Certification Practice Statement of Root Certificate Authority

Root Certification Centre of Republic of Azerbaijan

DPC of the Ministry of Communications and High Technologies

December 8, 2016

Version 2

Prepared by

Habib Abbasov

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change reference
December 4th, 2016	Habib Abbasov	2	Draft for review by head of CSC

Reviewers

Name	Version approved	Position	Date
Mailov Arif	2	Head of CSC	December 8th, 2016

Table of Contents

1 Introduction

This CPS covers the practices followed by the DPC CSC Root CA for the procedures related to Certificate application, issuance, use, validation, revocation and their expiry, as well as the operational maintenance of the DPC CSC Root CA.

The practices described in this CPS, together with the technologies, policies and procedures referred to in the documents contained illustrate the efforts made to convey trustworthiness by providing high levels of security of the DPC CSC Root CA.

DPC CSC CA management, organisation, processes and procedures was assessed by an independent auditor against ISO 27001:2013.

This CPS undergoes a regular review process, by which the reviewers involved strive to take into consideration developments in technology and information security, as well as other relevant circumstances. The structure of this CPS is broadly based on the RFC 3647.

1.1 User Community and Applicability of this CPS

This CPS states the practices related to DPC CSC's Root Certification Authority and covers practices for key- and Certificate lifecycle management of:

- DPC CSC RCA's key pair and self signed Certificate for Certificate and CRL signing;
- DPC CSC PCA's Certificate.

Furthermore, CPS states requirements for third parties who want to join the DPC CSC PKI.

User community of this CPS is all parties who rely on Certificates issued by DPC CSC RCA.

1.2 Document Name and Identification

The name or this CPS is DPC CSC Root CA CPS. The primary source of the current version of the CPS and other important DPC CSC documents is http://www.e-imza.az

The CPS has been approved by Head of DPC Certification Services Center on 8 December 2016.

Title: Certification Practice Statement of Root Certification Authority of Root Certification Center

Version: Version 2.0

Date: 8 December 2016

OID: 1.3.6.1.4.1. 32843.1.1

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

As a member of DPC CSC, the DPC CSC Root CA is operating in compliance with the Certificate Policy of DPC CSP [2] .

DPC CSC´s Certificate Policy is published at the URL http://www.e-imza.az

1.3 Identification of CP

This CPS states the practices that DPC CSC RCA employs in providing certification services that include issuing, managing, suspending and revoking Certificates in accordance with the specific requirements of the Certificate Policy of Data Processing Center Certification Services Center (DPC CSC CP) with the OID 1.3.6.1.4.1. 32843.1.1.

1.4 PKI Participants

1.4.1 Certificate Authority Hierarchy

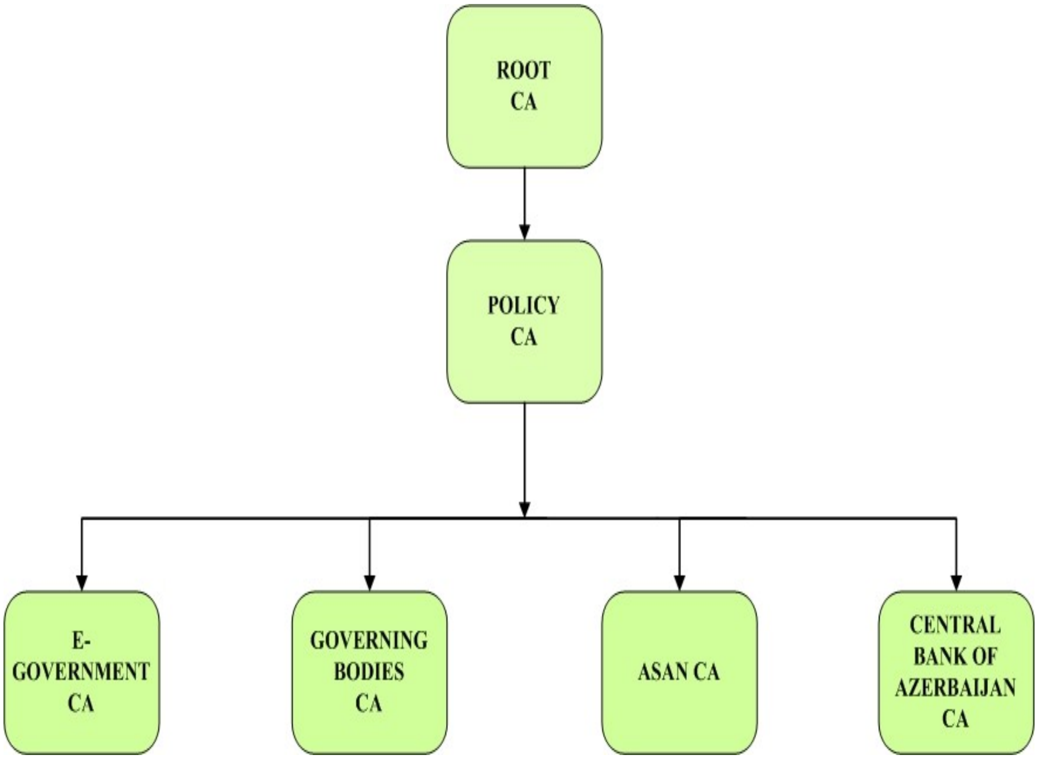
DPC CSC´s overall architecture is based on a three-tier CA structure. This architecture will allow the root CA, which serves as the basis of all subsequent CA's and Certificates, to be stored off-line. The offline nature of the root is the most secure method to protect this critical component of the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

The Root CA issues Certificates and Certificates Revocation Lists for the Policy CA.

The Policy CA issues Certificates and Certificate Revocation Lists for the Issuing CA's and the TSA.

The Issuing CA's defines Certificate templates for end users certificate types, issue End-User Certificates, Infrastructure Certificates and Certificate Revocation Lists.

The diagram on the following page shows the hierarchical architecture of DPC CSC´s Certification Services.



2 Publication and Repository Responsibilities

2.1 Directory and Certificate Validation Service

2.1.1 Directory Services

Directory Service is a service of the DPC CSC which provides online access via LDAP and HTTP to

- certificates issued by DPC CSC Root CA;
- CRL of DPC CSC Root CA;
- issued Certificates of DPC CSC's trusted CAs; and
- CRL's of DPC CSC's trusted CA's.

Access to Certificates published by DPC CSC is not restricted and available 24 hours 7 days a week.

2.1.1.1 Retention Period of Certificates

Certificates issued by DPC CSC RCA will be retained by DPC CSC Directory Services for 30 years after Certificate expiration.

2.1.1.2 Retention Period of CRL

CRL's of DPC CSC CAs will be retained by DPC CSC Directory Services for 30 years after CRL expiration. Thereby it will be possible to determine the validity of a Certificate at a specific point in time.

2.1.2 Certificate Validation Services

DPC CSC's Certificate Validation Service by means of OCSP Responder provides Certificate status checking for Certificates issued by GOV CSP CA's and EGOV CSP CA's. For Root Certification Center CA's, DPC CSC RCA and DPC CSC PCA) CRL mechanism is used to validate certificate status.

