Reference	Type		Classification		Owner	Version	Date	Page
OPS-OP-024	Type	**Document**	Classification	**Public**	**OP**	**13**	**06.12.2021**	**1 / 85**

Document Title

CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

REPUBLIC OF ALBANIA

Production & Distribution of
Identity Documents & Biometric Passports

CITIZEN AUTH CA CERTIFICATION
PRACTICE STATEMENT

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**2 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

TABLE OF CONTENTS

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**3 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**4 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

Reference	Type	Classification	Owner	Version	Date		Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**		**5 / 85**

Document Title

CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**6 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**7 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**8 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**9 / 85**

Document Title

CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**10 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**11 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

1. INTRODUCTION

1.1. Overview

Albania operates E-ID Public Key Infrastructure (PKI) to deliver certificates used in the electronic citizen identity card as well as Resident Permit. The certificates delivered to Albanian citizen are signed by Certificate Authority (CA). CA are signed by a Root Certification Authority (RCA or also named "Albanian Citizen ID Root CA").

CA are "on-line" (means CA use a network) and RCA is "Off-line" (means RCA is used without network).

The certificates for authentication and Auth OCSP are delivered by a CA named "Albanian Citizen ID Auth CA".
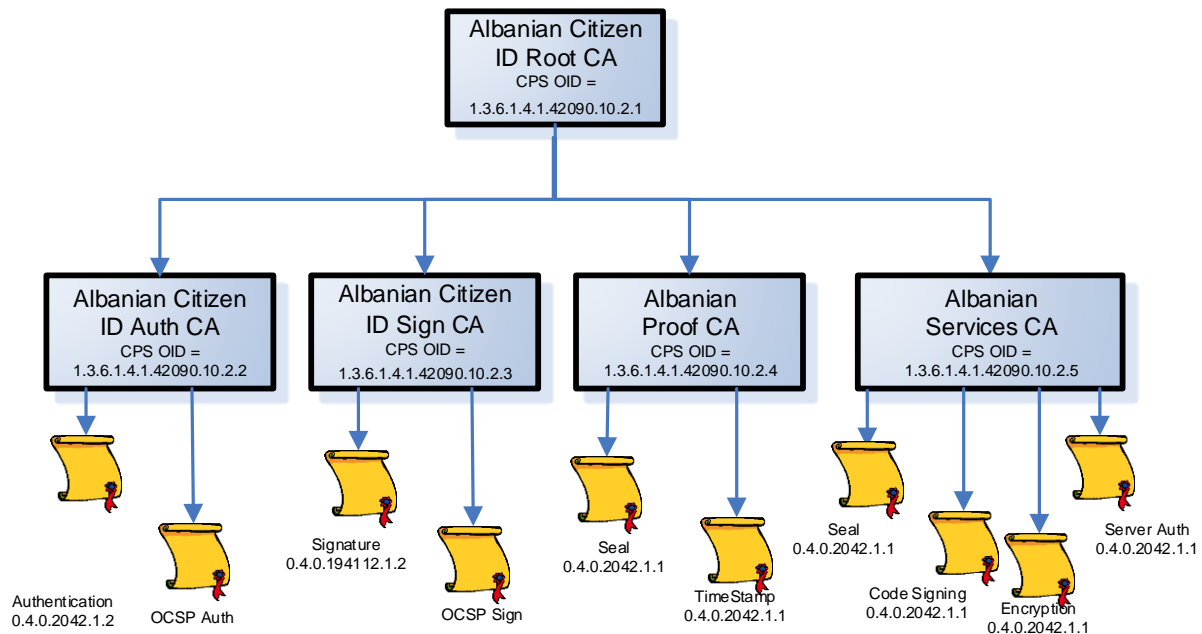
This Certificate Practice Statement (CPS) defines the procedure, applicable to the Albanian CitizenID Auth CA, implemented to certify Certification Authority (CA).

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 Practice Statement Framework;

- The Certification Policy (CPS) of the Albanian RCA;

- The Certification Policy (CPS) of the Albanian Citizen Auth CA.

1.2. Document name and Identification

This CPS is the OA property. The corresponding CP is normalized certificate policy that is 0.4.0.2042.1.2. This CPS document has its own OID (1.3.6.1.4.1.42090.10.2.2).

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**12 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

1.3. PKI Participants

On behalf of Albanian Ministry of Interior Operational Authority (OA) operates the CA in a dedicated trust center. For this purpose Aleat has established a PMA to manage the CA. To host, operate the CA and certify citizen, Aleat deploys a PKI (E-ID PKI). For the authentication certificate issuance activity delivered by the CA, this PKI is composed of the components described below and supports the following services:

- Generation of CA key: OA on behalf of Albanian Ministry of Interior operates the CA and generates the CA keys in the OA trust center during an operation called "Key ceremony";

- Smart card personalization: OA on behalf of Albanian Ministry of Interior operates a plat-form to personalize the identity citizen smart card. The personalization includes citizen fingerprint and activation data (PIN code and PUK code) in the smart card. This services transmit the smart card to the Local Registration Authority (LRA);

- Authentication of citizen: Aleat collects and verifies each citizen identity and information that will be included in the public key certificate to be delivered. This service is supported by LRA that is hosted and managed by Civil Registry Offices. LRA also authenticates citizen for revocation operation;

- Generation of auth certificate: the CA receives the certificate request from LRA and generates a digital certificate according to this CPS. This operation is performed by the CA in the OA trust center;

- Revocation of auth certificate: when the link between the citizen and public key defined within the certificate delivered by the auth certificate is considered no longer valid then the CA revokes the auth certificate. This operation is performed by the CA in the OA Trust Center;

- Renewal of a auth certificate: action of delivering a new certificate to the citizen with the same procedure used for the first auth certificate;

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

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

1.3.1. Aleat Policy Management Authority (PMA)

Aleat is the PMA on behalf of Albanian Ministry of Interior.

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

- The RCA CPS with the present 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 present CPS: the result of the mapping guarantees that the CA operates in compliance with the present 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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**13 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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. The OA ISMS policy document (ISO-QA-014) describes the management of the security and the Information System Security Policy (ISO-SC-023) which is accessible by all OA employees.

1.3.2. Root Certificate Authority (RCA)

Aleat on behalf of Albanian Ministry of Interior 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 Keyseed® software and Luna G5 HSM.

1.3.3. Certification Authorities (CA)

CA is managed by Aleat.

Citizen Auth CA generates certificates for citizen and for OCSP needs of the OA. CA uses SP to publish its auth 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-CA ID NOMIC PKI application software and Luna SA HSM.

1.3.4. Registration Authority (RA)

RA is managed by Aleat on behalf of the Albanian Ministry of Interior for organizational works (nominates the LRA). OA manage technical aspect of the RA (component communication with LRA and management of technical certificate used by LRA).

RA is an entity that nominates, authenticates and verifies the LRA. RA receives all certificates requests from LRA. RA is authenticated and recognized by CA. RA transmits certificate request to CA.

All the RA operations are performed in the OA trust center. E-ID PKI platform (for RA) is a set of server using ID NOMIC ID CA PKI application software.

1.3.5. Operational (OA)

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

The Operational Authority (OA) is the entity which sets up and performs all technical operations of E-ID PKI certificates life cycle management and personalization of identity citizen smart card on behalf of the Albanian Ministry of Interior. 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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**14 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

1.3.6. Local Registration Authority (LRA)

Selected Civil Registry Offices by RA are LRA. A trusted Aleat employee in the Civil Registry Offices has a computer with technical certificate to register citizen and manage communications with the RA.

An LRA is an entity that performs the authentication and identification of the citizen and delivers the identity smart card to the citizen. LRA transmits certificate request and revocation request to RA

An LRA is authenticated and recognized by RA.

1.3.7. Publication Service (PS)

The PS is an entity that makes available information such as CA CPS and CRL.

The PS is hosted and managed in the OA.

1.3.8. Citizen

Citizen is a natural person whose identity is contained in the auth certificate and certified by the Citizen Auth CA. Citizen holds the auth certificate and uses the corresponding private key to be authenticated in control access application (to consult document, to have access to service …). To request auth certificate, first of all, the citizen has to hold an identity smart card (Cf. § 6.4 that explain the identity smart card delivery process).

1.3.9. Service Providers

Service providers as Banks or government agencies or others can use the auth certificate to authenticate Albanian citizen to offer to the citizen access to services.

1.3.10. Other Participants

1.3.10.1. Relying Party (RP)

There is no relying party.

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

1.4.1.1. CA certificate

The Albanian Citizen ID Auth CA certificate is used to sign X.509 certificates (auth certificate and auth OCSP certificate) and CRL according to this CPS.

1.4.1.2. Auth certificate

The auth certificate is used to be authenticated in control access application (to consult document, to have access to service …) according to the policy of the application used by the citizen.

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

The auth certificate can be used to authenticate as a client to access Web site.

1.4.1.3. Auth OCSP certificate

The auth OCSP certificate is used to sign a certificate's status information responses related to Citizen Auth certificate according the policy of the application.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**15 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

The auth OCSP certificate is used by a relying party to check and verify the identity of the auth OCSP responder.

