REPUBLIC OF ALBANIA

Production & Distribution of Identity Cards & Biometric Passports

ALBANIA E-ID PKI CITIZEN ROOT CA CERTIFICATION PRACTICE STATEMENT

Aleat
an IDEMIA company

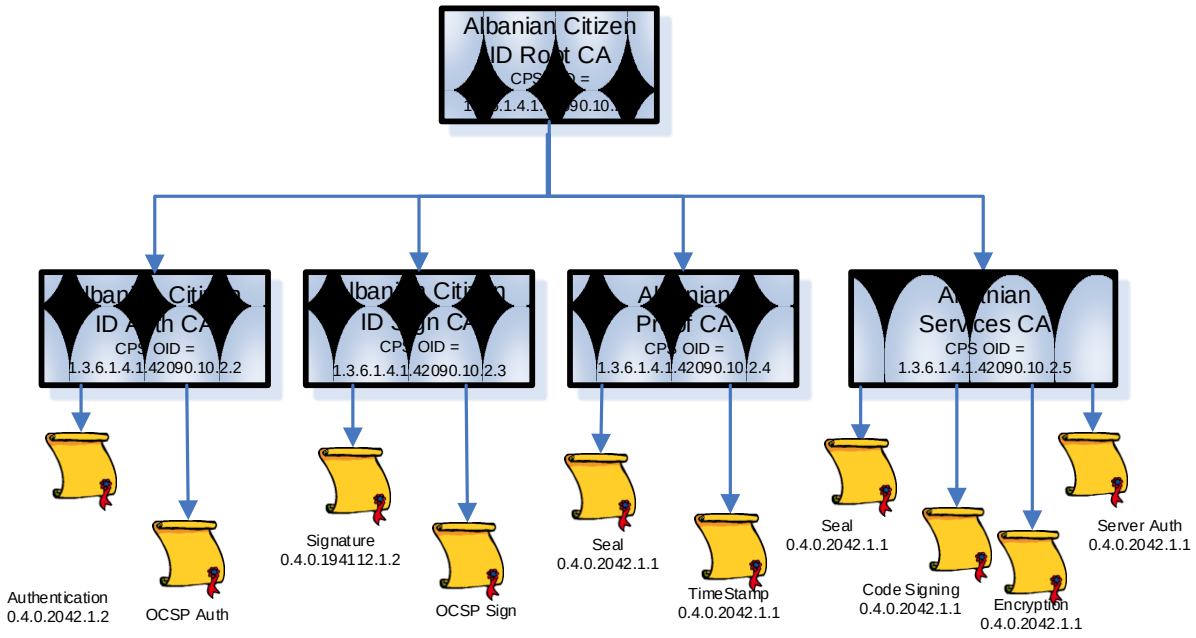
TABLE OF CONTENTS

1. INTRODUCTION

1.1. Overview

Albania operates E-ID Public Key Infrastructure (PKI) to deliver certificates used in the electronic citizen identity card and used for Aleat eServices. The certificates delivered are signed by a Certificate Authority (CA).

CA are signed by a Root Certification Authority (RCA). CA are “on-line” (means CA use a network) and RCA is “Off-line” (means RCA is not used with network).



This Certificate Practice Statement (CPS) defines the procedures applicable to the RCA implements to certify Certification Authority (CA). Each CA has normalized certificate policy as described in RFC 3647 clause 3.3. Each CA has to develop its own CPS.

The present CPS is consistent with:

- The Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practise Statement Framework;

1.2. Document name and Identification

This CPS is the OA property. The corresponding CP is a normalized certificate policy OID is 0.4.0.2042.1.2. This CPS document has its own OID: 1.3.6.1.4.1.42090.10.2.1.

1.3. PKI Participants

Albanian Ministry of Internal Affairs has delegated to Aleat (OA – Operational Authority) which operates the RCA in a dedicated trust center. For this purpose Aleat has established a PMA to manage the RCA and the CA. To host, operate the RCA and certify and host the CA, Aleat deploys a PKI (E-ID PKI).

For the CA certificate issuance activity delivered by the RCA, this PKI is composed of the components described below and supports the following services:

- Generation of RCA key: OA on behalf of Albanian Ministry of Internal Affairs operates the RCA and generates the RCA keys in the OA trust center during the operation called “Key ceremony”;

- Generation of RCA certificate: OA on behalf of Albanian Ministry of Internal Affairs operates the RCA and generates the RCA certificate in the OA trust center during an operation called “Key ceremony”;

- Authentication of CA: Aleat collects and verifies each CA identity and information that will be included in the public key certificate to be delivered. This service is supported by PMA that is hosted and managed by Albanian Ministry;

- Generation of CA certificate: the RCA certifies the CA and generates a CA digital certificate according to the RCA CPS. This operation is performed by the RCA in the OA trust center;

- Revocation of CA certificate: when the link between the CA and CA public key defined within the certificate delivered by the RCA is considered no longer valid, then the RCA revokes the CA certificate. This operation is performed by the RCA in the OA trust center;

- Renewal and Re-key of CA and RCA certificate: action of delivering a new certificate to the CA or RCA, renewing a CA or RCA certificate means creating a new certificate for the CA or the RCA with the same or different information (key, name …) as the previous one, Re-keying a certificate means creating a new certificate for the CA with a new public key. This operation is performed by the RCA in OA trust center;

- Publication services: the RCA certificate, all the CA certificates and corresponding ARL are published by the Publication Service (PS).

The RCA CPS gives the security requirements for all the described services and more details on the practices enforced by each entity participating to the RCA activities. As the RCA is hosted and operated in the Operational Authority (OA) trust center, the security policy of the OA is referenced in this CPS for the CP’s requirements covered by the operational procedures of the OA.

1.3.1. Aleat Policy Management Authority (PMA)

Aleat Sh.p.k. is the PMA.

The PMA defines and approves the RCA CPS and CA CPS. The PMA proceeds to the mapping of:

- The RCA CPS: the result of the mapping guarantees that the RCA operates in compliance with its CPS. The result of the compliance review is validated by the PMA;

- The CA CPS with the CA CPS: the result of the mapping guarantees that the CA operates in compliance with the CA CPS. The result of the compliance review is validated by the PMA;

- The Information Security Management System of the OA with ISO 27001 criteria: the result of the audit guarantee that the security policy of the OA is compliant with the security objective control of the ISO 27002 and the E-ID PKI is securely hosted and operated in compliance with the CPS and the security policy of the OA.

1.3.2. Root Certificate Authority (RCA)

Aleat on behalf of Albanian Ministry of Internal Affairs is RCA.

The RCA signs and revokes certificates for CA. In this CPS, when the term 'RCA' is used without reference to any component (RA, Publication Service…) it covers the overall deployed PKI, dealing with legal and business matters. The RCA supports the PKI services as described above. The RCA uses the publication service to publish the certificates and the ARL that it generates. The RCA operates its services according to the Root CA CPS. The RCA cannot start operation without prior approval of the PMA.

All the RCA operations are performed in the OA trust center. The RCA's key pair are also managed and protected in the OA trust center. The E-ID PKI platform (for RCA) is a dedicated computer using ID Nomic ID-CA and Safenet Luna G5 software and Safenet USB HSM.

1.3.3. Certification Authorities (CA)

Aleat manages the CA.

CA generates certificates for citizen or for technical needs of the OA. CA uses PS (Publication Service) to publish its certificates and the CRL it issues.

All the CA operations are performed in the OA trust center. The CA's key pair are also managed and protected in the OA trust center.
E-ID PKI platform (for CA) is a set of server using ID Nomic ID CA application software and Luna G5 HSM.

1.3.4. Operational Authority (OA)

Aleat is the OA for the E-ID PKI of the Albanian Ministry of Internal Affairs.

The Operational Authority (OA) is the entity which sets up and realizes all technical operations of E-ID PKI certificates life cycle management on behalf of the Albanian Ministry of Internal Affairs. This entity is responsible of the security of the cryptographic material (hardware security modules, key pair, activation data…) and the PKI application of the E-ID PKI and of the physical and logical infrastructure set up for the E-ID PKI.

Aleat elaborates its own security policy and emergency and recovery plan for the OA.

1.3.5. Publication Service (PS)

The PS is an entity that makes available information such as RCA CPS and ARL.

The PS is hosted and managed in the OA.

1.3.6. Other Participants

1.3.6.1. Relying Party (RP)

A Relying Party is an entity that relies on the validity of the binding of the CA's name to a public key. A Relying Party is responsible for deciding how to check the validity of a CA Certificate, at least by checking the appropriate certificate status information. A Relying Party may use information in the Certificate (such as Certificate Policy identifiers) to determine the suitability of the Certificate for a particular use.

1.4. Certificate Usage

1.4.1 Appropriate Certificate Uses

The Root CA is used to sign its X.509 RCA CA self signed certificate, X.509 CA certificate and ARL according the present CPS.

The Root CA certificate is used by a relying party to check and verify the identity of a CA.

1.4.1. Prohibited Certificate Uses

No other application (means different certificate format or different CA function) than the one stated in § **Error! Reference source not found.** and § **Error! Reference source not found.** above are covered by the RCA CPS. Albanian Ministry of Internal Affairs is not responsible for any other use that these stated in the RCA CPS

Certificates shall only be used in line with the applicable law, and in particular shall only be used to the extent permitted by applicable export or import laws. CA Certificates shall not be used for any functions except CA functions.

1.5. Policy Administration

1.5.1. Organization Administering the Document

The PMA is responsible for all aspects of this CPS.

1.5.2. Contact Person

The Certificate Policy Manager is responsible for the PMA

Aleat Sh.p.k.
Contact: Chief Operation Officer

Address: Rruga Xhanfize Keko, Tirana, Albania
Phone: +355 69 4050 500
Mail: security@aleat.com

1.5.3. Person Determining CPS Suitability for the Policy

The PMA approves the RCA and CPS and determines compliance of RCA and CA CPS. Entities will be required to attest to such compliance periodically as established by the PMA. Further, the PMA reserves the right to audit entity compliance as set in section 8 of the RCA CPS and in the contract between Albanian Ministry of Internal Affairs.

In each case, the determination of suitability shall be based on an independent compliance audit report and recommendations and/or by the PMA expert. See section 8 for definition of independent compliance auditor.

1.5.4. CPS Approval Procedure

The term CPS is defined in the Internet RFC 3647, X.509 Public Key Infrastructure Certificate Practices Framework as: "A statement of the practices, which a Certification Authority employs in issuing certificates". It is a comprehensive description of such details as the precise implementation of service offerings and detailed procedures of certificate life-cycle management. It shall be more detailed than the corresponding CPS described above.

The PMA approves and maintains the RCA and CA CPS.

The RCA and CA CPS, which are separate documents, are published where necessary by the PMA. The PMA approves the results of the review made by PMA experts or independent auditors on the RCA and CA CPS compliance with the RCA and CA CPS.

Amendments shall either be in the form of a new CPS (with a sum up of the modifications). The new version of CPS replaces automatically the previous one and becomes operational as soon as the PMA has established its agreement on the mapping result. A new version of CPS has to be still compliant with the present CPS to permit the RCA and CA to refer to this CPS and deliver certificates.

1.6. Definitions and Acronyms

1.6.1. Definitions

Activation data: Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a pass phrase, or a manually-held key share).

Administrative contact: the CA Entity representative that is authorized to act on behalf of the CA Entity for all interaction with the RCA (transmission of requests to the RA…).