2.1.2.1 Initial Verification of DPC CSC Root CA Certificate

As DPC CSC Root CAs Certificate is self signed it is the trust anchor for all issued Certificates of DPC CSC. Therefore the thumbprint of the DPC CSC Root CA Certificate must be examined before beginning of the procedure. Thumbprint of DPC CSC Root CA Certificates shall be shown on DPC CSC's website. The thumbprint may also be on printed letters of DPC CSC.

2.1.2.2 Types of provided Validation Services

CRL method should be used to validate Certificate status.

The maximum delay between receipt of a suspension or revocation request or report and the change to Certificate status information being available to all relying parties shall be at most 2 days (48 hours).

2.2 Publication of Information

DPC CSC maintains a Website for providing Applicants, Subjects, Subscribers and Relying Parties with information about application and handling of Certificates and DPC CSC services.

DPC CSC Website is available online at the URL **http://www.e-imza.az**

Access to DPC CSC public Website is not restricted and available 24 hours 7 days a week.

DPC CSC will at all times publish a current version of the following documents:

- Certificate Policy of DPC CSC Root Certification Center;

- Certificate Policy of DPC CSC Governing Bodies Certification Center;
- Certificate Policy of DPC CSC e-Government Certification Center;
- Certification Practice Statement of DPC CSC Root CA, Policy CA, Governing Bodies Center and e-Government Certification Center;
- Time Stamp Policy for Government Body Certification Center and e-Government Certification Center;
- Time Stamping Practice Statement for Government Body Certification Center and e-Government Certification Center.

Furthermore, the following information could be retrieved at DPC CSC's Website:

- information regarding Certificate usage and handling of smart cards;
- Subscriber Agreement templates;
- Subscriber application form;
- information about DPC CSC – name, registration number, address, contact information;
- a list of all registration authorities;
- a list of accredited Certification Centres;
- Root CA Certificate and its hash value (fingerprint, SHA1); and
- Certificates of DPC CSC's CAs and trusted services (TSA and OCSP responders).

2.3 Time or Frequency of Publication

The following guidelines for frequency and time of publication apply.

Issued Certificates	Publication immediately upon generation and acceptance by trusted CA
CRL of Root CA	Every 3 months with an overlapping period of one week and upon revocation of an issued Certificate
Policies, Guidelines	Policies and Guidelines will be published upon approval

2.4 Access Controls on Directory

Information published by DPC CSC Directory Services is publicly accessible information, continuously available. DPC CSC has implemented logical and physical security measures to prevent unauthorized persons from adding, deleting, or modifying repository entries.

Integrity of Certificates is ensured by limiting rights for changes in database and a restricted system access. Additionally DPC CSC Directory Services have an internal integrity mechanism. DPC CSC frequently performs an integrity check on the data file which can detect any kind of low-level database corruption.

3 Identification and Authentication (I&A)

3.1 Naming

3.1.1 Type of Names

All Certificates issued by DPC CSC RCA contain X.509 Distinguished Names in the **Issuer** field. The following attributes will be applied:

countryName (C)	**AZ**
organizationName (O)	CSP
organizationalUnitName (OU)	Certification Services
commonName (CN)	AZ Root Authority (RCA)

All Certificates issued by DPC CSC RCA contain X.509 Distinguished Names in the **Subject** field. The following attributes will be applied:

countryName (C)	**AZ**
organizationName (O)	CSC
organizationalUnitName (OU)	Certification Services
commonName (CN)	Depending on the entity receiving the Certificate (e.g. “AZ Policy Authority (PCA)”)

3.1.1.1 Need for Names to be Meaningful

The Subject name contained in a Certificate must be meaningful in the sense that the DPC CSC Root CA has proper evidence of the existent association between these names and the entities to which they belong.

3.1.2 Pseudonymity of Subscribers

No stipulations

3.1.3 Rules for Interpreting Various Name Forms

No stipulations

3.1.4 Uniqueness of Names

Subject field must contain an X.500 distinguished name (DN). The DN must be unique for each Subject certified by the CA as defined by the Issuer name field. A CA may issue more than one Certificate with the same DN to the same Subject.

As a minimum, it is checked that a proposed distinguished name has not already been used in a Certificate issued by the DPC CSC Root CA to another entity. Any digital Certificate request which is not unique will be rejected by the DPC CSC Root CA. Subscribers who are rejected by the CA on the grounds that their name is not unique will be notified as promptly as is operationally possible.

3.1.5 Recognition, Authentication, and Role of Trademarks

3.1.5.1 Public and Private Keys

All intellectual property rights in the public and private keys generated shall vest in the entity by which or for which such keys were generated (e.g. Trusted CA, End Users) or the entity designated by it. Subordinate PKI Entities and End Users shall not obtain any rights whatsoever in relation to the Certificates, their content, format or structure.

3.1.5.2 Certificate

Certificate Applicants are prohibited from using names in their Certificate applications that infringe upon the intellectual property rights of others. DPC CSC, however, does not verify whether a Certificate Applicant has intellectual property rights in the name appearing in a Certificate application. DPC CSC does not arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark.

DPC CSC reserves the right at any time to suspend or revoke any Certificate in accordance with the procedures and policies set out in this Certification Practice Statement and the applicable Certificate Policy. DPC CSC hereby grants a non-exclusive and revocable license to all Subordinate PKI Entities, End Users, Relying Parties and other entities to reproduce and distribute copies of the Certificates issued by DPC CSC CAs for the purposes of providing, using or relying on the Certificates and certification services in accordance with the provisions of this CPS.

3.2 Initial Identity Validation

Subject to proving their identity and capacity to provide Certification Authority services in accordance with the DPC CSC Root CPS, legal persons may become and operate a Trusted Certification Authority within DPC CSC's chain of trust.

To ensure the integrity and trustworthiness of operations throughout the PKI hierarchy, Trusted Certification Authorities must undertake to comply with the practices in this CPS and the CPS adopted by them, as part of the Certificate application process. This section states requirements for the verification of the identity of DPC CSC Trusted Certification Authority Applicants. The requirements for PKI entities subordinated to a Trusted CA are stated in the corresponding Trusted CA Certification Practice Statement.

DPC CSC Root CA or the RA acting on behalf of DPC CSC Root CA must ensure that Applicants are properly identified and authenticated, and that Applicant Certificate requests are complete, accurate and duly authorised.

3.2.1 Method to Prove Possession of the Private Key

Certificate Request to DPC CSC Root CA is only accepted as PKCS#10 Certificate request to be securely transported to the DPC CSC Root CA. Verification of the signature on the PKCS#10 request constitute sufficient proof of possession of the corresponding private key.

