AK

Certificate Profiles

For Fullgilt auðkenni 2021

Version: 1.5 – Effective date: 15.09.2023

Change control		
Published	Version	Changes
16.03.2021	1.0	Final approved version
06.04.2021	1.1	Added “Notice text” Fixed typos Effective date does not change.
26.04.2021	1.2	Removed “CertificateAuthorityIssuer” from Auðkenni CA Certificate Effective date does not change. Version recalled and not published.
21.9.2021	1.3	Changed Fullgilt auðkenni to Fullgilt auðkenni 2021 Fixed error – missing AuthorityKeyIdentifier in two profiles Fixed error – Policy OID in non-qualified Equipment authentication Key size in App certificate added 6143 and 6142 QCP-l NCP policy added and new profile. Mapping of product to OID updated.
23.11.2022	1.4	Added profile for TSU certificates for NCP+ Added explanation of OSCP response “revoked”
15.09.2023	1.5	Minor fixes to text.

TABLE OF CONTENTS

1 SCOPE AND PURPOSE

This document contains information about the certificates used at Auðkenni and complements the Certificate Policy and the Certification Practice Statement.

The purpose of this document is to provide one single place for specification of certificate contents. This serves to avoid inconsistency and contributes to a significant reduction in the risk for errors and misunderstandings in the maintenance of certificate contents.

1.1 Document structure

Chapter 5 lists contents of Islandsrot, Auðkenni Intermediate Certificate and Auðkenni certificates for Certificates on Cards, Certificates on Mobile, Certificates in App, Certificates in eSeals, Equipment Authentication and Time-stamping unit.

Chapter 6 lists the Auðkenni OCSP and CRL profile.

2 DEFINITIONS

Definition	Description
<PNO of subject> <PNO of subscriber>	An alphanumeric value representing the Personal ID Number or Identification Number of the Subscriber or Subject as defined in the Icelandic National Registry or the National Trade Registry.
<Unique ID>	Value in HEX code, unique for each certificate. Used for serial number of certificates.
<Name of subscriber>	Name of subscriber as it is recorded in the Icelandic National Registry or National Trade Registry.
<ID of subscriber>	ID of subscriber as recorded in the Icelandic National Registry. This is a ten-digit number in the form DDMMYY#### showing date of birth, sequence number, validation number and century. In the case of an organization the format has ten digits in the form of ##MMYY####. In case of eSeals this number will have “NTRIS-“ in front of the number.
<Subject given name>	Given name of subject is the name as recorded in the Icelandic National Registry.
<Subject surname>	Surname of subject is the name as recorded in the Icelandic National Registry.
<Subject full name>	The full name of the subject – Given name, surname, and middle name as recorded in the National Registry.
<Name of Organization>	The name of the Organization as it in the National Trade Registry.
<App account number>	Account number within App on Smart device. A unique number.

Since Auðkenni uses the same intermediate CA to issue all types of certificates it is necessary to distinguish between different types. Auðkenni differentiates between certificates using unique OIDs in each profile. The OIDs are described in the following tables:

Products for natural persons	OID	QCP-n-qscd Signing cert	NCP+ Authentication cert	NCP+ Signing cert
Cards natural person	2.16.352.1.2.10.1	0.4.0.194112.1.2	0.4.0.2042.1.2	NA
Cards natural person + legal person	2.16.352.1.2.10.2	0.4.0.194112.1.2	0.4.0.2042.1.2	NA
Mobile	2.16.352.1.2.11.1	0.4.0.194112.1.2	0.4.0.2042.1.2	NA
App on Smartphone – Qualified	2.16.352.1.2.12.1	0.4.0.194112.1.2	0.4.0.2042.1.2	NA

Products for legal persons	OID	QCP-l-qscd	QCP-l (NCP+)	QCP-l (NCP)
eSeal – Qualified	2.16.352.1.2.13.1	0.4.0.194112.1.3 Future service	NA	NA
eSeal – Advanced HSM	2.16.352.1.2.13.2	NA	0.4.0.194112.1.1 0.4.0.2042.1.2	NA
eSeal – Advanced SOFT	2.16.352.1.2.13.3	NA	NA	0.4.0.194112.1.1 0.4.0.2042.1.1

Product	OID	NCP	NCP+
Equipment Authentication	2.16.352.1.2.14.1	0.4.0.2042.1.1	
Time-Stamping Unit (TSU)	2.16.352.1.2.14.2		0.4.0.2042.1.2

3 OVERVIEW

Name of certificate	In the cert. path	Description
Root CA certificate (Islandsrot 2021)	Yes	This is the root CA that issues the intermediate CA Fullgilt auðkenni.
Intermediate CA certificate (Fullgilt auðkenni 2021)	Yes	This is the CA certificate that issues all end user certificates.
Subscriber certificates (Mobile)	Yes	Certificates issued on mobile (SIM card)
Subscriber certificates (App)	Yes	Certificates issued in App, both qualified.
Subscriber certificates (Cards)	Yes	Certificates issued on white cards.
Subscriber certificates (eSeals)	Yes	Certificates issued for eSeals.

Only certificates in the certification path of end user certificates are described in this document.

4 CERTIFICATES

The tables below list contents of certificates.

Certificate profiles follow ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3, X.509 version 3 and RFC 5280.

4.1 Islandsrot root certificate

4.1.1 Certificate-signing

This certificate is self-signed.

Certificate used from 2021. Certificates issued under the hierarchy of this root certificate, are issued from September 2021.

