Certificate Policy

Root Certification Authority of the Republic of Azerbaijan

DPC of the Ministry of Communications and High Technologies

14 October 2016

Version 2

Prepared by

Habib Abbasov

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change reference
October 12 2016	Habib Abbasov	2.0	Draft for review by head of CSC

Reviewers

Name	Version approved	Position	Date
Arif Mailov	2.0	Head of Certification Services Center	October 14, 2016

Table of Contents

1 Introduction

A Certificate Policy (CP) is a “named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements” [1]. The purpose of a CP is to create appropriate confidence in Certificates issued by a Certificate Authority (CA) complying with the particular policy.

This CP is intended to have broad applicability across the different technical platforms and organizational structures of the Certification Services Center of Data Processing Center (DPC CSC) of the Ministry of Communications and High Technologies. It is therefore focused on requirements that are not bound to specific technical solutions. The CP is complemented with the Certification Practice Statements (CPS) of specific Certification Authorities (CSC CPS RCA, CSC CPS PCA, CSC CPS GOV ICA, CSC CPS EGOV ICA) [2], which outline the technical, procedural and personnel policies and practices of DPC CSC.

This CP is intended to fulfill the provisions of the “Electronic Signature and Electronic Documents” Law of the Republic of Azerbaijan (AZ DSEDL) [3].

This CP is also intended to comply with ETSI TS 101 456 V1.4.3 “Policy requirements for certification authorities issuing Qualified Certificates” [4], which references to PKIX “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” IETF RFC 3647 (2003) [5].

1.1 Identification

This is the Certificate Policy of Root Certification Authority of DPC (DPC CSC CP). The primary source of the current version of the CP and other important DPC CSC documents is http://www.e-imza.az.

The CP has been approved by the Director of Data Processing Center CSC on 14 October, 2016.

Title: Certificate Policy of Root Certification Authority of the Republic of Azerbaijan

Version: 2.0

Date: 14 October 2016

OID: 1.3.6.1.4.1. 32843.1.1.1

Meaning of single numbering fields:

ISO	1
Identified Organization	3
DoD	6
Internet	1

Private enterprise	4
IANA registered private enterprise	1
IANA number	32843
Department (Certificate Services Center)	1
Type of document (Policy)	1
Version	1

Expiration: This version of the document is the most current one until a subsequent release.

The CP is published at URL http://*.e-imza.az/repository (value of prefix * depends on the certification authority and is either „ehm" for E-Government or „hom" for Governing bodies).

By including this unique object identifier in a Certificate the CA claims conformance to the identified CP.

The CA shall also include the identifier for this CP in the terms and conditions of contract made available to Subjects, Subscribers and Relying Parties to indicate its claim of conformance.

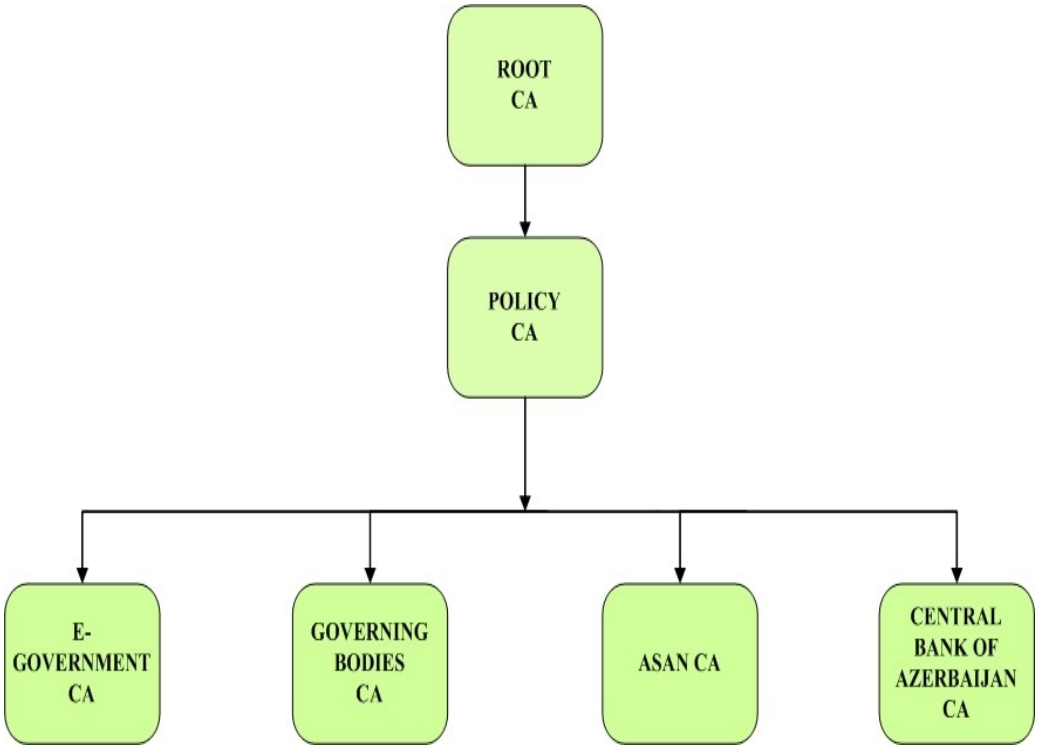
1.2 General Architecture

DPC CSC´s overall architecture is based on a three-tier CA structure. This architecture will allow the Root CA, which serves as the basis of all subsequent CAs and Certificates, to be stored off-line. The off-line nature of the root is the most secure method to protect this critical component of the CA. The three-tier architecture will also allow for maximum flexibility, as the second tier will be the Policy CAs. The Policy CA's will be responsible for the policy as applies to the Issuing CAs (the third tier).

The CA entities are defined as follows:

- Root Certificate will be self-signed as the Root CA is the top entity in this hierarchy ("Trust anchor"). The Root CA will issue Certificates for the Policy CA.
- according to DPC policy requirements there is one Policy CA. The Policy CA will issue CA Certificates to the Issuing CA's at Governing Bodies Certification Authority, e-Government Certification Authority, Time Stamping Authority (TSA) and other newly created Certificate centers;
- the Issuing CAs will be used to issue the Qualified Signature Certificates, Non-Qualified Authentication Certificates, Non-Qualified Infrastructure Certificates to the End Users, as well as Non-Qualified and Non-Public Certificates to the infrastructure systems of DPC CSC IS. Certificates of Issuing CA's will be signed by the Policy CA. An Issuing CA has its own Directory Services and publishes CRL's and Certificates directly to its Directory and Certificate Database.

The diagram below is showing the hierarchical architecture of DPC´s Certification Services



Hierarchical architecture of DPC´s Certification Services

1.3 Certificates and Holders

The following table shows Certificates issued by each Certification Authority. All DPC CSC´s Certification Authorities will be restricted to issuing only those Certificates required by their function.

Type	Name	Public	QC	Usage	Com-pliant to CP	Issuer
End-User Certificate	Qualified Digital Signature Certificate	✓	✓	Create and verify qualified digital signatures and support non-repudiation at high assurance level	✓	DPC CSC GOV ICA DPC CSC EGOV ICA
	Authentication Certificate	✓		Client authentication at high assurance level	✓	DPC CSC GOV ICA DPC CSC EGOV ICA
CA Certificate	DPC CSC RCA Certificate	✓		CA Certificate and CRL signing	✓	RCA
	DPC CSC PCA Certificate	✓		CA Certificate and CRL signing; TSA Certificate	✓	RCA
	DPC CSC GOV ICA Certificate	✓		End-User Certificate and CRL signing; OCSP Responder certificate; Infrastructure certificates	✓	PCA
	DPC CSC EGOV ICA Certificate	✓		End-User Certificate and CRL signing OCSP Responder certificate Infrastructure certificates	✓	PCA
Service Certificate	DPC CSP GOV OCSP Certificate			Certificate Validation Response signing	✓	DPC CSP GOV ICA
	DPC CSP EGOV OCSP Certificate			Certificate Validation Response signing	✓	DPC CSC EGOV ICA
	TSA Certificate	✓		Time Stamp Token signing	✓	PCA
Infrastructure Certificate	Code Signing Certificate			AuditLog Signing Archive Signing		DPC CSC GOV ICA DPC CSC EGOV ICA
	Enrolment Agent Certificate			Certificate request agent signing Certificate		DPC CSC GOV ICA DPC CSC EGOV ICA
	Web Server			Web server authentication within internal DPC CSC		DPC CSC

Certificate	environment and public CSC Web	GOV ICA DPC CSC EGOV ICA
CA Exchange Certificate	Encryption Certificate used by client systems to encrypt their private keys as part of their Certificate Request	DPC CSC GOV ICA DPC CSC EGOV ICA

This CP is valid only for Certificates which explicitly reference the OID number of this CP in their X509 V3 **CertificatePolicies** fields.

Furthermore, the following attributes shall be applied to Root CA:

X509 V3 Standard Fields	Content	Meaning
Signature Algorithm	Sha1WithRSAEncryption	Asymmetric cryptographic algorithm
Valid Not Before	Issuing Date	Validity begins
Valid Not After	Issuing Date + 18 years	Validity period of 18 years
RSA Public Key	4096 bit	Signature: 4096 bit Authentication: 4096 bit

1.3.1 End-User Certificates

In this CP, two different terms are used for End-Users: "*Subscriber*" who contracts with DPC CSC for the issuance of Certificates, and "*Subject*" to whom the Certificate applies. The Subscriber bears responsibility towards DPC CSC for the use of the Private Key associated with the Public Key Certificate but the Subject is the individual that is authenticated by the Private Key and that has control over its use. In the case of Certificates issued to individuals for their own use the Subscriber and Subject is the same entity.

In other cases, such as Certificates issued to organization employees, the Subscriber and Subject are different entities. The Subscriber would be, for example, the employer. The Subject would be the employee.

Certificates which will be issued to the Subject (Subscriber) are Qualified Signature Certificates and Non-Qualified Authentication Certificates.

- **Qualified Signature Certificates** issued to a Subject (Subscriber) to support creation and verification of electronic signatures.

- **Non-Qualified Authentication Certificates** issued to a Subject (Subscriber) to support authenticating purposes.

End User Certificates are issued under this CP.

1.3.2 CA Certificates

Each Certification Authority in the DPC CSC CA hierarchy needs an own Certificate to sign the Certificates it issues. As an exception, the Root CA´s Certificate will be self-signed.

Certificates which will be issued to a Certification Authority are Non-Qualified Signature Certificates.

- **DPC CSC RCA Certificate** is issued to DPC CSC´s Root CA;
- **DPC CSC PCA Certificate** is issued to DPC CSC´s Policy CA;
- **DPC CSC ICA Certificates** are issued to DPC CSC GOV ICA and DPC CSC EGOV ICA.
- **ASAN CA Certificate** is issued to CSC of State Ageny for Public Service and Social Innovations under the President of the Republic of Azerbaijan [registration information has been included in register of certificate services centers];
- **Central Bank of Azerbaijan CA Certificate** is issued to CSC of Central Bank of Azerbaijan [registration information has been included in register of certificate services centers].

