REPUBLIKA E SHQIPËRISË
KËSHILLI I MINISTRAVE
AGJENCIA KOMBËTARE E SHOQËRISË SË INFORMACIONIT

Date 15.12.2022

NAIS

CERTIFICATE POLICY
/
CERTIFICATION PRACTICE STATEMENT

for

QUALIFIED CERTIFICATES
FOR ELECTRONIC SIGNATURES AND SEALS

Version 2.0

Document details

Document Name	NAIS Certificate Policy / Certification Practice Statement for Qualified Certificates for Electronic Signatures and Seals
Document Owner	NAIS (National Agency of Information Society)
Contact	pki@akshi.gov.al

Version history

Version	**Date**	**Change**
1.0	2016	First version.
2.0	15.12.2022	The content of the CP/CPS was updated in accordance with IETF RFC 3647.

Table of Contents

1. INTRODUCTION

1.1 Overview

This Certificate Policy / Certification Practice Statement (hereinafter referred to as 'CP/CPS') for NAIS Qualified Certificates for Electronic Signatures and Seals describes the certification policy and practices that the National Agency for Information Society (NAIS) applies for the issuance of qualified certificates for electronic signature and qualified certificates for electronic seals (hereinafter referred to as certificates for electronic signature/seals).

NAIS PKI refers to the PKI infrastructure established at NAIS for the provision of trust services. Trust Services offered by NAIS as a Qualified Trust Service Provider in the scope of this CP/CPS are certificates for electronic signature and certificates for electronic seal.

NAIS has established a three-tier PKI architecture:

- Root Certification Authority:
  - NAIS Root Certification Authority (NAIS Root CA)
- Subordinate Certification Authority:
  - NAIS Certification Authority (NAIS CA)
- Class Certification Authorities:
  - NAIS Class 1 Certification Authority (NAIS Class 1 CA)
  - NAIS Class 2 Certification Authority (NAIS Class 2 CA)
  - NAIS Class 3 Certification Authority (NAIS Class 3 CA)
  - NAIS Class 4 Certification Authority (NAIS Class 4 CA)

NAIS Root CA has issued a self-signed certificate as well as certificate to its subordinate CA (NAIS CA).

NAIS CA has issued four class certificates: NAIS Class 1 CA, NAIS Class 2 CA, NAIS Class 3 CA, and NAIS Class 4 CA (collectively referred to as '**NAIS Class CAs**'). NAIS Class CAs issue end-user certificates. NAIS CA and NAIS Class CAs are collectively referred to as '**NAIS CAs**' throughout this document.

NAIS has also established a platform for remote electronic signing (Remote Signing Service Platform). Generation and management of the private keys for certificates used in the Remote Signing Service Platform is managed by NAIS on behalf of the Signatory.

The content of this CP/CPS is based on the "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" of the Network Working Group (RFC 3647).

1.1.1 Certificates issued by NAIS Class 1 Certification Authority

- Certificate for electronic signature for private entities
  This type of certificate is issued to natural persons associated with a private entity. The certificate is used in the Remote Singing Service Platform for the purpose of supporting electronic signing of documents. The certificate is issued in a Remote QSCD.

- Certificate for electronic signature for government employees
  This type of certificate is issued to government employees. The certificate is used in the Remote Singing Service Platform for the purpose of supporting electronic signing of documents.
  The certificate is issued in a Remote QSCD.

- Certificate for electronic signature for government employees for critical infrastructure
  This type of certificate is issued to government employees operating on critical infrastructure or accessing international systems for the purpose of authentication and electronic signing of documents. The certificate is issued on USB Token.

- Certificate for electronic seal
  This type of certificate is issued to public institutions in Albania which offer services in the e-Albania government portal. The certificate is used for the purpose of automated electronic sealing of documents in the e-Albania portal. The certificate is issued as a soft certificate.

1.1.2 Certificates issued by NAIS Class 2 Certification Authority

- Certificate for electronic signature for private entities for critical infrastructure
  This type of certificate is issued to a natural person associated with a private entity operating on critical infrastructure or accessing international systems for the purpose of authentication and electronic signing of documents. The certificate is issued on USB Token.

1.1.3 Certificates issued by NAIS Class 3 Certification Authority

- Certificate for the fiscalization project for public institutions
  This certificate for electronic seal is issued to public institutions in Albania to support the fiscalization project. It's issued as a soft certificate.

- Certificate for the fiscalization project for private entities
  This certificate for electronic seal is issued to private entities in Albania to support the fiscalization project. It's issued as a soft certificate.

- Certificate Test for the fiscalization project
  This certificate for electronic seal it's issued to software development companies for testing purposes to support the fiscalization project. It's issued as a soft certificate.

1.1.4 Certificates issued by NAIS Class 4 Certification Authority

- Certificate for authentication for the Remote Signing Service Platform
  This type of certificate for electronic signature is used as a component in the Remote Signing Service Platform.

1.2 Document name and identification

Document Name: NAIS Certificate Policy / Certification Practice Statement for Qualified Certificates for Electronic Signatures and Seals

Version: 2.0

Approval date: xx December 2022

1.3 PKI participants

The PKI participants are all the legal entities or natural persons who are involved in the activities of NAIS as a Trust Service Provider (TSP) or who may be impacted by the use of certificates issued by NAIS.

Participants within NAIS PKI are:

- Certification Authorities
- Registration Authorities
- Subjects
- Subscribers
- Relying parties

1.3.1 Certification authorities

A Certificate Authority (CA) is an authority trusted by subscribers, subjects and relying parties to create and assign public-key certificates.

Certification Authorities within NAIS PKI under the scope of this CP/CPS are:

- NAIS Root CA
- NAIS CA
- NAIS Class 1 CA
- NAIS Class 2 CA
- NAIS Class 3 CA
- NAIS Class 4 CA

1.3.2 Registration authorities

Registration Authorities are the entities that establish enrollment procedures for certificate applications, perform identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA.

The operational tasks of RA are performed by the RA function established at PKI Sector at NAIS.

1.3.3 Subscribers

Subscribers are legal or natural persons that have requested the issuance of a certificate from NAIS for which they have signed an agreement.

The **Subject** is the entity to whom a certificate is issued and is identified in a certificate as the holder of the private key associated with the public key in the certificate.

- NAIS issues certificates for electronic seal only to legal persons operating in the Republic of Albania.
- NAIS issues certificates for electronic signature to natural persons in association with a legal person. The natural person can be:
    - An Albanian citizen, or
    - A foreign citizen who owns a business in the Republic of Albania

1.3.4 Relying parties

A relying party is a natural or legal person that relies upon an electronic identification or a trust service. Relying parties include parties verifying a digital signature using a public key certificate.

Responsibilities of relying parties are defined in section 9.6.4 of this document.

1.3.5 Other participants

- Organizational units within NAIS responsible for the development, maintenance, and approval of policies and practices that are applied in the provision of certification services.
- Dissemination and repository service - this role (which is carried out by NAIS) refers to the publication of Certificate Policies, Certification Practice Statements, terms and conditions of certification services, CA certificates and related information to subscribers and relying parties.
- Revocation management and revocation status service - this role (which is carried out by NAIS) is responsible for processing requests related to revocation and providing certificate revocation status information to relying parties.
- External service providers supporting certification services under a signed agreement with NAIS.

1.4 Certificate usage

1.4.1. Appropriate certificate uses

Certificates for electronic signature for private entities should be used:

- *only* for the purpose of electronic signing of documents in the Remote Signing Service Platform
- *only* by the subject, in this case, the natural person associated with a private entity

Certificates for electronic signature for government employees should be used:

- *only* for the purpose of electronic signing of documents in the Remote Signing Service Platform
- *only* by the subject, in this case, the government employee

Certificates for electronic signature for government employees for critical infrastructure should be used:

- *only* for authentication and electronic signing of documents
- *only* by the subject, in this case, the government employee operating on critical infrastructure or accessing international systems
- *only* via USB Token issued by NAIS

Certificates for electronic seal should be used:

- *only* for the support of automated electronic sealing of documents in the e-Albania portal
- *only* by the subject, in this case, the legal person which is a public institution offering services in the e-Albania government portal

Certificates for electronic signature for private entities for critical infrastructure should be used:

- *only* for authentication and electronic signing of documents
- *only* by the subject, in this case, the natural person associated with a private entity operating on critical infrastructure or accessing international systems
- *only* via USB Token issued by NAIS

Certificates for the fiscalization project for public institutions should be used:

- *only* for the support of the fiscalization project under the Law 87/2019 "On the invoice and traffic monitoring system", amended

- *only* by the subject, in this case the legal person which is a public institution in the Republic of Albania.

Certificates for the fiscalization project for private entities should be used:

- *only* for the support of the fiscalization project under the Law 87/2019 "On the invoice and traffic monitoring system", amended
- *only* by the subject, in this case the legal person which is a private entity in the Republic of Albania

Certificate Test for the fiscalization project should be used:

- *only* for the support of the fiscalization project under the Law 87/2019 "On the invoice and traffic monitoring system", amended
- *only* by the subject, in this case the legal person which is a private entity in the IT field, interested in developing software applications in the context of the fiscalization project.

Certificates for authentication for the Remote Signing Service Platform should only by NAIS as a component in the Remote Signing Service Platform.

1.4.2 Prohibited certificate uses

Any usage of a certificate other than the usage defined in section 1.4.1 is prohibited.

1.5 Policy administration

1.5.1 Organization administering the document

NAIS is responsible for drafting, registering, maintaining, and updating this CP/CPS.

Name	National Agency for Information Society
Address	Street Papa Gjon Pali II, No. 3, 1st Floor, 1003 Tirana, Albania
TIN	K72301452S
Phone	+355(0)42277750
Fax	+355(0)42277764
Email	info@akshi.gov.al
Web	akshi.gov.al

1.5.2 Contact person

The PKI Sector at NAIS is the contact point for the administration and content of this CP/CPS.

