CERTIFICATION POLICY

FOR

PROJECT

ESTABLISHMENT OF CERTIFICATION AUTHORITY FOR REPUBLIC OF ARMENIA

Version 1.4

Nov 13, 2013

Contract:	signed May 11th, 2012
Purchaser:	E-Governance Infrastructure Implementation Unit CJSC (EKENG CJSC)
Supplier:	Polish Security Printing Works

Details of documents:

File name: CAAM Certification Policy 1v4.docx

Number of pages: 29

Approved by

This document requires the approval of the Purchaser's Project Manager.

Name	Signature	Date of Issue	Version
Arthur Ghulyan		25-05-2012	1.1
Arthur Ghulyan		22-06-2012	1.2
Arthur Ghulyan		22-06-2012	1.3
Arthur Ghulyan		13-11-2013	1.4

Version history

Version	Date	Author	Comments
0.1	2011-09-20	Artur Miękina	Working version of document.
1.0	2011-11-11	Franciszek Wołowski	Verification and corrections. First version of document.
1.1	2012-03-20	Artur Miękina Franciszek Wołowski	Modification of agreed parameters
1.2	2012-06-19	Artur Miękina	OCSP protocol
1.3	2012-11-09	Franciszek Wołowski	a number of minor modifications
1.4	2013-11-13	Jerzy Compa	Update of links

List of Contents

1. Introduction

1.1. Overview

The present document constitutes a Certification Regulation executed by e-ID CA, acting in accordance with Certification Policy. Certification Policy ought to be read together with Certification Practice Statement

Structure of the document was based on the document RFC 3647 *"Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework"*. In order to maintain uniform structure, particular chapters were maintained even there, where comprehensive content was enclosed in Certification Policy and Certification Practice Statement does not precise the manner of execution of activities described in Certification Policy.

The X.509 standard defines a CP as "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".

Currently the CSP for e-ID CA is the E-Governance Infrastructure Implementation Unit CJSC (EKENG CJSC) in Republic of Armenia.

EKENG CJSC assumes the role of Certification Services Provider (“CSP”) in the sense of the Law of 9 July 2001 (further called “the law on the digital signatures”) and of the European Directive 1999/93.
The e-ID CA is the technical name of the certification authority that issues identity and signature certificates for the Electronic Identification Cards. These services are provided in accordance with the requirements of the Law of the Republic of Armenia “On Electronic Document and Electronic Signature” of 15 January, 2005,

EKENG CJSC assumes, on behalf and for the account of the Republic of Armenia, both the roles of CA and CSP for the e-ID CA and is in that capacity responsible for the Subscriber Certificates issued under the e-ID CA. The Republic of Armenia is responsible for the e-ID CA and for the CA certificates issued under the e-ID CA.

1.2. Document name and identification

CP Name	CAAM Certification Policy
CP version	1.4
Status	Final
Policy classifier	None
Object Identifier (OID)	To be specified later
Beginning date	xx-xx-2013
Ending date	until recall

1.3. PKI participants

The present chapter covers Certification Authorities, Subscribers, Registration Authorities and Relying Parties from CA_AM CA.

Certification Policy regulates the most important relations between the entities belonging to CA_AM CA

The regulations particularly apply to:

- Certification Authorities,
- Registration Authority,
- Subscribers,
- Relying parties.

1.3.1. Certification Authority

A Certification Authority (CA_AM CA) issues digital certificates that are used in the Electronic Identification Cards. It is a root CA. The CA_AM CA ensures the availability of all services pertaining to the certificates, including the issuing, revocation and status verification, as they may become available or required in specific applications.
The CA_AM CA is supervised and accredited in application of Article 15 of the Law of the Republic of Armenia "On Electronic Document and Electronic Signature"
To deliver CA services including the issuance, suspension, revocation, renewal, status verification of certificates, the CA_AM CA operates a secure facility and provides for a disaster recovery facility in Republic of Armenia.
The domain of responsibility of the CA_AM CA comprises the overall management of the certificate lifecycle including:

- Issuance;
- Suspension/Unsuspension;

Establishment of Certification Authority for Republic of Armenia

- Revocation;
- Status verification
- Directory service.

