CERTIFICATION PRACTICE STATEMENT

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 Practice Statement 1v4.docx

Number of pages: 50

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		09-11-2012	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	Change the name of the Certification Authority and a number of minor modifications.
1.4	2013-11-13	Jerzy Compa	Update of the name of authority, links

List of Contents

1. Introduction

1.1. Overview

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

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.

Certification Practice Statement is a statement of the practices which a certification authority employs in issuing certificates.

The CP and CPS address the same set of topics that are of interest to the relying party in terms of the degree to and purpose for which a public key certificate should be trusted. Their primary difference is in the focus of their provisions. A CP sets forth the requirements and standards imposed by the PKI with respect to the various topics. In other words, the purpose of the CP is to establish what participants must do. A CPS, by contrast, states how a CA and other participants in a given domain implement procedures and controls to meet the requirements stated in the CP. In other words, the purpose of the CPS is to disclose how the participants perform their functions and implement controls.

An additional difference between a CP and CPS concerns the level of detail of the provisions in each. Although the level of detail may vary among CPSs, a CPS will generally be more detailed than a CP. A CPS provides a detailed description of procedures and controls in place to meet the CP requirements, while a CP is more general.

Currently the CSP for CA_AM 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 CA_AM 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 CA_AM and is in that capacity responsible for the Subscriber Certificates issued under the CA_AM. The Republic of Armenia is responsible for the CA_AM and for the CA certificates issued under the CA_AM.

1.2. Document name and identification

The present document of Certification Practice Statement is given a proper name of "***CAAM Certification Practice Statement"***. The document is available: As an electronic version at the repository at:

http://www.pki.am

Certification Practice Statement Object Identifier is not included in the contents of issued certificates. Only certification policies identifiers belonging to the collection of certification policies incorporated by the present Certification Practice Statement

1.3. PKI participants

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

Certification Practice Statement regulates the most important relations between the entities belonging to CA_AM

The regulations particularly apply to:

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

1.3.1. Certification Authority

A Certification Authority (CA_AM) issues digital certificates that are used in the Electronic Identification Cards. It is a root CA. The CA_AM 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 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 operates a secure facility and provides for a disaster recovery facility in Republic of Armenia.
The domain of responsibility of the CA_AM comprises the overall management of the certificate lifecycle including:

- Issuance;
- Suspension/Unsuspension;
- Revocation;
- Status verification
- Directory service.

CA_AM 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).

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.
- 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 are citizens who are holders of e-ID cards 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 e-ID application process whether (s)he wants 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, the 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 Practice Statement Administration

The present regulations were prepared for the purposes of CA_AM.

Valid version of the Certification Practice Statement is available in http://www.pki.am.

EKENG CJSC is obliged to establish PKI Management Board, whose task is to:

- development of new documents related to the provision of certification services;
- make changes to documents related to the provision of certification services;
- review of documentation related to the provision of certification services (with a frequency at least every 12 months)
- giving opinions on suggestions relating to the provision of certification services arising from Republic of Armenia, Subscribers, relying parties, external experts;
- maintenance of certification documentation;
- send information to Subscribers and Relying Parties to update the documentation.

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 Practice Statement:

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	Certification Authority for e-ID. CA issuing Subscriber's Certificates
e-ID	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)	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 (for authentication in electronic transactions
Infrastructure certificates	Certificates used to provide non-repudiation of origin, authentication and assurance of confidentiality in the exchange of information between the entities operating in the e-ID 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;
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. A place where Subscriber can apply for e-ID managed by National Police.
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. System SDMS system provides central biometric documents management system functionality
SDPS	Secure Documents Personalization System. System SDPS system responsible for documents personalization and cards management
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 publishes information about the digital certificates it issues in (an) online publicly accessible repository(ies) under the http://www.pki.am.
The CA_AM 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 CPS, which is accessible at http://www.pki.am. 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 CPS.
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 makes available an OCSP server at http://ocsp.pki.am/ocsp that provides notice on the status of a certificate, issued by the CA upon request from a relying party, in compliance with IETF RFC 2560. The status of any certificate listed in a CRL, must be consistent with the information, delivered by the OCSP server.
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 in its Repository at http://www.pki.am is accessible for the public.

CA_AM 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 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

CA issues certificates based on data supplied by the Subscriber provided by RA. Subscribers create distinguished name. 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.
Information concerning the Subscriber subject to the submission of the Certificate are subject to strict verification. Certification Centre monitors their compliance through verification of identity cards and other documents entitling the Subscriber to act on behalf of the organization (if that is the case). In order to implement this requirement to apply for a certificate only subscribers are authorized certification services, and authorized representatives of the Organization.
Information for subscribers which is subject to the submission of the Certificate must contain a non-empty distinguished name of the entity. It contains some or all of the attributes contained in the following set of attributes:

Attributes Name	Acronym	Description
common name	cn	The name that is commonly referred subscriber. Is normally created with content attributes name (s) and surname. In the case of Certificates for servers and network devices, this attribute contains the DNS name of the device or other name designated by the Organization.
name (names)	givenName	Subscribers name or names.
surname	sn	Subscribers surname.
User principal name	upn	Unique name that identifies a subscriber in computer systems (eg, a computer account name).
serial number	serialnumber	Unique identifier, which identifies the subscriber. Such an identifier for the CA_AM is Social Security number.
Organization	o	Organization name

Organization Unit	ou	Organization Unit In the Organization
Country Name	c	Name of the country of origin (the only allowable value is AM).
e-mail	emailAddress	Subscribers or Servers e-mail
Certificate Description	Description	Certification Name

Table 1. Permitted attributes of distinguished name.