Field	Value	Description
Version	V3	Certificate format version.
Serial number	<Unique ID>	Unique serial number of the certificate.
Signature Algorithm	Sha384WithRSAEncryption	Signature algorithm in accordance with RFC 5280.
Issuer Distinguished name		
CommonName (CN)	Islandsrot 2021	Certificate authority name.
Serial Number (S)	5501692829	Business registration number.
OrganisationName (O)	Fjármála- og efnahagsráðuneyti	Name of issuer organization.
CountryName (C)	IS	Country code „IS" for Iceland.
OrganisationIdentifier	NTRIS-5501692829	Business registration number.
Valid from	<First date of validity>	First date of Certificate validity.
Valid to	<Last date of validity>	Last date of Certificate validity. Max 30 years.

Subject Distinguished Name		
Serial Number (S)	5501692829	Business registration number backward compatible.
OrganisationName	Fjármála- og efnahagsráðuneyti	Business name.
OrganisationIdentifier	NTRIS-5501692829	Business registration number.
CommonName (CN)	Islandsrot 2021	Person full name in UTF8 format.
CountryName (C)	IS	Country code „IS" for Iceland.
Subject Public Key	RSA 4096	RSA algorithm in accordance with RFC 4055
Extensions		
Basic Constraints	Pathlength=none, CA=True	
Key Usage	KeyCertSign + CRLSign + Off-line CRL Signing	
AuthorityKeyIdentifier	SHA-1 hash of the public key	
SubjectKeyIdentifier	SHA-1 hash of public key. No name or serial number included	
Certificate Policies	Policy identifier: 2.16.352.1.1.1.1 https://cp.islandsrot.is	

KeyStore: Off-line HSM

4.2 Auðkenni CA Certificate

4.2.1 Certificate-signing and CRL-signing Certificate

This certificate is signed by the root certificate named “Islandsrot 2021”.

Certificate used from 2021. This certificate is issued to Auðkenni CA since April 2021 and is used to issue subscriber certificates.

Field	Value	Description
Version	V3	Certificate format version.
Serial number	<Unique ID>	Unique serial number of the certificate.
Signature Algorithm	Sha384WithRSAEncryption	Signature algorithm in accordance with RFC 5280.
Issuer Distinguished name		
CommonName (CN)	Islandsrot 2021	Certificate authority name.
Serial Number (S)	5501692829	Business registration number.
OrganisationName (O)	Fjármála- og efnahagsráðuneyti	Name of issuer organization.
CountryName (C)	IS	Country code „IS“ for Iceland.
OrganisationIdentifier	NTRIS-5501692829	Business registration number.
Valid from	<First date of validity>	First date of Certificate validity.
Valid to	<Last date of validity>	Last date of Certificate validity. Max 15 years.
Subject Distinguished Name		
Serial Number (S)	5210002790	Business registration number backward compatible.
OrganisationName	Auðkenni ehf.	Business name.
OrganisationIdentifier	NTRIS-5210002790	Business registration number.
CommonName (CN)	Fullgilt audkenni 2021	
CountryName (C)	IS	Country code „IS“ for Iceland.
Subject Public Key	RSA 4096	RSA algorithm in accordance with RFC 4055
Extensions		
Basic Constraints	Pathlength=0, CA=True	
Key Usage	KeyCertSign + CRLSign + Off-line CRL Signing	
AuthorityKeyIdentifier	SHA-1 hash of the public key	
SubjectKeyIdentifier	SHA-1 hash of public key. No name or serial number included	
Authority Information Access		
Oscp	Null	
Certificate Policies	Policy identifier: 2.16.352.1.1.1.1 https://cp.islandsrot.is	
CRLDisributionpoints	Only distributionPoint is used, DistributionPointName = http://crl.islandsrot.is/ISROT2021/latest.crl	

KeyStore: HSM

4.3 Subscriber Certificates

There are four different kinds of Subscriber Certificates for end-users and two for equipment. In all cases except for eSeals there are both Certificates for Authentication and Certificates for Signing:

- Certificates on Cards (individual and organization). KeyStore SSCD/QSCD
- Certificates on Mobile phones. KeyStore SIM Card (SSCD/QSCD)
- Certificates on App. KeyStore App and HSM (QSCD Split key) for Qualified.
- Certificates for eSeals (general equipment). KeyStore HSM at Client or HSM on Crypto Stick or File.

4.3.1 Certificates on Cards

Qualified End-user Signing Certificate – human end-users (Einkaskilriki)

