

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	1 / 81
Document Title ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

REPUBLIC OF ALBANIA

Production & Distribution of Identity Documents & Biometric Passports



ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	2 / 81

Document Title

ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

TABLE OF CONTENTS

1. INTRODUCTION.....	11
1.1. Overview	11
1.2. Document name and Identification	11
1.3. PKI Participants.....	12
1.3.1. Aleat Policy Management Authority (PMA).....	12
1.3.2. Root Certificate Authority (RCA)	12
1.3.3. Certification Authorities (CA).....	13
1.3.4. Registration Authority (RA)	13
1.3.5. Operational (OA)	13
1.3.6. Local Registration Authority (LRA).....	13
1.3.7. Publication Service (PS)	14
1.3.8. System	14
1.3.9. Other Participants	14
1.4. Certificate Usage.....	14
1.4.1. Appropriate Certificate Uses	14
1.4.2. Prohibited Certificate Uses	14
1.5. Policy Administration	15
1.5.1. Organization Administering the Document	15
1.5.2. Contact Person	15
1.5.3. Person Determining CPS Suitability for the Policy	15
1.5.4. CPS Approval Procedure	15
1.6. Definitions and Acronyms.....	15
1.6.1. Definitions	15
1.6.2. Acronyms	18
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES	19
2.1. Repositories	19
2.2. Publication of Certificate Information.....	19
2.3. Time or Frequency of Publication	19
2.4. Access Controls on Repositories	20
3. IDENTIFICATION AND AUTHENTICATION	21
3.1. Naming	21
3.1.1. Type of Names.....	21

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	3 / 81

Document Title

ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

3.1.2.	Need for Names to be Meaningful	21
3.1.3.	Anonymity or pseudonym of Subscribers	21
3.1.4.	Rules for Interpreting Various Name Forms	21
3.1.5.	Uniqueness of Names	22
3.1.6.	Recognition, Authentication, and Role of Trademarks	22
3.2.	Initial Identity Validation	22
3.2.1.	Method to Prove Possession of Private Key	22
3.2.2.	Authentication of Organization identity	22
3.2.3.	Authentication of Individual identity	22
3.2.4.	Non-Verified Subscriber information	23
3.2.5.	Validation of Authority	23
3.2.6.	Criteria for Interoperation	23
3.3.	Identification and Authentication for Renewal certificate Requests	23
3.3.1.	Identification and Authentication for renewal certificate	24
3.3.2.	Identification and Authentication for renewal certificate after Revocation	24
3.4.	Identification and Authentication for Revocation Request	24
4.	CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS	25
4.1.	Certificate Application	25
4.1.1.	Origin of a certificate request	25
4.1.2.	Enrolment Process and Responsibilities	25
4.2.	Certificate Application Processing	25
4.2.1.	Performing Identification and Authentication Functions	25
4.2.2.	Approval or Rejection of Certificate Applications	25
4.2.3.	Time to Process Certificate Applications	25
4.3.	Certificate Issuance	25
4.3.1.	CA Actions during Certificate Issuance	25
4.3.2.	Notifications to Subscriber by the CA of Issuance of Certificate	26
4.4.	Certificate Acceptance	26
4.4.1.	Conduct Constituting Certificate Acceptance	26
4.4.2.	Publication of the Certificate by the CA	26
4.4.3.	Notification of Certificate Issuance by the CA to Other Entities	26
4.5.	Key Pair and Certificate Usage	26
4.5.1.	CA Private Key and Certificate Usage	26
4.5.2.	Relying Party Public Key and Certificate Usage	26
4.6.	Certificate Renewal with Same Keys	26
4.7.	Certificate Renewal with Different Keys	27
4.8.	Certificate Modification with Same Keys	27

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	4 / 81

Document Title

ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

4.9. Certificate Revocation and Suspension	27
4.9.1. Circumstances for Revocation	27
4.9.2. Origin of Revocation Request	28
4.9.3. Procedure for Revocation Request	28
4.9.4. Revocation Request Grace Period	28
4.9.5. Time within Which CA Must Process the Revocation Request	28
4.9.6. Revocation Checking Requirements for Relying Parties	29
4.9.7. CRL Issuance Frequency	29
4.9.8. Maximum Latency for CRLs	29
4.9.9. On-Line Revocation/Status Checking Availability	29
4.9.10. On-Line Revocation Checking Requirements	30
4.9.11. Other Forms of Revocation Advertisements Available	30
4.9.12. Special Requirements regarding Key Compromise	30
4.9.13. Circumstances for Suspension	30
4.9.14. Who Can Request Suspension	30
4.9.15. Procedure for Suspension Request	30
4.9.16. Limits on Suspension Period	30
4.10. Certificate Status Services	30
4.10.1. Operational Characteristics	30
4.10.2. Service Availability	30
4.10.3. Optional Features	30
4.11. End of Subscription	30
4.12. Key Escrow and Recovery	30
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS	31
5.1. Physical Controls	31
5.1.1. Site Location and Construction	31
5.1.2. Physical Access	31
5.1.3. Power and Air Conditioning	31
5.1.4. Water Exposures	32
5.1.5. Fire Prevention and Protection	32
5.1.6. Media Storage	32
5.1.7. Waste Disposal	32
5.1.8. Off-Site Backup	33
5.2. Procedural Controls	34
5.2.1. Trusted Roles	34
5.2.2. Number of Persons Required per Task	34
5.2.3. Identification and Authentication for Each Role	35

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	5 / 81

Document Title

ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

5.2.4.	Roles Requiring Separation of Duties	35
5.3.	Personnel Controls	35
5.3.1.	Qualifications, Experience, and Clearance Requirements	35
5.3.2.	Background Check Procedures	35
5.3.3.	Training Requirements.....	36
5.3.4.	Retraining Frequency and Requirements	36
5.3.5.	Job Rotation Frequency and Sequence.....	36
5.3.6.	Sanctions for Unauthorized Actions	36
5.3.7.	Independent Contractor Requirements.....	36
5.3.8.	Documentation Supplied to Personnel.....	36
5.4.	Audit Logging Procedures	36
5.4.1.	Types of Events Recorded.....	36
5.4.2.	Frequency of Processing Log	38
5.4.3.	Retention Period for Audit Log.....	38
5.4.4.	Protection of Audit Log.....	38
5.4.5.	Audit Log Backup Procedures	38
5.4.6.	Audit Collection System	38
5.4.7.	Notification to Event-Causing Subject.....	38
5.4.8.	Vulnerability Assessments	38
5.5.	Records Archival.....	39
5.5.1.	Types of Records Archived	39
5.5.2.	Retention Period for Archive	39
5.5.3.	Protection of Archive	39
5.5.4.	Archive Backup Procedures.....	40
5.5.5.	Requirements for Time-Stamping of Records.....	40
5.5.6.	Archive Collection System (Internal or External)	40
5.5.7.	Procedures to Obtain and Verify Archive Information.....	40
5.6.	Key Changeover	40
5.6.1.	CA	40
5.6.2.	System	41
5.7.	Compromise and Disaster Recovery	41
5.7.1.	Incident and Compromise Handling procedures.....	41
5.7.2.	Computing resources, software, and/or data are corrupted	41
5.7.3.	Entity private key compromise procedures	42
5.7.4.	Business continuity capabilities after a Disaster	42
5.8.	RCA component termination	42

