REPUBLIC OF ALBANIA

Production & Distribution of Identity Cards & Biometric Passports

PKI Disclosure Statement

TABLE OF CONTENTS

1. INTRODUCTION

Aleat has created an e-security platform for its customers to facilitate role-based access, secure authentication and qualified electronic signature. The security services include a Public Key Infrastructure, which has a Certification Authority operated by Aleat (CA). The policy requirements on the operation and management of the CA issuing Certificates are defined in the Aleat Certificate Practice Statement (CPS) document such that Subjects certified by the CA and Relying Parties may have confidence in the reliability of the Certificates.

1.1. Document Description & Context

This document is the PKI Disclosure Statement herein after referred to as the PDS. This document does not substitute or replace the Certificate Practice Statement (CPS) under which digital certificates of Albanian Citizen ID PKI are issued by Aleat. The purpose of this document is to summarize the key points of the CPS for the benefit of Subscribers, Subjects and Relying Parties.

2. PDS

2.1. TSP Contact Information

Aleat Sh.p.k.

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

2.2. Certificate Type, Validation Procedure and Usage

The CA issues two types of Certificate:

1. **Authentication Certificates** – for use only where a SP delivers to the Albanian Citizen a service that need the usage secure authentication.

2. **Qualified Signature Certificates** – for use only where a SP delivers to the Albanian Citizen a service that need a documents to be electronically signed using Private Keys held on the Albanian Citizen IDC.

The CA ensures that evidence of Albanian Citizens identification and the accuracy of their names and associated data are correct since they are retrieved from the NCR service.

2.3. Reliance Limits

Refer to the section 9.8 of the CPS for reliance limits. The CA issues two types of Certificates and their limits are:

1. **Authentication Certificates** – for use in a specified validity time (the same validity as the Albanian IDC) and to be used only for authenticating the citizen through his national IDC.

2. **Electronic Signature Certificates** – for use in a specified validity time (the same validity as the Albanian IDC) and to be used only for digitally signing a document through the citizen national IDC.

According to digital signature laws and regulations, the only appropriate use for qualified digital certificates is signing.

All events involved in the generation of the key pairs are recorded. This includes all configuration data and registration information used in the process. Audit logs are retained as archive records for

a period no less than twenty (20) years for audit trails files, and no less than twenty (20) years for key and digital certificate information.

2.4. Obligations of Subscribers

The digital certificate holders are required to act in accordance with the CPS and the relevant certificate subscribers/holders agreement.

The subscriber's obligations are the items below:

1. When receiving the certificates and the identity card, the cardholder must ensure the accuracy of data in the identity card and in the certificates and refuse the identity card/certificates in case of mismatch of data;
2. The cardholder shall use key pair for electronic signature and authentication used in accordance with any limitations notified to the subscriber;
3. The cardholder shall refrain from signing any document containing macros or executable codes that alter the content of the document, which would cancel the qualified digital signature;
4. Exercise sole and complete control and use of the private key that corresponds to the certificate cardholder's public key;
5. The cardholder shall exercise reasonable care to avoid unauthorized use of cardholder's private keys;
6. The cardholder has to keep PIN code secret;
7. The cardholder shall promptly notify ALEAT, if any of the following events will occur within the validity period of the Certificates:
    - The identity card has been lost or the cardholder has forgotten the PIN code;
    - When the cardholder ascertains errors in the data of the certificates issued by ALEAT.
8. The use of an invalidated certificate is forbidden and any unauthorized use shall be subject of criminal and/or civil liability;
9. If the certificates shall be revoked, the cardholder shall immediately cease their use;
10. At all times, use the digital certificates in accordance with all applicable laws and regulations.

2.5. Certificate Status Checking Obligations of Relying Parties

The obligations of the Relying Party, if it is to reasonably rely on a Certificate, are to:

1. Verify the validity, suspension or revocation status of the Certificate using current revocation status information as indicated to the Relying Party in the CPS.

2. Take account of any limitations on the usage of the Certificate indicated to the Relying Party either in the Certificate or the terms and conditions (see Section 3 above for usage).

3. Take any other precautions prescribed in the Certification Practice Statement (CPS).

The status of digital certificates issued by Albanian Citizen ID PKI is published in a certificate revocation list or is made available via Online Certificate Status Protocol checking where available. Link to OCSP service is available inside the citizen certificates (Auth and Sign).

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

2.6. Limited Warranty & Disclaimer / Limitation of Liability

The liability taken by the CA is limited to the correct application of procedures as declared in the CPS these procedures relate to the issue and management of digital Certificates. Therefore any failure of transaction that utilises the digital Certificate is out of scope.

In essence the liability will include the correct identification of Subjects according to the declared practices. If a transaction is found to be in error through the incorrect identification of the Subject through failing to follow the declared practices, then the CA is liable. If the Subject is incorrectly identified, but the error was within the documents used to support the Subject's claim to an identity, then the CA shall not be liable.

Limitations on liability are covered in the terms and conditions see CPS.

2.7. Applicable agreements (CPS)

The following documents are available online at https://www.aleat.al/en/certificate-policies :

- Certificate Practice Statement documents (CPS)
- PKI Disclosure Statement

The subscriber agreement document is available online at https://www.aleat.al/en/id-card-activation

2.8. Privacy Policy

Data contained within the Aleat certificate is considered public information. All personal data obtained during the registration process will not be released without prior consent of the relevant certificate holder, unless required otherwise by law or to fulfil the requirements of the CPS.

The subscriber consents that Aleat keeps, on behalf of MIA during the concession duration plus 10 years, record information used in registration, subject device provision, including whether this is to the subscriber or to the subject where they differ, and any subsequent revocation, the identity and any specific attributes placed in the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of Aleat terminating its services;

2.9. Refund Policy

Not applicable.

2.10. Applicable Law, Complaints and Dispute Resolution

2.10.1. Governing Law

Subscribers and relying parties shall use Albanian Citizen ID certificates and any other related information and materials provided by Aleat only in compliance with all applicable laws and regulations. Aleat may refuse to issue or revoke certificates if, in the reasonable opinion of Aleat, issuance or the continued use of the Aleat certificates would violate applicable laws or regulations

2.10.2. Dispute Resolution

The CA has policies and procedures for the resolution of complaints and disputes received from customers or other parties about the provisioning of CA services or any other related matters. Details can be obtained by applying to the CA (see Section 2 above).

The Albanian Law shall govern the provision of CA services. All parties shall submit to the exclusive jurisdiction of the court of Albania.

2.11. TSP and Repository Licenses, Trust Marks and Audit

In the provision of Trust Services, Aleat maintains several accreditations and certifications of its Public Key Infrastructure:

- The perimeter where Aleat PKI is hosted is certified ISO 27001:2013
- Aleat is certified as a trusted Service Provider in Albania

The CA issues certificates using ID-NOMIC software solutions which have been submitted to be accredited to the relevant Common Criteria EAL 4 augmented requirements certified.

The CA service operation is eIDAS certified.

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