Contact	PKI Sector
Email	pki@akshi.gov.al

1.5.3 Person determining CPS suitability for the policy

The PKI Sector at NAIS as well as the authorized personnel participating in the development, maintenance, and approval of policies and practices that are applied in provision of certification services are collectively responsible for determining the CPS suitability.

The evaluation of the CPS suitability may also be based on the report results of an independent compliance audit.

1.5.4 CPS approval procedures

The PKI Sector submits the CPS for formal approval to AKSHI Top Management. Changes made to the CPS have to go through NAIS internal procedures for creating and updating documentation. The latest version of the CPS will be available at the public repository akshi.gov.al/repository both in English and in Albanian.

1.6 Definitions and acronyms

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 passphrase, or a manually-held key share).

Certification Authority (CA) – Authority trusted by one or more users to create and assign public-key certificates. Optionally the certification authority can create the subjects' keys.

A certification authority can be:

1) a trust service provider that creates and assigns public key certificates; or
2) a technical certificate generation service that is used by a certification service provider that creates and assigns public key certificates.

Certification Practice Statement (CPS) – A statement of the practices that a certification authority employs in issuing, managing, revoking, and renewing or re-keying certificates.

Certificate Revocation List (CRL) – signed list indicating a set of certificates that are no longer considered valid by the certificate issuer.

Certificate Policy (CP) – named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

Certificate for electronic signature – electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person.

Certificate for electronic seal – electronic attestation that connects the electronic seal validation data with the legal person and confirms the name of that person.

Creator of the seal – A legal person who creates an electronic seal.

e-Albania – refers to the government portal (e-albania.al) which is used for the provision of e-services and is administered by the National Agency for Information Society.

FIPS 140-2 – The Federal Information Processing Standard Publication 140-2 (FIPS PUB 140-2) is a U.S. government computer security standard used to approve cryptographic modules.

Public key certificate – public key of an entity, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority which issued it.

Note: For the purposes of this document, the term “certificate” refers to public key certificates.

Public Key Infrastructure (PKI) – infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.

Remote Signing Service Platform – refers to the platform (esign.akshi.gov.al) established by NAIS used to sign documents.

Registration Authority (RA) – entity that is responsible for identification and authentication of subjects of certificates.

Relying party – natural or legal person that relies upon an electronic identification or a trust service. Relying parties include parties verifying a digital signature using a public key certificate.

Root CA – certification authority which is at the highest level within TSP's domain and which is used to sign subordinate CA(s).

Secure Cryptographic Device – Device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user.

Subject – entity identified in a certificate as the holder of the private key associated with the public key given in the certificate.

Subordinate CA – certification authority whose certificate is signed by the root CA, or another subordinate CA.

Subscriber – legal or natural person bound by agreement with a trust service provider to any subscriber obligations.

Signatory – A natural person who creates an electronic signature.

Trust Service – electronic service which enhances trust and confidence in electronic transactions.

Trust Service Provider – natural or a legal person who provides one or more trust services.

Acronyms

CA Certification Authority

CPS Certification Practice Statement

CRL Certificate Revocation List

OCSP On-line Certificate Status Protocol

PKI Public Key Infrastructure

RA Registration Authority

TSP Trust Services Provider

QSCD Qualified Electronic Signature Creation Device

HSM Hardware Security Module

	Short name	**Full name**
English	NAIS	National Agency for Information Society
Albanian	AKSHI	Agjencia Kombëtare e Shoqërisë së Informacionit

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

NAIS operates and maintains a PKI repository which contains:

- Certificate Policy, Certification Practice Statement
- Certificates for NAIS Root CA, NAIS CA and NAIS Class CAs
- Certificate Revocation Lists
- Information on legislation in the field of trust services
- Communications to Subscribers and Relying Parties related to certification service provision
- Terms and conditions for the use of the certificates

The information available in this repository can be accessed in English and in Albanian language at the address akshi.gov.al/repository.

Address of the public LDAP directory: ldap://ldap.akshi.gov.al/.

2.2 Publication of certification information

NAIS is responsible for publishing and updating the information regarding CP, CPS, certificates, current status of certificates, terms and conditions and other relevant information regarding trust services. NAIS will make this information available at the repository. Due to their sensitivity, some information cannot be made publicly available.

2.3 Time or frequency of publication

NAIS reviews the documentation related to trust services annually and in cases of significant changes, to ensure that information is updated and accurate. The changes are published in the repository.

The frequency of publishing CRLs for certificates is defined in the section 4.9.7.

2.4 Access controls on repositories

All information and documentation published by NAIS in the Repository is available to the public at akshi.gov.al/repository.

To protect the integrity of the documentation, NAIS has implemented access controls to prevent unauthorized modifications and deletion of this information.

Only authorized personnel at NAIS can add, modify, update or delete information in the repository while external users can only read and download the available information.

3. IDENTIFICATION AND AUTHENTICATION

This chapter describes the procedures used to authenticate the identity and other attributes of an end-user certificate applicant prior to certificate issuance.

3.1 Naming

3.1.1 Types of names

NAIS Class CAs issue certificates to end-users. Certificates issued by NAIS Class CAs are in compliance with the X.509 V3 standard. The *Subject* field is in line with IETF RFC 5280.

- For certificates issued to natural persons associated with a legal entity, the *Subject* field should contain the person's name and surname, the registered name of the legal entity and its identifier.
- For certificates issued to legal persons, the *Subject* field should contain the full registered name of the legal entity.

3.1.2 Need for names to be meaningful

The names identifying a natural or legal person in the *Subject* field need to be meaningful.

- For natural persons, the name and surname should be the same as the name in the official identification document.
- For legal persons, the name of the legal entity should be the same as the name registered in the National Business Center.

Due to software restrictions, some letters in the Albanian alphabet are replaced as indicated below:

Letter	**Replaced by**
Ë/ë	E/e
Ç/ç	C/c

3.1.3 Anonymity or pseudonymity of subscribers

NAIS does not support the use of pseudonyms or other anonymous identifiers.

3.1.4 Rules for interpreting various name forms

The *Subject* field in the certificates should be interpreted using X.520 standard.

3.1.5 Uniqueness of names

NAIS ensures the uniqueness of each Subject name in the following ways:

- For certificates for electronic signature, the *Subject* field includes a serial number attribute value.
- For certificates for the fiscalization project, the *Subject* field includes a serial number attribute value.
- For certificates for electronic seal, the email of the public institution should be included.

3.1.6 Recognition, authentication, and role of trademarks

No stipulations.

3.2 Initial identity validation

Application process for the following:

- Certificates for electronic signature for private entities,
- Certificates for electronic signature for private entities for critical infrastructure,
- Certificates for electronic signature for government employees,
- Certificates for electronic signature for government employees for critical infrastructure,
- Certificates for the fiscalization project for public institutions,
- Certificates for the fiscalization project for private entities, and
- Certificate Test for the fiscalization project,

is carried out through the e-Albania government portal.

The data in the e-Albania government portal has been previously verified with the data of the National Registry of Civil Status for citizens and the National Commercial Registry for businesses.

After receiving a certificate application from e-Albania, the Registration Officer at NAIS verifies the data.

Applications for certificates for electronic signature for the government employees must go through an extra verification step for identity validation.

Application process for certificate for electronic seal is carried out through an official request submitted at NAIS by the public institution which offers services in the e-Albania portal.

3.2.1 Method to prove possession of private key

The companion private key that corresponds to a public key for which a certificate issuance is requested, is generated by the signatory, creator of a seal or by NAIS.

- **When the private key is generated by NAIS**, the request of presenting proof for the possession of the private key is not applicable. In this case, through secure technological means, NAIS ensures that the private key is linked with the signatory or the creator of the seal.

- **When the private key is not generated by NAIS**, the possession of the private key that corresponds to the public key for which a certificate generation is requested, will be proved by sending the Certificate Signing Request (CSR) (which will include the public key signed by the associated private key) in accordance with the PKCS#10 standard.

3.2.2 Authentication of organization identity

For the following types of certificates:

- Certificates for the fiscalization project for public institutions,
- Certificates for the fiscalization project for private entities, and
- Certificate Test for the fiscalization project,

data regarding the organization is automatically generated via the e-Albania government portal during the application process. This information has been previously verified and validated with the official information of the National Business Center.

For these types of certificates, the following organization information is required:

- TIN (Tax Identification Number)
- Legal name
- Legal representative
- Email and telephone number
- Address

For certificates for electronic seal, the application is submitted via an official request sent to NAIS. During the application process, the following information is required:

- Registration certificate and TIN (Tax Identification Number)
- Legal name
- Legal representative
- Email and telephone number
- Address

3.2.3 Authentication of individual identity

The following information is required for natural persons during the application process:

- Personal Number (National ID)
- Legal name and surname
- Phone number

This information is automatically generated via the e-Albania government portal. The data has been previously verified and validated with the official information of the National Registry of Civil Status.

For natural persons associated with a private entity, the following information is also required:

- Email (which is automatically generated via e-Albania)
- Job position
- TIN of the private entity
- Legal name of the private entity

For government employees, the following information is also required:

- Official email
- Job position
- Name of the public institution
- Organizational unit

3.2.4 Non-verified subscriber information

The Subscriber is entirely responsible for providing accurate and up-to-date information upon application. The information that is automatically generated through the e-Albania has been verified upon registration in the government portal and NAIS does not conduct further verification.

3.2.5 Validation of authority

Prior to issuing certificates to government employees and critical infrastructure operators, NAIS verifies whether the natural person has specific rights or permissions, to obtain a certificate.

3.2.6 Criteria for interoperation

No stipulations.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Routine re-key refers to the certificate renewal process performed for certificates which are about to expire and includes the procedure of generating a new key pair for existing Subjects.