These attributes may occur in the distinguished name of the Subscriber only once.
The following combinations of Subscribers distinguished names are allowed:

1. The Subscriber is an individual, the certificate may includes the following information:

- common name;
- name (s);
- surname;
- Serial number;
- Country name;
- e-mail address;
- certificate description.

2. In case of server or other computing device it is possible to insert in the certificate the following information:

- common name;
- organization;
- organization unit;
- Country name;
- e-mail address
- certificate description.

As a minimum set of attributes defining the name of the Subscriber or the server or other computer equipment will be allowed the inclusion of:

- common name ("cn");
- Country name ("c").

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 applicable to the delivery of e-ID card.

Subscribers identity verification is only possible at the personal appearance in RRA. Subscriber should provide the present Subscriber's ID and a completed Application for issuing the certificate. The application should be signed by the Subscriber.
The result of verification should be signing a contract for the provision of certification services.
The RA specifies the exact procedures to be implemented by the RRAs.
In the case of electronic issuance of certificates for servers or other devices, is subject the verification of the identity of an authorized representative of the Organization should be done.
Subscriber identity verification, or an authorized representative of the Organization should be done after the presentation of one of the following documents:
• ID card
• passport,

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.
When a Subscribers certificate has been revoked, Subscriber shall be subjected to the procedure described in section 3.2.

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 will be described in Chapter 4.

4. Certificate Life-Cycle - Operational Requirements

For all entities within the Certification Service Provider (CSP) domain including the Regional Registration Authorities (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. During this procedure, the Subscriber is obliged to:

- Read and accept the contents of the CP and CPS;
- Choose the type of digital certificate (referred to in section 1.4);
- Fill the application for issuing of certificate;
- Prepare the document to verification the identity (a list of acceptable documents specified in section 3.2)
- Go to the RRA to finish the procedure

4.2 Certificate Application Processing

EKENG CJSC performs identification and authentication of all required information.
Before issuing the certificate, Registration Authority is required to confirm the identity of the Subscriber. Identity verification is carried out in the RRA by the authorized personnel.
In case of discrepancies in the provided documentation, or inability to unequivocally determining of the Subscribers the identity, the RRA personnel have the right to reject a Subscriber application for certificate. If the application is approved, the RRA transmits the registration data to the RA. The RA in its turn either approves or rejects the application.

4.3 Certificate Issuance

Any certificate can be issued by presence of at least 2 members of the CVCA working group. Following approval of the certificate application, the RA sends a certificate issuance request to the CA. The CA does not verify the completeness, integrity and uniqueness of the data, presented by the RA, but relies completely on the RA for the correctness of all data. The CA

only verifies that the certificate serial number assigned to the certificate request by the RA is indeed a unique serial number that has not yet been used for any other Subscriber Certificate, in which case it notifies the RA.
All requests from the RA are granted approval provided that:

- They are validly formatted;
- Use the proper secure communication channel;
- All appropriate verifications have been performed as defined in the CA policy

The CA verifies the identity of the RA on the basis of credentials presented.
The CA ensures that the issued certificate contains all data that was presented to it in the request of the RA and especially a serial number assigned to the certificate by the RA.
Following issuance of a certificate, the CA posts an issued certificate on a Repository.
Following issuance, the CA suspends the certificate. The certificate is thereafter delivered to the RA. The RA requests the SDPS to load the Subcriber's Certificates on the e-ID card and SDMS delivers securely the Electronic Identification Card with the Subscriber Certificates to the RRA and PINs to the Subcriber by post.

Infrastructure certificates are issued according to internal procedure of EKENG CJSC.

4.4 Certificate Acceptance

After production of the Electronic Identification Card it is in a non activated state. The RRA activates the Electronic Identification Card in the presence of the Subscriber by updating its status in the RA identity database. Both the Subscriber and the RA require the activation data for the card, which has to be supplied by the SDMS in a secure manner. The card can only be activated when using the Subscriber PINs.
It is at the sole discretion of the Subscriber (upon request of an Electronic Identification Card for Subscriber from the age of 16) 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. Any discrepancies in the content of the Certificates, Subscriber is obliged to submit to the RRA personnel. In this case the issued certificate shall be canceled, and the Subscriber receives a new certificate. No reports of any errors in the issued Certificates means acceptance of the Certificate

A certificate may be rejected for example in case of inaccurate Subscriber data or if the Subscriber has not yet reached the legitimate age for the use of the certificate. Objections to accepting an issued certificate are notified via the RRA to the RA in order to requests the CA to revoke the certificates.

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 CPS, 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, OCSP 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 re-key

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. Initial activation of an Subscriber certificate must take place within one month from its issuance. The RA and RRAs act promptly to comply with this requirement. To request the suspension or revocation of a certificate, a Subscriber must contact an RRA or the RA Helpdesk. While an RRA opening hours are limited, the RA helpdesk is available 24 hours per day, 7 days a week.
RRA or RA Helpdesk requests promptly the suspension of the Subscriber certificates via the RA after:

- Having received notice by the Subscriber that a suspicion exist that there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of his Subscriber Certificates.
- The performance of an obligation of the RRA under this CPS is delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result, there is a suspicion that another person's information is materially threatened or compromised.
- Having received notice by the Subscriber that there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of his Subscriber Certificates
- There has been a modification of the information contained in a Subscriber Certificates.

Upon request from the RA or the CSP the CA suspends or revokes the Subscriber Certificates. The RA revokes a pair of suspended certificates after a period of one week if it does not receive notification from the Subscriber to un-suspend the certificate.
Under specific circumstances (e.g. circumvention of a disaster, a CA key comprise, a security breach, …) , the CSP may request suspension and / or revocation of certificates.
RA cares that the concerned Subscriber are warned of such suspension/revocation.
Relying parties must use on line resources that the CA makes available through its repository to check the status of certificates before relying on them. The CA updates CRLs and OCSP. CRLs are updated frequently with minimum intervals of three hours.
The CA grants access to OCSP resources and a web site to which status inquiries can be submitted.