CA Certificates are issued under this CP.

1.3.3 Service Certificates

On-line Certificate Validation Services are supported by the OCSP Responder which gives trusted information about the current state of End User and CA Certificates. Response Messages to Validation Request are signed with the OCSP Certificate.

Time Stamping Services are supported by the Time Stamping Authority which signs the Time Stamp Tokens with the TSA Certificate.

- **OCSP Certificate** is issued to DPC CSC GOV OCSP Responder and to DPC CSC EGOV OCSP Responder;
- **TSA Certificate** is issued to DPC CSC´s Time Stamp Authority.

CA Certificates are issued under this CP.

1.3.4 Infrastructure Certificates

Infrastructure Certificates will be rarely issued. In this CA hierarchy, DPC CSC GOV ICA and DPC CSC EGOV ICA issuing CA's will be mainly used for Infrastructure Certificate issuing purposes.

Holders of Infrastructure Certificates are server hardware and functions which are necessary for the operation of the DPC CSC infrastructure.

Requirements concerning the issuance, management and usage of Infrastructure Certificates are defined in an internal document, which is not intended for the public access.

1.4 User Community and Applicability

This CP describes the rights and obligations of all participants – i.e., all persons and entities authorized under this CP to fulfill any of the following roles:

- Policy Management Authority;
- Certification Authority;
- Registration Authority;
- Repository;
- Certificate Holder; and
- Authorised Relying Party.

1.4.1 PKI Participants

1.4.1.1 Policy Management Authority

The Policy Management Authority (PMA) for this CP is DPC CSC Head of Certification Services, who will administer the policy decisions regarding this CP.

1.4.1.2 Root CA

The Root CA is an organisation authorised by DPC CSC to create, sign, issue and manages Certificates for Policy CA as well as Trusted Subordinate CA's. The Root CA also signs its own Certificates. The Root CA is bound to act according to the terms of this CP.

1.4.1.3 Policy CA

The Policy CA is an organization authorized by DPC CSC to create, sign, issue and manages Certificates for Issuing CA's (DPC CSC GOV ICA and DPC CSC EGOC ICA) as well as Time Stamping Authority. The Policy CA is bound to act according to the terms of this CP.

1.4.1.4 Issuing CA's

Issuing CA's (DPC CSC GOV ICA and DPC CSC EGOV ICA) are organizations authorized by DPC CSC to create, sign, issue and manage End User Certificates. Each Issuing CA is bound to act

according to the terms of this CP. An Issuing CA's specific practices, in addition to the more general requirements set out in this CP, must be set out in a Certification Practice Statement adopted by the Issuing CA and approved by DPC CSC. The Issuing CA's CPS will set forth, among other things, the types of DPC CSC Certificates to be issued by the Issuing CA (e.g., signature Certificates, authentication Certificates, etc.). An Issuing CA must enter into an agreement with DPC CSC for the benefit of all End Entities, to be bound by and comply with the undertakings and representations of this CP, with respect to all Certificates it issues.

1.4.1.5 Registration Authorities (RA's)

Each Issuing CA will remain ultimately responsible for all DPC CSC Certificates it issues. However, under this CP, the Issuing CA may subcontract registration and I&A functions to an organization that agrees to fulfill the functions of an RA in accordance with the terms of this CP, and who will accept DPC CSC Certificate applications and locally collect and verify Applicant identity information to be entered into an DPC CSC Certificate. An RA operating under this CP is only responsible for those duties assigned to it by the Issuing CA pursuant to an agreement with the Issuing CA or as specified in this CP.

1.4.1.6 Repository

The CA will perform the role and functions of the Repository. The CA may subcontract performance of the Repository functions to a third party organization that agrees to fulfill the functions of a Repository, and who agrees to be bound by this Policy, but the CA remains responsible for the performance of those services in accordance with this Policy.

1.4.2 End Entities

1.4.2.1 Certificate Holders

The Issuing CA may issue DPC CSC Certificates to the following classes of Certificate Holders: Individuals or Businesses (e-Government Certification Authority) and Organizations (Governing Bodies Authority).

1.4.2.2 Authorized Relying Parties

This CP is intended for the benefit of Individuals and Organizations who have agreed on the terms of an Authorized Relying Party Agreement to be bound by this CP.

1.4.3 Applicability and Applications

1.4.3.1 Purpose

DPC CSC Certificates are intended to support verification of Digital Signatures in applications where:

- a message or file needs to be bound to the identity of its originator by a signature;
- the integrity of the file or message has to be assured; or
- the identity of communicating parties needs to be authenticated.

1.4.3.2 Approved Applications

Applications for which DPC CSC Certificates are suitable include:

Certificate Directory: Certificate Directory service provides the required functionality of publishing certificates. It contains CA and TSA certificates and active certificates issued to DPC CSC clients for which the client has given permission to be made publicly available. Certificate Directory contains also Certificate Revocation Lists (CRL) for CA's and TSA. DPC CSC services are responsible for maintaining information in the directory up-to-date. Certificate Directory service is public and therefore is available to callers using LDAPv3 over SSL.

Certificate Validation: Certificate Validation Service provides access to the following information:

- status of Root CA Certificate (CSC Web);
- status of Certificates issued by Root CA (CRL);
- status of Certificates issued by all Policy CAs (CRL);
- status of Certificates issued by all Issuing CAs (OCSP).

The OCSP Responders of DPC CSC (DPC CSC GOV OCSC and DPC CSC EGOV OCSP) are based upon Online Certificate Status Protocol (OCSP) according to RFC 6960.

Time Stamping: Time Stamping Services are based upon TSP (Time Stamping Protocol) defined by the RFC 3161 standard, which are extended to support authentication of the Time Stamp requestor. DPC CSP Time Stamping Services can be used by third party applications for time stamping the electronic documents. It is used also by stand alone electronic document signing application provided by DPC CSC.

Electronic Document Authoring: DPC CSC provides standalone application for document authoring and signing (signer application) as well as electronic document format specification. The application is distributed for free. The application for document authoring and signing provides the following functionality:

- creating electronic document, corresponding to the format specified by DPC CSC;
- Time Stamping the electronic document;
- digitally signing the electronic document; and
- verifying signature and Time Stamp.

Signer application is supported on Microsoft Windows XP SP2 and higher operating systems. It is

stand-alone rich-client application.

1.4.3.3 Prohibited Applications

DPC CSC Certificates may not be used for any application which is not approved and published by DPC CSC.

1.5 CA Conformance

The CA shall only use the identifier of this CP as given in section 1.1:

- if the CA claims conformance to this CP and makes available to Subjects and Relying Parties on request the evidence to support the claim of conformance; this evidence can be, for example, a report from an auditor confirming that the CA conforms to the requirements of this CP. The auditor may be internal to the CA organisation but should have no hierarchical relationship with the department operating the CA;
- if the CA has a current assessment of conformance to this CP by a competent independent party selected from the Ministry of Communications and High Technologies of the Republic of Azerbaijan. The results of the assessment shall be made available to Subjects and Relying Parties on request;
- if the CA is later shown to be non-conformant in a way that significantly affects its ability to meet the requirements for Qualified Certificates identified in DSEDL [3] it shall cease issuing Certificates using the identifiers in section 1.1 until it has demonstrated or been assessed as conformant, otherwise the CA shall take steps to remedy the non-conformance within a reasonable period; and
- the CA compliance shall be checked on a regular basis and whenever major change is made to the CA operations.

1.6 Policy Administration

1.6.1 Organization Administering this Document

This CP is registered by Data Processing Center of Ministry of Communications and High Technologies [Dilara Aliyeva 185, A1010, Baku, Republic of Azerbaijan].

DPC CSC is fully responsible for registration, maintenance and interpretation of the policy.

1.6.2 Contact Information

Contact information for questions related to this policy:

Address	**Data Processing Center of the Ministry of Communications and**

	High Technologies, Certificate Services Center [Dilara Aliyeva 185, A1010, Baku, the Republic of Azerbaijan]
Phone	+(99412) 5982691
Fax	+(99412) 5651452
Email	office@rabita.az

1.6.3 Person Determining CPS Suitability for the Certification Policy

The DPC's Head of Certificate Services Center has the final authority for approving the CPS [2] and the responsibility for ensuring the practices are properly implemented.

1.6.4 CPS Approval Procedures

Certification Practice Statements intended for use under DPC CSC must be approved by the Head of Certificate Services Center.

2 Obligations and Liability

2.1 CA Obligations

The CA operates Certification Authority Services. The main obligations are:

- provide protection of Private Keys;
- provide correct information in the issued Certificates;
- provide correct identification of the person for whom it is issuing the Certificate;
- provide publication of all public information such as Certificates and Certificate Revocation Lists;
- protect its Private Key used to sign the Certificates;
- handle Certificate Requests and issue new Certificates:
    - accept and confirm Certification Requests from entities requesting a Certificate according to the agreed procedures contained in this CP and in the CPS's;
    - ensure validity and correctness of information in Certificates;
    - authenticate entities requesting a Certificate, possibly by the help of separately designated Registration Authorities (RAs);
    - issue Certificates based on authenticated entities´ requests;
    - send notification of issued Certificate to requesters;
    - make issued Certificates publicly available;
- handle timely Certificate Suspension Requests and Certificate Suspension:

- accept and confirm Suspension Requests from entities requesting a Certificate to be suspended according to the agreed procedures contained in the CPS of the Issuing CA;
- authenticate entities requesting a Certificate to be suspended;
- revoke the Certificate in question;
- make CRLs publicly available;

- handle Certificate Suspension Termination Requests and terminate Suspension of Certificate:
  - accept and confirm Suspension Termination Requests from entities requesting a Termination of Suspension of Certificate according to the agreed procedures contained in the CPS of the Issuing CA;
  - authenticate entities requesting a Suspension Termination of a Certificate; and
  - remove re-activated Certificates from CRL's.

2.2 RA Obligations

An RA operates an RA service. RA obligations are:

- authenticate the identity of the Subject with help of the AZ Resident Register (or IAMAS ID Register);
- validate the connection between a Public Key and the Applicant´s identity including a suitable proof of possession method;
- to confirm such validation versus the CA; and
- to adhere to the agreement made with the CA.

2.3 Subscriber Obligations

The term “Subscriber” used in this context means End-User of Certificates issued by an Issuing CA.

A Subject (Subscriber) shall behave according to the CPS of the Issuing CA. This includes:

- to enter a Subscriber Agreement, which outlines the obligations of the Subscriber and Subject stating the terms and conditions of use of the issued Certificates, including permitted applications and purposes as specified in the CPS of the Issuing CA;
- to read and adhere to the agreed procedure;
- to properly protect its Private Key as the only possessor if the subscription refers to an individual person;
- use the Private Keys only for the purposes identified in the CP;
- to accept that in the usage of Public Key Certificates CA´s liability is limited according to what is specified by section 2.7;
- to authorise the treatment and preservation of personal data; and
- to notify immediately the Issuing CA upon a Private Key compromise.