Field	Value	Description
Version	V3	Certificate format version.
Serial number	<Unique ID>	Unique serial number of the certificate.
Signature Algorithm	Sha256WithRSAEncryption	Signature algorithm in accordance with RFC 5280.
Issuer Distinguished name		
CommonName (CN)	Fullgilt audkenni 2021	Certificate authority name.
OrganisationIdentifier	NTRIS-5210002790	Business registration number.
Serialnumber (S)	5210002790	Business registration number backward compatible.
OrganisationName (O)	Auðkenni ehf.	Name of issuer organisation.
CountryName (C)	IS	Country code „IS" for Iceland.
Valid from	<First date of validity>	First date of Certificate validity.
Valid to	<Last date of validity>	Last date of Certificate validity. Max one year.
Subject Distinguished Name		
Serial Number (S)	<PNO of subject>	Unique personal identity code.
Given Name (G)	<Subject given name>	Person given name in UTF8 format.
SurName (S)	<Subject surname>	Person surname in UTF8 format.
CommonName (CN)	<Subject full name>	Person full name in UTF8 format.
CountryName (C)	IS	Country code „IS" for Iceland.
Subject Public Key	RSA 2048	RSA algorithm in accordance with RFC 4055
Extensions		
Basic Constraints	Subject Type = End Entity Path Length Constraint = None	
Key Usage	nonRepudiation	
QC Statements	QC Compliance (0.4.0.1862.1.1) QC Secure Signature Creation Device (0.4.0.1862.1.4) QC PKI Disclosure Statements (0.4.0.1862.1.5) IS: https://repo.audkenni.is/pds QC Type EtsiQctEsign (0.4.0.1862.1.6.1)	
AuthorityKeyIdentifier	SHA-1 hash of the public key	
SubjectKeyIdentifier	SHA-1 hash of the public key	
Authority Information Access		
Oscp	http://ocsp.audkenni.is	
CertificateAuthorityIssuer	https://cdp.islandsrot.is/skilriki/FA2021.p7b	
Certificate Policies	Policy Identifier = 2.16.352.1.2.1.1.2 0.4.0.194112.1.2 2.16.352.1.2.10.1	https://repo.audkenni.is/cps Notice text: Cards natural person
CRLDisributionpoints	URI: http://crl.audkenni.is/FA2021/latest.crl	

End-user Authentication Certificate - human end-users (Einkaskilriki)

Field	Value	Description
Version	V3	Certificate format version.
Serial number	<Unique ID>	Unique serial number of the certificate.
Signature Algorithm	Sha256WithRSAEncryption	Signature algorithm in accordance with RFC 5280.
Issuer Distinguished name		
CommonName (CN)	Fullgilt audkenni 2021	Certificate authority name.
Serialnumber (S)	5210002790	Business registration number backward compatible.
OrganisationIdentifier	NTRIS-5210002790	Business registration number.
OrganisationName (O)	Auðkenni ehf.	Name of issuer organisation.
CountryName (C)	IS	Country code „IS" for Iceland.
Valid from	<First date of validity>	First date of Certificate validity.
Valid to	<Last date of validity>	Last date of Certificate validity. Max one year.
Subject Distinguished Name		
Serial Number (S)	<PNO of subject>	Unique personal identity code.
Given Name (G)	<Subject given name>	Person given name in UTF8 format.
SurName (S)	<Subject surname>	Person surname in UTF8 format.
CommonName (CN)	<Subject full name>	Person full name in UTF8 format.
CountryName (C)	IS	Country code „IS" for Iceland.
Subject Public Key	RSA 2048	RSA algorithm in accordance with RFC 4055
Extensions		
Basic Constraints	Subject Type = End Entity Path Length Constraint = None	
Key Usage	Digital Signature, Key Encipherment	
AuthorityKeyIdentifier	SHA-1 hash of the public key	
SubjectKeyIdentifier	SHA-1 hash of the public key	
Authority Information Access		
Oscp	http://ocsp.audkenni.is	
CertificateAuthorityIssuer	https://cdp.islandsrot.is/skilriki/FA2021.p7b	
Certificate Policies	Policy Identifier = 2.16.352.1.2.1.1.2 0.4.0.2042.1.2 2.16.352.1.2.10.1	https://repo.audkenni.is/cps Notice text: Cards natural person
CRLDisributionpoints	URI: http://crl.audkenni.is/FA2021/latest.crl	
Extended Key Usage	Client Authentication	

Qualified End-user Signing Certificate – Organization human end-users (Starfsskilríki)

Field	Value	Description
Version	V3	Certificate format version.
Serial number	<Unique ID>	Unique serial number of the certificate.
Signature Algorithm	Sha256WithRSAEncryption	Signature algorithm in accordance with RFC 5280.
Issuer Distinguished name		
CommonName (CN)	Fullgilt audkenni 2021	Certificate authority name.
Serialnumber (S)	5210002790	Business registration number backward compatible.
OrganisationIdentifier	NTRIS-5210002790	Business registration number.
OrganisationName (O)	Auðkenni ehf.	Name of issuer organisation.
CountryName (C)	IS	Country code „IS" for Iceland.
Valid from	<First date of validity>	First date of Certificate validity.
Valid to	<Last date of validity>	Last date of Certificate validity. Max four years.
Subject Distinguished Name		
Serial Number (S)	<PNO of subject>:<ID of subscriber>	Unique personal identity code and ID of organisation.
Given Name (G)	<Subject given name>	Person given name in UTF8 format.
SurName (S)	<Subject surname>	Person surname in UTF8 format.
CommonName (CN)	<Subject full name>	Person full name in UTF8 format.
CountryName (C)	IS	Country code „IS" for Iceland.
OrganisationName (O)	<Subscriber Organisation name>	Organisation name in UTF8 format.
OrganisationIdentifier	<ID of subscriber>	Business ID in form NTRIS-#
Subject Public Key	RSA 2048	RSA algorithm in accordance with RFC 4055
Extensions		
Basic Constraints	Subject Type = End Entity Path Length Constraint = None	
Key Usage	nonRepudiation	
QC Statements	QC Compliance (0.4.0.1862.1.1) QC Secure Signature Creation Device (0.4.0.1862.1.4) QC PKI Disclosure Statements (0.4.0.1862.1.5) IS: https://repo.audkenni.is/pds QC Type EtsiQctEsign (0.4.0.1862.1.6.1)	
AuthorityKeyIdentifier	SHA-1 hash of the public key	
SubjectKeyIdentifier	SHA-1 hash of the public key	
Authority Information Access		
Oscp	http://ocsp.audkenni.is	
CertificateAuthorityIssuer	https://cdp.islandsrot.is/skilriki/FA2021.p7b	
Certificate Policies	Policy Identifier = 2.16.352.1.2.1.1.2 0.4.0.194112.1.2 2.16.352.1.2.10.2	https://repo.audkenni.is/cps Notice text: Cards natural person + legal person
CRLDisributionpoints	URI: http://crl.audkenni.is/FA2021/latest.crl	