4.9.1 Term and Termination of Suspension and Revocation

Suspension may last for a maximum of seven calendar days in order to establish the conditions that caused the request for suspension. Following negative evidence of such conditions a

Subscriber may request to re-activate (un-suspension of) the Subscriber Certificates on the following conditions:

- The Subscriber has ascertained without any doubt that his suspicion that there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of his Subscriber Certificates was incorrect;
- No other reasons exist to doubt the reliability and confidentiality of the private keys of both of his Subscriber certificates.
- To request the un-suspension of his Subscriber Certificates, a Subscriber must present himself to RRA.

The RRA requests promptly the un-suspension of a pair of Subscriber Certificates via the RA after:

- Having received notice from the Subscriber that a suspicion that there has been a loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of his Subscriber Certificates was undoubtedly incorrect;
- The suspicion has proven undoubtedly incorrect that another person's information would be materially threatened or compromised due to the fact that the performance of an obligation of the RA under this CPS was delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control;
- Upon request from the RA, the CA suspends or revokes a pair of Subscriber Certificates.

The CA automatically revokes a suspended certificate after a period of one week if it does not receive in the meantime notification from the RA to un-suspend the certificate. The CA notifies the RA of all revocations made.
The CA publishes notices of suspended or revoked certificates in the Repository.

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 and OCSP,

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

a) Location and structure: CA_AM is used in the area that is physically secured, e.g. due to separation of rooms into safety zones and due to suitable wall structure; The CA operations are conducted inside a high-security room in a high security zone, within a physically protected building that deters, prevents, and detects unauthorized access, based on multiple tiers of physical security.

b) Physical access: Access to CA_AM is controlled and audited. Only the authorized persons have physical access to CA_AM environment. Cyclic verification of personnel employed in CA_AM ought to take place. In order to provide suitable level of physical protection of CA_AM system, it is required to assure also the following means of protection;

- suitable doors and locks;
- access control;
- movement sensors;
- CCTV systems;
- armoured cabinets;
- windows with suitable structure;
- the system of guaranteed non-interrupted power supply and air conditioning;
- attack and burglary signalling system;
- electromagnetic protection system;
- protection system against flooding
- fire detection and protection system.

a) Storage of carriers: All media containing production software, data, audit, archive or backup information are stored in locked safes and cabinets, protected from accidental damage. Access to media is limited to authorised working group.

b) Waste disposal: Sensitive documents and materials are shredded before disposal.

Media used to collect or transmit sensitive information are rendered unreadable (securely erased or physically destroyed) before disposal. Cryptographic devices and keying material as well as all storage hardware are physically destroyed prior to 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, generating certificates for CA_AM infrastructure or cancellation of certificates.

CA_AM 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) 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.

In particular, the following requirements are used:

a) Protections (e.g . firewalls) are used for protection of internal CV network domains against the access of third parties from domains of external network. The way leading from user's terminal to computer services shall be controlled in scope of network connection route. Mechanisms limiting the number of services shall e used (e.g. HTTP, FTP, etc.) to the available users, in accordance with access control procedures to AR-CA.
b) Sensitive data is protected against unauthorized access or modification; System Uses have direct access only to these services, in relation to which they obtained authorization, usage of system tool programs shall be limited and strictly controlled, and access to CA_AM system ought to use the safe login system. In addition, inactive terminals handling CA_AM system ought to be blocked after a set inactivity period, in order to prevent from access of unauthorized persons (i.e. screensaver with a password).
c) Sensitive data is protected (e.g. using encoding and mechanisms that provide integrity) during transfer in an unsecured network;
d) CA_AM provides effective administration of access of all users (including operators, administrators and all users who have direct access to the system) in order to keep

safety of the system, including management, audit and correct (in time) modification or removal of access, and also assure that access to information and functions of the system is limited to the authorized personnel:

- CA_AM Manager – Management position, covering the scope of duties connected with the total CA_AM operating activity. He is responsible for functioning of CA_AM, for rendering and development of services, investments, operating readiness and continuity of functioning. He has a divided access to CA_AM infrastructure. He has no access to operating data and AR-CA cryptographic keys.
- Safety Inspector – person responsible for the total overview of safety issues. His duties cover constant monitoring of the state of CA_AM safety and reacting to incidents. He controls safety of CA_AM area and personnel. He has the access to CA_AM operating activity registers (system logs) and divided access to CA_AM infrastructure. He is responsible for execution of safety policy. He actively co-creates CA_AM safety documentation. He prepares safety plans for protection of continuity of CA_AM functioning.
- Audit Inspector – analyzes the records of event registers, which take place in data communication systems used whilst certification service rendering
- Network administrator, Data base administrator, System administrator – are responsible for operational exploitation, efficiency and readiness of technical CA_AM equipment. They have a divided access to CA_AM infrastructure. There obliges the principles of distribution of duties for exploitation team members. Sensitive activities must be performed by at least two persons with separate competnces. They have no access to CA_AM cryptographic keys. They are subject to management that manages CA_AM.

The whole CA_AM system contains sufficient IT protections to separate trusted roles, including distribution of safety administrators and exploitation functions. Application of system tool programs is to be particularly strictly controlled. Access is limited in such manner that it is made available only in order to perform the role (roles) assigned to a user.

e) CA_AM personnel is successively identified and authenticated in the above mentioned way, against the use CA_AM PKI applications connected with certification management or access to e-ID cards

f) CA_AM personnel is settled from its activity; for example by keeping event journals, as it was specified in sub-chapter 5.4. Key decisions for safety issues made by CA_AM operators must be settled completely with exactness to a person who performs the operation.