CA_AM CA issues and publish CRL's on publicly available at: http://crl.pki.am/citizenca_2013.crl.

1.3.2. Registration Authorities

The Registration Authority ("RA"), certifies that a given public key belongs to a given entity (for example, a person) by issuing a digital certificate and signing it with its private key.

RA is responsible for:

- the authentication of the Subscribers,
- the registration of the to be certified data,
- the authorization to issue a certificate for a particular Subscriber,
- taking care that Subscriber's Certificates are stored on the correct identity card,
- taking care that a Subscriber receives that precise card he is expected to receive and activate the card in question only when dully attributed to the correct Subscriber,
- suspension and revocation: the entity who suspends and/or revokes the certificates in the sense of the law on the digital signatures.

1.3.3. Subscribers

The Subscribers of the CA_AM CA are citizens who are holder of an e-ID card with activated certificates.
Subscribers are identified in both in certificates and hold the private key corresponding to the respective public key that are listed in his certificate.
The Subscriber has the right to indicate at the beginning of the CA_AM application process whether they want to use certificate. The e-ID card is delivered to the Subscribers with certificate loaded. For Subscribers who do not wish to use the Subscriber Certificates, these certificates will be suspended.
The certificate for identification and electronic signature will always be suspended for Subscribers not having reached the age of 16.

1.3.4. Relying Parties

Relying parties are entities including natural or legal persons who rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a Subscriber's Certificate. To verify the validity of a digital certificate they receive, relying parties must always check the validity period of the certificate and the validity declaration of the certificate by the CA service (via CRL) prior to relying on information featured in a certificate.

1.4. Certificate usage

Certificate applicability range states the scope of permitted certificate usage. This scope defines the character of certificate applicability (e.g. electronic signature, confidentiality or certification policy identifier).

Certificate Name	Application
e-Signature	Digital signature (Non-repudation) - ONLY
e-Identification	Digital signature and key encipherment
Infrastructure certificates	In particular, Infrastructure certificates are used to: a. agreeing protocols or providing key distribution data confidentiality, b. ensuring that, during transmission or storage, confidentiality and integrity of the certificate requests, key users, registers events c. verifying access to equipment, verification, signatory software,.

1.5. Certification Policy Administration

The present regulations were prepared for the purposes of CA_AM CA.

Valid version of the Certification Policy is available in http://www.pki.am/policy

EKENG CJSC is obliged to establish PKI Management Board.

On the composition of the PKI Management Board decides the EKENG CJSC.

1.5.1 Contact points

Contact point for handling of all issues connected with execution of the present Certification Policy:

E-Governance Infrastructure Implementation Unit CJSC

Address: Republic Square, Government House 1, 0010 Yerevan, RA

Tel: *+ 374 10 212 333*; **E-mail:** support@ekeng.am

1.6. Glossary of terms and acronyms used

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

The following notions stall be used in this document with the below mentioned meanings:

notion	**description**
CA_AM CA	Certification Authority for CA_AM. CA issuing Subscriber's Certificates
CA_AM	The complete system of the e-ID card including the organisation, infrastructure, procedures, contacts and all necessary resources, pertaining to the e-ID card.
Certification Service Provider	Any physical or moral person who delivers and manages Certificates or provides other services related to electronic signatures. In the context of this CPS, the Certification Service Provider is EKENG SJSC.
Certificate Policy (CP)	The present document – a named set of rules, defining application of a certificate for a particular community of users and / or application class with common requirements in scope of safety;
Certification Practice Statement (CPS)	Document supporting certification Policy describing the operating part of public key certification process, participants of this process (Certification Authorities, Registration Authorities, Subscribers and Trusting Parties) and describing the areas of application of certificates obtained as its result;
Subscriber	Owner of a certificate, user directly linked with a public key enclosed in the certificate on the basis of the content of suitable fields of a certificate;
Subscriber Certificates	The certificates issued for Subscriber for two application: • e-Signature certificate (to create electronic signature) • e-Identification certificate (to authentication in electronic transactions
Infrastructure certificate	Certificates used to provide non-repudiation of origin, authentication and assurance of confidentiality in the exchange of information between the entities operating in the CA_AM system