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	6 / 81

Document Title

ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

6.	TECHNICAL SECURITY CONTROLS	43
6.1.	Key Pair Generation and Installation	43
6.1.1.	Key Pair Generation.....	43
6.1.2.	Private Key Delivery to system	43
6.1.3.	Public Key Delivery to CA	43
6.1.4.	CA Public Key Delivery to Relying Parties.....	43
6.1.5.	Key Sizes	43
6.1.6.	Public Key Parameters Generation and Quality Checking	44
6.1.7.	Key Usage Purposes (as per X.509 v3 Key Usage Field)	44
6.2.	Private Key Protection and Cryptographic Module Engineering	44
6.2.1.	Cryptographic Module Standards and Controls	44
6.2.2.	Private Key (m out of n) Multi-Person Control	44
6.2.3.	Private Key Escrow	44
6.2.4.	Private Key Backup.....	44
6.2.5.	Private Key Archival	44
6.2.6.	Private Key Transfer Into or From a Cryptographic Module	44
6.2.7.	Private Key Storage on Cryptographic Module.....	45
6.2.8.	Method of Activating Private Key	45
6.2.9.	Method of Deactivating Private Key	46
6.2.10.	Method of Destroying Private Key	46
6.2.11.	Cryptographic Module Rating	46
6.3.	Other Aspects of Key Pair Management.....	46
6.3.1.	Public Key Archival	46
6.3.2.	Certificate Operational Periods and Key Pair Usage Periods.....	46
6.4.	Identity Smart Card and Activation Data	47
6.4.1.	Identity Smart Card delivery process	47
6.4.2.	Activation Data Generation and Installation.....	47
6.4.3.	Activation Data Protection.....	47
6.4.4.	Other Aspects of Activation Data	47
6.5.	Computer Security Controls	47
6.5.1.	Specific Computer Security Technical Requirements.....	47
6.5.2.	Computer Security Rating	48
6.6.	Life Cycle Technical Controls.....	48
6.6.1.	System Development Controls	48
6.6.2.	Security Management Controls.....	48
6.6.3.	Life Cycle Security Controls	48
6.7.	Network Security Controls	48

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	7 / 81

Document Title

ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

6.8. Time-Stamping 49

7. CERTIFICATE, ARL, AND OCSP PROFILES..... 50

7.1. CA Certificate Profile 50

- 7.1.1. Version Number 50
- 7.1.2. CA Certificate Extensions 50
- 7.1.3. Algorithm Object Identifiers 52
- 7.1.4. Name Forms 52
- 7.1.5. Name Constraints 52
- 7.1.6. Certificate Policy Object Identifier 52
- 7.1.7. Usage of Policy Constraints Extension 52
- 7.1.8. Policy Qualifiers Syntax and Semantics 52
- 7.1.9. Processing Semantics for the Critical Certificate Policies Extension ... 52

7.2. Seal Certificate Profile 52

- 7.2.1. Version Number 52
- 7.2.2. Seal Certificate Extensions 52
- 7.2.3. Algorithm Object Identifiers 54
- 7.2.4. Name Forms 54
- 7.2.5. Name Constraints 54
- 7.2.6. Certificate Policy Object Identifier 54
- 7.2.7. Usage of Policy Constraints Extension 54
- 7.2.8. Policy Qualifiers Syntax and Semantics 54
- 7.2.9. Processing Semantics for the Critical Certificate Policies Extension ... 55

7.3. Code Signing Certificate Profile 55

- 7.3.1. Version Number 55
- 7.3.2. Code Signing Certificate Extensions..... 55
- 7.3.3. Algorithm Object Identifiers 57
- 7.3.4. Name Forms 57
- 7.3.5. Name Constraints 57
- 7.3.6. Certificate Policy Object Identifier 57
- 7.3.7. Usage of Policy Constraints Extension 57
- 7.3.8. Policy Qualifiers Syntax and Semantics 57
- 7.3.9. Processing Semantics for the Critical Certificate Policies Extension ... 57

7.4. Encryption Certificate Profile 57

- 7.4.1. Version Number 57
- 7.4.2. Encryption Certificate Extensions 57
- 7.4.3. Algorithm Object Identifiers 59
- 7.4.4. Name Forms 59

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	8 / 81

Document Title

ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

7.4.5.	Name Constraints	59
7.4.6.	Certificate Policy Object Identifier	59
7.4.7.	Usage of Policy Constraints Extension	59
7.4.8.	Policy Qualifiers Syntax and Semantics	60
7.4.9.	Processing Semantics for the Critical Certificate Policies Extension ...	60
7.5.	Server Auth Certificate Profile	60
7.5.1.	Version Number	60
7.5.2.	Server Auth Certificate Extensions	60
7.5.3.	Algorithm Object Identifiers	62
7.5.4.	Name Forms	62
7.5.5.	Name Constraints	62
7.5.6.	Certificate Policy Object Identifier	62
7.5.7.	Usage of Policy Constraints Extension	62
7.5.8.	Policy Qualifiers Syntax and Semantics	62
7.5.9.	Processing Semantics for the Critical Certificate Policies Extension ...	62
7.6.	CRL Profile	62
7.6.1.	Version Number	62
7.6.2.	CRL and CRL Entry Extensions	62
7.7.	OCSP Profile	63
7.7.1.	Version Number(s)	63
7.7.2.	OCSP Extensions	63
8.	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	64
8.1.	Frequency and Circumstances of Assessment	64
8.2.	Identity/Qualifications of Assessor	64
8.3.	Assessor's Relationship to Assessed Entity	64
8.4.	Topics Covered by Assessment	64
8.5.	Actions Taken as a Result of Deficiency	65
8.6.	Communications of Results	65
9.	OTHER BUSINESS AND LEGAL MATTERS	66
9.1.	Fees	66
9.1.1.	Certificate Issuance or Renewal Fees	66
9.1.2.	Certificate Access Fees	66
9.1.3.	Revocation or Status Information Access Fees	66
9.1.4.	Fees for Other Services	66
9.1.5.	Refund Policy	66
9.2.	Financial Responsibility	66

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	9 / 81

Document Title

ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

9.2.1.	Insurance Coverage.....	66
9.2.2.	Other Assets	66
9.2.3.	Insurance or Warranty Coverage for End-Entities	66
9.3.	Confidentiality of Business Information	66
9.3.1.	Scope of Confidential Information	66
9.3.2.	Information Not Within the Scope of Confidential Information	67
9.3.3.	Responsibility to Protect Confidential Information	67
9.4.	Privacy of Personal Information	67
9.4.1.	Privacy Plan	67
9.4.2.	Information Treated as Private.....	67
9.4.3.	Information Not Deemed Private.....	67
9.4.4.	Responsibility to Protect Private Information	67
9.4.5.	Notice and Consent to Use Private Information.....	67
9.4.6.	Disclosure Pursuant to Judicial or Administrative Process.....	68
9.4.7.	Other Information Disclosure Circumstances	68
9.5.	Intellectual Property rights	68
9.6.	Representations and Warranties	68
9.6.1.	PMA Representations and Warranties.....	68
9.6.2.	CA Representations and Warranties	68
9.6.3.	OA Representations and Warranties	68
9.6.4.	RA Representations and Warranties	70
9.6.5.	LRA Representations and Warranties	70
9.6.6.	Citizen Representations and Warranties	71
9.6.7.	Representations and Warranties of Other Participants	71
9.7.	Disclaimers of Warranties	71
9.8.	Liability limitation.....	71
9.9.	Indemnities	71
9.10.	Term and Termination	71
9.10.1.	Term	71
9.10.2.	Termination	72
9.10.3.	Effect of Termination and Survival	72
9.11.	Individual Notices and Communications with Participants.....	72
9.12.	Amendments	72
9.12.1.	Procedure for Amendment.....	72
9.12.2.	Notification Mechanism and Period	72
9.12.3.	Circumstances under Which OID Must be Changed	72
9.13.	Dispute Resolution Provisions.....	73