1.4.2. Prohibited Certificate Uses

No other application (means different certificate format or different CA function) than the one stated in § 1.4.1.1, § 1.4.1.2 and § 1.4.1.23 above are covered by the CA CPS. Albanian Ministry of Interior is not responsible for any other use that these stated in the CA 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. Auth certificates and CA certificate shall not be used for any functions except theses stated in § 1.4.1.1 § 1.4.1.2 and § 1.4.1.23 above.

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 Chief Operation Officer is the contact 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 CA 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 Interior.

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 Policy and 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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**16 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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 CA to have a certificate delivered by the CA.

Certification Practice Statement (CPS)

A statement of the practices that Albanian Ministry of Interior (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 end certificates signed by the CA.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**17 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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].

Identity Smart Card : Identity Card or Resident Permit

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]

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**18 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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. § 1.3.7.

Relying Party: Cf. § 1.3.10.1.

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 Organization for Standardization;

PMA: Aleat Management Authority;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**19 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**20 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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:

- For the AUTH CA with the suffix 04, the naming is the following

    o Root CA CPS; https://www.aleat.al/pdf/cps-citizen-root-ca.pdf;

    o CA CPS: https://www.aleat.al/pdf/cps-citizen-auth-ca.pdf;

    o RCA certificate: https://www.aleat.al/csp/albanian-citizen-id-root-ca-04.cer;

    o CA certificate: https://www.aleat.al/csp/albanian-citizen-id-auth-ca-04.cer>;

    o Certificate status (CRL): https://www.aleat.al/csp/albanian-citizen-id-auth-ca-04.crl;

    o CA Certificate status (ARL): https://www.aleat.al/csp/albanian-citizen-id-root-ca-04.crl.

- For the AUTH CA with the suffix 05, the naming is the following

    o Root CA CPS; https://www.aleat.al/pdf/cps/citizen-root-ca-05.pdf;

    o CA CPS: https://www.aleat.al/pdf/cps-citizen-auth-ca.pdf;

    o RCA certificate: https://www.aleat.al/csp/albanian-citizen-id-root-ca-04.cer;

    o CA certificate: https://www.aleat.al/csp/albanian-citizen-id-auth-ca-05.cer;

    o Certificate status (CRL): https://www.aleat.al/csp/albanian-citizen-id-auth-ca-05.crl;

    o CA Certificate status (ARL): https://www.aleat.al/csp/albanian-citizen-id-root-ca-04.crl.

This information is 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;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**21 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

- 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 unauthorized 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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**22 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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 RFC3280. The CPS gives all the details for the identity given to the CA and for a citizen.

3.1.1.1. 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	C = AL OI= NTRAL-K82018015V O = Aleat CN=Albanian Citizen ID Auth CA

3.1.1.2. Citizen

The DN of the Auth certificate is:

Base certificate	Value
Issuer DN	C = AL OI= NTRAL-K82018015V O = Aleat CN=Albanian Citizen ID Auth CA
Subject DN	C = AL Pseudo=<NID> CN= <FirstName LastName> SN= PNOAL-<National ID>

3.1.1.3. Auth OCSP

The DN of the Auth OCSP certificate is:

Base certificate	Value
Issuer DN	C = AL OI = NTRAL-K82018015V O = Aleat CN = Albanian Citizen ID Auth CA
Subject DN	C = AL OI = NTRAL-K82018015V O = Aleat CN =<System Name>

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**23 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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 CA certificates is not a pseudonym or an anonymous name.
The identity used for the auth certificate contains also a pseudonym (NID of the Citizen) but not 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 7.2.

3.1.5. Uniqueness of Names

The citizen and CA identity (refer to § 3.1.1) is unique for all certificates generated by the CA. 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

The citizen's key pair are generated and stored by the RA directly in the identity smart card. This operation requires the presence of the citizen to activate the identity smart card (Cf. § 6.2.8). RA ensures that citizen owns the private key corresponding to the public key to be certified by CA, using certification request in Pkcs#10, and the signature of the certificate request using the citizen's public key (Cf. § 6.1.3).

3.2.2. Authentication of Organization identity

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

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

- RCA: Aleat on behalf of Albanian Ministry of Interior;
- CA: Aleat;
- PMA: Aleat on behalf of Albanian Ministry of Interior;
- OA: Aleat;
- LRA: there is a list maintained by PMA and OA of all authorized Civil Registry Offices.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**24 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

3.2.3. Authentication of Individual identity

3.2.3.1. 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 § below) regarding the trusted roles that individual person may own within the PMA.

3.2.3.2. 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 § 10.1 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 § 10.1 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 § 10.1 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 § 10.1 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 § 10.1 below). This form is also signed by the E-ID PKI Administrator of the OA. E-ID PKI 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. 12.1) 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 § 12.1 below).

3.2.3.3. LRA

Evidence of the Individual identity, for persons who work in LRA is checked against a physical person who is responsible of the deployment of the LRA platform. Each person has to sign a form (refer to § 10.1 below) regarding the trusted roles that individual person may own within the LRA. The form is returned to the PMA.

3.2.3.4. Citizen

Authentication of citizen is performed by LRA against a physical person during a face to face meeting. Evidence of the citizen is verified by LRA using its identity smart card.

The LRA check that the fingerprint from the citizen match whit fingerprint contained in the identity smart card provided by the citizen. Actually the citizen identity smart card is block with the fingerprint and the default PIN code. If the card is activated, then the LRA knows that it is the right citizen that holds the identity smart card.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**25 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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 of OA.

Validation of authority of the individual (confirmation of the employment and authorization of the person enrolling, existence and identity of the service named, possession of a function …) with trusted roles who works in OA are authenticated by the PMA.

PMA uses the same procedure as described in sections 3.2.2 and 3.2.3.

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 Renewal certificate Requests

3.3.1. Identification and Authentication for renewal certificate

A request for renewal auth certificate may only be made by the citizen in whose name the certificate has been issued. The citizen identifies itself using the initial identity-proving process as described above. At each re-key request the identity of a citizen, identified as required in § 3.2.3, is re-established through the initial registration process.

3.3.2. Identification and Authentication for renewal certificate after Revocation

After the auth certificate has been revoked, the citizen is required, if he/she wants a new auth certificate, to go through the initial registration process described in § 3.2.3 to obtain a new auth certificate.

3.4. Identification and Authentication for Revocation Request

Auth certificate revocation requests are authenticated by the LRA or RA. The authentication procedure requires to go through the initial registration process (See § 3.2.3) for citizen. If the citizen has lost its identity smart car, then the document to be provided to the LRA are the documents requested for the delivery of an identity smart card (Cf. § 6.4.1). The LRA Operator transmits the technical revocation request to the RA (OA, K.Registration® software). The revocation request is file signed by LRA platform and transmitted to K.Registration® software during SSL communication

Albanian Ministry of Interior is authorized to request certificate revocation. The Security Officer of OA authenticates the employee of the Ministry of Interior according to rules defined by PMA. PMA defines a list of trusted employee allowed to request such revocation to the OA. The E-ID PKI Operator, upon the order of the Security Officer, uses the ID-Nomic web interface to transmit the revocation request during a TLS communication.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**26 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Origin of a certificate request

Albanian citizen is in charge of requesting an auth certificate.

Before requesting an auth certificate, the citizen must have an identity smart card (Cf. § 6.4). The Albanian citizen provides his/her identity card giving his/her address from civil registry.

There are two different cases:

- Automatic creation of the auth certificate at identity card creation process. This is performed by RA at CA site
- Citizen auth certificate request at LRA location with creation of certificate inside the card under the control of the citizen

4.1.2. Enrolment Process and Responsibilities

The auth certificate request, named "E-Government access form", is established by the citizen.
The citizen manually signs (hand written signature) the E-Government access form.
The subscriber obligations are the following:

1. Submit complete and accurate information and will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy in accordance with the policy with regards to registration.

2. The key pair is only used in accordance with any limitations notified to the subscriber and the subject if the subject is a natural or legal person.

3. Comply fully with any and all information and procedures required in connection with the Identification and authentication relevant to auth certificate issued

4. Promptly review, verify and accept or reject the digital certificates that are issued and ensure that all the information set out therein is complete and accurate and to notify CA, registration authority or Aleat immediately in the event that the digital certificates contain any inaccuracies

5. Secure the private keys and take all reasonable and necessary precautions to prevent the theft, unauthorized viewing, tampering, compromise, loss, damage, interference, disclosure, modification or unauthorized use of its private keys (to include password, hardware token, or other activation data used to control access to participant's privates keys)

6. Exercise sole and complete control and use of the private key that corresponds to the certificate holder's public key

7. Unauthorized use of the subject's private key is avoided.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**27 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

8. Take all reasonable measures to avoid the compromise of the security or integrity of Aleat PKI

9. Notify the TSP without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:

    a. The subject's private key has been lost, stolen, potentially compromised.

    b. Control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons.

    c. Inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject.

10. At all times, use the digital certificates in accordance with all applicable laws and regulations

11. Following compromise, the use of the subject's private key is immediately and permanently discontinued, except for key decipherment.