3.2.2 Authentication of Organization Identity

An Applicant's identity and capacity to provide Trusted CA services within the DPC CSC PKI is determined during the process of negotiating and establishing an Trusted Certification Authority. Such process includes:

- high-level management contacts between DPC CSC and the Applicant;
- a visit by DPC CSC staff to the premises of the Applicant;
- the registration number (in the Enterprise or Commercial Registry or other similar register) of the legal entity;
- in case of a governmental or public entity, an official letter by the superior governmental entity under which the applicant operates indicating its support and the authority of the Applicant to provide Trusted CA services; and

- verification of the following facts:
  - the full legal name and postal address of the entity; and
  - the identity and authority of the natural person(s) with the mandate to represent the applicant, in accordance with sec. 0 of this CPS.

3.2.2.1 Verification of the Identity of Persons Representing the Trusted CA Applicant

The authentication of individual identity is based on the personal (physical) presence of the Applicant in the RA. The Applicant has to identify himself with valid identification document issued by trustworthy authority, e.g., identity card of citizen of the Republic of Azerbaijan.

Authentication of Trusted CA's representative is performed in a three-step process:

1. the Applicant has to identify himself with valid document of identification;
2. information submitted by the Applicant is validated against IAMAS;
3. result of validation and correctness of Initial Identity Validation procedure is checked by an authorised second person of DPC CSC.

3.2.3 Validation of Authority

Every time an Applicant requires the inclusion of information about a certain organisation in a Certificate, Applicant must provide written evidence that the organisation has complete knowledge about this fact. DPC CSC CA provides appropriate form.

3.2.4 Criteria for Interoperation

At present no interoperability criteria are defined by the DPC Certification Services Center. Cross certification with other certification services centers is not foreseen at this moment.

3.3 I&A for Rekey Requests

Re-keying of Certificates may be conducted after communication with the DPC CSC Officer, the DPC CSC Security Officer and the representative of the Trusted CA. A request of re-keying of Trusted CA Certificates must be done in written form on paper.

Procedure for Identification and authentication of re-keying requests follows the initial identity validation procedures defined in this CPS.

3.4 I&A for Revocation Requests

A request of revocation of Certificates must be done in written form on paper.

All revocation requests are required to be valid. The DPC CSC Security Officer must authenticate that a request for revocation of the DPC CSC PCA Certificate is complete, accurate and duly authorised. Such validity shall be determined by their compliance or non-compliance with the procedures of this CPS (see 0),which include references to the authority of the person who may make a request.

Revocation of CA Certificates will be conducted after communication with the ICS Head of Certification services and the DPC CSC Security Officer.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit A Certificate Application?

Any registered organisation or legal entity is allowed to apply for Certificates of DPC CSC RCA.

The Certificate application procedure for Certificates issued by the DPC CSC Root CA is an integral part of the setting up of a subordinated Trusted Certification Authority. As such, the procedure will only be initiated once DPC CSC Root CA consider the applicant has met or is in a position to meet all technical, financial, infrastructural, know-how, legal and regulatory requirements.

The ICS Head of Certification Services shall approve the application after necessary inspection.

4.1.2 Certificate Application Submission

Certificate applications include a fully documented file referencing the compliance with the requirements to become a DPC CSC Trusted CA or Service, including a full set of documents concerning the identity of the legal entity and the natural persons authorised to represent it. Natural persons may not act as Trusted Certification Authorities.

4.1.3 Approval or Rejection of Certificate Application

After the initial application is complete, the evaluation process of applications to become DPC CSC trusted CA comprises the following:

- review of the full Certificate application by DPC CSC staff in order to determine its compliance with DPC CSC PKI requirements and parameters;
- visit of a DPC CSC representative in order to verify their technical, financial, infrastructural, and know-how capacity to provide certification services within the DPC CSC PKI; and
- performance of a full Certification Authority audit at the applicant's premises by a specialised entity designated by DPC CSC in accordance with chapter **0** of this CPS.

Any non-compliance detected during the Certificate application evaluation shall be notified to the applicant and its rectification shall be required in the shortest time possible. If noncompliance is substantial, a new Certificate application evaluation may be required.

4.1.4 Procedure for Processing Certificate Application (Certificate Request)

The Certificate application procedure for Certificates issued by the DPC CSC Root CA is an integral part of the setting up of a subordinated Trusted Certification Authority. As such, the procedure will only be initiated once DPC CSC consider the applicant has met or is in a position to meet all technical, financial, infrastructural, know-how, legal and regulatory requirements.

Certificate Request procedure will be documented and witnessed by DPC CSC Security Officer and a representative of subscribing organisation. Particularly DPC CSC Security Officer ensures the secure transport of Subscriber Certificate request.

Certificate Request to DPC CSC RCA is only accepted as PKCS#10 Certificate request to be securely transported to the DPC CSC RCA. Verification of the signature on the PKCS#10 request constitute sufficient proof of possession of the corresponding private key.

Certificate applications include a fully documented file referencing the compliance with the requirements to become a DPC CSC Trusted CA, including a full set of documents concerning the identity of the legal entity and the natural persons authorised to represent it.

Applications must be in original paper form and as requested by DPC CSC Root CA.

4.1.5 Time to Process Certificate Application

Processing of Certificate application is done timely after creation and acceptance by DPC CSC Root CA. A Certificate application remains active until rejected.

4.2 Certificate Issuance and Publication

To ensure proper security of the Root CA key pair, the server running Root CA services is not connected to the network and is located in offline security vault which complies with security standards for cryptographic modules set forth in chapter 0. Procedures are established and approved in order to ensure integrity and non repudiation of Certificate requests, certification of Trusted CA's Public Key and Certificate dissemination. Access to DPC CSC Root CA devices is granted only for authorised personnel. Furthermore, M*N authentication is used to ensure proper access to the Root CA services.

Certificate issuance to an DPC CSC Trusted CA entails the following:

- the Trusted CA conducts its CA Creation Ceremony, which will have gained prior approval by DPC CSC, and shall be witnessed by DPC CSC staff and an independent auditor designated by DPC CSC;
- the applicant will generate its key pairs in an approved cryptographic module in accordance with chapter 0 of this CPS and will generate a PKCS#10 Certificate request;
- the Certificate request will be securely transported to the DPC CSC Root CA on computer readable media, where DPC CSC operating staff will verify the request and then generate the CA Certificate and create the Subordinate PKI Entity within the DPC CSC logical infrastructure;
- the Trusted CA Certificate will then be taken from the Root CA on computer readable media for incorporation into the Trusted CA system and dissemination as required;
- all valid Certificates issued to Trusted Certification Authorities are manually published on the DPC CSC Web site.

4.3 Certificate Acceptance

Certificate acceptance shall take place as part of or as a result of the Trusted CA Creation Ceremony and will occur at the moment the applicant and DPC CSC approves compliance of the ceremony with the documented Trusted CA creation rules. Upon acceptance of its Certificates, the applicant becomes a Trusted Certification Authority.

4.4 Key Pair and Certificate Usage

4.4.1 Private Key and Certificate Usage

The Root CA Private Key is only used for:

- issuance of Certificates to Certification Authorities that have been approved to become DPC CSC Trusted Certification Authorities;
- issuance of DPC CSC Root CA's Certificate Revocation Lists;
- cross-certification, as approved by the DPC CSC (currently not foreseen).