EKENG CJSC (CSP)	E-Governance Infrastructure Implementation Unit CJSC (EKENG CJSC)
Object Identifier OID (Object Identifier)	Unique numeric identifier subordinated to an information unit – defines its meaning;
OCSP	On-line Certificate status Protocol
Public Key Infrastructure PKI (Public Key Infrastructure) -	All technical, operational and organizational issues enabling rendering of various services for protection of information, with application of public key cryptography and public key certificates;
Electronic Identification Card (e-ID card)	The card which to equip Subscribers with the possibility for identification, authentication and electronic signatures for transfers,
CRL list	List of cancelled certificates and certification certificates.
Auto-signed certificate	Certification Authority Certificate containing an identifier that distinguishes the Certification Authority, in place provided for details concerning the issuer of a certificate and in place provided for the details concerning the owner of a certificate; auto-signed certificate contains a public key of the Certification Authority, which is assigned for verification of this certificate.
Repository	A database and/or directory listing digital certificates and other relevant information accessible on-line.
RRA	Regional Registration Authority
RSA algorithm	Encoding algorithm, which technical specification is unequivocally specified b6 the following object identifier *{joint-iso-ccitt(2) ds(5) module(1) algorithm(8) encryption Algorithm(1) 1}.*
Key ceremony	Procedure, in which a pair of keys is generated with the use of a cryptographic module and where a public key is
Trusted certification path	Chain of many certificates required to identify validity of a certificate containing the required public key.
SDMS	Secure Documents Management System
SDPS	Secure Documents Personalization System
CRL	Certificate Revocation List

HSM (Hardware Security Module, Host Security Module)	Hardware safety module assigned for storage of cryptographic keys and execution of cryptographic operations;

2. Publication and repository responsibilities

The CA_AM CA publishes information about the digital certificates it issues in (an) online publicly accessible repository(ies) under the http://www.pki.am.

The CA_AM CA retains an online Repository of documents where it makes certain disclosures about its practices, procedures and the content of certain of its policies including its CP, which is accessible at http://www.pki.am/policy

The CA reserves its right to make available and publish information on its policies by any means it sees fit.

PKI participants are notified that the CA may publish information they submit directly or indirectly to the CA on publicly accessible directories for purposes associated with the provision of electronic certificate status information. The CA publishes digital certificate status information in frequent intervals as indicated in this CP.

The CA sets up and maintains a Repository of all certificates it has issued. This Repository also indicates the status of a certificate issued.

The CA publishes CRL's at regular intervals at http://crl.pki.am/citizenca_2013.crl

The CA maintains the CRL distribution point and the information on this URL until the expiration date of all certificates, containing the CRL distribution point. Approved versions of documents to be published on the Repository are uploaded within 24 hours.

The whole information published by CA_AM CA in its Repository at http://www.pki.am is accessible for the public.

CA_AM CA service unit has implemented logical a physical mechanisms protecting against unauthorized adding, removing and modifying of the information published in the repository.

On discovering the breach of information integrity in the Repository, CA_AM CA shall take appropriate actions intending to re-establish the information integrity, impose legal sanctions in relation to the abusers, notify the affected entities and compensate their loss

3. Identification and authentication

3.1 Naming

Certification Authority is required to upload data Subscribers in issued certificates. Subscribers create a so-called names. distinguished name DN (distinguished name stands for). Distinguished name is a set of attributes that identify the Subscriber. Certification Center determines acceptable set of attributes and their importance. Subscriber name attributes should contain national characters, if they were included in the Subscriber Data.