2.4 Relying Party Obligations

Before using a Certificate, a Relying Party must ensure that:

- the CA can be trusted;
- the Certificate is appropriate for the intended use;
- the Certificate was issued as a valid Certificate, by using the Certification Path Validation Procedure specified in PKIX RFC 5280 ”Internet X.509 Public Key Infrastructure Certificate and CRL Profile” [8];
- the Certificate is valid by consulting the Certification Status Service of the CA; and
- the application software can process the content of the Certificate and its extensions in accordance with this CP and PKIX RFC 5280 ”Internet X.509 Public Key Infrastructure Certificate and CRL

Profile"[8].

A Relying Party must be familiar with the CPS's and this CP before drawing any conclusion on how much trust he can put in the use of a Certificate issued from the CA. A Relying Party must check Directory or Validation Services when validating a Certificate. Moreover, a Relying Party must only use a Certificate for the proscribed applications and must not use the Certificates for forbidden applications.

2.5 Cross-Certification

DPC CSC shall support the establishment of certification services by third parties at agreed levels.

The DPC CSC Root CA shall issue CA Certificates to third parties´ Subordinate Certification Authorities only upon a complete auditing review to ensure compliance and interoperability for cross-certification purposes.

By issuing Certificates for Subordinate center's, the DPC CSC Root CA shall control the policy of Subordinate CA's including whether additional CA's can be added to the hierarchy by Subordinate CA's.

2.6 Publication and Repository Obligations

2.6.1 Publication of CA Information

DPC CSC shall be responsible for repository functions. DPC CSC shall publish Certificates in the DPC CSC´s repository based on Certificate Applications approved by the RA as well as revocation information concerning such Certificates.

CPS documents of DPC CSC´s Root CA, Policy CA, Issuing CAs, Infrastructure Certificates, Subscriber Agreements, and Relying Party Agreements and a link to this CP shall appear in DPC CSC´s repository on DPC CSC Website.

DPC CSC´s Certification Authorities shall publish issued Certificates as disclosed in the appropriate CPS. Upon revocation of a Subscriber's Certificate, the Issuing CA that issued the Certificate shall publish notice of such revocation in the repository. In addition, the CAs shall issue CRLs and provide Certificate Validation Services with the OCSP Responder. Meaning and legal strengths of provided validation methods should be specified in appropriate CPS.

2.6.2 Frequency of Publication

CA information shall be published promptly after it is made available to the appropriate CA. CPS's shall contain provisions relating to amendments made to them, and changes to the CPSs shall be

published in accordance with such provisions.

CRL's for Subscriber Certificates shall be issued at least weekly. CRL's for CA Certificates shall be issued at least quarterly, but also whenever a CA Certificate is revoked. CRL's for Root CA Certificates are published quarterly and also whenever a CA Certificate is revoked. If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs after the Certificate's expiration.

Online revocation and other Certificate status information shall be available via a public directory and OCSP. DPC CSC shall provide Relying Parties with information on how to find the appropriate repository to check Certificate status and the OCSP Responder.

2.6.3 Access Controls

DPC CSC shall not intentionally use technical means of limiting access to this CP, the CPS's, Certificates, Certificate Status Information, or CRL's. DPC CSC shall, however, require persons to agree to a Relying Party Agreement as a condition to accessing Certificates, Certificate Status Information or CRLs.

DPC CSC shall implement controls to prevent unauthorized persons from adding, deleting or modifying repository entries.

2.6.4 Help Desk

DPC CSC shall offer a Help Desk (DPC CSC HD) whose functions include the following:

- accessible 24 hours a day 7 days a week;
- querying information about Certificate Status;
- accepting request for suspension of Certificates; and
- forward specific calls considering operations with Certificates to appropriate DPC CSC employee.

2.7 Liability

2.7.1 CA Liability

By signing a Certificate containing a Policy Identifier, which indicates the use of this policy (e.g. OID of the CP), the CA ensures that its certification and publication services, issuance and revocation of Certificates, and issuance of CRLs is in accordance with this CP. It will also ensure that all RAs and Subscribers (Subjects) will follow the requirements of this policy when dealing with any Certificates containing this policy's ID or the associated keys.

CA liability will be restricted to the guarantee of making the necessary controls to verify the identity of

every requester as described in the CPS's and to the adoption of the minimal security measures needed to protect CA´s Private Key. Moreover:

- The CA shall be liable for losses that are caused to a person or organisation who reasonably relied upon the Certificate in relation to:
  - compliance with the requirements of this CP;
  - the information included in the Certificate;
  - the conformity of the Private Key to the Public Key included in the Certificate at the moment of the issue the Certificate; and
  - the utilization of both keys in an appropriate way.
- The CA shall be liable for losses that are caused to a person or organisation who reasonably relied upon the Certificate if the revocation or suspension of operation of such Certificate was not registered according to the provisions of DSEDL; and
- The CA shall not be liable for losses that are caused to a person who reasonably relied upon the Certificate that is utilised disregarding the conditions or restrictions included therein or exceed the transaction amount indicated in the Certificate.

2.7.2 RA Liability

See section 2.2.

2.7.3 Disclaimers of Warranties and Obligations

DPC CSC disclaims all liability for any use other than the intended, as identified by this CP, of Certificates issued under this CP. Any dispute concerning key or Certificate management under this CP is to be resolved by the parties concerned as stated in this CP.

Certificates issued in compliance with this CP and containing this policy's OID are only used for purposes specified in certification practice statements.

The CA makes effort to warrant nearly 100% availability of services offered under this CP. System maintenance, system repair or factors outside the control of the CA may affect such availability.

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Name Convention

CA and Subscriber Certificates shall contain an X.501 Distinguished Name in the Subject Name field. The Subject Distinguished Name of CA or Subscriber Certificates shall include a Common Name (CN) component. The authenticated Common Name value included in the Subject Distinguished Names of CA Certificates shall be the legal name of the organization or unit within the organization. The common name value included in the Subject Distinguished Name of individual Certificates shall represent the individual's generally accepted personal name.

3.1.2 Uniqueness of Names

Each Certificate shall contain a unique set of Distinguished Name attributes. These attributes include a collection of the person's name, company name, organizational unit and a unique identifier. The unique identifier is either the personal code from the document of identification or a unique identifier assigned by the CA system (for each Certificate that uses a pseudonym).

Any Certificate Request which is not unique shall be rejected by the DPC CSC. Subscribers who are rejected by the CA because their name is not unique shall be notified as promptly as is operationally possible.

A Subject may have two or more Certificates with the same Subject Distinguished Name.

3.1.3 Names Problem Resolving

In their Certificate Applications, Applicants shall not use names that infringe upon the intellectual property rights of others. DPC CSC shall not be required to determine whether a Certificate Applicant has intellectual property rights in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark.

DPC CSC shall be entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.1.4 Way of Confirmation Private Key Ownership

This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber, for example where pre-generated keys are placed on smart cards.

3.1.5 Authentication of Organization Identity

The identity of organizational Subscribers and other enrolment information provided by Certificate Applicants shall be confirmed in accordance with the procedures set forth in DPC CSC's documented Certificate Application processing procedures.

Procedures for the authentication of organizational identity established by third parties´ Certification Services shall be submitted to DPC CSC for approval. Such approval shall be a condition of a third party beginning its operation as a CA to approve Certificate issuance.

3.1.6 Authentication of Individual Identity

The authentication procedures are confirming that the Certificate Applicant is the person identified in the Certificate Application.

The authentication related to non-organizational Certificates is based on the personal (physical) presence of the Certificate Applicant before an RA Officer. The RA Officer shall check the identity of the Certificate Applicant against a well-recognized form of government-issued identification, such as a passport.

3.2 Certificate Renewal

Certificate Renewal is the process of issuing of a new Certificate with a new Certificate number and a new validity period but with the same public key and other information included in the Certificate.

Certificate Renewal is not supported.

3.3 Request for Suspension or Revocation

The DPC CSC System Officer must authenticate that a Request for Suspension or Revocation of a Subject Certificate is complete, accurate and duly authorized.

All Suspension or Revocation Requests are required to be valid. Such validity shall be determined by their compliance or non-compliance with the procedures defined in the CPSs, which include references to the authority of the person who may make a request.

Revocation of Certificates will be conducted after communication with the DPC CSC System Officer and the DPC CSC Security Officer. A Request of Revocation of Subject Certificates must be done in written form on paper.

4 Requirements on CA Practice

CA practice includes the provision of services for registration, Certificate generation, Certificate dissemination, revocation management, suspension management, and revocation or suspension status.

4.1 Certification Practice Statement (CPS)

The appropriate CA shall ensure that it demonstrates the reliability necessary for providing Certification Services. In particular:

- the appropriate CA shall have a statement of the practices and procedures used to address all the requirements identified in this CP;
- the CPS of the appropriate CA shall identify the obligations of all external organisations supporting the CA services including the applicable policies and practices;
- the appropriate CA shall make available to Subscribers, Subjects and Relying Parties its CPS and other relevant documentation, as necessary to assess conformance to this CP;
- the appropriate CA shall disclose to all Subscribers, Subjects and Relying Parties the terms and conditions regarding use of the Certificate as specified in section 4.3.3;
- the appropriate CA shall have a high level management body with final authority and responsibility for approving the CPS;
- as senior management of the CA, the CA Officer is responsible for ensuring that the certification practices established to meet the applicable requirements specified in the current document are properly implemented;
- the appropriate CA shall define a review process for certification practices including responsibilities for maintaining the CPS;
- the appropriate CA shall give due notice of changes it intends to make in its CPS and shall make the revised CPS immediately available as required; and
- the appropriate CA shall document the signature algorithms and parameters employed.

4.2 Public Key Infrastructure - Key Management Lifecycle

4.2.1 Certification Authority Key Generation

The CA shall ensure that CA keys are generated in described and controlled circumstances. In particular:

- Certification Authority Key Generation shall be undertaken in a physically secure environment (see section 4.4.5) by personnel in Trusted Roles (see section 4.4.4) under, at least, dual control. The number of personnel authorised to carry out this function shall be kept to a minimum and be consistent with the CA's practices;
- CA Key Generation shall be carried out within a device which meets the requirements identified in

FIPS 140-2 [10], level 3 or higher;

- Certification Authority Key Generation shall be performed using an algorithm recognised as being fit for the purposes of Certificates;
- the selected key length and algorithm for CA Signing Key shall be one which is recognised as being fit for the purposes of Certificates as issued by the CA; and
- a suitable time before expiration of its CA Signing Key (for example, as indicated by expiration of CA Certificate), the CA shall generate a new Certificate signing key pair and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA key. The new CA key shall also be generated and distributed in accordance with this CP.

