



# Certification Practice Statement

---

Post.Trust CA For Adobe Certified  
Document Services (CDS)

Issue date: 12.12.2009  
Release Version: 1.0

# Contents

1	Introduction .....	7
1.1	Overview .....	7
1.2	Identification .....	8
1.3	Community and Applicability .....	8
1.4	Contact Details .....	10
1.4.1	Administrative Authority .....	10
2	General Provisions.....	11
2.1	Obligations .....	11
2.1.1	Post.Trust Certification 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	Liability .....	13
2.2.1	Warranty .....	13
2.2.2	Limited Liability .....	13
2.2.3	Force Majeure.....	13
2.2.4	Certificate Content .....	13
2.2.5	Relying Parties.....	13
2.3	Financial Responsibility.....	14
2.3.1	Fiduciary .....	14
2.4	Interpretation and Enforcement.....	14
2.4.1	Governing Law.....	14
2.4.2	Dispute Resolution Process.....	14
2.4.3	General .....	14
2.5	Fees .....	14
2.6	Publication and Repository .....	15
2.6.1	Publication of CA information .....	15
2.6.2	Frequency of CRL publication .....	15
2.6.3	Access controls.....	15
2.6.4	Repositories – LDAP Directory .....	15
2.7	Compliance Audit .....	15
2.7.1	Frequency of Compliance Audit.....	15
2.7.2	Identity/Qualifications of Auditor .....	15
2.7.3	Auditor’s Relationship to Post.Trust.....	15
2.7.4	Topics Covered by Audit.....	16
2.7.5	Actions Taken as a Result of Deficiency .....	16
2.7.6	Compliance Audit Results.....	16
2.8	Confidentiality.....	16
2.8.1	Types of Information to be kept Confidential .....	16
2.8.2	Types of Information not considered Confidential .....	17
2.8.3	Disclosure of Certificate Revocation Information.....	17
2.9	Intellectual Property Rights .....	17
3	Identification and Authentication.....	18
3.1	Registration .....	18
3.1.1	Types of names .....	18
3.1.2	Need for names to be meaningful.....	19
3.1.3	Uniqueness of names .....	19
3.1.4	Name claim dispute resolution procedure .....	19
3.1.5	Recognition, authentication and role of trademarks .....	19
3.1.6	Method to prove possession of private key .....	19
3.1.6.1	Subscribers .....	19
3.1.7	Authentication of organization identity.....	19
3.1.8	Authentication of individual identity.....	20

3.2	Routine Certificate Rollover .....	20
3.3	Rekey after Revocation .....	20
3.4	Revocation Request .....	20
4	Operational Requirements .....	20
4.1	Certificate Registration Process .....	20
4.2	Certificate Issuance/Distribution Process .....	20
4.3	Certificate Acceptance .....	21
4.4	Certification Revocation .....	22
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 .....	23
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
4.5.1.1	Post.Trust CA For Adobe CDS Installation Procedure: .....	23
4.5.1.2	Private Key and Password holders within the Post.Trust PKI .....	23
4.5.1.3	All End User Registration Data .....	24
4.5.1.4	The certification process including certificate/key pair delivery .....	24
4.5.1.5	Certificate and CRL Publication .....	24
4.5.1.6	Certificate Revocation .....	24
4.5.1.7	Firewall monitoring .....	24
4.5.1.8	Oracle Auditing .....	24
4.5.1.9	Backup and Recovery procedures on the Post.Trust PKI .....	24
4.5.1.10	System Maintenance and Error detection .....	25
4.5.1.11	Backup of Records/Audit Material .....	25
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
4.6	Records Archive .....	25
4.6.1	Requirement for Time-Stamping of Records .....	26
4.7	Key Changeover .....	27
4.8	Compromise and Disaster Recovery .....	27
4.8.1	If Computing Resources, Software and/or Data become corrupted .....	28
4.8.2	Post.Trust CA For Adobe CDS Certificate Lifespan .....	28
4.9	CA Termination .....	28
4.9.1	Private Key Destruction Procedures .....	28
5	Physical, Procedural and Personnel Security Controls .....	29
5.1	Physical Security Controls .....	29
5.1.1	Site Location and Construction .....	29
5.1.2	Physical Access .....	29
5.1.3	Power and Air Conditioning .....	29
5.1.4	Fire Prevention and Protection .....	29
5.1.5	Off-site Backup & Recovery Procedures .....	29
5.1.6	Media Storage .....	30
5.1.7	Waste Disposal .....	30
5.2	Procedural Controls .....	30
5.2.1	Trusted Roles .....	30
5.2.1.1	Certification Authority Technical Operation and Support .....	30
5.2.1.2	Certificate and Registration Authority Administration .....	31
5.2.1.3	Hardware Security Module (HSM) Operations .....	31
5.2.1.4	QA Management .....	31
5.2.1.5	Database Administrator .....	31
5.2.1.6	Registration Authority Administrator (RAA) .....	31
5.2.1.7	CA Application Support Engineer .....	31

5.2.1.8	Operations Support Engineer.....	31
5.2.1.9	Certification Authority Administrator (CAA).....	32
5.2.1.10	HSM Operator.....	32
5.2.1.11	HSM Security Officer .....	32
5.2.1.12	HSM Key Component Holder .....	33
5.2.2	Number of Persons Required per Task .....	33
5.2.3	Identification and Authentication for Each Role.....	33
5.3	Personnel Security Controls.....	33
5.3.1	Background, Qualifications, Experience, and Clearance Requirements.....	33
5.3.2	Background Check Procedures .....	34
6	Technical Security Controls .....	34
6.1	Key Generation .....	34
6.1.1	Key pair generation.....	34
6.1.2	Post.Trust CA For Adobe CDS Private Key Distribution Service .....	34
6.1.3	Certificate delivery to certificate requester.....	34
6.1.4	Access to Post.Trust CA For Adobe CDS Certificate to End Users .....	35
6.1.5	Key sizes.....	35
6.1.5.1	Review of Private Key Usage Periods .....	35
6.1.6	Hardware/Software Key Generation .....	35
6.2	Private Key Protection.....	35
6.2.1	Standards for Cryptographic Module.....	35
6.2.2	Private Key Escrow.....	35
6.2.3	Method of Activating Private Keys .....	35
6.2.4	Method of Deactivating and Destroying Private Keys .....	35
6.3	Other Aspects of Key Pair Management.....	36
6.3.1	Usage periods for the public and private keys.....	36
6.4	Life Cycle Technical Security Controls .....	36
6.4.1	Security management controls .....	36
6.5	Network Security Controls.....	36
7	Certificate and CRL Profiles.....	37
7.1	Certificate Profile .....	37
7.2	CRL PROFILE.....	37
8	Specification Administration.....	37
8.1	Specification Change Procedures.....	37
8.1.1	Items that can change without notification.....	37
8.1.2	Changes with notification.....	37
8.1.2.1	List of items .....	37
8.1.2.2	Notification mechanism .....	37
8.1.2.3	Comment period.....	37
8.1.2.4	Mechanism to handle comments .....	38
8.1.2.5	Period for final change notice.....	38
8.1.3	Items whose change requires a new policy .....	38
8.2	CPS APPROVAL PROCEDURES .....	38
9	Appendix A – Registration, Certification and Delivery .....	39
9.1	Post.Trust CA for Adobe Employee Certificates .....	39
9.2	Post.Trust CA for Adobe Employee Qualified Certificates.....	42
10	Appendix B – Digital Certificate Profiles .....	45
10.1	Post.Trust CA for Adobe Certificate Profile.....	45
10.1.1	Limited Liability .....	45
10.2	Post.Trust CA for Adobe Qualified Certificate Profile .....	47
10.2.1	Limited Liability .....	47
11	Appendix C – Post.Trust CA For Adobe CDS Certificate Profile.....	49
12	References.....	51

## 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.

**Company Registration Administrator (CRA):** A person designated and authorized by a subscriber organization acting on its behalf to process registration applications for certification services provided to the organization and its employees by Post.Trust.

