECAUTIONS TO PREVENT ITS LOSS EXCLUSION MODIFICATION OR UNAUTHORISED USE.

BY ACCEPTING A DIGITAL CERTIFICATE, THE SUBSCRIBER AGREES TO INDEMNIFY AND HOLD POST.TRUST AND ITS AGENTS AND CONTRACTORS HARMLESS FROM ANY ACTS OR OMISSIONS RESULTING IN LIABILITY, ANY LOSS OR DAMAGE, AND ANY SUITS, PROCEEDINGS OR CLAIMS, AND EXPENSES OF ANY KIND, INCLUDING REASONABLE ATTORNEYS FEES, THAT POST.TRUST, ITS AGENTS AND/OR CONTRACTORS MAY INCUR, THAT ARE CAUSED BY THE USE OR PUBLICATION OF A DIGITAL CERTIFICATE AND THAT ARISE FROM (I) FALSEHOOD OR MISREPRESENTATION OF FACT BY THE SUBSCRIBER (OR A PERSON ACTING UPON INSTRUCTIONS FROM ANYONE AUTHORISED BY THE SUBSCRIBER); (II) FAILURE BY THE SUBSCRIBER TO DISCLOSE A MATERIAL FACT, IF THE MISREPRESENTATION OR OMISSION WAS MADE NEGLIGENTLY OR WITH INTENT TO DECEIVE POST.TRUST OR ANY PERSON RECEIVING OR RELYING ON THE CERTIFICATE; (III) FAILURE TO PROTECT THE SUBSCRIBER'S PRIVATE KEY, TO USE A TRUSTWORTHY SYSTEM OR TO OTHERWISE TAKE THE PRECAUTIONS NECESSARY TO PREVENT THE COMPROMISE LOSS, DISCLOSURE, MODIFICATION OR UNAUTHORISED USE OF THE SUBSCRIBER'S PRIVATE KEY; (IV) USE OF THE DIGITAL CERTIFICATE FOR A PURPOSE WHICH IS LIBELLOUS OR CONSTITUTES MALICIOUS FALSEHOOD OR DISPARAGEMENT OF GOODS OR SERVICES, OR IS OTHERWISE DEFAMATORY, IS IMMORAL, OBSCENE, PORNOGRAPHIC, IS ILLEGAL OR ADVOCATES ILLEGAL ACTIVITY, OR CONSTITUTES A VIOLATION OF PRIVACY OR INFRINGES THE INTELLECTUAL PROPERTY RIGHTS OF POST.TRUST OR A THIRD PARTY.

4.4 CERTIFICATE REVOCATION

The Post.Trust CA reserves the right to revoke any of its issued digital certificates. All revocation information is published and held in LDAP directory server where it is made publicly available when required for certificate verification processes.

4.4.1 Circumstances for Revocation

Digital certificates shall be revoked when any of the information on a digital certificate changes or becomes obsolete or when the private key associated with the digital certificate is compromised or suspected to be compromised.

A digital certificate will be revoked in the following instances on notification:

1. Key Compromise (includes unauthorised access or suspect unauthorised access to private keys lost or suspected lost keys, stolen or suspected stolen keys, or destroyed keys.
2. Affiliation change
3. Superseded
4. Cessation of operation
5. Non payment of invoice
6. Incorrect information contained in digital certificate
7. Subscriber bankruptcy
8. Subscriber liquidation
9. Subscriber death
10. Breach of subscriber agreement with Post.Trust
11. Subscriber profile creation error
12. Post.Trust CA key compromise

4.4.2 Who Can Request Revocation

The following entities may request revocation of a subscriber digital certificate:

- The Post.Trust CA.
- The subscriber.
- The Post.Trust RA, on behalf of the individual subscriber.
- The end entity/user.

4.4.3 Procedure for Revocation Request

Revocations shall be requested following the detection of a compromise or any other event necessitating revocation. Post.Trust will revoke the digital certificate upon such valid requests. Each time a digital certificate is revoked the Post.Trust CA issues and publishes a new CRL to the LDAP directory where it is available for public use in certificate verification. The subscriber may be required to submit the revocation request via the Post.Trust Help Desk or directly over an Internet connection. The subscriber may be required to provide a pass phrase that will be used to activate the revocation process. From here on, the revocation process takes place automatically assuming the pass phrase has been verified. Digital certificate revocation requests may also be issued by contacting the administrators of the Post.Trust CA or RA administrators directly.

4.4.4 CRL Issuance Frequency

The Post.Trust CA will issue CRLs once per hour. In addition to this configuration, the Post.Trust CA will automatically publish a CRL to the LDAP directory immediately after each digital certificate revocation takes place.

4.4.5 CRL Checking Requirements

An entity that downloads a CRL from a repository shall verify the authenticity of the CRL by checking its digital signature and the associated certification path.

4.4.6 Online Revocation/Status Checking Availability

Post.Trust hosts a dedicated LDAP directory server. Details of the directory path will be provided in the Post.Trust CA certificate. The public will have unlimited access to the information contained within this directory.

4.5 DATA TO BE AUDITED WITHIN THE POST.TRUST PKI

The Post.Trust Service is operated in a secure environment based upon the Post.Trust Information Security and Management Policy to protect the service from compromise through unauthorised access to systems or data. Robust security measures and controls are in place to ensure confidentiality, integrity and availability of customer encryption keys (where Post.Trust, at the request of the subscriber, holds and archives subscriber's encryption keys), digital certificates and CRLs.

4.5.1 Types of Data to be recorded

Post.Trust CA Installation Procedure:

All events involved in the generation of the Post.Trust CA key pairs (the Root Post.Trust CA Key, all Post.Trust Operational CA keys and all associated backup key pairs) will be recorded. This includes all configuration data used in the process. The configuration of all the Post.Trust PKI components will also be recorded at this stage. This will ensure that all the necessary security procedures will be adhered to during PKI creation and that important configuration details are recorded.

Private Key and Password holders within the Post.Trust PKI

The Post.Trust CA will consist of several passwords and key pairs, which are crucial to the administration, operation and fundamental security of the PKI environment. Details of the individuals within Post.Trust who have access to particular key pairs and passwords will be carefully audited. Key pair access will take the form of PIN protected smart cards. Access to the Oracle database will take the form of a user name and password. Access control in certain cases may take the form of one individual having access to the smart card and another individual having access to the corresponding PIN to unlock the smart card. This ensures that a minimum of two people being present to perform certain tasks on the Post.Trust PKI system.

All End User Registration Data

All data involved in each individual digital certificate registration process will be carefully recorded for future reference if needed.

The Certification process including certificate/key pair delivery

All data and procedures involved in the certification and distribution of digital certificates will be recorded. Most of this information will be recorded in the form of event logs recorded in the Oracle database (the underlying DBMS used by the PKI software). This includes information such as Digital certificate request acceptance

- Key pair generation
- Digital certificate generation
- All request and response information sent between the various PKI modules themselves
- Digital certificate distribution mechanisms

Certificate and CRL Publication

All data relevant to the publication of digital certificates and CRLs by the Post.Trust CA to the Post.Trust LDAP server will be recorded. Digital certificates are issued to the LDAP server immediately after issuance. Information relating to this transaction can be viewed from the event logs maintained by the Post.Trust CA (in the Oracle database). A CRL is issued to the LDAP server immediately after a digital certificate gets revoked and also at periodic intervals as configured in the Post.Trust CA (once an hour). Again details of this can be viewed in the Post.Trust CA event log.

Certificate Revocation

All digital certificate revocation request details will be recorded including reason for revocation.

Firewall monitoring

As the Post.Trust PKI environment will consist of several important machines hosting the various PKI modules, careful monitoring of all communication between these machines will take place to ensure that only legitimate connections with legitimate transactions take place. A firewall with rigid rules will restrict malicious users from making non-legitimate connections. Logs recording all network traffic to and from these machines will be recorded.

Oracle Auditing

As several of the important PKI components rely on making Oracle client logins to an Oracle server for their operations, Oracle auditing will be set-up to monitor all client logins to ensure that only clients from the legitimate terminals and profiles make connections. Any breach of this will be promptly noticed and investigated.

Backup and Recovery procedures on the Post.Trust PKI

All aspects of the configuration of the Post.Trust backup site will be recorded. Backing up the Post.Trust PKI involves making a backup of the important PKI key pairs at PKI creation, backing up important module specific files necessary for private key access (PSE files) and making regular backups of the Oracle database used by the individual PKI components themselves. All procedures involved in the backup process will be recorded.