4.2.2 Certification Authority Key Storage

The CA shall ensure that CA Private Keys remain confidential and maintain their integrity. In particular:

- the CA Private Signing Key shall be held and used within a secure cryptographic device which meets the requirements identified in FIPS 140-2 [10], level 3 or higher; and
- where the keys are stored in a dedicated key processing hardware module, access controls shall be in place to ensure that the keys are not accessible outside the hardware module.

CA Private Keys are not backed up. In case of losses, Private Keys can be re-created by means of System Cards of the cryptographic hardware device.

4.2.3 Certification Authority Public Key Distribution

The CA shall ensure that the integrity and authenticity of the CA Public Key for Signature Verification and any associated parameters are maintained during its distribution to Relying Parties.

In particular, CA Public Key shall be made available to Relying Parties in a manner that assures the integrity of the CA Public Key and authenticates its origin.

4.2.4 Key Escrow

Key escrow is not supported.

4.2.5 Certification Authority Key Usage

The CA shall ensure that CA Private Signing Key is not used inappropriately.

In particular:

- CA Private Signing Key used for generating Certificates or issuing revocation status information, shall

not be used for any other purpose; and

- the Certificate Signing Key shall only be used within physically secure premises.

4.2.6 End of CA Key Lifecycle

The CA shall ensure that CA Private Signing Key is not used beyond the end of its lifecycle. In particular, all copies of the CA Private Signing Key shall be destroyed or put beyond use.

4.2.7 Lifecycle Management of Cryptographic Hardware Used to Sign Certificates

The CA shall ensure the security of cryptographic hardware throughout its lifecycle. In particular, the CA shall ensure that:

- Certificate and revocation status information signing cryptographic hardware is not tampered with during shipment;
- Certificate and revocation status information signing cryptographic hardware is not tampered with while stored;
- the installation, activation, backup and regeneration of the CA's Signing Keys in cryptographic hardware shall require simultaneous control of at least of two Trusted Persons;
- Certificate and revocation status information signing cryptographic hardware is functioning correctly; and
- CA private signing key stored on CA cryptographic hardware is destroyed upon device retirement.

4.2.8 CA-Provided Subject Key Management Services

The CA shall ensure that Subject keys are generated in described and controlled circumstances in a secure environment operated by DPC CSC or its contracting party. In particular:

- Subject keys shall be generated using an algorithm recognised as being fit for the purposes of Qualified electronic signatures during the validity time of the Certificate;
- Subject keys shall be of a key length and for use with a Public Key algorithm which is recognised as being fit for the purposes of qualified electronic signatures during the validity time of the Certificate;
- Subject keys shall be generated
  - for qualified certificates, within an SSCD type 3 which was EAL4+ evaluated in accordance to ISO/IEC 15408;
  - for non-qualified certificates, in a manner such that the secrecy and the integrity of the key is not compromised;
- Subject's Private Key

- for qualified certificates shall be delivered to the Subject, if required via the Subscriber, in a manner such that the secrecy and the integrity of the key is not compromised and, once delivered to the Subject, the Private Key can be maintained under the Subject's sole control;
- for non-qualified certificates shall be stored in a manner such that the secrecy and the integrity of the key is not compromised and the Private Key can be maintained under the Subject's sole control;

- Subject's Private Key shall not be backed up and recovered.

4.2.9 Secure-Signature-Creation Device Preparation

The CA shall ensure that if it issues SSCD this is carried out securely. In particular:

- SSCD preparation shall be securely controlled;
- SSCD shall be securely stored and distributed;
- SSCD activation and deactivation shall be securely controlled; and
- where the SSCD has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the SSCD.

4.3 Certificate Management Lifecycle

4.3.1 Subject Registration

4.3.1.1 Certificate Application

All procedures and requirements with respect to an application for a Certificate are set out in the CPS of the Issuing CA. RA must ensure that each application be accompanied by:

- proof of the identity of the Subject;
- when the Applicant is not the Subject, proof of authorisation to act on behalf of the Subject;
- proof of authorisation for any requested Certificate attributes; and
- a signed Subscriber agreement.

The decision of whether to issue a Certificate is at the sole discretion of the RA.

Upon successful performance of all required authentication procedures, the RA receiving the Certificate Application shall approve the Certificate Application. If authentication is unsuccessful, the RA shall deny the Certificate Application.

4.3.1.2 Subscriber´s Data Recording

Before entering into a contractual relationship with a Subscriber, the RA shall inform the Subscriber of

the terms and conditions of contract. The CA shall record all the information used to verify the Subject's identity, including any reference number on the documentation used for verification, and any limitations on its validity.

The CA shall record the signed agreement with the Subscriber including:

- agreement to the Subscriber's obligations;
- consent to the keeping of a record by the CA of information used in registration, Subject device provision and any subsequent revocation, and passing of this information to third parties under the same conditions as required by this policy in the case of the CA terminating its services; and
- confirmation that the information held in the Certificate is correct.

The records identified in above shall be retained for the period of time as indicated to the Subscriber and as necessary for the purposes for providing evidence of certification in legal proceedings.

The CA shall ensure that the requirements of the national data protection legislation are adhered to within their registration process.

4.3.1.3 Certificate Issuance

After the authentication accomplished by RA, the CA shall issue the Certificate. If for any reasons CA decides not to issue the Certificate (even if the checks and the authentication were correct) it should notify the reason for this choice to the Applicant.

Upon issuance, Certificates shall be made available to Subjects.

The CA shall, either directly or through an RA, notify Subjects that their Certificates are available and that the Subjects may retrieve the Certificate.

4.3.1.4 Subscriber Private Key and Certificate Usage

The CA shall make available to Subscribers, Subjects and Relying Parties the terms and conditions regarding the use of the Certificate:

- the CP being applied;
- any limitations on its use;
- the Subscriber's and Subject ´s obligations as defined in section 2.3;
- information on how to validate the Certificate, including requirements to check the revocation status of the Certificate;
- limitations of liability including the purposes or uses for which the CA accepts (or excludes) liability;
- the period of time for which registration information is retained;

- the period of time for which CA event logs are retained;
- procedures for complaints and dispute settlement;
- the applicable legal system; and
- whether the CA has been certified to be conformant with the identified Qualified Certificate Policy, and if so, through which scheme.

The information identified in above shall be available through a durable means of communication, which may be transmitted electronically, and in readily understandable language.

The use of Private Keys is only permissible after activation of Certificates. Permissible and inadmissible applications of the keys and Certificates are defined in this CP. In addition, the Certificate Subject must fulfill Subscriber obligations when using his Private Keys.

4.3.1.5 Relying Party Public Key and Certificate Usage

Certificates compliant to this CP shall only be applied to applications specified in Certification Practice Statement.

The use of the Certificates by Relying Parties must follow this CP.

4.3.1.6 Certificate Modification, Re-key and Key Change Over

Certificate Modification is the issuance of a new certificate due to changes in the information in the certificate other than the subscriber public key. Certificate Modification is not supported.

Certificate Re-Key means the generation of a new key pair and applying for the issuance of a new certificate that certifies the new public key. Certificate Re-Key is not supported. A new certificate must be applied for as indicated in section 3.1.

Key Changeover is the procedure to publish the new Certificate following a certificate Re-Key by the CA. DPC CSC's Key Changeover procedures may be the same as the procedure for providing the current key. Also, the new key may be certified in a certificate signed using the old key. Key changeover of CA, TSA and OCSP signing keys must be planned in order to ensure a continuous availability of DPC CSC's Certification Services (see section 4.4.9.6).

4.3.2 Certificate Generation

The CA shall ensure that it issues Certificates securely to maintain their authenticity. In particular:

- the Qualified Certificates and Non-Qualified authentication Certificates are generated and issued in accordance with DSEDL;

- Infrastructure Certificates are generated in secure environment;
- the CA shall take measures against forgery of Certificates and guarantee confidentiality during the process of generating such data;
- the procedure of issuing the Certificate is securely linked to the associated registration including the provision of the Public Key generated to the Subject;
- the procedure of issuing the Certificate is securely linked to the generation of the key pair by the CA;
- the Private Key of Qualified Certificate and Authentication Certificate is securely passed to the registered Subject;
- the CA shall ensure over time the uniqueness of the Distinguished Name assigned to the Subject within the domain of the CA (i.e. over the life time of the CA a distinguished name which has been used in an issued Certificate shall never be re-assigned to another entity);
- the confidentiality and integrity of registration data shall be protected especially when exchanged with the Subscriber, Subject or between distributed CA system components; and
- in the event that external registration service providers are used, the CA shall verify that registration data is exchanged with recognised registration service providers, whose identity is authenticated.

4.3.3 Dissemination of Terms and Conditions

The CA shall ensure that the terms and conditions of use of Certificate are made available to Subjects, Subscribers and Relying Parties. These are:

- the CP being applied, including a clear statement as to whether the policy is for Certificates issued to the public;
- any limitations on its use;
- the Subscriber's and Subject´s obligations;
- information on how to validate the Certificate, including requirements to check the revocation status of the Certificate, such that the Relying Party is considered to reasonably rely on the Certificate;
- limitations of liability including the purposes and uses for which the CA accepts (or excludes) liability;
- the period of time for which registration information is retained;
- the period of time for which CA event logs are retained;
- procedures for complaints and dispute settlement;
- the applicable legal system; and
- if the CA has been certified to be conformant with the identified CP, and if so through which scheme.

The information identified above shall be available through a durable means of communication, which may be transmitted electronically, and in readily understandable language.

4.3.4 Certificate Dissemination

The CA shall ensure that Certificates are made available as necessary to Subscribers, Subjects and Relying Parties. In particular:

a) upon generation, the complete and accurate Certificate shall be available to the Subject for whom the Certificate is being issued;

b) Certificates are available for retrieval in only those cases for which the Subject's consent has been obtained;

c) the CA shall make available to Relying Parties the terms and conditions of the use of the Certificate;

d) the applicable terms and conditions of use shall be readily identifiable for a given Certificate;

e) the information identified in b) and c) above shall be available 24 hours per day, 7 days per week. Upon system failure, service disruption or other factors which are not under the control of the CA, the CA shall make best efforts to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the CPS; and

f) the information identified in b) and c) above shall be publicly available.

4.3.5 Certificate Revocation and Suspension

The CA shall ensure that Certificates are revoked and suspended in a timely manner based on authorized and validated Certificate Revocation or Suspension Requests.

4.3.5.1 Definition of Terms

The revocation of a Certificate is the recognizing of the Certificate as permanently invalid. The operation of a revoked Certificate cannot be renewed. The suspension of a Certificate is recognition of the Certificate as invalid for a time period. The termination of suspension of a Certificate shall also be provided.

The suspension and termination of suspension of a Certificate shall be performed by DPC CSC on the basis of court adjudication or an authorized request of the Subject, the Subscriber or DPC CSC. Any secure electronic signature issued from the moment of the revocation or suspension of the Certificate is not valid.

The secure electronic signature issued after the death of the Subject shall not be valid [3].