Audit: Independent review and examination of system records and activities to assess the adequacy and effectiveness of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [ISO/IEC POSIX Security]

Authority Revocation List (ARL): A list digitally signed by a CA, and contains certificates identities that are no longer valid. The list contains the issuing CA identity, the date of issue and the revoked certificates serial numbers.

Availability: The property of being accessible and upon demand by an authorized entity [ISO/IEC 13335-1:2004].

Certificate: The public key of a citizen, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it [ISO/IEC 9594-8; ITU-T X.509].

CA-certificate: A certificate for one CA issued by another CA. [ISO/IEC 9594-8; ITU-T X.509]. In this context, the CA-certificates are RCA-certificate (self-signed certificate) and CA-certificate (sign by the RCA).

Certificate Policies (CP): 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. [ISO/IEC 9594-8; ITU-T X.509].

Certificate Request: A message transmitted to the RCA to have a CA-certificate delivered by the RCA.

Certification Practice Statement (CPS)
A statement of the practices that Albanian Ministry Of Internal Affairs (acting as a Certification Authority) employs in approving or rejecting Certificate Applications (issuance, management, renewal and revocation of certificates). [RFC 3647].

Certificate validity period: The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. [RFC 3280].

Citizen: Albanian person who is authorized to have a citizen identity card.

Certification Path: A chain of multiple certificates needed to validate a certificate containing the required public key. A certificate chain consists of a RCA-certificate, CA-certificate and the certificates signed by the CA.

Compromise: A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.

Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC 13335-1:2004].

CRL distribution point*:* A directory entry or other distribution source for CRLs (ARL); a CRL or ARL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs. [ISO/IEC 9594-8; ITU-T X.509].

Cryptographic modules: a set of software and hardware components that are used to operate private cryptographic key to enable cryptographic operations (signature, encryption, authentication, key generation …). When a cryptographic module stores private key it needs an activation data to activate the private key stored inside. For a CA, a cryptographic module is a Hardware Secure Module evaluated (FIPS or EAL) that is used to store and operate the CA private key.

Disaster Recovery Plan: A plan defined by a CA to recover its all or part of PKI services, after they've been destroyed following a disaster, in a delay define in the CPS.

Hash function: A function which maps string of bits to fixed-length strings of bits, satisfying the following two properties:

- It is computationally infeasible to find for a given output an input which maps to this output;
- It is computationally infeasible to find for a given input a second input which maps to the same output [ISO/IEC 10118-1].

Integrity: Refers to the correctness of information, of originator of the information, and the functioning of the system which processes it.

Interoperability: Implies that equipment and procedures in use by two or more entities are compatible, and hence that it is possible to undertake common or related activities.

Key Ceremony A procedure whereby a CA's or component's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.

Online Certificate Status Protocol (OCSP): A protocol for providing Relying Parties with real-time Certificate status information.

PKCS #10 Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.

Policy qualifier: Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate. [RFC 3647]

Private key: That key of an entity's asymmetric key pair which should only be used by that entity [ISO/IEC 9798-1].

Public key: That key of an entity's asymmetric key pair which can be made public. [ISO/IEC 9798-1]

Public Key Infrastructure (PKI): The infrastructure needed to generate, distribute, manage and archive keys, certificates and certificate-revocation lists and the repository to which certificates and CRLs are to be posted. [2nd DIS ISO/IEC 11770-3 (08/1997)]

Publication Services: Cf. § 1.3.5.

Relying Party: Cf. § 1.3.6.1.

RSA: A public key cryptographic system invented by Rivest, Shamir, and Adelman.

Root Certificate Authority (RCA): Cf. § 1.3.2.

Secure Socket Layer (SSL): The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and optional client authentication for a Transmission Control Protocol/Internet Protocol connection.

Security policy: The set of rules laid down by the security authority governing the use and provision of security services and facilities. In this context, the security policy will be set up by the OA which host and operate E-ID PKI.

Self-signed certificate: A certificate for one CA signed by that CA.

Token: The hardware device used to transport keys to an entity and which can protect those keys in operation [ISO/IEC 9798-1 (2nd edition): 1997].

Trustworthy System: Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a “trusted system” as recognized in classified government nomenclature.

Time stamping services: A service that provides a digitally signed assertion (a Digital Receipt) that a particular document or set of data existed at a particular point in time. Time Stamping Service: A service that provides a trusted association between a datum and a particular point in time, in order to establish reliable evidence indicating the time at which the datum existed.

1.6.2. Acronyms

ANSI: The American National Standards Institute;
ARL: Authority Revocation List;
CC: Common Criteria (ISO 15408 standard)
CPS: Certification Practice Statement;
CRL: Certificate Revocation List;
DN: Distinguished Name;
EAL: Evaluation assurance level (pursuant to the Common Criteria);
FIPS: United State Federal Information Processing Standards;
HTTP: Hypertext Transport Protocol;
IP: Internet Protocol;
ISO: International Organisation for Standardization;
PMA: Aleat Management Authority;
KTS: Aleat Trust Center;
LDAP: Lightweight Directory Access Protocol;
LRA : Local Registration Authority
OA: Operational Authority
OCSP: Online Certificate Status Protocol;
OID: Object Identifier;
PIN: Personal identification number;
PKCS: Public-Key Cryptography Standard;
PKI: Public Key Infrastructure;
PS: Publication Service;

RA: Registration Authority;
RCA: Root Certification Authority;
RFC: Request for comment;
RP: Relying Party
RSA: Rivest, Shamir, Adleman (Public-Key Cryptosystem);
SHA: Secure Hash Algorithm (US Standard);
CA: Certificate Authority that delivers end user certificate to citizen and to system;
SSL: Secure Socket Layer;
URL: Uniform Resource Locator.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

The OA operates a repository (PS) to make available the information defined below to relying parties.

2.2. Publication of Certificate Information

The OA ensure that the terms and conditions of the CPS as necessary (for instance on a need to know basis), and certificates are made available to citizen and relying parties by their PS. OA makes available the following information through its PS:

- Root CA CPS: https://www.aleat.al/pdf/cps-citizen-root-ca.pdf;
- RCA certificate: https://www.aleat.al/csp/albanian-citizen-id-root-ca-04.cer;
- CA Certificate status (ARL): https://www.aleat.al/csp/albanian-citizen-id-root-ca-04.crl;

These information are available through a durable means of communication and in readily understandable language.

2.3. Time or Frequency of Publication

The information identified above at § 2.2 are available:

- Before service starts for initial RCA CPS, no later than 48 hours after Root CA CPS update is approved by the PMA for any RCA CPS update;
- Before service starts for initial CA CPS, no later than 48 hours after CA CPS update is approved by the PMA for any CA CPS update;
- Before service starts for Root CA certificate and CA certificates;
- No later than 24 hours after generation for CA Certificate status (ARL);
- Before service starts for initial CA certificates, no later than 48 hours after generation for CA certificate renewal or re-key;
- No later than 24 hours after generation for Certificate status (CRL …) of the certificates issued by CA.

2.4. Access Controls on Repositories

The PS ensures that the information is made available and protected in integrity and authenticity from unauthorised modification. Information is publicly and internationally available through the Internet.

OA ensure that the PS is accessible for:

- Writing only for internal authorized trusted roles;
- Reading and downloading for external users.

The mechanisms and procedures are described in the OA's security policy.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Type of Names

RCA and CA have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate subject name field and in accordance with RFC 3280. The CPS gives all the details for the identity given to the RCA and for a CA.

3.1.1.1. RCA

The DN of the RCA certificate is:

Base certificate	Value
Issuer DN	C = AL OI=NTRAL-K82018015V O = Aleat CN = Albanian Citizen ID Root CA
Subject DN	C = AL OI=NTRAL-K82018015V O = Aleat CN = Albanian Citizen ID Root CA

3.1.1.2. CA

The DN of the CA certificate is:

Base certificate	Value
Issuer DN	C = AL OI=NTRAL-K82018015V O = Aleat CN = Albanian Citizen ID Root CA
Subject DN	Described in CA CPS.

3.1.2. Need for Names to be Meaningful

The certificates issued pursuant to this CPS are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person or object to which they are assigned in a meaningful way.

3.1.3. Anonymity or pseudonym of Subscribers

The identity used for the RCA and CA certificates is not a pseudonym or an anonymous name.

3.1.4. Rules for Interpreting Various Name Forms

Rules for interpreting name forms are self contained in the applicable certificate profile as defined in § 3.1.1 and 7.1.

3.1.5. Uniqueness of Names

The RCA and CA identity (refer to § 3.1.1) is unique for all certificates generated by the RCA. The PMA ensures this uniqueness through its registration process (refer to § 3.2.2).

3.1.6. Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2. Initial Identity Validation

3.2.1. Method to Prove Possession of Private Key

Key ceremonies for RCA and CA certificate generation are preceded in OA trust center under the control of OA's and Albanian Ministry of Internal Affair's trusted roles, according to [2016_2000021244 - Citizen PKI - Key Ceremony 2016 v0.3]. During the initial key ceremony, activation data holders (refer to § 6.1.1 below)receive their activation data, such that the RCA and CA private key is under the control of activation data holders.

The key ceremony is authorized by the PMA and realized according to creation document, called [2016-2000021870 - Naming Document - Citizen PKI V0.3] issued by the PMA's administrative contact. This naming document defines the identity of the PMA (refer to § 3.1.1.1).

3.2.2. Authentication of Organization identity

Organizations acting on behalf of PMA are appointed by the Albanian Ministry of Internal Affairs. The PMA is the primary organization to be appointed, the PMA then assigns all other entities acting on behalf of RCA and CA.

Organization acting on behalf of RCA and CA are the following:

- RCA : Aleat on behalf of Albanian Ministry of Internal Affairs
- CA: Aleat;
- PMA: Aleat on behalf of Albanian Ministry of Internal Affairs
- OA: Aleat.

3.2.3. Authentication of Individual identity

3.2.3.1. IDEMIA Identity & Security

The Administrative contact is authenticated by IDEMIA Identity & Security and OA.

3.2.3.2. RCA and CA

Evidence of the Individual identity, for persons who work in PMA is checked against a physical person. Each person has to sign a form (refer to § Annex 2: description of trusted roles below) regarding the trusted roles that individual person may own within the PMA.

3.2.3.3. OA

Evidence of the Individual identity, for persons who work in OA is checked against a physical person. Each person has to sign a form (refer to § OA roles below) regarding the trusted roles that individual person may own within the OA.

Authentication and trusted roles assignment is performed following rules that are:

- Security Officer: the chief executive officer of the OA authenticates and authorizes a person to own the trusted role Security Officer. Each Security Officer signs a form (refer to § ANNEX 1: trusted roles forms below). This form is also signed by the chief executive officer of the OA. Security Officer belongs to the OA;

- E-ID PKI Administrator: the Security Officer authenticates and authorizes a person to own the trusted role E-ID PKI Administrator. Each E-ID PKI Administrator signs a form (refer to § Authorization form below). This form is also signed by the Security Officer of the OA. E-ID PKI Administrator belongs to the OA;

- System Administrator: the Security Officer authenticates and authorizes a person to own the trusted role System Administrator. Each System Administrator signs a form (refer to § Authorization form below). This form is also signed by the Security Officer of the OA. System Administrator belongs to the OA;

- E-ID PKI Operator: the E-ID PKI Administrator authenticates and authorizes a person to own the trusted role E-ID PKI Operator. Each E-ID PKI Operator signs a form (refer to § Authorization form below). This form is also signed by the E-ID PKI Administrator of the OA. E-ID PKI Operator belongs to the OA;

- Personalization Operator: the E-ID PKI Administrator authenticates and authorizes a person to own the trusted role Personalization Operator. Each Personalization Operator signs a form (refer to § ANNEX 1: trusted roles forms below). This form is also signed by the E-ID PKI Administrator of the OA. Personalization Operator belongs to the OA.