**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 or relying party:** A recipient who acts in reliance on a certificate and digital signature.

**Subscriber or subscriber:** An applicant for and/or a holder of a Post.Trust digital certificate, including without limitation, organizations, individuals and/or hardware and/or software devices, provided, however, that any provisions of this CPS that require the approval or action of an organization shall not be interpreted as allowing such approvals or actions to be taken by an individual Subscriber.

**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 Union Directive on Electronic Signatures, *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*.

## LIST OF ABBREVIATIONS

**CA** Certification Authority  
**CDS** Certified Document Services  
**CPS** Certification Practice Statement  
**CRA** Company Registration Administrator  
**CRL** Certificate Revocation List  
**DN** Distinguished Name  
**FIPS** Federal Information Processing Standard  
**LDAP** Lightweight Directory Access Protocol  
**PDF** Portable Document Format  
**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

# 1 Introduction

This document is the certification practice statement (CPS) which applies to those Post.Trust Limited (Post.Trust) services involved in the issuance and management of digital certificates distributed by Post.Trust under the Adobe Certified Document Services program (“Adobe CDS”) (hereinafter the “Post.Trust Services For Adobe CDS”). The Adobe CDS allows documents created in Adobe Portable Document Format (PDF) to be digitally signed using certain Adobe document creation software products and digital certificates issued by Post.Trust, where the resulting digital signatures are then automatically verified when the signed documents are opened using standard Adobe Reader or Acrobat products, without the requirement for any additional software or configuration.

These certificates are issued by Post.Trust as a Level 1 Certification Authority subordinate to the Adobe Root Certification Authority (the “Adobe RCA”) as set out in the Adobe CDS Certificate Policy Revision #14 dated October 2005 at the URL [http://www.adobe.com/misc/pdfs/Adobe\\_CDS\\_CP.pdf](http://www.adobe.com/misc/pdfs/Adobe_CDS_CP.pdf) (or a successor website) (the “Adobe CDS CP”) and are subject to the Adobe CDS CP (including without limitation any exclusions from and limitations on liability thereunder), this CPS and the relevant subscriber agreement. This CPS does not apply to services provided and certificates issued under the Post.Trust Root Certification Authority which are covered by a separate CPS available at <http://www.post.trust.ie/download/posttrustcps.pdf>.

This CPS covers the practices and procedures employed by Post.Trust to operate the Post.Trust Services For Adobe CDS. Information contained within this CPS outlines the 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 and relying parties.

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

- Identification, authentication and registration of individuals and organizations
- Certificate holder key pair generation
- Certificate generation (Qualified Certificates and non-Qualified Certificates)
- Certificate issuance and publication
- Certificate revocation

## 1.1 Overview

This CPS is applicable to digital certificates issued by Post.Trust binding the identity of individuals and organizations to a public key for the purpose of digitally signing Adobe PDF documents under the Adobe CDS.

The purpose of this document is to describe the procedures employed by Post.Trust to undertake Post.Trust Services For Adobe CDS and to provide explanation of the methods used to manage tasks associated with subscriber identity verification, digital certificate generation, distribution and revocation.

This CPS is compliant with the requirements of the Adobe CDS CP. For the purposes of this CPS audit against ETSI 101 456 V1.2.1 is equivalent to audit against WebTrust for CA as required by section 2.7 of the CDS CP.

The Adobe CDS CP describes the operational framework for Adobe CDS certificates in the wider community of use including the practices employed by Adobe in managing the Adobe Root Certification Authority and enrolment of third party CAs such as Post.Trust into the Adobe CDS program. Post.Trust Services For Adobe CDS subscribers and relying parties should read the Adobe CDS CP in conjunction with this CPS to achieve comprehensive and inclusive understanding of the end to end operational processes and practices governing the issuance and management of digital certificates and services offered by Post.Trust under the Post.Trust Services For Adobe CDS.

## 1.2 Identification

This document is the Certification Practice Statement for the Post.Trust Services for Adobe CDS.

## 1.3 Community and Applicability

Within the Post.Trust Services For Adobe CDS CA hierarchy there is one Post.Trust Operational CA entity that is linked by a signed CA certificate to the Adobe Root CA. This Post.Trust Operational CA is known as an Adobe CDS Subordinate or Level 1 CA whose top level certificate is signed by the Adobe Root CA. Post.Trust has undergone a registration process with the Adobe Registration Authority to obtain the signed Post.Trust Level 1 CA (hereinafter referred to as Post.Trust CA For Adobe CDS) certificate. Post.Trust issues certificates to subscribers signed with the private key linked to the Post.Trust CA For Adobe CDS.

Digital certificates are issued by Post.Trust under the Post.Trust Services For Adobe CDS both to individuals and to organizations. Where issued for an organization (or organizational unit/department) a certificate can be bound to the organization identity however a single individual must act as custodian of the certificate and act on behalf of the organization when signatures are created. Certificates can also be issued to roles within an organization but again a natural person must act as sole custodian of each specific certificate for the purpose of signing while acting in that role on behalf of the organization.

The only application permitted for certificates issued by the Post.Trust CA is digital signing and verification of Adobe PDF documents.

Figure 1 illustrates the Certification Authority and Registration Authority hierarchy