12. Discontinue the use of the digital certificates in the case of being informed that the subject's certificate has been revoked, or the issuing CA has been compromised.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

In both cases, the citizen establishes and provides the auth certificate request during the face to face meeting with the LRA.
The LRA authenticates and identifies the citizen during a face to face meeting.
The LRA verifies all the information given by the citizen checking its fingerprint against the fingerprint contained in the identity smart card (Cf. § 3.2.3.4).

4.2.2. Approval or Rejection of Certificate Applications

In the automatic certificate creation case (the citizen has no identity card), if all verifications are passed, then:

- The LRA Operator accepts the auth certificate request from the citizen;

- The LRA Operator signs the E-Government access form that the citizen has signed;

- The LRA Operator transmits the auth certificate request to the RA as well as the identity card creation.

- The LRA Operator transmits the E-Government access form to the RA by means that guarantee confidentiality and integrity. The transmission is done by transport selected by Aleat;

In the certificate issuance under the citizen control case (the citizen has his/her identity card), if all verifications are passed, then:

- The LRA Operator accepts the auth certificate request;

- The LRA Operator signs the E-Government access form that the citizen has signed;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**28 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

- The LRA Operator transmits the auth certificate request to the RA (RA, MORPHOCS software). The certificate request is signed by citizen private key (LRA platform) and transmitted to RA (MORPHOCS software) on TLS communication;

- The LRA Operator transmits the E-Government access form to the RA by means that guarantee confidentiality and integrity. The transmission is done by transport selected by Aleat.

4.2.3. Time to Process Certificate Applications

No stipulation.

4.3. Certificate Issuance

4.3.1. CA Actions during Certificate Issuance

In the automatic certificate creation case (the citizen has no identity card), this is executed during the production of identity card:

- RA (MorphoPerso Core) requests the creation of RSA key pair and certificate request to MorphoPerso PKI

- RA (MorphoPerso PKI) requests the creation of RSA key pair to MorphoPerso KPS

- RA (MorphoPerso PKI) stores the RSA key pair in database as encrypted and signed

- RA (MorphoPerso PKI) creates the CSR with Albanian citizen information and sends the certificate request signed with the dedicated private key to the RA (MorphoPerso Core software) through TLS communication

- The RA (MorphoPerso Core) transmits auth certificate request to the Citizen Auth CA (ID-NOMIC software).

- Citizen Auth CA (ID-NOMIC software) verifies the RA (MorphoPerso) certificates and signature.

- Citizen Auth CA (ID-NOMIC software) transmits the auth certificate to the RA (MorphoPerso Core software).

- RA (MorphoPerso PKI) checks the auth certificate and transmits the RSA key pair and corresponding auth certificate to MorphoPerso ePersoServer for insertion in the identity smart card through secure channel

In the certificate issuance under the citizen control case (the citizen has his/her identity card), if all verifications are passed, then:

- LRA sends the certificate request signed with the citizen private key to the RA (MORPHOCS software) through TLS communication

- RA (MORPHOCS software) verifies the LRA platform certificate and signature to authenticate the LRA platform and the certificate request.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**29 / 85**

Document Title

CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

- The RA (MORPHOCS software) transmits auth certificate request, signed file, to the Citizen Sign CA (ID-NOMIC software).

- Citizen Sign CA (ID-NOMIC software) verifies the RA (MORPHOCS software) certificates and signature.

- Citizen Sign CA (ID-NOMIC software) transmits the auth certificate to the RA (MORPHOCS software).

- RA (MORPHOCS software) transmits the auth certificate to the LRA platform and inserts the certificate in the identity smart card under the control of citizen.

In both cases, Citizen has to change the current PIN code of the identity smart card. The operation is done with the LRA platform at certificates insertion or at identity card delivery.

All the operations, performed in the OA trust center, are protected in a manner to guarantee the integrity, confidentiality (when it is necessary) and origin of transmitted data and secure link between RA, CA and LRA.

The technical mechanisms are described in section ANNEX 5: Technical security mechanisms of this CPS.

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

No stipulation.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

As soon as the LRA Operator gets information meaning that citizen auth certificate has been inserted inside the identity card, then LRA Operator requires the citizen to check and verify the information contained in the "Subject DN" (Cf. § 3.1.1.2) of the citizen auth certificate.

If the citizen agrees with the information then the certificate his accepted.

4.4.2. Publication of the Certificate by the CA

The auth certificate is not published by PS.

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 CA key pair is used to sign certificates and corresponding CRL for citizen managed by the CA.

The citizen key pair is used to be authenticated in control access application (to consult document, to have access to service …).

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**30 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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 citizen's identity according to the present CPS and the CPS supported by the RCA.

4.6. Certificate Renewal with Same Keys

This section addresses auth certificate generation without changing the public key or any other information in the certificate. This operation is not allowed for auth certificate.

4.7. Certificate Renewal with Different Keys

This section addresses auth certificate generation changing the key pair.

The procedures that apply are the same than the ones for initial auth certificate generation.

If the citizen has broken or lost its identity smart card, then the citizen has to request a new identity smart card using the same procedure defined in section 6.4.

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 not allowed for auth certificate.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

An auth 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 CA is revoked;
- Change in the key length size recommendation coming from national agencies or international standard institute;
- DN information filled incorrectly;
- The private key corresponding to the auth certificate has been lost or compromised;
- The citizen has used a wrong DN in his initial auth certificate request.

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

PMA will request the revocation of Albanian Citizen ID Auth CA if the CA is compromised. In this case, the Albanian Citizen ID Auth CA will request the revocation of all en entity certificate belonging to the CA. Examples of circumstances that invalidate the binding are:

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**31 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

- The private key corresponding to the CA certificate has been lost or compromised;

In case of Albanian Citizen ID Auth CA compromision, PMA will trigger the following steps:

- Stop generation of Auth certificates
- Communication with Ministry of Interior
- Communication to the third parties about the CRL signed with the compromised Auth CA as non trusted
- Auth CA is revoked and all the Auth certificates generated with this CA
- Schedule and run a new key ceremony for a new Auth CA
- Sign the last Auth CA CRL with the new Auth CA and publish this last CRL
- Communication to all citizen having those revoked 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 certificates with the new CA

4.9.2. Origin of Revocation Request

On PMA request or MoI request, Albanian Citizen ID Auth CA has authority to make revocation requests for the following reasons:

- The CA is revoked;
- Change in the key length size recommendation coming from national agencies or international standard institute;
- DN information filled incorrectly;
- The private key corresponding to the auth certificate has been lost or compromised ;
- The citizen has used a wrong DN in his initial auth certificate request.

On RA/LRA request, Albanian Citizen ID Auth CA has authority to make revocation requests for the following reasons:

- DN information filled incorrectly;
- The private key corresponding to the auth certificate has been lost or compromised ;
- The citizen has used a wrong DN in his initial auth certificate request.

On Citizen request, Albanian Citizen ID Auth CA has authority to make revocation requests for the following reasons:

- DN information filled incorrectly;
- The private key corresponding to the auth certificate has been lost or compromised.

4.9.3. Procedure for Revocation Request

There are several ways to request the revocation of sign certificate:

- By phone

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**32 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

- o The citizen called an identified phone number (see phone number at 1.5.2)
- o The Revocation Officer will ask for identification and authentication information before to proceed to revocation

- By physical presence in the Aleat Service Point (nearest CSO at your Municipality/Commune) during working hours
  - o The Revocation Officer will ask for identification and authentication information before to proceed to revocation

RA or LRA authenticates authorized revocation request for a auth certificate (Cf. 3.3.4).

RA (OA, MORPHOCS software) transmits the revocation request to the CA (OA, ID-CA of ID-NOMIC software)) for the identified auth certificate.

Citizen Auth CA (OA, ID-CA of ID-NOMIC software) verifies the RA (OA, MORPHOCS software) certificates and signature.

CA revokes the auth certificate.

Citizen is notified by SMS when auth certificate is revoked

All the operations, performed in the OA trust center, are protected in a manner to guarantee the integrity, confidentiality (when it is necessary) and origin of transmitted data and secure link between RA, CA and LRA.

The technical mechanisms are described in the section 14 of this CPS

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 CA, the OA makes best endeavours to ensure that this service is not unavailable for longer than a maximum period of time of twenty four (24) hours.

The CA (OA, ID-CA of ID-NOMIC software) generates a new CRL every 24 hours.

4.9.6. Revocation Checking Requirements for Relying Parties

The 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 present CPS, whose authenticity cannot be guaranteed to the standards of this CPS.

4.9.7. CRL Issuance Frequency

CRL are issued every 24 hours. They are rendered available 24 hours per day, 7 days a week, by the PS.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**33 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

4.9.8. Maximum Latency for CRLs

The maximum delay between the time when an auth certificate is revoked by the Albanian Citizen ID Auth CA and the time when revocation information is available to relying parties is no longer than 24 hours.

The maximum delay between the generation of the CRL and the publication is 1 hour.

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.
OCSP service is available at the following URL: https://www.ealeat.al/ocsp/albanian-citizen-id-auth-ca-04.

4.10.2. Service Availability

The PS availability is described in section 2.3.
OCSP service is available 24/24, 7 days a week. In case of OCSP unavailability, CRL is published on PS. CRL can be found at the following location: https://www.aleat.al/csp/albanian-citizen-id-auth-ca-04.crl.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**34 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

The OCSP response is sent by a OCSP Token signed by a key issued from OCSP profile in the same CA than certificate tested.