Certificate re-key is processed by the RA Officer at NAIS after receiving a request by the Subject via the e-Albania government portal. The Subject is required to confirm that the data submitted in the initial application process is still valid and correct.

Certificate re-key for certificates issued via secure cryptographic devices is performed by physical presence of the Subject at NAIS premises.

In this case, the Subject is required to submit the following:

- Official request form signed by the administrator of the associated legal entity
- Copy of the official identification document
- The secure cryptographic token (USB Token)

3.3.2 Identification and authentication for re-key after revocation

Identification and authentication for re-key after revocation follows the same process as the initial identification procedure referred to in section 3.2.

3.4 Identification and authentication for revocation request

For certificates for electronic signature for government employees and certificates for electronic signature for government employees for critical infrastructure, a revocation request can be submitted:

- By the Subject, by submitting a request to pki@akshi.gov.al using the official email address that was used in the initial application process
- By the public institution, via an official request submitted to NAIS

For certificates for electronic seal and certificates for the fiscalization project for public institutions, the revocation request can be submitted by the institution via an email sent to pki@akshi.gov.al or an official request submitted to NAIS.

For the following certificates:

- Certificate for electronic signature for private entities
- Certificate for electronic signature for private entities for critical infrastructure
- Certificate for the fiscalization project for private entities
- Certificate Test for the fiscalization project

a revocation request can be submitted to pki@akshi.gov.al by the Subject using the same email address that was used in the initial application process. The request is validated by the PKI Sector by comparing the data submitted with the data in the RA. If the data match, the revocation request is accepted.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Application for the following certificates:

- Certificate for electronic signature for private entities can be submitted by the Subject of the certificate who is an Albanian citizen associated with a private entity in Albania or a foreign citizen who owns a business in Albania.
- Certificate for electronic signature for government employees can be submitted by the Subject of the certificate who is a government employee in Albania.
- Certificate for electronic signature for private entities for critical infrastructure can be submitted by the Subject of the certificate who is an Albanian citizen associated with a private entity in Albania operating on critical infrastructure or accessing international systems.
- Certificate for electronic signature for government employees for critical infrastructure can be submitted by the Subject of the certificate who is a government employee in Albania operating on critical infrastructure or accessing international systems.
- Certificates for electronic seal can be submitted by a public institution in Albania which offers services in the e-Albania government portal.
- Certificates for the fiscalization project for public institutions can be submitted by a public institution in Albania.
- Certificates for the fiscalization project for private entities can be submitted by the private entity in Albania.
- Certificate Test for the fiscalization project can be submitted by a private entity in the IT field in Albania, interested in developing software applications in the context of the fiscalization project.

4.1.2 Enrollment process and responsibilities

The application process for the following:

- Certificates for electronic signature for private entities,
- Certificates for electronic signature for private entities for critical infrastructure,
- Certificates for electronic signature for government employees,
- Certificates for electronic signature for government employees for critical infrastructure,
- Certificates for the fiscalization project for public institutions,
- Certificates for the fiscalization project for private entities, and
- Certificate Test for the fiscalization project,

is carried out through the e-Albania government portal.

The Subscriber shall sign an agreement with NAIS in electronic form before the submission of the application. By signing the agreement, the Subscriber accepts the terms and conditions of the agreement and the conditions of this CP/CPS. It is the Subscriber's responsibility to make sure the information filled in the application form is complete and accurate.

The obligations and responsibilities of CA, RA, and Subscriber are given in section 9.6 herein.

The application process for certificates for electronic seal is carried out through an official request sent to NAIS. The Subscriber shall sign an agreement with NAIS during the application process. By signing the agreement, the Subscriber accepts the terms and conditions of the agreement and the conditions of this CP/CPS.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Upon the receipt of the application, the RA Officer reviews the application and data submitted within the processing time described in section 4.2.3. Identification and authentication of the identity of natural and legal persons is described in chapter 3 herein.

4.2.2 Approval or rejection of certificate applications

The RA Officer validates the data that the applicant has submitted. If the data is correct, the application is accepted and forwarded to CA. If there are any inconsistencies or incorrect information, the application is rejected.

4.2.3 Time to process certificate applications

The normal time for processing certificate applications is 10 business days.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CA will process requests and proceed with certificate issuance only after receiving a certificate request from RA. The CA and the RA are trusted systems, integrated together. The *Serial Number* field in the certificate ensures the uniqueness of the certificates.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The RA Officer at the PKI Sector notifies the Subscriber about the issuance of the certificate.

- For certificates for electronic signature in the Remote Signing Service Platform:
  - Certificate for electronic signature for private entities
  - Certificate for electronic signature for government employees

  the PKI Sector sends an email to the Subscriber providing instructions for login to the Remote Signing Service Platform. The certificate is generated when the Subject signs for the first time.

- For certificates issued via USB Token:
  - Certificate for electronic signature for private entities for critical infrastructure
  - Certificate for electronic signature for government employees for critical infrastructure

  the PKI Sector send an email to the Subscriber notifying them about the issuance of the certificate. Subscribers must physically present themselves at NAIS to receive the USB Token.

- For certificates for electronic seal, the PKI Sector sends an e-mail to the Subscriber notifying them about the issuance of the certificate.

- For certificates for the fiscalization project:
  - Certificate for the fiscalization project for public institutions
  - Certificate for the fiscalization project for private entities
  - Certificate Test for the fiscalization project

  the PKI Sector sends an email to the Subscriber notifying them about the issuance of the certificate. The certificate can be downloaded via their account on e-Albania.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The certificate is considered accepted by the Subject upon signing the declaration on terms and conditions and after the Subject's first use of the certificate.

The Subject has the right to reject the certificate before the first use, provided at least one of the following applies:

- The information in the certificate is incorrect.
- The information in the certificate is no longer valid (from the application date).
- The Subject is no longer entitled to the certificate (for example when the natural person associated with the legal entity has terminated the relationship with the legal entity).

4.4.2 Publication of the certificate by the CA

If the Subscriber has authorized the public disclosure of the certificate, NAIS will make the certificate available for relying parties in the repository. Publication of the certificates is described in chapter 2.

4.4.3 Notification of certificate issuance by the CA to other entities

Notification of certificate issuance to other entities is done through the publication of the certificate in the repository as described in chapter 2 herein.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

a. Subject private key is generated and controlled by NAIS

When NAIS generates and controls the private key, NAIS is responsible for:

- Ensuring usage of the Subject's key pair in accordance with the rules specified in this CP/CPS.
- Establishing technical and security controls to ensure that the use of the private key is under the sole control of the signatory or creator of the seal.

b. Subject is in possession of and manages the private key

When the Subject is in possession of and manages the private key, the Subject is responsible for:

- Using the private key and certificate only for the intended use as set forth in this CP/CPS and in the declaration on terms of use of the certificate.
- Certificate should be used in consistency with the key usage field.
- Protecting the private key from theft, loss, compromise or unauthorized use.
- Ensuring that the private key is under the sole control of the signatory or creator of the seal.
- Notifying NAIS to request certificate revocation in case the private key has been lost, stolen, compromised or when the Signatory or Creator of a seal is no longer in the sole possession of the private key.
- Ensuring the confidentiality of the secret activation data and not sharing it with another party.
- Notifying NAIS in case the certificate data is incorrect or for some reason becomes invalid after the registration process.
- Correct usage of the secure cryptographic device, when the Subject has received a cryptographic device from NAIS.

4.5.2 Relying party public key and certificate usage

The relying party that intends to rely on certificates which are issued according to this CPS should:

- Rely on certificates only for appropriate use as set forth in this CP/CPS and in consistency with the certificate key usage field.
- Use the certificate for the purposes of the electronic signature/seal and its corresponding public key solely to validate the electronic signature/seal.
- Assume responsibility to check the status of a certificate using the mechanisms set forth in this CP/CPS.

If the certificate has been revoked or has expired the relying party should stop trusting the certificate. By relying on an expired or revoked certificate the relying party loses the warranties provided by NAIS as a trust service provider.

4.6 Certificate renewal

Certificate renewal means the issuance of a new certificate to the subscriber without changing the subscriber or other participant's public key or any other information in the certificate.

NAIS does not renew existing certificates for existing keys. The only way of renewal is to generate a new key pair and issue a new certificate for an existing Subject whose certificate expires soon.

Refer to section 4.7 for information on certificate renewal.

4.6.1 Circumstance for certificate renewal

Refer to section 4.7.

4.6.2 Who may request renewal

Refer to section 4.7.

4.6.3 Processing certificate renewal requests

Refer to section 4.7.

4.6.4 Notification of new certificate issuance to subscriber

Refer to section 4.7.

4.6.5 Conduct constituting acceptance of a renewal certificate

Refer to section 4.7.

4.6.6 Publication of the renewal certificate by the CA

Refer to section 4.7.

4.6.7 Notification of certificate issuance by the CA to other entities

Refer to section 4.7.

4.7 Certificate re-key

This section describes certificate renewal in cases of generating a new key pair and a new certificate for existing Subjects.

4.7.1 Circumstance for certificate re-key

NAIS performs certificate rekeying for existing Subjects for valid digital certificates which do not require changes of the certificate data or extensions. The rekeying process consists of re-issuing a certificate with a new key pair to extend its expiry date without changing the identity of the Subject or other certificate extensions.

NAIS notifies Subscribers via the same email used in the registration process regarding the certificate validity date 30 days before expiry.

4.7.2 Who may request certification of a new public key

Certificate re-key can be requested by the Subject or Subscriber, as the case may be, by sending a request to PKI Sector at NAIS.

4.7.3 Processing certificate re-keying requests

Certificate re-key is processed by the RA Officer at the PKI Sector after receiving a request by the Subject via the same email used in the initial registration process. The Subject is required to confirm that the data submitted in the initial application process is still valid and correct.