Main decisions are:

- modification of CA_AM PKI system architecture,
- generating certificates,

- cancelling certificates,
- creating and modification of system documentation.

CA_AM must generate suitable automatic (electronic) event journals.

All event records created by key modules for CA_AM ought to contain the following elements:

- date and hour of a record,
- unique event identifier,
- type of event,
- information indicating the place of event (e.g. terminal, port, location, etc.),

For the remaining subsystems, vent records ought to contain at least the following elements:

- date and hour of a record,
- data concerning the event, containing information that allows for unequivocal identification of the source of the event, character of the event and event parameters.

Current and archive event journals ought to be handled in a manner, which precludes from unauthorized modification or damage.

CA_AM shall periodically fill the event journal data of particular subsystems.

CA_AM shall store filled event journals in a safe external location for the agreed period.

Current and filed event journals may be viewed only by authorized persons in justified safety purposes.

5.3 Personnel controls

All CA_AM PKI systems, are used by a qualified and experienced personnel. In particular, they meet the following requirements:

a) CA_AM employs sufficient number of employees, who have specialist knowledge, experience and qualifications, which are required for a particular service and suitable for this official function, i.e.:
   - CA_AM Manager;
   - Safety Inspector;
   - Audit Inspector;
   - Network Administrator;
   - Data Base Administrator;

- System Operator.

b) The personnel are subjected to local safety tests, suitable for the performed role (roles).

c) In relation to persons who violate the policy or procedures of CA_AM, applicable disciplinary sanctions are applied.

d) In scope of duties, safety and responsibility roles are specified in system safety policy. Trusted roles, on which safety of the applied system depend, are exactly specified in chapter 5.2.

e) All personnel (both temporary and permanent) has the scope of duties, defined with consideration of distribution of duties and the smallest privileges, specified in chapter 5.2.

f) All CA_AM personnel of trusted roles is free of interest conflicts, which could have impaired system usage.

g) Personnel, who has the access to CA_AM private keys is officially assigned to trusted roles by the main manager.

h) CA_AM does not assign any person trusted roles or management, about whom it has been recognized that he was sentenced for a serious crime or other action, which could have the influence on his/ her adequateness to the position. Personnel has no access to the trusted functions until the required check-up is performed

5.4 Audit logging procedures

CA_AM makes use of even registration procedures for the purposes of analysis and recognition of all their correct and incorrect uses in CA_AM PKI system.

All significant events in the system must generate auditable logs. These include, at least, the following:

- certificate application, request, issuance, renewal, re-key or revocation
- access attempts to sensitive system resources (e.g. HSM)
- operations performed by the working group members
- physical entry/exit
- For all events the log entry shall include:
- event identifier
- date and time of event

- subject identity that initiated the event
- description of the event

CA_AM assures that significant information concerning a certificate are recorded in a suitable time interval and at least comply with audit requirements described in chapter 8 Audit and other assessments.

CA_AM assures that confidentiality and integrity of the current and filed reserves is maintained, which are connected with certificates and they are filed in full and confidential manner. CA_AM also assures that in event journals are recorded the events concerning key and certificate management, beginning with registration process of certification applications, and ending with cancellation of certificates, and precise time concerning these events is provided, as well as the events connected with the cycle of lifetime of keys and certificates.

Specific events and data, which are to be recorded in the event journal are documented in accordance with the records of the document Operating and Security Procedures.

It is important that the events are recorded in the event journal in such manner that during the required storage period they cannot be easily deleted or destroyed (except for transfer to long-term storage carrier). Details were described in Operating and Security Procedures

5.5 Record Archival

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

The archived data shall be protected:

- against modification and deletion
- against unauthorised access to the data
- against storage media ageing by periodical migration to new media
- against format obsolescence by transformation to general and open standards

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

5.6 Key changeover

CA_AM assures that the keys are generated in supervised conditions and in accordance with the procedures provided in sub-chapter 5.2 Procedural securities and system access management.

CA_AM assures creation of an auto-signed certificate and bookmark certificate. The policy that corresponds to the present Certification Practice Statement specifies two possibilities of key exchange:

1. auto-signed CA_AM certificate is issued and distributed in accordance with chapter 2
2. CA_AM publishes a new CA_AM public key with the use of a bookmark certificate

Bookmark certificate provides continuity of business activity without the need of remote exchange into a new trusted self-signed CA_AM certificate.

Exchange of AR-CA key is necessary if CA_AM certificate loses its validity or CA_AM private key is unavailable. Such cases occur as a result as expiry of CA_AM certificate or lack of access to CA_AM private key (e.g. as a result of failure of hardware, which stores the public key).

However, remote issue of a new self-signed certificate is rather inconvenient. The certificate must be generated and made available and Trusting Parties must trust to the auto-signed certificate. Therefore, if a private CA_AM key is useless for certain non-critical reasons (e.g. as a result of failure of hardware, which stores the private key), bookmark certificate ought to be used for exchange of the key

5.7 Compromise and disaster recovery

CA_AM undertakes the measures in order to provide continuity of services, covering:

a) the measures that minimize the effect of interference in supply delivery due to application of guaranteed uninterrupted supply system. It is forecasted to use the infrastructure of power engineering network supply, which is available within the selected location, after previous verification of supply parameters and possible supplementation with interference filtrating equipment, which also guarantee continuity of supply in the forecasted work time without the access to electric energy from the public network
b) the measures that minimize the effect of such events as flooding or fire, e.g. due to application of suitable protective systems;

c) the measures that minimize the effect of lack of accessibility of key personnel due to implementation of a suitable employment system, which assures continuity of functioning of CA_AM. Critical positions specified in chapter 5.3 must be provided with a complete back-up staff, with reservation of the principles concerning safe distribution of roles.

