Date 11.01.2023

ELECTRONIC CERTIFICATE PROFILES

ISSUES BY NAIS

Version 1.0

Document details

Document Name	Electronic certificate profiles issued by NAIS
Document Owner	NAIS (National Agency of Information Society)
Contact	pki@akshi.gov.al

Version history

Version	Date	Change
1.0	11.01.2023	First version.

Table of Contents

1. CERTIFICATES ISSUED BY NAIS CLASS 1 CERTIFICATION AUTHORITY

1.1 Certificate for electronic signature for private entities

Field	Attribute	Value
Version	Version	Version 3 (value= '2')
Serial Number	CertificateSerialNumber	[Unique value, randomly generated]
Signature Algorithm	AlgorithmIdentifier	sha256WithRSAEncryption
Issuer	commonName (CN)	NAIS Class 1 Certification Authority
	organizationName (O)	NAIS
	countryName (C)	AL
Validity	notBefore	[Date and time of certificate issuance]
	notAfter	[12 months after the certificate issuance date]
Subject	commonName (CN)	[Subject's name and surname as in official ID]
	serialNumber	[First letter(s) of SN, first letter(s) of G and a random generated number]
	localityName (L)	[City where the Subject is located]
	countryName (C)	AL
	surname (SN)	[Subject's surname as in official ID]
	givenName (G)	[Subject's name as in official ID]
	organizationName (O)	[Legal name of the associated private entity]
	organizationUnit (OU)	[TIN of the associated private entity]
	Title (T)	[Subject's job title]
Subject Public Key Info	subjectPublicKey	[Subject public key, 2048 bits long]

Certificate's extension fields

Field	Value	Critical
Key Usage	Digital Signature, Non-Repudiation	Yes
Certificate Policies	[1] Certificate Policy: Policy Identifier = 1.3.6.1.4.1.39148.10.1.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.akshi.gov.al/repository	No
CRL Distribution Points	[1] CRL Distribution Point: Distribution Point Name:	No

	Full Name: URL = http://crl.akshi.gov.al/class1.crl URL = ldap://ldap.akshi.gov.al/CN=NAIS Class 1 Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	
Authority Key Identifier	KeyID=42d78665150a4f63e5bffa820fbc3f72c5251d47	No
Subject Key Identifier	[Identification of the certificate's public key]	No
Authority Information 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/class1.crt	No

1.2 Certificate for electronic signature for government employees

Field	Attribute	Value
Version	Version	Version 3 (value= '2')
Serial Number	CertificateSerialNumber	[Unique value, randomly generated]
Signature Algorithm	AlgorithmIdentifier	sha256WithRSAEncryption
Issuer	commonName (CN)	NAIS Class 1 Certification Authority
	organizationName (O)	NAIS
	countryName (C)	AL
Validity	notBefore	[Date and time of certificate issuance]
	notAfter	[12 months after the certificate issuance date]
Subject	commonName (CN)	[Subject's name and surname as in official ID]
	serialNumber	[First letter(s) of SN, first letter(s) of G and a random generated number]
	localityName (L)	[City where the Subject is located]
	countryName (C)	AL
	surname (SN)	[Subject's surname as in official ID]
	givenName (G)	[Subject's name as in official ID]
	organizationName (O)	[Official name of the public institution]
	organizationUnit (OU)	[Organization unit at the public institution]
	Title (T)	[Subject's job title]

Subject Public Key Info	subjectPublicKey	[Subject public key, 2048 bits long]

Certificate's extension fields

Field	Value	Critical
Key Usage	Digital Signature, Non-Repudiation	Yes
Certificate Policies	[1] Certificate Policy: Policy Identifier = 1.3.6.1.4.1.39148.10.1.1.1 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.akshi.gov.al/repository	No
CRL Distribution Points	[1] CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/class1.crl URL = ldap://ldap.akshi.gov.al/CN=NAIS Class 1 Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	No
Authority Key Identifier	KeyID=42d78665150a4f63e5bffa820fbc3f72c5251d47	No
Subject Key Identifier	[Identification of the certificate's public key]	No
Authority Information 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/class1.crt	No

1.3 Certificate for electronic signature for government employees for critical infrastructure

Field	Attribute	Value
Version	Version	Version 3 (value= '2')
Serial Number	CertificateSerialNumber	[Unique value, randomly generated]
Signature Algorithm	AlgorithmIdentifier	sha256WithRSAEncryption
Issuer	commonName (CN)	NAIS Class 1 Certification Authority
	organizationName (O)	NAIS
	countryName (C)	AL
Validity	notBefore	[Date and time of certificate issuance]
	notAfter	[12 months after the certificate issuance date]