The private key and corresponding Certificate of DPC CSC Trusted Certification Authorities are used for the purposes referred to in the corresponding Certification Practice Statement. The following general obligations are to be applied:

- the Certificate shall be used in accordance with Trusted CA Agreement, the terms of this CPS and appropriate CP; and
- use of the private key corresponding to the public key in the Certificate is only permitted once the CA has agreed to the Trusted CA Agreement and accepted the Certificate contents by acknowledgement.

4.4.2 Relying Party Public Key and Certificate Usage

Before any act of reliance, Relying Parties shall:

- take account of any limitations on the usage and liability limits of the Certificate as indicated in the applicable Certificate Policy; and
- securely obtain the DPC CSC Root CA Certificate, the Trusted CA Certificate and any other Certificates within the corresponding Certificate chain.

4.5 Certificate Renewal

Certificate renewal is the issuance of a new Certificate to the Trusted CA without changing the public key or any other information in the Certificate. DPC CSC RCA does not provide Certificate renewal services.

4.6 Certificate Re-key

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.

Subject or Subscriber will be informed 30 days prior to expiration of the validity of Certificate by postal notice or e-mail. If a Certificate is expired, Subscriber is required to apply for a new Certificate in accordance with section 0.

4.7 Certificate Modification

DPC CSC RCA makes no changes to an existing Certificate, since this would prevent the verification of any digital signatures on the Certificate and cause the Certificate to be invalid. In a situation where the information referred to in the Certificate has changed or should be changed DPC CSC RCA issues a new Certificate containing the modified information.

4.8 Certificate Suspension

Certificate suspension for Certificates issued by DPC CSC Root CA is not provided.

4.9 Certificate Revocation

Certificate revocation is the process of changing the status of a Certificate from ‘valid’ to ‘revoked’. Certificate status ‘revoked’ means that it should not longer be relied upon by any entity for whatever purpose.

DPC CSC Root CA provides services for revocation of Trusted CA Certificates.

4.9.1 Circumstances for Revocation

DPC CSC Root CA revokes without delay a Certificate in the following circumstances:

- an eligible request for the revocation of the Certificate is received;
- the private key corresponding to the public key in the Certificate has been lost, disclosed without authorisation, stolen or compromised in any way;
- the Certificate Subscriber does not meet material obligations of the Root CA or Subordinate Trusted CA agreement with DPC CSC, those of any applicable CPS, or this CPS;
- the Certificate Subscriber ceases its operations as an Trusted Certification Authority;
- fulfillment of a court adjudication regarding the revocation of the Certificate; or
- whether the probable suspicion exists that the algorithms, parameters and devices used for the production and application of the private key any longer do not ensure the falsification safeness of the produced signatures.

4.9.2 Who Can Request Revocation

Revocation may be requested by the following entities outside of DPC CSC:

- a representative of the Certificate Subscriber explicitly given authority to perform revocation requests and presentation of proof of such authority in accordance with chapter 0;
- Azerbaijan court decision by which a decision of a foreign court or public authority requesting the revocation of the Certificate issued by DPC CSC is declared executable in Azerbaijan.

Revocation is performed by duly authorised DPC CSC Revocation Officer upon a lawful and authorised request.

4.9.3 Procedure for Revocation Request

Revocation is performed by duly authorised DPC CSC Security Officer upon a lawful and authorised request.

- DPC CSC RCA receives a revocation request;
- Security Officer ensures that revocation request is properly formed;
- Security Officer ensures that requesting representative is properly identified, authenticated and authorised;
- Security Officer authenticates himself in DPC CSC IS;
- Security Officer processes revocation (updating OCSP status information and publishing of new CRL);
- DPC CSC RCA informs the Subscriber by letter or e-mail

4.9.4 Time within Which CA Must Process the Revocation Request

The maximum delay between receipt of a revocation request or report and the change to Certificate status information being available to all Relying parties depends on method of Certificate validation:

- for Certificate validation using the most recent CRL it shall be at most 2 days (48 hours).

4.9.5 Revocation Checking Requirements for Relying Parties

Before any act of reliance, Relying Parties shall verify the validity of the Certificate using current revocation status information and taking into consideration the delays in the dissemination of Certificate status information. The aspects to be considered shall include whether:

- the digital signature was created during the validity period of the Certificate;
- all of the public key hashes (fingerprints) on the Certificates within the corresponding Certificate chain are verified successfully;
- the Certificates in the Certificate chain have not expired;
- the Certificate and Certificate chain are successfully validated.

One method by which Relying Parties may check Certificate status is by consulting the most recent CRL using DPC CSC Directory Service.

4.9.5.1 CRL Issuance Frequency

CRL Type	Content	Issuance Frequency	Validity **(incl. overlapping time)**	Overlapping Time
Total/ complete	Revoked Certificates issued by DPC CSC Root CA	Every three month and after revocation	3 month	1 week

If a Certificate listed in a CRL expires, it will be removed from later-issued CRL's.

4.9.6 Maximum Latency for CRLs

CRL's are posted to the repository within a commercially reasonable time after generation. This is generally done within minutes of generation.

4.9.7 On-Line Revocation and Status Checking Availability

DPC CSC RCA provides only CRL method for checking status of issued Certificates.

4.9.8 Special Requirements Regarding Key Compromise

If suspicion exists that the algorithms, parameter or devices used for generation and usage of private keys are no longer secure an appropriate investigation is initiated by DPC CSC Security Officer.

4.10 Certificate Status Services

DPC CSC RCA provides only CRL method to check statuses of issued Certificates.

4.11 Key Escrow and Recovery

Key Escrow is not permitted.

5 Facility, Management, and Operational Controls

5.1 Physical Security Controls

DPC CSC uses trustworthy systems and products which are protected against modification and ensure the technical and cryptographic security of the process supported by them.

DPC CSC has implemented Physical Security Regulations and Procedures [7] , which supports the security requirements of this CPS. The Physical Security Regulations and Procedures contain sensitive security information and is only available upon agreement with DPC CSC. An overview of the requirements is described below.

5.1.1 Site Location and Construction

DPC CSC services are conducted within a physically protected environment that deters, prevents, and detects unauthorised use of, access to, or disclosure of sensitive information and systems whether covert or overt.

5.1.2 Physical Access

DPC CSC Root CA systems are protected by a minimum of 3 tiers of physical security, with access to the lower tier required before gaining access to the higher tier. Progressively restrictive physical access privileges control access to each tier.

The protection provided is commensurate with the identified risks. The DPC CSC ensures that physical access to critical services is controlled and physical risks to its assets are minimised.