3.2 Initial Identity Validation

The identification of the Subscriber who applies for an e-ID card will be done according the procedures and regulations describing in the Certification Policy.

3.3 Identification and Authentication for Re-key Requests

When a Subscribers certificate has expired and renewal of certification services is made, Subscriber shall be subjected to the procedure described in section 3.2. in CPS
When a Subscribers certificate has been revoked, Subscriber shall be subjected to the procedure described in section 3.2. in CPS

3.4 Identification and Authentication for Revocation and Suspension Requests

Certificate status management procedures are particularly important aspects, fundamentally affecting the credibility of the Certification Centre and certification services it provides.

Application for revocation, suspension or (un) suspension of the certificate should be provided:

- personally (through RRA);
- via e-mail to EKENG CJSC;
- using helpdesk established by the RA for this purpose.

The detailed procedure for the management of the state of the validity of the certificate has been described in Chapter 4.

4. Certificate Life-Cycle Operational Requirements

For all entities within the CSP domain including the RRAs, Subscribers, relying parties and/or other participants there is a continuous obligation to inform directly or indirectly the RA of all changes in the information featured in a certificate during the operational period of such certificate or of any other fact that materially affects the validity of a certificate. The RA will then take appropriate measures to make sure that the situation is rectified (e.g. ask the CA for the revocation of the existing certificates and the generation of new certificates with the correct data).
The CA issues, revokes or suspends certificates only at the request of the RA or the CSP to the exclusion of any other, unless explicitly instructed so by the RA.

4.1 Certificate Application

The procedure of certificate application describes the Subscribers steps to obtain the certificate.

4.2 Certificate Application Processing

EKENG CJSC performs identification and authentication of all required information.

4.3 Certificate Issuance

Any certificate can be issued by presence of at least 2 members of the CVCA working group.

4.4 Certificate Acceptance

The certificates activation process requires that Subscriber check the content of Subscribers Certificates. The procedure for approval of the Subscribers Certificate should be carried out by the Subscriber immediately upon receipt of them.

4.5 Key Pair and Certificate Usage

The responsibilities relating to the use of keys and certificates include the ones addressed below.

4.5.1 Subscriber duties

Unless otherwise stated in this CP, Subscriber's duties include the ones below:

- Refraining from tampering with a certificate.
- Only using certificates for legal and authorised purposes in accordance with the CPS.
- Using a certificate, as it may be reasonable under the circumstances.
- Preventing the compromise, loss, disclosure, modification, or otherwise unauthorised use of their private keys.

4.5.2 Relying party duties

A party relying on a certificate will:

- Validate a certificate by using a CRL validation in accordance with the certificate path validation procedure;
- Trust a certificate only if it has not been suspended or revoked;
- Rely on a certificate, as may be reasonable under the circumstances.

4.6 Certificate Renewal

The Subscriber certificates will be renewed in the case of:

- Electronic Identification Card renewal;
- Rekey after revocation.

The procedure is the same like in a first time application

4.7 Certificate Rekey

After revocation the Subscriber certificates can not be activated again and must therefore be replaced by new certificates. On request of the Subscriber the RRA will generate a new key-pair on the Electronic Identification Card and replace the revoked certificates by new certificates.

4.8 Certificate Modification

Section is not applicable.

4.9 Certificate Revocation and Suspension

Until acceptance or denial by the Subscriber, Subscriber Certificates remain suspended in an Electronic Identification Card. To request the suspension or revocation of a certificate, a Subscriber must contact an RRA or the RA Helpdesk.

4.10 On-line revocation/status checking availability

EKENG provides real-time certificate status verification service OCSP – according to RFC 2560. Using OCSP, it is possible to acquire more frequent and up-to-date information (in comparison to CRL usage) about a certificate status.