4.10.3. Optional Features

The OCSP responder requests and answers are logged. Those logs are kept for 1 year.

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.

When the PMA ends its relationship with OA, then the OA will 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 citizen or a CA key is escrowed by a third-party or any else other entity.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**35 / 85**

Document Title

CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. Physical Controls

The CA physical and environmental security policy for systems concerned with certificate generation, CA 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

The OA is materialized by different separated physical locations. The E-ID PKI and personalization platform are located within dedicated area in different OA's locations.

The E-ID PKI and personalization components (rack servers, ID-CA ID-NOMIC software and Luna Network HSM) are located in a dedicated area and dedicated cabinet. MORPHOCS software is in another secure area.

The trusted role use and/or manage the E-IK PKI and personalization platform operates with dedicated OA's computer.

The OA's locations for E-ID PKI and personalization platform don't have any windows.

5.1.2. Physical Access

Access to the E-ID PKI and personalization plat-form requires positive authentication process based on access with strong authentication, using a combination of badges and biometrics (means "what you have" and "what you are").

All OA employees own badges that allow them to access OA security perimeter in accordance with their privileges. Only OA employees that have trusted roles are cleared to access the key ceremony room and E-ID PKI and personalization platform room.

All external person involved in E-ID PKI and personalization may be cleared to enter the key ceremony room after positive authentication performed by Security Officer. External person are always escorted by OA employee, when they are physically inside OA security perimeter.

All physical access rights are defined in a way not to allow a single person to have access to any sensitive data or proceed to a sensitive operation.

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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**36 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

5.1.4.   Water Exposures

OA ensures that E-ID PKI and personalization platform are protected in a way that minimize 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.

HSM are always stored in the E-ID PKI cabinet or in a safe in the OA trust center. Server and computer are always stored in closed location in OA trust center (when there are set in production). Only the System administrator can have access and prepare the server and the computer. A server and a computer are always locked with login and password only known by the System administrator.

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.   Documents Protection

The blank identity cards and the personalized identity cards are monitored and protected with the following procedures and work orders in the central site:

- OPS-PR-017 Blank documents Reception

    o Reception of the ID Card Blank document from Supplier.

- OPS-PR-019 Document transfer to Operational Vault

    o Transfer of ID Card from Vault to Dispatch.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**37 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

- OPS-PR-037 Allocation and Dispatch Stock Management

    o Transfer of ID Card from Dispatch to Production with the ID Card quantities (and contain Form01-Worklist of production unit, from Dispatch - Production - CQC - Dispatch, signed between each physical hand over).

- OPS-PR-018 Personalization of blank documents

    o Production of the ID Card + handover from production operator to CQC signed.

- OPS-PR-039 Control Quality Check of Personalized Documents

    o Quality control (CQC) + handover from CQC Operator to Dispatch signed.

- OPS-PR-038 Sending the documents to status Distribution

    o Physical and electronic transfer of the ID Card in Status ready for the shipment (Electronic confirmation from Dispatch with Package closed and weight quantities confirmation by the system).

- OPS-PR-020 Sending the documents from Dispatch to Shipment

    o Shipment of the ID Card to the CSO Office.

- OPS-PR-015 ID Documents Shipment Process

    o Inventory of ID Card in Central Site (Vault, Dispatch, CQC and Production)

The personalized identity cards are monitored and protected with the following procedures and work orders in the CSO:

- OPS-EN-009 Post Sending and Receiving process and reporting

    o At the ID Card reception in the CSO office, the operator check that the delivery note corresponds with the Quantities sent from Aleat Central Site.

- OPS-EN-005 ID Card Distribution, Lost Receipt, Inventory and Reporting

    o In §n, Monthly and Semestral inventory of the ID Card in the CSO.

- OPS-EN-014 ID Card and Passport Invalidation procedures and reporting

    o Invalidation of the ID Card when returned from citizen or not collected after more than 1 year of production.

5.1.8. 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:

- Server: the server 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;

- 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;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**38 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

- Smart card: all the content of the smart card is deleted with logical function provided by the administration tools of the smart card. Then, the chip of the smart card is taken off from the smart card and broken in several pieces;

- 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 ;

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

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 auth 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.

5.1.9. Off-Site Backup

The back-up is composed of the following data:

- Back-up of the private key of the RCA, CA certificate distribute to the Security Officer on the Backup HSM;

- Back-up of the certificate of the RCA, CA, on CD-ROM to distribute to the Security Officer;

- 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;

- Back-up of the database of the E-ID PKI platform (Refer to § 5.4.1);

- Back-up of citizen PUK code;

- Archive data (refer to § 5.5).

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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**39 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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 2: description of trusted roles 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 sensitive operation is:

- Auth certificate generation: one LRA Operator;

- CA activation: see section § 6.2.8;

- Auth certificate revocation: one LRA Operator or one E-DI PKI Operator;

- Personalization identity smart card: one E-DI PKI Operator;

- Unblock identity smart card with PUK code: one LRA Operator and one E-DI PKI Operator.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**40 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

5.2.3. Identification and Authentication for Each Role

Identification and authentication of 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 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 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.

The identification and authentication of the person who have privileges on E-ID PKI is done during TLS authentication between trusted role and E-ID PKI platform. Persons with trusted roles on E-ID PKI platform have certificate on a dedicated smart card.

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

OA 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. OA 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. OA 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. OA 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 CA personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the CA operations. The CA 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. CA asks the candidate to provide past convictions and turn down

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**41 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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

PMA and OA ensure that all personnel performing duties with respect to the operation of a CA receive comprehensive training in:

- LRA and OA security principles and mechanisms;

- Software versions in use in the E-ID PKI system;

- 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 CA 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

CA 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 CA functions operations according to the same requirements as defined in section 3.

5.3.8. Documentation Supplied to Personnel

The CA makes available to its personnel the present 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 E-ID PKI and personalization platform, the logs include, but are not limited to, the following events:

- Operating System start-up and shutdown;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**42 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

- o Log by System administrator in a log book each time that a server or a computer is set in production (initial or after a crash);
- o Log by server and computer in current uses;
- E-ID PKI and personalization application start-up and shutdown;
  - o Log by System administrator in a log book each time that a server or a computer is set in production (initial or after a crash);
  - o Log by server and computer in current uses;
- Attempts to create, remove, set passwords or change the system privileges of the privileged users (Trusted Roles);
  - o Log by System administrator in a log book each time that a server or a computer is set in production (initial or after a crash);
  - o Log by server and computer in current uses;
- Changes to CA certificate and keys (insert key cf. 6.2.6);
  - o Log by Security Officer in a log book;
  - o Log by E-ID PKI software and HSM in current uses;
- Changes to certificate creation policies (e.g., validity period);
  - o Log by Security Officer in a log book;
  - o Log by E-ID PKI software in current uses;
- Login and logoff attempts, both successes and failures;
  - o Log by server, firewall and computer in current uses;
- Authorized attempts at network access to the E-ID PKI and personalization platform;
  - o Log by server, firewall and computer in current uses;
- Unauthorized attempts to access system files;
  - o Log by server, firewall and computer in current uses;
- Successful and failed read and write operations on the repository;
  - o Log by server and computer in current uses;
- Failures during the generation of a certificate;
  - o Log by E-ID PKI software in current uses;
- Certificate lifecycle management-related events (e.g., certificate applications, issuance, revocation and renewal);
  - o Log by E-ID PKI software and HSM in current uses;
  - o This log are manually copy, by System Administrator, on a dedicated tape for back-up purpose (Cf. 5.1.8);
  - o Kind of identification document presented by the certificate applicant
  - o All event logs related to the preparation of SSCD
- Identity smart card and associated lifecycle management-related events:

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**43 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

- o Log by personalization software in current uses;
- Removing or replacing the cryptographic hardware security module in its assigned secure storage location;
  - o Log by System Administrator in a log book;
  - o Log by Security Officer in a log book;
- Activation and deactivation of the cryptographic hardware module;
  - o Log by Security Officer in a log book;
  - o Log by E-ID PKI software and HSM in current uses;
- Cloning, for disaster recovery or any other purpose, the private keys contained in the cryptographic hardware security module;
  - o Log by Security Officer in a log book;
- Physical access to the enclave;
  - o Log by access system control;
  - o OA register (id badge, name, first name and date) in log book the distribution of badge that allow access to the OA;
- Hardware errors, equipment failures, power events, fire, smoke, or water alarms;
  - o Log by system Administrator.

5.4.2. Frequency of Processing Log

Audit logs are examined on at least a weekly basis for significant security and operational events. In addition, audit logs are reviewed for suspicious or unusual activity in response to alerts generated based on E-ID PKI and personalization platform.

Audit log processing consists of a review of the audit logs and documentation for all significant events in an audit log summary. Audit log reviews include a verification that the log has not been tampered with, an inspection of all log files stored in central log repository and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also documented.

5.4.3. Retention Period for Audit Log

Records concerning 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.