A clear description of the physical environment of DPC CSC is available. This includes:

- the implemented security zones and their protection properties (preventive, repressive, detective and corrective);
- the relation with the security critical assets;
- documentation about which members of the DPC CSC staff have access to what zones;
- implementation of adequate protection (preventive, detective and corrective) against fire and smoke, power failures, water, storm etc., based on a documented risk-analysis;
- implemented access control systems;
- procedures to regularly change access codes to high-security zones;
- implemented devices and procedures to ensure that any person entering the physically secure area is always in presence of an authorised person; and

- the responsibility of maintaining the above description, risk-analysis and inventory is assigned to the DPC CSC Security Officer. Periodically reviewing of the above description is a management task.

5.1.3 Power and Air Conditioning

DPC CSC's secure facilities are equipped with primary and backup:

- power systems to ensure continuous, uninterrupted access to electric power; and
- heating, ventilation, air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

DPC CSC has taken reasonable precautions to minimise the impact of water exposure to information systems.

5.1.5 Fire Prevention and Protection

DPC CSC has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. DPC CSC's fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within DPC CSC facilities. These facilities have appropriate physical and logical access controls designed to limit access to authorised personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroised in accordance the manufacturers' guidance prior to disposal.

5.1.8 Off-Site Backup

DPC CSC performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media is stored in a physically secure manner using a bonded third party storage facility or DPC CSC's disaster recovery facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

All critical and sensitive activities of DPC CSC are combined into roles, which are described in DPC CSC´s Organization Description [6] . According to ETSI 101 456 [8] , Trusted Roles include roles that involve the following responsibilities:

- Security Officer: overall responsibility for administering the implementation of the security practices;
- System Officer: responsible for operating the CA trustworthy systems on a day-to-day basis. Authorised to perform system backup and recovery;
- System Administrator: authorised to install, configure and maintain the CA trustworthy systems for registration, Certificate generation, Subject device provision and revocation management;
- System Operator: authorised to backup and restore the operating system and the CA database; and
- System Auditor: authorised to view archives and audit logs related to the activities of the CA trustworthy systems.

DPC CSC considers the categories of personnel identified in this section as Trusted Persons having Trusted Roles

Trusted Roles and responsibilities include the requirement to:

- implement and act in accordance with the organisation's information security policies;
- protect assets from unauthorised access, dICSlosure, modification, destruction or interference;
- execute particular security processes or activities;
- ensure responsibility is assigned to the individual for actions taken;
- report security events or potential events or other security risks to the organisation.

5.2.2 Number of Persons required per Task

DPC CSC has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

The following activities require at a minimum, that two Trusted Persons have either physical or logical access to the device or location:

- logical and physical access to HSM's;
- physical access to data archive; and
- logical access to central, sensitive or critical systems of DPC CSC Root CA and their backup-systems.

5.2.3 Identification and Authentication for Each Role

Identification and authentication of persons take place by admission to safety-relevant areas and by the access to critical systems by smart cards. In the control systems the authorisation of the users are managed by roles.

5.3 Personnel Controls

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel and a check of well-recognised documents of identification e.g., passports. Identity is further confirmed through the background checking procedures as described in this CPS. DPC CSC ensures that personnel have achieved trusted status, and departmental approval has been given before such personnel are:

- issued access devices and granted access to the required facilities;
- issued electronic credentials to access and perform specific functions on DPC CSC Root CA.

5.3.1 Qualifications, Experience, and Clearance Requirements

Well described job descriptions are used to document security and other Trusted Roles and responsibilities and they are clearly communicated to job candidates during the pre-employment process.

Background verification checks on all candidates for employment (contractors and external users) are carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

5.3.2 Background Check Procedures

DPC CSC will 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 CPS and the DPC

CSC Root 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.

5.3.3 Training Requirements

The DPC CSC Root CA ensures that all personnel performing managerial duties with respect to the operation of the Root CA receive comprehensive training in:

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

5.3.4 Retraining Frequency and Requirements

The requirements of Section 0 must be kept current to accommodate changes in the DPC CSC IS. Refresher training must be conducted as required, and DPC CSC must review these requirements at least once a year.

5.3.5 Job Rotation Frequency and Sequence

This CPS makes no stipulation regarding frequency or sequence of job rotation. Individual policies, which do impose requirements, will provide for continuity and integrity of the DPC CSC service.

5.3.6 Sanctions for Unauthorized Actions

DPC CSC establishes, maintains, and enforces employment policies for the discipline of personnel following unauthorised actions. DICSiplinary actions include measures up to and including termination and shall be commensurate with the frequency and severity of the unauthorised actions.

5.3.7 Contracting Personnel Requirements

DPC CSC permits independent contractors or consultants to become Trusted Persons only to the extent necessary to accommodate clearly-defined outsourcing relationships and only under the following conditions:

- the entity 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 entity 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.

5.3.8 Documentation Supplied To Personnel

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

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

5.4.1.1 Root CA Operation Procedures

All events related to the operation of DPC CSC Root CA will be recorded:

- system start-up and shutdown;
- Root 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 Certificate creation policies e.g., validity period;
- login and logoff attempts;
- certificate lifecycle management-related events (e.g., Certificate Applications, issuance, revocation, and renewal);
- cryptographic module lifecycle management-related events (e.g., receipt, use, de-installation, and retirement); and
- system configuration changes and maintenance.

5.4.1.2 Events In Lifecycle Of HSM And System Cards

- initializing Administrator and Operator Card Sest (ACS, OCS);
- initializing of HSM;
- changes at configuration of an HSM;
- log on and log out at HSM;

- key generation in HSM with ACS;
- key-regeneration in new HSM with ACS; and
- deactivating Private Keys.

5.4.1.3 Registration Data

All data involved in each Certificate registration process will be carefully recorded for future reference if needed. The Root CA shall ensure that all registration information including the following is recorded:

- type of documents presented by the Applicant to support registration;
- record of unique identification data, numbers, or a combination thereof of identification documents, if applicable;
- storage location of copies of applications and identification documents, including any signed Trusted CA Agreements;
- any specific choices in the Trusted CA Agreement (e.g. consent to publication of Certificate); and
- identity of the person accepting the application.

5.4.1.4 The Certificate Generation

All data and procedures involved in the certification and distribution of Certificates will be recorded. This includes information such as

- Certificate request;
- Certificate issuance;
- Certificate acceptance; un
- Certificate publication.

5.4.1.5 Certificate and CRL Publication

All data relevant to the publication of Certificates and CRLs by the DPC CSC Root CA to the LDAP server will be recorded.

5.4.1.6 Certificate Revocation

All Certificate revocation request details will be recorded including:

- name of Revocation Officer;

- date, time and identity of person who initiated the request; and
- reason for revocation.

5.4.1.7 System Maintenance and Error Detection

As the DPC CSC environment will involve maintenance by appointed DPC CSC CA administrators, all details of maintenance performed on the machines will be recorded. The DPC CSC CA administrators will also log critical error messages detected on any of the designated machines.

5.4.2 Frequency of Processing Log

DPC CSC Root CA ensures that its audit logs are reviewed by appointed personnel at least weekly and all significant events are explained in an audit log summary. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Supporting manual and electronic logs from the Root CA shall be compared where any action is deemed suspicious. Actions taken following these reviews must be documented.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained onsite for at least two months after processing and thereafter archived in accordance with Section 0.