In the event that backup and recovery procedures come into play, the entire procedures surrounding the restoration of the Post.Trust PKI will be recorded.

System Maintenance and Error detection

As the Post.Trust PKI environment will involve maintenance by appointed system administrators (SAs), all details of maintenance performed on the machines will be recorded. The SAs will also log all error messages detected on any of the designated machines.

Backup of Records/Audit Material

All data recorded as mentioned in the above sections will be backed up. Therefore there will be two copies of all record/audit material, stored in separate locations to protect against disaster scenarios.

4.5.2 Retention Period for Archived Audit Data

All audit material collected (as specified in 4.5.1) will be retained for a period not less than 5 years.

4.5.3 Vulnerability Assessments

The relevant audit data collect shall be regularly analysed by the appointed Post.Trust personnel for any attempts to violate the integrity of any element of the Post.Trust PKI. In the unlikely event that this situation arises it will be quickly detected and acted upon.

4.5.4 Protection of Archived Audit Records

Archives shall be retained and protected against modification or destruction.

4.5.5 Requirement for Time-Stamping of Records

All events that are recorded within Post.Trust Service include the date and time of when the event took place. This date and time are based on the system time on which the CA program is operating. Post.Trust use procedures to review and ensure that all servers within the PKI maintain accurate time.

4.6 KEY CHANGEOVER

Once an issued digital certificate has expired the subscriber may be required to reapply for a new digital certificate in the same manner as they originally applied. The subscriber will be notified in advance of the expiration date and they will be given details as to how they must reapply for their new digital certificate. This process will involve the subscriber obtaining a new private and public key.

Depending on the digital certificate policy chosen by the subscriber, there will be the option to automatically reissue the subscriber with a new digital certificate prior to the expiry date of the original digital certificate. In practice this will mean that the subscriber will automatically receive a new digital certificate which will contain the same public key as before. This will enable the subscriber to still make use of the original key pair with which he/she was issued.

The subscriber will be made fully aware of the key lifetime once they apply for a digital certificate. The subscriber will also be notified as to how they will need to reapply for a new digital certificate once the expiration date has passed. As mentioned in some cases the subscriber will be automatically issued a new digital certificate without any manual intervention.

4.7 COMPROMISE AND DISASTER RECOVERY

Post.Trust have formulated a comprehensive disaster recovery procedure. This process will ensure that the Post.Trust Service will be quickly operational again in the event of computing resources, software, and/or data are corrupted or suspected to be corrupted. This process incorporates a thoroughly tested independent disaster recovery site. The procedures describe how a secure environment is reestablished, from the live site to a backup location within the Post.Trust infrastructure.

In the unlikely event of the Post.Trust Root CAs' private key becoming compromised all Operational CA certificates will be revoked as promptly as is operationally possible. In the event of any of the Post.Trust Operational CAs' private keys becoming compromised then the relevant operational CA certificate will be revoked as promptly as is operationally possible. In the case of any of the above events occurring all digital certificates issued pursuant to the Operation CA Certificate(s) will be revoked.

In the case of a Root CA and therefore all operational CA(s) private keys becoming compromised, a new Root and Operation CA hierarchy will be created and all digital certificates will be reissued. In the event of a single Operation CA private key becoming compromised, only digital certificates issued by this Operation CA will need to be revoked and an alternative Operational CA will reissue each. All new digital certificates will then be automatically republished to the Post.Trust dedicated directory service. During all stages of the disaster recovery procedure the Post.Trust System will remain within a secure environment. There will be no risk that end user personal details will be accessible from an outside source.

4.7.1 If Computing Resources, Software and/or Data become corrupted

The Post.Trust disaster recovery plan incorporates measures to minimise system down time for all critical components of the PKI system, including the hardware, software and keys, in the event of a failure or compromise of one or more of these components.

4.7.2 Post.Trust CA Certificate Lifespan

Each Post.Trust Operational CA Certificate and the Root CA certificate have a certificate lifetime of 10 years. Post.Trust reserve the right to extend the lifetime of the both the Post.Trust Operational CA certificates and the Root CA certificate. It should be noted that the Post.Trust CA private key is protected from compromise with a level Hardware Security Module (HSM) designed to US FIPS 140 level 4 standard.

4.8 CA TERMINATION

In the unlikely event that the Post.Trust operational CA certificate becomes compromised, all interested parties will promptly be made aware of this fact. Post.Trust will take it upon themselves to notify all subscribers via email of the implications of this unlikely event. If such an event occurs the Post.Trust operational CA certificate will be revoked and all issued digital certificates will automatically become revoked.

4.8.1 Private Key Destruction Procedures

All subscribers have an obligation to protect their private keys from compromise. Private keys shall be destroyed in a way that prevents their loss, theft, modification, unauthorised disclosure or unauthorised use. Upon termination of the Post.Trust CA operations, Post.Trust personnel shall destroy the Post.Trust CA private key by deleting, overwriting or physical destruction.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

This section describes the physical, procedural, and personnel security controls of the Post.Trust CA environment.

5.1 PHYSICAL SECURITY CONTROLS

The host site has been designed and built to the An Post strong room standards. An Post drafted the secure site architecture with the help of An Garda Síochana (Irish Police Force) in order to ensure that the best possible protection is maintain at the Post.Trust CA site. This facility is securely protected from unauthorised access by proactive access control alarm systems and surveillance equipment, and employees are only allowed access after being security cleared. A minimum of two people is required to be present to gain access into the secure CA room itself.

5.1.1 Site Location and Construction

The CA site has been constructed with the highest possible security standards in mind. The location can only be accessed by correctly authenticated Post.Trust staff. In addition to this, there are certain areas of the location that require two specific individuals to be authenticated before access is granted.

5.1.2 Physical Access

Post.Trust employees who possess the expert knowledge, experience and qualifications necessary to perform the allocated duties will operate all services.

5.1.3 Power and Air Conditioning

Alternative power sources have been put into place at the Post.Trust CA site. The secure location is also supplied with an air conditioning source.

5.1.4 Fire Prevention and Protection

There have been sufficient fire prevention mechanisms put into place at the Post.Trust CA site. The secure site is supplied with a piped source of halogen gas in order to minimise the risk or damage from fire.

5.1.4 Off-site Backup & Recovery Procedures

The CA and RA Oracle databases shall be replicated at a site different to that in which the CA system resides, to permit restoration in the event of a natural disaster to the primary facility. This back up site is in a separate physical building to the operational site. The off-site back up is a replica of the operational site and will only be used in the event of failure where it will become the operational site. Post.Trust will

engage in regular recovery procedure testing to ensure soundness of the adopted strategies. This testing will take place a minimum of once every six months.

5.2 PROCEDURAL CONTROLS

Procedures are established, documented and implemented for all trusted and administrative roles required to operate the Post.Trust Service. Where possible and appropriate duties associated with Post.Trust specific operations are kept separate from general operations. This is accomplished through the assignment of different staff if possible, and with the use of separate physical and logical access controls.

There are a number of trusted roles assigned to different personnel involved in the operation of Post.Trust operations. These roles have been defined and assigned by senior management and are periodically reviewed as part of the Information Security Management System operated by Post.Trust. These reviews seek to reassign roles if necessary following staff changes or following company reorganization, to ensure no potential security risks exist as a consequence of multiple roles held by individuals, and to ensure that no conflicts of interest exist where staff are assigned multiple roles.

The trusted roles defined for Post.Trust personnel and the policies employed in assigning staff members to these roles are designed to guarantee best practice is maintained in relation to information security, while at the same time providing flexibility required by the business in maximising employee productivity.

5.2.1 Trusted Roles

Post.Trust has designated a number of trusted roles for Certificate Authority operations.

These roles fall under different categories as follows:

Certificate Authority Technical Operation and Support

- Quality Assurance (QA) Management
- Database Administrator
- CA Application Support Engineer
- Operations Support Engineer

Certificate and Registration Authority Administration

- Registration Authority Administrator (RAA)
- Certificate Authority Administrator (CAA)

Hardware Security Module (HSM) Operations

- HSM Operator
- HSM Security Officer
- HSM Key Component Holder

Post.Trust have allocated a number of trusted qualified personnel to each one of the named role types.

The responsibilities of the persons assigned to these roles include:

QA Management

- General management of QA environment and testing principles.
- Ensure integrity of developed software.
- Testing newly developed software prior to sign-off and release into live environment.