5.4.4. Protection of Audit Log

The log created by E-ID PKI and personalization platform 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 media (tape …), 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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**44 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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

There is a central server with syslog application that performed the audit collection.
The System administrator collects the log data, on tape, directly on the central server, computer and firewall that are located in the OA trust center (Cf. § 5.1.8).

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

When, there are suspected information in log, the System administrator try to solve the reason and alert the Security Officer. The Auditor checks the E-ID PKI's application events.

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;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**45 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

- RCA and CA Certificates, ARL: PMA and Security Officer safe on CD Rom;
- Certificates and revocation information: back-up events logs (Cf. § 5.4.1) System Administrator;
- 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 20 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 and tape can be copied on another media (same or different).

5.5.5. Requirements for Time-Stamping of Records

No stipulation.

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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**46 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

5.6. Key Changeover

5.6.1. 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 auth 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:
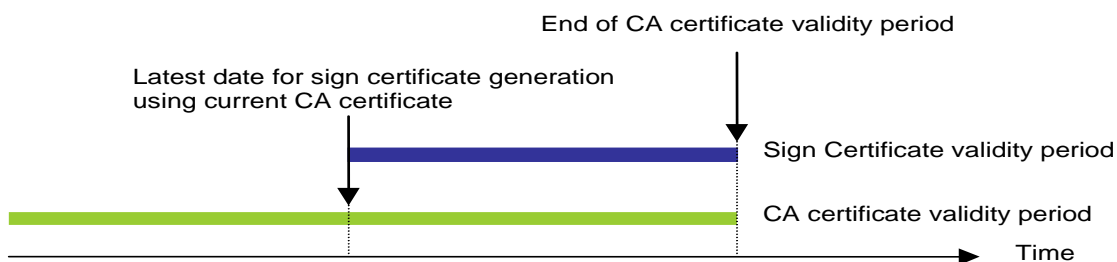
As soon as a new CA key pair is generated, only this new key can be used to sign "auth certificate" and associated CRL.

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.

When a new CA 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 CA key pair and the associated certificate signed by the current RCA (Cf. § 6.1). To sign the CA public key, it is necessary to insert the RCA private key in the HSM used for key ceremony (Cf. § 6.2.6);
- The new key is backed-up on Backup HSM (Cf. § 6.2.4);
- The old CA private key is destroyed (Cf. § 6.2.10) in the E-ID PKI's HSM platform;
- The new CA private key is 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. Citizen

The maximum validity period of an auth certificate is 3655 days. The end date of the auth certificate is aligned on the validity date of the identity card. When the citizen changes the current key to have new certificate, then the previous keys are destroyed in the smart card.

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**47 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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 be 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 Auth CA termination:
- Auth CA archives all audit logs and other records prior to termination;
- Auth CA destroys all its private keys upon termination;
- Archive records are transferred to an appropriate authority such as the Albanian Ministry of Interior;
- Auth CA uses means to notify the citizen to delete all trust anchors representing the RCA.
The details about the termination plan is indicated at § 9.10 in this document.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**48 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key Pair Generation

6.1.1.1. CA

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 Safenet Backup USB HSM.

6.1.1.2. Citizen

Citizen's key generation is performed by the identity smart card in the LRA office. The citizen activates its identity smart card and LRA Operator request identity smart card to generate a key pair.

6.1.2. Private Key Delivery to citizen

There is no delivery of private key to citizen because key are generated inside the identity smart card (Cf. § 6.1.1.2).

6.1.3. Public Key Delivery to CA

Citizen's public key is delivered securely to the CA (ID-CA of ID-NOMIC) for certificates issuance. The LRA Operator request to the identity smart card to generate a Pkcs#10 file that contains the public key generated by the identity smart card. Then the Pkcs#10 file is securely transmitted during TLS communication between LRA platform and RA (Cf. § 4.2.2).

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. The Security Officer transmits the RCA and CA certificates to the System Administrator to be set in the PS server.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**49 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

6.1.5. Key Sizes

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

CA keys for the RSA algorithm are 2048 bits length using at minimum the SHA-256 hash function.

Citizen key for the RSA algorithm is 2048 bits length using at minimum the SHA-256 hash function.

6.1.6. Public Key Parameters Generation and Quality Checking

CA keys and citizen 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 citizen and CA are defined in the certificate profiles (refer to § 7.2). The CA key usage is set to allow private keys to only sign certificates and CRL. The citizen key usage is set to allow private key to only be authenticated in control access application (to consult document, to have access to service …).

These restrictions are 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

Citizen identity smart card and CA hardware security module is approved FIPS 140-2 level 2 and 3 or EAL 4+ certified, or higher.

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

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

A key contained in a Luna Network HSM can only be exported in a backup HSM (Cf. § 6.2.6).The key has to be destroyed in the HSM after the end of validity period of the CA key, therefore CA key is always under multiple controls.

6.2.3. Private Key Escrow

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

6.2.4. Private Key Backup

The citizen private signature keys are not backed 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 HSMs are made during key ceremony [2016_2000021244 - Citizen PKI - Key Ceremony 2016 v0.3.docx]. Backup HSM (s) are stored in a safe (refer to § 5.1.8) under the responsibility of Security Officer.

CA private key is back-up on 2 identical Luna backup HSM devices.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**50 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

6.2.5. Private Key Archival

Private citizen and CA keys 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 Interior;
- 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):
  - o Insert: Black USB token used to initialize the HSM (System Administrator);
  - o 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):
  - o Insert:
    - ▪ Initial Red USB token: Activation holder of Albanian Ministry of Interior;
    - ▪ Initial Blue USB token: Security Officer;
    - ▪ Black USB token: System Administrator and E-ID PKI Administrator.
  - o Export (Append case): Black USB token used to load the HSM (System Administrator).
  - o Export (Replace case):
    - ▪ Initial Red USB token: Activation holder of Albanian Ministry of Interior;
    - ▪ 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.

Citizen's key is stored in the identity smart card.

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).

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**51 / 85**

Document Title

CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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 Interior;
- Initial Blue USB token: Security Officer;
- Black USB token: System Administrator and E-ID PKI Administrator.

E-ID PKI software use CA private key to sign CRL and certificate.

Citizen's private key is activated with activation data associated to the identity smart card.

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 server or HSM, requires at least the following trusted roles and activation data:

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

Citizen's private key is deactivated after each operation using the identity smart card.

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 back-up HSM (Security officer).

Normally the key, contained in citizen identity smart card, are destroyed logically by LRA Operator each time citizen renew its certificate.

When the identity smart card can't be used longer by the citizen, the citizen transmits the identity smart card to the LRA. The LRA destroyed logically the key inside the identity smart cart and transmit the smart card to the OA. The OA destroys physically the identity smart card.

6.2.11. Cryptographic Module Rating

The CA cryptographic module is FIPS 140-2 level 2 and 3.

The identity smart card is EAL 4+ certified.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**52 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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 § 0.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1. CA

The CA certificate lifetime is 15 years.

The CA private key lifetime is 15 years.

6.3.2.2. Citizen

The auth certificate maximum lifetime is 3655 days. The end date of validity of the auth certificate is the end date of the citizen identity card.

The auth certificate's private key maximum lifetime is 3655 days. The end date of validity of the auth certificate's private key is the end date of the citizen identity card.

6.3.2.3. Auth OCSP

The auth OCSP certificate maximum lifetime is 5 years.

The auth OCSP private key lifetime is 5 years.

6.4. Identity Smart Card and Activation Data

6.4.1. Identity Smart Card delivery process

The citizen is in charge of requesting an identity smart card.

The citizen provides the following information, during the face to face meeting with LRA Operator, to the LRA:

- Birth Certificate;
- Albanian ID number.

LRA Operator do the following action:

- Verifies the information provided by the citizen. The LRA Operator verifies the Albanian ID number using the national Albanian identity register;
- Takes biometrics (photo and fingerprints) to the citizen;
- Transmits the identity smart card request with citizen's biometrics to the OA. The communication is mutually authenticated and protected in confidentiality and integrity.".

The OA (personalization software and E-ID PKI Operator) personalizes the identity smart card with the information transmitted by the LRA.

The OA blocks the identity smart card with activation data that are the default PIN code (known by LRA and OA) and the citizen's fingerprint.

The OA transmits the identity smart card to the LRA who had registered the citizen.

The citizen has to retrieve its identity smart card in the LRA office.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**53 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

The LRA check that the fingerprint from the citizen match whit fingerprint contained in the identity smart card provided by the citizen or the delivered identity smart card to the citizen.

If the verification is successful, then the LRA give the identity smart card to the citizen. The citizen has to change the default PIN code. The operation is made with the LRA platform.

6.4.2. Activation Data Generation and Installation

For citizen, the generation of activation data used to activate auth certificate's private keys is made during the personalization of the identity smart card.

For an identity smart card, there are the following activation data:

- PIN code: this activation is defined by the citizen. This code is used to activate auth certificate's private keys contained in the identity smart card;

- PUK code: this activation data is defined by the OA. This code is used to unblock the identity smart card;

- Fingerprint's citizen: this activation data is set in the identity smart card. The fingerprint is used to block the use of the identity smart card before to be delivered to the citizen."

The first PIN code is a default PIN code defined by the OA.

The OA uses the default PIN code and citizen's PIN code to block the identity smart card.