Once he receives the authorization for a person to own a trusted role, the Security Officer or the E-ID PKI Administrator (depending of the certificate to generate cf. Annex2) authenticates the person who is cleared to own the trusted role during a face to face meeting to deliver him/her a technical certificate (refer to § ANNEX 1: trusted roles forms 10 below).

3.2.4. Non-Verified Subscriber information

Information that is not verified is not included in Certificates.

3.2.5. Validation of Authority

PMA mandates and authorizes OA to generate RCA and CA certificates, under the control of PMA, with the identity and in the name of the Aleat.

PMA and OA are the authority for all the E-ID PKI trusted roles (refer to § 3.2.3.2 and 3.2.3.3 above).

3.2.6. Criteria for Interoperation

Certificate delivered by E-ID PKI are managed according to the rules and requirements stated by the PMA.

3.3. Identification and Authentication for Re-key Requests

3.3.1. Identification and Authentication for Routine Re-key

A request for re-key may only be made by the organization in whose name the keys have been issued. The CA and RCA identify itself using the initial identity-proving process as described above. At each re-key request the identity of a CA, identified as required in § 3.2, is re-established through the initial registration process.

3.3.2. Identification and Authentication for Re-key After Revocation

After the RCA or a CA has been revoked other than during a renewal or update action, the CA and RCA is required to go through the initial registration process described in § 3.2 to obtain a new certificate.

If the RCA or CA has been revoked for key compromise, then the RCA or CA cannot use the revoked key to be certified again and needs the agreement of the organisation it belongs to generate a new key pair and be issued a new certificate.

3.4. Identification and Authentication for Revocation Request

RCA and CA revocation requests are authenticated by the PMA. The authentication procedure requires to go through the initial registration process (See § 3.2.2 and 3.2.3).

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Origin of a certificate request

PMA authorizes the creation of the initial RCA and CA certificate signing a [2016-2000021870 - Naming Document - Citizen PKI V0.3.docx] prepared by IDEMIA Identity & Security. IDEMIA Identity & Security gives the [2016-2000021870 - Naming Document - Citizen PKI V0.3.docx] to the Administrative contact. Following RCA and CA certificate requests, in case of RCA and CA certificate change or renewal, are authorized by the PMA using a [2016-2000021870 - Naming Document - Citizen PKI V0.3].

4.1.2. Enrolment Process and Responsibilities

Prior to the RCA and CA certificate initial creation, the PMA's administrative contact transmits the [2016-2000021870 - Naming Document - Citizen PKI V0.3] to the Master of Key Ceremony of IDEMIA Identity & Security. Master of key ceremony authenticates the administrative contact (refer to § 1.5.2**Error! Reference source not found.** above).

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

Cf. § 4.1.

4.2.2. Approval or Rejection of Certificate Applications

In case the [2016-2000021870 - Naming Document - Citizen PKI V0.3.docx] (refer to § 4.1 above) is complete and accepted by PMA, then PMA approves the RCA and CA certificate generation.

4.2.3. Time to Process Certificate Applications

No stipulation.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

RCA and CA certificates are created during key ceremonies (refer to § 6.1.1**Error! Reference source not found.**). PMA verifies that the RCA and CA generated certificate are compliant with [2016-2000021870 - Naming Document - Citizen PKI V0.3].

4.3.2. Notifications to Subscriber by the CA of Issuance of Certificate

PMA notifies Ministry of Internal Affairs of certificate issuance.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

Notification of RCA and CA certificate issuance to the Albanian Ministry of Internal Affairs means acceptance of the RCA certificate and CA certificate by Albanian Ministry of Internal Affairs.

Once the RCA and CA certificate acceptance has been received by the PMA, the CA may start delivery of certificates to citizen.

4.4.2. Publication of the Certificate by the CA

The PMA uses PS for the publication of its certificate (refer to § 2.2). The Security Officer gives the certificate to the System Administrator. System Administrator set RCA and CA certificates are set in the PS server.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5. Key Pair and Certificate Usage

4.5.1. CA Private Key and Certificate Usage

The Root CA key pair is used to sign CA certificates, ARL and its own self-signed certificate.

4.5.2. Relying Party Public Key and Certificate Usage

Relying parties use the trusted certification path and associated public keys for the purposes constrained in the certificates extensions (such as key usage, extended key usage, certificate policies, etc.) and to authenticate the trusted common identity of the services according to the RCA and the CPS supported by the CA.

4.6. Certificate Renewal with Same Keys

This section addresses RCA and CA certificate generation without changing the public key or any other information in the certificate. Only the validity period and the serial number of the certificate are changed.

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised and the RCA or CA name and attributes are unchanged. This operation is possible only if the key re-used in the certificate is still compliant with cryptographic security recommendation for key size length issued by national bodies or international standard institutes.

The validity period of the new certificate cannot exceed the remaining lifetime of the private key, as specified in § 5.6. The PMA proceeds to the check of the existence and validity status of the

certificate to be renewed and authenticates organizations and individuals using the process described in § 3.2.2 and 3.2.3.

For further RCA and/or CA, the PMA authorizes the creation of the RCA and/or CA certificate signing a [2016-2000021870 - Naming Document - Citizen PKI V0.3] prepared by PMA's Administrative contact. PMA gives the [2016-2000021870 - Naming Document - Citizen PKI V0.3] to the Administrative contact. PMA decides who makes the Key Ceremony.

Prior to the RCA and/or certificate creation, the PMA's Administrative contact transmits the [2016-2000021870 - Naming Document - Citizen PKI V0.3] to the Master of Key Ceremony of the OA which proceed the key ceremony operation. OA authenticates the administrative contact.

RCA and/or CA certificates are created during key ceremonies (refer to § 6.1.1).

4.7. Certificate with Different Keys

This section addresses RCA or CA certificate generation changing the RCA or CA key pair.

The procedures that apply are the same than the ones for initial certificate generation keeping the same identity for the CA as defined and used in the previous CA certificate delivered by the RCA.

For further RCA and/or CA, the PMA authorizes the creation of the RCA and/or CA certificate signing a [2016-2000021870 - Naming Document - Citizen PKI V0.3] prepared by PMA's Administrative contact. PMA gives the [2016-2000021870 - Naming Document - Citizen PKI V0.3] to the Administrative contact. PMA decides who makes the Key Ceremony.

Prior to the RCA and/or certificate creation, the PMA's Administrative contact transmits the [2016-2000021870 - Naming Document - Citizen PKI V0.3] to the Master of Key Ceremony of the OA which proceed the key ceremony operation. OA authenticates the administrative contact.

RCA and/or CA certificates are created during key ceremonies (refer to § 6.1.1**Error! Reference source not found.**).

4.8. Certificate Modification with Same Keys

This section addresses CA certificate generation of a new certificate keeping the same key pair. This operation is possible only if the key re-used in the certificate is still compliant with cryptographic security recommendation for key size length issued by national bodies or international standard institutes and has not been compromised.

Changing a CA or RCA name is a possible circumstance for certificate modification.

For further RCA and/or CA, the PMA authorizes the creation of the RCA and/or CA certificate signing a [2016-2000021870 - Naming Document - Citizen PKI V0.3] prepared by PMA's Administrative contact. PMA gives the [2016-2000021870 - Naming Document - Citizen PKI V0.3] to the Administrative contact. PMA decides who makes the Key Ceremony.

Prior to the RCA and/or certificate creation, the PMA's Administrative contact transmits the [2016-2000021870 - Naming Document - Citizen PKI V0.3] to the Master of Key Ceremony of the OA which proceed the key ceremony operation. OA authenticates the administrative contact.

RCA and/or CA certificates are created during key ceremonies (refer to §6.1.1).

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

4.9.1.1. RCA

A RCA certificate is revoked when the binding between the certificate and the public key it contains is considered no longer valid. Examples of circumstances that invalidate this binding are:

- The private key is suspected of compromise;
- The private is compromised;
- The RCA can be shown to have violated the stipulations of the present CPS;
- End of the RCA services;
- Privilege attributes asserted in the RCA certificate are reduced;
- Change in the key length size recommendation coming from national agencies or international standard institute;

Whenever any of the above circumstances occurs, the associated certificate shall be revoked and placed in the ARL.

In case of Albanian Citizen ID Root CA compromission, PMA will trigger the following steps:

- Stop generation of Auth and Sign certificates
- Communication with Ministry of Internal Affairs
- Root CA is revoked and all sub CAs are revoked as well as all Auth and Sign citizen certificates generated with those sub CAs
- Schedule and run a new key ceremony for a new Root CA and all sub CA
- Communication to all citizen having those revoked sign and auth certificates
- Update of this CPS and publication of the new CPS
- Publication of new CRLs
- Update of OCSP responder
- Restart the generation of citizen auth and sign certificates with the new Sub CAs

4.9.1.2. CA

A CA certificate is revoked when the binding between the certificate and the public key it contains is considered no longer valid. Examples of circumstances that invalidate the binding are:

- The RCA is revoked.
- The private key is suspected of compromise or is compromised;
- The CA can be shown to have violated the stipulations of the present CPS;
- The CA can be shown to have violated the stipulations of the CA CPS;
- The CA can be shown to have violated the stipulations of its agreement with Albanian Ministry of Internal Affairs;
- End of the CA services;
- Privilege attributes asserted in the CA's certificate are reduced;

- Change in the key length size recommendation coming from national agencies or international standard institute;

Whenever any of the above circumstances occurs, the associated certificate shall be revoked and placed in the ARL.

In case of Albanian Citizen ID CA compromission, PMA will trigger the following steps:
- Stop generation of CA citizen certificates
- Communication with Ministry of Internal Affairs
- Sub CA is revoked and all the ceitizen certificates generated with this CA
- Schedule and run a new key ceremony for a new Sub CA
- Communication to all citizen having those revoked certificates
- Update of the CA CPS and publication of the new CA CPS
- Publication of new CRLs
- Update of OCSP responder
- Restart the generation of citizen certificates with the new CA

4.9.2. Origin of Revocation Request

It is the responsibility of the PMA to propose the revocation of a RCA to the Albanian Ministry of Internal Affairs.

4.9.3. Procedure for Revocation Request

Once the Albanian Ministry of Internal Affairs receives the RCA or CA certificate revocation request from the PMA, it reviews the request.

Once the RCA certificate revocation request is approved by the Albanian Ministry of Internal Affairs, the PMA uses the RCA to revoke:

- All the CA certificate if it is a RCA revocation;
- The CA certificate if it is a CA to revoke.

PMA authorizes the revocation of the RCA and/or CA certificate signing a [2016-2000021870 - Naming Document - Citizen PKI V0.3 prepared by PMA's Administrative contact. PMA gives the [2016-2000021870 - Naming Document - Citizen PKI V0.3] to the Administrative contact. The Key Ceremony of revocation is performed in the OA trust center. The required activation holder has to be present to activate the RCA private key (Cf. § 6.2.8).