Database Administrator

- Standard DBA administration tasks (e.g.: Archiving, Standby and Replicated Database Configuration, Checking Logs, Tuning, Hardening, Security Scanning) for databases used in the CA infrastructure.

Registration Authority Administrator (RAA)

- Collecting registration details from companies seeking to secure digital certificates
- Verifying documentation presented in support of applications
- Point of contact for customer support relating to registration
- Secure storage and care of customer data and documentation used during registration

CA Application Support Engineer

- Expert support in PKI and Cryptography technology used
- Assist in review and design of PKI architecture
- Trouble shooting
- Installation, build, configuration and testing of CA equipment
- Setup and support of local backup and Disaster Recovery infrastructure
- Provide training to other Post.Trust operations staff
- Out of hours on call support

The following responsibilities are carried out under multi person control:

- Root and Operational CA private key generation and PIN storage
- Root and Operational CA private key activation and recovery

Operations Support Engineer

- Carry out scheduled backups of database, logs, files etc.
- Ensure backups are stored securely and cycled correctly according to the policies employed by Post.Trust for offsite storage and tape cycling
- Ensure that integrity of backups are verified periodically and that the Post.Trust data retention policy is adhered to correctly
- Provide trouble shooting and on call out of hours support for common hosting infrastructure supporting Post.Trust operations. This includes networks, firewalls, Intrusion Detection Systems, routers, switches etc.

Certificate Authority Administrator (CAA)

- Digital Certificate generation and secure distribution of all PKI component key pairs within the Root and Operational CA environments

- Generating, distributing, and otherwise managing CRLs
- Administrative functions associated with maintaining the CA and registration databases
- Assisting in incident investigations
- CA event log maintenance and query
- Revocation of Root and/or Operational CA certificates in the unlikely event of this becoming necessary
- Creation of certificate registration policies following management approval
- Monitoring of the entire digital certificate registration process
- Creation and secure storage of the private keys associated with the various CA and RA modules themselves and creation and secure storage of backup copies of the corresponding container files, access passwords and PINs.
- Activation of the various CA and RA modules
- Authentication of certificate requests from the RA (where not handled automatically)
- Passing valid authenticated certificate digital requests to the Operational CA (where not handled automatically)
- Receiving digital certificates back from the Operational CA (where not handled automatically)
- Making available end user key pairs (Private and public key pairs in some cases and certificates only in other cases) available for collection (where not handled automatically).
- The revocation of subscriber digital certificates and/or private key containers (eg: wallets)

HSM Operator

- Change or view network settings for the HSM

HSM Security Officer

The following operations require one security officer:

- Place the HSM online/offline

The following operations require two security officers:

- Backup / Restore of encrypted application keys to/from smartcards
- Backup / Restore of HSM encrypting keys to/from smartcards
- Creation / Removal / Replacement of HSM encrypting keys
- Issue security officer smartcards and PINs
- Backup of security officer smartcards and PINs to secure storage locations
- Erase all keys from the HSM
- Set the HSM real time clock
- Re-initialise the HSM

HSM Key Component Holder

- Custodian of smartcard backups of encrypted application keys and HSM encrypting keys exported in N of M components onto backup smartcards and stored in secure locations.
- Adherence to Post.Trust HSM backup smartcard custody procedures when responding to requests for access to any backup components. These procedures are designed to ensure at least dual control (2 persons) is employed when backups of Root or Operational CA private key backups are requested.
- Custodian of backups of other private key container files, PINs, passwords etc. used in the operation of the CA and held in secure storage locations.

5.2.2 Number of Persons Required per Task

At least two people are assigned to each trusted role to ensure adequate support at all times.

Some roles are assigned to different people to ensure no conflict of interest occurs and to prevent the possibility of accidental or intentional compromise of any component of the CA infrastructure, most especially the Root CA and Operational CA private keys, and customer private keys if held temporarily by Post.Trust during the registration process.

CA key-pair generation and initialisation of each of the CAs (Root and Operational) shall require the active participation of at least two trusted individuals in each case. Such sensitive operations also required the active participation and oversight of senior management.

5.2.3 Identification and Authentication for Each Role

Identification and authentication mechanisms (such as passwords and tokens) are used to control account access for each role. All access by each role to accounts requires password and/or token identification and authentication. Separate accounts and passwords to those used for general operations, will be used for Post.Trust specific equipment and operations. These will be changed periodically in line with the Post.Trust password change policy and procedures.-

5.3 PERSONNEL SECURITY CONTROLS

Post.Trust employees who possess the expert knowledge will operate all services, experience and qualifications necessary to perform allocated duties. In accordance with the requirements for specific duties, employees undergo An Post security clearance prior to being granted permission to partake in the service and or related operations.

5.3.1 Background, Qualifications, Experience, and Clearance Requirements

Personnel appointed to the trusted roles will be chosen in accordance with An Post hiring practices for positions of this sensitivity.

Personnel in key operational positions will:

- Not be assigned other duties that may conflict with their duties and responsibilities;
- Not as far as is known have been previously relieved of a past assignment for reasons of negligence or non-performance of duties;
- Have received proper training in the performance of their duties.
- Be aware of disciplinary measures for breaches of security controls/processes.

5.3.2 Background Check Procedures

Background checks shall be carried out and staff fulfilling sensitive roles shall be formally appointed. Staff shall not take up their duties until any such vetting/clearance process has been completed.

6. TECHNICAL SECURITY CONTROLS

The Post.Trust CA private keys are protected within a hardware security module ("HSM"). The use of a HSM, with FIPS-140 level 4 capabilities ensures that Post.Trust are adhering to the highest industry standard regarding the generation and protection of the Operational and Root CAs' private keys. Access to the modules within the Post.Trust environment including the Root and Operational CAs' private keys are restricted by the use of token/smartcards and associated pass phrases. These smartcards and pass phrases are allocated among the multiple members of the Post.Trust management team. Such allocation ensures that no one member of the team holds total control over any component of the system.

6.1 KEY GENERATION

6.1.1 Key pair generation

Post.Trust will retain the right to generate the subscriber's public and private key pair. The subscriber will be required to provide all the necessary identification and authentication information when the digital certificate is being requested. Once all the registration information is collected by the Post.Trust CA system the subscribers public and private key pair are generated within a secure environment. Post.Trust will also offer the facility to allow subscribers to generate their own private key prior to submitting of a digital certificate request. This service will involve the subscribers generating their own private key pair and submitting a digital certificate request direct to the Post.Trust Service. Post.Trust subscribers will be made fully aware of how to avail of the services on offer and how that can apply for the various digital certificates on offer.

6.1.2 Post.Trust CA Private Key Distribution Service

Once the subscriber certificate request has been signed by the Post.Trust CA system the subscriber's digital certificate and private key will be distributed via a secure channel whereby only the subscriber will have access to his/her private key. Refer to Appendix A for the various methods of distribution.

6.1.3 Certificate delivery to certificate requester

The digital certificate will be delivered to the subscriber in one of the defined methods as specified in Appendix A.

6.1.4 Access to Post.Trust CA Certificate to End Users

The Post.Trust CA certificate will be made available to the general public from the dedicated Post.Trust LDAP directory service. It is also available from the Post.Trust Web site for download.

6.1.5 Key sizes

The key length of the Post.Trust CA modules (both Root and Operational CAs) will be 2048 bit. The key sizes issued to subscribers will depend on the digital certificate policy chosen by the subscriber. There are a

number of digital certificate policies in place within the Post.Trust CA environment and each one documents the key size. The Post.Trust CA will primarily be issuing 1024 and 2048 bit key pairs. The Root CA is a 2048 bit Key.

6.1.5.1 Review of Private Key Usage Periods

The operational periods for new certificates will be reviewed on an on going basis and shall be based on forecasts of new technology developments. Both operating system and browser version developments will be carefully monitored when reviewing usage periods for private keys.

6.1.6 Hardware/Software Key Generation

Initially the subscriber key generation process will take place in software. This will mean that for each digital certificate request received by the Post.Trust Service the subscriber will be issued with a PKCS#12 file which consists of the private key and certificate in a Triple DES encrypted file format. The Post.Trust subscribers may in the future be given the option to have their private key generated on a hardware device such as a smartcard.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for Cryptographic Module

The generation and maintenance of both the Root and Operational CAs' private keys are facilitated through the use of an advanced cryptographic device known as a HSM (Hardware Security Module). The HSM used in the case of the Post.Trust CAs' is designed to provide FIPS-140 Level 4 security standards in both the generation and the maintenance in all Root and Operational CA private keys.