The OA transmits the PIN code and the identity smart card to the LRA.

The citizen changes the default PIN code by its the PIN code during the personalization of the identity smart card with certificate.

6.4.3. Activation Data Protection

Activation data are protected from disclosure by the OA during the generation and until their transmission to LRA or citizen as described in the OA security policy. See the documents protection section 5.1.7.

Citizen has to protect in confidentiality its PIN code.

6.4.4. Other Aspects of Activation Data

When the identity smart card is blocked, then the citizen has to go the LRA to unblock its identity smart card.

The LRA operator transmit a "unblock request" to the OA (E-ID PKI Operator).

The E-ID PKI Operator unblock the identity smart card with PUK code and LRA platform.

The LRA check that the fingerprint from the citizen match whit fingerprint contained in the identity smart card provided by the citizen. If the verification is successful, then the LRA give the identity smart card to the citizen. The citizen has to change the default PIN code. The operation is made with the LRA platform.

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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**54 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

All the server and computer must under the control of the System administrator. The E-ID PKI Operator and E-ID PKI Administrator have simple user account with no Administration privilege. System Administrator has an account with Administration privilege on all the computer and server.

The computer for trusted role (LRA Operator …) 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 server for E-ID PKI and personalization platform respects the following rules:

- E-ID PKI and personalization software can only be set up in the E-ID PKI and personalization server stored in the dedicated cabinet;
- Only authorized data can be inserted in the server;
- E-ID PKI software can only be used authenticating the trusted role with certificate delivered by Technical CA (TLS protocol);
- Smart card that contains certificate delivered by Technical CA has to need a PIN and PUK code to be activated and unlocked;
- The smart card is under the responsibility of the trusted role. The trusted role doesn't communicate its smart card and the associated PIN code. The smart card is always under the control of the trusted roles.

The Backup HSMs are only connected to a computer dedicated to key ceremony or to the server that hosts the HSM. A Backup HSM key whose purpose is to be a "Backup HSM key" must never has been connected to anything else than a key ceremony computer or a E-ID PKI server hosting a HSM.

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**55 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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

The E-ID PKI and personalization platform are protected by firewalls. These firewalls only allow required network traffic. The firewall systems block all traffic through unused ports. Services which are not required for the E-ID PKI and personalization platform are denied by the firewalls.

Only network software which is necessary to the functioning of the E-ID PKI and personalization platform is used in the production network.

The network is managed according OA security policy. Configuration of network 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 but there is a NTP server used for the E-ID PKI and personalization platform.

System Administrator verifies every week that the time delivered by NTP server and used by E-ID PKI and personalization component is correct. If there is a difference between the time and date delivered by the NTP server and trusted source (radio, internet …) and E-ID PKI and personalization component, then System Administrator set the right time and date. He logs the event in the System administrator log book. If the difference is bigger than an hour, then System administrator inform Security Officer to elaborate corrective action. In this circumstance, if the difference could become a source of compromising (one year of difference for example) in the certificate and CRL life cycle, then certificate can be revoked.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**56 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. AUTH CA 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

Base certificate	Value
Version	2 (=version 3)
Serial number	Defined by Keyseed®
Key length	2048
Certificate duration	15 years
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 Auth CA
NotBefore	YYMMDDHHMMSS (date of certificate generation)
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	
policyIdentifiers				0.4.0.2042.1.2 (Normalized Certificate Policy requiring a secure cryptographic device)
policyQualifiers				n/a
CPSpointer				CPS URI: https://www.aleat.al/pdf/cps-citizen-root-ca.pdf or

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**57 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

				CPS URI: https://www.aleat.al/pdf/cps-citizen-root-ca-05.pdf
OID				n/a
Value				**n/a**
noticeRef				n/a
OID				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	X	FALSE	
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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**58 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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. 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. Citizen Auth Certificate Profile

7.2.1. Version Number

The Auth certificate is X.509 v3 certificates (populate version field with integer "2").

The certificate fields are those defined in the RFC 5280.

7.2.2. Certificate Extensions

Base certificate	Value
Version	2 (=version 3)
Serial number	Defined by ID-CA ID-NOMIC®
Key length	2048
Certificate duration	3655 days maximum with NotAfter = Identity Card End Date
Issuer DN	C = AL OI = NTRAL-K82018015V O = Aleat CN= Albanian Citizen ID Auth CA
Subject DN	C = AL CN=<FirstName LastName> Pseudo=<National ID> SN=PNOAL-<National ID>
NotBefore	YYMMDDHHMMSS (date of certificate generation)
NotAfter	YYMMDDHHMMSS (identity card end date)
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**

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**59 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

Select AKI Fields				**Key Identifier**
Basic Constraint	{id-ce 19}	**X**	**TRUE**	
CA				**False**
PathLengthConstraint				**n/a**
Certificate Policies	{id-ce 32}	**X**	**FALSE**	
policyIdentifiers				0.4.0.2042.1.2 (Normalized Certificate Policy requiring a secure cryptographic device)
policyQualifiers				n/a
CPSpointer				CPS URI: https://www.aleat.al/pdf/cps-citizen-auth-ca.pdf
OID				n/a
Value				**n/a**
noticeRef				n/a
OID				n/a
organization				n/a
noticeNumbers				n/a
explicitText				n/a
CRL Distribution Points	{id-ce 31}	**X**	**FALSE**	
distributionPoint				[1]Certificates Revocation List DistributionPoint Name of the distribution point : Complete Name : URI https://www.aleat.al/csp/albanian-citizen-id-auth-ca-04.crl or https://www.aleat.al/csp/albanian-citizen-id-auth-ca-05.crl
reasons				n/a
cRLIssuers				n/a
Extended Key Usage	{id-ce 37}	**X**	**FALSE**	
Server Authentication	1.3.6.1.5.5.7.3.1			**Clear**
Client Authentication	1.3.6.1.5.5.7.3.2			**Set**
email protection	1.3.6.1.5.5.7.3.4			**Clear**
Document signing	1.3.6.1.4.1.311.10.3.12			**Clear**
PDF Signing	1.2.840.113583.1.1.5			**Clear**
OCSPsigning	1.3.6.1.5.5.7.3.9			**Clear**
timeStamping	1.3.6.1.5.5.7.3.8			**Clear**
Code signing	1.3.6.1.5.5.7.3.3			**Clear**
Issuer Alternative Name	{id-ce 18}			n/a
Subject Alternative Name				n/a
Qualified Certificate Statement	1.3.6.1.5.5.7.1.3	**X**	**FALSE**	0.4.0.1862.1.5 (id-etsi-qcs-QcPDS) + URL of PDS: https://www.aleat.al/pdf/AleatPDS.pdf
Key Usage	{id-ce 15}	**X**	**TRUE**	

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**60 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

Digital Signature				**Set**
Non Repudiation				**Clear**
Key Encipherment				**Clear**
Data Encipherment				**Clear**
Key Agreement				**Clear**
Key CertSign				**Clear**
Key CRL Sign				**Clear**
Private Key Usage Period	{id-ce 16}			
Subject Key Identifier	{id-ce 14}	**X**	**FALSE**	
Methods of generating key ID				**Method 1**
privateInternetExtensions	AIA authorityInformation Access	**X**	**FALSE**	
	CA Issuer			https://www.aleat.al/csp/albanian-citizen-id-auth-ca-04.cer or https://www.aleat.al/csp/albanian-citizen-id-auth-ca-05.cer
	OCSP			https://www.ealeat.al/ocsp/albanian-citizen-id-auth-ca-04 or https://www.ealeat.al/ocsp/albanian-citizen-id-auth-ca-05
Other Extensions				n/a

7.2.3.   Algorithm Object Identifiers

See section 7.1.

7.2.4.   Name Forms

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

7.2.5.   Name Constraints

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

7.2.6.   Certificate Policy Object Identifier

See section 7.1.

7.2.7.   Usage of Policy Constraints Extension

See section 7.1.

7.2.8.   7.1.8 Policy Qualifiers Syntax and Semantics

See section 7.1.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**61 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

7.2.9. Processing Semantics for the Critical Certificate Policies Extension

See section 7.1.

7.3. CRL Profile

7.3.1. Version Number

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

CA shall issue the last CRL when all certificates in the scope of this CRL are expired or revoked.

CRL and last CRL are publicly available on the publication site (PS).

7.3.2. CRL and CRL Entry Extensions

Features of the CRL:	Duration (expressed in days): 7 days
	Periodicity of update : 24 hours
	CRL version (v1 or v2) : V2
	Issuer: C=AL
	OI=NTRAL-K82018015V
	O=Aleat
	CN=Albanian Citizen ID Auth CA
	Extensions : CRL Number + AKI + Expire Cert on CRL
	CRL Number : incremented 1 by 1
	Signature Algorithm:SHA256 RSA
	Hash Algorithm: SHA256
	Next Publication Date: generation date + 1 day
	Next Publication date for the last CRL : "99991231235959Z"
	http URL for publication : https://www.aleat.al/csp/albanian-citizen-id-auth-ca-04.crl or https://www.aleat.al/csp/albanian-citizen-id-auth-ca-05.crl

7.4. OCSP Profile

7.4.1. Version Number

The OCSP Auth certificate is X.509 v3 certificates (populate version field with integer "2").