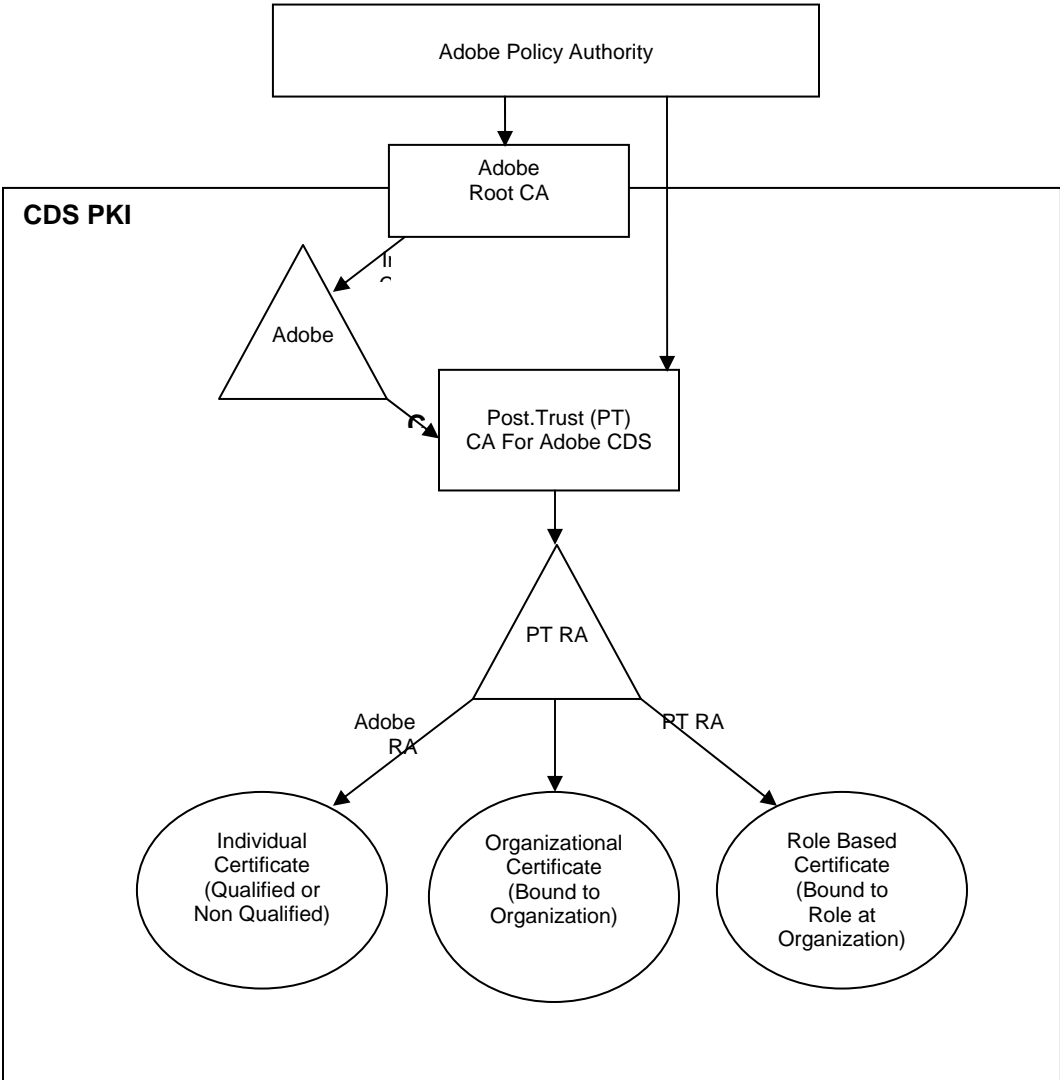


Figure 1 – Adobe and Post.Trust CA For Adobe CDS Certificate Hierarchy

## **1.4 Contact Details**

### **1.4.1 Administrative Authority**

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

**Email Address:** [info@post.trust.ie](mailto:info@post.trust.ie)

**Telephone:** 1890 617171

## **2 General Provisions**

This section contains provisions relating to the respective obligations of the Post.Trust CA For Adobe CDS, Post.Trust RA, subscribers and relying parties, as well as other issues pertaining to law and dispute resolution. Notwithstanding any other provision within this CPS, in the event of a conflict between this CPS and the Adobe CDS CP, the Adobe CDS CP shall control.

### **2.1 Obligations**

#### **2.1.1 Post.Trust Certification Authority (CA) Obligations**

The Post.Trust CA For Adobe CDS obligations include the following:

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

#### **2.1.2 Post.Trust Registration Authority (RA) Obligations**

The Post.Trust RA obligations include the following:

- Authentication of subscriber's identification information, which is necessary to issue a digital certificate, to the Post.Trust CA For Adobe CDS;
- Notification of authenticated digital certificate request to the Post.Trust CA For Adobe CDS;
- 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 Post.Trust CA For Adobe CDS.

Registration activities may be delegated to third parties other than the Post.Trust RA, for example to Company Registration Administrators (CRAs) within customer organizations, but in all such cases the activities of such third parties must be carried out in accordance with this CPS and any specific policies agreed between such third parties and Post.Trust, and must be approved by Post.Trust, provided, however, that such specific policies remain in compliance with the Adobe CDS CP and this CPS.

#### **2.1.3 Subscriber Obligations**

Following acceptance of the certificate provided to it, a subscriber is solely responsible for the protection of its private keys. A subscriber must not disclose to anyone any information needed to access its private keys including, without limitation, the PINs, passwords, passphrases, or other information or mechanisms used to protect private keys. In addition to the obligations articulated in this Section 2.1.3, Subscriber further agrees to any applicable obligations contained in this CPS (including all obligations in any Subscriber Agreement).

Subscribers shall notify Post.Trust immediately if they believe a private key has or may have been compromised in any way. Subscribers 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 For Adobe CDS 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.

BY RELYING ON A DIGITAL CERTIFICATE, THE RELYING PARTY AGREES TO INDEMNIFY AND HOLD POST.TRUST, ADOBE AND ITS AND THEIR 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, ADOBE OR ITS OR THEIR AGENTS AND/OR CONTRACTORS MAY INCUR, THAT ARE CAUSED BY THE USE OR RELIANCE ON A DIGITAL CERTIFICATE AND THAT ARISE FROM (I) FAILURE BY THE RELYING PARTY TO CHECK THE STATUS OF THE DIGITAL CERTIFICATE IN ADVANCE OF RELYING ON IT; (II) BREACH BY THE RELYING PARTY OF ANY RELYING PARTY AGREEMENTS, ANY ADOBE OR THIRD PARTY LICENSE AGREEMENTS; AND (III) USE OF THE DIGITAL CERTIFICATE FOR A PURPOSE WHICH IS LIBELOUS 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, ADOBE OR A THIRD PARTY. THE RELYING PARTY ACKNOWLEDGES THAT POST.TRUST MAY ENFORCE THESE INDEMNITY PROVISIONS FOR THE BENEFIT OF NOT ONLY POST.TRUST, BUT ALSO ADOBE AND OTHER THIRD PARTIES, AND THAT TO THIS LIMITED EXTENT POST.TRUST IS ACTING AS AGENT OF ADOBE AND OTHER THIRD PARTIES IN ISSUING THIS CPS.

### **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 For Adobe CDS, facilitating public access to download these digital certificates for subscriber and relying party requirements.
- Receiving (from the Post.Trust CA For Adobe CDS), storing and making publicly available regularly updated CRL v 2 information, for the purpose of digital certificate validation.

## 2.2 Liability

### 2.2.1 Warranty

Post.Trust hereby warrants (a) it has taken reasonable steps (including as specified in Appendix A) 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 have 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 only be liable to subscribers or relying parties for the direct loss arising from any breach of this CPS or for any other liability they may incur in contract, tort or otherwise, including liability for negligence up to an aggregated maximum limit specified in Appendix 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 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.

### 2.2.4 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 indemnification obligations, limitations of liability and disclaimers of warranty, with a reference to the full text of such indemnities, obligations, warnings, limitations and disclaimers in this CPS. In accepting a digital certificate, subscribers and relying parties are acknowledging and agreeing to all such indemnities, limitations and disclaimers.**

### 2.2.5 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 the Adobe CDS CP, this CPS and the current set of revoked digital certificates published by Post.Trust.

## **2.3 Financial Responsibility**

### **2.3.1 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.

## **2.4 Interpretation and Enforcement**

### **2.4.1 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 CPS.

### **2.4.2 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) .

### **2.4.3 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 Adobe CDS CP, the subscriber agreement and any indemnities, 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.

## **2.5 Fees**

No stipulation in this CPS. Fees charged for Post.Trust Services For Adobe CDS are either published on the Post.Trust web site at [www.post.trust.ie](http://www.post.trust.ie) or stipulated in commercial agreements between Post.Trust and its customers.

## **2.6 Publication and Repository**

### **2.6.1 Publication of CA information**

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

Post.Trust will ensure that all current and past copies of this CPS shall be published on its web site along with the effective periods for each copy.