5.4.4 Protection of Audit Log

Audit logs shall be protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorised viewing, modification, deletion, or other tampering. The electronic audit log system must also include mechanisms to time-stamp entries. Manual audit information must be protected from unauthorised viewing, modification and destruction.

5.4.5 Audit Log Backup Procedures

Incremental backups of audit logs are created weekly and full backups are performed monthly.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application and operating system level. Manually generated audit data is recorded by DPC CSC personnel in Trusted Roles.

5.5 Records Archival

5.5.1 Types of Records Archived

DPC CSC RCA records concerning the operation of its certification services are archived and are retained for the minimum period given in sec. 0. All physical records and Identification Information shall be archived by the entity that directly provides certification services to a Subscriber (i.e. DPC CSC Client Service Points). In all cases, the records may be archived in paper or electronic form.

Written documents will be archived in Client Service Points or DPC CSC's centralised archive in accordance to Latvian State Archives regulations.

5.5.2 Retention Period for Archive

Archive records will be kept for a period of at least ten (10) years without any loss of data. Such period may be extended with regard to specific records and information upon request of special archiving services.

5.5.3 Protection of Archive

The archive shall be protected against unauthorised 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 0.

5.5.4 Archive Backup Procedures

Adequate backup procedures are in place so that in the event of the loss or destruction of the primary archives, a complete set of backup copies will be readily available within a short period of time.

5.5.5 Requirements for Time-Stamping of Records

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

5.5.6 Archive Collection System (Internal or External)

DPC CSC archive collection systems shall be internal.

5.5.7 Procedures to Obtain and Verify Archive Information

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

5.6 Key Changeover

Key changeover is not automatic. Keys expire at the same time as their associated Certificates. DPC CSC RCA instigates key changeover nine (9) years before the expiration of its Certificates (stop issuance date). Other stop issuance dates of end user's Certificate chain of trust are shown in table below.

CA	Validity period	Operational period (Stop Issuance Date)
DPC CSC Root CA	18 years	9 years
DPC CSC Policy CA	12 years	6 years
DPC CSC GOV CA	6 years	3 years
DPC CSC EGOV CA	6 years	3 years

At "Stop Issuance Date" CA stops issuing Certificates with the old key and initiates generation of new keys. CA Key Changeover must be approved by DPC Head of Certification Services Center and will be witnessed by DPC CSC Security Officer. The new Certificate of the new public key is published by DPC CSC Directory Service. Certificate Requests received after the "Stop Issuance Date," will be signed with the new CA Private Key.

DPC CSC RCA minimises disruption by CA key changeover to End Users and Relying Parties in their chain of trust. In this regard, DPC CSC Root CA continues to issue CRLs signed with the original private key until the expiration date of the original key pair has been reached. That means after “Stop Issuance Date” two CRLs will be available, the first CRL signed with the old key and the second CRL signed with the new key.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: Certificate Application data, audit data, and database records for all Certificates issued. Back-ups of CA private keys shall be generated and maintained in accordance with sec. 0.

The procedures for handling of information security incidents and for compromising of private keys of DPC CSC’s Certification Authorities are documented in DPC CSC internal Disaster Recovery Plan. The DPC CSC internal Disaster Recovery Plan describes procedures and responsibilities for handling these types of incidents. Objective of the Disaster Recovery Plan is the immediate recovery of availability and continuous securing of Certification Services. The fundamentals of these procedures are specified in the following sections.

5.7.2 Recovery after Corruption of Computing Resources

After an assumed or actual compromising of resources, software or data disaster recovery procedures will be enacted (in accordance with section 0).

5.7.3 Entity Private Key Compromise Procedures

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

- inform 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 RCA’s Certificate.

5.7.4 Business Continuity Capabilities after a Disaster

The High Availability of Certification Services provided by DPC CSC is guaranteed with the implementation of the hot-standby installation of the information system.

In the event of the corruption or loss of computing resources, software or data, DPC CSC has in place an appropriate Disaster Recovery and Business Continuity Plan. The plan requires setting up and rendering operational a facility located in a geographically diverse area that is capable of providing CA services in accordance with this CPS.

Re-establishment of critical services like Certificate Suspension and Revocation, Certificate Validation and Publication of CRLs will be done within a time scale of 4 hours max. Full functionality will be provided within seventy two (72) hours. This plan includes a complete and periodic test of readiness for such facility. Such plan will be referenced within an appropriate documentation and available to authorised parties for inspection.

5.8 CA Termination

In the event that it is necessary for DPC CSC Root CA to cease operation, DPC CSC makes a commercially reasonable effort to notify Trusted CAs, Relying Parties, and other affected entities of such termination in advance of the CA termination. The following termination plan should minimise disruption to customers, Trusted CAs, and Relying Parties:

- publication of a notification to parties affected by the termination;
- revocation of Certificates issued to DPC CSC Trusted CAs;
- preservation of the CA’s archives and records for the time periods required in this CPS;
- continuation of Customer Support and Help Desk services;
- continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services;
- disposition of the Root CA’s private key; and provisions needed for the transition of the DPC CSC Root CA’s services to a successor Root CA.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

DPC CSC Root CA key pair generation is performed by trained and trusted personnel using trustworthy systems that provide for the security and required cryptographic strength for the generated keys. Key pair generation follows a documented Root CA key ceremony witnessed by an independent auditor.

DPC CSC Root CA keys will be generated and stored in a Hardware Security Module (HSM) which is certified for FIPS 140-2 Level 3 for key generation and storage, which protects the key from external compromise. The RCA private key may never leave the HSM in a readable form.

HSM in FIPS compliance mode requires two sets of HSM system cards: one for administrative purposes and another set for operational purposes. The sets are not interchangeable.

6.1.2 Public Key Delivery to Root CA

When a public key of a Trusted CA is transferred to the DPC CSC Root CA to be certified, it will be delivered through a secure mechanism ensuring that the public key has not been altered during transit and that the Trusted CA possesses the private key corresponding to the transferred public key.

6.1.3 Public Key Delivery to Users and Relying Parties

The Certificate of the Root CA is distributed to End Users and Relying Parties for Certificate path validation purposes. Root CA public key is available from the Certificate repository.

6.1.4 Key Sizes

The key size of DPC CSC Root CA is 4096 bits. The RSA algorithm is used. Keys of Trusted Subordinate CAs are all 2048 bits in length and use the RSA algorithm. The size of the OCSP signing keys is 2048 bits in length, the RSA algorithm is also in use.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

HSM used by DPC CSC Root CA meets the requirements identified in FIPS 140-2, level 3.

6.2.2 Private Key Multi-Person Control

DPC CSC has implemented technical and procedural mechanisms that require the participation of multiple Trusted Persons to perform sensitive Root CA cryptographic operations. In order to gain access to the private keys, 3 out of 6 persons are required. No single person has all the activation data needed for accessing any of the Root CA private key.

6.2.3 Private Key Escrow

Escrow of Root CA private keys is not permitted.