5.7.1 Incident and Compromise Handling Procedures

CA_AM 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, with reservation of the below mentioned issues.

1. CA_AM defines and keeps the "Business Continuity Plan" in order to act in case of a disaster (see also sub-chapter 5.7.3)
2. CA_AM system data required to renew the usage of CA_AM are copied and stored in suitable safe places, so that it is possible to timely renew the usage in case of failure/ disaster. Off-site backup is used for it
3. Due to the need to take into account the occurrence of a disaster and planning the processes connected with it, "Business Continuity Plan" considers violation of protection or suspicion of violation of private key protection.

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

All information about corruption of computing resources, software and/or data are communicated to the security inspector who assigns the performance of activities under the procedures developed.

These procedures are designed to analyze the intensity of an attack, investigate the incident, to minimize its effects and eliminating it in the future. If necessary, in the case of CA_AM private key compromise or other corruption events appropriate steps must be taken with the Disaster Recovery Plan including 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

CA_AM in the document "Business Continuity Plan" provides in detail how it is going to perform the services of his CA_AM in case of failure, which interferes his regular abilities.

Urgent cases in functioning of CA_AM are natural disasters or cryptographic errors, e.g:

1. Earthquakes, flooding, several days' interruptions in power supply.
2. Violation of the applied algorithms (problems in EC or SHA-1)

Violation of CA_AM private key.

5.7.4 Business Continuity Capabilities After a Disaster

CA_AM has a Disaster Recovery Plan to prevent or limit various threats, like:

- physical corruption to the computer system of CA_AM,
- software and application malfunction;
- loss of important network services
- corruption of a part of the network

All subscribers and relying parties are informed, as soon as possible and in a manner most appropriate for the existing situation, about every significant malfunction or corruption, associated with any information system or network environment component. Disaster recovery plan includes number of procedures executed in the event any part of the system has been subjected to compromise (corruption, revelation, etc).

5.8 CA_AM Termination

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

- Procedures for the issuance of certificates by a successor CA_AM,
- Forward the certification service provided to an external certification authority. In the event of termination of activity, CA_AM 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.

6 Technical security controls

6.1 Key Pair Generation and Installation

The CA protects its private key(s) in accordance with this 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. Generating CA_AM private key is confirmed in accordance with the principle of two pairs of eyes. Persons available for the process of generation authenticate themselves to CA system with the use of a password – a secured cryptographic card.
Generating CA private key takes place in a physically separated safe room and it is performed by trusted personnel with at least dual control. Number of persons responsible for execution of this process ought to be limited to the minimum and the process ought to be performed in accordance with the rules of CA.

6.1.2 Private Key Delivery to a Subscriber

CA_AM 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. The Electronic Identification Card is delivered to the Subscriber with Subscriber Certificates loaded and suspended. Subscribers can un-suspend their certificates in the RRA using activation PIN, which have been sent via post.
Infrastructure certificates with private key are delivered to the personnel of CA_AM according the internal procedure of EKENG CJSC.

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 certificates have a form of self-certificates.
CA_AM 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

Under these CPS and the corresponding CP, determined that:

- A pair of keys should be generated using a cryptographic algorithm RSA;
- The length of Certification Authority key pair is 4096 bits,
- The length of the Subscribers key pair is 2048 bits,
- The length of the Infrastructure certificates (eg system administrators) is 2048 bits.

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) **digitalSignature**: certificate intended for verification of electronic signature created for purposes different than the purposes mentioned in b), f) and g),
b) **nonRepudiation**: certificate intended to provide a non repudiation service by private individuals, although for other purposes than described in f) and g). **NonRepudiation** bit may be set only in a public key certificate intended to verify electronic signatures and should not be combined with any other purposes, especially described in points c)-e) and connected with providing confidentiality,
c) **keyEncipherment**: intended to encrypt symmetric algorithm keys, providing data confidentiality,
d) **dataEncipherment**: intended to encryption of subscriber's data, other than described in c) and e),
e) **keyAgreement**: intended for protocols of key agreement,
f) **keyCertSign**: public key is used for electronic signature verification in certificates issued by entities providing certification services,
g) **cRLSign**: public key is used for verification of electronic signatures on revoked and suspended certificates lists issued by the entities providing certification services,
h) **encipherOnly**: may be used solely with **keyAgreement** bit to indicate its purpose of data encryption in key agreement protocols,
i) **decipherOnly**: may be used solely with **keyAgreement** bit to indicate its purpose of data decryption in key agreement protocols.

6.1.7 Extended Key Usage

This field defines one or more areas, in addition to standard key usage, defined by keyUsage field, of the possible usage of a certificate.

The following key usage purposes are defined:

a) **serverAuth** - TLS WWW server authentication. Key usage bits that may be consistent: digitalSignature, keyEncipherment or keyAgreement;
b) **client authentication** Key usage bits that may be consistent: digitalSignature and/or keyAgreement;
c) **codeSigning** - signing of downloadable executable code. Key usage bits that may be consistent: digitalSignature;
d) **emailProtection** - Key usage bits that may be consistent: digitalSignature, nonRepudiation, and/or (keyEncipherment or keyAgreement)
e) **timeStamping** - Binding the hash of an object to a time. Key usage bits that may be consistent: digitalSignatureand/or nonrepudiation
f) **OCSPSigning** - Signing OCSP responses. Key usage bits that may be consistent: digitalSignature and/or nonRepudiation

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. This process is witnessed by representatives of Republic of Armenia to ensure confidence of the government in the proper and secure execution of the CA Key Generation procedure. The CA implements and documents key generation procedures, in line with this CPS. The CA acknowledges public, international and European standards on trustworthy systems. At least three trusted operatives participate in the generation and installation of CA private key(s).