6.2.2 Private Key Escrow

Subscriber may be escrowed on behalf of the subscriber. This service will be provided to the subscriber in order that they can recover their private key in case of loss or damage. This facility will only be applicable for encryption keys and will not be available for signing keys. This will be offered as an extra service to the Post.Trust subscribers.

6.2.3 Method of Activating Private Key

The activation of the Post.Trust CA private key pair requires more than one person. The activation procedure will require the relevant persons, to possess between them, a series of smart cards and pass phrases to unlock the Post.Trust CA private key.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Usage periods for the public and private keys

The Post.Trust CA private key will have a key validity period of 10 years. Post.Trust retains the right to extend the validity period of the Post.Trust CA certificate. The validity period of subscriber certificates will

be dependent on the class of digital certificate in question. Refer to Appendix B for details of the various validity periods.

6.4 LIFE CYCLE TECHNICAL SECURITY CONTROLS

6.4.2 Security management controls

The Post.Trust CA environment will adhere to best practices in relation to security controls. The objective will be to ensure that these computer systems have the minimum number of accounts required, use passwords which meet the required policy, have only the required network services enabled, and have appropriate discretionary access controls on all security-relevant directories and files.

6.5 NETWORK SECURITY CONTROLS

The Post.Trust CA and RA environments will be accessed through a secure DMZ environment. These firewall rules are configured to allow the minimal amount of connectivity. Only those protocols identified as being necessary to accomplish the CA or RA functions shall be allowed to pass through; all others will be disabled.

7. CERTIFICATE AND CRL PROFILES

All digital certificates issued by the Post.Trust Service comply with digital certificate and CRL profiles as described in RFC 2459.

7.1 CERTIFICATE PROFILE

The Post.Trust operational CA certificate(s) is signed by the Post.Trust Root CA entity. The Root CA acts as the source of trust within the Post.Trust PKI. The Root CA will sign all operational Post.Trust CA entities.

To ensure global compatibility and conformity to public key standards, the Post.Trust CA will utilize the ITU-T X.509 version 3 digital certificate standard.

For a detailed description of the Post.Trust CA certificate profile refer to Appendix C.

7.2 CRL PROFILE

To ensure global compatibility and conformity to public key standards, Post.Trust CA will utilise the ITU-T X.509 version 2 Certificate Revocation List standard. An X.509 version 2 CRL contains a signed list of digital certificates that have been revoked with the date and other useful information used in the certificate verification process.

8. SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

8.1.1 Items that can change without notification

The only changes that may be made to this specification without notification are editorial or typographical corrections, or changes to the contact details.

8.1.2 Changes with notification

8.1.2.1 List of items

- (a) Any item in this certificate policy statement may be changed with 45 days notice.
- (b) Changes to items which, in the judgement of the policy administration organisation, will not materially impact a substantial majority of the subscribers or relying parties using this policy may be changed with 15 days notice.

8.1.2.2 Notification mechanism

All notification of changes to this document shall be made via the Post.Trust Web site.

8.1.2.3 Comment period

Impacted subscribers **and relying parties** may file comments with the policy administration organisation as follows:

- For changes in accordance with (a) of 8.1.2.1, comments shall be received within 30 days of original notice.
- For changes in accordance with (b) of 8.1.2.1, comments shall be received within 10 days of original notice.

8.1.2.4 Mechanism to handle comments

Any action taken as a result of comments filed in accordance with 8.1.2.3 is at the sole discretion of the Post.Trust elected committee.

8.1.2.5 Period for final change notice

If the proposed change is modified as a result of comments pursuant to 8.1.2.2 and 8.1.2.3, notice of the modified proposed change shall be given, in accordance with 8.1.2.1, at least 10 days prior to the change taking effect.

8.1.3 Items whose change requires a new policy

If a policy change is determined to have a material impact on a significant number of subscribers **and relying parties** of the policy, Post.Trust may, at its sole discretion, assign a new object identifier to the modified policy.

8.2 CPS APPROVAL PROCEDURES

The following bodies will verify the CPS approval procedure

- The An Post Legal Dept
- The An Post Company Solicitors

APPENDIX A - REGISTRATION, CERTIFICATION AND DELIVERY

The procedure which Post.Trust follows for registration, certificate generation, and certificate distribution is described below for each type of certificate issued. Please note that the precise registration process and types of information gathered can vary from that described below depending on the specific application and customer requirements. Additionally specific certificate policies and Post.Trust liability arrangements not described here may be drawn up under contract for individual customers.

Certificate CATEGORY: Post.Trust Server SSL Certificates

INITIAL REGISTRATION
<p>An organisation applying for a Post.Trust SSL Server Certificate must complete a Post.Trust SSL Certificate Registration form.</p> <p>The following information needs to be provided during the registration process:</p> <ul style="list-style-type: none"> ✓ Company or Organisation Name ✓ Company Registration Number or Other Official Organisation Identifier ✓ Organisation Address ✓ Domain name ✓ Contact Name ✓ Contact Title ✓ Contact Phone Number ✓ Contact Email Address ✓ Certificate Signing Request generated on the Web server requiring the certificate <p>During the registration process, it is a requirement for the applicant to accept a certificate subscriber agreement. This details the terms and conditions under which the certificate is being supplied including the subscriber's obligations.</p>
IDENTIFICATION AND AUTHENTICATION
<p>It is mandatory during the registration process for the organisation information provided to be verified by Post.Trust. Therefore the organisation will be asked to submit a number of documents to aid in the verification process. The documents may include the following:</p> <ul style="list-style-type: none"> ✓ Relevant document providing proof of organisation registration ✓ Relevant document providing proof of domain registration ✓ A request for a Post.Trust Certificate on company or organisation headed paper, signed by a senior manager or director. ✓ A letter on company or organization headed paper nominating the employee as the designated contact. <p>Post.Trust may at its discretion take steps to verify the documentation received, for example it may:</p> <ul style="list-style-type: none"> ✓ Verify company details provided with the Companies Registration Office

<ul style="list-style-type: none"> ✓ Verify domain details with the relevant Domain Registration Authority ✓ Contact management of the applicant organization to authenticate requests for certificates. <p>The Post.Trust Registration Authority Administrator (RAA) will verify the information supplied and is the person with the final authority to permit a certificate application to proceed to completion.</p>
REGISTRATION COMPLETION
<p>All registration details provided and the Certificate Signing Request generated by the Web server will be stored on the Post.Trust registration database as soon as they are received.</p> <p>These details will remain on the registration database while any verification is being completed.</p> <p>Following successful completion of the verification phase, the certificate request is flagged as ready for processing.</p>
CERTIFICATE GENERATION
<p>All successful certificate requests will be processed by the Post.Trust Operation CA. The CA will apply to the certificate request:</p> <ul style="list-style-type: none"> ✓ A unique serial number ✓ Operational CA's signature
CERTIFICATE DELIVERY
<p>Following the certification process, the server SSL certificate may be distributed to the customer via one of the following media:</p> <ul style="list-style-type: none"> ✓ Download over the Internet ✓ CD or Floppy Disk ✓ E-mail <p>The subscriber, end user or relying party should ensure that the certificate received was indeed issued by the Post.Trust operational CA by verifying the thumbprint of the issuing CA certificate against that published for the Post.Trust Operational CA at www.post.trust.ie/reposit/rootcert.html.</p>