OCSP supplies the following information about the certificate status:

good – meaning a positive response to the request, which should be interpreted as confirmation of certificate validity,

revoked – meaning the certificate has been revoked,

unknown – meaning the certificate has not been issued by any of the affiliated certification authorities.

Certificate status is available in real-time

4.11 Certificate Status Services

The CA makes available certificate status checking services including CRLs,

CRL http://crl.pki.am/citizenca_2013.crl

CRLs are signed by the CA. A CRL is issued every 3 hours.
The CA makes all CRLs issued in the previous 12 months available in the Repository.

4.12 End of subscription

Does not apply

4.13 Key Escrow and Recovery

Key escrow and recovery are not allowed.

5 Facility, Management and Operational Controls

This section describes non-technical security controls used by the CA_AM CA and the other PKI partners, to perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival.

5.1 Physical controls

The aim of physical controls for non-technical security is to prevent unauthorised access, damage and interference in the information connected with the issuance, validation and use of certificates and into the spaces in which equipment is located that is used for handing this information.

CA_AM CA assure that it render its services in a safe environment, which cover:

a) Location and structure;
b) Physical access;
c) Storage of carriers;
d) Waste disposal.

5.2 Procedural controls

Procedural securities are applied, and in particular distribution of duties due to application of the principle of two pairs of eyes for critical, e.g. for modification of CA_AM CA, generating certificates for CA_AM CA infrastructure or cancellation of certificates.

CA_AM CA assure that system access to all PKI devices is limited – on the basis of the necessary knowledge – to the group of people holding suitable entitlements, i.e. at least suitable individual operator's account.

Key activities connected with the actions of operators handling certification Policies and of high level of protection, require dual control. It shall be reached due to division of the secret that is necessary to perform a particular action into two parts or by multiple authentications. Assignment of passwords must be controlled by a formalized management process.

Activities of Certification (CA_AM CA) and Registration Authorities is subject to constant audit and is monitored by safety inspectors or auditors. Key system events for system safety are additionally remembered by audit mechanisms of the applied operating systems.

5.3 Personnel controls

All CA_AM CA PKI systems, are used by a qualified and experienced personnel.
Detailed rules for personal protection described in section 5.3. CPS

5.4 Audit logging procedures

CA_AM CA makes use of even registration procedures for the purposes of analysis and recognition of all their correct and incorrect uses in CA_AM CA PKI system.
Detailed rules for audit logging procedures described in section 5.4. CPS

5.5 Record Archival

EKENG is responsible for archiving all audit data - electronic and paper records related to CA activity.

CA_AM CA implemented in its PKI system the correct filing procedures, which provide integrity and confidentiality of data.

5.6 Key changeover

CA_AM CA assures that the keys are generated in supervised conditions and in accordance with the procedures security and system access management.

5.7 Compromise and disaster recovery

CA_AM CA undertakes the measures in order to provide continuity of services, in the case of compromise and disaster recovery.

5.7.1 Incident and Compromise Handling Procedures

CA_AM CA assures that in case of a disaster, including violation of protection of a private key of a participant, to restore operations as quick as possible

5.7.2 Computing Resources, Software, and/or Data Are Corrupted

If the computing resources, software, and/or data are corrupted, appropriate incident response should be taken. The incident response can include the re-establishment of the corrupted equipment/data, using similar equipment and/or restoring backup/archived data.

5.7.3 Entity Private Key Compromise Procedures

When CA_AM CA private key cannot to be used for some reasons, the procedure for key changeover shall succeed.

When the CA_AM CA s private key security has been violated the supervising CVCA shall immediately be informed.

5.7.4 Business Continuity Capabilities After a Disaster

CA_AM CA has a Disaster Recovery Plan to prevent or limit various threats.