6.2.1 Cryptographic module standards and controls

The generation of the private key of the CA_AM occurs within a secure cryptographic device meeting appropriate requirements including FIPS 140-1 level 3.
The generation of the private key of the CA requires the control of more than one appropriately authorised member of CA staff serving in trustworthy positions, and at least one representative of the government and of the CSP. More than one member of the CA management makes authorisation of key generation in writing.

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". This means that any 3 secrets from the set of 5 secrets allow for CA private key recovery. Subscribers private keys shall not be divisible for secrets.
Shared secrets are stored on cryptographic cards, protected by a PIN number and transferred in an authenticated manner to their holders.
At least three members of the CA must act concurrently to activate the CA private key.

6.2.3 Private Key Escrow

The present Certification Practice Statement 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 Practice Statement do not provide private key archival.

6.2.6 Private key transfer into or from a cryptographic module

The present Certification Practice Statement 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 - we have a secret division of 3 / 5

Activating the Subscriber key pair requires knowing the PIN codes to the e-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. The CA keys are destroyed by

shredding their primary and backup storage media, by deleting and shredding their shares and by deleting, powering off and removing permanently any hardware modules the keys are stored on.
The key destruction process is documented and any associated records are archived.
The Subscriber is responsible for the destruction his key pair,

6.3 Other aspects of key pair management

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods

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

Certificate Type	Validity Period
National Root	25 years
Parent CA:	14 years
e-Signature	10 years
e-Identification	10 years
Infrastructure certificates	5 years

Table 2: Certificate usage periods

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 are secured against modification.

In order to assure that IT systems are safe, at the stage of designing and preparing specification of requirements for each of the prepared projects undertaken by CA_AM, which have the influence on safe systems or their products, safety requirements analysis is executed.

These is a documented and shared management procedure for changes, modifications and for settlement of emergency software for the total CA_AM software used.

6.7 Network Security Controls

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

In specific:

All communications between the CA and the RA operator regarding any phase of the life cycle of Subscriber Certificates is secured with PKI based encryption and signing techniques, to ensure confidentiality and mutual authentication. This includes communications regarding certificate requests, issuance, suspension, unsuspension and revocation.

The CA web site provides for encrypted connections through the Secure Socket Layer (SSL) protocol and anti-virus protection.

The CA network is protected by a managed firewall and intrusion detection system. It is prohibited to access sensitive CA resources including CA databases from outside of the CA operator's own network. Internet sessions for request and delivery of information are encrypted.

6.8 Time stamping

Does not apply.

7 Certificate and CRL Profile

This section specifies the certificate format, CRL and OCSP formats.

7.1 Certificate Profile

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

Electronic certificate is a sequence of fields forming a data structure that contains the Subscriber data, the public key assigned to it and any other information required for effective use of digital certificate.

The certificate contains the following primary fields:

Field name	Value	Field description
Version	2	third version (X.509 v.3) of certificate format
Serial number	numerical value	certificate serial number, unique within certification authority domain,
Signature algorithm	Sha256withRSA	identifier of the algorithm applied by a certification authority issuing certificates,
Issuer	distinguished name (DN)	distinguished name (DN) of a certification authority,
Not Before	UTC time	validity period, described by the beginning date (**notBefore**) of the certificate validity period,
Not After	UTC time	validity period, described by the ending date (**notAfter**) of the certificate validity period,
Subject	distinguished name (DN)	distinguished name (DN) of the subscriber that is the subject of the certificate,
Subject Public Key Info	RSA public key	value of a public key along with the identifier of the algorithm associated with the key
Extensions	A set of extensions	The set of extensions specifying additional information related to the use of the certificate. The full set of permissible extensions, see Chapter 7.1.1
Signature	Digital signature	Digital signature generated by the CA on the Subscriber Certificate.

The fields specified above are located in each of the Subscribers Certificates issued by the CA_AM.

7.1.1 Certificates Extensions

Extensions carry additional information such as the use of public key stored in the certificate, the additional information that identifies the Subscriber, etc. Below there are all acceptable extensions that may be included in the Subscribers Certificates issued under these CPS and corresponding CP.

Extension name	Value	Extension description	Extension status
keyUsage	Bit combination	Indicates limit the possibility of using the key pair. Permissible combinations are described in Chapter 6.1.6.	Critical
extendedKey Usage	Bit combination	Permissible combinations are described in Chapter 6.1.7.	No-critical
SubjectKey Identifier	data structure	The subject key identifier extension provides a means of identifying certificates that contain a particular public key	No-Critical
Authority Key Identifier	data structure	The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a CRL.	No-critical
SubjectAlternative Name	e-mail - RFC 822	The subject alternative names extension allows additional identities to be bound to the subject of the certificate	No-critical
CRLDistribution Points	URL link	point of distribution of Certificate Revocation List	No-critical
Authority Info Access	URL link	OCSP: http://ocsp.pki.am/ocsp	No-critical
Basic Constraints	Bit combination	The basic constraints extension identifies whether the subject of the certificate is a CA and the maximum depth of valid certification paths that include this certificate.	Critical

Published in the certificate extensions can be crucial to the interpretation of the certificate and the associated public key. It is permissible to mark the expansion as:
• Critical - the information stored in the extension must be unconditionally processed and interpreted by a relying party (eg via an appropriate application). If the information contained in the extension can not be interpreted correctly, relying party is obliged to reject the

information electronically using a secure certificate processed.
• Non-critical - information stored in labeled non-critical extension may be optionally processed by a relying party. If the relying party is unable to properly process the data, it can be omitted without fear that the trust certificate has been disrupted