The certificate fields are those defined in the RFC 5280.

The OCSP Auth does not use ArchiveCutOff extension.

When Auth CA certificate will expire, CA will compute the last OCSP answer for each and every issued certificate (wether revoked or not), with the "nextUpdate" filed set to "99991231235959Z".

7.4.2. Certificate Extensions for OCSP

Base certificate	Value
Version	2 (=version 3)
Serial number	Defined by ID-CA ID-NOMIC®

Reference OPS-OP-024	Type **Document**	Classification **Public**	Owner **OP**	Version **13**	Date **06.12.2021**	Page **62 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

Key length	2048
Certificate duration	5 years
Issuer DN	C = AL OI = NTRAL-K82018015V O = Aleat CN= Albanian Citizen ID Auth CA
Subject DN	C = AL OI = NTRAL-K82018015V O = Aleat CN = <System Name>
NotBefore	YYMMDDHHMMSS (date of certificate generation)
NotAfter	YYMMDDHHMMSS (date of certificate generation + 5 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				**Key Identifier**
Basic Constraint	{id-ce 19}	X	FALSE	
CA				**False**
PathLengthConstraint				**n/a**
Certificate Policies	{id-ce 32}	X	FALSE	
policyIdentifiers				1.3.6.1.4.1.42090.10.1.2
policyQualifiers				n/a
CPSpointer				CPS URI: https://www.aleat.al/pdf/cps-citizen-auth-ca.pdf
OID				n/a
Value				n/a
noticeRef				n/a
OID				n/a
organization				n/a
noticeNumbers				n/a
explicitText				n/a
CRL Distribution Points	{id-ce 31}	X	FALSE	
distributionPoint				[1]Certificates Revocation List DistributionPoint Name of the distribution point : Complete Name : URI https://www.aleat.al/csp/albanian-citizen-id-auth-ca-04.crl or https://www.aleat.al/csp/albanian-citizen-id-auth-ca-05.crl
reasons				n/a

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**63 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

cRLIssuers				n/a
Extended Key Usage	{id-ce 37}	X	TRUE	
Server Authentication	1.3.6.1.5.5.7.3.1			**Clear**
Client Authentication	1.3.6.1.5.5.7.3.2			**Clear**
email protection	1.3.6.1.5.5.7.3.4			**Clear**
Document signing	1.3.6.1.4.1.311.10.3.12			**Clear**
PDF Signing	1.2.840.113583.1.1.5			**Clear**
OCSPsigning	1.3.6.1.5.5.7.3.9			**Set**
timeStamping	1.3.6.1.5.5.7.3.8			**Clear**
Code signing	1.3.6.1.5.5.7.3.3			**Clear**
Issuer Alternative Name	{id-ce 18}			n/a
Subject Alternative Name				n/a
Qualified Certificate Statement	1.3.6.1.5.5.7.1.3	X	FALSE	n/a
Key Usage	{id-ce 15}	X	TRUE	
Digital Signature				**Set**
Non Repudiation				**Set**
Key Encipherment				**Clear**
Data Encipherment				**Clear**
Key Agreement				**Clear**
Key CertSign				**Clear**
Key CRL Sign				**Clear**
Private Key Usage Period	{id-ce 16}			n/a
Subject Key Identifier	{id-ce 14}	X	FALSE	
Methods of generating key ID				**Method 1**
privateInternetExtensions	AIA authorityInformation Access	X	FALSE	
Other Extensions				n/a

7.4.3.   Algorithm Object Identifiers

See section 7.3.

7.4.4.   Name Forms

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

7.4.5.   Name Constraints

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

7.4.6.   Certificate Policy Object Identifier

See section 7.3.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**64 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

7.4.7. Usage of Policy Constraints Extension

See section 7.3.

7.4.8. 7.1.8 Policy Qualifiers Syntax and Semantics

See section 7.3.

7.4.9. Processing Semantics for the Critical Certificate Policies Extension

See section 7.3.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**65 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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) CA to be operated by OA under the CA 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) CA to be operated by OA under the CA 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 determines 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 CA CPS and the OA's security policy.

The purposes of a compliance audit are to verify that a component operates in accordance with the 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 [Naming Document];
- 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;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**66 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

- Activation data (refer to § 6.4.1) are correctly distributed and managed by the right trusted roles;

- Back-up files still exist and correctly protected (refer to § 5.1.8.1);

- 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 CA is not complying with its obligations set forth in the CA CPS. When such a determination is made, the PMA may suspend or direct to stop affected CA and may request that corrective actions be taken which allow to continue operation of the operation of the noncompliant CA. When the compliance auditor finds a discrepancy between how the CA 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 CA 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 CA, to revoke a certificate issued by the CA, 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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**67 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

Defined by PMA.
There is no specific fee for certificate issuance except the citizen has to have an Identity Card.
There no certificate renewal.

9.1.2. Certificate Access Fees

The CA PS is free access on the internet for relying parties and for subjects.

9.1.3. Revocation or Status Information Access Fees

The CA PS including OCSP is free access on the internet for relying parties and for subjects.

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 CA duties.

9.2.3. Insurance or Warranty Coverage for End-Entities

If there is damage for a relaying party due to Albanian Ministry of Interior or OA fault, Albanian Ministry of Interior 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

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

- Records and archive;

- Personal identity data;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**68 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

- CA PKI private keys;

- CA Audit result and reports;

- CA Disaster recovery plans;

- Contractual arrangements with OA;

- OA trust center security policy;

- Part of the CA CPS defined as confidential,

- Revocation reason;

- Identity smart card activation data;

- Citizen's fingerprint;

- PIN code;

- PUK code.

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 Citizen and CA are:

- Naming document;

- Citizen's fingerprint;

- Citizen's face photography;

- Revocation request form;

- Certificate 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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**69 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

9.4.4. Responsibility to Protect Private Information

E-ID PKI and personalization 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 Interior requirements on the privacy data protection.

9.4.5. Notice and Consent to Use Private Information

All private information coming from E-ID PKI and personalization 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 Interior 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, auth certificate and revocation information that are issued by the CA.

The citizen retains all intellectual rights it has on information contained in the auth certificate delivered by Citizen Auth CA and for which he/she is the proprietary (fingerprints …).

9.6. Representations and Warranties

9.6.1. PMA Representations and Warranties

PMA define the present CPS. PMA establishes that CA 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 and in the corresponding CPS, are implemented as applicable to deliver and manage auth certificate.

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

9.6.2. 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);

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**70 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

- 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 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 CA 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);

- Protect identity smart card and associated activation data;

- Document their internal procedures to complete global CPS and its security policy;

- Respect total or part of agreements that binds it to the PMA.

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 files 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;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**71 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

- 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. E-ID PKI Administrator

E-ID PKI Administrator obligations are:

- Respect their obligation regarding the function they have to perform (as specified in Annex 11 and in the present CPS);
- Respect the present CPS;
- Protects the smart card and the associated PIN code;
- Protects the activation data and the associated PIN code;
- Conduct application audit on E-ID PKI and personalization platform;
- Manage and deliver technical certificate for trusted roles;
- Respect the OA security policy.

9.6.3.4. E-ID PKI Operator

E-ID PKI Operator 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 smart card and the associated PIN code;
- Revoke certificate on PMA request;
- Unblock identity smart card on LRA request;
- Protects identity smart card and corresponding activation data;
- Respect the OA security policy.

9.6.4. RA Representations and Warranties

The RA has the responsibility to:

- Submit accurate and complete information to the CA;
- Nominates and identifies LRA;
- 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 CA services that the OA performed;
- Respect the CA CPS.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**72 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

9.6.5. LRA Representations and Warranties

The LRA has the responsibility to:

- Submit accurate and complete information to the RA;
- Keep secret activation data;
- Alert and notify RA for revocation request;
- Protect identity smart card and associated activation data;
- 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 CA services that the OA performed;
- Respect the CA CPS.

9.6.6. Citizen Representations and Warranties

The citizen has the responsibility to:

- Submit accurate and complete information to the LRA;
- Keep secret its activation data (PIN code);
- Alert and notify LRA for revocation request;
- Respect the CA CPS.

9.6.7. Representations and Warranties of Other Participants

9.6.7.1. 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 CA services only guarantees the identification and authentication of the citizen with auth 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 present 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 present CPS requirements and principles, for the compliance audit for the present CA CPS.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**73 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

CA is responsible for any damage caused to relying parties because of improperly operating of the CA CPS.

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

9.10. Term and Termination

9.10.1. Term

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

CA has a termination plan. The termination plan document reference is OPS-OP-065

Before to terminate, CA will inform the Albanians citizen, the Ministry of Interior and the different eServices providers like the bank. CA will also inform the relevant authorities like LSTI, The Albanian MOI, the supervisory body like AKCE.

CA will update its publication server to inform all parties about the termination.

CA will stop the authorization given to any subcontractors.

Before to terminate, CA will see with the MOI to whom transfer its obligation (required evidences) for the maintenance of TSP operation.

Before to terminate CA will destroy all the secret keys belonging to the CA in order to avoid the retrieval of those secret keys.

Before to terminate, CA will arrange (if it will be possible) with the Ministry of Interior to whom transfer the CA trust services.