4.7.4 Notification of new certificate issuance to subscriber

The process used for initial certificate issuance applies.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

The process used for initial certificate issuance applies.

4.7.6 Publication of the re-keyed certificate by the CA

The process used for initial certificate issuance applies.

4.7.7 Notification of certificate issuance by the CA to other entities

The process used for initial certificate issuance applies.

4.8 Certificate modification

Certificate modification refers to issuance of a new certificate due to changes in the information in the certificate other than the Subscriber's public key.

NAIS does not perform modifications of the issued certificates. The Subject or the Subscriber, as the case may be, should submit a request for revocation of the certificate in case where the information included in the certificate is no longer valid.

4.8.1 Circumstance for certificate modification

Not applicable.

4.8.2 Who may request certificate modification

Not applicable.

4.8.3 Processing certificate modification requests

Not applicable.

4.8.4 Notification of new certificate issuance to subscriber

Not applicable.

4.8.5 Conduct constituting acceptance of modified certificate

Not applicable.

4.8.6 Publication of the modified certificate by the CA

Not applicable.

4.8.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.9 Certificate revocation and suspension

Revoked certificates refer to certificates that are no longer considered valid by the certificate issuer. Certificates issued by NAIS can be revoked. The process of certificate revocation is irreversible. This section describes the process of certificate revocation.

4.9.1 Circumstances for revocation

The following conditions describe circumstances under which a certificate is revoked:

- The Subject requests the certificate revocation.
- The information contained in the certificate has changed or is no longer valid.
- The private key associated with the public key was either compromised or there is strong reason to believe it has been compromised.
- In the case of certificates issued for natural persons associated with a legal entity (i.e. certificates issued for electronic signature), the relationship between the natural person and the legal entity has ended (i.e. employment has been terminated).
- Subscribers do not agree with and do not accept the terms and conditions specified in an updated CPS.
- NAIS terminates its activity. In this case, all certificates issued by NAIS CAs will be revoked along with the certificates of the CAs.
- The private key of NAIS CAs under which the end-entity certificate was issued, has been compromised.
- The Subject does not comply with the rules of this CP/CPS or Subscriber declaration on terms and conditions.
- The secure cryptographic device has been lost, stolen or compromised.

4.9.2 Who can request revocation

A revocation request can be requested by the following:

- The Subject who is identified as the holder of the private key associated with the public key given in the certificate.
- The Registration Authority which can request revocation either on behalf of a Subject or if it has information that justifies the certificate revocation under the circumstances described in section 4.9.1.

4.9.3 Procedure for revocation request

The process of submission of a certificate revocation request and the process for identification and authentication of revocation requests is described in section 3.4.

After the Revocation Officer has accepted the revocation request, the request is forwarded to the corresponding NAIS Class CA.

The information about the revoked certificates is placed on the Certificate Revocation List (CRL) issued by NAIS Class CAs.

4.9.4 Revocation request grace period

Revocation request should be submitted as soon as a circumstance for revocation arises.

4.9.5 Time within which CA must process the revocation request

NAIS performs the revocation of the certificate within 24 hours upon receiving the revocation request.

4.9.6 Revocation checking requirement for relying parties

Relying parties should use the mechanisms provided by NAIS to check the status of certificates on which they wish to rely on. Information about revocation is published using CRLs and OSCP.

4.9.7 CRL issuance frequency

NAIS Class CAs issue their respective Certificate Revocation Lists. CRLs are published within 24 hours of receiving a certificate revocation request and are automatically updated every 5 days.

4.9.8 Maximum latency for CRLs

The CRL issuance frequency is in accordance with section 4.9.7. CRLs are published without delay.

4.9.9 On-line revocation/status checking availability

NAIS Class CAs support the online verification of the issued certificate revocation status via NAIS OCSP service.

NAIS OCSP service address is ocsp.akshi.gov.al, and it is entered in the Authority Information Access extension of all certificates issued by NAIS Class CAs.

4.9.10 On-line revocation checking requirements

In order to use the NAIS OCSP service, the relying party must have an application solution which can use the OCSP service by using the GET or POST method.

4.9.11 Other forms of revocation advertisements available

No stipulations.

4.9.12 Special requirements re key compromise

No stipulations.

4.9.13 Circumstances for suspension

NAIS does not perform certificate suspensions.

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

Mechanisms used by NAIS for certificate status services are CRL and OCSP.

CRLs are published on the NAIS server and in the directory. CRL publication addresses are also contained in the *CRL Distribution Points* extension of every issued certificate.

- NAIS CA certs.akshi.gov.al/ca.crl
- NAIS Class 1 CA certs.akshi.gov.al/class1.crl
- NAIS Class 2 CA certs.akshi.gov.al/class2.crl
- NAIS Class 3 CA certs.akshi.gov.al/class3.crl
- NAIS Class 4 CA certs.akshi.gov.al/class4.crl

The NAIS OCSP service address is ocsp.akshi.gov.al, and it is entered in the *Authority Information Access* extension for all certificates issued by NAIS CAs.

4.10.2 Service availability

Certificate status services are available 24 hours a day, 7 days a week.

4.10.3 Optional features

No stipulations.

4.11 End of subscription

End of subscription occurs if:

- The certificate of the Subject has expired and the Subject does not request certificate renewal.

- The Subscriber terminates the agreement before the certificate expiry date. In this case NAIS revokes the certificate that is subject to this agreement.

4.12 Key escrow and recovery

Key escrow of Subscriber private keys is not allowed.

4.12.1 Key escrow and recovery policy and practices

No stipulations.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulations.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

NAIS performs its CA and RA operations in a primary production site with multiple levels of physical and technical security controls.

A secondary location is used as a disaster recovery center, for the purpose of recovery and restoration of the services in cases of a natural disaster or system failure. This location is protected by physical security controls with the same level of security as those implemented at the primary production site.

5.1.2 Physical access

NAIS has deployed a physical access control system to ensure that only authorized personnel can have access to the production site. Logs of physical access are maintained.

Physical control measures have been established to protect critical equipment from unauthorized access and to reduce the risk of equipment tampering.

High-security zones can be accessed only by authorized personnel assigned trusted roles and only under the principle of dual control.

Physical access is controlled and monitored by security alarm systems and video surveillance 24/7.

5.1.3 Power and air conditioning

Premises where CA/RA operations are performed and systems and equipment are located, are equipped with primary and secondary power supplies to ensure continuous and uninterrupted access to electric power.

These premises use HVAC systems for heating, cooling, and air ventilation to prevent overheating and maintain appropriate humidity levels.

5.1.4 Water exposures

Premises where equipment are located are ensured against floods and placed on raised flooring.

5.1.5 Fire prevention and protection

NAIS has implemented a fire alarm and fire suppression mechanism at the premises where the PKI infrastructure is located, compliant with fire safety standards and regulations.

5.1.6 Media storage

Media containing data of NAIS PKI are stored safely at the primary facility in a way that ensures protection from accidental damage and unauthorized physical access. Backup files are maintained at another location, separate from the primary facility.

5.1.7 Waste disposal

Documentation and data of NAIS PKI that are no longer needed or that have reached the retention period are destroyed in a safe manner. Disposal of special equipment such as HSMs follows the recommendations provided by the manufacturer.

5.1.8 Off-site backup

NAIS performs backups to secure off-site locations. The frequency, retention, and extent of the backup is determined by NAIS internal policy.

5.2 Procedural controls

5.2.1 Trusted roles

Trusted roles within NAIS PKI follow the recommendations described in ETSI EN 319 401 and ETSI EN 319 411-1. Following these recommendations, NAIS has appointed the following trusted roles to perform duties related to the provision of trust services:

1. **Security Officer** with the overall responsibility of administering the implementation of the security practices.
2. **System Administrator** who's authorized to install, configure and maintain the NAIS trustworthy systems for service management.
3. **System Operator** who's responsible for operating the NAIS trustworthy systems on a day-to-day basis. This role is also authorized to perform system backup.
4. **System Auditor** who's authorized to view archives and audit logs of NAIS trustworthy systems.
5. **Registration Officer** with the overall responsibility of verifying information for certificate issuance and approval of certification requests.
6. **Revocation Officer** with the overall responsibility of performing certificate status changes.

5.2.2 Number of persons required per task

For critical operations where dual control is needed, at least two persons who are assigned trusted roles need to be present.

5.2.3 Identification and authentication for each role

NAIS employees who are assigned a trusted role need to be identified and authenticated to access NAIS premises, critical systems, and high security zones. Every employee is equipped with an access control card. Multi-factor authentication is required to access critical systems for performing CA/RA operations.

5.2.4 Roles requiring separation of duties

NAIS has established security controls to ensure the separation of duties for trusted roles described in section 5.2.1. In particular, the roles of administrator, operator, and auditor can't be performed by one person.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

NAIS follows internal organizational procedures to ensure that employees who are involved in the delivery of trust services have the adequate knowledge, experience and expertise.

Additional requirements are applied for personnel assigned in trusted roles to ensure their integrity, trustworthiness, and commitment in protecting classified information.

All NAIS employees are required to be equipped with the security certificate from the Classified Information Security Directorate in Albania.

5.3.2 Background check procedures

As part of the application process to be equipped with the security certificate from the Classified Information Security Directorate, employees have to complete a detailed security questionnaire and sign a declaration for the protection of classified information.

Background checks and clearance procedures are carried out by the Classified Information Security Directorate in accordance with the law on classified information.

5.3.3 Training requirements

NAIS ensures that employees involved in the provision of certification services are equipped with the necessary knowledge needed to perform their duties.

Personnel involved in the delivery of trust services is trained in the following areas:

- Requirements of NAIS internal information security policies,
- Requirements of certification practice statement,
- PKI software used in the provision of certification services,
- Disaster recovery and business continuity procedures,
- Performing daily operations and individual duties based on the assigned role.