7.1.2 Certificate for e-Signature

Field	Description/Value	Status field
AuthorityKeyIdentifier	This extension identifies the public key used to verify a issued.certificate	No-critical
keyUsage	This extension specifies the use of the Subscriber key Permissible values: • nonRepudiation	Critical
certificatePolicies	determination or an indication of the certification policy	No-critical
policyIdentifier	OID {....} (An indication of the CP, under which the certificate is issued)	No-critical
subjectAltName	optional extension of the permissible values • rfc822Name (adres email)	No-critical
basicConstraints	empty sequence (to determine whether the subscriber is end user, or whether entity issuing certificates)	Critical
CRL Distribution Point	Field indicates the server address from which you can download a CRL.	No-critical
Authority Info Access	OCSP: http://ocsp.pki.am/ocsp	No-critical

7.1.3 Certificate for e-Identification

Field	Description/Value	Status field
AuthorityKeyIdentifier	This extension identifies the public key used to verify a issued.certificate	No-critical

keyUsage	This extension specifies the use of the Subscriber key Permissible values: • digitalSignature • keyEncipherment • dataEncipherment	Critical
certificatePolicies	determination or an indication of the certification policy	No-critical
policyIdentifier	OID {....} (An indication of the CP, under which the certificate is issued)	No-critical
subjectAltName	optional extension of the permissible values • rfc822Name (adres email)	No-critical
basicConstraints	empty sequence (to determine whether the subscriber is end user, or whether entity issuing certificates)	Critical
CRL Distribution Point	Field indicates the server address from which you can download a CRL.	No-critical

7.1.4 Certificate for Infrastructure

Infrastructure certificates may not be used to make and verification. secure electronic signatures. Profile of Infrastructure certificates are based on a e-Identification certificates profile, in particular used are identical to the encryption algorithms and their parameters, as defined in Chapter 6, and have the same hash functions.

The differences are as follows:

a) lack of acceptable standard and custom extensions,

b) In the event of an extension keyUsage, is possible to use combinations bits indicate the following uses of the certificate:

- "DigitalSignature" to ensure that, during transmission or storage, integrity certificate requests, key users, and event logs to verify access to facilities,
- "KeyEncipherment" and "keyAgreement" to agreement protocols and key distribution ensuring the confidentiality of data. Cryptographic keys associated with Infrastructure certificates are stored in cryptographic components.

7.2 CRL Profile

CRL is a sequence of fields forming a data structure containing information about revoked and suspended certificates and an indication of the Certification Authority responsible for generating the list. Each CRL mandatory contains information about the period of its validity.

The structure of the CRL contains the following fields and extend the basic:

Field or extension name	Value	Field description
Version	1	X.509 version number.
Serial number	numerical value	CRL serial number, unique within certification authority domain,
Signature algorithm	Sha256withRSA	identifier of the algorithm applied by a certification authority issuing CRLs,
Issuer	distinguished name (DN)	distinguished name (DN) of a certification authority,
ThisUpdate	UTC time	the beginning date of the CRL validity period,
NextUpdate	UTC time	ending date of the CRL validity period,
revokedCertificates:	The list of revoked or suspended certificates	The information consist of four sub-fields: • userCertificate - serial number of a revoked certificate, • revocationDate - date of the certificate revocation, • crlEntryExtensions - **e**xtended access to CRL (contains additional information about revoked certificates – optional), CRLReason (contains information about a reason for the revocation of a certificate – optional)
userCertificate	numerical value	Revoked or suspended certificate serial number
revocationDate	Czas wg UTC	Date and time of revocation or suspension.
CRLReason	numerical value	The reason for certificate revocation or information about suspension of certificate. Acceptable field values specified in section 7.2.2.
Extensions	A set of extensions	The set of extensions specifying additional information related to the use of the certificate
Signature	Digital signature	Digital signature generated by the CA on the CRL.

Below are all acceptable extensions that may be included in the CRL.

extension name	Value	Field description	Field status
Authority Key Identifier	data structure	Indicates on a CA certificate, which contains the search (eg by the application) public key.	No-critical

With reference to ITU-T X.509 v3 (RFC 2459), it is acceptable to the inclusion in the CRL of one of the following information about the cause of changes in the validity of the certificate:

Reason code	Code value	Description
unspecified	0	Not specified
keyCompromise	1	Key revelation or compromise
cACompromise	2	CA key compromise
affiliationChanged	3	Subscribers data modification
superseded	4	Certificate renewal
cessationOfOperation	5	Cessasion of certificate usage
certificateHold	6	Suspension of certificate

Information about (un) suspension of the certificate is not published in the CRL.

(Un)suspension causes that suspended certificate is removed from the CRL

7.3 OCSP Profile

The OCSP profile follows IETF PKIX RFC2560 OCSP v1. Certificate status verification service is provided by EKENG on behalf of affiliated certification authority. OCSP server, which issues certificate status confirmations, has a special key pair, developed solely for this purpose.

Certificate status verification server certificate has to contain in its body the extension of extKeyUsage, described in RFC 5280. This extension should be set as critical, and means that a certification authority issuing the certificate to the OCSP server, confirms with its signature delegation of the authorization to issue certificate status conformation (of this authority subscriber's certificates).

e-Signature certificates may also contain non-critical extension AuthorityInfoAccess, indicating the possibility to use the service to confirm the validity of the certificate on-line (OCSP).