4.9.4. Revocation Request Grace Period

There is no revocation grace period. Responsible parties must request revocation as soon as they identify the need for revocation.

4.9.5. Time within Which CA Must Process the Revocation Request

Upon system failure, service or other factors, which are not under the control of the RCA, the RCA makes best endeavours to ensure that this service is not unavailable for longer than a maximum

period of time as denoted in the OA security policy. The RCA shall process a revocation request as soon as practical after receiving the revocation request and preferably immediately.

4.9.6. Revocation Checking Requirements for Relying Parties

Use of revoked certificates could have damaging or catastrophic consequences in certain applications for a relying party. The matter of how often new revocation data should be obtained is a determination to be made by relying parties. If it is temporarily infeasible to obtain revocation information, then the relying parties either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate, i.e. certification path provided according to the CPS.

4.9.7. ARL Issuance Frequency

ARL are issued every year with a publication every 6 months. They are rendered available 24 hours per day, 7 days a week, by the PS.

Security Officer and System Administrator ensure that superseded ARLs are removed from the repository of PS upon posting of the latest ARL.

4.9.8. Maximum Latency for ARLs

The maximum delay between the time a CA certificate is revoked by the RCA and the time when revocation information is available to relying parties is no longer than 24 hours.

4.9.9. On-Line Revocation/Status Checking Availability

No stipulation.

4.9.10. On-Line Revocation Checking Requirements

No stipulation.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements regarding Key Compromise

There are no more specific requirements than those specified in section 4.9.3.

4.9.13. Circumstances for Suspension

Not applicable.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

The information status is available through the PS as described in section 2.

4.10.2. Service Availability

The PS availability is described in section 2.3.

4.10.3. Optional Features

No stipulation.

4.11. End of Subscription

RCA and CA certificates that have expired prior to or upon end of subscription are not required to be revoked.

Where the PMA ends its relationship with OA, then the OA transfer all material and files related to the E-ID PKI infrastructure to an entity appointed by the PMA.

4.12. Key Escrow and Recovery

Under no circumstances the RCA or a CA key is escrowed by a third-party or any else other entity.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical Controls

The RCA physical and environmental security policy for systems concerned with certificate generation, RCA cryptographic module operation and revocation management services address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery. Controls are implemented to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities and protection against equipment, information, media and software being taken off-site without authorization.

5.1.1. Site Location and Construction

Security Officer chooses a location for the key ceremony, named key ceremony room, inside the OA that full fill the following requirements:

- This area is a dedicated room with only door for the access, no windows,
- There is no telephone in the room,
- There is no communication network (to connect the key ceremony computer in the room),
- The sole authorized wirings are the power supply cable.

5.1.2. Physical Access

Access to the key ceremony room is under the control of the Security Officer.

5.1.3. Power and Air Conditioning

OA ensures that power and air conditioning facilities are sufficient to support the operation of the E-ID PKI and personalization platform, using primary and back up installations according to its security policy.

5.1.4. Water Exposures

OA ensures that E-ID PKI and personalization platform are protected in a way that minimizes from water exposure consequences according to its security policy.

5.1.5. Fire Prevention and Protection

OA ensures that E-ID PKI and personalization platform are protected with fire detection and suppression systems according to its security policy.

5.1.6. Media Storage

Media used within OA are securely handled to protect media from damage, theft and unauthorized access. Media are under the responsibility of OA. A trusted role has to protect all the media that contains sensitive data under his/her responsibility. Trusted role that has smart car has to

store it in a secure place (safe, closed location …) and never give it to other person. Media storage in OA is managed according OA security policy.

When it's not used, the RCA's dedicated computer is stored in a locked location in the OA.

All the components are identified in a list. The list contains the inventory of all the server, computer, smart card … that are distribute or available in OA. The list is under the responsibility of the system administrator. When a component is distribute to a trusted role or set in production in the OA trust center, then a component distribution form is signed by the System administrator and by the holder of the component (if it is required).

The component distribution form contains the following information:

- Type of component (computer, smart card, server, firewall, …),
- The reason of the distribution of the component (set in production or give to a trusted role),
- Name and first name of the system administrator,
- Software deployed on the component (for server only),
- Name and first name of the person who receive the component,
- Signature of the trusted role (if it is required),
- Signature of the System administrator,
- Date.

5.1.7. Waste Disposal

All media used for the storage of sensitive information such as keys, activation data or files shall be destroyed before released for disposal according OA security policy.

Before released for disposal:

- Computer: the computer is formatted with logical function provided by the Operating system. Then, the hard disk, the processor and the electronic component has to be physically destroyed;

- HSM: all the data are deleted using the logical function provided with the HSM software. Then the HSM is physically destroyed;

- USB token: connect the USB key to a computer of Security officer OA, all the data of the USB key are destroyed with a dedicated software developed to securely delete data files. Then, the USB key is broken and the chip or electronic micro-circuit is also broken and taken off from the USB key ;

- HSM back-up: connect the HSM Backup to the key ceremony computer, all the data of the MSM backup key are destroyed with a dedicated software developed to securely delete data in HSM Backup devices.

A destruction operation is always under the control of Security Officer and System administrator. When a component has to be destroyed, the responsible of the component sign a destruction request form and transmit it to the Security Officer. The form indicates:

- The type of component,
- The identification of the component,

- The reason of the destruction,
- The name and first name of the System administrator responsible of the destruction,
- The name and first name of the holder of the component (only for trusted roles),
- The name and the first name of the Security Officer,
- Date,
- Signature of the trusted role (if required),
- Signature of the System administrator,
- Signature of the Security Officer.

5.1.8. Off-Site Backup

The back-up is composed of the following data:

- Back-up of the private key of the RCA, CA, to distribute to the Security Officer on a Backup HSM;
- Back-up of the certificate of the RCA, CA, to distribute to the Security Officer on a CD Rom;
- Back-up of the E-ID PKI software and associated platform configuration;
- Back-up of USB token's PIN code distribute to the Security Officer in temper evident envelop.

Al those following data are in a safe at OA back up site under the control of a Security Officer according OA security policy. The tests are done during the training period according the OA emergency and recovery plan.

5.2. Procedural Controls

5.2.1. Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The functions performed in these roles form the basis of trust for all uses of the RCA.

Trusted roles include roles that involve the following responsibilities:

Role	Description ETSI EN 319 411 (ETSI EN 319 401 and CEN TS 419 261)
Security Officer	Overall responsibility for administering the implementation of the security practices. Additionally approve the generation/revocation/suspension of Certificates.
System Administrator	Authorized to install, configure and maintain the CA trustworthy systems for registration, certificate generation, subscriber device provision and revocation management.
System Operator	Responsible for operating the CA trustworthy systems on a day to day basis. Authorized to perform system backup and recovery.
System Auditor	Authorized to view and maintain archives and audit logs of the CA trustworthy system.
CA Activation Data Holder	Authorized person to have a CA activation data that is necessary for cryptographic module operation.
Card Stock Manager	Subscriber device provision (Card stock and order management); Person which manage the Cryptographic tokens (Blank ID Cards).

Revocation Officer	Responsible for operating certificate status changes;
Registration Officer	Responsible for verifying information that is necessary for certificate issuance and approval of certification requests

All personnel are formally appointed to trusted roles by PMA. The annex 11.1 gives more details about the function and the tools used by the trusted role.

5.2.2. Number of Persons Required per Task

The number of persons required per tasks is given in each procedure as stated in the present CPS, by indicating the required trusted roles for the operation. The number of required persons for any sensitive operation (certificate generation, activation …) is not less than 2 persons (Cf. section 6.2).

5.2.3. Identification and Authentication for Each Role

Identification and authentication of a all person involved during key ceremony is done by OA employee according to Section 3.2.3 above.

OA ensures effective administration of users in compliance with ISO 27001 policies and procedures. The administration includes user account management, periodic reviews and audit, and timely modification or removal of access.

The identification and authentication of the person who have privileges on Luna G5 HSMs is assimilated to the possession of a physical item (USB token and corresponding PIN code). These items are required to set up functionality on HSMs. Only cleared person can enter the key ceremony room to activate the Luna G5 HSM that contained the RCA and CA private key.

The list of person cleared to access OA security perimeter and associated access rights is available in the document OA information system security policy.

5.2.4. Roles Requiring Separation of Duties

A person can only have one trusted role as described in Annex 3. No individual shall be assigned more than one identity.

5.3. Personnel Controls

5.3.1. Qualifications, Experience, and Clearance Requirements

RCA employs a sufficient number of personnel which possess the expert knowledge, experience and qualifications necessary for the offered services and appropriate for the job function. RCA personnel fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in the OA security policy, are documented in job descriptions and clearly identified. RCA personnel (both temporary and permanent) have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity

based on the duties and access levels, background screening and employee training and awareness. RCA personnel shall be formally appointed to trusted roles by senior management responsible for security.

The job descriptions include skills and experience requirements. Managerial personnel who are employed possess experience or training in electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

OA manages qualifications, experience and clearance requirements through ISO 27001 policy and procedure.

5.3.2. Background Check Procedures

All RCA personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the RCA operations. The RCA shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position. Personnel shall not have access to the trusted functions until any necessary checks are completed. RCA asks the candidate to provide past convictions and turn down an application in case of refusal. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation.

Background check procedures are performed according OA security policy and by PMA.

5.3.3. Training Requirements

OA ensures that all personnel performing duties with respect to the operation receive comprehensive training in:

- OA security principles and mechanisms;
- Software versions in use in the E-ID PKI and personalization platform;
- Duties they are expected to perform;
- Disaster recovery and business continuity procedures.

5.3.4. Retraining Frequency and Requirements

Individuals responsible for trusted roles shall be aware of changes in the RCA operations, as applicable. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented.

5.3.5. Job Rotation Frequency and Sequence

RCA ensures that any change in the staff will not affect the operational effectiveness of the service or security of the system.

5.3.6. Sanctions for Unauthorized Actions

Appropriate disciplinary sanctions are applied to personnel violating CPS.

5.3.7. Independent Contractor Requirements

Contractor personnel employed have to perform RCA functions operations according to the same requirements as defined in section 3.

5.3.8. Documentation Supplied to Personnel

Security Officer makes available to its personnel the CPS, and any relevant statutes, policies or contracts. Other technical, operations, and administrative documents (e.g., Administrator Manual, User Manual, etc.) are provided in order for the trusted personnel to perform their duties.
Documentation shall be maintained identifying all personnel who received training and the level of training completed.

5.4. Audit Logging Procedures

5.4.1. Types of Events Recorded

For a key ceremony the logs include, but are not limited to, the following events:

- Physical access to the key ceremony room: Log by access system control. Security Officer register (id badge, name, first name and date) in log book the distribution of badge that allow access to the trust center;
- Signed : PMA's administrative contact retains this document;
- CD Rom with Keyseed logs;
- List, established by Security Officer, of all the attendees to the key ceremony.

IDEMIA Identity & Security and/or PMA have the key ceremony script used to generate RCA and or CA.

5.4.2. Frequency of Processing Log

Audit logs are reviewed periodically for a reasonable search for any evidence of malicious activity and following each important operation. According OA security policy, audit logs are collected each 3 months.

5.4.3. Retention Period for Audit Log

Records concerning RCA and CA certificates are held for a period of time appropriate for providing necessary legal evidence in accordance with applicable legislation. The records could be needed at least as long as a transaction relying on a valid certificate can be questioned.
The audit logs are retained during 15 years.