Subject	commonName (CN)	[Subject's name and surname as in official ID]
	serialNumber	[First letter(s) of SN, first letter(s) of G and a random generated number]
	localityName (L)	[City where the Subject is located]
	countryName (C)	AL
	surname (SN)	[Subject's surname as in official ID]
	givenName (G)	[Subject's name as in official ID]
	organizationName (O)	[Official name of the public institution]
	organizationUnit (OU)	[Organization unit at the public institution]
	Title (T)	[Subject's job title]
Subject Public Key Info	subjectPublicKey	[Subject public key, 2048 bits long]

Certificate's extension fields

Field	Value	Critical
Key Usage	Digital Signature, Non-Repudiation	Yes
CRL Distribution Points	[1] CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/class1.crl URL = ldap://ldap.akshi.gov.al/CN=NAIS Class 1 Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	No
Authority Key Identifier	KeyID=42d78665150a4f63e5bffa820fbc3f72c5251d47	No
Subject Key Identifier	[Identification of the certificate's public key]	No
Authority Information 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/class1.crt	No
Subject Alternative Name	Other Name: Principal Name = [Subject's email] RFC822 Name = [Subject's email]	No

1.4 Certificate for electronic seal

Field	Attribute	Value
Version	Version	Version 3 (value= '2')
Serial Number	CertificateSerialNumber	[Unique value, randomly generated]
Signature Algorithm	AlgorithmIdentifier	sha256WithRSAEncryption
Issuer	commonName (CN)	NAIS Class 1 Certification Authority
	organizationName (O)	NAIS
	countryName (C)	AL
Validity	notBefore	[Date and time of certificate issuance]
	notAfter	[12 months after the certificate issuance date]
Subject	commonName (CN)	[Official name of the public institution]
	organizationName (O)	[Official name of the public institution]
	countryName (C)	AL
	localityName (L)	[City where the public institution is located]
Subject Public Key Info	subjectPublicKey	[Subject public key, 2048 bits long]

Field	Value	Critical
Key Usage	Digital Signature, Non-Repudiation	Yes
CRL Distribution Points	[1] CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/class1.crl URL = ldap://ldap.akshi.gov.al/CN=NAIS Class 1 Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	No
Authority Key Identifier	KeyID=42d78665150a4f63e5bffa820fbc3f72c5251d47	No
Subject Key Identifier	[Identification of the certificate's public key]	No
Authority Information 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/class1.crt	No
Subject Alternative Name	Other Name: Principal Name = [official email of the public institution] RFC822 Name = [official email of the public institution]	No

2. CERTIFICATES ISSUED BY NAIS CLASS 2 CERTIFICATION AUTHORITY

2.1 Certificate for electronic signature for private entities for critical infrastructure

Field	Attribute	Value
Version	Version	Version 3 (value= '2')
Serial Number	CertificateSerialNumber	[Unique value, randomly generated]
Signature Algorithm	AlgorithmIdentifier	sha256WithRSAEncryption
Issuer	commonName (CN)	NAIS Class 2 Certification Authority
	organizationName (O)	NAIS
	countryName (C)	AL
Validity	notBefore	[Date and time of certificate issuance]
	notAfter	[12 months after the certificate issuance date]
Subject	commonName (CN)	[Subject's name and surname as in official ID]
	serialNumber	[First letter(s) of SN, first letter(s) of G and a random generated number]
	localityName (L)	[City where the Subject is located]
	countryName (C)	AL
	surname (SN)	[Subject's surname as in official ID]
	givenName (G)	[Subject's name as in official ID]
	organizationName (O)	[Legal name of associated the private entity]
	organizationUnit (OU)	[Organization unit at the private entity]
	Title (T)	[Subject's job title]
Subject Public Key Info	subjectPublicKey	[Subject public key, 2048 bits long]

Certificate's extension fields

Field	Value	Critical
Key Usage	Digital Signature, Non-Repudiation	Yes
CRL Distribution Points	[1] CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/class2.crl URL = ldap://ldap.akshi.gov.al/CN=NAIS Class 2 Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	No

Authority Key Identifier	KeyID=5fd64efdbc49c5e27c1782ba4d483d9b76b961cb	No
Subject Key Identifier	[Identification of the certificate's public key]	No
Authority Information 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/class2.crt	No
Subject Alternative Name	Other Name: Principal Name = [Subject's email] RFC822 Name = [Subject's email]	No

3. CERTIFICATES ISSUED BY NAIS CLASS 3 CERTIFICATION AUTHORITY

3.1 Certificate for the fiscalization project for public institutions

Field	Attribute	Value
Version	Version	Version 3 (value= '2')
Serial Number	CertificateSerialNumber	[Unique value, randomly generated]
Signature Algorithm	AlgorithmIdentifier	sha256WithRSAEncryption
Issuer	commonName (CN)	NAIS Class 3 Certification Authority
	organizationName (O)	NAIS
	countryName (C)	AL
Validity	notBefore	[Date and time of certificate issuance]
	notAfter	[12 months after the certificate issuance date]
Subject	Title (T)	Production
	organizationUnit (OU)	IT
	organizationName (O)	[Official name of public institution]
	serialNumber	[First letter(s) of SN, first letter(s) of G and a random generated number]
	localityName (L)	[City where the public institution is located]
	commonName (CN)	[Name and TIN of public institution]
	surname (SN)	[TIN of public institution]
	givenName (G)	[Name of public institution]
	countryName (C)	AL
Subject Public Key Info	subjectPublicKey	[Subject public key, 2048 bits long]