5.3.4 Retraining frequency and requirements

New employees have to go through the training areas mentioned in section 5.3.3. Throughout their employment, NAIS makes sure that personnel involved in the provision of certification services receive training, mentoring and support when needed.

In case of changes in the provision of trust services, changes in operation or adaptation of a new technology, retraining is required.

Information security awareness training is performed at least once a year for all employees.

5.3.5 Job rotation frequency and sequence

No stipulations.

5.3.6 Sanctions for unauthorized actions

Sanctions for unauthorized actions and disclosure of confidential information are defined in the NAIS internal regulation. These sanctions can vary from disciplinary actions, termination of employment to civil or criminal proceedings.

5.3.7 Independent contractor requirements

Requirements for independent contractors are defined in the contractual agreement with NAIS. Organizations providing services to NAIS PKI are required to be ISO 27001 certified. Work of independent contractors at NAIS premises is supervised by NAIS employees assigned trusted roles. The same requirements for the protection of confidential information that are applied for NAIS employees are applicable for independent contractors.

5.3.8 Documentation supplied to personnel

NAIS provides to personnel all the documentation necessary to perform their duties. This includes the information security policies, internal operational procedures, manuals and work instructions. Other documentation is provided on a need-to-know basis depending on specific job functions.

5.4 Audit logging procedures

5.4.1 Types of events recorded

NAIS ensures that relevant information concerning the operation of the trusted services is recorded.

The following events are logged (either manually or automatically):

- CA and certificate lifecycle management events such as key generation, backup, storage, and recovery, CRL updates, etc.
- Subscriber certificate and key life cycle management events such as certificate applications, issuance, renewal, and revocation as well as key generation, backup, storage and recovery.
- Security-related events such as system downtime, hardware failures, system actions performed by NAIS personnel in trusted roles, access in high security zones, etc.

These logs include information on the date and time of entry and identity of the entity making the log entry.

5.4.2 Frequency of processing log

NAIS monitors systems on a continuous basis to provide real-time alerts of security events. These events are reviewed on a periodic basis by NAIS personnel assigned in trusted roles.

5.4.3 Retention period for audit log

Retention period for audit log is described in the internal procedure.

5.4.4 Protection of audit log

Audit logs are protected by mechanisms and procedures ensuring confidentiality and integrity of the logs and protection from unauthorized viewing, modification, deletion, or other tampering.

5.4.5 Audit log backup procedures

Incremental backups of audit logs and full backups are performed on a periodic basis as defined by the internal backup procedure.

5.4.6 Audit collection system (internal vs. external)

The automated audit collection process is performed at the application, network and operating system level. Manually generated audit data is recorded by NAIS personnel assigned in trusted roles.

5.4.7 Notification to event-causing subject

For events which are logged by the audit collection system, no notice is required to be given to the participant that caused the event, unless such notice is compulsory according to the law.

5.4.8 Vulnerability assessments

NAIS performs regular vulnerability assessments to identify and assess internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of assets, including certification services and sensitive data. Penetration test is performed on periodic basis as described in internal procedure. NAIS outsources external parties for conducting penetration testing.

5.5 Records archival

5.5.1 Types of records archived

NAIS archives the following data either in electronic or paper format:

- Certificate Policy/Certification Practice Statement
- Declaration on terms and conditions of trusted services
- Certificate applications and data collected during this process
- Certificate lifecycle information
- Data related to NAIS CAs key pair generation and NAIS CAs certificates
- Internal policies, procedures, and work instructions
- Log information referred to in section 5.4.1

5.5.2 Retention period for archive

Retention period for archives is defined in the internal procedure.

5.5.3 Protection of archive

NAIS protects archived records and information so that only authorized personnel can have access to the archive. Archives are protected by mechanisms and procedures ensuring confidentiality and integrity of the logs and protection from unauthorized viewing, modification, deletion, or other tampering.

5.5.4 Archive backup procedures

Incremental backups of audit logs and full backups are performed on a periodic basis as defined by the internal backup procedure.

5.5.5 Requirements for time-stamping of records

No stipulations.

5.5.6 Archive collection system (internal or external)

Documentation in paper form is collected manually and archived internally at NAIS protected premises. Records in electronic form are collected automatically and archived internally.

5.5.7 Procedures to obtain and verify archive information

Only authorized personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key changeover

To ensure the continuity of certification services, NAIS will generate a new pair of CA keys in advance of expiration of one of the certificates of NAIS CAs.

The generation of a CA key pair is described in section 6.1 herein. The new certificate with a newly generated public key will be signed by NAIS Root CA.

NAIS will notify in advance the PKI participants regarding the key modification.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

NAIS has developed an incident response procedure within the Information Security Management System for handling incidents, reducing the risk to systems and data, and returning systems to operational state as quickly as possible.

NAIS has appointed trusted role personnel to follow up on alerts of critical systems to ensure that relevant incidents are reported in line with the established procedure.

Within 24 hours of the breach being identified, NAIS should notify the National Authority on Electronic Certification and Cyber Security in Albania.

If the breach of security has had an adversarial effect on a natural or legal person to whom the trusted service has been provided, NAIS will also notify the natural or legal person.

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

If computing resources, software or data are corrupted, NAIS takes appropriate measures, as described in internal procedure, for incident investigation, appropriate escalation and incident response.

As part of the Information Security Management System, NAIS has implemented a Business Continuity Policy.

5.7.3 Entity private key compromise procedures

In case the private key of any of the NAIS CAs is compromised, NAIS will revoke the CA certificate that is associated with the compromised key. NAIS will notify the affected PKI participants of the key compromise and certificate revocation.

After the root cause of the key compromise is evaluated and measures are taken to prevent the event from happening in the future, NAIS will generate a new CA key pair and NAIS Root CA will issue a new certificate. The new CA will issue certificates to the affected Subscribers.

5.7.4 Business continuity capabilities after a disaster

NAIS uses a secondary location as a disaster recovery center and will move the operations to this secondary site in case of a disaster. The internal Business Continuity Policy describes the steps which will be taken in more detail.

5.8 CA or RA termination

Before terminating the CA activities, NAIS will:

- Provide notice to the National Authority on Electronic Certification and Cyber Security in Albania.
- Inform all subscribers, relying parties and other PKI participants regarding the termination of certification services.
- Transfer the continuation of certification service provision to another Qualified Trust Service Provider. During this process, NAIS will deliver to the new QTSP all the documentation collected during the registration process of Subscribers and documentation on issued certificates. NAIS will also transfer to the new QTSP all obligations to continue smooth operation of certification services.
- Revoke all issued certificates and destroy Subscriber's private keys (when NAIS manages the private keys on behalf of the Subscriber).
- Revoke the CA certificates and destroy the private keys of NAIS CAs that will no longer continue their operation.

6. TECHNICAL SECURITY CONTROLS

This chapter describes security measures taken by NAIS to protect NAIS CAs cryptographic keys and activation data. It also describes other technical security controls used by NAIS CAs to securely perform functions such as key generation, user authentication, certificate registration, certificate revocation, auditing, and archiving.

6.1 Key pair generation and installation

6.1.1 Key pair generation

Generation of NAIS CAs Key Pair

The generation of the NAIS CAs key pair is performed in accordance with the documented internal process, in a high security zone. This process is performed by suitable personnel in accordance with the assigned trusted roles, under at least dual control and is witnessed from authorized persons at NAIS PKI.

Cryptographic algorithms used for key generation and key length for NAIS CAs are based on recommendations specified in ETSI TS 119 312.

Subscriber Key Pair Generation

a. Subscriber key pair generation inside HSM

The HSM used for key generation is in compliance with the requirements described in section 6.2. In this case, the key pair generation is performed in a high secure zone. This applies for key pair generation for certificates used in the Remote Signing Service Platform:

- Certificate for electronic signature for private entities
- Certificate for electronic signature for government employees

b. Subscriber key pair generation in a secure cryptographic device (USB Token)

The secure cryptographic device used for key generation is in compliance with the requirements described in Section 6.2. The key pair can be generated by RA Officer at NAIS, in a high secure zone. This applies for the following certificates:

- Certificate for electronic signature for private entities for critical infrastructure
- Certificate for electronic signature for government employees for critical infrastructure

c. Subscriber key pair generation in a software module

Key pair generation is performed within a secure software module in PKCS#12 format. In this case the key pair is generated by the RA Officer. This applies for the following certificates:

- Certificate for electronic seal
- Certificate for the fiscalization project for public institutions
- Certificate for the fiscalization project for private entities
- Certificate Test for the fiscalization project

6.1.2 Private key delivery to subscriber

In cases where NAIS generates and manages the private key on behalf of the signatory or the creator of the seal, NAIS ensures the secure storage of the private key. NAIS applies security controls for the protection of the private key from disclosure, corruption and unauthorized reproduction.

If the key pair is generated by the subscriber, the private key is considered to be in the possession of the subscriber.

In cases where NAIS delivers the private key to the subscriber:

- If NAIS generates the private key in a software module, the private key is delivered to the subscriber through a secure channel in PKCS#12 format.
- If NAIS generates the private key in a secure cryptographic device, the private key is delivered to the subscriber via the secure cryptographic device in person, at NAIS premises.

6.1.3 Public key delivery to certificate issuer

In cases when NAIS generates and manages the key pair on behalf of the signatory or the creator of the seal, delivery of public key to NAIS is not necessary.

In cases when the key pair is generated by the subscriber, the subscriber will submit a Certificate Signing Request (CSR) (which will include the public key signed by the associated private key) in accordance with the PKCS#10 standard.

6.1.4 CA public key delivery to relying parties

NAIS CAs public keys are available to relying parties in NAIS CAs certificates issued by NAIS Root CA to ensure integrity and verification of the certificate chain.