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	10 / 81

Document Title

ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

9.14. Governing Law	73
9.15. Compliance with Applicable Law	73
9.16. Miscellaneous Provisions	73
9.16.1. Entire Agreement	73
9.16.2. Assignment	73
9.16.3. Severability.....	73
9.16.4. Waiver of Rights.....	73
9.16.5. Act of God	73
9.17. Other Provisions	73
10. ANNEX 1: TRUSTED ROLES FORMS	74
10.1. Authorization form	74
10.2. Trusted roles certificate delivery form.....	74
10.3. Activation data delivery form.....	75
11. ANNEX 2: DESCRIPTION OF TRUSTED ROLES	76
11.1. OA roles	76
11.2. Albanian trusted roles	77
11.2.1. Ministry of Interior.....	77
11.2.2. Civil Registry Offices	77
12. ANNEX 3: MANAGEMENT OF TRUSTED ROLES CERTIFICATES	78
12.1. Delivery of technical certificates to trusted roles.....	78
12.2. Revocation of a technical certificates delivered to trusted roles	78
12.3. Renewal of technical certificates for trusted roles.....	79
12.4. Protection of smart cards	79
13. ANNEX 4: LIST OF REFERENCED DOCUMENTS	81

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	11 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

1. INTRODUCTION

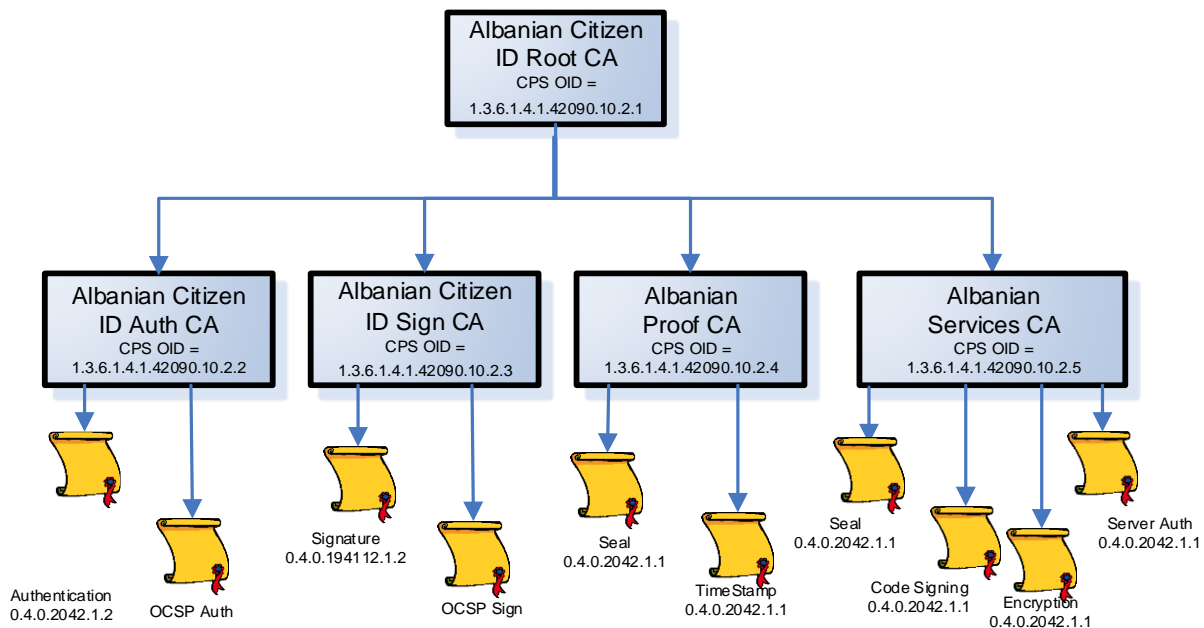
1.1. Overview

Albania operates E-ID Public Key Infrastructure (PKI) to deliver certificates used in the electronic citizen identity card and Aleat eServices system.

The certificates delivered are signed by a 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 are “Off-line” (means RCA is not used with network).

The certificates to seal, to sign code, to encrypt and to authenticate server are delivered by a CA named “Albanian Services CA”.



This Certificate Practice Statement (CPS) defines the procedures applicable to the Albanian Services CA implements 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 Practise Statement Framework;
- The Certification Practice Statement (CPS) of the Albanian RCA.

1.2. Document name and Identification

This CPS is the OA property. The corresponding CP is a normalized certificate policy OID is 0.4.0.2042.1.2. This CPS document has its own OID (1.3.6.1.4.1.42090.10.2.5).

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	12 / 81
Document Title						
ALBANIAN SERVICES 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 systems, Aleat deploys a PKI (E-ID PKI). For the proof certificates 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”;
- Generation of Services 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 Services certificate: when the link between the system and public key defined within the certificate delivered by the Services certificate is considered no longer valid then the CA revokes the Services certificate. This operation is performed by the CA in the OA trust center;
- Renewal of a Services certificate: action of delivering a new certificate to the system with the same procedure used for the first Services 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 all 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 requirements covered by the operational procedures of the OA.

1.3.1. Aleat Policy Management Authority (PMA)

Aleat is the PMA on behalf of Ministry of Interior.

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

- The RCA CPS: the result of the mapping guarantees that the RCA operates in compliance with its CPS. The result of the compliance review is validated by the PMA;
- The CA CPS with the CA CPS: the result of the mapping guarantees that the CA operates in compliance with the present CPS and the CA CPS. The result of the compliance review is validated by the PMA;
- The Information Security Management System of the OA with ISO 27001 criteria: the result of the audit guarantee that the security policy of the OA is compliant with the security objective control of the ISO 27002 and the E-ID PKI is securely hosted and operated in compliance with the CPS and the security policy of the OA. 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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	13 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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® and Luna G5 software.

1.3.3. Certification Authorities (CA)

CA is managed by Aleat .

Albanian Services CA generates certificates for system or for technical needs of Aleat. CA uses SP to publish its Services 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 of Id-NOMIC PKI application software and Luna Network HSM.

1.3.4. Registration Authority (RA)

RA is managed by Aleat for organisational 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-CA of ID-NOMIC PKI application software.

1.3.5. Operational (OA)

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

PKI components are operated by Aleat that is the OA for the CA and PS.

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

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

1.3.6. Local Registration Authority (LRA)

An LRA is an entity that realizes the authentication and identification of the services needs of the systems. LRA transmits certificate request and revocation request to RA (ID-CA of ID-NOMIC PKI software).

An LRA is authenticated and recognized by RA (ID-CA of ID-NOMIC PKI software).

Aleat is the LRA.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	14 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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. System

A system is a software component the identity of which is contained in the Services certificate and certified by the Albanian Services CA.
System holds the Services certificates and uses the corresponding private key it to sign, time-stamp, or authenticate code or documents or server.