5.4.4. Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

When the log data of the component and software are stored on a CDROM, they are place in a safe under the control of the System administrator and/or Security Officer.

The log book of the System administrator and Security Officer are always in OA trust center in a safe.

5.4.5. Audit Log Backup Procedures

Back-up audit logs (Cf. § 5.1.8) are backed-up in a secure location (System Administrator's and Security Officer's safe), under the control of authorized trusted role, separated from their component source generation. Audit logs backup are protected with the same level of trust defined for the original logs.

5.4.6. Audit Collection System

The System administrator collects the log data directly on the computer.

5.4.7. Notification to Event-Causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

System administrator verify at minimum in the log that:

- Only authorized trusted roles are contained in the software log;
- Only authorized used are contained in the software and computer log.

When, there are suspected information in log, the System administrator try to solve the reason and alert the Security Officer.

OA security policy defines complementary action in audit analysis.

5.5. Records Archival

5.5.1. Types of Records Archived

At a minimum, the following data shall be archived:

- All the back-up log collected by the System administrator (refer to § 5.1.8): System Administrator safe;
- All the back-up log and data collected by the Security Officer (refer to § 5.1.8): Security officer safe;
- The Security Officer log book: Security officer safe;
- The System Administrator log book: System Administrator safe;
- CPS document: PMA and OA;
- Any contractual agreements between PMA and OA: OA and PMA;
- Any contractual with supplier which provides services and software for E-ID PKI and personalization platform: PMA;
- Server, computer and firewall equipment configuration: System Administrator safe;
- E-ID PKI and personalization software configuration: System Administrator safe;
- RCA and CA Certificates, ARL: PMA and Security Officer safe on CD Rom;
- All the trusted role created with their certificate: E-ID PKI software in OA trust center;

- All the used forms: Security Officer;
- Other data or applications sufficient to verify archive contents: System Administrator;
- All work related to or from the PMA and compliance auditors: PMA and OA.

5.5.2. Retention Period for Archive

The minimum retention period for archive data is 10 years after the event occurred. The signed application forms are stored in Aleat central site premises in the archived room.

5.5.3. Protection of Archive

The archives are created in a way that they cannot be deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held. Archive protections ensure that only authorized trusted access can make operation regarding their profile role without modifying integrity, authenticity and confidentiality of the data. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media is defined by the OA.

5.5.4. Archive Backup Procedures

OA incrementally backs up electronic archives of its issued Certificate information on a daily basis and performs full backups on a weekly basis. Paper-based records shall be maintained in archive room secure facility

If it is necessary, to keep the data readable, the:

- Log book can be photocopied and signed again by the required trusted role;
- CDROM can be copied on another media (same or different).

5.5.5. Requirements for Time-Stamping of Records

For key ceremony, the security officer verifies that the time used for computer is correct.

5.5.6. Archive Collection System (Internal or External)

The archive collection system respects the security requirements defined in § 5.4.

5.5.7. Procedures to Obtain and Verify Archive Information

Only authorized OA equipment, trusted role and other authorized person (legal person …) are allowed to access the archive. Access to archive information is requested to the PMA and OA according OA security policy and agreement between OA and PMA. The integrity of information is verified when it is restored.

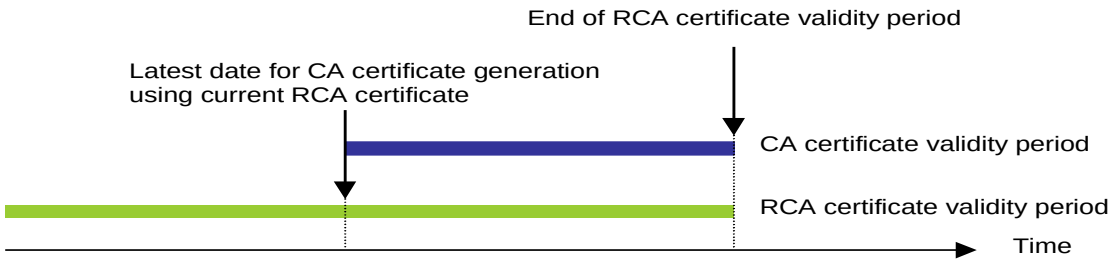
5.6. Key Changeover

5.6.1. RCA

The RCA maintains its private key operational period compliant with the cryptographic recommendation for key size length issued by national bodies or international standard institutes.

The PMA reserves its right to take decision to change the RCA key pair at any time. In this case the CA Entities will be informed.

As the RCA cannot generate CA certificates whose validity period would be superior to the RCA certificate validity period, the RCA is re-keyed at the latest the duration period of CA certificates before the end of the RCA certificate validity period, such as illustrated on the following diagram:



As soon as a new RCA key pair is generated, only this new key can be used to sign CA certificate and associated ARL.
The previous RCA certificate stay valid for validation process of certification path until all CA certificates signed using the previous RCA key pair are expired.
When a new RCA key pair and certificate has to be created, then the following operation has to be done:

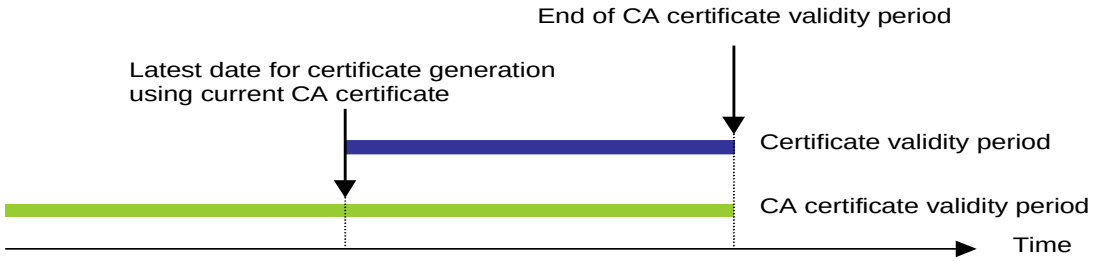
- A key ceremony is done to create the new RCA key pair and the associated self-signed certificate as listed in [2016_2000021244 - Citizen PKI - Key Ceremony 2016 v0.3.docx] (Cf. § 6.1);
- The new keys are backed-up on Backup HSM (Cf. § 6.2.4);
- The old privates keys are destroyed (Cf. § 6.2.10);
- The new RCA and CA privates keys are inserted in the E-ID PKI's HSM platform (Cf. § 6.2.6).

For these operations it is necessary to have the required trusted roles with the right activation data (Cf. Annex 2 and § 6.2.6, § 6.2.4 and § 6.2.10).

5.6.2. CA

The CA maintains its private key operational period compliant with the cryptographic recommendation for key size length issued by national bodies or international standard institutes.

As the CA cannot generate certificates whose validity period would be superior to the CA certificate validity period, the CA is re-keyed at the latest the duration period of the certificates it issues before the end of its certificate validity period, such as illustrated on the following diagram:



As soon as a new CA key pair is generated, only this new key can be used to sign certificate and associated CRL.
The previous CA certificate stay valid for validation process of certification path until all issued certificates signed using the previous CA key pair are expired.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling Procedures

OA has established business continuity procedures (emergency and recovery plan of the OA), for the E-ID PKI that outlines the steps to be taken in the event of the corruption or loss of computing resources, software and/or data that could disturb or compromise the RCA services. OA carries out a risk assessment to evaluate business risks and determines the necessary security requirements and operational procedures and elaborates in consequences its disaster recovery plan. This risk analysis is regularly reviewed and revised if necessary (threat evolution, vulnerability evolution …).

OA personnel that have trusted role and/or operation role are specially trained to operate according to procedure defined in the OA disaster recovery plan for the most sensitive activities.

The integrity of CA systems is protected against virus, malicious and unauthorized software in compliance with ISO 27001 security policy and procedures.

If OA detects a potential hacking attempt or other form of compromise, it performs an investigation in order to determine the nature and the degree of damage. Otherwise, the scope of potential damage is assessed by the PMA in order to determine if the RCA needs to be rebuilt, only some certificates need to be revoked, and/or the E-ID PKI platform needs to be declared compromised, and which services has to be maintained (revocation and certificate status information) and how.

OA has the capability to restore or recover essential operations within twenty four (24) hours following a disaster with, at minimum, support for the following functions:

- Certificate issuance
- Certificate revocation
- Publication of revocation information

OA maintains offsite backup of important CA information.

5.7.2. Computing resources, software, and/or data are corrupted

In case an E-ID PKI equipment is damaged or rendered inoperative, but the signature keys are not destroyed, the operation is re-established as quickly as possible, giving priority to the ability to generate certificate status information according to the OA emergency and recovery plan.

5.7.3. Entity private key compromise procedures

If a RCA, CA, private key is compromised, lost, destroyed or suspected to be compromised:

- PMA, after investigation on the “key-problem” decides that the RCA certificate and/or CA certificate has to revoked;
- A new key pair and certificate are generated.

5.7.4. Business continuity capabilities after a Disaster

The OA’s emergency and recovery plan addresses the business continuity as described in § 5.7.1.

5.8. RCA component termination

In the event of termination of a RCA component, the RCA requests all certificates issued to this component to be revoked.
In the event of RCA termination:

- RCA archives all audit logs and other records prior to termination;
- RCA destroys all its private keys upon termination;
- Archive records are transferred to an appropriate authority such as the PMA;
- RCA uses means to notify the citizen to delete all trust anchors representing the RCA.

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

Before starting key ceremonies, it is necessary that Security Officer and PMA identifies and make sure that all involved employees are educated about key ceremony operation and their responsibilities, especially for person who hold activation data, according to [2016_2000021244 - Citizen PKI - Key Ceremony 2016 v0.3].

Key generation is always undertaken and witnessed (PMA witness at minimum) in a physically secure environment, called key ceremony room (Cf. 5.1.1); by personnel in trusted roles as described in [2016_2000021244 - Citizen PKI - Key Ceremony 2016 v0.3]. Activation data are distributed to holders that are trusted person from OA and PMA (Cf. Annex 2). Key generation is carried out within a HSM that is FIPS 140 – 2 Level 3 compliant. Key ceremony is always performed in an off-line HSM on a dedicated computer.

Main steps of the key ceremony are identified in [2016_2000021244 - Citizen PKI - Key Ceremony 2016 v0.3]. During the key ceremony, the master of ceremony and witness(es) are using a script that details all operation to be carried out.

At the end of the key ceremony, the generated keys are backed-up (Cf. § 6.2.4) and destroyed in the HSM (Cf. 6.2.10). Therefore, generated key only exist in the back-up HSM devices.

6.1.2. Private Key Delivery to CA

CA generates itself its private key, as described in its CPS.

6.1.3. Public Key Delivery to CA

The CA keys are always generated during a key ceremony operation. The CA public is generated in the same HSM used for RCA key. The CA signature operation by RCA consist in a signing operation of a Pkcs#10 containing the CA's public key. All the files are generated in the HSM used for key ceremony operation.

6.1.4. CA Public Key Delivery to Relying Parties

OA makes RCA and CA certificates available to relying parties by publishing them in the PS. RCA and CA certificates are also delivered to the PMA's administrative contact during the key ceremony (Cf. § 4.3). The Security Officer transmits the RCA and CA certificates to the System Administrator to be set in the PS server.

6.1.5. Key Sizes

If the PMA determines that the security of a particular algorithm may be compromised**,** it may require the RCA and CAs to revoke the affected certificates.