6.2.4 Private Key Backup

DPC CSC RCA Private Key will be backed up and securely stored for the unlikely event of key loss due to unexpected power interruption or hardware failure. Key backup will occur as part of CA key generation ceremony. Backed up CA private key shall remain secret and its integrity and authenticity shall be retained.

Private keys will be re-generated using a key regeneration card set. Key re-generation procedure is documented and must be done under dual control in a physically secure site.

Subject’s private keys for secure e-signatures are generated and stored on a smart card. As the private keys can not be extracted from the smart card they are therefore not backed up.

6.2.5 Private Key Archival

When DPC CSC Root CA key pair reaches the end of their validity period, it will be securely destroyed in accordance with this CPS.

6.2.6 Private Key Transfer into a Cryptographic Module

DPC CSC generates Root CA key pairs in the HSM modules in which the keys will be used.

6.2.7 Private Key Storage on Cryptographic Module

DPC CSC Root CA private key is held in HSM modules in encrypted form.

6.2.8 Method of Activating Private Key

Root CA private key can be activated by introducing the pre-defined number of Operator Cards in the HSM. Root CA Private key activation requires entry and validation of a PIN compliant with specified security parameters.

6.2.9 Method of Deactivating Private Key

After use, they must be deactivated by taking the Operator Cards out of the HSM.

6.2.9 Method of Destroying Private Key

Private keys shall be destroyed if they are no longer needed, or when the Certificates to which they correspond expire or are revoked. Private keys shall be destroyed in a way that prevents their loss, theft, modification, unauthorised disclosure, or unauthorised use.

Root CA private key shall be considered destroyed, if all Operator Cards which are necessary for activating it are destroyed.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

DPC CSC Root CA public keys are backed up and archived as part of DPC CSC’s routine backup procedures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The operational period of a Certificate ends upon its expiration or revocation. The operational period for key pairs is the same as the operational period for the associated Certificates, except that they may continue to be used for signature verification. The maximum operational periods for Certificates issued during the validity period of this CPS are set forth in table below.

Certificate	Validity Period
DPC CSC Root CA Certificate	18 years

The applicability of cryptographic algorithms and parameters is constantly supervised by the management. If an algorithm or the appropriate key length offers no sufficient security during validity period of the Certificate, the concerned Certificate will be revoked and new Certificate application will be initiated.

6.4 Activation Data

Activation data protection complies with FIPS 140-1, level 3.

6.5 Computer Security Controls

DPC CSC has established and documented all computer security technical controls implemented for the DPC CSC Root CA and Certificate Validation Service in accordance to requirements from ISO 27002:2013.

6.6 Life Cycle Technical Controls

No Stipulation

6.7 Network Security Controls

The DPC CSC Root CA is maintained off-line and is not networked with any external components.

7 Certificate Profile of DPC CSC Root CA

All digital Certificates issued by the DPC CSC comply with digital Certificate and CRL profiles as described in RFC 5280 [4] .

7.1 Certificate Profile of Root CA and Policy CA

	Self-signed Root Certification Authority	**Subordinate Policy Certification Authority**
Description	Self-signed certificate used by root authority of AZ CSP.	Certificate used to issue Issuing CA certificates for various certification authorities operating in Azerbaijan.
Basic Certificate Fields		
X509 Version	3	
Serial Number	*Unique integer (unique for each certificate issued by given CA).* *Example: 34:74:cc:10:d4:2a:fa:d2:00:00:00:00:00:03*	
Signature Algorithm	sha1WithRSAEncryption	
Issuer	*Name of the CA that issued certificate. In this case the same as the name of DN.*	*Name of the CA that issued certificate.*
Validity Period	18 years	12 years

Subject	CN = AZ Root Authority (RCA)
	OU = Certification Services
		CN = AZ Policy Authority (PCA)
		OU = Certification Services

	Self-signed Root Certification Authority	Subordinate Policy Certification Authority

	O = CSP
	C = AZ
		O = CSP
		C = AZ

Subject Public Key Info	Algorithm = RSA Key Value = *BIT STRING containing public key* *Key length = 4096 bit*	Algorithm = RSA Key Value = *BIT STRING containing public key* *Key length = 2048 bit*
Key Usage	Certificate Sign, CRL Sign (critical)	Certificate Sign, CRL Sign (critical)
Basic Constraints	Subject Type = CA Path Length Constraint = None	Subject Type = CA Path Length Constraint = None
Subject Key Identifier		
CA Version	*Version of CA keys (certificates). Value is incremented with each renewal.* *Example: V0.0*	*Version of CA keys (certificates). Value is incremented with each renewal.* *Example: V0.0*
Certificate Policies	[1]Certificate Policy: Policy Identifier= 1.3.6.1.4.1. 32843.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://asxm.e-imza.az/repository	[1]Certificate Policy: Policy Identifier=1.3.6.1.4.1. 32843.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://asxm.e-imza.az/repository
Authority Key Identifier		*OCTET STRING containing hash of the issuer's public key*
CRL Distribution Points		[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://asxm.e-imza.az/cdp/<rootcaname>.crl URL=ldap://asxm.e-imza.az/<RootCANameAsDN>?certificaterevocationlist?base?objectclass=certificationauthority
Authority Information Access		[1]Authority Info Access Access Method= Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://asxm.e-imza.az/aia/<caname>.crt [2]Authority Info Access Access Method= Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=ldap://asxm.e-

	Self-signed Root Certification Authority	Subordinate Policy Certification Authority
		imza.az/<CANameAsDN>?cacertificate?base?objectclass=certificationauthority
Enhanced Key Usage		

7.2 CRL Profile of Root CA

		DPC CSC Root Certification Centre **CRL Root CA** **Root CA Signed**
CRL Standard	**Attribute**	**Content**
Version		*V2*
Issuer		*RootCA Name as DN*
Effective date		Issuing Date and Time
Next update		Date and Time of Next Update
Signature algorithm		*sha1RSA*
Authority Key Identifier	Key Identifier	Sha1 hash of Root CA Public Key
CA Version		*V0.0*
CRL Number		Allocated automatically by Root CA
Next CRL Publish		Issuing Date + 3 months

8 Compliance Audit and Other Assessment

Root CA conformance to this CPS will 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 organisation but should have no hierarchical relationship with the department operating the DPC CSC Root CA.

The scope of annual audit includes Root CA environmental controls, key management operations, Infrastructure and Administrative Root CA controls, Certificate life cycle management and Root CA business practices dICSlosure.

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 renewal 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 CA Trusted Agreement.

9.1.2 Certificate Validation Fees

DPC CSC may charge fees for Certificate Validation Services in cases not prohibited by e-Signature Law.

9.1.3 Refund Policy

DPC CSC Root CA or a Subordinate Certification Authority may establish a refund policy. Where a refund policy applies to End Users, 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 Subordinate Issuing Certification Authorities are regulated through Trusted CA Agreements with such entities. This CPS is incorporated into such agreements.