### **2.6.2 Frequency of CRL publication**

Publication of the Post.Trust Certificate Revocation List will be configured to occur at least once every 24 hours. 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 For Adobe CDS at any given time.

### **2.6.3 Access controls**

Public access to the Post.Trust CA For Adobe CDS 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.

### **2.6.4 Repositories – LDAP Directory**

All digital certificate information shall be published to the dedicated Post.Trust LDAP directory server. Each time the Post.Trust CA For Adobe CDS 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.

## **2.7 Compliance Audit**

### **2.7.1 Frequency of Compliance Audit**

A qualified independent external auditor shall audit services of the Post.Trust CA For Adobe CDS and any designated authorized agents at least annually.

### **2.7.2 Identity/Qualifications of Auditor**

The auditor who performs these audits is accredited to perform such audits by the Irish National Accreditation Board ([www.inab.ie](http://www.inab.ie)) (provided such accreditation either remains (a) equivalent to the requirements in Section 2.7.2 of the CDS CP or (b) acceptable to Adobe.

### **2.7.3 Auditor's Relationship to Post.Trust**

The auditor carrying out the audits is completely independent of Post.Trust and has no relationship which could in any way impair its independence or result in a conflict of interest. The auditors are themselves regularly audited by the Irish National Accreditation Board and other international auditors who may on occasion be present as observers during audits to assure quality with international best practice.

## 2.7.4 Topics Covered by Audit

Post.Trust is audited to the following standards:

- International Information Security Standard ISO 27001:2005
- European Union Electronic Signatures Directive 1999/93/EC Annexes I and II as guided by European Telecommunications Institute specification ETSI 101 456 Policy Requirements for Certificate Authorities issuing Qualified Certificates

## 2.7.5 Actions Taken as a Result of Deficiency

Any failure to comply with the specified requirements of this CPS will be addressed by the Post.Trust CA For Adobe CDS or its authorized agent as soon as is operationally possible.

Any deficiencies arising from audits are addressed in the audit report as either (i) major non-conformities (ii) minor non-conformities (iii) observations. A single major non-conformity or a number of minor conformities may lead to suspension of Post.Trust's certification and are addressed immediately with urgency if they arise. Observations do not generally require urgent action but nevertheless remedial action is generally taken prior to the subsequent audit taking place.

## 2.7.6 Compliance Audit Results

Audit results are verbally communicated to Post.Trust management at the end of each site audit and are subsequently formally documented in the form of an audit report which is delivered to Post.Trust senior management as soon as possible. A summary of the results of such audit reports, along with all sections of the results that directly relate to the CDS CP, shall be provided to Adobe promptly upon Adobe's request.

## 2.8 Confidentiality

The Post.Trust CA For Adobe CDS 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 For Adobe CDS, 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.

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 permitted or compelled to do so by law or competent regulatory authority, or the subscriber has agreed to the disclosure.

### 2.8.1 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.

## **2.8.2 Types of Information not considered Confidential**

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

## **2.8.3 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.

## **2.9 Intellectual Property Rights**

All Intellectual Property Rights in the Post.Trust Services For Adobe CDS and any associated documentation (including any and all functional and performance specifications (the "Specifications")) shall vest in Post.Trust Limited and/or its licensors (including, without limitation, Adobe). For the purposes of this CPS, "Intellectual Property Rights" shall mean all patents, copyrights (including copyright in computer software), design rights, trademarks, 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 For Adobe CDS 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 systems and services only to the extent and solely for the purpose of availing of the Post.Trust Services For Adobe CDS. The granting of this limited license 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 organizations requesting certification under the Post.Trust CA For Adobe CDS. As the Post.Trust CA For Adobe CDS 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.

Post.Trust provides identification and authentication services for certificate holders. 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 generally require applicants to present themselves for face-to-face verification directly at time of registration. Alternatively in some cases it may be possible for identity verification documentation acquired as a consequence of face to face verification which occurred prior to registration to be presented as equivalent to that presented during registration.

#### 3.1 Registration

Post.Trust has implemented 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. Refer to 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"> <li>• <b>Individual Digital Certificate:</b> The digital certificate holders given name</li> <li>• <b>Role based Digital Certificate:</b> The digital certificate holders organizational role (e.g. general manager)</li> <li>• <b>Company Digital Certificate:</b> The organization name</li> </ul>
Organization (O=)	Registered business name of organization
Country (C=)	Ireland
Organization Unit (OU=)	<ul style="list-style-type: none"> <li>• Internal organization department (e.g. Sales and Marketing)</li> <li>• Job description</li> <li>• Certificate description</li> </ul>
Locality (L=)	Town/ City of certificate holder or organization
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 meaningful<sup>1</sup>. The names provided on the digital certificate must be as accurate as possible when describing the person or organization or role within the organization. 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, organization unit, common name, and postal address. Any digital certificate requests which are not unique will be automatically rejected by the Post.Trust CA For Adobe CDS. Subscribers who have been rejected by the Post.Trust CA For Adobe CDS 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 Method to prove possession of private key**

#### **3.1.6.1 Subscribers**

Where subscribers generate their own private key locally, for example using on-board smartcard or USB PKI token key generation, proof of possession of the private key must be communicated to the Post.Trust CA For Adobe CDS through digital signing of the certificate request sent to the Post.Trust CA For Adobe CDS. This signature will then be verified by Post.Trust CA For Adobe CDS using the subscriber public key.

Private keys generated by Post.Trust CA For Adobe CDS on behalf of the subscriber will be generated and delivered to the certificate subject in a secure manner which is fully accountable and auditable, and which fully satisfies the requirement for ensuring that the private key generated cannot be accessed or copied and subsequently used by any party during generation and delivery to the certificate subject, other than by the certificate subject.

### **3.1.7 Authentication of organization 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.

---

<sup>1</sup> 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.

### **3.1.8 Authentication of individual identity**

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

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 license or photographic ID determined by the Post.Trust RA to be equivalent to a passport or driving license,

## **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 For Adobe CDS 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.

## **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 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 CPS on the Post.Trust CA For Adobe CDS, 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.

In the event that a subscriber requires both a private and public key from the Post.Trust CA For Adobe CDS, the subscriber will be supplied with a secure private key container which meets or exceeds FIPS 140-1 Level 2 certification standards in addition to the certificate containing the public key.

In the event that a subscriber requires only a digital certificate (as the private and public keys have been generated outside the Post.Trust CA For Adobe CDS) 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 For Adobe CDS, 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 unauthorized 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 authorized and legal purposes, consistent with this CPS.

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, MODIFICATION OR UNAUTHORISED USE.

BY ACCEPTING A DIGITAL CERTIFICATE, THE SUBSCRIBER AGREES TO INDEMNIFY AND HOLD POST.TRUST, ADOBE AND ITS AND THEIR 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, ADOBE OR ITS OR THEIR AGENTS AND/OR CONTRACTORS MAY INCUR, THAT ARE CAUSED BY THE USE OR PUBLICATION OF A DIGITAL CERTIFICATE AND THAT ARISE FROM ANY BREACH OF THE SUBSCRIBER AGREEMENT OR (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, ADOBE 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 LIBELOUS 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, ADOBE OR A THIRD PARTY.

THE SUBSCRIBER ACKNOWLEDGES THAT POST.TRUST MAY ENFORCE THESE INDEMNITY PROVISIONS FOR THE BENEFIT OF NOT ONLY POST.TRUST, BUT ALSO ADOBE AND OTHER THIRD PARTIES, AND THAT TO THIS LIMITED EXTENT POST.TRUST IS ACTING AS AGENT OF ADOBE AND OTHER THIRD PARTIES IN ISSUING THIS CPS.