End-user Authentication Certificate - Organization human end-users (Starfsskilriki)

Field	Value	Description
Version	V3	Certificate format version.
Serial number	<Unique ID>	Unique serial number of the certificate.
Signature Algorithm	Sha256WithRSAEncryption	Signature algorithm in accordance with RFC 5280.
Issuer Distinguished name		
CommonName (CN)	Fullgilt audkenni 2021	Certificate authority name.
Serialnumber (S)	5210002790	Business registration number backward compatible.
OrganisationIdentifier	NTRIS-5210002790	Business registration number.
OrganisationName (O)	Auðkenni ehf.	Name of issuer organisation.
CountryName (C)	IS	Country code „IS" for Iceland.
Valid from	<First date of validity>	First date of Certificate validity.
Valid to	<Last date of validity>	Last date of Certificate validity. Max four years.
Subject Distinguished Name		
Serial Number (S)	<PNO of subject>:<ID of subscriber>	Unique personal identity code and ID of subscriber.
Given Name (G)	<Subject given name>	Person given name in UTF8 format.
SurName (S)	<Subject surname>	Person surname in UTF8 format.
CommonName (CN)	<Subject full name>	Person full name in UTF8 format.
OrganisationIdentifier	<ID of subscriber>	Business ID in form NTRIS-#
OrganisationName (O)	<Subscriber Organisation name>	Organisation name in UTF8 format.
CountryName (C)	IS	Country code „IS" for Iceland.
Subject Public Key	RSA 2048	RSA algorithm in accordance with RFC 4055
Extensions		
Basic Constraints	Subject Type = End Entity Path Length Constraint = None	
Key Usage	Digital Signature, Key Encipherment	
AuthorityKeyIdentifier	SHA-1 hash of the public key	
SubjectKeyIdentifier	SHA-1 hash of the public key	
Authority Information Access		
Oscp	http://ocsp.audkenni.is	
CertificateAuthorityIssuer	https://cdp.islandsrot.is/skilriki/FA2021.p7b	
Certificate Policies	Policy Identifier = 2.16.352.1.2.1.1.2 0.4.0.2042.1.2 2.16.352.1.2.10.2	https://repo.audkenni.is/cps Notice text: Cards natural person + legal person
CRLDisributionpoints	URI: http://crl.audkenni.is/FA2021/latest.crl	
Extended Key Usage	Client Authentication	

4.3.2 Certificates on Mobile

Qualified End-user Signing Certificate – human end-users (Rafræn skilríki á farsímum)

Field	Value	Description
Version	V3	Certificate format version.
Serial number	<Unique ID>	Unique serial number of the certificate.
Signature Algorithm	Sha256WithRSAEncryption	Signature algorithm in accordance with RFC 5280.
Issuer Distinguished name		
CommonName (CN)	Fullgilt audkenni 2021	Certificate authority name.
Serialnumber (S)	5210002790	Business registration number backward compatible.
OrganisationIdentifier	NTRIS-5210002790	Business registration number.
OrganisationName (O)	Auðkenni ehf.	Name of issuer organisation.
CountryName (C)	IS	Country code „IS" for Iceland.
Valid from	<First date of validity>	First date of Certificate validity.
Valid to	<Last date of validity>	Last date of Certificate validity. Max five years.
Subject Distinguished Name		
Serial Number (S)	<PNO of subject>	Unique personal identity code.
Given Name (G)	<Subject given name>	Person given name in UTF8 format.
SurName (S)	<Subject surname>	Person surname in UTF8 format.
CommonName (CN)	<Subject full name>	Person full name in UTF8 format.
CountryName (C)	IS	Country code „IS" for Iceland.
Subject Public Key	RSA 2048	RSA algorithm in accordance with RFC 4055
Extensions		
Basic Constraints	Subject Type = End Entity Path Length Constraint = None	
Key Usage	nonRepudiation	
QC Statements	QC Compliance (0.4.0.1862.1.1) QC Secure Signature Creation Device (0.4.0.1862.1.4) QC PKI Disclosure Statements (0.4.0.1862.1.5) IS: https://repo.audkenni.is/pds QC Type EtsiQctEsign (0.4.0.1862.1.6.1)	
AuthorityKeyIdentifier	SHA-1 hash of the public key	
SubjectKeyIdentifier	SHA-1 hash of the public key	
Authority Information Access		
Oscp	http://ocsp.audkenni.is	
CertificateAuthorityIssuer	https://cdp.islandsrot.is/skilriki/FA2021.p7b	
Certificate Policies	Policy Identifier = 2.16.352.1.2.1.1.2 0.4.0.194112.1.2 2.16.352.1.2.11.1	https://repo.audkenni.is/cps Notice text: Mobile
CRLDisributionpoints	URI: http://crl.audkenni.is/FA2021/latest.crl	

End-user Authentication Certificate - human end-users (Rafræn skilríki á farsímum)