Unless otherwise explicitly agreed or explicitly provided for in a Certificate Policy approved by DPC CSC, DPC CSC´s liability to Subordinate CAs, Relying Parties and any other entities that are not Subordinate CAs, 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 CPS.

Subject to the foregoing limitations, DPC CSC´s liability limit towards all Subordinate CAs, Relying Parties and any other entities that are not Subordinate CAs for the whole of the validity period of a Certificate issued by DPC CSC Root CA (e.g. 6 years unless revoked) towards all persons with regard to such Certificate is limited by an amount defined by DPC CSC.

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 Root CA is done in compliance with the " Law on Personal Data" and based on the distinction provided in this CPS. Personal information collected and used by Trusted Certification Authorities shall also be required to comply with the applicable data protection legislation.

In the cases where a Trusted Certification Authority 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 Subordinate 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 is 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 End User through the Subscriber Agreement or other agreements. Unless explicitly otherwise stated in a Certificate Policy or Certification Practice Statement, upon acceptance of Certificates, the End Users shall authorize DPC CSC Root CA and the Subordinate CA's 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 Root CA and its Certificate Validation 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 Root CA, its Certificate Validation Services or any other Subordinate CA 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.

When required by law and the appropriate procedures, warrants or other legal requirements have been obtained or met, the full audit data may be released in accordance with sections 0 and 0.

9.3.2 Types of Information Not Considered Confidential

9.3.2.1 Certificate And Certificate Status Information

All Certificates issued by the DPC CSC Root CA for public use shall be publicly available. The Certificates issued by Trusted CAs shall be treated in accordance with the applicable CPS and Certificate Policies. 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 CPS, Trusted CA CPS, Certificate Policies and any relevant agreements (e.g. Relying Party Agreement).

9.3.2.2 PKI Documentation

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

- approved public Certificate Policies and Certification Practice Statements;
- this Root CA CPS;
- 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 a Trusted CA shall be made public, in accordance with applicable law or in the sole and absolute discretion of DPC CSC or the Trusted CA that issued the Certificate which was revoked.

Information about Certificate revocation or validity is disclosed using the OCSP protocol and Certificate Revocation Lists (CRL's). 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 Trusted 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.

Trusted CAs 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

All personal information collected or used by the DPC CSC RCA is protected in accordance with the Personal Data Protection Law. Personal information is disclosed to a third party only if mandated by legal requirements.

The personal privacy by collecting, storing and using personal information about Subjects, Subscribers, Staff and Relying Parties shall be protected in accordance with law and standards.

9.4.1 Information Treated As Confidential

All personal information collected or used by this DPC CSC RCA is done in compliance with the "Law on Personal Data" and based on the distinction provided in this CPS.

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

In the cases where this Certification Authority 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 Subordinate 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.

9.4.2 Information Not Deemed Confidential

Subject to LR laws, Certificate and Certificate status information shall be dICSlosed for any purposes that may be relevant for the use of such information and Certificate status in accordance with the consent given by the Trusted CA through appropriate agreements. Unless explicitly otherwise stated in a Certificate Policy or Certification Practice Statement, upon acceptance of Certificates, the Subordinate CAs shall authorise 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.

9.4.3 Responsibility to Protect Private Information

All entities of DPC CSC's PKI receiving private information shall secure it from compromise and dICSlosure to third parties and shall comply with all local privacy laws in their jurisdiction.

9.4.4 Notice and Consent to Use Private Information

Unless otherwise stated in the applicable privacy laws, in this CPS or by special agreement, private information will not be used without the consent of the party to whom that information applies.

9.4.5 Disclosure Pursuant to Judicial or Administrative Process

DPC CSC shall be entitled to disclose confidential information related to natural persons if, in good faith, DPC CSC believes that:

- disclosure is necessary in response to subpoenas and search warrants;
- disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

9.4.6 Other Information Disclosure Circumstances

No Stipulations

9.5 Intellectual Property Rights

All intellectual property rights including copyright in all Certificates, Certificate revocation lists, OCSP Certificate status messages, Certificate directories and, unless otherwise explicitly provided for, all practices, policy, operational and security documents concerning the DPC CSC PKI (electronic or otherwise) 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 Root CA Certification Services in accordance with this CPS. Section 0 of this CPS states the only warranties provided by DPC CSC in the operation of DPC CSC Root CA. 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 or a Trusted CA;
- that deviate from this CPS; or
- 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 End Users 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 CPS;
- third party products or services (including hardware and software);
- non-compliance by a Trusted CA with the "Law on Personal Data" , personal data protection legislation, or any other legislative or regulatory compliance required;
- non renewal of a Certificate as a result of non-compliance with the Certificate renewal requirements as indicated in this CPS; 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 0 of this CPS and those provided in the Certification Practice Statement and Certificate Policies under which a Certificate is issued.

9.8 Indemnities

9.8.1 Indemnification by Subscribers

To the extent permitted by applicable law, Subordinate Certification Authorities are required to indemnify DPC CSC Root CA for:

- falsehood or misrepresentation of fact on the Trusted CA's Certificate Application;
- failure by the Trusted CA to dICSlose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party;
- the Trusted CA's failure to protect the Trusted CA's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, dICSlosure, modification, or unauthorised use of the Trusted CA's private key; or

- the Trusted CA'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 Trusted CA 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 Root CA 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 CPS becomes effective upon publication in the DPC CSC repository. Amendments to this CPS become effective upon publication in the DPC CSC repository.

9.9.2 Termination

This CPS 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 CPS

For maintenance and approval of the CPS 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 actualisation of the CPS is given on the web page of DPC CSC.

9.11.3 Changes in OID

In the case of an actualisation 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 actualisation of the CPS.

9.12 Dispute Resolution Procedures

9.12.1 Hierarchy of the Certification Practice Statement

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

- a Trusted CA Agreement, this CPS shall prevail;
- any agreement between Subordinate Trusted CAs, this CPS shall prevail;
- an End User agreement or Relying Party agreement, this CPS shall prevail; and
- any policy, plan, procedures or any other operational or practices documentation whatsoever, this CPS 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.

Regardless of the measures taken by the parties to resolve the dispute in accordance with this CPS, DPC CSC shall retain its right to seek injunctive relief in the event of alleged or effective material breach of this CPS 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 CPS 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

Terms and acronyms

CA	Certification Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certification Service Provider
DN	Distinguished Name
FIPS	United States Federal Information Processing Standards
I&A	Identification and Authentication
IS	Information System

IAMAS	State register on entrance-departure and registration of citizens of the Republic of Azerbaijan
DPC CSC CA	DPC Certification Services Center Certification Authority
O	Organization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organisational Unit
PCA	Policy CA
PKI	Public Key Infrastructure
RFC	Request for Comments
RSA	A specific public key algorithm
URL	Uniform Resource Locator

References

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

[2] Certificate Policy of DPC Certification Services Center

[3] DPC CSC Security Regulations, internal documentation

[4] 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]

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

[6] DPC CSC Organisation Description, internal documentation

[7] Physical Security Regulations and Procedures, DPC CSC internal documentation

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

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