## **4.4 Certification Revocation**

The Post.Trust CA For Adobe CDS reserves the right to revoke any of its issued digital certificates. All revocation information is published and held in an 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 contained within 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 unauthorized access or suspect unauthorized 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 or organization bankruptcy
8. Subscriber or organization liquidation
9. Subscriber death
10. Breach of subscriber agreement with Post.Trust
11. Subscriber no longer authorized to represent the organisation
12. Subscriber profile creation error
13. Post.Trust CA For Adobe CDS key compromise or certificate revocation
14. Adobe RCA key compromise or certificate revocation

### **4.4.2 Who Can Request Revocation**

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

- The Post.Trust CA For Adobe CDS
- The individual subscriber
- The Post.Trust RA, on behalf of the individual subscriber
- The Adobe RCA
- The CRA
- The organization as represented by an authorized senior manager

### **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 For Adobe CDS issues and publishes a new CRL to the LDAP directory where it is available for public use in certificate verification. The

subscriber shall be required to submit the revocation request via the Post.Trust Help Desk or directly over an Internet connection. The subscriber shall 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 For Adobe CDS or RA administrators directly.

#### **4.4.4 CRL Issuance Frequency**

The Post.Trust CA For Adobe CDS will issue CRLs at least once every 24 hours. In addition to this configuration, the Post.Trust CA For Adobe CDS 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 For Adobe CDS 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 Management Policy to protect the service from compromise through unauthorized access to systems or data. Robust security measures and controls are in place to ensure confidentiality, integrity and availability of private keys, digital certificates and CRLs.

#### **4.5.1 Types of Data to be recorded**

##### **4.5.1.1 Post.Trust CA For Adobe CDS Installation Procedure:**

All events involved in the generation of the Post.Trust CA For Adobe CDS 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.

##### **4.5.1.2 Private Key and Password holders within the Post.Trust PKI**

The Post.Trust CA For Adobe CDS 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 databases will take the form of a user name and password. Access control in certain cases shall 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 to enforce dual-person control. In other cases where necessary multi-person control shall be enforced through the use of multiple smartcards and PINs held separately by different trusted individuals. This ensures that a minimum of two people being present to perform certain tasks on the Post.Trust PKI system.

#### **4.5.1.3 All End User Registration Data**

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

#### **4.5.1.4 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 an 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

#### **4.5.1.5 Certificate and CRL Publication**

All data relevant to the publication of digital certificates and CRLs by the Post.Trust CA For Adobe CDS 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 For Adobe CDS (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 For Adobe CDS. Details of this can be viewed in the Post.Trust CA For Adobe CDS event log.

#### **4.5.1.6 Certificate Revocation**

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

#### **4.5.1.7 Firewall monitoring**

As the Post.Trust PKI environment consists 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. Firewalls 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.

#### **4.5.1.8 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 (including to Adobe) and investigated.

#### **4.5.1.9 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.

#### 4.5.1.10 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.

#### 4.5.1.11 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 analyzed 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.

## 4.6 Records Archive

### 4.6.1 Types of Event Recorded

The following types of records will be archived by the Post.Trust CA For Adobe CDS:

Item / Data to be Archived	Method
Certificate Policy	CP details are specified in this CPS of which all versions are stored in a document management system and/or X.509 V3 certificates issued which are archived in an LDAP directory.
Certification Practice Statement	All historic versions of the CPS are maintained in a document management system with version tracking.
Contractual Obligations	All contract details are stored in secure filing cabinets when in paper form or in a document management system when in electronic form.
System & Equipment Configurations	Build, security hardening and configuration documents for all major servers and other hardware and software components are securely

	stored in a document management system.
Modification & Updates to System or Configuration (Scripts)	Configuration scripts and files are stored in a document management system with version tracking.
Revocation Requests	All revocation requests are recorded in databases used in certificate registration and management systems including an LDAP directory where details of fulfilled revocations are recorded.
Subscriber Identity Authentication (per Section 3.1.9)	Details of subscriber identity authentication are stored in secure filing cabinets if in paper form or secure document management systems if in electronic form.
Documentation of Receipt and Acceptance of Certificates	Receipt and acceptance of certificates is automatically recorded in the registration system as part of the end to end registration process.
Documentation of Receipt of Tokens	As above
All Certificates Issued or Published	All certificates issued or published are stored in an LDAP directory
A Complete Listing of All Certificates Revoked	As above
All Audit Logs	Audit logs are automatically maintained by the CA infrastructure.
Documentation Required by Compliance Auditors	All documentation used by compliance auditors is stored in a document management system.

#### 4.6.2 Retention Period for Archive

Archives shall be kept for a minimum of three (3) years.

#### 4.6.3 Protection of Archive

Archives are stored in secure locations with appropriate physical and logical access controls to prevent unauthorized access. Archive media are stored in physical locations which are protected from environmental threats such as temperature, humidity, and magnetism.

#### 4.6.4 Archive Backup Procedures

All archives are backed up as part of normal daily operational procedures.

#### 4.6.1 Requirement for Time-Stamping of Records

All events that are recorded within Post.Trust Adobe CDS Services 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 including automatic synchronization with a master time server which is itself synchronized with a stratum 1 time server using Network Time Protocol or Simple Network Time Protocol.

#### 4.6.6 Archive Collection System (internal or external)

No stipulation

### **4.6.7 Procedures to Obtain and Verify Archive Information**

Archive information may be retrieved by authorized operations personnel and verified using integrity verification methods employed by the underlying storage mechanism.

## **4.7 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 profile chosen by the subscriber, there may 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.

## **4.8 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 Adobe Root CA private key becoming compromised the Post.Trust CA For Adobe CDS certificate will be revoked as promptly as is operationally possible. In the event of the Post.Trust CA For Adobe CDS private key becoming compromised then the Post.Trust CA For Adobe CDS 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 Post.Trust CA For Adobe CDS Certificate will be revoked.

In the case of the Adobe Root CA private keys becoming compromised, a new Root and Post.Trust CA For Adobe CDS hierarchy may be created and all digital certificates may be reissued. In the event of only the Post.Trust CA For Adobe CDS private key becoming compromised, only digital certificates issued by Post.Trust CA For Adobe CDS will need to be revoked and an alternative Post.Trust CA For Adobe CDS 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.

#### **4.8.1 If Computing Resources, Software and/or Data become corrupted**

The Post.Trust disaster recovery plan incorporates measures to minimize 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.

#### **4.8.2 Post.Trust CA For Adobe CDS Certificate Lifespan**

Each Post.Trust CA For Adobe CDS certificate has a certificate lifetime of 15 years. Post.Trust reserves the right to extend the lifetime of the Post.Trust CA For Adobe CDS certificate. It should be noted that the Post.Trust CA For Adobe CDS private key is protected from compromise with a level Hardware Security Module (HSM) designed to US FIPS 140-1 level 4 standard.

### **4.9 CA Termination**

In the unlikely event that Post.Trust CA For Adobe CDS decides to terminate its CA services, all interested parties will promptly be made aware of this fact. Post.Trust will take it upon itself to notify all subscribers via email of the implications of this unlikely event. If such an event occurs the Post.Trust CA For Adobe CDS certificate will be revoked and all issued digital certificates will automatically become revoked. In such an eventuality Post.Trust will consult with Adobe on what specific termination procedures are appropriate..