Field	Value	Description
Version	V3	Certificate format version.
Serial number	<Unique ID>	Unique serial number of the certificate.
Signature Algorithm	Sha256WithRSAEncryption	Signature algorithm in accordance with RFC 5280.
Issuer Distinguished name		
CommonName (CN)	Fullgilt audkenni 2021	Certificate authority name.
Serialnumber (S)	5210002790	Business registration number backward compatible.
OrganisationIdentifier	NTRIS-5210002790	Business registration number.
OrganisationName (O)	Auðkenni ehf.	Name of issuer organisation.
CountryName (C)	IS	Country code „IS" for Iceland.
Valid from	<First date of validity>	First date of Certificate validity.
Valid to	<Last date of validity>	Last date of Certificate validity. Max five years.
Subject Distinguished Name		
Serial Number (S)	<PNO of subject>	Unique personal identity code.
Given Name (G)	<Subject given name>	Person given name in UTF8 format.
SurName (S)	<Subject surname>	Person surname in UTF8 format.
CommonName (CN)	<Subject full name>	Person full name in UTF8 format.
CountryName (C)	IS	Country code „IS" for Iceland.
Subject Public Key	RSA 2048	RSA algorithm in accordance with RFC 4055
Extensions		
Basic Constraints	Subject Type = End Entity Path Length Constraint = None	
Key Usage	Digital Signature, Key Encipherment	
AuthorityKeyIdentifier	SHA-1 hash of the public key	
SubjectKeyIdentifier	SHA-1 hash of the public key	
Authority Information Access		
Oscp	http://ocsp.audkenni.is	
CertificateAuthorityIssuer	https://cdp.islandsrot.is/skilriki/FA2021.p7b	
Certificate Policies	Policy Identifier = 2.16.352.1.2.1.1.2 0.4.0.2042.1.2 2.16.352.1.2.11.1	https://repo.audkenni.is/cps Notice text: Mobile
CRLDisributionpoints	URI: http://crl.audkenni.is/FA2021/latest.crl	
Extended Key Usage	Client Authentication	

4.3.3 Certificates on eSeals and Equipment Authentication

Qualified End-user Signing Certificate – eSeal – QCP-l-qscd

This is a future service not yet implemented.

Field	Value	Description
Version	V3	Certificate format version.
Serial number	<Unique ID>	Unique serial number of the certificate.
Signature Algorithm	Sha256WithRSAEncryption	Signature algorithm in accordance with RFC 5280.
Issuer Distinguished name		
CommonName (CN)	Fullgilt audkenni 2021	Certificate authority name.
OrganisationIdentifier	NTRIS-5210002790	Business registration number.
Serial Number(S)	5210002790	Business registration number backward compatible.
OrganisationName (O)	Auðkenni ehf.	Name of issuer organisation.
CountryName (C)	IS	Country code „IS" for Iceland.
Valid from	<First date of validity>	First date of Certificate validity.
Valid to	<Last date of validity>	Last date of Certificate validity. Max four years.
Subject Distinguished Name		
Serial Number (S)	<ID of subscriber>	Business registration number
OrganisationName (O)	<Name of subject>	Organisation name in UTF8 format.
CommonName (CN)	<Name of Service>	Name connected to the business in UTF8 format.
OrganisationIdentifier	<ID of Subscriber>	Business registration number in the form NTRIS-#
CountryName (C)	IS	Country code „IS" for Iceland.
Subject Public Key	RSA 2048, 4096	RSA algorithm in accordance with RFC 4055
Extensions		
Basic Constraints	Subject Type = End Entity Path Length Constraint = None	
Key Usage	nonRepudiation	
QC Statements	QC Compliance (0.4.0.1862.1.1) QC Secure Signature Creation Device (0.4.0.1862.1.4) QC PKI Disclosure Statements (0.4.0.1862.1.5) IS: https://repo.audkenni .is/pds QC Type EtsiQctEseal (0.4.0.1862.1.6.2) QC id-etsi-qcs-semanticsId-Legal (0.4.0.194121.1.2)	
AuthorityKeyIdentifier	SHA-1 hash of the public key	
SubjectKeyIdentifier	SHA-1 hash of the public key	
Authority Information Access		
Oscp	http://ocsp.audkenni.is	
CertificateAuthorityIssuer	https://cdp.islandsrot.is/skilriki/FA2021.p7b	
Certificate Policies	Policy Identifier = 2.16.352.1.2.1.1.2 0.4.0.194112.1.3 2.16.352.1.2.13.1	https://repo.audkenni.is/cps Notice text: eSeal - Qualified
CRLDisributionpoints	URI: http://crl.audkenni.is/FA2021/latest.crl	