If DPC CSC without a legal basis, on wrongful purpose or due to negligence revokes or suspends a Certificate, DPC CSC shall compensate losses caused to a person that have arisen because of the unjustified revocation or suspension of the Certificate.

4.3.5.2 Revocation by DPC CSC

DPC CSC shall revoke without delay a Certificate in the following cases:

- the Subject or Subscriber requests the revocation of the Certificate;
- DPC CSC receives official information regarding the death of the Subject, or other information included in the Certificate changes;
- the Subject has provided DPC CSC with false or misleading information in order to receive a Certificate; or
- fulfilment of a court adjudication regarding the revocation of the Certificate.

4.3.5.3 Revocation Management

The CA shall document as part of its CPS the procedures for revocation of Certificates including:

- who may submit revocation reports and requests;
- how they may be submitted;
- any requirements for subsequent confirmation of revocation reports and requests. A confirmation may be required from the Subject if a compromise is reported by a third party;
- whether and for what reasons Certificates may be suspended;
- the mechanism used for distributing revocation status information; and
- the maximum delay between receipt of a revocation request or report and the change to revocation status information being available to all Relying Parties. This shall be at most one day.

Moreover, the revocation and suspension procedures shall fulfill the following requirements:

- requests and reports relating to revocation or suspension shall be processed on receipt;
- requests and reports relating to revocation or suspension shall be authenticated, checked to be from an authorised source;
- a Certificate's revocation or suspension status may be set to suspended whilst the revocation is being confirmed. The CA shall ensure that a Certificate is not kept suspended for longer than is necessary to confirm its status;
- the Subject, and where applicable the Subscriber, of a revoked or suspended Certificate, shall be informed of the change of status of its Certificate;
- once a Certificate is definitively revoked (i.e. not suspended) it shall not be reinstated;
- where Certificate Revocation Lists (CRLs) including any variants (e.g. Delta CRLs) are used, these shall be published at least daily and:
    - every CRL shall state a time for next CRL issue; and
    - a new CRL may be published before the stated time of the next CRL issue;
    - the CRL shall be signed by the Certification Authority or an entity designated by the CA;

- in order to maximize interoperability it is recommended that the CA issue Certificate Revocation Lists as defined in ISO/IEC 9594-8 [1].

- Revocation Services shall be available 24 hours per day, 7 days per week. Upon system failure, due to service interruption or other factors which are not under the control of the CA, the CA shall make best endeavours to ensure that this service is not unavailable for longer than a maximum period of time as denoted in the CPS of the Issuing CA.

4.3.5.4 Revocation Status

Information about revocation status of Certificates shall be managed and protected as follows:

- revocation status information shall be available 24 hours per day, 7 days per week. Upon system failure, due to service interruption or other factors which are not under the control of the CA, the CA shall make best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the CPS of the Issuing CA. Revocation status information may be provided, for example, using on-line Certificate status service or through distribution of CRLs through a repository;
- the integrity and authenticity of the status information shall be protected;
- revocation status information shall be publicly and internationally available;
- revocation status information (CRL) shall include information on the status of (revoked) Certificates at least until the Certificate expires.

4.4 CA Management and Operation

4.4.1 Trusted Roles

A Trusted Role is one whose task is to perform functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people who should fill Trusted Roles must be carefully selected. The functions performed in Trusted Roles form the basis of trust in the CA.

CA and RA's shall consider the categories of their personnel identified in this section as Trusted Persons having a Trusted Role. Trusted Persons shall include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, or key changeover requests, or registration information;
- the issuance or revocation of Certificates, including personnel having access to restricted portions of its repository; or
- the handling of Subject or Subscriber information or requests.

Trusted Persons may also include any other persons identified by DPC CSC. Trusted Persons include

system administration personnel, designated engineering personnel and security personnel:

- System Officer;
- Security Officer;
- System Administrators;
- System Operators; and
- System Auditors.

4.4.2 Security Management

The CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards. In particular:

- the CA shall carry out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. The risk analysis shall be regularly reviewed and revised if necessary;
- the CA shall retain responsibility for all aspects of the provision of certification services, even if some functions are outsourced to subcontractors. Responsibilities of third parties including on-site contractors shall be clearly defined by the CA. Appropriate arrangements shall be made to ensure that third parties are bound to implement any controls required by the CA. The CA shall retain responsibility for the disclosure of relevant practices of all parties;
- the CA management shall provide direction on information security through a suitable high level steering forum that is responsible for defining the CA's information security policy and ensuring publication and communication of the policy to all employees who are impacted by the policy;
- the CA shall have a system or systems for quality and information security management appropriate for the certification services it is providing;
- the information security infrastructure necessary to manage the security within the CA shall be maintained at all times. Any changes that will impact on the level of security provided shall be approved by the DPC CSC management;
- the security controls and operating procedures for CA facilities, systems and information assets providing the certification services shall be documented, implemented and maintained; and
- CA shall ensure that the security of information shall be maintained when the responsibility for CA functions has been outsourced to another organisation or entity.

4.4.3 Asset Classification and Management

The CA shall ensure that its assets and information receive an appropriate level of protection. In particular, the CA shall maintain an inventory of all information assets and shall assign a classification for the protection requirements to those assets consistent with the risk analysis.

4.4.4 Personnel Security

4.4.4.1 Background, Qualifications, Experience and Clearance Requirements

The personnel operating the CA must be technically and professionally competent.

Issuing CA and RA's will formulate and follow personnel and management policies sufficient to provide reasonable assurance of the trustworthiness and competence of their employees and of the satisfactory performance of their duties in a manner consistent with this CP.

4.4.4.2 Background Check Procedures

The CA shall conduct an appropriate investigation of all personnel who serve in Trusted Roles (prior to their employment and periodically thereafter as necessary) to verify their trustworthiness and competence in accordance with the requirements of this CP and the CA's personnel practices or equivalent. All personnel who fail an initial or periodic investigation will not serve or continue to serve in a Trusted Role.

4.4.4.3 Training Requirements

The CA must ensure that all personnel performing managerial duties with respect to the operation of the CA and RAs receive comprehensive training in:

- the CA and RA security principles and mechanisms;
- security awareness;
- all CSC software versions in use on the CA system;
- all duties they are expected to perform; and
- disaster recovery and business continuity procedures.

The requirements must be kept current to accommodate changes in the ICA system. Refresher training must be conducted as required, and the CA must review these requirements at least once a year.

4.4.4.4 Sanctions for Unauthorized Actions

The CA shall establish, maintain, and enforce employment policies for the discipline of personnel following unauthorized actions. Disciplinary actions may include measures up to and including termination and shall be commensurate with the frequency and severity of the unauthorized actions.

In the event of actual or suspected unauthorized action by a person performing duties with respect to the operation of the CA or RA, the CA should suspend his or her access to the CA system.

4.4.4.5 Contracting Personnel Requirements

The CA shall permit independent contractors or consultants to become Trusted Persons only under clearly-defined outsourcing relationships and only under the following conditions:

- CA using the independent contractors or consultants as Trusted Persons does not have suitable employees available to fill the roles of Trusted Persons, and
- the contractors or consultants are trusted by the CA to the same extent as if they were employees.

Otherwise, independent contractors and consultants shall have access to DPC CSC secure facility only to the extent they are escorted and directly supervised by Trusted Persons.

DPC CSC shall give their personnel (including Trusted Persons) the requisite training and other documentation needed to perform their job responsibilities competently and good.

4.4.5 Physical and Environmental Security

4.4.5.1 Physical Security Controls

Critical or sensitive information processing facilities are housed in secure areas, protected by defined security perimeters, with appropriate security barriers and entry controls. They are physically protected from unauthorized access, damage, and interference.

The CA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized. In particular:

- physical access to facilities concerned with Certificate generation, Subject device preparation, and revocation management services shall be limited to properly authorised individuals;
- controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities;
- controls shall be implemented to avoid compromise or theft of information and information processing facilities for Certificate generation, Subject device provision (in particular preparation) and revocation management;
- the facilities concerned with Certificate Generation and Revocation Management shall be operated in an environment which physically protects the services from compromise through unauthorised access to systems or data;
- physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the Certificate generation and revocation management services. Any parts of the premises shared with other organisations shall be outside this perimeter;

- physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. The CA's physical and environmental security policy for systems concerned with Certificate generation and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery, etc.; and
- controls shall be implemented to protect against equipment, information, media and software relating to the CA services being taken off-site without authorisation.

The CA system must be run on dedicated workstations or servers. The workstations or servers must be physically secured.

4.4.5.2 Site Locations and Construction

All CA and RA operations shall be conducted within a physically protected environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems.

The site for the CA's servers must satisfy the requirements for a high-security zone, including:

- be manually or electronically monitored for unauthorised intrusion at all times;
- ensure that access to the CA servers is limited to those personnel identified on an access list. Implement dual access control requirements to the CA servers for such personnel;
- ensure personnel not on the access list are properly escorted and supervised;
- ensure a site access log is maintained and inspected periodically; and
- ensure all removable media and paper containing sensitive plain text information is stored in secure, protective containers.

All RA sites must be located in areas that satisfy the controls required for a reception zone. If an RA workstation is used for online entity management with the issuing CA, the workstation must be located in either:

- a security zone; or
- an operations zone while attended, with all media security protected when unattended.

4.4.5.3 Physical Access

CA equipment shall always be protected from unauthorized access.

Authenticating RA equipment will be protected from unauthorized access while the crypto-module is

installed and activated. The RA will implement physical access controls to reduce the risk of equipment tampering even when the crypto-module is not installed and activated. These security mechanisms will be commensurate with the level of threat in the RA equipment environment.

RA equipment in facilities with controlled access occupied primarily by security personnel will not require an additional layer of controlled access surrounding inactivated RA equipment. RA equipment in less secure environments will require additional protection, such as being located in a room that is kept locked when the RA security or authorized personnel are not present.

Removable CA crypto-modules will be inactivated and placed in locked containers sufficient for housing equipment commensurate with the classification, sensitivity, or value level of the information being protected by the Certificates issued. Any activation data used to access or enable the crypto-module or issuing CA equipment will be stored separately. Such information should be memorized and not written down. If such information is written, it must be securely stored in a locked container.

A security check to the facility housing CA equipment will occur at least once every 24 hours. The check should ensure that:

- the equipment is in a state appropriate to the current mode of operation (e.g., that crypto-modules and removable hard disks are in place when “open”, and secured when “closed”);
- any security containers are properly secured;
- physical security systems (e.g., door locks, vent covers) are functioning properly; and
- the area is secured against unauthorised access.

4.4.5.4 Power and Air Conditioning

The facility which houses CA equipment shall be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power and create a reliable operating environment. Also, these secure facilities shall be equipped with primary and backup heating, ventilation and air conditioning systems to control temperature and relative humidity. In addition, personnel areas within the facility must be supplied with sufficient utilities to satisfy operational, health, and safety needs. The actual quantity and quality of utility service will depend on how the facility operates, e.g., its times of operation (24 hours/7 days or 8 hours/5 days), or whether online Certificate status checking is provided.