Certificate CATEGORY: Post.Trust Employee Class A Certificates

INITIAL CRA REGISTRATION
<p>An organisation applying for a set of digital certificates for its employees can do so by following the procedure below.</p> <p>Within each organisation one or more CRAs (Company Registration Administrators) are appointed. These people are responsible for applying to Post.Trust for batches of certificates, collecting personal details for each employee for whom a certificate is required, ensuring that the information supplied is correct, and supplying the information collected to the Post.Trust Registration Authority Administrator (RAA).</p> <p>During the registration process, it is a requirement for an applicant to accept a certificate subscriber agreement. This details the terms and conditions under which the certificate is being supplied including the subscriber's obligations.</p> <p>A CRA initially enters the batch registration page on a secure and private area of the Post.Trust Web site and supplies the following information:</p> <ul style="list-style-type: none"> ✓ CRA Name ✓ No. of Certificates Required ✓ Company or Organisation Name ✓ Department Name ✓ Email Address ✓ Organisation Address ✓ Company Registration Number or other Official Organisation Identifier ✓ CRA Passport Number or Driving Licence Number and/or PPS Number <p>A batch of employee certificate application identifiers are then assigned to the CRA. These identifiers are distributed to the employees within the organization for whom the CRA is responsible in relation to the Post.Trust registration process.</p>
EMPLOYEE REGISTRATION
<p>The employee registration process requires each employee to supply his or her personal registration details online. The first field on the registration page is filled with the unique employee certificate application identifier provided by the CRA. The following personal details are then required (Some will be pre-populated):</p> <ul style="list-style-type: none"> ✓ Employee Name ✓ Company or Organisation Name ✓ Department ✓ Email Address ✓ The relevant CRA ✓ Organisation Address ✓ Company Registration Number or other Official Organisation Identifier ✓ Employee Passport Number or Driving Licence Number and/or PPS Number <p>The Post.Trust RAA will verify the information entered by each employee against the corresponding documentation supplied by the CRA. The RAA is the person with the final authority to permit a certificate application to proceed to completion.</p>

CERTIFICATION GENERATION
<p>All successful certificate requests will be processed by the Post.Trust Operation CA. The CA will apply to the certificate request:</p> <ul style="list-style-type: none">✓ A unique serial number✓ Operational CA's signature
CERTIFICATE DELIVERY
<p>Following the certification process, the certificate may be distributed via one of the following media:</p> <ul style="list-style-type: none">✓ Download over the Internet✓ CD/Floppy Disk✓ Smart Card or other secure hardware token✓ E-mail <p>If a private key was also generated centrally by Post.Trust for an employee, this will be distributed in a secure key container such as a PKCS#12 file or Arcot Wallet (www.arcot.com). The method of distribution will typically mirror that of the certificate.</p> <p>The subscriber, end user or relying party should ensure that the certificate received was indeed issued by the Post.Trust operational CA by verifying the thumbprint of the issuing CA certificate against that published for the Post.Trust Operational CA at www.post.trust.ie/reposit/rootcert.html. Where a private key container is also issued, the user application which accesses the key should verify that the key matches the corresponding certificate issued and verified above.</p>

Certificate CATEGORY: Post.Trust Client Signing, Encryption and Authentication Qualified Certificates

Please note that where a certificate is issued as a Qualified Certificate within the meaning of EU Directive 199/93/EC, the individual applying for the certificate must undergo a face to face identify verification procedure.

The procedure below assumes an application by a company or organisation on behalf of its employees for qualified certificates (similar to Employee Class A Certificates).

Qualified certificates may also be applied for in other circumstances such as by customers of an organisation (business or consumer) with whom Post.Trust has a contract to supply certificates. In these situations a somewhat modified approach to that described below may be used however there will be no deviation from the basic requirement for rigorous identity verification.

INITIAL CRA REGISTRATION
<p>An organisation applying for a set of qualified digital certificates for its employees can do so by following the procedure below:</p> <p>Within each organisation one or more CRAs (Company Registration Administrators) will be appointed. These people are responsible for applying to Post.Trust for batches of certificates, collecting personal details for each employee for whom a certificate is required, ensuring that the information supplied is correct, and supplying the information collected to the Post.Trust central Registration Authority Administrator (RAA).</p> <p>During the registration process, it is a requirement for an applicant to accept a certificate subscriber agreement. This details the terms and conditions under which the certificate is being supplied including the subscriber's obligations.</p> <p>A CRA may also be responsible for ensuring that the identity of the applicant is proven by conducting a face-to-face identify verification with the applicant against a passport or driving licence. Alternatively an applicant may present themselves at one of a designated number of Post Offices nationwide where a Post Office clerk will conduct the face-to-face identity verification.</p> <p>If a CRA requires a qualified digital certificate, he or she must physically present himself or herself to the Post.Trust Registration Authority Administrator (RAA) for identity verification.</p> <p>A CRA initially enters the batch registration page on the Post.Trust Web site and supplies the following information:</p> <ul style="list-style-type: none"> ✓ CRA Name ✓ No. of Certificates Required ✓ Company or Organisation Name ✓ Department Name ✓ Email Address ✓ Organisation Address

<ul style="list-style-type: none"> ✓ Company Registration Number or other Official Organisation Identifier ✓ CRA Passport Number or Driving Licence Number and/or PPS Number <p>A batch of employee certificate application identifiers are then assigned to the CRA. These identifiers are distributed to the employees within the organization for whom the CRA is responsible in relation to the Post.Trust registration process.</p>
EMPLOYEE REGISTRATION
<p>The employee registration process requires each employee to supply his or her personal registration details online. The first field on the registration page is filled with the unique employee certificate application identifier provided by the CRA. The following personal details are then required (Some will be pre-populated):</p> <ul style="list-style-type: none"> ✓ Employee Name ✓ Company or Organisation Name ✓ Department ✓ Email Address ✓ The relevant CRA ✓ Organisation Address ✓ Company Registration Number or other Official Organisation Identifier ✓ Employee Passport Number or Driving Licence Number and/or PPS Number <p>An employee must present himself or herself in front of a CRA or attend one of a number of designated Post Offices nationwide for face-to-face identity verification. Documentation supporting the applicant's identity must be also supplied at this point, copies of which will be forwarded by the CRA or Post Office to the Post.Trust RAA.</p> <p>The Post.Trust RAA will verify the information entered by each employee against the corresponding documentation supplied by the CRA or Post Office. The RAA is the person with the final authority to permit a certificate application to proceed to completion.</p>
CERTIFICATION GENERATION
<p>All successful certificate applications will be processed by the Post.Trust Operational CA. The CA will apply to the certificate request:</p> <ul style="list-style-type: none"> ✓ A unique serial number ✓ Operational CA's signature
CERTIFICATE DELIVERY
<p>Following the certification process, the certificate may be distributed via one of the following media:</p> <ul style="list-style-type: none"> ✓ CD/Floppy Disk ✓ Smart Card or other secure hardware token <p>Other methods are possible provided that a secure delivery channel from Post.Trust to the certificate recipient can be guaranteed.</p> <p>If a private key was also generated centrally by Post.Trust for the employee, this will be distributed in a secure key container such as a PKCS#12 file or Arcot Wallet (www.arcot.com). The method of distribution will typically mirror that of the certificate.</p> <p>The subscriber, end user or relying party should ensure that the certificate received was indeed issued by the Post.Trust operational CA by verifying the thumbprint of the issuing CA certificate against that published for the Post.Trust Operational CA at</p>

www.post.trust.ie/repokit/rootcert.html. Where a private key container is also issued, the user application which uses the key should verify that the key matches the corresponding certificate issued and verified above.

Certificate CATEGORY: Post.Trust Qualified Document Signing Certificates

Please note that where a certificate is issued as a Qualified Certificate within the meaning of EU Directive 199/93/EC, the individual applying for a Post.Trust Qualified Document Signing certificate must undergo a face to face identify verification procedure.

The procedure below assumes an application by a company or organisation on behalf of its employees for qualified certificates.

Qualified certificates may also be applied for in other circumstances such as by customers of an organisation (business or consumer) with whom Post.Trust has a contract to supply certificates. In these situations a somewhat modified approach to that described below may be used however there will be no deviation from the basic requirement for rigorous identity verification.

REGISTRATION PROCESS
<p>An organisation applying for a Post.Trust Qualified Document Signing Certificates for its employees can do so by following the procedures below.</p> <p>Where the organisation requirements are for a small batch of certificates, Post.Trust can process the registration details of each individual employee and conduct the face-to-face identity verification process directly.</p> <p>Such applicants must physically present himself or herself to the Post.Trust Registration Authority Administrator (RAA) for identity verification.</p> <p>Where the organisation requirements are deemed to be for a large batch of certificates, Post.Trust will appoint one or more CRAs (Company Registration Administrators) to the trusted role of processing registration details of each individual employee, conducting a face-to-face identity verification process and ensuring that each applicant accepts and signs the relevant Post.Trust Qualified Document Signing Certificate Subscriber Agreement.</p> <p>CRAs are responsible for applying to Post.Trust for batches of certificates, collecting personal details for each employee for whom a certificate is required, ensuring that the information supplied is correct, and supplying the information collected to the Post.Trust central Registration Authority Administrator (RAA).</p> <p>CRAs may also be responsible for ensuring that the identity of the applicant is proven by conducting face-to-face identify verification with the applicant against a passport or driving license.</p> <p>During the registration process, it is a requirement for a senior member of the organizations management to accept and sign a Qualified Document Signing Certificate Organisation Agreement. This agreement details some of the terms and conditions under which the certificate is being supplied, including the subscriber’s obligations.</p>
CRA REGISTRATION
<p>The CRA registration process requires each CRA to supply their personal registration details in person to a Post.Trust RAA. The following personal details are required:</p>

- ✓ Company or Organisation Name
- ✓ Organisation Registered Office and principle place of business
- ✓ Company Registration Number or other Official Organisation Identifier
- ✓ Nominated CRA Name
- ✓ Nominated CRA Job Title
- ✓ Nominated CRA Contact Address
- ✓ Email Address
- ✓ Employee Passport Number or Driving Licence Number and/or PPS Number

A letter of authorisation on company headed paper is required from a senior member of the organisations management confirming that the CRA is authorized to act as a CRA on behalf of the organisation.