#### **4.9.1 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, unauthorized disclosure or unauthorized use. Upon termination of the Post.Trust CA For Adobe CDS operations, Post.Trust personnel shall destroy the Post.Trust CA For Adobe CDS 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 For Adobe CDS environment.

### **5.1 Physical Security Controls**

The security of the site used to host the Post.Trust CA For Adobe CDS was designed in order to ensure that the best possible physical protection is afforded to the Information Security assets present at the site. This facility is securely protected from unauthorized 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 Post.Trust CA For Adobe CDS room itself.

#### **5.1.1 Site Location and Construction**

The Post.Trust CA For Adobe CDS 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 For Adobe CDS 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 For Adobe CDS site. The secure site is supplied with a piped source of halogen gas in order to minimize the risk or damage from fire.

#### **5.1.5 Off-site Backup & Recovery Procedures**

The Post.Trust CA For Adobe CDS and RA Oracle databases are replicated at a site different to that in which the Post.Trust CA For Adobe CDS 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. The LDAP repository is similarly replicated. Replication synchronization will take place at least once daily. Full system backups to tape of all essential data are taken at least once daily.

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.

### **5.1.6 Media Storage**

All media used by Post.Trust in the operation of its services including but not limited to tapes, hard disks, memory keys, CDs and DVDs are stored securely within Post.Trust's facilities.

### **5.1.7 Waste Disposal**

All electronic media used in Post.Trust operations is securely disposed of when no longer needed as follows:

- Hard disks, diskettes, memory keys and other devices which are used as external disk drives but which are not being permanently decommissioned are securely erased using a high grade zeroizing process.
- Cryptographic devices being decommissioned will be reset and have all key storage areas securely according to the manufacturer instructions.
- Hard disks which are being permanently decommissioned will be securely zeroized and then physically drilled to render them destroyed. Equivalent measures will be taken to destroy other external disk drive devices.
- Paper records are shredded on-site using a high quality shredding device

## **5.2 Procedural Controls**

Procedures are established, documented and implemented for all trusted and administrative roles required to operate the Post.Trust Services. Where possible, appropriate duties associated with Post.Trust Services For Adobe CDS 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 the Post.Trust Services For Adobe CDS 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 Post.Trust CA For Adobe CDS operations.

These roles fall under different categories as follows:

#### **5.2.1.1 Certification Authority Technical Operation and Support**

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

### **5.2.1.2 Certificate and Registration Authority Administration**

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

### **5.2.1.3 Hardware Security Module (HSM) Operations**

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

Post.Trust has 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:

### **5.2.1.4 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

### **5.2.1.5 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.

### **5.2.1.6 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

### **5.2.1.7 CA Application Support Engineer**

- Expert support in PKI and Cryptography technology used
- Assist in review and design of PKI architecture
- Troubleshooting
- Installation, build, configuration and testing of Post.Trust CA For Adobe CDS 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:

- Post.Trust CA private key generation and PIN storage
- Post.Trust CA For Adobe CDS private key activation and recovery
- All HSM Operations (in which the private key is generated and stored) which automatically enforce presentation of two separate security officer smartcards and PINs, and/or of multiple smartcards which hold key components used to recover complete symmetric keys used in the HSM key hierarchy,

### **5.2.1.8 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.

#### **5.2.1.9 Certification Authority Administrator (CAA)**

- Digital Certificate generation and secure distribution of all PKI component key pairs within the Post.Trust CA For Adobe CDS environments
- Generating, distributing, and otherwise managing CRLs
- Administrative functions associated with maintaining the Post.Trust CA For Adobe CDS and registration databases
- Assisting in incident investigations
- CA event log maintenance and query
- Revocation the Post.Trust CA For Adobe CDS certificate 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 Post.Trust CA For Adobe CDS 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 Post.Trust CA For Adobe CDS 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 (e.g.: wallets)

#### **5.2.1.10 HSM Operator**

- Change or view network settings for the HSM

#### **5.2.1.11 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-initialize the HSM

#### **5.2.1.12 HSM Key Component Holder**

- Custodians 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 Post.Trust CA For Adobe CDS 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.

The principles of dual (or more than 2) roles and split knowledge are always adhered to so as to ensure no conflict of interest occurs and to prevent the possibility of accidental or intentional compromise of any component of the Post.Trust CA For Adobe CDS infrastructure, most especially the Post.Trust CA For Adobe CDS private key, and customer private keys if held temporarily by Post.Trust during the registration process.

CA key-pair generation and initialization of the Post.Trust CA For Adobe CDS 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 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 standard 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 For Adobe CDS private keys are protected within a hardware security module ("HSM"). The use of a HSM, with FIPS 140-1 level 4 capabilities ensures that Post.Trust adheres to the highest industry standard regarding the generation and protection of the Post.Trust CA For Adobe CDS private keys. Access to the modules within the Post.Trust environment including the Post.Trust CA For Adobe CDS 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**

The Post.Trust CA For Adobe CDS key generation procedure will be documented by Post.Trust in such a manner as to provide auditable evidence that the correct procedures were followed. An independent auditor will witness the key generation procedure.

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 For Adobe CDS system the subscriber's public and private key pair are generated within a secure environment. Post.Trust may 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 Services. Post.Trust Services For Adobe CDS 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.

Subscriber private keys generated for use with a Post.Trust CA For Adobe CDS certificate must be generated in a secure medium that prevents duplication and exportation and that meets or exceeds FIPS 140-1 Level 2 Certification.

#### **6.1.2 Post.Trust CA For Adobe CDS Private Key Distribution Service**

Once the subscriber certificate request has been signed by the Post.Trust CA For Adobe CDS 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 For Adobe CDS Certificate to End Users**

The Post.Trust CA For Adobe CDS 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 Post.Trust CA For Adobe CDS uses RSA key pairs with length 2048 bits. Subscribers are issued RSA key pairs with length 2048 bits.

#### **6.1.5.1 Review of Private Key Usage Periods**

The operational periods for new certificates will be reviewed on an ongoing 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**

Key generation meets the requirements of 6.1.1 and 6.1.5.

## **6.2 Private Key Protection**

### **6.2.1 Standards for Cryptographic Module**

The generation and maintenance of the Post.Trust CA For Adobe CDS 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 CA For Adobe CDS is designed to provide FIPS 140-1 Level 4 security standards in both the generation and the maintenance in CA private keys.

Subscriber private keys are generated and stored in secure containers which meet or exceed FIPS 140-1 Level 2 standards.

### **6.2.2 Private Key Escrow**

Subscriber private keys for Post.Trust Services For Adobe CDS certificates will not be escrowed.

### **6.2.3 Method of Activating Private Keys**

The activation of the Post.Trust CA For Adobe CDS private key 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 For Adobe CDS private key. Subscribers activate private keys using methods including but not limited to PINs, Passwords, Passphrases and biometrics.

### **6.2.4 Method of Deactivating and Destroying Private Keys**

Private keys are deactivated when no longer in use. The method of deactivation varies with the type of private key container involved. For Post.Trust CA For Adobe CDS keys secure erasure of HSM memory is carried out.

In the case of subscriber private keys methods to deactivate private keys will vary depending on the specific certificate type and subscriber registration / deregistration process agreed with the

customer. This deactivation may for example involve repossession of the physical cryptographic token in which the private key is stored.

Where deactivation is permanent the private keys in question will be destroyed. HSMs and hardware tokens will be securely and permanently erased as will any smartcard backups.