CA equipment will have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. The revocation mechanisms will be supported by uninterruptible power supplies and sufficient backup power generation.

4.4.5.5 Water Exposures

CA equipment shall be installed such that it is not in danger of exposure to water, e.g., on tables or elevated floors. Moisture detectors will be installed in areas susceptible to flooding. CA facilities with sprinklers for fire control will have a contingency plan for recovery should the sprinklers malfunction, or cause water damage outside of the fire area.

4.4.5.6 Fire Prevention and Protection

Facilities which house CA or RA equipment shall be constructed and equipped, and procedures shall be implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures shall meet all local applicable safety regulations.

An automatic fire extinguishing system shall be installed in accordance with local code. The CA will have a contingency plan, which accounts for damage by fire.

4.4.5.7 Media Storage

The CA shall protect the magnetic media holding back ups of critical system data or any other sensitive information from water, fire, or other environmental hazards, and shall use protective measures to deter, detect, and prevent the unauthorized use of, access to, or disclosure of such media.

Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains audit archive, or backup information will be stored in a location separate from the CA equipment.

4.4.5.8 Waste Disposal

The CA shall implement procedures for the disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing Confidential or High Risk Information.

Media used to collect or transmit Confidential or High Risk information will be destroyed, such that the information is unrecoverable, prior to disposal.

4.4.5.9 Off-site Backup

The CA shall maintain backups of critical system data or any other sensitive information, including audit data, in a secure off-site facility.

System backups, sufficient to recover from system failure, shall be made on a periodic schedule, as

described in the CPS's. At least one backup copy will be stored at an offsite location (separate from the CA equipment). Only the latest backup needs be retained. The backup will be stored at a site with physical and procedural controls commensurate to that of the operational CA system.

4.4.6 Operations Management

The CA shall ensure that the CA systems and components are secure and correctly operated, with minimal risk of failure.

4.4.6.1 CA Security Operations

This CP is focused on following requirements regarding the security of the operations of the CA:

- operational procedures and responsibilities;
- the integrity of CA systems and information shall be protected against viruses, malicious and unauthorised software;
- operational procedures shall be established and implemented for all Trusted and Administrative Roles that impact on the provision of certification services.
- housekeeping;
- network management;
- active monitoring of audit journals, event analysis and follow-up; and
- data and software exchange.

4.4.6.2 Media Handling and Security

All media shall be handled securely in accordance with requirements of the information classification scheme. Media containing sensitive data shall be securely disposed of when no longer required.

Media management procedures shall protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

4.4.6.3 System Planning

Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

4.4.6.4 Incident Reporting and Response

This CP is focused on the following requirements regarding the incident reporting and response:

- the CA shall act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents shall be reported as soon as possible after the incident;
- audit processes shall be invoked at system start-up, and cease only at system shutdown;
- the CA should collect and consolidate, either electronically or manually, security information generated outside the CA system. The CA should also record in audit log files, electronic or manual, all events relating to the security of the CA system. All logs should contain the date and time of the event, and the identity of the entity which caused the event. Events to be recorded are:
  - system start-up and shutdown;
  - CA application start-up and shutdown;
  - attempts to create, remove, set passwords or change the system privileges of the privileged users (Trusted Roles);
  - changes to CA details or keys;
  - changes to Certificate creation policies e.g., validity period;
  - login and logoff attempts;
  - unauthorized attempts at network access to the CA system;
  - unauthorized attempts to access system files;
  - generation of a CA's own keys and the keys of subordinate CAs;
  - failed read and write operations on the Certificate and repository; and
  - Certificate lifecycle management-related events (e.g., Certificate Applications, issuance, revocation, and key changeover);
- audit logs shall be monitored or reviewed regularly to identify evidence of malicious activity.

4.4.7 System Access Management

4.4.7.1 Access to CA

Access to CA should be compliant to the following requirements:

- controls (e.g. firewalls) shall be implemented to protect the CA's internal network domains from external network domains accessible by third parties;
- sensitive data shall be protected against unauthorised access or modification. Sensitive data shall be protected (e.g. using encryption and an integrity mechanism) when exchanged over networks which are not secure;
- the CA shall ensure effective administration of user (this includes operators, administrators and any users given direct access to the system) access to maintain system security, including user account management, auditing and timely modification or removal of access;
- the CA shall ensure access to information and application system functions are restricted in

accordance with the access control policy and that the CA system provides sufficient computer security controls for the separation of Trusted Roles identified in CA's practices, including the separation of security administrator and operation functions. Particularly, use of system utility programs shall be restricted and tightly controlled. Access shall be restricted only allowing access to resources as necessary for carrying out the role(s) allocated to a user;

- CA personnel shall be successfully identified and authenticated before using critical applications related to Certificate management;
- CA personnel shall be accountable for their activities, for example by retaining event logs;
- sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) being accessible to unauthorised users;
- the CA shall ensure that local network components (e.g. routers) are kept in a physically secure environment and their configurations periodically audited for compliance with the requirements specified by the CA; and
- continuous monitoring and alarm facilities shall be provided to enable the CA to detect, register and react in a timely manner upon any unauthorised or irregular attempts to access its resources.

4.4.7.2 Dissemination

Access to this CP, the CPSs, Certificates, Certificate status information or CRLs should not be intentionally limited by use of technical means. The CA shall, however, require persons to agree to a Relying Party Agreement as a condition to accessing Certificates, Certificate status information, or CRLs. The CA shall implement controls to prevent unauthorized persons from adding, deleting, or modifying repository entries.

4.4.7.3 Revocation Status

Revocation status application shall enforce access control on attempts to modify revocation status information.

4.4.8 Trustworthy Systems Deployment and Maintenance

The CA shall use trustworthy systems and products that are protected against modification. Requirements for the trustworthy systems may be ensured using, for example, systems conforming to a suitable protection profile (or profiles), defined in accordance with ISO/IEC 15408 [11]. In particular:

- an analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the CA or on behalf of the CA to ensure that security is built into the IT systems; and
- change control procedures exist for releases, modifications and emergency software fixes for any operational software.

4.4.9 Business Continuity Management and Incident Handling

The CA shall ensure that in the event of a disaster, including compromise of the CA's private signing key, operations are restored as soon as possible.

4.4.9.1 Secure Facility after a Natural or Other Type of Disaster

The CA must define and maintain a continuity plan to enact in case of a disaster outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. Disaster recovery plans shall address the restoration of information systems services and key business functions. Disaster recovery sites shall have the physical security protections.

The CA shall have the capability of restoring or recovering operations within twenty-four (24) hours following a disaster with, at a minimum, support for the following functions:

- Certificate issuance;
- Certificate revocation;
- Certificate suspension; and
- Publication of revocation and suspension information.

4.4.9.2 CA Systems Data Backup and Recovery

CA systems data necessary to resume CA operations shall be backed up and stored in safe places suitable to allow the CA to timely go back to operations in case of incident or disasters.

Backup copies of essential business information and software should be taken regularly. Adequate backup facilities should be provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Backup arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans.

Back-up and restore functions shall be performed by the relevant Trusted Roles.

4.4.9.3 CA Key Compromise

The CA's business continuity plan (or disaster recovery plan) shall address the compromise or suspected compromise of a CA's private signing key as a disaster. In the case of compromise the CA shall as a minimum provide the following undertakings:

- inform the following of the compromise: all Subscribers, Subjects and other entities, among which are Relying Parties and CAs, with which the CA has agreements or other form of established relations. In

addition, this information shall be made available to other Relying Parties; and

- indicate that Certificates and revocation status information issued using this CA key may no longer be valid.

4.4.9.4 Algorithm Compromise

Should any of the algorithms or associated parameters used by the CA or its Subscribers or Subjects become insufficient for its remaining intended usage then the CA shall:

- inform all Subscribers, Subjects and Relying Parties with which the CA has agreement or other form of established relations. In addition, this information shall be made available to other Relying Parties; and
- revoke any affected Certificate.

4.4.9.5 Revocation of CA Certificate

In the case where a Root, Policy or Issuing CA Certificate is revoked, the Revocation Procedure shall take the following steps:

- Requesting CA submits a revocation request;
- Revocation Officer ensures that revocation request is properly formed;
- Revocation Officer ensures that requesting CA is properly identified, authenticated and authorised;
- Revocation Officer authenticates himself (using Certificate); and
- Revocation Officer processes revocation.

DPC CSC shall inform the Requesting CA by letter or e-mail upon successful completion of the Revocation.

4.4.9.6 CA Key Changeover

A Root, Policy or Issuing CA of DPC CSC shall stop issue new CA or subject Certificates no later than 30 days before the point in time (“Stop Issuance Date”). Upon successful validation of CA Certificate requests received after the “Stop Issuance Date,” Certificates will be signed with a new CA key pair.

An DPC CSC´s Root or parent CA shall continue to issue CRL's signed with the original Private Key until the expiration date of the last Certificate issued using the original key pair has been reached.

Upon expiration of the actual Certificate, it will be removed from the repository. The new Certificate of the new Public Key is published at the web site; the original Certificate is put into the actual CRL.

4.4.10 CA Termination

The CA shall ensure that potential disruptions to Subscribers, Subjects and Relying Parties are minimized as a result of the termination of the CA's services as covered by this CP. CA shall ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings.

Before the CA terminates its services the following procedures shall be executed as a minimum:

- the CA shall inform the following of the termination: all Subscribers, Subjects and other entities with which the CA has agreements or other form of established relations, among which Relying Parties and CAs. In addition, this information shall be made available to other Relying Parties;
- the CA shall terminate all authorisation of subcontractors to act on behalf of the CA in the performance of any functions related to the process of issuing Certificates;
- the CA shall perform necessary undertakings to transfer obligations for maintaining registration information, and event log archives, including revocation status information for their respective period of time as indicated to the Subscriber, Subject and Relying Party; and
- the CA shall destroy, or withdraw from use, its Private Keys.

The CA shall have an arrangement to cover the costs to fulfill these minimum requirements in case the CA becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

The CA shall state in its practices the provisions made for termination of service. This shall include:

- the notification of affected entities;
- the transfer of its obligations to other parties;
- the handling of the revocation status for not expired Certificates that have been issued.

4.4.11 Compliance with Legal Requirements

The CA shall ensure compliance with legal requirements. In particular:

- CA shall ensure it meets all applicable statutory requirements (including requirements of “Law on Personal Data” [13]) for protecting records from loss, destruction and falsification. Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities;
- the CA shall ensure that the requirements of Personal Data Protection Law **Error! Reference source ot found.**are met. Data protection issues specific to this CP are addressed in:
    - registration (including use of pseudonyms);
    - confidentiality of records;
    - protecting access to personal information; and
    - user consent;

- appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

The information that users contribute to the CA shall be completely protected from disclosure without the user's agreement, a court order or other legal authorization.