A nominated CRA must present himself or herself in person to a Post.Trust RAA for face-to-face identity verification. Documentation supporting the applicant's identity must be also supplied at this point.

During the face-to-face process the CRA must agree to and sign a Post.Trust Qualified Document Signing Certificate Subscriber Agreement.

Post.Trust RAA will verify the information from the corresponding documentation supplied. The RAA is the person with the final authority to permit a certificate application to proceed to completion.

EMPLOYEE REGISTRATION

The employee registration process requires each employee to supply their personal registration details to the Post.Trust RAA or the authorized company CRA. The following personal details are required:

- ✓ Employee Name
- ✓ Employee Job Title
- ✓ Employee Contact Address
- ✓ Company or Organisation Name
- ✓ Department
- ✓ Email Address
- ✓ Nominated CRA Name
- ✓ Official Organisation Address
- ✓ Company Registration Number or other Official Organisation Identifier
- ✓ Employee Passport Number or Driving Licence Number and/or PPS Number

An employee must present himself or herself to a RAA or a CRA for face-to-face identity verification. Documentation supporting the applicant's identity must also be supplied at this point. Where the nominated CRA conducts the fact-to-face process, copies of presented documents will be verified and countersigned and will be forwarded by the CRA to the Post.Trust RAA.

During the fact-to-face process the employee must agree to and sign a Post.Trust Qualified Document Signing Certificate Subscriber Agreement.

The Post.Trust RAA will verify the information entered by each employee or CRA on behalf of each employee. The RAA is the person with the final authority to permit a certificate application to proceed to completion.

CERTIFICATION GENERATION

All successful certificate applications will be processed by the Post.Trust operation CA. The CA will apply to the certificate request:

A unique serial number
Operational CA's signature

CERTIFICATE DELIVERY

Following the certification process, the certificate may be distributed via one of the following media:

- ✓ CD/Floppy Disk
- ✓ Smart Card or other secure hardware token

Other methods are possible provided that a secure delivery channel from Post.Trust to the certificate recipient can be guaranteed.

If a private key was also generated centrally by Post.Trust for the employee, this will be distributed in a secure key container such as a PKCS#12 file.

The subscriber, end user or relying party should ensure that the certificate received was indeed issued by the Post.Trust Operational CA by verifying the thumbprint of the issuing CA certificate against that published for the Post.Trust operational CA at www.post.trust.ie/reposit/rootcert.html.

Where a private key container is also issued, the user application which uses the key should verify that the key matches the corresponding certificate issued and verified above.

Certificate CATEGORY: Post.Trust Client SSL Authentication Certificates

INITIAL REGISTRATION
<p>An organisation wishing to apply for one or more client SSL certificates for authentication purposes may do so by following the procedure below.</p> <p>A contact person representing the organisation is responsible for applying to Post.Trust for batches of certificates. This person collects details required for each client certificate required, and supplies the information collected to the Post.Trust central Registration Authority Administrator (RAA).</p> <p>It is not normally a requirement that the information collected is verified by the Post.Trust RAA where the certificates are for use exclusively within an organisation, although it is expected that the CRA will have verified that the information supplied is correct. Where the purpose of the certificates is to identify employees, machines or other entities within an organisation to a person, machine or entity outside the organisation, then more stringent verification of identity information is required.</p> <p>During the registration process, it is a requirement for an applicant to accept a certificate subscriber agreement. This details the terms and conditions under which the certificate is being supplied including the subscriber's obligations.</p> <p>SSL client certificates may be applied for in the name of an individual or a role name. In either case the common name applied to the certificate must be unique.</p> <p>The information required of the applicant organisation must be supplied to the RAA in electronic form. This may be in a file or through use of the Post.Trust Internet registration system.</p>
REGISTRATION PROCESS
<p>The information required to apply for an SSL client certificate may include:</p> <ul style="list-style-type: none"> ✓ Person or Role Name ✓ Organisation Name ✓ Department ✓ Email Address ✓ Name of contact for organisation ✓ Organisation Address <p>The RAA may populate the Post.Trust registration database directly using the data supplied by the applicant organisation or may require that the Internet registration system be used. This will depend on the nature of the application for which the certificates are intended and the agreement between Post.Trust and the applicant organisation.</p>
CERTIFICATION GENERATION
<p>All successful certificate requests will be processed by the Post.Trust Operation CA. The CA will apply to the certificate request:</p> <ul style="list-style-type: none"> ✓ A unique serial number ✓ Operational CA's signature

CERTIFICATE DELIVERY

Following the certification process, the server certificate may be distributed via one of the following media:

- ✓ Download over the Internet
- ✓ CD/Floppy Disk
- ✓ Smart Card or other secure hardware token.
- ✓ E-mail

If a private key was also generated centrally by Post.Trust for the employee, this will be distributed in a secure key container such as a PKCS#12 file or Arcot Wallet (www.arcot.com). The method of distribution will typically mirror that of the certificate.

The subscriber, end user or relying party should ensure that the certificate received was indeed issued by the Post.Trust operational CA by verifying the thumbprint of the issuing CA certificate against that published for the Post.Trust Operational CA at www.post.trust.ie/reposit/rootcert.html. Where a private key container is also issued, the user application which uses the key should verify that the key matches the corresponding certificate issued and verified above.

APPENDIX B - DIGITAL CERTIFICATE PROFILE DETAILS

This appendix describes the various classes of digital certificate that Post.Trust issues, and the limitations on liability in respect of each of these. The profile of each digital certificate type is also detailed. Note that the specific details described in each certificate profile may vary in any implementation from those described below.

Post.Trust Server SSL Certificate Profile Details

Limited Liability

Post.Trust shall be liable to subscribers or relying parties for direct loss arising from any breach of this CPS or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to an aggregated maximum limit of **€63,500** for any one event or series of related events (in any one twelve month period). Post.Trust shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of this CPS, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term “loss” means a partial loss or reduction in value as well as a complete or total loss.

Field	Content
X.509v1 Field	
Version	v3
Serial Number	Allocated automatically by issuing CA
Signature Algorithm	SHA-1 with RSA Signature
Issuer Distinguished Name	
Country (C)	IE
Organisation (O)	An Post
Organisational Unit (OU)	Post.Trust Ltd.
Common Name (CN)	Post.Trust Operational CA
Validity Period	365 days
Subject	
Country (C)	User Entry
Organisation (O)	Company or Organisation Name – User Entry
Organisational Unit (OU)	Post.Trust Server Certificate
Common Name (CN)	Server URL – User Entry
Subject Public Key Info	Public key encoded in accordance with RFC2459 & PKCS#1
X.509v3 Key Details and Extensions	
Key Size & Algorithm	512 bit or 1024 bit RSA
Key Usage	
Digital Signature	Selected
Non Repudiation	Selected
Key Encipherment	Selected
Data Encipherment	Selected
Key Agreement	Selected
Key Certificate Signature	Selected
CRL Signature	Selected

Field	Content
Extended Key Usage	
2.2.1 Server Authentication	Selected
Certificate Policies	
Policy Identifier OID	1.2.372.980002.2.1.1.1
Policy Notice	http://www.post.trust.ie/reposit/cps.html
Policy Qualifier	This certificate is issued subject to the Post.Trust CPS terms and conditions. By accepting this certificate a relying party is acknowledging acceptance of the terms and conditions.