5.8 CA_AM CA Termination

CA_AM CA is required to implement the procedures and measures to minimize the impact of the effects of closure of the CA_AM CA. These effects are minimized by:

- Procedures for the issuance of certificates by a successor CA_AM CA,
- Forward the certification service provided to an external certification authority. In the event of termination of activity, CA_AM CA is required to notify this to the Subscribers and Relying Parties. Subscribers are informed through e-mail, and Relying Parties through an appropriate message is stated in the Repository. Notification should be made at least one month in advance. Completion of activity associated with the cancellation of all valid certificates of Subscribers, and the cancellation of the certificate of CA_AM CA.

6 Technical security controls

6.1 Key Pair Generation and Installation

The CA protects its private key(s) in accordance with this CP and CPS. The CA uses private signing keys only for signing certificates, CRLs, in accordance with the intended use of each of these keys.

6.1.1 Key Pair Generation

Private key is generated in this safe device (e.g. HSM, cryptographic key). The private key cannot leave the safe device.

6.1.2 Private Key Delivery to a Subscriber

CA_AM CA delivers the private key to a Subscriber.

The Subscribers have the right to indicate at the beginning of the Electronic Identification Card application process whether they want to use Subscriber's Certificates.

6.1.3 Public Key Delivery to Certification Authority

Subscribers public keys are delivered to Certification Authority through the RA. They are sent electronically, via the mechanism implemented in the software of Certification Authority. These mechanisms ensure the integrity and non-repudiation of sending a public keys.

6.1.4 CA Public Key Delivery to relying parties

CA public key issuing certificates to Subscribers are distributed in a form of certificates complying with ITU-T X.509 v.3 recommendations. In the case of CA_AM CA certificates have a form of self-certificates.

CA_AM CA certification authority distribute its certificate in two different methods:

- placement in the publicly available web Repository of EKENG at http://www.pki.am
- distribution together with a dedicated software (e.g. web browsers, email clients, etc.), which allows usage of services offered by EKENG

6.1.5 Key size and cryptographic algorithms

Detailed rules for key size and cryptographic algorithms described in section 6.1.5. CPS (Certificate Practice Statement).

6.1.6 Key Usage Purposes

Usage of every bit of **KeyUsage** field has to comply with the following rules (every bit meaning appropriately):

a) erification of electronic signature created
b) provide a non repudiation service,
c) encrypt symmetric algorithm keys, providing data confidentiality,
d) encryption of subscriber's data,
e) protocols of key agreement,
f) electronic signature verification,
g) verification of electronic signatures on revoked and suspended certificates lists issued by the entities providing certification services,
h) indicate its purpose of data encryption in key agreement protocols,
i) indicate its purpose of data decryption in key agreement protocols,

6.1.7 Extended Key Usage

See chapter 6.1.7 in Certification Practice Statement.

6.2 Private keys protection and technical securities of cryptographic modules

The CA securely generates and protects the private key(s), using a trustworthy system, and takes necessary precautions to prevent the compromise or unauthorised usage of it.

6.2.1 Cryptographic modules standards and controls

The generation of the private key of the CA_AM CA occurs within a secure cryptographic device meeting appropriate requirements including FIPS 140-1 level 3.

6.2.2 Private key (n out of m) multi-person control

The private key of Certification Authority has been generated in a safe device (e.g. HSM, cryptographic key) and divided into the secrets of the principle of "3 of 5".

6.2.3 Private Key Escrow

The present Certification Policy do not provide key-escrow.

6.2.4 Private Key Backup

CA backup mechanism is realized through the division private key on the number of fragments larger than is required to recovery the key.

6.2.5 Private key Archival

The present Certification Policy do not provide private key archival.

6.2.6 Private key transfer into or from a cryptographic module

The present Certification Policy do not provide private key entry into cryptographic module.

6.2.7 Private key activation method

Activation of the CA private key requires cooperation between two people with cards with PIN codes and key parts . Activating the Subscriber key pair requires knowing the PIN codes to the ID card.