## **6.3 Other Aspects of Key Pair Management**

### **6.3.1 Usage periods for the public and private keys**

The Post.Trust CA For Adobe CDS 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 For Adobe CDS 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**

### **6.4.1 Security management controls**

The Post.Trust CA For Adobe CDS 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 For Adobe CDS 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 Post.Trust CA For Adobe CDS 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 Services For Adobe CDS comply with digital certificate and CRL profiles as described in RFC 2459.

### 7.1 Certificate Profile

The Post.Trust CA For Adobe CDS certificate is signed by the Adobe Root CA entity. The Adobe Root CA acts as the source of trust within the Post.Trust CA For Adobe CDS PKI.

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

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

### 7.2 CRL PROFILE

To ensure global compatibility and conformity to public key standards, Post.Trust CA For Adobe CDS will utilize 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 Certification Practice Statement may be changed with 45 days notice.

(b) Changes to items which, in the judgment of the policy administration organization, 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 organization 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 Post.Trust Company Solicitors
- The Adobe PA

## 9 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, provided such specific arrangements do not change the obligations or liabilities articulated in this CPS.

### 9.1 Post.Trust CA for Adobe Employee Certificates

INITIAL REGISTRATION
<p>An organization applying for a set of digital certificates for its employees to sign Adobe PDF documents can do so by following the procedure below.</p>
<p><b>Authentication of Organization Identity</b>                      Following initial application by an organization for certification services, Post.Trust will undertake to verify the mandatory organization details required in the application including at least the organization’s registration number and registered address by referring to the Company Registration Office (CRO).</p>
<p><b>CRA Registration</b>                      Where the organization requirements are for a small batch (&lt;10) of certificates, Post.Trust CA For Adobe CDS can process the registration details of each individual employee directly.</p> <p>Where the organization requirements are deemed to be for a large batch (&gt;10) of certificates organizational CRAs (Company Registration Administrators) must be appointed.</p>
<p>Within each organization one or more CRAs 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>A letter of authorization on company headed paper is required from a senior member of the organization’s management confirming that the CRA is authorized to act as a CRA on behalf of the organization. This letter is required each time a new CRA is requested or for an existing CRA to be removed. The letter is forwarded to the Post.Trust RAA, is verified by contacting the signatory (senior manager) and/or other appropriate senior manager by phone to assure its authenticity, and is retained by Post.Trust as part of its overall document archive.</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>

- ✓ CRA Name
- ✓ No. of Certificates Required
- ✓ Company or Organization Name
- ✓ Department Name
- ✓ Email Address
- ✓ Organization Address
- ✓ Company Registration Number or other Official Organization Identifier
- ✓ CRA Passport Number or Driving License Number and/or PPS (Personal Public Service) Number

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.

#### EMPLOYEE REGISTRATION

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):

- ✓ Employee Name
- ✓ Company or Organization Name
- ✓ Department
- ✓ Email Address
- ✓ The relevant CRA
- ✓ Organization Address
- ✓ Company Registration Number or other Official Organization Identifier
- ✓ Employee Passport Number or Driving License Number and/or PPS Number

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.

#### CERTIFICATION GENERATION

All successful certificate requests will be processed by the Post.Trust CA For Adobe CDS. The CA will apply to the certificate request:

- ✓ A unique serial number
- ✓ Post.Trust CA For Adobe CDS signature

Note the validity period of a generated certificate will vary depending on the specific requirements of a customer but will generally not exceed three years,

#### CERTIFICATE DELIVERY

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

- ✓ Download over the Internet
- ✓ CD/Floppy Disk/USB Memory Key
- ✓ Smart Card, PKI USB or other secure hardware token
- ✓ E-mail

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 smart card or PKI USB token. 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 CA for Adobe CDS by verifying the thumbprint of the issuing CA certificate against that published for the Post.Trust CA For Adobe CDS at <http://www.post.trust.ie/Downloads/AdobeRootCertCheck.pdf>. 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.

## 9.2 Post.Trust CA for Adobe Employee 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 identity verification procedure directly at time of registration or have undergone a face to face identity verification prior to registration which is assessed by Post.Trust to having equivalent evidential value.

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

Qualified certificates may also be applied for in other circumstances for example by customers of an organization (business or consumer) with whom Post.Trust has a contract to supply certificates. In these situations a 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
An organization applying for a set of qualified digital certificates for its employees can do so by following the procedure below.
<p><b>Authentication of Organization Identity</b> Following initial application by an organization for certification services, Post.Trust will undertake to verify the mandatory organization details required in the application including at least the organization's registration number and registered address by referring to the Company Registration Office (CRO).</p> <p><b>CRA Registration</b> Where the organization requirements are for a small batch of certificates (&lt;10), Post.Trust CA For Adobe CDS 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 organization requirements are deemed to be for a large batch (&gt;10) of certificates organizational CRAs (Company Registration Administrators) must be appointed.</p>
Within each organization 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 central Registration Authority Administrator (RAA).
A letter of authorization on company headed paper is required from a senior member of the organization's management confirming that the CRA is authorized to act as a CRA on behalf of the organization. . This letter is required each time a new CRA is requested or for an existing CRA to be removed. The letter is forwarded to the Post.Trust RAA, is verified by contacting the signatory (senior manager) and/or other appropriate senior manager by phone to assure its

authenticity, and is retained by Post.Trust as part of its overall document archive.

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.

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, driving license or other photo ID specified by Post.Trust as being acceptable. 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.

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.

A CRA initially enters the batch registration page on the Post.Trust Web site and supplies the following information:

- ✓ CRA Name
- ✓ No. of Certificates Required
- ✓ Company or Organization Name
- ✓ Department Name
- ✓ Email Address
- ✓ Organization Address
- ✓ Company Registration Number or other Official Organization Identifier
- ✓ CRA Passport Number or Driving License Number and/or PPS (Personal Public Service) Number

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.

#### EMPLOYEE REGISTRATION

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):

- ✓ Employee Name
- ✓ Company or Organization Name
- ✓ Department
- ✓ Email Address
- ✓ The relevant CRA
- ✓ Organization Address
- ✓ Company Registration Number or other Official Organization Identifier
- ✓ Employee Passport Number or Driving License Number and/or PPS (Personal Public Service) Number

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.

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.

**CERTIFICATION GENERATION**

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

- ✓ A unique serial number
- ✓ Operational CA's signature

Note the validity period of a generated certificate will vary depending on the specific requirements of a customer but will generally not exceed three years,

**CERTIFICATE DELIVERY**

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

- ✓ Download over the Internet
- ✓ CD/Floppy Disk/USB Memory Key
- ✓ Smart Card, PKI USB or other secure hardware token
- ✓ E-mail

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 an employee, this will be distributed in a secure key container such as smart card or PKI USB token. 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 CA For Adobe CDS by verifying the thumbprint of the issuing certificate against that published for the Post.Trust CA For Adobe CDS at <http://www.post.trust.ie/Downloads/AdobeRootCertCheck.pdf>. 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.

## 10 Appendix B – Digital Certificate Profiles

This appendix describes the various classes of Adobe CDS digital certificates 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.

### 10.1 Post.Trust CA for Adobe Certificate Profile

#### 10.1.1 Limited Liability

Post.Trust shall only be liable to subscribers or relying parties for direct loss arising from any breach of this CPS or for any other liability they 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. Subscribers and relying parties, by accepting and relying on digital certificates are agreeing to indemnify Post.Trust, the RA and associated parties in accordance with the terms of the CPS.