Qualified End-user Signing Certificate – eSeal QCP-l NCP+

Field	Value	Description
Version	V3	Certificate format version.
Serial number	<Unique ID>	Unique serial number of the certificate.
Signature Algorithm	Sha256WithRSAEncryption	Signature algorithm in accordance with RFC 5280.
Issuer Distinguished name		
CommonName (CN)	Fullgilt audkenni 2021	Certificate authority name.
OrganisationIdentifier	NTRIS-5210002790	Business registration number.
Serial Number(S)	5210002790	Business registration number.
OrganisationName (O)	Auðkenni ehf.	Name of issuer organisation.
CountryName (C)	IS	Country code „IS" for Iceland.
Valid from	<First date of validity>	First date of Certificate validity.
Valid to	<Last date of validity>	Last date of Certificate validity. Max four years.
Subject Distinguished Name		
Serial Number (S)	<ID of subscriber>	Business registration number
OrganisationName (O)	<Name of subject>	Organisation name in UTF8 format.
CommonName (CN)	<Name of Service>	Name connected to the business in UTF8 format.
OrganisationIdentifier	<ID of Subscriber>	Business registration number in the form NTRIS-#
CountryName (C)	IS	Country code „IS" for Iceland.
Subject Public Key	RSA 2048, 4096	RSA algorithm in accordance with RFC 4055
Extensions		
Basic Constraints	Subject Type = End Entity Path Length Constraint = None	
Key Usage	nonRepudiation	
QC Statements	QC Compliance (0.4.0.1862.1.1) QC PKI Disclosure Statements (0.4.0.1862.1.5) IS: https://repo.audkenni .is/pds QC Type EtsiQctEseal (0.4.0.1862.1.6.2) QC id-etsi-qcs-semanticsId-Legal (0.4.0.194121.1.2)	
AuthorityKeyIdentifier	SHA-1 hash of the public key	
SubjectKeyIdentifier	SHA-1 hash of the public key	
Authority Information Access		
Oscp	http://ocsp.audkenni.is	
CertificateAuthorityIssuer	https://cdp.islandsrot.is/skilriki/FA2021.p7b	
Certificate Policies	Policy Identifier = 2.16.352.1.2.1.1.2 0.4.0.194112.1.1 0.4.0.2042.1.2 2.16.352.1.2.13.2	https://repo.audkenni.is/cps Notice text: eSeal – Advanced HSM
CRLDisributionpoints	URI: http://crl.audkenni.is/FA2021/latest.crl	

Qualified End-user Signing Certificate – eSeal QCP-l – NCP

Field	Value	Description
Version	V3	Certificate format version.
Serial number	<Unique ID>	Unique serial number of the certificate.
Signature Algorithm	Sha256WithRSAEncryption	Signature algorithm in accordance with RFC 5280.
Issuer Distinguished name		
CommonName (CN)	Fullgilt audkenni 2021	Certificate authority name.
OrganisationIdentifier	NTRIS-5210002790	Business registration number.
Serial Number(S)	5210002790	Business registration number.
OrganisationName (O)	Auðkenni ehf.	Name of issuer organisation.
CountryName (C)	IS	Country code „IS" for Iceland.
Valid from	<First date of validity>	First date of Certificate validity.
Valid to	<Last date of validity>	Last date of Certificate validity. Max four years.
Subject Distinguished Name		
Serial Number (S)	<ID of subscriber>	Business registration number
OrganisationName (O)	<Name of subject>	Organisation name in UTF8 format.
CommonName (CN)	<Name of Service>	Name connected to the business in UTF8 format.
OrganisationIdentifier	<ID of Subscriber>	Business registration number in the form NTRIS-#
CountryName (C)	IS	Country code „IS" for Iceland.
Subject Public Key	RSA 2048, 4096	RSA algorithm in accordance with RFC 4055
Extensions		
Basic Constraints	Subject Type = End Entity Path Length Constraint = None	
Key Usage	nonRepudiation	
QC Statements	QC Compliance (0.4.0.1862.1.1) QC PKI Disclosure Statements (0.4.0.1862.1.5) IS: https://repo.audkenni .is/pds QC Type EtsiQctEseal (0.4.0.1862.1.6.2) QC id-etsi-qcs-semanticsId-Legal (0.4.0.194121.1.2)	
AuthorityKeyIdentifier	SHA-1 hash of the public key	
SubjectKeyIdentifier	SHA-1 hash of the public key	
Authority Information Access		
Oscp	http://ocsp.audkenni.is	
CertificateAuthorityIssuer	https://cdp.islandsrot.is/skilriki/FA2021.p7b	
Certificate Policies	Policy Identifier = 2.16.352.1.2.1.1.2 0.4.0.194112.1.1 0.4.0.2042.1.1 2.16.352.1.2.13.3	https://repo.audkenni.is/cps Notice text: eSeal – Advanced SOFT
CRLDisributionpoints	URI: http://crl.audkenni.is/FA2021/latest.crl	

Non-Qualified Certificate End-user signing and authentication - Equipment Authentication

Field	Value	Description
Version	V3	Certificate format version.
Serial number	<Unique ID>	Unique serial number of the certificate.
Signature Algorithm	Sha256WithRSAEncryption	Signature algorithm in accordance with RFC 5280.
Issuer Distinguished name		
CommonName (CN)	Fullgilt audkenni 2021	Certificate authority name.
OrganisationIdentifier	NTRIS-5210002790	Business registration number.
Serial Number (S)	5210002790	Business registration number backward compatible.
OrganisationName (O)	Auðkenni ehf.	Name of issuer organisation.
CountryName (C)	IS	Country code „IS" for Iceland.
Valid from	<First date of validity>	First date of Certificate validity.
Valid to	<Last date of validity>	Last date of Certificate validity. Max four years.
Subject Distinguished Name		
Serial Number (S)	<ID of subscriber>	Business registration number backward compatible.
OrganisationName (O)	<Name of subject>	Organisation name in UTF8 format.
CommonName (CN)	<Name of service>	Name connected to the business in UTF8 format.
OrganisationIdentifier	<ID of Subscriber>	Business registration number in the form NTRIS-#
CountryName (C)	IS	Country code „IS" for Iceland.
Subject Public Key	RSA 2048, 4096	RSA algorithm in accordance with RFC 4055
Extensions		
Basic Constraints	Subject Type = End Entity Path Length Constraint = None	
Certificate Policies	Policy Identifier = 2.16.352.1.2.1.1.2 0.4.0.2042.1.1 2.16.352.1.2.14.1	https://repo.audkenni.is/cps Notice text: Equipment Authentication
Key Usage	Digital Signature, Key Encipherment, nonRepudiation	
CRLDisributionpoints	URI: http://crl.audkenni.is/FA2021/latest.crl	
AuthorityKeyIdentifier	SHA-1 hash of the public key	
SubjectKeyIdentifier	SHA-1 hash of the public key	
Authority Information Access		
Oscp	http://ocsp.audkenni.is	
CertificateAuthorityIssuer	https://cdp.islandsrot.is/skilriki/FA2021.p7b	