4.4.12 Recording of Information Concerning Certificates

The CA shall ensure that all relevant information concerning a Certificate is recorded for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings.

4.4.12.1 Records Concerning Certificates

Records concerning Certificates include registration information and information concerning significant CA environmental, key management and Certificate management events. The following requirements should be fulfilled:

- the confidentiality and integrity of current and archived records concerning Certificates shall be maintained;
- records concerning Certificates shall be completely and confidentially archived in accordance with disclosed business practices;
- records concerning Certificates shall be made available if required for the purposes of providing evidence of certification for the purpose of legal proceedings. The Subject, and within the constraints of data protection requirements the Subscriber, shall have access to registration and other information relating to the Subject;
- the precise time of significant CA environmental, key management and Certificate management events shall be recorded. It is recommended that the CA states in its practices the accuracy of the clock used in timing of events, and how this accuracy is ensured;
- records concerning Certificates shall be held for a period of time as appropriate for providing necessary legal evidence in support of electronic signatures in accordance with applicable legislation;
- the events shall be logged in a way that they cannot be easily deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held. This may be achieved, for example, through the use of write-only media, a record of each removable media used and the use of off-site backup; and
- the specific events and data to be logged shall be documented by the CA.

4.4.12.2 Registration Data to be Recorded

The CA shall verify that registration data is exchanged with recognized registration service providers,

whose identity is authenticated, in the event that external registration service providers are used. It is also required that:

- the CA shall ensure all events relating to registration are logged;
- the CA shall ensure that all registration information including the following is recorded:
  - type of document(s) presented by the Applicant to support registration;
  - record of unique identification data, numbers, or a combination of identification documents;
  - storage location of copies of applications and identification documents, Subscriber agreements;
  - any specific choices in the Subscriber agreement (e.g. consent to publication of Certificate);
  - identity of entity accepting the application;
  - method used to validate identification documents; and
  - name of receiving CA and submitting Registration Authority;
- the CA shall ensure that privacy of Subject information is maintained.

4.4.12.3 Recording of Certificate Related Events

Upon generation of Certificates,

- the CA shall log all events relating to the lifecycle of CA keys;
- the CA shall log all events relating to the lifecycle of Certificates; and
- the CA shall log all events relating to the lifecycle of keys managed by the CA, including any Subject keys generated by the CA.

4.4.12.4 Revocation Management

The CA shall ensure that all requests and reports relating to revocation, as well as the resulting action, are logged.

4.5 Organizational

The CA shall ensure that its organization is reliable. In particular that:

- controls and procedures under which the CA operates shall be non-discriminatory;
- the CA shall make its services accessible to all Applicants whose activities fall within its declared field of operation;
- the CA is a legal entity according to national law;
- a risk assessment is carried out to evaluate business requirements and determine the security requirements for all the areas of this CP. Risk analysis shall also consider mitigation of risk by

contracting insurance or making provisions;

- the CA has adequate arrangements to cover liabilities arising from its operations or activities;
- the CA has the financial stability and resources required to operate in conformity with this policy;
- the CA has policies and procedures for the resolution of complaints and disputes received from customers or other parties about the provisioning of electronic trust services or any other related matters;
- the CA has a properly documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements;
- the parts of the CA concerned with Certificate generation and revocation management shall be independent of other organisations for its decisions relating to the establishing, provisioning and maintaining and suspending of services. In particular its senior executive, senior staff and staff in Trusted Roles must be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides; and
- the parts of the CA concerned with Certificate generation and revocation management shall have a documented structure which safeguards impartiality of operations.

5 Archiving

5.1 Types of Events Recorded

Records shall be maintained and made available to DPC CSC upon request that include:

- documentation of the recording entity's own compliance with the applicable CPS and other obligations under their agreements with their Superior Entities; and
- documentation of actions and information that are material to each Certificate Application and to the creation, issuance, use, revocation and expiration of each Certificate it issues. These records shall include all relevant evidence in the recording entity's possession regarding:
  - the identity of the Subject named in each Certificate;
  - the identity of persons requesting Certificate revocation;
  - Time Stamps; and
  - facts related to issuing Certificates including information relevant to successful completion of a Compliance Audit under chapter 8.

Records may be kept in the form of either computer-based messages or paper-based documents, provided their indexing, storage, preservation, and reproduction are accurate and complete.

5.2 Retention Period for Archive

Records associated with a Certificate compiled under section 5.1 shall be retained for at least ten (10) years following the date the Certificate expires or is revoked.

5.3 Protection of Archive

An entity maintaining an archive of records compiled under section 5.1 shall protect the archive so that only the entity's authorized Trusted Persons are able to obtain access to the archive. The archive shall be protected against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy System. The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in section 5.2.

5.4 Archive Backup Procedures

Entities compiling electronic information under section 5.1 shall incrementally backup system archives of such information on a daily basis and perform full backups on a weekly basis.

Copies of paper-based records under section 5.1 shall be maintained in an off-site disaster recovery facility in accordance with chapter 6.

5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

5.6 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

6 Compromise and Disaster Recovery

6.1 Incident and Compromise Handling Procedures

The high availability of Certification Services provided by DPC CSC is guaranteed with the implementation of the standby installation of the DPC CSC IS.

In future to counteract interruptions to business activities, DPC CSC IS will be supported by standby components, which will be located in a separate Standby Site, the Secondary Data Centre (SDC). In the event of a malfunction, the standby system can directly take over the function of the live system, following appropriate user interaction.

The DPC CSC internal Business Continuity Plan describes procedures and responsibilities for handling these types of incidents. Objective of the Business Continuity Plan is the immediate recovery of availability and continuous securing of certification services.

6.2 Recovery after Corruption of Computing Resources

After an assumed or actual compromising of resources, software or data disaster recovery procedures will be enacted.

6.3 Private Key Compromise Procedures

If DPC CSC ICA´s Private Key is compromised or suspected to be compromised, DPC CSC ICA shall at least:

- inform Subscribers, Subjects, cross-certifying CA's and Relying Parties;
- terminate the Certificate and CRL distribution service for Certificates and CRLs issued using the compromised Private Key; and
- request the revocation of the CA’s Certificate.

7 Management and Conformance of CP

7.1 Management of CP

The CA shall ensure that the CP is effective. In particular:

- there shall be a body (e.g. ICS Head of Certification Services) with final authority and responsibility for specifying and approving this CP;
- a risk assessment shall be carried out to evaluate business requirements and determine the security requirements to be included in this CP for all the areas identified above;
- this CP shall be approved and modified in accordance with a defined review process, including responsibilities for maintaining this CP;
- a defined review process shall exist to ensure that the Policies are supported and described in the CPSs;
- the CA shall make available the Policies supported by the CA to all appropriate Subjects, Subscribers and Relying Parties;
- revisions to Certificate Policies supported by the CA shall be made available to Subjects, Subscribers and Relying Parties;
- this CP shall incorporate, or further constrain, all the requirements identified in sections **Error! eference source not found.** and 3 with the exclusions indicated below. In the case of any conflict the requirements of the present document prevail; and
- a unique object identifier shall be obtained for this CP of the form required in ITU-T Recommendation X.509 [1].

7.2 Conformance to CP

The CA shall only claim conformance to this CP:

- if the CA claims conformance to this CP and makes available to Subjects, Subscribers and Relying Parties on request the evidence to support the claim of conformance; or
- if the CA has a current assessment of conformance to this CP by a competent independent party. The results of the assessment shall be made available to Subjects, Subscribers and Relying Parties on request;
- if the CA is later shown to be non-conformant in a way that significantly affects the ability of the CA to meet the requirements for Certificates identified in section 16 of DSEDL [3] it shall cease issuing Certificates using this CP, until it has demonstrated or been assessed as conformant, otherwise the CA shall take steps to remedy the non-conformance within a reasonable period; and
- the CA compliance shall be checked on a regular basis and whenever major change is made to the CA operations.

8 Compliance Audit and Other Assessment

The conformance to this CP shall be checked for significant changes annually with a full re-assessment first after three years and then after every four years.

The auditor may be internal to the DPC CSC organization but should have no hierarchical relationship with the department operating the CA being audited.

The scope of the annual audit includes environmental controls, key management operations and Infrastructure and Administrative controls, Certificate life cycle management and business practices disclosure of the CA being audited, as documented in section 4.4.

Following any Compliance Audit, the audited CA shall provide DPC CSC with the annual report and attestations based on its audit within fourteen (14) days after the completion of the audit.

Significant exceptions or deficiencies identified during the compliance audit will result in a determination of actions to be taken. This determination is made by DPC CSC management with input from the auditor. DPC CSC management is responsible for developing and implementing a corrective action plan.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Management Fees

Fees may be payable for the Certificate application process and for the issuance, revocation or re-key of Certificates. Where fees are payable, DPC CSC will provide up-to-date fee schedules to the Certification Authorities, based on the particular business arrangements reached with them in the Subscriber Agreement.

9.1.2 Certificate Validation Fees

DPC CSC´s Certificate Validation Services for validating qualified e-signature certificates are costs. The appropriate CPS shall contain or refer to a pricelist.

9.1.3 Refund Policy

DPC CSC shall establish a refund policy. Where a refund policy applies to Subscribers, an up-to-date version shall be provided to them and may be published on a nominated Web site.

9.2 Financial Responsibility

DPC CSC's liability limits towards Subscribers are regulated through Subscriber´s Agreements. This CP is incorporated into such contracts.

Unless otherwise explicitly agreed or explicitly provided for in this CP, DPC CSC´s liability to Subscribers and Relying Parties is limited against claims of any kind, including those of contractual nature, on a per Certificate basis regardless of the number of transactions, digital signatures, or causes of action arising out of or related to such Certificate or any services provided in respect of such Certificate and on a cumulative basis.

Any and all claims within the DPC CSC services arising with regard to a Certificate (regardless of the entity causing the damages or the entity that issued a Certificate or provided certification services) shall be subject to the liability limitations applicable to it as per this CP.

Subject to the foregoing limitations, DPC CSC´s liability limit towards all Subscribers and Relying Parties for the whole of the validity period of a Certificate issued by DPC CSC CA's towards all persons with regard to such Certificate is limited.

In no event shall DPC CSC's liability exceed the defined limits.

9.3 Confidentiality of Business Information

9.3.1 Types of Information to be Kept Confidential

9.3.1.1 Collection and Use of Personal Information

All personal information collected or used by the DPC CSC is done in compliance with laws and regulations of the Republic of Azerbaijan and based on the procedures provided in this CP. Personal information collected and used by DPC CSC CA shall also be required to comply with the applicable data protection legislation.

In the cases where a DPC CSC CA ceases to provide certification services, as part of the termination procedure it is required to transfer the personal and other data corresponding to its provision of certification services to another local Certification Authority or other entity designated by DPC CSC or the competent authorities. In all cases, the storage and availability of such data for the purpose of maintaining the provision of certification services to the corresponding End Users shall be sought.

9.3.1.2 Registration Information

Registration information shall be treated as confidential information unless consent is explicitly given otherwise by the entity to which the information refers.