Post.Trust Employee Class A Profile Details

Limited Liability

Post.Trust shall be liable to subscribers or relying parties for direct loss arising from any breach of this CPS or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to an aggregated maximum limit of **€63,500** for any one event or series of related events (in any one twelve month period). Post.Trust shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of this CPS, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term “loss” means a partial loss or reduction in value as well as a complete or total loss.

Field	Content
X.509v1 Field	
Version	v3
Serial Number	Allocated automatically by issuing CA
Signature Algorithm	SHA-1 with RSA Signature
Issuer Distinguished Name	
Country (C)	IE
Organisation (O)	An Post
Organisational Unit (OU)	Post.Trust Ltd.
Common Name (CN)	Post.Trust Operational CA
Validity Period	
Cert Start Date	DD/MM/YYYY-hh:mm:ss
Cert End Date	DD/MM/YYYY-hh:mm:ss
Subject	
Country (C)	IE
Organisation (O)	Employee Organisation
Organisational Unit (OU)	Post.Trust Class A Employee Certificate
Organisational Unit (OU)	Employee Department
Common Name (CN)	Employee Name
Subject Public Key Info	Public key encoded in accordance with RFC2459 & PKCS#1
X.509v3 Key Details and Extensions	
Key Size & Algorithm	1024 bit RSA
Key Usage	Digital Signature, Non-Repudiation, Data Encipherment(d0)
Enhanced Key Usage	Secure Email(1.3.6.1.5.5.7.3.4) Time Stamping(1.3.6.1.5.5.7.3.8) Microsoft Trust List Signing(1.3.6.1.4.1.311.10.3.1) Encrypting File System(1.3.6.1.4.1.311.10.3.4)
Subject Alternative Name	Client eMail Address
Certificate Policies	
Policy Identifier OID	1.2.372.980002.2.1.1.2
Policy Notice	http://www.post.trust.ie/reposit/cps.html
Policy Qualifier	This certificate is issued subject to the Post.Trust CPS terms and conditions. By accepting this certificate a relying party is acknowledging acceptance of the terms and conditions.

Post.Trust Client Authentication SSL Certificate Profile Details

Limited Liability

Post.Trust shall be liable to subscribers or relying parties for the direct loss arising from any breach of this CPS or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to an aggregated maximum limit of €63,500 for any one event or series of related events (in any one twelve month period). Post.Trust shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of this CPS, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term “loss” means a partial loss or reduction in value as well as a complete or total loss.

Field	Content
X.509v1 Field	
Version	v3
Serial Number	Allocated automatically by issuing CA
Signature Algorithm	SHA-1 with RSA Signature
Issuer Distinguished Name	
Country (C)	IE
Organisation (O)	An Post
Organisational Unit (OU)	Post.Trust Ltd.
Common Name (CN)	Post.Trust Operational CA
Validity Period	
Cert Start Date	DD/MM/YYYY-hh:mm:ss
Cert End Date	DD/MM/YYYY-hh:mm:ss
Subject	
Organisational Unit (OU)	Client Supplied
Common Name (CN)	Client Supplied
Email (E)	Client Supplied
Organisation (O)	Client Supplied
Certificate Policies	
Policy Identifier OID	1.2.372.980002.2.1.1.3
Policy Notice	http://www.post.trust.ie/reposit/cps.html
Policy Qualifier	This certificate is issued subject to the Post.Trust CPS terms and conditions. By accepting this certificate a relying party is acknowledging acceptance of the terms and conditions.

Post.Trust Qualified Encryption Certificate Profile Details

Limited Liability

Post.Trust shall be liable to subscribers or relying parties for direct loss arising from any breach of this CPS or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to an aggregated maximum limit of €63,500 for any one event or series of related events (in any one twelve month period). Post.Trust shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of this CPS, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term “loss” means a partial loss or reduction in value as well as a complete or total loss.

Field	Content
X.509v1 Field	
Version	v3
Serial Number	Allocated automatically by issuing CA
Signature Algorithm	SHA-1 with RSA Signature
Issuer Distinguished Name	
Country (C)	IE
Organisation (O)	An Post
Organisational Unit (OU)	Post.Trust Ltd.
Common Name (CN)	Post.Trust Operational CA
Validity Period	2 Years
Cert Start Date	DD/MM/YYYY-hh:mm:ss
Cert End Date	DD/MM/YYYY-hh:mm:ss
Subject	
Country (C)	IE
Organisation (O)	Client Organisation Name
Organisational Unit (OU)	Post Trust Encryption
Organisational Unit (OU)	Optional Client Supplied Identifier
Organisational Unit (OU)	Post.Trust Unique Identifier
Common Name (CN)	Person's Name
Subject Public Key Info	Public key encoded in accordance with RFC2459 & PKCS#1
X.509v3 Key Details and Extensions	
Key Size & Algorithm	1024 bit RSA
Key Usage	Key Encipherment (20)
Extended Key Usage	Secure Email (1.3.6.1.5.5.7.3.4)
Subject Alternative Name	RFC822 Name=Client email Address
Certificate Policies	
Policy Identifier OID	1.2.372.980002.2.1.1.4
Policy Notice	http://www.post.trust.ie/reposit/cps.htm
Policy Qualifier	This certificate is issued subject to the Post.Trust CPS terms and conditions. By accepting this certificate a relying party is acknowledging acceptance of the terms and conditions.

Post.Trust Qualified Signing Certificate Profile Details

Limited Liability

Post.Trust shall be liable to subscribers or relying parties for the direct loss arising from any breach of this CPS or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to an aggregated maximum limit of **€63,500** for any one event or series of related events (in any one twelve month period). Post.Trust shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of this CPS, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term “loss” means a partial loss or reduction in value as well as a complete or total loss.

Field	Content
X.509v1 Field	
Version	v3
Serial Number	Allocated automatically by issuing CA
Signature Algorithm	SHA-1 with RSA Signature
Issuer Distinguished Name	
Country (C)	IE
Organisation (O)	An Post
Organisational Unit (OU)	Post.Trust Ltd.
Common Name (CN)	Post.Trust Operational CA
Validity Period	
Cert Start Date	DD/MM/YYYY-hh:mm:ss
Cert End Date	DD/MM/YYYY-hh:mm:ss
Subject	
Country (C)	IE
Organisation (O)	Client Company Name
Organisational Unit (OU)	Post Trust Signing
Organisational Unit (OU)	Optional Client Supplied Identifier
Organisational Unit (OU)	Post.Trust Unique Identifier
Common Name (CN)	Person's Name
Subject Public Key Info	Public key encoded in accordance with RFC2459 & PKCS#1
X.509v3 Key Details and Extensions	
Key Size & Algorithm	1024 bit RSA
Key Usage	Digital Signature, Non-Repudiation(c0)
Extended Key Usage	Secure Email(1.3.6.1.5.5.7.3.4)
Subject Alternative Name	RFC822 Name=Client email Address
Certificate Policies	
Policy Identifier OID	1.2.372.980002.2.1.1.5
Policy Notice	http://www.post.trust.ie/reposit/cps.htm
Policy Qualifier	This certificate is issued subject to the Post.Trust CPS terms and conditions. By accepting this certificate a relying party is acknowledging acceptance of the terms and conditions.

Post.Trust Qualified Authentication Certificate Profile Details

Limited Liability

Post.Trust shall be liable to subscribers or relying parties for the direct loss arising from any breach of this CPS or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to an aggregated maximum limit of €63,500 for any one event or series of related events (in any one twelve month period). Post.Trust shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of this CPS, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term “loss” means a partial loss or reduction in value as well as a complete or total loss.

Field	Content
X.509v1 Field	
Version	v3
Serial Number	Allocated automatically by issuing CA
Signature Algorithm	SHA-1 with RSA Signature
Issuer Distinguished Name	
Country (C)	IE
Organisation (O)	An Post
Organisational Unit (OU)	Post.Trust Ltd.
Common Name (CN)	Post.Trust Operational CA
Validity Period	
Cert Start Date	DD/MM/YYYY-hh:mm:ss
Cert End Date	DD/MM/YYYY-hh:mm:ss
Subject	
Country (C)	IE
Organisation (O)	Post.Trust
Organisational Unit (OU)	Post Trust Authentication
Organisational Unit (OU)	Post.Trust Unique Identifier
Common Name (CN)	Client Name
Organisational Unit (OU)	Account Reference Number
Subject Public Key Info	Public key encoded in accordance with RFC2459 & PKCS#1
X.509v3 Key Details and Extensions	
Key Size & Algorithm	1024 bit RSA
Key Usage	Digital Signature (80)
Enhanced Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2)
Certificate Policies	
Policy Identifier OID	1.2.372.980002.1.1.6
Policy Notice	http://www.post.trust.ie/reposit/cps.htm
Policy Qualifier	This certificate is issued subject to the Post.Trust CPS terms and conditions. By accepting this certificate a relying party is acknowledging acceptance of the terms and conditions.