RCA keys for the RSA algorithm are 4096 bits length using at minimum the SHA-2 hash function.
CA keys for the RSA algorithm are 2048 bits length using at minimum the SHA-2 hash function.

6.1.6. Public Key Parameters Generation and Quality Checking

RCA keys and CA keys are generated in accordance with the cryptography tools of hardware security modules (see section 6.2.11).

6.1.7. Key Usage Purposes (as per X.509 v3 Key Usage Field)

Private key usage of RCA and CA are defined in the certificate profiles (refer to § 7.1). The key usage is set to allow private keys to only sign certificates and ARL or CRL. This restriction is implemented in the certificate using the extension “Key usage”.

6.2. Private Key Protection and Cryptographic Module Engineering

6.2.1. Cryptographic Module Standards and Controls

RCA and CA hardware security module is approved FIPS 140-2 level 2 or EAL 4+ certified, or higher.

6.2.2. Private Key (m out of n) Multi-Person Control

To use a back up HSM of RCA key it is necessary to initialize a Luna G5 HSM, on an off-line dedicated computer, with Albanian trusted domain (Cf. § 6.2.8), created during a key ceremony, in order to use the RCA key in the HSM. After the initialization of the HSM, the RCA key has to be inserted in the HSM to be used (Cf. § 6.2.6).

A key contained in a Luna G5 HSM can only be exported in a back up HSM (Cf. § 6.2.6). The key has to be destroyed in the HSM after the end of an operation with RCA key, therefore the RCA key is always under multiple controls.

To use a back up HSM of secret key it is necessary to initialize, or use a pre-initialized, Luna G5 HSM, on the on-line E-ID PKI’s network HSM platform, with Albanian trusted domain (Cf. § 6.2.8), created during a key ceremony, in order to use the secret key in the HSM. After the initialization of the HSM, the keys has to be inserted in the HSM to be used (Cf. § 6.2.6).

A key contained in a Luna G5 HSM can only be exported in a back up HSM device (Cf. § 6.2.6).The key has to be destroyed in the HSM after the end of validity period of the secret and technical CA keys, therefore keys are always under multiple controls.

6.2.3. Private Key Escrow

The RCA and CA private keys are never escrowed, for any reason.

6.2.4. Private Key Backup

RCA and technical CA privates keys and secret keys are back-up on 2 identical Luna backup HSM devices :

- RCA offline back-up;
- CA online back-up;
- Technical CA online back-up;

The key are ciphered, and to use the keys it is necessary to insert it in a HSM (refer to § 6.2.6). The back-up HSM are loaded during key ceremony [2016_2000021244 - Citizen PKI - Key Ceremony 2016 v0.3]. Backup HSM(s) are stored in a safe (refer to § 5.1.8) under the responsibility of Security Officer.

6.2.5. Private Key Archival

Private RCA and CA keys are never archived.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

A key only exist on back-up HSM devices created during the key ceremony. Therefore, to be used, a key has to be inserted inside a Luna G5 HSM personalized with the Albanian trusted domain. To personalize a Luna G5 HSM with Albanian trusted domain, the following activation data and trusted roles for:

- Initial Red USB token: Activation holder of Albanian Ministry of Internal Affairs;
- Initial Blue USB token: Security Officer;
- Black USB token: System Administrator and E-ID PKI Administrator.

Operation of transfer into or from HSM required the following activation data and trusted roles for:

- E-ID PKI's HSM platform (on-line, means pre-initialized with Albanian trusted domain):
  - Insert: Black USB token used to initialize the HSM (System Administrator);
  - Export (no use case): Black USB token used to initialize the HSM (System Administrator);

- E-ID PKI's HSM computer (off-line, means not initialized with Albanian trusted domain):
  - Insert:
    - Initial Red USB token: Activation holder of Albanian Ministry of Internal Affairs;
    - Initial Blue USB token: Security Officer;
    - Black USB token: System Administrator and E-ID PKI Administrator.
  - Export (Append case): Black USB token used to load the HSM (System Administrator).
  - Export (Replace case):
    - Initial Red USB token: Activation holder of Albanian Ministry of Internal Affairs;
    - Initial Blue USB token: Security Officer;
    - Black USB token used to initialize the HSM (System Administrator

The Luna network HSM, when it is in production inside the cabinet in the OA trust center, is managed by the System administrator with HSM (Black USB token) and Security Officer (Blue USB token) (depending of operation).

6.2.7. Private Key Storage on Cryptographic Module

Keys are stored in hardware security modules (Luna network HSM). They are not accessible outside the hardware module.

6.2.8. Method of Activating Private Key

All keys can only be activated inside a Luna G5 HSM. The key has to be inserted in the Luna G5 HSM (Cf. § 6.2.6).

RCA private key pair is activated by Master of Key ceremony when the RCA key is inside the HSM.

Other technical CA that are in the E-ID PKI's HSM platform, in the Albanian trusted domain are only used by the trusted role Security Officer and E-ID PKI Administrator to deliver the technical certificate (Cf. Annex 11). Each time a trusted role wants to use the private key inside the HSM, is authenticated (with TLS protocol) using its technical certificate contained in its smart card (refer to § 11.1).

If the E-ID PKI's HSM server turn off, then the HSM has to be reactivated using initial Blue USB token (Security Officer) and Black USB token used to initialize the HSM (System Administrator).

If the E-ID PKI's HSM server turn off and HSM crash, then the HSM has to be reactivated (reinitialized) using backup HSM and:

- Initial Red USB token: Activation holder of Albanian Ministry of Internal Affairs;
- Initial Blue USB token: Security Officer;
- Black USB token: System Administrator and E-ID PKI Administrator.

6.2.9. Method of Deactivating Private Key

A HSM is only activated for operation in the OA trust center is restricted to authorized personal of the OA. In case the usage of a key stored in the HSM is not required, the corresponding will be destroyed (Cf. § 6.2.10). In case the HSM has to be removed, for termination reason, from the E-ID platform, then all the HSM is deactivated destroying all the key inside (Cf. § 6.2.10) and the Albanian trusted domain.

Deactivation (different from switch off the server or the HSM) requires at least the following trusted roles and activation data:

- Initial Red USB token: Activation holder of Albanian Ministry of Internal Affairs;
- Initial Blue USB token: Security Officer.

6.2.10. Method of Destroying Private Key

Keys are destroyed when they are no longer needed, or when certificates to which they correspond expire or are revoked. Destroying key requires the following operations:

- Destruction of the key inside HSM performed with Black USB token used to connect to the HSM (System Administrator);
- Destruction of the corresponding backup HSM (Security officer).

6.2.11. Cryptographic Module Rating

RCA and CA hardware security module are FIPS 140-2 level 2 and 3.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archival

The public key is archived as part of the certificate archival as described in § 5.5.2.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1. RCA

The RCA certificate lifetime is 25 years.
The RCA private key lifetime is 25 years.

6.3.2.2. CA

The CA certificate lifetime is 15 years.
The CA private key lifetime is 15 years maximum.

6.4. Activation Data

6.4.1. Activation Data Generation and Installation

The Luna G5 and the back-up HSM require the following activation data:

- Trusted domain: red USB token. Created during the key ceremony at initialization to elaborate the trusted domain. This USB token is used to recreate the trusted domain on a Luna G5 that may contain all keys created during the key ceremony,

- Security Officer: blue USB token. Created during the key ceremony at initialization to manage the trusted domain created during key ceremony on a Luna G5. This USB token has to be available for the creation of new partitions and to reactivate a Luna G5 that contains the trusted domain,

- User (M of N for offline only): black USB token. These USB tokens (5 in total) are necessary during activation of the Luna G5 HSM. USB token created during the key ceremony at initialization, it allows the operation of the Luna G5 and activation of partition in Luna G5 and backup HSM device.
- User (online only): black USB token. USB token created during the key ceremony at initialization, it allows the operation of the Luna G5 and activation of partition in Luna G5, network and backup HSM device.

6.4.2. Activation Data Protection

All USB tokens need a unique and proper PIN code to be used. This PIN code is set during the key ceremony. Therefore, the smart cards require the following data:

PIN code: secret data. This secret data is used to activate the private key contained in a USB token.

6.4.3. Other Aspects of Activation Data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

All the computer and server used for E-ID PKI and personalization platform are described in a list maintained by System administrator according OA security policy.

The computer for trusted role respects the following rules:

- Is always locked when the trusted role is not in front of the computer;
- The computer is systematically switched off at the end of the work day;
- The component can only have software that are exclusively required to use the E-ID PKI and personalization software and administration needs;
- The trusted role must have dedicated login/password to use their computer;
- The trusted role has to keep the login/password confidential;
- Only authorized data can be inserted in the server.

The backup HSM devices are only connected to a computer dedicated to key ceremony or to the network HSM.

A key ceremony computer must never be connected to any kind of network. A computer for key ceremony is dedicated to this kind of operation and can't be used for other operation.

All the complementary rules are described in OA security policy.

6.5.2. Computer Security Rating

All the E-ID PKI components software of the OA have been developed following the requirements of common criteria rules.

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

Applications are tested, developed and implemented in accordance with industry best practice development and change management standards.

6.6.2. Security Management Controls

The E-ID PKI equipment are dedicated to the RCA and CA. No other unrelated applications shall be installed that are not part of the E-ID PKI configuration.

The System administrator is sole responsible of computer and server. The System administrator is the sole to have access to the Administration count on the all the server and computer but not on the HSM. The other trusted roles don't have the login and password of the Administration count of the server and computer for E-ID PKI and personalization platform.

All the complementary rules are described in OA security policy.

6.6.3. Life Cycle Security Controls

For the software and hardware that are evaluated, PMA keeps watching on the maintenance scheme requirements to keep the level of trust.

OA security policy describes the life cycle security controls for E-ID PKI and personalization platform. ISO 27001 processes are in place and are followed. Policies are defined and procedures are implemented for risk management, change management, vulnerability management and security control analysis.

6.7. Network Security Controls

Key ceremony operations are made in off-line environment on a dedicated computer. Configuration of equipment is reviewed periodically following ISO 27001 procedures.
OA protects its communication of sensitive data through the use of encryption and digital signature.

6.8. Time-Stamping

Time stamping is not used for records or key ceremony operation.

7. CERTIFICATE, ARL, AND OCSP PROFILES

7.1. Certificate Profile

7.1.1. Version Number

The RCA and CA certificate are X.509 v3 certificates (populate version field with integer "2"). The certificate fields are those defined in the RFC 5280.