4.3.4 Certificates on App

Qualified End-user Signing Certificate – human end-users (App)

Field	Value	Description
Version	V3	Certificate format version.
Serial number	<Unique ID>	Unique serial number of the certificate.
Signature Algorithm	Sha256WithRSAEncryption	Signature algorithm in accordance with RFC 5280.
Issuer Distinguished name		
CommonName (CN)	Fullgilt audkenni 2021	Certificate authority name.
OrganisationIdentifier	NTRIS-5210002790	Business registration number.
Serial Number (S)	5210002790	Business registration number backward compatible.
OrganisationName (O)	Auðkenni ehf.	Name of issuer organisation.
CountryName (C)	IS	Country code „IS" for Iceland.
Valid from	<First date of validity>	First date of Certificate validity.
Valid to	<Last date of validity>	Last date of Certificate validity. Max five years.
Subject Distinguished Name		
Serial Number (S)	<PNO of subject>	Unique personal identity code.
Given Name (G)	<Subject given name>	Person given name in UTF8 format.
SurName (S)	<Subject surname>	Person surname in UTF8 format.
CommonName (CN)	<Subject full name>	Person full name in UTF8 format.
CountryName (C)	IS	Country code „IS" for Iceland.
Subject Public Key	RSA 6144, 6143, 6142, 8192	RSA algorithm in accordance with RFC 4055
Extensions		
Basic Constraints	Subject Type = End Entity Path Length Constraint = None	
Certificate Policies	Policy Identifier = 2.16.352.1.2.1.1.2 0.4.0.194112.1.2 2.16.352.1.2.12.1	https://repo.audkenni.is/cps Notice text: App on Smartphone - Qualified
CRLDisributionpoints	URI: http://crl.audkenni.is/FA2021/latest.crl	
Key Usage	nonRepudiation	
QC Statements	QC Compliance (0.4.0.1862.1.1) QC Secure Signature Creation Device (0.4.0.1862.1.4) QC PKI Disclosure Statements (0.4.0.1862.1.5) IS: https://repo.audkenni.is/pds QC Type EtsiQctEsign (0.4.0.1862.1.6.1)	
AuthorityKeyIdentifier	SHA-1 hash of the public key	
SubjectKeyIdentifier	SHA-1 hash of the public key	
Authority Information Access		
Oscp	http://ocsp.audkenni.is	
CertificateAuthorityIssuer	https://cdp.islandsrot.is/skilriki/FA2021.p7b	

End-user Authentication Certificate - human end-users (App)

Field	Value	Description
Version	V3	Certificate format version.
Serial number	<Unique ID>	Unique serial number of the certificate.
Signature Algorithm	Sha256WithRSAEncryption	Signature algorithm in accordance with RFC 5280.
Issuer Distinguished name		
CommonName (CN)	Fullgilt audkenni 2021	Certificate authority name.
OrganisationIdentifier	NTRIS-5210002790	Business registration number.
Serial Number (S)	5210002790	Business registration number backward compatible.
OrganisationName (O)	Auðkenni ehf.	Name of issuer organisation.
CountryName (C)	IS	Country code „IS" for Iceland.
Valid from	<First date of validity>	First date of Certificate validity.
Valid to	<Last date of validity>	Last date of Certificate validity. Max five years.
Subject Distinguished Name		
Serial Number (S)	<PNO of subject>	Unique personal identity code.
Given Name (G)	<Subject given name>	Person given name in UTF8 format.
SurName (S)	<Subject surname>	Person surname in UTF8 format.
CommonName (CN)	<Subject full name>	Person full name in UTF8 format.
CountryName (C)	IS	Country code „IS" for Iceland.
Subject Public Key	RSA 6144, 8192	RSA algorithm in accordance with RFC 4055
Extensions		
Basic Constraints	Subject Type = End Entity Path Length Constraint = None	
Certificate Policies	Policy Identifier = 2.16.352.1.2.1.1.2 0.4.0.2042.1.2 2.16.352.1.2.12.1	https://repo.audkenni.is/cps Notice text: App on Smartphone - Qualified
CRLDisributionpoints	URI: http://crl.audkenni.is/FA2021/latest.crl	
AuthorityKeyIdentifier	SHA-1 hash of the public key	
SubjectKeyIdentifier	SHA-1 hash of the public key	
Key Usage	Digital Signature, Key Encipherment	
Extended Key Usage	Client Authentication	
Authority Information Access		
Oscp	http://ocsp.audkenni.is	
CertificateAuthorityIssuer	https://cdp.islandsrot.is/skilriki/FA2021.p7b	