1.3.9. Other Participants

1.3.9.1. Relying Party (RP)

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

1.4. Certificate Usage

1.4.1. Appropriate Certificate Uses

1.4.1.1. CA certificate

The Albanian Services CA certificate is used to sign X.509 certificates (Services certificate) and CRL according to this CPS.

The CA certificate is used to authenticate Albanian Services certificates and CRL delivered by the CA.

1.4.1.2. Albanian services certificate

The Albanian services certificates are used by a system to seal or to encrypt or to sign code or authenticate server.

The Albanian services certificates are used by a relying party to check and verify the identity of a system.

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 and § 1.4.1.2 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. Albanian Services certificates and CA certificate shall not be used for any functions except theses stated in § 1.4.1.1 and § 1.4.1.2 above.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	15 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

1.5. Policy Administration

1.5.1. Organization Administering the Document

The PMA is responsible for all aspects of this CPS.

1.5.2. Contact Person

The Certificate Policy Manager is responsible for the PMA

Aleat

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.

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).

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	16 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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 or system, 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.

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	17 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

activate the private key stored inside. For a CA, a cryptographic module is a Hardware Secure Module evaluated (FIPS or EAL) that is used to store and operate the CA private key.

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

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

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

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

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

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

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

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

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

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

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

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

Publication Services: Cf. § 1.3.7.

Relying Party: Cf. § 1.3.9.1.

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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	18 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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

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

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

1.6.2. Acronyms

ANSI: The American National Standards Institute;
ARL: Authority Revocation List;
CC: Common Criteria (ISO 15408 standard)
CPS: Certification Practice Statement;
CRL: Certificate Revocation List;
DN: Distinguished Name;
EAL: Evaluation assurance level (pursuant to the Common Criteria);
FIPS: United State Federal Information Processing Standards;
HTTP: Hypertext Transport Protocol;
IP: Internet Protocol;
ISO: International Organisation for Standardization;
PMA: Aleat Management Authority;
KTS: Aleat Trust Center;
LDAP: Lightweight Directory Access Protocol;
LRA: Local Registration Authority
OA: Operational Authority
OCSP: Online Certificate Status Protocol;
OID: Object Identifier;
PIN: Personal identification number;
PKCS: Public-Key Cryptography Standard;
PKI: Public Key Infrastructure;
PS: Publication Service;
RA: Registration Authority;
RCA: Root Certification Authority;
RFC: Request for comment;
RP: Relying Party
RSA: Rivest, Shamir, Adleman (Public-Key Cryptosystem);
SHA: Secure Hash Algorithm (US Standard);
CA: Certificate Authority that delivers end user certificate to citizen and to system;
SSL: Secure Socket Layer;
URL: Uniform Resource Locator.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	19 / 81
Document Title						
ALBANIAN SERVICES 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 system and relying parties by their PS. OA makes available the following information through its PS:

- For the ALB SERVICES CA with the suffix 04, the naming is the following:
 - Root CA CPS : <https://www.aleat.al/pdf/cps-citizen-root-ca.pdf>;
 - CA CPS : <https://www.aleat.al/pdf/cps-services-ca.pdf>;
 - RCA certificate: <https://www.aleat.al/csp/albanian-citizen-id-root-ca-04.cer>;
 - CA certificate: <https://www.aleat.al/csp/albanian-services-ca-04.cer>;
 - Certificate status (CRL): <https://www.aleat.al/csp/albanian-services-ca-04.crl>;
 - CA Certificate status (ARL): <https://www.aleat.al/csp/albanian-citizen-id-root-ca-04.crl>.
- For the ALB SERVICES CA with the suffix 05, the naming is the following:
 - Root CA CPS : <https://www.aleat.al/pdf/cps-citizen-root-ca-05.pdf>;
 - CA CPS : <https://www.aleat.al/pdf/cps-services-ca.pdf>;
 - RCA certificate: <https://www.aleat.al/csp/albanian-citizen-id-root-ca-04.cer>;
 - CA certificate: <https://www.aleat.al/csp/albanian-services-ca-05.cer>;
 - Certificate status (CRL): <https://www.aleat.al/csp/albanian-services-ca-05.crl>;
 - CA Certificate status (ARL): <https://www.aleat.al/csp/albanian-citizen-id-root-ca-04.crl>.

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

2.3. Time or Frequency of Publication

The information identified above at § 2.2 are available:

- Before service starts for initial RCA CPS, no later than 48 hours after Root CA CPS update is approved by the PMA for any RCA CPS update;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	20 / 81
Document Title						
ALBANIAN SERVICES 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 unauthorised modification. Information is publicly and internationally available through the Internet.

OA ensure that the PS is accessible for:

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

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	21 / 81
Document Title						
ALBANIAN SERVICES 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 system

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 Services CA

3.1.1.2. System

The DN of the different Albanian services certificates is:

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

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 system or object to which they are assigned in a meaningful way.

3.1.3. Anonymity or pseudonym of Subscribers

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

3.1.4. Rules for Interpreting Various Name Forms

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	22 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

3.1.5. Uniqueness of Names

The system 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 system's key pairs are generated and stored in a hardware security module. The LRA ensures that the system 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 LRA's private 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.

Organization acting on behalf of RCA an 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 : Aleat

3.2.3. Authentication of Individual identity

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

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	23 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

§ 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).

3.2.3.1. 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.

3.2.3.2. System

Authentication of system is done by LRA. Evidence of the system is verified by LRA. The LRA checks that the system is entitled to issue certificate requests, and that the proof need matches the system requirements. The procedure used to request Albanian proof certificates is reference as OPS-IS-005.

3.2.4. Non-Verified Subscriber information

Information that is not verified is not included in certificates.

3.2.5. Validation of Authority

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

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 3.2.3.1 and 3.2.3.2.

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	24 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

3.3.1. Identification and Authentication for renewal certificate

A request for renewal Services certificate may only be made by the LRA. At each re-key request the identity of a system, 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 Albanian services certificate has been revoked, the LRA proceeds to the initial registration process described in § 3.2.3 to obtain a new Services certificate.

3.4. Identification and Authentication for Revocation Request

Services 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 system). The LRA Operator transmits the technical revocation request to the RA (OA, ID-CA of ID-NOMIC software). The revocation request is file signed by LRA platform and transmitted to ID-CA of ID-NOMIC software during SSL communication

OA is authorized to request certificate revocation. The Security Officer of OA authenticates the employee of the OA according to rules defined by PMA. PMA defines a list of trusted employees allowed to request such revocation to the OA. The E-ID PKI Operator, on the order of the Security Officer, uses the ID-CA of ID-NOMIC web interface to transmit the revocation request during an SSL communication.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	25 / 81
Document Title ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Origin of a certificate request

LRA is in charge of requesting a Services certificate.

4.1.2. Enrolment Process and Responsibilities

The Services certificate request is established by the LRA.
The LRA manually signs (hand written signature) the request.

4.2. Certificate Application Processing

4.2.1. Performing Identification and Authentication Functions

The LRA establishes and provides the Services certificate request.
The LRA authenticates and identifies the system.
The LRA verifies all the information of the system.

4.2.2. Approval or Rejection of Certificate Applications

If verifications are successful, then:

- The LRA Operator accepts the Services certificate request;
- The LRA Operator transmits the technical Services certificate request to the RA (OA, ID-CA of ID-NOMIC software). The certificate request is file signed by LRA platform and transmitted to ID-CA of ID-NOMIC software during SSL communication ;
- The LRA Operator transmits the request 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

RA (OA, ID-CA of ID-NOMIC software) verifies the LRA platform certificate and signature to authenticate the LRA platform and the certificate request.