NAIS has made the certificates publicly available in the repository akshi.gov.al/repository. Access controls of the repository are described in section 2.4 herein.

Links for direct retrieving of NAIS Root CA, NAIS CA, NAIS Class CAs certificates are:

Root certificate:

- NAIS Root CA: certs.akshi.gov.al/root.crt

Subordinate certificate:

- NAIS CA: certs.akshi.gov.al/ca.crt

Class certificates:

- NAIS Class 1 CA: certs.akshi.gov.al/class1.crt
- NAIS Class 2 CA: certs.akshi.gov.al/class2.crt
- NAIS Class 3 CA: certs.akshi.gov.al/class3.crt
- NAIS Class 4 CA: certs.akshi.gov.al/class4.crt

6.1.5 Key sizes

The key sizes are as follows:

- NAIS Root CA uses sha256WithRSA algorithm with 4096-bit long keys

- NAIS CA uses sha256WithRSA algorithm with 2048-bit long keys
- NAIS Class CAs use sha256WithRSA algorithm with 2048-bit long keys
- Subscriber certificates use 2048-bit long RSA key pairs

6.1.6 Public key parameters generation and quality checking

Generation of the key pair for all NAIS CAs is performed using generation parameters recommended in ETSI TS 119 312.

NAIS ensures quality checking by using HSM modules and secure cryptographic devices which are in compliance with the standards referred to in section 6.2 herein.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Section 7.1.2 provides information on the *KeyUsage* field of certificates issued by NAIS complying with X.509 V3 standard.

The bits set in the *KeyUsage* field are used as follows:

- digitalSignature bit (0) is asserted when the subject public key is used for verifying digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), such as those used in an entity authentication service, a data origin authentication service, and/or an integrity service.
- nonRepudiation bit (1) is asserted when the subject public key is used to verify digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), used to provide a non-repudiation service that protects against the signing entity falsely denying some action.
- keyEncipherment bit (2) is asserted when the subject public key is used for enciphering private or secret keys, i.e., for key transport.
- dataEncipherment bit (3) is asserted when the subject public key is used for directly enciphering raw user data without the use of an intermediate symmetric cipher.
- keyAgreement bit (4) is asserted when the subject public key is used for key agreement.
- keyCertSign bit (5) is asserted when the subject public key is used for verifying signatures on public key certificates.
- cRLSign bit (6) is asserted when the subject public key is used for verifying signatures on certificate revocation lists.
- encipherOnly bit (7) - when the *encipherOnly* bit is asserted and the *keyAgreement* bit is also set, the subject public key may be used only for enciphering data while performing key agreement.
- decipherOnly bit (8) - when the *decipherOnly* bit is asserted and the *keyAgreement* bit is also set, the subject public key may be used only for deciphering data while performing key agreement.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The HSMs used for the protection of private keys for NAIS CA and NAIS Class CAs meet the requirements of FIPS 140-2 Level 3.

The protection of Subscribers' private keys for:

- Certificates used in the Remote Signing Service Platform is carried out by a remote QSCD using HSMs compliant with FIPS 140-2 Level 3 standard.
- Certificates for critical infrastructure operators is carried out by secure cryptographic devices which meet the requirements of the FIPS 140-2 Level 2 or 3.

- Certificates issued as software certificates, the private key is protected by a software token.

6.2.2 Private key (n out of m) multi-person control

The HSMs, which are used for the protection of private keys for NAIS CA and NAIS Class CAs, are located in a high-security zone which can be accessed only under dual control of authorized personnel who are assigned trusted roles at NAIS PKI.

Generation of NAIS Class CAs key pair is described in section 6.1.1.

6.2.3 Private key escrow

NAIS CA and NAIS Class CAs private key escrow is not allowed. Private keys of subscribers are not in escrow.

6.2.4 Private key backup

NAIS performs backup of private keys to ensure recovery in case of emergency. Private key backup for NAIS CA and NAIS Class CAs is performed by trusted roles, under the dual control principle, in a high security zone. When used outside of the HSM, the private keys are always in an encrypted form.

6.2.5 Private key archival

Private keys of NAIS CA, NAIS Class CAs and Subscribers are not archived.

6.2.6 Private key transfer into or from a cryptographic module

Private key transfer into or from the HSM can only be performed by authorized personnel who are assigned trusted roles, under the dual control principle, in a high security zone.

The transfer of the private key into or from the HSM is performed in a way that ensures the same security level as when the key is inside the HSM. In such cases, the private key is always protected by encryption.

Transfer of the private key might occur during backup procedures or in cases of module failure.

6.2.7 Private key storage on cryptographic module

NAIS uses HSMs to protect the private keys. HSMs are located in a high security zone which can be accessed only by authorized personnel who are assigned trusted roles. Private keys used in certificates for electronic signature in the Remote Signing Service Platform, can be used only when they are properly activated.

6.2.8 Method of activating private key

Activation of NAIS CAs private keys on hardware cryptographic modules is carried out under dual control by authorized personnel assigned trusted roles at NAIS.

When the private key of the Subject is stored on a secure cryptographic device, the private key is under the sole control of the Subject. The key can be accessed only by using the secret activation data.

For certificates for electronic signature which will be used in the Remote Signing Service Platform, the signature activation module allows Subjects to retain exclusive control over their keys.

6.2.9 Method of deactivating private key

Deactivation of NAIS CAs private keys is carried out in accordance with the procedure described in the manual for the HSMs. This process is performed under dual control by authorized personnel assigned trusted roles at NAIS.

For certificates used in the Remote Signing Service Platform, private keys are deactivated after the signing process has finished.

For certificates stored in a secure cryptographic device, the Subject can deactivate the private key by physically removing or detaching the device.

6.2.10 Method of destroying private key

Private keys of NAIS CAs are destroyed by NAIS personnel assigned trusted roles, in the presence of a representative from NAIS management to ensure that private keys cannot be retrieved or used again. The process is carried out in accordance with the steps described in the HSM manual.

6.2.11 Cryptographic Module Rating

Refer to section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

All NAIS CAs and Subscriber public keys are archived. Section 5.5 describes the process of archival.

6.3.2 Certificate operational periods and key pair usage periods

Usage period of public keys is set in the validity field of every public key certificate. The private key period of validity is equal to the period of validity of the corresponding certificate.

- The validity period of NAIS CA is 15 years.
- The validity period of NAIS Class CAs is 7 years.
- The validity period of a Subscriber certificate is one year.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data related to NAIS CAs private keys are generated and installed during NAIS CAs key pair generation.

Activation data used to protect secure cryptographic devices containing Subject's private keys are generated in accordance with the manual of the cryptographic device.

Activation data for private keys used in the Remote Signing Service Platform consist of activation data associated with HSM which are generated in accordance with the manual of the HSM.

6.4.2 Activation data protection

The activation data related to NAIS CAs private keys are stored in a secure manner, using a combination of control mechanisms to protect them from disclosure.

Activation data of secure cryptographic devices are delivered to the Subscriber in a secure manner, by a separate channel. NAIS recommends the Subscriber to change the activation data on the cryptographic device prior to the first use. After several unsuccessful attempts to access the cryptographic module, this will result in its blockage.

6.4.3 Other aspects of activation data

No stipulations.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Only authorized persons assigned trusted roles can have access to systems and applications which are used in the provision of certification services. Access to these systems is granted based on the specific job functions. Segregation of duties is performed for the assigned trusted roles described in section 5.2.1 herein.

System monitoring procedures are in place to detect and respond to unusual activity or unauthorized access.

NAIS has implemented technical solutions to protect the trustworthy systems against malware.

An internal procedure for password management requires users the use of strong passwords and change of these passwords on a periodic basis.

All media containing sensitive data, audit, archive, or backup information are protected through appropriate physical and logical access controls.

6.5.2 Computer security rating

No stipulations.

6.6 Life cycle technical controls

6.6.1 System development controls

NAIS uses trustworthy systems for the provision of certification services which have undergone an extensive security testing process before being approved for usage within PKI environments.

Software that is developed on behalf of NAIS goes through secure development procedures before moving to the production environment.

NAIS has established a procedure for change management. Changes made to the software are implemented in accordance with this procedure.

6.6.2 Security management controls

NAIS has policies and mechanisms in place to control and monitor the configuration of the systems used for the provision of certification services. NAIS validates the integrity of its systems on a periodic basis.

6.6.3 Life cycle security controls

NAIS performs periodic review of policies, systems and other assets to ensure their continuing suitability, adequacy and effectiveness. NAIS has implemented an internal capacity management process to monitor and estimate the capacity requirements of systems used in the provision of certification services.

6.7 Network security controls

NAIS performs all its CA and RA functions using networks secured in accordance with ISMS to prevent unauthorized access and other malicious activity.

NAIS performs segmentation of certification systems into networks/zones based on their functional, logical, and physical relationship. Network zones are separated by firewalls and equal security measures are applied to systems located within the same network zone.

The security level of the internal network and external connections is monitored.