7.1.2. Certificate Extensions

7.1.2.1. RCA

Base certificate	Value
Version	2 (=version 3)
Serial number	Defined by KeySeed®
Issuer DN	C = AL OI= NTRAL-K82018015V O = Aleat CN= Albanian Citizen ID Root CA
Subject DN	C = AL OI= NTRAL-K82018015V O = Aleat CN= Albanian Citizen ID Root CA
NotBefore	YYMMDD000000Z (Key Ceremony date)
NotAfter	YYMMDD000000Z (Key Ceremony date + 25 years)
Public Key Algorithm	rsaEncryption
Signature Algorithm	Sha2WithRSAEncryption (sha256RSA or 1.2.840.113549.1.1.11)
Parameters	NULL

Standard extensions	OID	Include	Critical	Value
Authority Info Access	(1.3.6.1.5.5.7.1.1)			n/a
Authority Key Identifier	{id-ce 35}	**X**	**FALSE**	
Methods of generate key ID				**Method 1**
Select AKI Fields				**n/a**
Basic Constraint	{id-ce 19}	**X**	**TRUE**	
CA		X		**True**
PathLengthConstraint		X		**3**
Certificate Policies	{id-ce 32}			
policyIdentifiers				n/a
policyQualifiers				n/a
CPSpointer				n/a
OID				n/a
value				**n/a**
User Notice				n/a
OID				n/a

value				n/a
noticeRef				n/a
organization				n/a
noticeNumbers				n/a
explicitText				n/a
CRL Distribution Points	{id-ce 31}			n/a
distributionPoint				n/a
reasons				n/a
cRLIssuers				n/a
Extended Key Usage	{id-ce 37}			n/a
Issuer Alternative Name	{id-ce 18}			n/a
Key Usage	{id-ce 15}	**X**	**TRUE**	
Digital Signature				**Clear**
Non Repudiation				**Clear**
Key Encipherment				**Clear**
Data Encipherment				**Clear**
Key Agreement				**Clear**
Key CertSign				**Set**
Key CRL Sign				**Set**
Private Key Usage Period	{id-ce 16}			n/a
Subject Alternative Name	{id-ce 17}			n/a
Subject Key Identifier	{id-ce 14}	**X**	**FALSE**	
Methods of generating key ID				**Method 1**
privateInternetExtensions	AIA authorityInformationAccess			n/a
Other Extensions				

7.1.2.2. CA

Base certificate	**Value**
Version	2 (=version 3)
Serial number	Defined by KeySeed®
Issuer DN	C = AL OI= NTRAL-K82018015V O = Aleat CN = Albanian Citizen ID Root CA
Subject DN	Described in CA CPS.
NotBefore	YYMMDD000000Z (Key Ceremony date)
NotAfter	YYMMDD000000Z (Key Ceremony date + 15 years)
Public Key Algorithm	rsaEncryption
Signature Algorithm	Sha2WithRSAEncryption (sha256RSA or 1.2.840.113549.1.1.11)
Parameters	NULL

Standard extensions	**OID**	**Include**	**Critical**	**Value**

Authority Info Access	(1.3.6.1.5.5.7.1.1)			n/a
Authority Key Identifier	{id-ce 35}	**X**	**FALSE**	
Methods of generate key ID				**Method 1**
Select AKI Fields				**n/a**
Basic Constraint	{id-ce 19}	**X**	**TRUE**	
CA		X		**True**
PathLengthConstraint		X		**0**
Certificate Policies	{id-ce 32}	**X**	**FALSE**	n/a
policyIdentifiers				**0.4.0.2042.1.2 (Normalized Certificate Policy requiring a secure cryptographic device)** **CPS URI: https://www.aleat.al/pdf/cps-citizen-root-ca.pdf**
policyQualifiers				n/a
CPSpointer				n/a
OID				n/a
value				n/a
User Notice				n/a
OID				n/a
value				n/a
noticeRef				n/a
organization				n/a
noticeNumbers				n/a
explicitText				n/a
CRL Distribution Points	{id-ce 31}	**X**	**FALSE**	
distributionPoint				[1]Certificates Revocation List Distribution Point Name of the distribution point : Complete Name : URI https://www.aleat.al/csp/albanian-citizen-id-root-ca-04.crl
reasons				n/a
cRLIssuers				n/a
Extended Key Usage	{id-ce 37}			n/a
Issuer Alternative Name	{id-ce 18}			n/a
Key Usage	{id-ce 15}	**X**	**TRUE**	
Digital Signature				**Clear**
Non Repudiation				**Clear**
Key Encipherment				**Clear**
Data Encipherment				**Clear**
Key Agreement				**Clear**
Key CertSign				**Set**
Key CRL Sign				**Set**
Private Key Usage Period	{id-ce 16}			n/a
Subject Alternative Name	{id-ce 17}			n/a
Subject Key Identifier	{id-ce 14}	**X**	**FALSE**	
Methods of generating key ID				**Method 1**
privateInternetExtensions	AIA authorityInformationAccess			n/a
Other Extensions				n/a

7.1.3. Algorithm Object Identifiers

See section 7.1.

7.1.4. Name Forms

The name forms follow the requirements described in the section 3.1.

7.1.5. Name Constraints

The name forms follow the requirements described in the section 3.1.

7.1.6. Certificate Policy Object Identifier

See section 7.1.

7.1.7. Usage of Policy Constraints Extension

See section 7.1.

7.1.8. Policy Qualifiers Syntax and Semantics

See section 7.1.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

See section 7.1.

7.2. ARL Profile

7.2.1. Version Number

RCA shall issue X.509 version two (v2) ARLs (populate version field with integer "1"). The ARL fields are those defined in the RFC 5280.

7.2.2. ARL and ARL Entry Extensions

Features of the ARL:	Duration (expressed in years): 1 year Periodicity of update : 1 year CRL version (v1 or v2) : V2 Issuer: C=AL OI=NTRAL-K82018015V O=Aleat CN=Albanian Citizen ID Root CA Extensions : CRL Number + AKI

	CRL Number : incremented 1 by 1 Signature Algorithm:SHA256 RSA Hash Algorithm: SHA256 http URL for publication : http://www.aleat.al/csp/citizen-root-ca-04.crl

7.3. OCSP Profile

No stipulation.

7.3.1. Version Number(s)

No stipulation.

7.3.2. OCSP Extensions

If an OCSP is used, then the CPS will give details.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency and Circumstances of Assessment

The E-ID PKI is subject to periodic compliance audits, to allow PMA to authorize or not (regarding the audit result) RCA to be operated by OA under the RCA CPS.

The E-ID PKI and personalization infrastructure are subject to periodic compliance audits, to allow PMA to authorize or not (regarding the audit result) RCA to be operated by OA under the RCA CPS.

8.2. Identity/Qualifications of Assessor

The compliance auditor shall demonstrate competence in the field of compliance audits, and shall be thoroughly familiar with requirements of this CPS. The PMA and OA looks carefully, regarding its own audit requirements basis, to the methods employed to E-ID PKI. Auditor must be certified to conduct ISO 27001 audit.

8.3. Assessor's Relationship to Assessed Entity

The compliance auditor is either a private firm, which is independent from the entity being audited, or sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation.

The PMA and OA determine whether a compliance auditor meets this requirement.

8.4. Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a component operates in accordance with the RCA CPS and the OA’s security policy.

The purposes of a compliance audit are to verify that a component operates in accordance with the the present CPS.

The conducted audit is to verify, at minimum, the following topics:

- Knowledge of the CPS, procedure and technical guide by the trusted role;
- E-ID PKI and personalization software are deployed on the correct server;
- E-ID PKI and personalization component respect the network security policy of OA and the present CPS;
- Materials and HSM are used correctly regarding the software deployed on it;
- IP configuration is correct and well administrated by System administrator;
- Each certificate delivered with the E-ID PKI respect [2016-2000021870 - Naming Document - Citizen PKI V0.3];
- OA trust center respect the physical and logical security as described in the present CPS and OA security policy;
- All the media are managed according OA security policy and the present CPS;
- E-ID PKI and personalization platform has a correct time;

- Activation data (refer to § 6.4.1 **Error! Reference source not found.**) are correctly distributed and managed by the right trusted roles;
- Back-up HSM still exist and correctly protected (refer to § 5.1.8);
- All the trusted role have their smart card;
- Only authorized components (Operator computer and personalization platform) are connected to E-ID PKI and personalization platform. This verification is made with System Administrator with System Administrator log book, firewall and server audit files.

8.5. Actions Taken as a Result of Deficiency

The PMA may determine that the RCA are not complying with its obligations set forth in the RCA CPS. When such a determination is made, the PMA may suspend or direct to stop affected RCA and may request that corrective actions be taken which allow to continue operation of the operation of the noncompliant RCA. When the compliance auditor finds a discrepancy between how the RCA is designed or is operated or maintained, and the requirements of the CPS, the following actions shall be performed:

- The compliance auditor notes the discrepancy;
- The compliance auditor notifies the PMA of the discrepancy;
- The party responsible for correcting the discrepancy determines what further notifications or actions are necessary pursuant to the requirements of the RCA CPS, and then proceed to make such notifications and take such actions without delay in relation with the approval of PMA.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the PMA may decide to stop temporarily operation of a RCA, to revoke a certificate issued by the RCA, or take other actions it deems appropriate.

8.6. Communications of Results

An Audit Compliance Report, including identification of corrective measures taken or being taken by the component, is provided to the PMA as set forth in § 8.1. The report identifies the versions of the CPS and OA's security policy used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in § 8.5 above. The Audit Compliance Report is not available on Internet for relying parties.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

Defined by OA and PMA.

9.1.2. Certificate Access Fees

The RCA PS is free access on the internet for relying parties.

9.1.3. Revocation or Status Information Access Fees

The RCA PS is free access on the internet for relying parties.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

No stipulation.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

OA maintains reasonable levels of insurance coverage.

9.2.2. Other Assets

OA maintains sufficient financial resources to maintain operations and fulfil RCA duties.

9.2.3. Insurance or Warranty Coverage for End-Entities

If there is damage for a relaying party due to Albanian Ministry of Internal Affairs or OA fault, Albanian Ministry of Internal Affairs and/or OA will cover part of the relaying party damage in the limits stated in the PMA and OA.

9.3. Confidentiality of Business Information

9.3.1. Scope of Confidential Information

OA and PMA guarantees a special treatment for the confidential following:

- Records and archive;
- Personal identity data;
- RCA private keys;
- RCA Audit result and reports;
- RCA Disaster recovery plans;
- Contractual arrangements with OA;
- OA trust center security policy;
- Part of the RCA CPS defined as confidential,
- Revocation reason;
- Activation data;
- Private and secret key.

9.3.2. Information Not Within the Scope of Confidential Information

All information that is published in the PS is not considered confidential, but can be covered by the law on intellectual property right.

9.3.3. Responsibility to Protect Confidential Information

OA enforces Albanian law for the protection of data (confidential and personal data) and secures confidential and personnel data from compromise and disclosure.

9.4. Privacy of Personal Information

9.4.1. Privacy Plan

PMA collects, stores, processes and discloses personally identifiable information in accordance with the European law on privacy data protection.

9.4.2. Information Treated as Private

PMA considers that information considered as private for RCA and CA are:

- Naming document;
- Revocation request form.

9.4.3. Information Not Deemed Private

Any and all information within a certificate, CRL or printed upon the smart card is inherently public information and shall not be considered confidential information.

9.4.4. Responsibility to Protect Private Information

E-ID PKI component treat and protect all the private information in a manner that only authorize access to trusted role (internal or legal entity) according to the Albanian Ministry of Internal Affairs requirements on the privacy data protection.

9.4.5. Notice and Consent to Use Private Information

All private information coming from E-ID PKI cannot be used without any explicit consent from the PMA.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

OA is compliant with the national law and use secure procedures to allow access to the private data for any legal entity with authentication and secured controlled access to those data.

9.4.7. Other Information Disclosure Circumstances

PMA obtains consent from Albanian Ministry of Internal Affairs to transfer its private data in case of transfer of activity, as described in the § 5.8.

9.5. Intellectual Property rights

OA retains all intellectual property rights, and is proprietary of the RCA CPS, RCA certificate, CA certificate and revocation information that are issued by the RCA.

9.6. Representations and Warranties

9.6.1. PMA Representations and Warranties

PMA define the CPS. PMA establishes that RCA complies with the present CPS. The processes and procedures and audit framework used to determine compliance are documented within the CPS.