The RA (OA, ID-CA of ID-NOMIC software) transmits Services certificate request, signed file, to the Albanian Services CA (OA, ID-CA of ID-NOMIC software).

Albanian Services CA (OA, ID-CA of ID-NOMIC software) verifies the RA (OA, ID-CA of ID-NOMIC software) certificates and signature.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	26 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

Albanian Services CA (OA, ID-CA of ID-NOMIC software) transmits the Services certificate to the RA (OA, ID-CA of ID-NOMIC software).

RA (OA, ID-CA of ID-NOMIC software) transmits the Services certificate to the LRA platform.

LRA Operator puts certificates in the system.

All the operations, realized 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.

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 has downloaded its Services certificate, then requester checks and verifies the information contained in the "Subject DN" (Cf. § 3.1.1.2) of the Services certificate.

If the requester agrees with the information then the certificate is accepted.

4.4.2. Publication of the Certificate by the CA

The Services 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 systems managed by the CA.

The system key pair is used to seal, to sign, to authenticate and to encrypt.

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

4.6. Certificate Renewal with Same Keys

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	27 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

4.7. Certificate Renewal with Different Keys

This section addresses Services certificate generation changing the key pair. The procedures that apply are the same than the ones for initial Services certificate generation.

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 Services certificate.

4.9. Certificate Revocation and Suspension

4.9.1. Circumstances for Revocation

A Services 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 Services certificate corresponding to the private key has been lost or compromised;
- The LRA has used a wrong DN in his initial Services 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 ALB SERVICES CA if the CA is compromised. In this case, the Albanian ALB SERVICES CA will request the revocation of all an 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;
- The private key corresponding to the CA certificate has been lost or compromised;

In case of Albanian ALB SERVICES CA compromision, PMA will trigger the following steps:

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	28 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

- 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

Albanian Services 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 Services certificate corresponding to the private key has been lost or compromised;
- The LRA has used a wrong DN in his initial Services certificate request.

LRA has authority to make revocation requests for the following reasons:

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

LRA has authority to make revocation requests for the following reasons:

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

4.9.3. Procedure for Revocation Request

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

RA (OA, ID-CA of ID-NOMIC software) transmits the revocation request to the CA (OA, ID-CA of ID-NOMIC software) for an identify Services certificate.

Albanian Services CA (OA, ID-CA of ID-NOMIC software) verifies the RA (OA, ID-CA of ID-NOMIC software) certificates and signature.

CA revokes the Services certificate.

All the operations, realized 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.

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	29 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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) generate a new CRL each 24 hours.

4.9.6. Revocation Checking Requirements for Relying Parties

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

4.9.8. Maximum Latency for CRLs

The maximum delay between the time a Services certificate is revoked by the Albanian Services 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 2 hours

4.9.9. On-Line Revocation/Status Checking Availability

No stipulation.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	30 / 81
Document Title ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

4.9.10. On-Line Revocation Checking Requirements

No stipulation.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements regarding Key Compromise

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

4.9.13. Circumstances for Suspension

Not applicable.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

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

4.10.2. Service Availability

The PS availability is described in section 2.3.

4.10.3. Optional Features

No stipulation.

4.11. End of Subscription

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

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

4.12. Key Escrow and Recovery

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	31 / 81
Document Title						
ALBANIAN SERVICES 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 location. The E-ID PKI and personalization platform are located within dedicated area in different OA's location.

The E-ID PKI and personalization components (rack servers, ID-CA of ID-NOMIC software Luna HSM) have to be located in dedicated area and dedicated cabinet.

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 platform 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 realized 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-038	Document	Public	OP	06	10.12.2021	32 / 81
Document Title						
ALBANIAN SERVICES 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. 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;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	33 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

- 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;
- 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 key: insert the CD Rom in the key ceremony computer, all the data of the Backup HSM are destroyed with a dedicated software developed to securely delete data files.

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 proof a destruction request form and transmit it to the Security Officer. The form indicates:

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

5.1.8. Off-Site Backup

The back-up is composed of the following data:

- Back-up of the private key of the RCA, CA, distributed to the Security Officer on a Backup HSM;
- Back-up of the certificate of the RCA, distributed to the Security Officer on a CD Rom;
- Back-up of the E-ID PKI software and associated platform configuration;
- Back-up of USB token's PIN code distributed to the Security Officer in temper evident envelop;
- Back-up of the database of the E-ID PKI platform (Refer to § 5.4.1);
- Archive data.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	34 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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

5.2. Procedural Controls

5.2.1. Trusted Roles

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

Trusted roles include roles that involve the following responsibilities:

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

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

5.2.2. Number of Persons Required per Task

The number of persons required per tasks is given in each procedure as stated in the present CPS, by indicating the required trusted roles for the operation. The number of required persons for 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-038	Document	Public	OP	06	10.12.2021	35 / 81
Document Title						
ALBANIAN SERVICES 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 G5 HSM that contained the RCA and CA private key.

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

The identification and authentication of the person who have privileges on E-ID PKI is done during SSL 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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	36 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

necessary checks are completed. CA asks the candidate to provide past convictions and turn down an application in case of refusal. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation.

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

5.3.3. Training Requirements

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;
 - 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);

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	37 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

- Log by server and computer in current uses;
- E-ID PKI and personalization application start-up and shutdown;
 - 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);
 - 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);
 - 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);
 - Log by server and computer in current uses;
- Changes to CA certificate and keys (insert key)
 - Log by Security Officer in a log book;
 - Log by E-ID PKI software and HSM in current uses;
- Changes to certificate creation policies (e.g., validity period);
 - Log by Security Officer in a log book;
 - Log by E-ID PKI software in current uses;
- Login and logoff attempts, both successes and failures;
 - Log by server, firewall and computer in current uses;
- Authorized attempts at network access to the E-ID PKI and personalization platform;
 - Log by server, firewall and computer in current uses;
- Unauthorized attempts to access system files;
 - Log by server, firewall and computer in current uses;
- Successful and failed read and write operations on the repository;
 - Log by server and computer in current uses;
- Failures during the generation of a certificate;
 - Log by E-ID PKI software in current uses;
- Certificate lifecycle management-related events (e.g., certificate applications, issuance, revocation and renewal);
 - Log by E-ID PKI software and HSM in current uses;
 - This log are manually copy, by System Administrator, on a dedicated tape for back-up purpose (Cf. 5.1.8);
 - Kind of identification document presented by the certificate applicant
 - All event logs related to the preparation of SSCD
- Identity smart card and associated lifecycle management-related events:
 - Log by personalization software in current uses;
- Removing or replacing the cryptographic hardware security module in its assigned secure storage location;
 - Log by System Administrator in a log book;
 - Log by Security Officer in a log book;
- Activation and deactivation of the cryptographic hardware module;
 - Log by Security Officer in a log book;
 - 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;
 - Log by Security Officer in a log book;
- Physical access to the enclave;
 - Log by access system control;
 - 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;
 - Log by system Administrator.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	38 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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 placed in a safe under the control of the System administrator and/or Security Officer.

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

5.4.5. Audit Log Backup Procedures

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

5.4.6. Audit Collection System

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 users are contained in the firewall, server, software and computer log.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	39 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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;
- RCA and CA Certificates, ARL: PMA and Security Officer safe on CD Rom;
- Certificates and CRL (or other 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 10 years after the event occurred. The signed application forms are stored in Aleat central site premises in the archived room.