6.8 Time-stamping

Certificates, CRLs, and other revocation entries contain time and date information. Time in NAIS certification systems is synchronized with UTC time.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

The profile of basic fields for **NAIS Root CA** certificate is described below:

Field name	Value	
Version	Version 3	
Serial Number	11530b05a0db73c682	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Root Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Valid from	Thursday, February 11, 2016 11:06:42 AM	
Valid to	Saturday, February 9, 2041 11:06:42 AM	
Subject	Organizational Unit (OU)	NAIS Root Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Subject Public Key Info	RSA (4096 Bits)	
Signature	sha256WithRSAEncryption	

The profile of basic fields for **NAIS CA** certificate is described below:

Field name	Value
Version	Version 3
Serial Number	1001352ea8aaad2022fd

Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Root Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Valid from	Thursday, February 11, 2016 11:16:06 AM	
Valid to	Monday, February 10, 2031 11:16:06 AM	
Subject	Organizational Unit (OU)	NAIS Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Subject Public Key Info	RSA (2048 Bits)	
Signature	sha256WithRSAEncryption	

The profile of basic fields for **NAIS Class 1 CA** certificate is described below:

Field name	Value	
Version	Version 3	
Serial Number	2001b464c5574b29f500	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Valid from	Thursday, February 11, 2016 11:19:53 AM	
Valid to	Friday, February 10, 2023 11:19:53 AM	

Subject	Organizational Unit (OU)	NAIS Class 1 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Subject Public Key Info	RSA (2048 Bits)	
Signature	sha256WithRSAEncryption	

The profile of basic fields for **NAIS Class 2 CA** certificate is described below:

Field name	Value	
Version	Version 3	
Serial Number	2002d37d1fe47e327b1d	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Valid from	Thursday, February 11, 2016 11:23:43 AM	
Valid to	Friday, February 10, 2023 11:23:43 AM	
Subject	Organizational Unit (OU)	NAIS Class 2 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Subject Public Key Info	RSA (2048 Bits)	
Signature	sha256WithRSAEncryption	

The profile of basic fields for **NAIS Class 3 CA** certificate is described below:

Field name	Value	
Version	Version 3	
Serial Number	20038b09625165fadf49	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Valid from	Thursday, February 11, 2016 11:26:17 AM	
Valid to	Friday, February 10, 2023 11:26:17 AM	
Subject	Organizational Unit (OU)	NAIS Class 3 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Subject Public Key Info	RSA (2048 Bits)	
Signature	sha256WithRSAEncryption	

The profile of basic fields for **NAIS Class 4 CA** certificate is described below:

Field name	Value	
Version	Version 3	
Serial Number	2004cd6bb1a82a33ce32	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Certification Authority

	Organization Name (O)	NAIS
	Country (C)	AL
Valid from	Thursday, February 11, 2016 11:27:26 AM	
Valid to	Friday, February 10, 2023 11:27:26 AM	
Subject	Organizational Unit (OU)	NAIS Class 4 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Subject Public Key Info	RSA (2048 Bits)	
Signature	sha256WithRSAEncryption	

7.1.1 Version number(s)

All certificates issued by NAIS are X.509 Version 3.

7.1.2 Certificate extensions

Certificate extensions for **NAIS CA** are shown below.

Extension Field	Value	Critical
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.akshi.gov.al [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certs.akshi.gov.al/root.crt	No
Basic Constraints	Subject type=CA Path Length Constraint=None	Yes
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	Yes
Authority Key Identifier	KeyID= 53011db30451cb76ccb6a1a426aaeb80e5e2edda	No
Subject Key Identifier	eb1ed6948abdf0de2c812f9753b99b216b345db3	No

Certificate Policies	[1] Certificate Policy: Policy Identifier= 1.3.6.1.4.1.39148.10.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.akshi.gov.al/repository [2] Certificate Policy: Policy Identifier= 1.3.6.1.4.1.39148.10.1.1 [2,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.akshi.gov.al/repository	No
CRL Distribution Points	CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/root.crl URL = ldap://ldap.akshi.gov.al/OU=NAIS Root Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	No

Certificate extensions for **NAIS Class 1 CA** are shown below.

Extension Field	Value	Critical
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.akshi.gov.al [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certs.akshi.gov.al/ca.crt	No
Basic Constraints	Subject type=CA Path Length Constraint=None	Yes
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	Yes
Authority Key Identifier	KeyID= eb1ed6948abdf0de2c812f9753b99b216b345db3	No
Subject Key Identifier	42d78665150a4f63e5bffa820fbc3f72c5251d47	No
Certificate Policies	[1] Certificate Policy: Policy Identifier= 1.3.6.1.4.1.39148.10.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS	No

	Qualifier: http://www.akshi.gov.al/repository	
CRL Distribution Points	CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/ca.crl URL = ldap://ldap.akshi.gov.al/OU=NAIS Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	No

Certificate extensions for **NAIS Class 2 CA** are shown below.

Extension Field	Value	Critical
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.akshi.gov.al [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certs.akshi.gov.al/ca.crt	No
Basic Constraints	Subject type=CA Path Length Constraint=None	Yes
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	Yes
Authority Key Identifier	KeyID= eb1ed6948abdf0de2c812f9753b99b216b345db3	No
Subject Key Identifier	5fd64efdbc49c5e27c1782ba4d483d9b76b961cb	No
Certificate Policies	[1] Certificate Policy: Policy Identifier= 1.3.6.1.4.1.39148.10.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.akshi.gov.al/repository	No
CRL Distribution Points	CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/ca.crl URL = ldap://ldap.akshi.gov.al/OU=NAIS Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	No

Certificate extensions for **NAIS Class 3 CA** are shown below.

Extension Field	Value	Critical
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.akshi.gov.al [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certs.akshi.gov.al/ca.crt	No
Basic Constraints	Subject type=CA Path Length Constraint=None	Yes
Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	Yes
Authority Key Identifier	KeyID= eb1ed6948abdf0de2c812f9753b99b216b345db3	No
Subject Key Identifier	8726a8fbdb2b519b39d098d6f4c63356475cd805	No
Certificate Policies	[1] Certificate Policy: Policy Identifier= 1.3.6.1.4.1.39148.10.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.akshi.gov.al/repository	No
CRL Distribution Points	CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/ca.crl URL = ldap://ldap.akshi.gov.al/OU=NAIS Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	No

Certificate extensions for **NAIS Class 4 CA** are shown below.

Extension Field	Value	Critical
Authority Info Access	[1] Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.akshi.gov.al [2] Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://certs.akshi.gov.al/ca.crt	No
Basic Constraints	Subject type=CA Path Length Constraint=None	Yes

Key Usage	Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)	Yes
Authority Key Identifier	KeyID= eb1ed6948abdf0de2c812f9753b99b216b345db3	No
Subject Key Identifier	947b502134c449dc19d29807e9b0d9f8ae777508	No
Certificate Policies	[1] Certificate Policy: Policy Identifier= 1.3.6.1.4.1.39148.10.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.akshi.gov.al/repository	No
CRL Distribution Points	CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/ca.crl URL = ldap://ldap.akshi.gov.al/OU=NAIS Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	No

7.1.3 Algorithm object identifiers

Algorithms with pertaining OID identifiers for all certificates issued by NAIS CAs are shown below:

Algorithm	OID
sha256WithRSAEncryption	1.2.840.113549.1.1.11
rsaEncryption	1.2.840.113549.1.1.1

7.1.4 Name forms

Refer to section 3.1.

7.1.5 Name constraints

The extension *Name Constraints* is not used.

7.1.6 Certificate policy object identifier

The table below summarizes the certificate type and OID.

Certificate Name	Issued by	OID
- Certificate for electronic signature for private entities - Certificate for electronic signature for government employees - Certificate for electronic signature for government employees for critical	NAIS Class 1 CA	1.3.6.1.4.1.39148.10.1.1.1

infrastructure - Certificate for electronic seal		
- Certificate for electronic signature for private entities for critical infrastructure	NAIS Class 2 CA	1.3.6.1.4.1.39148.10.1.1.2
- Certificate for the fiscalization project for public institutions - Certificate for the fiscalization project for private entities - Certificate Test for the fiscalization project	NAIS Class 3 CA	1.3.6.1.4.1.39148.10.1.1.3
- Certificate for authentication for the Remote Signing Service Platform	NAIS Class 4 CA	1.3.6.1.4.1.39148.10.1.1.4

7.1.7 Usage of Policy Constraints extension

The extension *Policy Constraints* is not used.

7.1.8 Policy qualifiers syntax and semantics

Policy qualifiers in the extension Certificate Policies contain a pointer in the URI format with the website address of the repository.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulations.

7.2 CRL profile

CRL profile for **NAIS CA** is described in the table below:

Field Name	Value	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Effective date	Date of CRL issuance	
Next update	Date of next expected CRL update	

Revoked certificates	List of revoked certificates

CRL profile for **NAIS Class 1 CA** is described in the table below:

Field Name	Value	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Class 1 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Effective date	Date of CRL issuance	
Next update	Date of next expected CRL update	
Revoked certificates	List of revoked certificates	

CRL profile for **NAIS Class 2 CA** is described in the table below:

Field Name	Value	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Class 2 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Effective date	Date of CRL issuance	
Next update	Date of next expected CRL update	

Revoked certificates	List of revoked certificates

CRL profile for **NAIS Class 3 CA** is described in the table below:

Field Name	Value	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Class 3 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Effective date	Date of CRL issuance	
Next update	Date of next expected CRL update	
Revoked certificates	List of revoked certificates	

CRL profile for **NAIS Class 4 CA** is described in the table below:

Field Name	Value	
Version	V2	
Signature Algorithm	sha256WithRSAEncryption	
Issuer	Organizational Unit (OU)	NAIS Class 4 Certification Authority
	Organization Name (O)	NAIS
	Country (C)	AL
Effective date	Date of CRL issuance	
Next update	Date of next expected CRL update	

Revoked certificates	List of revoked certificates

7.2.1 Version number(s)

All CRLs issued by NAIS are X.509 Version 2.

7.2.2 CRL and CRL entry extensions

CRL extensions for **NAIS CAs** are described in the table below:

Field Name	Critical
Authority Key Identifier	No
CRL Number	No

7.3 OCSP profile

OCSP (Online Certificate Status Protocol) is used to check the revocation status of an X.509 digital certificate.

Information about certificate status is included in the *certStatus* field. It can return one of the following values:

- "good" which indicates a positive response to the status inquiry. At a minimum, this positive response indicates that the certificate is not revoked, but does not necessarily mean that the certificate was ever issued or that the time at which the response was produced is within the certificate's validity interval.
- "revoked" indicates that the certificate has been revoked.
- "unknown" which indicates that the responder doesn't know about the certificate being requested.