Before to terminate, CA will transfer its obligations to make available its public key to a relying parties defined by the Ministry of Interior.

9.10.3. Effect of Termination and Survival

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

RCA and CA cannot keep on delivering electronic certificate referring to the CPS. End of validity of the 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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**74 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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 CA.

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.

As the OID of this CPS is registered inside the certificates generated by the CA, any evolution of this CPS, having a major impact on the certificates already issued, must be reflected by an evolution of the OID in order that the subjects can clearly distinguish which certificates correspond to which 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 Interior and OA contains a dispute resolution clause.

9.14. Governing Law

The applicable laws that govern the CA 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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**75 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**76 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**77 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

10.3. Activation data delivery form

- Person who receive activation data:
  - o Date:
  - o Name;
  - o First name;
  - o Telephone;
  - o Address;
  - o Type of activation data ;

Signature of the Activation data holder

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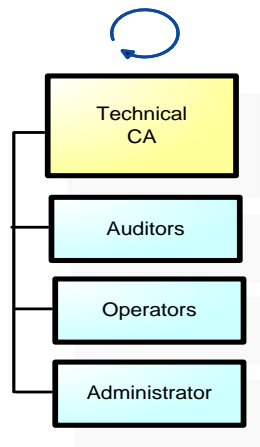 - o Telephone;
  - o Address.

Signature of Security Officer

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**78 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

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 perform RCA and CA initial key ceremony	Using Keyseed® software
E-ID PKI Operator (*Aleat System Operator*)	RA Operator certificate on dedicated smart card	Revoke Auth certificates. Those certificates are revoked using the Citizen Auth CA. Audit PKI events.	Using ID NOMIC ID CA software.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**79 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

Revocation Officer	RA Operator	Revoke Auth certificates. Those certificates are revoked using the Citizen Auth CA Portal.	Using IDEMIA CS software.
System Auditor (Aleat Quality & Investigation 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. Albanian trusted roles

11.2.1. Ministry of Interior

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

11.2.2. Civil Registry Offices

Trusted roles	Certificates and/or tools	Function	Comments
LRA Operator (Revocation Officer or Registration Officer)	NA	LRA Operator	Sign and transmits E-Government access form
		LRA platform	Use the LRA platform to transmit technical certificate and revocation request to the OA.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**80 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

12. ANNEX 3: MANAGEMENT OF TRUSTED ROLES CERTIFICATES

12.1. Delivery of technical certificates to trusted roles

When a trusted role needs a technical certificate, he/she receives it from another trusted role (refer to § 11). The section 11 indicates which roles can deliver technical certificate with which technical CA. the section 11 indicates also which software is used to signs technical certificates.

The authorization and authentication of the person who has a trusted role is done by another trusted role as describes in section 3.2.3.3.

When an authorized person, with a trusted role, needs a technical certificate (refer to § 11), this certificate is delivered by Security Officer or the E-ID PKI Administrator (named "master trusted role" for explanation in this paragraph). The following procedures, in this paragraph, are only explained with "master trusted role" and a trusted role.

"Master trusted role" has to use the right technical certificate on a dedicated smart card to issue other technical certificate (refer to § 11) for trusted roles.

"Master trusted role" uses the dedicated computer in the OA trust center.

"Master trusted role" uses the right smart card and technical certificate with a browser to be authenticated on the E-ID PKI software.

"Master trusted role" generates the key pair on a smart card. This smart will be distributed to the trusted role.

"Master trusted role" creates the certificate requests and transmits the public key to the technical CA with Trust.Center® software interface.

"Master trusted role" uses the right technical CA to sign the certificate.

"Master trusted role" then store the certificate on the same smart card.

"Master trusted role" chooses a PUK code for the smart card.

"Master trusted role" distributes the smart card to the trusted role.

Trusted role chooses a PIN code.

The trusted role and the "Master trusted role" sign the Trusted roles certificate delivered form (Cf. § 10.2).

12.2. Revocation of a technical certificates delivered to trusted roles

Revocation of a technical certificate is also done by the "Master trusted role".

"Master trusted role" has to use the right technical certificate on a dedicated smart card to revoke other technical certificate (refer to § 11) for trusted roles.

"Master trusted role" uses the dedicated computer in the OA trust center.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**81 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

"Master trusted role" uses the right smart card and technical certificate with a browser to be authenticated on the E-ID PKI software.

The "Master trusted role" revoke the technical certificate with E-ID PKI software functions.

12.3. Renewal of technical certificates for trusted roles

The renewal of technical certificate is the done by "Master trusted role".

The authorization and authentication of the person who has a trusted role is done by another trusted role as describes in section 3.2.3.3.

When an authorized person, with a trusted role, needs a new technical certificate (refer to § 11), this certificate is delivered by "Master trusted role". The following procedures, in this paragraph, are only explained with the role "Master trusted role" and trusted role.

There is tow choice for the smart card of the trusted role:

- Same smart card: trusted role will keep the same smart card. Before to use the smart card, the "Master trusted role" has to revoke the technical certificate (refer to § 12.2) and delete the key pair on the smart card. "Master trusted role" keep the same PUK code and trusted role keep the same PIN code ;

- New smart card: trusted role will have a new smart card. The "Master trusted role" has to has to revoke the technical certificate (refer to § 12.2) and delete the key pair on the smart card. Then "Master trusted role" has to destroy the old smart card (refer to § 5.1.7). After the generation of the generation of the new certificate on the new smart card, "Master trusted role" has to choose a PUK code and trusted role has to choose a new PIN code.

"Master trusted role" has to use the right technical certificate on a dedicated smart card to issue other technical certificate (refer to § 11) for trusted roles.

"Master trusted role" uses the dedicated computer in the OA trust center.

"Master trusted role" uses the right smart card and technical certificate with a browser to be authenticated on the E-ID PKI software.

"Master trusted role" generate new key pairs on the smart cards provided by the trusted role or on new smart cards.

"Master trusted role" create certificate requests and transmit public keys to the technical CA using E-ID PKI software.

"Master trusted role" use the appropriate technical CA to sign certificates.

"Master trusted role" store generated certificates on the smart cards.

12.4. Protection of smart cards

All trusted role's technical certificates and corresponding private keys are stored in dedicated smart cards with PIN codes to activate them and PUK codes to unblock them.

The PUK code could be the same for all the smart card, but it is recommended to have one PUK code per smart card. The PIN code is associated to one smart card. There is a different PIN code for each smart card.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**82 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

When the smart card is not used by the trusted role, then the trusted role has to protect the smart and the associated PIN code in confidentiality and integrity. Trusted role never let the smart card in the smart card reader of the computer when trusted role is not in front of the used computer.

"Master trusted role" has to protect the PUK code in integrity and in confidentiality.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**83 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

13. ANNEX 4: 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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**84 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

14. ANNEX 5: TECHNICAL SECURITY MECHANISMS

The technical security mechanisms to secure certificate issuance and certificate revocation are summarized in this section.

- Auth Certificate Issuance (Post Issuance)

    o LRA operator identifies and authenticates with his/her identity card auth certificate to LRA workstation

    o Communication flow between LRA and RA is protected in confidentiality and integrity with the use of TLS certificate generated by Aleat Technical CA

    o Communication flow between LRA and CA central site (VPN Gateway) is protected in confidentiality and integrity with VPN IPsec

    o Certificate request is signed for integrity protection with the citizen private key

    o Communication flow between RA and CA is protected in confidentiality and integrity with the use of TLS certificate generated by Aleat Technical CA

    o The certificate issuance message sends by RA to CA is signed with certificate generated by Aleat Technical CA

- Auth Certificate Issuance (At Identity Card production)

    o Identity Card Request Registration

        ▪ LRA operator identifies and authenticates with his/her identity card auth certificate to LRA workstation

        ▪ Communication flow between LRA and RA is protected in confidentiality and integrity with the use of TLS certificate generated by Aleat Technical CA

        ▪ Communication flow between LRA and CA central site (VPN Gateway) is protected in confidentiality and integrity with VPN IPsec

    o Identity Card Production

        ▪ Certificate request filled with citizen information is signed for integrity protection with dedicated private key generated by RA (MorphoPerso KPS)

        ▪ Communication flow between RA and CA is protected in confidentiality and integrity with the use of TLS certificate generated by Aleat Technical CA

        ▪ The certificate issuance message sends by RA to CA is signed with certificate generated by Aleat Technical CA

- Auth Certificate Revocation

    o LRA or RA operator identifies and authenticates with his/her identity card auth certificate to RA portal

    o Communication flow between RA portal and RA is protected in confidentiality and integrity with the use of TLS certificate generated by Aleat Technical CA

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-024	**Document**	**Public**	**OP**	**13**	**06.12.2021**	**85 / 85**

Document Title
CITIZEN AUTH CA CERTIFICATION PRACTICE STATEMENT

- o Communication flow between LRA and CA central site (VPN Gateway) is protected in confidentiality and integrity with VPN IPsec

- o Communication flow between RA and CA is protected in confidentiality and integrity with the use of TLS certificate generated by Aleat Technical CA

The revocation message sends by RA to CA is signed with certificate generated by Aleat Technical CA.

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