4.3.5 TSU Certificate

Non-Qualified End-user Time-Stamping Unit

Field	Value	Description
Version	V3	Certificate format version.
Serial number	<Unique ID>	Unique serial number of the certificate.
Signature Algorithm	Sha256WithRSAEncryption	Signature algorithm in accordance with RFC 5280.
Issuer Distinguished name		
CommonName (CN)	Fullgilt audkenni 2021	Certificate authority name.
OrganisationIdentifier	NTRIS-5210002790	Business registration number.
Serial Number(S)	5210002790	Business registration number.
OrganisationName (O)	Auðkenni ehf.	Name of issuer organisation.
CountryName (C)	IS	Country code „IS" for Iceland.
Valid from	<First date of validity>	First date of Certificate validity.
Valid to	<Last date of validity>	Last date of Certificate validity. Six years.
Subject Distinguished Name		
Serial Number (S)	<ID of subscriber>	Business registration number
OrganisationName (O)	<Name of subject>	Organisation name in UTF8 format.
CommonName (CN)	<Name of Service>	Name connected to the business in UTF8 format.
OrganisationIdentifier	<ID of Subscriber>	Business registration number in the form NTRIS-#
CountryName (C)	IS	Country code „IS" for Iceland.
Subject Public Key	RSA 3072	RSA algorithm in accordance with RFC 4055
Extensions		
Basic Constraints	Subject Type = End Entity Path Length Constraint = None	
Key Usage	nonRepudiation, Digitalsignature	
AuthorityKeyIdentifier	SHA-1 hash of the public key	
SubjectKeyIdentifier	SHA-1 hash of the public key	
Private Key Usage Period	Not Before: [issuing date & time] Not After: [1 year and 42 days after issuing date & time]	
Authority Information Access		
Oscp	http://ocsp.audkenni.is	
CertificateAuthorityIssuer	https://cdp.islandsrot.is/skilriki/FA2021.p7b	
Certificate Policies	Policy Identifier = 2.16.352.1.2.1.1.2 0.4.0.2042.1.2 2.16.352.1.2.14.2	https://repo.audkenni.is/cps Notice text: Time-Stamping Unit
CRLDisributionpoints	URI: http://crl.audkenni.is/FA2021/latest.crl	
Extended Key Usage	Time Stamping (1.3.6.1.5.5.7.3.8)	

5 OCSP PROFILE

OCSP profile. The version for OCSP profile shall be 1.

OCSP profile is as defined in RFC 6960.

Name	Format	Description	Necessity
ResponeseStatus	#	0 for success or error number	M
ResponseBytes			O
ResponseType	Id-pkiz-ocsp-basic	Basic OCSP Response	M
BasicOCSPResponse			M
ResponseData			M
Version	1	Version of response format	M
Responder ID	CN = ocsp.audkenni.is SERIALNUMBER = 5210002790 OrganisationIdentifier=NTRIS-5210002790 O = Audkenni ehf. C = IS		M
Produced At	<Date signed>		M
Responses			M
CertID	SHA1 hash of CertID	Issuer Name hash, Issuer Key Hash, Serial Number	M
Cert Status	<GOOD | REVOKED | UNKNOWN >		M
Revocation Time	<Date revoked>		O
Revocation Reason	<Code>	Code for Revocation	O
This Update	<Date of CRL Update>		M
Next Update	<Date of next CRL Update>	In case of CA certificate is about to expire NextUpdate will be set to 99991231235959Z	
Archive Cutoff	<CA Valid from date>	CA's certificate "valid from" date.	M
Nonce		Value copied from request if included.	O
Signature algorithm	Sha256WithRSAEncryption		M
Signature			M
Certificate		Certificate for private key used to sign response.	M

Non-issued certificates or "unknown" certificates can by identified by the OCSP answer "revoked" in combination with the reason "certificateHold" and revocation date "1.1.1970. This is according to RFC 6960

6 CRL PROFILE

Validation services need to ensure that most recent CRL is available.

CA and RAs SHALL be able to suspend Certificates on Cards, and subsequently either revoke or reinstate it. Other types of Certificates cannot be suspended.

CRL profile is as defined in RFC 5280.

6.1 Version number(s)

The version of CRLs shall be version 2.

6.2 CRL and CRL entry extensions

Name	Format	Description	Necessity
Version	INTEGER	Version shall be v2, i.e., value 1	M
Signature	Sha256WithRSAEncryption	Defines the algorithm used to sign the CRL	M
Issuer Distinguished Name	Name	The field shall contain the subject DN of the CA that issued the CRL	M
Common Name (CN)	Fullgilt auðkenni 2021	Name of the issuing certification authority	M
OrganisationIdentifier	NTRIS-5210002790	Identification of the issuer.	M
Organization (O)	Auðkenni ehf		M
Country (C)	IS	Country code for Iceland (IS)	M
EffectiveDate		Date and time of issuance.	M
ThisUpdate	UTCTime	Specifies when the CRL was generated	M
NextUpdate	UTCTime ThisUpdate + 24 hours	Specifies when the CRL expires. The next CRL shall be issued before the current CRL expires. In case of CRL Termination NextUpdate will be set to 99991231235959Z	M
RevokedCertificates		List of revoked certificates.	M
SerialNumber	INTEGER	The serial number of the revoked certificate	M
RevocationDate	UTCTime	The date of revocation	M
Signature		Confirmation signature of the authority that issued the CRL	
CrlExtensions	Extensions	CRLNumber	M
CRL Number			

Name	Format	Description	Necessity
Authority Key Identifier	SHA-1 hash of the public key		
Issuing Distribution Point	URL=http://crl.audkenni.is/FA2021/latest.crl		
ExpiredCertsOnCRL		Expired Revoked Certificates not removed from list.	M

Note that revoked Certificates may be empty.

Expired revoked certificates are not removed from the CRL.

None of the Extensions are marked as critical.