6.2.8 Private key destruction method

At the end of their lifetime the CA private keys are destroyed with the principle of two pairs of eyes in the presence of a representative of the Armenian State, in order to ensure that these private keys cannot ever be retrieved and used ever again

6.3 Other aspects of key pair management

6.3.1 Public Key Archival

CA issuing certificates, archives public keys of Subscribers whom certificates were issued to

6.3.2 Certificate Operational Periods

Usage periods depend on the certificate. The maximum and minimum usage periods were presented in Table 2 in section 6.3.2. CPS.

6.4 Activation data

The CA securely stores and archives activation data associated with its own private key and operations.
The Subscriber is obliged to protect a PIN codes allowing access to the private key

6.5 Computer Security Controls

The CA implements certain computer security controls.

6.6 Life cycle technical controls

Safe devices used by CA_AM CA are secured against modification.

6.7 Network Security Controls

The CA maintains a high-level network of systems security including firewalls. Network intrusions are monitored and detected.

6.8 Time stamping

Does not apply.

7 Certificate and CRL Profile

7.1 Certificate Profile

Certificates and CRLs profiles are compatible with the formats specified in ITU-T standard X.509 v3 (RFC 3280).

OCSP profile is compatible with RFC 2560.

Detailed rules for certificate profile described in section 7. CPS (Certificate Practice Statament).

8 Compliance audit and other assessments

The CSP accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CP. The CSP accepts this auditing of its own practices and procedures it does not publicly disclose under certain conditions such as confidentiality, trade secrets etc. Such audits may be carried out directly or through an agent by:

- The supervising authority for Certification Service Providers
- The Armenian government or a third party appointed by the Armenian government.

The CSP evaluates the results of such audits before further implementing them. To carry out the audits an independent auditor will be appointed who will not be affiliated directly or indirectly in any way with the CA or any CA nor having any conflicting interests thereof. If irregularities are detected, the CSP will submit a report to the auditor, stating the measures that will be taken to rectify the situation and ensure compliance. If the proposed measures are deemed insufficient a second audit will be carried out to ensure compliance.

9 Other provisions and legal issues

9.1 Fees

All necessary information is available at EKENG website

9.2 Financial responsibility

Does not apply.

9.3 Confidentiality of business information

The CSP complies with personal data privacy rules and confidentiality rules as described in this CPS rules for confidentiality of business information described in section 9.3. CPS
The following items are not confidential information:

- Certificates and their content;
- Status of a certificate.

9.4 Privacy of Personal Information

All necessary data should be protected according to internal law of Republic of Armenia.
The CSP does not store any other data on certificates or on Subscribers, other than the data, transferred to it and authorised by the RA. Without consent of the data subject or explicit authorization by law, personal data processed by the CSP will not be used for other purposes.

9.5 Intellectual property rights

The Republic of Armenia owns and reserves all intellectual property rights associated with its own databases, web sites, the CA digital certificates and any other publication whatsoever originating from the CA including this CPS. The CSP owns and reserves any and all intellectual property rights it holds on its own infrastructure, databases, web site etc.

9.6 Representation and warranties

All parties including the CA itself, the RA, the RRAs and the Subscribers warrant the integrity of their respective private key(s).

9.7 Disclaimers of warranties

Warranties of CSP are based on the general rules stated in the present Certification Policy and it is in accordance with the superior legal acts in force in the Republic of Armenia.

9.8 Limitations of liability

Does not apply.

9.9 Indemnities

Does not apply.

9.10 Term and termination

This CP remains in force until notice of the opposite is communicated by the CA on its Repository under http://www.pki.am.
Notified changes are appropriately marked by an indicated version

9.11 Individual notices and communications with participants

Notices related to this CP can be addressed to EKENG which can be contacted:
E-Governance Infrastructure Implementation Unit CJSC

Establishment of Certification Authority for Republic of Armenia

Address: Republic Square, Government House 1, 0010 Yerevan, RA
Tel: *+ 374 10 212 333*; **E-mail:** support@ekeng.am