9.3.1.3 Certificate and Certificate Status Information

Certificate and Certificate Status Information shall be disclosed for any purposes that may be relevant for the use of such information and Certificate status in accordance with the consent given by the Subscriber (Subject) through the Subscriber Agreement. Unless explicitly otherwise stated in this CP, upon acceptance of Certificates, the Subscriber (Subject) shall authorize DPC CSC to publish the information as contained in the Certificate issued as well as other information required for the provision of the Certification Services.

9.3.1.4 Operational and Configuration Documentation

DPC CSC maintains a number of sensitive internal documents that detail the operation and configuration of the DPC CSC´s Certification Services. These documents are treated as Confidential and are not released outside of DPC CSC, with the exceptions required for consulting and auditing purposes.

9.3.1.5 Audit Information

All audit information received by DPC CSC concerning DPC CSC CA and its Certificate Validation Services shall be treated as Confidential Information, with the exception of limited summaries of such audits which may be published by DPC CSC, in its sole and absolute discretion or as required by applicable law.

9.3.2 Types of Information Not Considered Confidential

9.3.2.1 Certificate and Certificate Status information

All Certificates issued under this CP for public use shall be publicly available, if Subjects or Subscribers agree on their publishing. In all cases, the Certificate status information of all Certificates issued within the DPC CSC services shall be made available to anybody who accesses the Certificate Validation Services in accordance with this CP and any relevant agreements (e.g. Relying Party Agreement).

9.3.2.2 Documentation

The following DPC CSC documents are publicly available and are not considered to be confidential information:

- this CP;
- approved public Certification Practice Statements;
- other approved Certificate Policies; and
- other documents approved for publication by DPC CSC.

9.3.3 Disclosure of Certificate Revocation Information

The reason for the revocation of the Certificate of DPC CSC CA shall be made public in accordance with applicable law or in the sole and absolute discretion of DPC CSC or the Subordinate CA that issued the Certificate which was revoked.

Information about Certificate revocation or validity is disclosed using the OCSP protocol. DPC CSC´s Certificate Validation Services disclose whether a requested Certificate is valid, revoked or suspended, or whether the Certificate Validation Services are unaware of the Certificate's status. No further information is disclosed.

9.3.4 Release to Law Enforcement Officials

No document or record retained by DPC CSC is released to law enforcement agencies or officials

except where:

- a properly constituted warrant or request is produced;
- the law enforcement official is properly identified; and
- other applicable legal procedures are complied with.

The documents retained by Subordinate CAs shall be treated similarly, but in accordance with the corresponding CPS and applicable law.

9.3.5 Release as Part of Civil Evidence or Discovery Purposes

In general, no confidential document or record stored by DPC CSC is released to any person except where:

- a properly constituted request (i.e. that has complied with all legal procedures) for the production of the information is produced; and
- the person requiring production is a person authorised to do so and is properly identified.

DPC CSC will be required to release information for civil evidence or discovery purposes from any part of the DPC CSC Services in any jurisdiction where the appropriate legal procedures have been followed. An internal efficient procedure may be established across the DPC CSC Services for these purposes, subject to compliance with applicable law and approval by the relevant authorities.

9.4 Privacy of Personal Information

Any information about Subscribers and Subjects that is not publicly available through the content of the issued Certificate, Certificate directory or online CRL's is treated as confidential. All personal information collected or used by the DPC CSC is protected in accordance with the “Law on Personal Data” [13] and chapter 15 of the "Electronic Signature and Electronic Documents" Law [3].

Confidential information is disclosed to a third party only if mandated by legal requirements.

All information made public in a Certificate is deemed not confidential.

9.5 Intellectual Property Rights

All intellectual property rights including copyright in all Certificates, CRLs, OCSP Certificate Status Messages, and Certificate Directories and, unless otherwise explicitly provided for, all practices, policy, operational and security documents concerning the DPC CSC Certification Services as well as agreements belong to and will remain the property of DPC CSC.

9.6 Representations and Warranties

No Stipulations.

9.7 Liability Limits and Disclaimers

DPC CSC shall provide the DPC CSC Certification Services in accordance with this CP. All other warranties (implied by law or otherwise) are excluded, including any warranties:

- with regard to the accuracy or reliability of information contained in Certificates that is not provided by or verified by DPC CSC CAs;
- that deviate from this CP; and
- with regard to matters outside DPC CSC's reasonable control.

DPC CSC is not liable for any type of damages (including special, consequential, incidental, indirect or punitive damages), regardless of whether it has been notified of them (or their potential) or not, or whether they are reasonably foreseeable or not, arising from:

- underlying transactions between Subscribers, Subjects and Relying Parties;
- use of or reliance on the Certificates, cryptographic keys, digital signatures or the certification services in ways not compliant or for purposes not allowed by this CP;
- third party products or services (including hardware and software);
- non re-keying of a Certificate as a result of non-compliance with the Certificate re-keying requirements as indicated in this CP; or
- any indirect or consequential loss or damage, loss of profits, loss of goodwill, loss of anticipated savings, loss of revenue, loss of business, business interruption; or loss of information.

In no case shall DPC CSC be liable for any type of damages for a sum beyond the reliance limits referred to in section 2.7 of this CP and those provided in the Certification Practice Statement under which a Certificate is issued.

9.8 Indemnities

9.8.1 Indemnification by Subscribers

To the extent permitted by applicable law, Subscribers are required to indemnify DPC CSC for:

- falsehood or misrepresentation of fact on the Certificate Application;
- failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party;
- the Subscriber´s 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; or

- the Subscriber´s use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

The applicable Subscriber Agreement may include additional indemnity obligations.

9.8.2 Indemnification by Relying Parties

To the extent permitted by applicable law, Relying Party Agreements shall require Relying Parties to indemnify DPC CSC for:

- the Relying Party's failure to perform the obligations of a Relying Party;
- the Relying Party's reliance on a Certificate that is not reasonable under the circumstances; or
- the Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

The applicable Relying Party Agreement may include additional indemnity obligations.

9.9 Term and Termination

9.9.1 Term

The CP becomes effective upon publication in the DPC CSC repository. Amendments to this CP become effective upon publication in the DPC CSC repository.

9.9.2 Termination

This CP as amended from time to time shall remain in force until it is replaced by a new version.

9.10 Individual Notices and Communications with Participants

No Stipulations.

9.11 Amendments

9.11.1 Procedure for Amendment of CP

For maintenance and approval of the CP an internal process with an appropriate role on management level is defined. Thus it is made possible that the CPS always shows the current practices of the

certification services of the DPC CSC.

9.11.2 Notification Mechanism and Period

An actualization of the CP is given on the DPC CSC Website.

9.11.3 Changes in OID

In the case of an actualization of this CPS, it will be assigned a new OID only if significant differences to the last version exist. The decision for the assignment of a new OID is part of the process for the actualization of the CP.

9.12 Dispute Resolution Procedures

9.12.1 Hierarchy of the Certification Practice Statement

In the event of a conflict between this CP and other policies, plans, agreements, contracts or procedures, where the conflict is between this CPS and:

- a Subscriber Agreement or Relying Party Agreement, this CP shall prevail;
- any policy, plan, procedures or any other operational or practices documentation whatsoever, this CP shall prevail.

9.12.2 Process

Should a dispute arise out of or in connection with these practices or related contracts, prior to resorting to legal proceedings, the parties to the dispute shall attempt to settle such dispute or differences by negotiations between them in good faith.

If the parties are not able to resolve the dispute through negotiation within one (1) month from the date the dispute first arose, then the parties agree to enter into binding court in accordance with the “Law on Courts and Judges” [14].

Regardless of the measures taken by the parties to resolve the dispute in accordance with this CP, DPC CSC shall retain its right to seek injunctive relief in the event of alleged or effective material breach of this CP or any other circumstance related to the dispute which may affect partially or wholly the security of the DPC CSC Services.

9.13 Governing Law

This CP is be governed and construed in accordance with the laws of the Republic of Azerbaijan.

9.14 Miscellaneous Provisions

No Stipulations.

9.15 Other Provisions

No Stipulations.

10 List of Abbreviations

CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSC	Certification Services Center
DSEDL	Electronic Signature and Electronic Document Law
I&A	Identification and Authentication
ICA	Issuing Certification Authority
IE	International Electro-technical Commission
IETF	Internet Engineering Task Force
ISO	International Organisation for Standardisation
ITU	International Telecommunications Union
LDAP	Light-Weight Directory Access Protocol
DPC	Data Processing Center of the Ministry of Communications and High Technologies
DPC CSC CA	DPC Certification Services Center Certification Authority
DPC PKI	DPC Public Key Infrastructure
AZ	Republic of Azerbaijan
O	Organization
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PCA	Policy Certification Authority or Policy CA

PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
PMA	Policy Management Authority
QC	Qualified Certificate
RA	Registration Authority
RCA	Root Certification Authority or Root CA
RFC	Request for Comments
RSA	A specific public key algorithm
SSCD	Secure Signature Creation Device
TP	Time Stamp Policy
TPS	Time Stamping Practice Statement
TSA	Time Stamping Authority
TST	Time Stamp Token
URL	Uniform Resource Locator

11 References

[1] ITU-T Recommendation X.509 (2000)/ISO/IEC 9594-8 (2017): "Information technology – Open Systems Interconnection - The Directory: Public-key and attribute Certificate frameworks"

[2] Root Certification Authority - Certification Practice Statement of Root Certification Authority (ICS CPS RCA).

Root Certification Authority - Certification Practice Statement of Policy Certification Authority (ICS CPS PCA)

Governing Bodies Certification Authority - Certification Practice Statement of Issuing Certification Authority (ICS CPS GOV ICA)

e-Government Certification Authority - Certification Practice Statement of Issuing Certification Authority (ICS CPS EGOV ICA)

[3] "Electronic Signature and Electronic Document" Law of the Republic of Azerbaijan, 9 March 2004

[4] ETSI TS 101 456 V1.4.3 “Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing Qualified Certificates”, May, 2007

[5] RFC 3647 “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” November 2003

[6] Directive 1999/93/EC “Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures”

[7] RFC 2119 “Key words for use in RFCs to Indicate Requirement Levels” March 1997

[8] RFC 5280 “Internet X.509 Public Key Infrastructure: Certificate and CRL Profile”, May 2008

[ftp://ftp.man.szczecin.pl/pub/rfc/pdfrfc/rfc5280.txt.pdf]

[9] RFC 6960 “Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol – OCSP” June 2013 [https://tools.ietf.org/html/rfc6960]

[10] FIPS 140-2 “Security Requirements for Cryptographic Modules”, Issued May 25, 2001

[11] ISO/IEC 15408 (2009) (parts 1 to 3): "Information technology - Security techniques – Evaluation criteria for IT security"

[12] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[13] "The Law on Personal Data", 998-IIIQ, 11 May 2011

[14] "The Law on courts and judges", 310-IQ, 10 June 1997