Field	Description/Value	Status field
AuthorityKeyIdentifier	This extension identifies the public key used to verify a issued certificate	No-critical
keyUsage	This extension specifies the use of the Subscriber key Permissible values: • Digital signature	No-critical
extendedKeyUsage	ocspSigning	No-critical
ocspNoCheck	Null	No-critical

8 Compliance audit and other assessments

The CSP accepts compliance audits to ensure it meets requirements, standards, procedures and service levels according to this CPS. 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.
The audit addresses the following aspects:

- Compliance of the CSP operating procedures and principles with the procedures and service levels defined in the CPS;
- Management of the infrastructure that implements CSP services;
- Management of the physical site infrastructure;
- Adherence to the CPS;
- Adherence to relevant Armenian laws;
- Asserting agreed service levels;
- Inspection of audit trails, logs, relevant documents etc.;
- Cause of any failure to comply with the conditions above.

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. Confidential information includes:

- Any personal identifiable information on citizens, other than that contained in a certificate;
- Exact reason for the revocation or suspension of a certificate;
- Audit trails;
- Logging information for reporting purposes, such as logs of requests by the RA.
- Correspondence regarding CA services.
- CA Private key(s).

The following items are not confidential information:

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

The CSP does not release nor is it required to release any confidential information without an authenticated and justified request specifying either:

- The party to whom the CA owes a duty to keep information confidential. The CA owes such a duty to the RA and promptly responds to any such requests;
- A court order.

Within the framework of the CSP contract with the Armenian Government, the CSP may charge an administrative fee to process such disclosures. Parties requesting and receiving confidential information are granted permission on the condition that they use it for the requested purposes, secure it from compromise, and refrain from using it or disclosing it to third parties. Also these parties are bound to observe personal data privacy rules in accordance with the law.

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).

Subscriber obligations:

Unless otherwise stated in this CPS, Subscriber's obligations include the ones below:

- Refraining from tampering with a certificate.
- Only using certificates for legal and authorised purposes in accordance with the CPS;
- Applying for a new Electronic Identification Card (and thus Subscribers Certificates) in case of any changes in the information published in the certificate;
- 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;
- Request for the suspension of a certificate in case of the suspicion of an occurrence that materially affects the integrity of a certificate. Such occurrences include indications of loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of the Subscribers Certificates;
- Request the revocation of a certificate in case of an occurrence that materially affects the integrity of a certificate. Such occurrences include loss, theft, modification, unauthorised disclosure, or other compromise of the private key of one or both of the Citizen Certificates, or in case control over private keys has been lost due to compromise of activation data (e.g. PIN code).
- Use the key pair for electronic signature and in accordance with any other limitations notified to the Subscriber;
- Exercise reasonable care to avoid unauthorised use of the subscriber's private key;

- Following compromise, the obligation to immediately and permanently discontinue the use of the subject's private key.

Relying Party Obligations:
A party relying on a CA certificate will:

- Be sufficiently informed about the use of digital certificates and PKI;
- Receive notice and adhere to the conditions this CPS and associated conditions for relying parties;
- Validate a certificate by using a CRL or OCSP in accordance with the certificate path validation procedure;
- Trust a certificate within its validity period only if it has not been suspended or revoked;
- Rely on a certificate, as may be reasonable under the circumstances.

CSP (EKENG CJSC) Obligations:

CSP will:

- Comply with this CPS and its amendments as published under http://www.pki.am
- Provide infrastructure and certification services, including the establishment and operation of the CA Repository and web site for the operation of public certification services;
- Provide Trust mechanisms, including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure;
- Issue electronic certificates in accordance with this CPS and fulfil its obligations presented herein;
- Notify the RA if the CA is unable to validate the application according to this CPS;
- Upon receipt of an authenticated request sent by the RA act promptly to issue a certificate in accordance with this CPS;
- Upon receipt of an authenticated request for revocation from the RA to revoke promptly a certificate in accordance with this CPS;
- Upon receipt of an authenticated request for suspension from the RA to suspend promptly a certificate in accordance with this CPS;
- Upon receipt of an authenticated request for un-suspension from the RA to unsuspend promptly a certificate in accordance with this CPS;
- Publish certificates in accordance with this CPS.
- Publish CRLs and OCSP responses on a regular basis in accordance with this CPS;
- Operate in compliance with the requirements of the Law of the Republic of Armenia "On Electronic Document and Electronic Signature" of 15 January, 2005European Directive 1999/93 on a Community framework for electronic signatures.
- The CSP is responsible towards Subscribers and Relying Parties for the following acts or omissions:
  Issue digital certificates not listing data as submitted by the RA;
  - If a private signing key of the CA is compromised;
  - The failure to revoke a suspended certificate after a period of 7 days;
  - Failure to list a revoked or suspended certificate in a CRL;
- Unauthorised disclosure of confidential information or private data according to

Registration Authority Obligations

The RA operating within the CA domain will:

- Provide correct and accurate information in their communications with the CA;
- Ensure that the public key submitted to the CA corresponds to the private key used;
- Create certificate requests in accordance with this CPS.
- Perform all verification and authenticity actions prescribed by the CA procedures and this CPS;
- Submit to the CA the applicant's request in a signed message;
- Receive, verify and relay to the CA all requests for revocation, suspension and unsuspension of a certificate in accordance with the CA procedures and the CPS;
- Verify the accuracy and authenticity of the information provided by the citizen at the time of renewal of a certificate according to this CPS;

The RA and not the CA is liable for any damages suffered as a result of unverified data that has been listed in a certificate.

9.7 Disclaimers of warranties

Warranties of CSP are based on the general rules stated in the present Certification Practice Statement 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 CPS 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 CPS can be addressed to EKENG which can be contacted:

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