5.5.3. Protection of Archive

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	40 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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

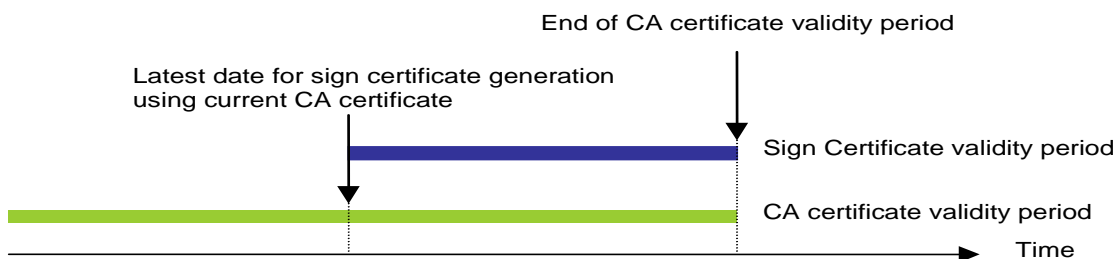
Only authorized OA equipment, trusted role and other authorized person (legal person ...) are allowed to access the archive. Access to archive information is requested to the PMA and OA according OA security policy and agreement between OA and PMA. The integrity of information is verified when it is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

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 Services 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 "Services 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:

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	41 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

- 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;
- The new key is backed-up on CD Rom;
- The old CA private key is destroyed in the E-ID PKI's HSM platform;
- The new CA private key is inserted in the E-ID PKI's HSM platform.

For these operations it is necessary to have the required trusted roles with the right activation data (Cf. Annex 2).

5.6.2. System

The validity period of a Services certificate is 5 years. When the system changes the current key to have new certificate, then the previous keys are destroyed in the HSM.

5.7. Compromise and Disaster Recovery

5.7.1. Incident and Compromise Handling procedures

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

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

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

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

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

- Certificate issuance
- Certificate revocation
- Publication of revocation information

OA maintains offsite backup of important CA information.

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

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	42 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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.

5.8. RCA component termination

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

In the event of RCA termination:

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	43 / 81
Document Title						
ALBANIAN SERVICES 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 [DSQ_Preparation guide for key ceremony].

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.docx]. 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 (Safenet G5 HSM) on a dedicated computer.

Main steps of the key ceremony are identified in [2016_2000021244 - Citizen PKI - Key Ceremony 2016 v0.3.docx]. 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 and destroyed in the HSM. Therefore, generated key only exist in the backed-up files stored on CD Rom.

6.1.1.2. System

System's key generation is performed by LRA Operator using the HSM.

6.1.2. Private Key Delivery to system

The system accesses the private key directly from the HSM.

6.1.3. Public Key Delivery to CA

System's public key is delivered securely to the CA (ID-CA of ID-NOMIC) for certificates issuance. The LRA Operator generates a Pkcs#10 file that contains the public key generated. Then the Pkcs#10 file is securely transmitted during SSL communication between LRA platform and OA (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.

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 LRA to revoke the affected certificates.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	44 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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

6.1.6. Public Key Parameters Generation and Quality Checking

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 system and CA are defined in the certificate profiles (refer to § 7.1). The CA key usage is set to allow private keys to only sign Services certificates and CRL. The system key usage is set to allow private key to only sign, authenticate, or time-stamp documents. 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

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 back up file of CA key it is necessary to initialize, or use a pre-initialized, Luna PCI HSM, on the on-line E-ID PKI’s HSM platform, with Albanian trusted domain, 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.

A key contained in a Luna HSM can only be exported in a back up file format. 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 system and CA private keys are never escrowed, for any reason.

6.2.4. Private Key Backup

The system private signature keys are backed up.

The keys are ciphered, and to use the keys it is necessary to insert them in a HSM. The backed-up keys are stored in a dedicated backup HSM under the responsibility of Security Officer.

CA private key is backed-up on file stored on two different CD Rom (s).

6.2.5. Private Key Archival

Private system and CA keys are never archived.

6.2.6. Private Key Transfer Into or From a Cryptographic Module

A key only exist on Backup HSM 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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	45 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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;
 - o Black USB token used to initialize the HSM (System Administrator)

The Luna 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

CA keys are stored in hardware security modules (Luna Network HSM). They are not accessible outside the hardware module.

System keys are stored in a HSM.

6.2.8. Method of Activating Private Key

CA 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).

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

- Initial Red USB token: Activation holder of Albanian Ministry of Interior;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	46 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

- 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.

System private key is auto activated .

6.2.9. Method of Deactivating Private Key

A HSM is only activated for operation in the OA trust center is restricted to authorised 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 remove, 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.

CA key 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.

System private key is not deactivated till destruction.

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 preformed with Black USB token used to initialize the HSM (System Administrator);
- Destruction of the corresponding back-up files (Security officer).

Normally the keys, contained in HSM, are destroyed by LRA Operator each time he/she renews the key pairs.

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.

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 5 years.
The CA private key lifetime is 5 years.

6.3.2.2. Systems

The Services certificates lifetime is 5 years.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	47 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

The Services certificate's private key lifetime is 5 years.

6.4. Identity Smart Card and Activation Data

6.4.1. Identity Smart Card delivery process

No stipulation.

6.4.2. Activation Data Generation and Installation

No stipulation.

6.4.3. Activation Data Protection

No stipulation.

6.4.4. Other Aspects of Activation Data

No stipulation.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

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

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 (SSL protocol);
- Smart card that contains certificate delivered by Technical CA has to need a PIN and PUK code to be activated and unlocked;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	48 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

- 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 CD Rom back-up files are only connected to a computer dedicated to key ceremony or to the server that hosts the HSM. A CD Rom key whose purpose is to be a "CD Rom key back-up files" 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.

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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	49 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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 a 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-038	Document	Public	OP	06	10.12.2021	50 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

7. CERTIFICATE, ARL, AND OCSP PROFILES

7.1. 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. CA Certificate Extensions

Base certificate	Value
Version	2 (=version 3)
Serial number	Defined by Keyseed®
Key length	2048
Certificate duration	5 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 Services CA
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	Includ e	Critica l	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	TRUE	
CA		X		True
Maximum Path Length		X		0
Certificate Policies	{id-ce 32}	X	FALSE	n/a
policyIdentifiers				0.4.0.2042.1.2 (Normalized Certificate Policy requiring a secure cryptographic device)
policyQualifiers				n/a
CPSpointer				CPS URI: https://www.aleat.al/pdf/cps-citizen-root-ca.pdf
OID				n/a

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	51 / 81

Document Title

ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

Value				n/a
User Notice				n/a
OID				n/a
value				n/a
noticeRef				n/a
organization				n/a
noticeNumbers				n/a
explicitText				n/a
CRL Distribution Points	{id-ce 31}	X	FALSE	
distributionPoint				[1]Certificates Revocation List Distribution Point Name of the distribution point : Complete Name : URI http://www.aleat.al/csp/alb-services-ca-04.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			Clear
emailProtection	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			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 Key Identifier	{id-ce 14}	X	FALSE	
Methods of generating key ID				Method 1
privateInternetExtensions	AIA authorityInformation Access			n/a

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	52 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

<i>Other Extensions</i>				n/a
-------------------------	--	--	--	-----

7.1.3. Algorithm Object Identifiers

See section 7.1.