Certificate's extension fields

Field	Value	Critical
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment	Yes
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	No
Certificate Policies	[1] Certificate Policy: Policy Identifier = 1.3.6.1.4.1.39148.10.1.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.akshi.gov.al/repository	No

CRL Distribution Points	[1] CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/class3.crl URL = ldap://ldap.akshi.gov.al/CN=NAIS Class 3 Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	No
Authority Key Identifier	KeyID=8726a8fbdb2b519b39d098d6f4c63356475cd805	No
Subject Key Identifier	[Identification of the certificate's public key]	No
Authority Information 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/class3.crt	No
Subject Alternative Name	Other Name: Principal Name = [official email of the public institution] RFC822 Name = [official email of the public institution]	No

3.2 Certificate for the fiscalization project for private entities

Field	Attribute	Value
Version	Version	Version 3 (value= '2')
Serial Number	CertificateSerialNumber	[Unique value, randomly generated]
Signature Algorithm	AlgorithmIdentifier	sha256WithRSAEncryption
Issuer	commonName (CN)	NAIS Class 3 Certification Authority
	organizationName (O)	NAIS
	countryName (C)	AL
Validity	notBefore	[Date and time of certificate issuance]
	notAfter	[12 months after the certificate issuance date]
Subject	Title (T)	Production
	organizationUnit (OU)	IT
	organizationName (O)	[Legal name of the private entity]
	serialNumber	[First letter(s) of SN, first letter(s) of G and a random generated number]
	localityName (L)	[City where the private entity is located]
	commonName (CN)	[Name and TIN of private entity]

	surname (SN)	[TIN of private entity]
	givenName (G)	[Legal name of private entity]
	countryName (C)	AL
Subject Public Key Info	subjectPublicKey	[Subject public key, 2048 bits long]

Certificate's extension fields

Field	Value	Critical
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment	Yes
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	No
Certificate Policies	[1] Certificate Policy: Policy Identifier = 1.3.6.1.4.1.39148.10.1.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.akshi.gov.al/repository	No
CRL Distribution Points	[1] CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/class3.crl URL = ldap://ldap.akshi.gov.al/CN=NAIS Class 3 Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	No
Authority Key Identifier	KeyID=8726a8fbdb2b519b39d098d6f4c63356475cd805	No
Subject Key Identifier	[Identification of the certificate's public key]	No
Authority Information 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/class3.crt	No
Subject Alternative Name	Other Name: Principal Name = [email of private entity] RFC822 Name = [email of private entity]	No

3.3 Certificate Test for the fiscalization project

Field	Attribute	Value
Version	Version	Version 3 (value= '2')

Serial Number	CertificateSerialNumber	[Unique value, randomly generated]
Signature Algorithm	AlgorithmIdentifier	sha256WithRSAEncryption
Issuer	commonName (CN)	NAIS Class 3 Certification Authority
	organizationName (O)	NAIS
	countryName (C)	AL
Validity	notBefore	[Date and time of certificate issuance]
	notAfter	[12 months after the certificate issuance date]
Subject	Title (T)	Test
	organizationUnit (OU)	IT
	organizationName (O)	[Legal name of the private entity]
	serialNumber	[First letter(s) of SN, first letter(s) of G and a random generated number]
	localityName (L)	[City where the private entity is located]
	commonName (CN)	[Name and TIN of private entity]
	surname (SN)	[TIN of private entity]
	givenName (G)	[Legal name of private entity]
	countryName (C)	AL
Subject Public Key Info	subjectPublicKey	[Subject public key, 2048 bits long]

Certificate's extension fields

Field	Value	Critical
Key Usage	Digital Signature, Non-Repudiation, Key Encipherment	Yes
Extended Key Usage	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)	No
Certificate Policies	[1] Certificate Policy: Policy Identifier = 1.3.6.1.4.1.39148.10.1.1.3 [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.akshi.gov.al/repository	No
CRL Distribution Points	[1] CRL Distribution Point: Distribution Point Name: Full Name: URL = http://crl.akshi.gov.al/class3.crl URL = ldap://ldap.akshi.gov.al/CN=NAIS Class 3 Certification Authority,O=NAIS,C=AL?certificateRevocationList;binary	No

Authority Key Identifier	KeyID=8726a8fbdb2b519b39d098d6f4c63356475cd805	No
Subject Key Identifier	[Identification of the certificate's public key]	No
Authority Information 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/class3.crt	No
Subject Alternative Name	Other Name: Principal Name = [email of private entity] RFC822 Name = [email of private entity]	No