This service is implemented in accordance with RFC 2560.

7.3.1 Version number(s)

OCSP server issues certificate status confirmations in accordance with the RFC 2560. Version number is V1.

7.3.2 OCSP extensions

The OCSP server accepts *Nonce* extension.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

As a Qualified Trust Service Provider in Albania under the law No. 107/2015, dated 1.1.2015 "On Electronic Identification and Trusted Services" amended, NAIS is required to comply with the requirements laid down in this law.

NAIS is subject to periodic conformity assessment of certification services towards the criteria from Regulation 910/2014, its implementing acts and relevant ETSI standards.

NAIS has also implemented an integrated management system in compliance with the requirements of ISO 27001, ISO 9001 and ISO 20000-1 standards, which is assessed through compliance audits throughout the certification cycle.

8.1 Frequency or circumstances of assessment

The frequency and circumstances are determined by the type of the assessment, requirements of industry standards and national applicable laws.

Internal compliance audits are carried out by the relevant structures at NAIS to verify compliance with internal policies, procedures and practices as well as national legislation, international and industry standards. In some cases, NAIS may decide to appoint an external organization or body to perform internal audit functions.

8.2 Identity/qualifications of assessor

Depending on the standard or regulation, external compliance audits are performed by an accredited Conformity Assessment Body.

Internal compliance audits are conducted by knowledgeable experts in the area of PKI, ISO and ETSI standards and legislation related to trust services.

8.3 Assessor's relationship to assessed entity

To ensure credibility, objectivity and impartiality, external audits are conducted by an independent Conformity Assessment Body which is not affiliated directly or indirectly with NAIS. When performing internal audits, no personnel will audit their own areas of responsibility.

8.4 Topics covered by assessment

Depending on the scope of each assessment, the following topics may be covered:

- Trust service policies and practices
- Physical and environmental security
- Information security management
- Internal organization, processes and procedures
- Compliance with the standards ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3, ETSI EN 319 412-5
- Other topics may be subject to the scope of each individual assessment.

8.5 Actions taken as a result of deficiency

If non-conformities have been detected during internal and external audits, NAIS will take the necessary steps to eliminate the deficiency detected. NAIS will establish a corrective action plan and deadline for resolution of non-conformities. The result of the resolution will be communicated to management.

8.6 Communication of results

Internal audit results containing confidential information will be communicated internally at NAIS only with the authorized personnel.

The conformity assessment body will communicate the audit result to NAIS management. These reports will be made available to the supervisory body.

Because of the sensitivity of the information, compliance reports will not be publicly available on the Internet.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees regarding PKI services are described in the Decision of Council of Ministers No. 35, dated 22.1.2020 "On the approval of fees for electronic services of the National Agency for Information Society". This document is published at NAIS website under 'legislation' akshi.gov.al/legjislacion.

9.1.1 Certificate issuance or renewal fees

NAIS applies fees for certificate issuance and renewal to Subscribers in accordance with the Decision of Council of Ministers.

9.1.2 Certificate access fees

There is no fee applied for certificate access.

9.1.3 Revocation or status information access fees

There is no fee applied for revocation or status information access.

9.1.4 Fees for other services

Fees of other services are described in the Decision of Council of Ministers published on NAIS website.

9.1.5 Refund policy

NAIS does not apply a refund policy.

9.2 Financial responsibility

9.2.1 Insurance coverage

NAIS has sufficient financial resources and maintains insurance coverage for its liabilities to other participants.

9.2.2 Other assets

No stipulations.

9.2.3 Insurance or warranty coverage for end-entities

Refer to section 9.2.1.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

Confidential information includes all information related to the provision of certification services that is not made publicly available in the repository (refer to section 2.1 herein) by NAIS.

Confidential information includes:

- Private keys and activation data used to access private keys.
- Information held by NAIS as private information which is described in section 9.4 herein.

- Internal procedures, manuals and other documents used by trusted roles in performance of their duties.
- PKI infrastructure, network topology, software and hardware information.
- Audit logs and records.
- Any other information that could compromise the security of the public key infrastructure established at NAIS and certification services.

9.3.2 Information not within the scope of confidential information

Information which is not classified as confidential is considered public information. The information that NAIS publishes in the repository (described in section 2.1 herein), including published certificates and revocation data, is considered public information.

9.3.3 Responsibility to protect confidential information

NAIS employees are responsible for and required to protect the confidentiality of information during and after the termination of employment. Outsourced organizations are contractually obligated to safeguard the confidentiality of NAIS information.

9.4 Privacy of personal information

9.4.1 Privacy plan

During the registration process, NAIS collects information about Subscribers for the purpose of provisioning of certification services. Personal information of subscribers is handled in accordance with the law No. 9887, dated 10.3.2008 'On Protection of Personal Data', amended.

9.4.2 Information treated as private

Subscriber personal information that is submitted during the registration process and is not publicly available in the contents of a certificate or CRL is treated as private information.

9.4.3 Information not deemed private

Certificates, CRLs, or their contents are not deemed private information.

9.4.4 Responsibility to protect private information

NAIS is responsible for protecting the private information of subscribers and handling personal data in compliance with applicable legislation as described in section 9.4.1.

9.4.5 Notice and consent to use private information

Notice to use private information is provided to subscribers during the application process. By signing the declaration on terms and conditions of the certificate, subscribers give consent for the collection of private information for the purpose of provisioning of certification services.

9.4.6 Disclosure pursuant to judicial or administrative process

NAIS does not make available the data referred to in section 9.4.2, except in cases required by law or competent administrative or governmental bodies.

9.4.7 Other information disclosure circumstances

No stipulations.

9.5 Intellectual property rights

NAIS owns the intellectual property rights of applications developed on behalf of NAIS, such as the Remote Signing Service Platform. NAIS does not own intellectual property rights of software used in NAIS PKI which is owned by third parties. Documentation and policies published at akshi.gov.al is owned by NAIS.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Representations and warranties of NAIS as a Trust Service Provider are as follows:

- Comply with this CP/CPS as well as NAIS internal policies and procedures.
- Issuance of certificates in a secure manner, based on the identity of the natural or legal person.
- Issuance of certificates in accordance with certificate profiles defined in section 7.1 and according to the certificate type given in the certification application.
- Act in accordance with relevant laws and regulations.

9.6.2 RA representations and warranties

Representations and warranties of the RA function at NAIS are as follows:

- Comply with this CP/CPS as well as NAIS internal policies and procedures.
- Perform the registration and identification procedures by following the process described in this CP/CPS.

9.6.3 Subscriber representations and warranties

The subscriber:

- Is responsible for providing accurate information during the registration process.
- Read and agree with the terms and conditions of the certificate.
- Take appropriate measures to protect their secure cryptographic device, private key and activation data.
- Request certificate revocation in case of private key compromise.
- Uses the certificate in accordance with the rules defined in section 1.4 herein.

9.6.4 Relying party representations and warranties

Relying parties are responsible for:

- Performance of public key operations as a prerequisite for relying on a certificate
- The validation of a certificate by using the CRLs or certificate validation services.
- Not relying on a certificate if it has been revoked or when expired.

9.6.5 Representations and warranties of other participants

No stipulations.

9.7 Disclaimers of warranties

NAIS is not liable for damage, including indirect damage, as well as for any loss of profit, loss of data or other indirect damage in cases when this damage is caused:

- Due to unauthorized use of the user keys and certificates,
- By the use of certificate that is not permitted by this document,
- By fraudulent or negligent use of the certificate, CRL or OCSP service,
- As a result of incorrect or incomplete information submitted during the application process.

9.8 Limitations of liability

Legal responsibility is defined in the law No.9880, dated 25.2.2008 "on electronic signature", amended and law No. 107/2015 "on electronic identification and trust services" amended.

Liability is limited to legally provable damages. NAIS is not liable for:

- Liability related to fraud or misconduct of the Subscriber.
- Liability related to the use of certificates beyond the limitations stated in this CP/CPS.
- Liability related to the compromise of a Subscriber's private key.

9.9 Indemnities

Each participant is liable to the damaged party for damages caused by not complying with the provisions of this CP/CPS.

9.10 Term and termination

9.10.1 Term

The term of this CP/CPS begins upon publication to the Repository and remains in effect until replaced by a new CP/CPS.

9.10.2 Termination

The CP/CPS will remain in effect until replaced by a new version.

9.10.3 Effect of termination and survival

When a new CP/CPS is published in the repository, the provisions of the CP/CPS are applied for all new certificates that are issued. However, all current agreements remain effective until the certificate is revoked or expired.

9.11 Individual notices and communications with participants

Individual communication with participants is conducted via the official email address: pki@akshi.gov.al.

9.12 Amendments

9.12.1 Procedure for amendment

This CP/CPS will be amended when necessary. After the PKI Sector has made the necessary changes, NAIS Top Management formally approves these changes.

9.12.2 Notification mechanism and period

All changes made to this CP/CPS will be recorded on the version history table. The updated CP/CPS will be made available in the repository after formal approval from NAIS Top Management.

9.12.3 Circumstances under which OID must be changed

Major changes in the certificate policy or certification practice statement may require a change in the CP OID or CPS pointer. The PKI Sector together with NAIS Top Management will determine whether the OID will need to be changed.

9.13 Dispute resolution provisions

In the event of a dispute, parties involved are encouraged to resolve the dispute amicably. If this is not possible, disputes can be resolved by the competent court in Albania.

9.14 Governing law

NAIS as a Trust Service Provider follows all applicable laws and regulations in the Republic of Albania.

9.15 Compliance with applicable law

The present CP/CPS is in compliance with relevant and applicable Albanian laws.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulations.

9.16.2 Assignment

No stipulations.

9.16.3 Severability

No stipulations.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulations.

9.16.5 Force Majeure

No stipulations.

9.17 Other provisions

No stipulations.