7.1.4. Name Forms

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

7.1.5. Name Constraints

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

7.1.6. Certificate Policy Object Identifier

See section 7.1.

7.1.7. Usage of Policy Constraints Extension

See section 7.1.

7.1.8. Policy Qualifiers Syntax and Semantics

See section 7.1.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

See section 7.1.

7.2. Seal Certificate Profile

7.2.1. 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.

7.2.2. Seal Certificate Extensions

Base certificate	Value
Version	2 (=version 3)
Serial number	Defined by ID-CA of ID-NOMIC
Key length	2048
Certificate duration	5 years
Issuer DN	C = AL OI=NTRAL-K82018015V O = Aleat CN=Albanian Services CA
Subject DN	C = AL OI=NTRAL-K82018015V O = Aleat

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	53 / 81

Document Title
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

	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	Includ e	Critica l	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		X		False
Maximum Path Length		X		n/a
Certificate Policies	{id-ce 32}	X	FALSE	n/a
policyIdentifiers				0.4.0.2042.1.1 (Normalized Certificate Policy)
policyQualifiers				n/a
CPSpointer				CPS URI: https://www.aleat.al/pdf/cps-services-ca.pdf
OID				n/a
Value				n/a
User Notice				n/a
OID				n/a
value				n/a
noticeRef				n/a
organization				n/a
noticeNumbers				n/a
explicitText				n/a
CRL Distribution Points	{id-ce 31}	X	FALSE	
distributionPoint				[1]Certificates Revocation List DistributionPoint Name of the distribution point : Complete Name : URI https://www.aleat.al/csp/albanian-services-ca-04.crl or https://www.aleat.al/csp/albanian-services-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			Clear
emailProtection	1.3.6.1.5.5.7.3.4			Set
document signing	1.3.6.1.4.1.311.10.			Clear

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	54 / 81

Document Title
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

	3.12			
PDF signing	1.2.840.113583.1.1.5			Clear
OCSFsigning	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			n/a
Key Usage	{id-ce 15}	X	TRUE	
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}			n/a
Subject Key Identifier	{id-ce 14}	X	FALSE	
Methods of generating key ID				Method 1
privateInternetExtensions	AIA authorityInformation Access			n/a
Other Extensions				n/a

7.2.3. Algorithm Object Identifiers

See section 7.2.

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 7.2.

7.2.7. Usage of Policy Constraints Extension

See section 7.2.

7.2.8. Policy Qualifiers Syntax and Semantics

See section 7.2.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	55 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

7.2.9. Processing Semantics for the Critical Certificate Policies Extension

See section 7.2.

7.3. Code Signing Certificate Profile

7.3.1. 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.

7.3.2. Code Signing Certificate Extensions

Base certificate	Value
Version	2 (=version 3)
Serial number	Defined by ID-CA of ID-NOMIC
Key length	2048
Certificate duration	5 years
Issuer DN	C = AL OI=NTRAL-K82018015V O = Aleat CN=Albanian Services 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	Includ e	Critica l	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		X		False
Maximum Path Length		X		n/a
Certificate Policies	{id-ce 32}	X	FALSE	n/a
policyIdentifiers				0.4.0.2042.1.1 (Normalized Certificate Policy)
policyQualifiers				n/a
CPSpointer				CPS URI: https://www.aleat.al/pdf/cps-services-ca.pdf
OID				n/a

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	56 / 81

Document Title
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

Value				n/a
User Notice				n/a
OID				n/a
value				n/a
noticeRef				n/a
organization				n/a
noticeNumbers				n/a
explicitText				n/a
CRL Distribution Points	{id-ce 31}	X	FALSE	
distributionPoint				[1]Certificates Revocation List DistributionPoint Name of the distribution point : Complete Name : URI https://www.aleat.al/csp/albanian-services-ca-04.crl or https://www.aleat.al/csp/albanian-services-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			Clear
emailProtection	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			Set
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			n/a
Key Usage	{id-ce 15}	X	TRUE	
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}			n/a
Subject Key Identifier	{id-ce 14}	X	FALSE	
Methods of generating key ID				Method 1

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	57 / 81

Document Title
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

privateInternetExtensions	AIA authorityInformation Access			n/a
Other Extensions				n/a

7.3.3. Algorithm Object Identifiers

See section 7.3.

7.3.4. Name Forms

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

7.3.5. Name Constraints

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

7.3.6. Certificate Policy Object Identifier

See section 7.3.

7.3.7. Usage of Policy Constraints Extension

See section 7.3.

7.3.8. Policy Qualifiers Syntax and Semantics

See section 7.3.

7.3.9. Processing Semantics for the Critical Certificate Policies Extension

See section 7.3.

7.4. Encryption Certificate Profile

7.4.1. 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.

7.4.2. Encryption Certificate Extensions

Base certificate	Value
Version	2 (=version 3)
Serial number	Defined by ID-CA of ID-NOMIC
Key length	2048
Certificate duration	5 years
Issuer DN	C = AL OI=NTRAL-K82018015V O = Aleat CN=Albanian Services CA
Subject DN	C = AL

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	58 / 81

Document Title
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

	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	Includ e	Critica l	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		X		False
Maximum Path Length		X		n/a
Certificate Policies	{id-ce 32}	X	FALSE	n/a
policyIdentifiers				0.4.0.2042.1.1 (Normalized Certificate Policy)
policyQualifiers				n/a
CPSpointer				CPS URI: https://www.aleat.al/pdf/cps-services-ca.pdf
OID				n/a
Value				n/a
User Notice				n/a
OID				n/a
value				n/a
noticeRef				n/a
organization				n/a
noticeNumbers				n/a
explicitText				n/a
CRL Distribution Points	{id-ce 31}	X	FALSE	
distributionPoint				[1]Certificates Revocation List DistributionPoint Name of the distribution point : Complete Name : URI https://www.aleat.al/csp/albanian-services-ca-04.crl or https://www.aleat.al/csp/albanian-services-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			Clear

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	59 / 81

Document Title
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

emailProtection	1.3.6.1.5.5.7.3.4			Set
document signing	1.3.6.1.4.1.311.10.3.12			Clear
PDF signing	1.2.840.113583.1.1.5			Clear
OCSFsigning	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			n/a
Key Usage	{id-ce 15}	X	TRUE	
Digital Signature				Clear
Non Repudiation				Clear
Key Encipherment				Set
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			n/a
Other Extensions				n/a

7.4.3. Algorithm Object Identifiers

See section 7.4.

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 7.4.

7.4.7. Usage of Policy Constraints Extension

See section 7.4.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	60 / 81

Document Title
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

7.4.8. Policy Qualifiers Syntax and Semantics

See section 7.4.

7.4.9. Processing Semantics for the Critical Certificate Policies Extension

See section 7.4.

7.5. Server Auth Certificate Profile

7.5.1. 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.