PMA ensures that all requirements on E-ID PKI component, as detailed in the present CPS, are implemented as applicable to deliver and manage CA certificate.

PMA has the responsibility for compliance with the procedures prescribed in this CPS, even when RCA functionality is undertaken by sub-contractors (OA …). RCA provides all its certification services consistent with its certification practice statement.

9.6.1.1. Activation holder of Albanian Ministry of Internal Affairs

Activation holder of Albanian Ministry of Internal Affairs obligations are:

- Respect its obligation regarding the function they have to perform (as specified in Annex 11 and in the present CPS);
- Respect the present CPS;
- Protects the activation data and the associated PIN code;
- Respect the OA security policy;
- Manage and signs [2016-2000021870 - Naming Document - Citizen PKI V0.3].

9.6.2. RCA and CA Representations and Warranties

Common obligations for RCA and CA are delegated to OA and are:

- Protect and guarantee integrity and confidentiality of their secret data and/or private key;
- Only use their cryptographic key and certificate, with associated tools specified in CPS, for what purpose they have been generated for;
- Respect and operate CPS part that deals with their duty (this part of CPS has to be transmitted to the corresponding component);
- Let auditor team audit and communicate every useful information to them, according to the PMA intention, control and check the compliance with the CPS and with the components CPS;
- Document their internal procedures to complete global CPS;
- Use every means (technical and humans) necessary to achieve the realization of the CPS it has to implement and they are responsible for.

9.6.3. OA Representations and Warranties

The OA has the responsibility to:

- Respect its security policy;
- Protect and guarantee integrity and confidentiality of their secret data and/or private key;
- Let auditor team audit and communicate every useful information to them, according to the PMA intention, control and check the compliance with the present CPS and the OA's security policy;
- Alert PMA when there is an security incident about the RCA services that the OA performed;
- Respect and operate CPS part that deals with their duty (this part of CPS has to be transmitted to the corresponding component);
- Document their internal procedures to complete global CPS and its security policy;
- Respect total or part of agreements that binds it to the PMA;
- Nominate person to have trusted role defined in Annex 11 and ensure that a person has only one trusted role.

9.6.3.1. Security Officer

Security Officer obligations are:

- Respect its obligation regarding the function they have to perform (as specified in Annex 11 and in the present CPS);
- Respect CPS;
- Protects the activation data and the associated PIN code;
- Protects the smart card and the associated PIN code;
- Manage and deliver technical certificate for trusted roles;
- Conduct internal audit and external audit (ISO 27001);
- Protect back up HSMs of keys;
- Respect the OA security policy.

9.6.3.2. System Administrator

System Administrator obligations are:

- Respect its obligation regarding the function they have to perform (as specified in Annex 11 and in the present CPS);

- Administrate all server, computer and firewall of E-IDPKI platform according present CPS and OA security policy;
- Make the periodic back-up of the E-ID PKI and personalization component;
- Protect and guarantee integrity and confidentiality of IP addresses, login/password and account of server, computer and firewall;
- Respect the OA security policy;
- Protects the activation data and the associated PIN code;
- Conducts vulnerable analysis of the network.

9.6.3.3. Master of key ceremony

Master of key ceremony obligations are:

- Respect its obligation regarding the function they have to perform (as specified in Annex 11 in the present CPS);
- Respect the present CPS;
- Respect the OA security policy;
- Performed key ceremony operation.

9.6.4. Representations and Warranties of Other Participants

9.6.4.1. Relying party

The RP has the responsibility to valid an electronic certificate from E-ID PKI's CA using:

- The valid RCA and CA certificates;
- The ARL and the CRL to validate certificates;
- The information accessible from the SP about RCA and CA;
- Procedures described in the RFC 5280.

9.7. Disclaimers of Warranties

The RCA services only guarantees the identification and authentication of the RCA, with RCA self-signed certificate, and of CA that own a certificate issued by the RCA, and the management of the corresponding certificate and certificate status information regarding the CPS. Not any more guarantees can be pinpointed by PMA and relying parties in their contractual relationship (if there is any).

9.8. Liability limitation

PMA is only responsible for the CPS requirements and principles, for the compliance audit between the present CPS and the CA CPS.

RCA are responsible for any damage caused to relying parties because of improperly operating of the RCA CPS.

OA assumes no liability whatsoever in relation to the use of RCA certificate and CA certificates or associated public/private key pairs for any use other than the one stated in the CPS.

9.9. Indemnities

In a damage proved to be under OA responsibility, the indemnities are limited to maximum sum of money that is given by the PMA.

9.10. Term and Termination

9.10.1. Term

The RCA CPS becomes effective, and after its amendments, upon ratification by the PMA, adoption by the OA and publication in the PS.

9.10.2. Termination

In the event that the RCA ceases to operate, a public announcement must be made by the PMA. Upon termination of service, the RCA must properly archive its records including certificates issued, RCA certificate, CA certificate, CPS and ARL for a period of 10 years after the date of service termination.

9.10.3. Effect of Termination and Survival

End of validity of the present CPS stops all obligation and liability for RCA and CA.

RCA and CA cannot keep on delivering electronic certificate referring to the present CPS. End of validity of the present CPS stops all obligation and liability for PMA.

9.11. Individual Notices and Communications with Participants

PMA provides participants with new version of CPS as soon as it is validated by OA, via the PS.

9.12. Amendments

9.12.1. Procedure for Amendment

PMA reviews CPS at least yearly. Additional reviews may be enacted at any time at the discretion of PMA. Spelling errors or typographical corrections which do not change the meaning of the CPS are allowed without notification. Prior to approving any changes to this CPS, PMA notifies RCA.

9.12.2. Notification Mechanism and Period

PMA notifies RCA and CA on its intention to modify CPS no less than 30 days before entering the modification process.

9.12.3. Circumstances under Which OID Must be Changed

Present CPS OIDs are changed if the PMA determines that a change in the CPS modify the level of trust provided by the CPS requirements.

9.13. Dispute Resolution Provisions

OA proposes to solve dispute on identity to set in the certificate and in the case that parties in conflict cannot find an arrangement; the problem will be solved in a Albanian court. The contractual arrangements between Albanian Ministry of Internal Affairs and OA contains a dispute resolution clause.

9.14. Governing Law

The applicable laws that govern the RCA CPS applicability are the laws of the State of Albany, according to the entire relevant European directive that could apply to the present CPS.

9.15. Compliance with Applicable Law

This CPS is subject to applicable national, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing cryptographic software, hardware, or technical information.

9.16. Miscellaneous Provisions

9.16.1. Entire Agreement

If there is any, the PMA has to approve it according to the OA approval procedures.

9.16.2. Assignment

Except where specified by other contracts, only the PMA may assign and delegate this CPS to any party of its choice.

9.16.3. Severability

If any part of the CPS is unenforceable by a court of law, it doesn't make the other part of the CPS invalid.

9.16.4. Waiver of Rights

The requirements defined in the CPS are to be implemented as described in CPS without possible waiver of right in the intention of changing any defined rights or obligation.

9.16.5. Act of God

OA is not responsible for indirect damage and interruption of services due to act of god that direct caused direct damage to citizen and relying party.

9.17. Other Provisions

No stipulation.

10. ANNEX 1: TRUSTED ROLES FORMS

The following annex gives all the content for the required forms used to attribute trusted roles.

10.1. Authorization form

- Role requester:
  - Date:
  - Name;
  - First name;
  - Telephone;
  - Address;
  - Role requested ;

Signature of the Role requester

- Name of the Authorizer;
  - Date:
  - Name;
  - First name;
  - Telephone;
  - Address;
  - Authorizer role.

Signature of the Authorizer.

10.2. Trusted roles certificate delivery form

- Person who will receive smart card and certificate for trusted role:
  - Date:
  - Name;
  - First name;
  - Telephone;
  - Address;
  - Role;

Signature of the trusted role certificate applicant

- Name of the “master trusted role” who deliver the certificate ;
  - Date:
  - Name;
  - First name;
  - Telephone;
  - Address.

Signature of “master trusted role” who deliver the certificate

10.3. Activation data delivery form

- Person who receive activation data:
  - Date:

- Name;
- First name;
- Telephone;
- Address;
- Type of activation data ;

Signature of the Activation data holder

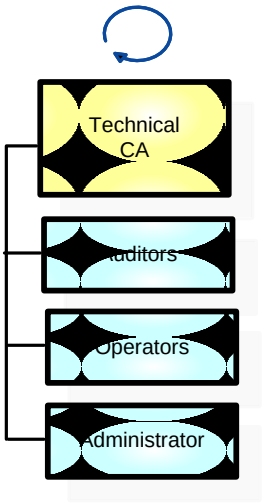
- Name of Security Officer;
  - Date:
  - Name;
  - First name;
  - Telephone;
  - Address.

Signature of Security Officer

11. ANNEX 2: DESCRIPTION OF TRUSTED ROLES

11.1. OA roles

The Technical CA used to manage the E-ID PKI trusted roles are the following:



Trusted roles	Certificates and/or tools	Function	Comments
Security Officer (*Aleat IT Security Manager*)	Administrator certificate on dedicated smart card	Manage certificate profiles and PKI configuration on ID CA ID NOMIC software	Using ID NOMIC ID CA software.
		Create and revoke PKI roles certificates. Those certificates are signed using the Technical CA.	Using ID NOMIC ID CA software.
	2 Blue USB tokens	Activation holder (HSM init)	Using Safenet HSM
System Administrator (*Aleat IT System Administrator*)	Black USB token	Key and partition management	Using Safenet HSM
	Login and password of server	Administrate all E-ID PKI and personalization server	Using ID NOMIC ID CA software.
Master of key ceremony (*Aleat IT Security Manager*)	NA	Prepare and realize RCA and CA initial key ceremony	Using Keyseed® software
System Auditor (Aleat Quality & Inspection Manager)	Auditor certificate on dedicated smart card	Authorized to view and maintain archives and audit logs of the CA trustworthy system. Audit all E-PKI activity.	Using ID NOMIC ID CA software.

11.2. IDEMIA Identity & Security roles

Trusted roles	Functions	Comments
Master of key ceremony (*Aleat IT Security Manager*)	Prepare and realize RCA and CA initial key ceremony.	An IDEMIA identity & Security employee.
IDEMIA Identity & Security witness	Survey and control RCA and CA initial key ceremony. . Check the progression of the key ceremony and validate the steps according to the ceremony report, also guarantee the security guidance	A Aleat employee

11.3. Albanian trusted roles

11.3.1. Ministry of Internal Affairs

Trusted roles	Certificates and/or tools	Function	Comments
Activation holder of Albanian Ministry of Internal Affairs Known as "Domain Manager"	NA	PMA's witness	Assist to key ceremony
		PMA's Administrative contact	Sign [Key ceremony record]
	2 Red USB token	Activation holder	Using HSM

12. ANNEX 3: LIST OF REFERENCED DOCUMENTS

This annex contains all references of documents mentioned in the present CPS between.

Acronym	Name of the document	Date	Version
[2016_2000021244 - Citizen PKI - Key Ceremony 2016 v0.3	key ceremony preparation guide	13/09/2016	0.3
[2016-2000021870 - Naming Document - Citizen PKI V0.3]	Creation of the certificate authorities' hierarchy for Albanian E-ID PKI.	13/09/2016	0.3

---------- END of DOCUMENT ---------