Post.Trust Qualified Document Signing Certificate Profile Details

Limited Liability

Post.Trust shall be liable to subscribers or relying parties for the direct loss arising from any breach of this CPS or for any other liability it may incur in contract, tort or otherwise, including liability for negligence up to an aggregated maximum limit of **€63,500** for any one event or series of related events (in any one twelve month period). Post.Trust shall not in any event be liable for any loss of profits, loss of sales or turnover, loss or damage to reputation, loss of contracts, loss of customers, loss of the use of any software or data, loss or use of any computer or other equipment save as may arise directly from breach of this CPS, wasted management or other staff time, losses or liabilities under or in relation to any other contracts, indirect loss or damage, consequential loss or damage, special loss or damage, and for the purpose of this paragraph, the term “loss” means a partial loss or reduction in value as well as a complete or total loss.

Field	Content
X.509v1 Field	
Version	v3
Serial Number	Allocated automatically by issuing CA
Signature Algorithm	SHA-1 with RSA Signature
Issuer Distinguished Name	
Country (C)	IE
Organisation (O)	An Post
Organisational Unit (OU)	Post.Trust Ltd.
Common Name (CN)	Post.Trust Operational CA
Validity Period	
Cert Start Date	DD/MM/YYYY-hh:mm:ss
Cert End Date	DD/MM/YYYY-hh:mm:ss
Subject	
Country (C)	IE
Organisation (O)	Client Company Name
Organisational Unit (OU)	CertifID Qualified Signing Certificate
Organisational Unit (OU)	Optional Client Supplied Identifier
Organisational Unit (OU)	Post.Trust Unique Identifier
Common Name (CN)	Person's Name
Subject Public Key Info	Public key encoded in accordance with RFC2459 & PKCS#1
X.509v3 Key Details and Extensions	
Key Size & Algorithm	1024 bit RSA
Key Usage	Digital Signature, Non-Repudiation(c0)
Extended Key Usage	E-mail Protection
Subject Alternative Name	RFC822 Name=Client email Address
Certificate Policies	
Policy Identifier OID	1.2.372.980002.1.1.7
Policy Notice	http://www.post.trust.ie/reposit/cps.htm
Policy Qualifier	This certificate is issued subject to the Post.Trust CPS terms and conditions. By accepting this certificate a relying party is acknowledging acceptance of the terms and conditions.

APPENDIX C - POST.TRUST CA PROFILE DETAILS

This appendix details the profiles of the Post.Trust Root CA and Operational CA certificates.

Post.Trust Root CA Certificate Profile Details

Corresponds to the key used to sign all subordinate operational Post.Trust Operational CA certificates.

Field	Content
1. X.509v1 Field	
1.1. Version	v3
1.2. Serial Number	39 a6 97 15
1.3. Signature Algorithm	SHA-1 with RSA Signature
1.4. Issuer Distinguished Name	
1.4.1. Country (C)	IE
1.4.2. Organisation (O)	An Post
1.4.3. Organisational Unit (OU)	Post.Trust Ltd.
1.4.4. Common Name (CN)	Post.Trust Root CA
1.5. Validity	
1.5.1. Not Before	05 July 2007 10:14:08
1.5.2. Not After	05 July 2022 10:12:33
1.6. Subject	
1.6.1. Country (C)	IE
1.6.2. Organisation (O)	An Post
1.6.3. Organisational Unit (OU)	Post.Trust Ltd.
1.6.4. Common Name (CN)	Post.Trust Root CA
1.7. Subject Public Key Info	Public key encoded in accordance with RFC2459 & PKCS#1
2. X.509v3 Key Details and Extensions	
2.1. Key Size & Algorithm	2048 bit RSA
2.1. Key Usage	
2.1.1. Digital Signature	Selected
2.1.2. Non-Repudiation	Selected
2.1.3. Certificate Signing	Selected
2.1.4. Off-line CRL Signing	Selected
2.1.5. CRL Signing (c6)	Selected
2.2. Certificate Policies	
2.2.1. Policy Identifier OID	1.2.372.980002.1
2.2.2. Policy Notice	http://www.post.trust.ie/reposit/cps.html
2.2.3. Policy Qualifier	Issued as a certificate subject to Post.Trust CPS which limits warranties and liability of Post.Trust Limited. By accepting, the relying party acknowledges it has read and accepted the CPS.
2.3. Basic Constraints	
2.3.1. Subject Type	CA
2.3.2. Path Length Constraint	None

Post.Trust Operational CA Certificate Profile Details

Corresponds to the key used to sign all certificates issued by Post.Trust to subscribers and end users.

Field	Content
1. X.509v1 Field	

Field	Content
1.2. Version	v3
1.3. Serial Number	39 a6 97 1f
1.4. Signature Algorithm	SHA-1 with RSA Signature
1.5. Issuer Distinguished Name	
1.5.1. Country (C)	IE
1.5.2. Organisation (O)	An Post
1.5.3. Organisational Unit (OU)	Post.Trust Ltd.
1.5.4. Common Name (CN)	Post.Trust Root CA
1.6. Validity	
1.6.1. Not Before	05 July 2007 11:10:26
1.6.2. Not After	05 July 2022 10:12:33
1.7. Subject	
1.7.1. Country (C)	IE
1.7.2. Organisation (O)	An Post
1.7.3. Organisational Unit (OU)	Post.Trust Ltd.
1.7.4. Common Name (CN)	Post.Trust Operational CA
1.8. Subject Public Key Info	Public key encoded in accordance with RFC2459 & PKCS#1
2. X.509v3 Key Details & Extensions	
2.1. Key Size & Algorithm	2048 bit RSA
2.2. Key Usage	
2.2.1. Digital Signature	Selected
2.2.2. Non Repudiation	Selected
2.2.3. Data Encipherment	Selected
2.2.4. Key Agreement	Selected
2.2.5. Key Certificate Signature	Selected
2.2.6. Off-line CRL Signing	Selected
2.2.7. CRL Signing (de)	Selected
2.3. Certificate Policies	
2.3.1. Policy Identifier OID	1.2.372.980002.2.01
2.3.2. Policy Notice	http://www.post.trust.ie/reposit/cps.html
2.3.3. Policy Qualifier	This certificate is issued subject to the Post.Trust CPS terms and conditions which outline the warranties provided with this certificate and the extent of the liability of Post.Trust Limited.
2.4. Basic Constraints	
2.4.1. Subject Type	CA
2.4.2. Path Length Constraint	3

REFERENCES

[ABA] American Bar Association, Section of Science & Technology, *Digital Signature Guidelines* (1996) (hereinafter ABA Guidelines). For information on ordering, see: <http://www.abanet.org/scitech/home.html>.

[FIPS] U.S. Department of Commerce, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication FIPS PUB 140-1, 1994. Available at: <http://csrc.nist.gov>.

[CHO] S. Chokhani and W. Ford, “Certificate Policy and Certification Practice Statement Framework,” Internet Draft <draft-ietf-pkix-ipki-part4-00.txt>.

[HOU] R. Housley, W. Ford, T. Polk, D. Solo, *Internet Public Key Infrastructure Part I: X.509 Certificate and CRL Profile*, Internet Draft: draft-ietf-pkix-ipki-part1-04.txt, 03/26/1997.

[TCSEC] U.S. Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, National Computer Security Center, Fort Meade, MD, December 1985. Available at <http://www.disa.mil/MLS/info/orange/intro.html>; <http://csrc.nist.gov/secpubs/rainbow/std001.txt>.

[TSDM] U.S. Department of Defense, “Trusted Software Methodology,” Volume 1, SDI-S-SD-91-000007, Department of Defense, Strategic Defense Initiative Organisation, 17 June 1992.

[X509] ISO/IEC 9594-8, *Information Technology—Open Systems Interconnection—The Directory: Authentication Framework*. Also published as ITU-T X.509 Recommendation. For X.509 v3 certificates, see edition ITU-T Rec. X.509 (1993 E) or ISO/IEC 9594-8:1995 with Technical Corrigendum 1 and Amendment 1 (Certificate Extensions) applied.