7.5.2. Server Auth Certificate Extensions

Base certificate	Value
Version	2 (=version 3)
Serial number	Defined by ID-CA of ID-NOMIC
Key length	2048
Certificate duration	5 years
Issuer DN	C = AL OI=NTRAL-K82018015V O = Aleat CN=Albanian Services 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	Includ e	Critica l	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		X		False
Maximum Path Length		X		n/a
Certificate Policies	{id-ce 32}	X	FALSE	n/a
policyIdentifiers				0.4.0.2042.1.1 (Normalized Certificate Policy)
policyQualifiers				n/a

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	61 / 81

Document Title

ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

CPSpointer				CPS URI: https://www.aleat.al/pdf/cps-services-ca.pdf
OID				n/a
Value				n/a
User Notice				n/a
OID				n/a
value				n/a
noticeRef				n/a
organization				n/a
noticeNumbers				n/a
explicitText				n/a
CRL Distribution Points	{id-ce 31}	X	FALSE	
distributionPoint				[1]Certificates Revocation List DistributionPoint Name of the distribution point : Complete Name : URI https://www.aleat.al/csp/albanian-services-ca-04.crl or https://www.aleat.al/csp/albanian-services-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			Set
Client Authentication	1.3.6.1.5.5.7.3.2			Set
emailProtection	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			n/a
Key Usage	{id-ce 15}	X	TRUE	
Digital Signature				Set
Non Repudiation				Clear
Key Encipherment				Set
Data Encipherment				Clear
Key Agreement				Clear
Key CertSign				Clear
Key CRL Sign				Clear
Private Key Usage Period	{id-ce 16}			n/a

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	62 / 81

Document Title
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

Subject Key Identifier	{id-ce 14}	X	FALSE	
Methods of generating key ID				Method 1
privateInternetExtensions	AIA authorityInformation Access			n/a
Other Extensions				n/a

7.5.3. Algorithm Object Identifiers

See section 7.5.

7.5.4. Name Forms

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

7.5.5. Name Constraints

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

7.5.6. Certificate Policy Object Identifier

See section 7.5.

7.5.7. Usage of Policy Constraints Extension

See section 7.5.

7.5.8. Policy Qualifiers Syntax and Semantics

See section 7.5.

7.5.9. Processing Semantics for the Critical Certificate Policies Extension

See section 7.5.

7.6. CRL Profile

7.6.1. Version Number

RCA 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).

7.6.2. 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
-----------------------------	-------------------------------------------------------------------------------------------------------------------------

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	63 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

	OI=NTRAL-K82018015V O=Aleat CN=Albanian Services 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 http URL for publication : https://www.aleat.al/csp/albanian-services-ca-04.crl or https://www.aleat.al/csp/albanian-services-ca-05.crl
--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

7.7. OCSP Profile

No stipulation.

7.7.1. Version Number(s)

No stipulation.

7.7.2. OCSP Extensions

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

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	64 / 81
Document Title						
ALBANIAN SERVICES 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 present CPS.

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

- Knowledge of the CPS, procedure and technical guide by the trusted role;
- E-ID PKI and personalization software are deployed on the correct server;
- E-ID PKI and personalization component respect the network security policy of OA and the present CPS;
- Materials and HSM are used correctly regarding the software deployed on it;
- IP configuration is correct and well administrated by System administrator;
- Each certificate delivered with the E-ID PKI respect [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-038	Document	Public	OP	06	10.12.2021	65 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

- Activation data are correctly distributed and managed by the right trusted roles;
- Back-up files still exist and correctly protected;
- 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-038	Document	Public	OP	06	10.12.2021	66 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate Issuance or Renewal Fees

Defined by OA and PMA.

9.1.2. Certificate Access Fees

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

9.1.3. Revocation or Status Information Access Fees

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

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

No stipulation.

9.2. Financial Responsibility

9.2.1. Insurance Coverage

OA maintains reasonable levels of insurance coverage.

9.2.2. Other Assets

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

9.2.3. Insurance or Warranty Coverage for End-Entities

If there is damage for a relying party due to Albanian Ministry Of Interior or OA fault, Albanian Ministry Of Interior and/or OA will cover part of the relying 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;
- CA PKI private keys;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	67 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

- 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;

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 System and CA are:

- Naming document;
- 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.

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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	68 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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, Services certificate and revocation information that are issued by the CA.

The LRA retains all intellectual rights it has on information contained in the Services certificate delivered by Albanian Services CA and for which he/she is the proprietary.

9.6. Representations and Warranties

9.6.1. PMA Representations and Warranties

PMA defines 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, are implemented as applicable to deliver and manage Services 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);
- 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;
- 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:

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	69 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

- 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;
- 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:

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	70 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

- 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 a security incident about the CA services that the OA performed;
- Respect the CA CPS.

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;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	71 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

- 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

No stipulation.

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 system with Services 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 between the present CPS.

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 Services 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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	72 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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, Services 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 Ministry of Interior and the different eServices providers like the bank. CA will also inform the relevant authorities like 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.

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.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	73 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

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.

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 directly caused direct damage to system and relying party.

9.17. Other Provisions

No stipulation.

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	74 / 81
Document Title						
ALBANIAN SERVICES 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:
 - o Date;
 - o Name;
 - o First name;
 - o Telephone;
 - o Address;
 - o Role requested ;

Signature of the Role requester

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

Signature of the Authorizer.

10.2. Trusted roles certificate delivery form

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

Signature of the trusted role certificate applicant

- Name of the “master trusted role” who deliver the certificate ;
 - o Date;
 - o Name;

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	75 / 81
Document Title						
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT						

- First name;
- Telephone;
- Address.

Signature of “master trusted role” who deliver the certificate

10.3. Activation data delivery form

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

Signature of the Activation data holder

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

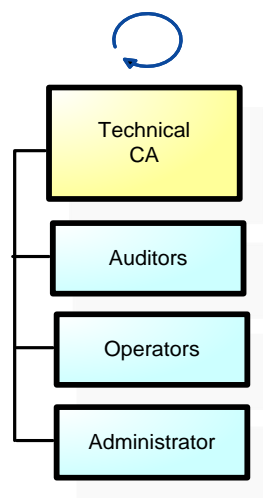
Signature of Security Officer

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	76 / 81
Document Title						
ALBANIAN SERVICES 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 realize RCA and CA initial key ceremony	Using Keyseed® software
E-ID PKI Operator (Aleat System Operator)	RA Operator certificate on dedicated smart card	Revoke services certificates. Those certificates are revoked using the Proof CA. Audit PKI events.	Using ID NOMIC ID CA software.
Revocation Officer	RA Operator	Revoke certificates. Those certificates are revoked using the Citizen Sign CA Portal.	Using ID NOMIC ID CA software.
System Auditor	Auditor certificate on	Authorized to view and maintain	Using ID NOMIC ID CA

Reference	Type	Classification	Owner	Version	Date	Page
OPS-OP-038	Document	Public	OP	06	10.12.2021	77 / 81

Document Title
ALBANIAN SERVICES CA CERTIFICATION PRACTICE STATEMENT

(Aleat Quality & Investigation Manager)	dedicated smart card	archives and audit logs of the CA trustworthy system. Audit all E-PKI activity.	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	Sign [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 (Registration officer or revocation officer)	NA	LRA Operator	Generate the requested certificate from LRA platform
		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-038	Document	Public	OP	06	10.12.2021	78 / 81
Document Title						
ALBANIAN SERVICES 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-038	Document	Public	OP	06	10.12.2021	79 / 81
Document Title						
ALBANIAN SERVICES 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-038	Document	Public	OP	06	10.12.2021	80 / 81
Document Title						
ALBANIAN SERVICES 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-038	Document	Public	OP	06	10.12.2021	81 / 81
Document Title						
ALBANIAN SERVICES 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

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