Field	Critical	Value
Issuer		CN = Post.Trust CA for Adobe OU = Post.Trust CDS O = Post.Trust C = IE
Version		V3
Serial Number		(Software Generated)
Signature Algorithm		sha1RSA
Valid From		(TBD)
Valid To		(TBD)
Subject		CN = (Vendor Generated) OU = OU = L = S = E = C =
Public Key	N	RSA(2048bit)
Key Usage		Digital Signature Non-Repudiation
Basic Constraint	Y	CA: No Path Length Constraint: None
Certificate Policies	N	[1]Certificate Policy: Policy Identifier=1.2.840.113583.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier:

Notice Text=Issued subject to Post.Trust CPS for Adobe CDS & Adobe CDS CP, which limit warranties and liability of Post.Trust & Adobe. By accepting, the relying party acknowledges it has read and accepted both.

[1,2]Policy Qualifier Info:

Policy Qualifier Id=CPS

Qualifier:

<http://www.post.trust.ie/Downloads/posttrustcdscps.pdf>

Enhanced Key Usage Authority Key Identifier	Y	1.2.840.113583.1.1.5 (Acrobat Authentic Documents) KeyID=1c 7d 3f c4 00 fe aa 61 43 d6 0d fa 0e fb f2 52 6b 56 c1 e9 Certificate Issuer: Directory Address: CN=Adobe Root CA OU=Adobe Trust Services O=Adobe Systems Incorporated C=US Certificate Serial Number=3e 1c be 15
Subject Key Identifier Friendly Name CRL Distribution Points	N	f0 d0 36 c7 9b c7 fa da 04 44 0d 06 b1 2d bb 4d d7 a3 d4 d1 (Software Generated) [1]CRL Distribution Point Distribution Point Name: Full Name: URL= <a href="http://crl.trust.ie/documentsecurity/adobecds/adobe_cds.crl">http://crl.trust.ie/documentsecurity/adobecds/adobe_cds.crl</a>
Thumbprint Algorithm Thumbprint Time-Stamp		sha1 (Software Generated) URI = <a href="http://timestamp.trust.ie/tss-webclient/RequestHandler">http://timestamp.trust.ie/tss-webclient/RequestHandler</a> Authentication = Required
ArchiveRevInfo		1

## 10.2 Post.Trust CA for Adobe Qualified Certificate Profile

### 10.2.1 Limited Liability

Post.Trust shall only 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. Subscribers and relying parties, by accepting and relying on digital certificates are agreeing to indemnify Post.Trust, the RA and associated parties in accordance with the terms of the CPS.

Field	Critical	Value
Issuer		CN = Post.Trust CA for Adobe OU = Post.Trust CDS O = Post.Trust C = IE
Version		V3
Serial Number		(Software Generated)
Signature Algorithm		sha1RSA
Valid From		(TBD)
Valid To		(TBD)
Subject		CN = (Vendor Generated) OU =
	Y	OU = Qualified Certificate L = S = E = C =
Public Key	N	RSA(2048bit)
Key Usage		Digital Signature Non-Repudiation
Basic Constraint	Y	CA: No Path Length Constraint: None
Certificate Policies	N	[1]Certificate Policy: Policy Identifier=1.2.840.113583.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text=Issued subject to Post.Trust CPS for Adobe CDS & Adobe CDS CP, which limit warranties and liability of Post.Trust & Adobe. By accepting, the relying party acknowledges it has read and accepted both. [1,2]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="http://www.post.trust.ie/Downloads/posttrustcdscps.pdf">http://www.post.trust.ie/Downloads/posttrustcdscps.pdf</a>
Enhanced Key Usage		1.2.840.113583.1.1.5 (Acrobat Authentic Documents)

Post.Trust CA for Adobe Certified Document Services • Certification Practice Statement

Authority Key Identifier	Y	KeyID=1c 7d 3f c4 00 fe aa 61 43 d6 0d fa 0e fb f2 52 6b 56 c1 e9 Certificate Issuer: Directory Address: CN=Adobe Root CA OU=Adobe Trust Services O=Adobe Systems Incorporated C=US Certificate Serial Number=3e 1c be 15
Subject Key Identifier	N	f0 d0 36 c7 9b c7 fa da 04 44 0d 06 b1 2d bb 4d d7 a3 d4 d1
Friendly Name		(Software Generated)
CRL Distribution Points		[1]CRL Distribution Point Distribution Point Name: Full Name: URL= <a href="http://crl.trust.ie/documentsecurity/adobecds/adobe_cds.crl">http://crl.trust.ie/documentsecurity/adobecds/adobe_cds.crl</a>
Thumbprint Algorithm		sha1
Thumbprint		(Software Generated)
Time-Stamp		URI = <a href="http://timestamp.trust.ie/tss-webclient/RequestHandler">http://timestamp.trust.ie/tss-webclient/RequestHandler</a> Authentication = Required
ArchiveRevInfo		1

## 11 Appendix C – Post.Trust CA For Adobe CDS Certificate Profile

Field	Critical	Value
Issuer		CN = Adobe Root CA OU = Adobe Trust Services O = Adobe Systems Incorporated C = US
Version		V3
Serial Number		3E 1C BE 15
Signature Algorithm		sha1RSA
Valid From		2008/12/11 19:26:49 +01'00'
Valid To		2019/12/11 09:00:00 +01'00'
Subject		CN = Post.Trust CA for Adobe OU = Post.Trust CDS O = Post.Trust C = IE
Public Key	N	RSA(2048bit)
Key Usage		Certificate Signing Off-line CRL Signing CRL Signing (06)
Basic Constraint	Y	Subject Type=CA Path Length Constraint=1
Certificate Policies	N	[1]Certificate Policy: Policy Identifier=1.2.840.113583.1.2.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: <a href="https://www.adobe.com/misc/pki/cds_cp.html">https://www.adobe.com/misc/pki/cds_cp.html</a> [1,2]Policy Qualifier Info: Policy Qualifier Id=User Notice Qualifier: Notice Text= This certificate has been issued in conformance with the Certificate Policy found at <a href="https://www.adobe.com/misc/pki/cds_cp.html">https://www.adobe.com/misc/pki/cds_cp.html</a>
Enhanced Key Usage		1.2.840.113583.1.1.5 (Acrobat Authentic Documents)
Authority Key Identifier		KeyID=82 b7 38 4a 93 aa 9b 10 ef 80 bb d9 54 e2 f1 0f fb 80 9c de
Subject Key Identifier	N	1c 7d 3f c4 00 fe aa 61 43 d6 0d fa 0e fb f2 52 6b 56 c1 e9
Friendly Name		Post.Trust CA for Adobe
CRL Distribution Points		[1]CRL Distribution Point Distribution Point Name: Full Name: URL= <a href="http://crl.adobe.com/cds.crl">http://crl.adobe.com/cds.crl</a> [2]CRL Distribution Point Distribution Point Name: Full Name: Directory Address: CN=CRL1

	CN=Adobe Root CA
	OU=Adobe Trust Services
	O=Adobe Systems Incorporated
	C=US
1.2.840.11533.7.65.0	30 0A 1B 04 56 36 2E 30 03 02 04 90
Thumbprint Algorithm	sha1
Thumbprint	07 bb 0d 55 31 7d 05 dd 90 6e 89 f2 95 0c 97 8a 2a 81 a0 53

## 12 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.