

AK

Certificate Profiles

Version: 1.1 – 05.05.2021

| Change control | | | |
|----------------|---------|---|--------------------|
| Published | Version | Changes | Approval |
| 16.03.2021 | 1.0 | Final approved version | Security Committee |
| 06.04.2021 | 1.1 | Added "Notice text" Fixed typos Effective date does not change. | |
| | | | |

TABLE OF CONTENTS

| | |
|--|-----------|
| 1 SCOPE AND PURPOSE | 4 |
| 1.1 DOCUMENT STRUCTURE | 4 |
| 2 DEFINITIONS | 4 |
| 3 OVERVIEW | 5 |
| 4 CERTIFICATES | 6 |
| 4.1 ISLANDSROT ROOT CERTIFICATE | 6 |
| 4.1.1 <i>Certificate-signing</i> | 6 |
| 4.2 AUDKENNI CA CERTIFICATE | 7 |
| 4.2.1 <i>Certificate-signing and CRL-signing Certificate</i> | 7 |
| 4.3 SUBSCRIBER CERTIFICATES | 8 |
| 4.3.1 <i>Certificates on Cards</i> | 9 |
| 4.3.2 <i>Certificates on Mobile</i> | 13 |
| 4.3.3 <i>Certificates on eSeals and Equipment Authentication</i> | 15 |
| 4.3.4 <i>Certificates on App</i> | 18 |
| 5 OCSP PROFILE | 22 |
| 6 CRL PROFILE | 23 |
| 6.1 VERSION NUMBER(S) | 23 |
| 6.2 CRL AND CRL ENTRY EXTENSIONS | 23 |

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 of 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 and Certificates in eSeals.

Chapter 6 lists the Auðkenni OCSP and CRL profile.

2 DEFINITIONS

| Definition | Description |
|---|---|
| <SSN of subject> <SSN of subscriber> | An alphanumeric value representing the Social Security 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 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 OIs are described in the following table:

| Service Type | OID | QCP-n-qscd | NCP+ | NCP |
|--|-------------------|------------------|------------------|----------------|
| 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 |
| App on Smartphone – Non-Qualified | 2.16.352.1.2.12.2 | NA | 0.4.0.2042.1.2 | NA |
| | | QCP-l-qscd | QCP-l | NCP |
| eSeal – Qualified | 2.16.352.1.2.13.1 | 0.4.0.194112.1.3 | NA | NA |
| eSeal – Advanced | 2.16.352.1.2.13.2 | NA | 0.4.0.194112.1.1 | NA |
| Equipment Authentication | 2.16.352.1.2.14.1 | NA | NA | 0.4.0.2042.1.1 |

3 OVERVIEW

| Name of certificate | In the cert. path | Description |
|---|-------------------|--|
| Root CA certificate (Islandsrot) | Yes | This is the root CA that issues the intermediate CA Fullgilt audkenni. |
| Intermediate CA certificate (Fullgilt audkenni) | 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 and non-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 April 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) | Fjarmalaraduneyti | 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 | Fjarmalaraduneyti | 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 http://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) | Fjarmalaraduneyti | 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 | |
| QC Statements | QC Compliance (0.4.0.1862.1) 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 public key. No name or serial number included | |
| Authority Information Access | | |
| Oscp | Null | |
| CertificateAuthorityIssuer | http://cdp.islandsrot.is/skilriki/FA2021.p7b | |
| Certificate Policies | Policy identifier: 2.16.352.1.1.1.1 http://cp.islandsrot.is | |
| CRLDistributionpoints | 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 and Non-qualified.
- Certificates for eSeals (general equipment). KeyStore HSM at Client or HSM on Cryptostick or File in case of NQ Certificate

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 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 one year. |
| Subject Distinguished Name | | |
| Serial Number (S) | <SSN 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 | http://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 |
| CRLDistributionpoints | 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 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) | <SSN 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 | http://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 |
| CRLDistributionpoints | URI: http://crl.audkenni.is/FA2021/latest.crl | |
| Extended Key Usage | Client Authentication | |

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

| Field | Value | Description |
|-------------------------------------|---|---|
| Version | V3 | Certificate format version. |
| Serial number | <Unique ID> | Unique serial number of 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-521000279 | 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) | <SSN 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> | |
| 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 | http://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 |
| CRLDistributionpoints | URI: http://crl.audkenni.is/FA2021/latest.crl | Notice text: Cards natural person + legal person |

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 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) | <SSN 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> | |
| 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 | http://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 |
| CRLDistributionpoints | 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 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) | <SSN 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 | http://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 |
| CRLDistributionpoints | 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 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) | <SSN 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 | http://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 |
| CRLDistributionpoints | 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-I-qscd

| Field | Value | Description |
|-------------------------------------|---|---|
| Version | V3 | Certificate format version. |
| Serial number | <Unique ID> | Unique serial number of 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 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-semanticId-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 | http://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 |
| CRLDistributionpoints | URI: http://crl.audkenni.is/FA2021/latest.crl | |

Qualified End-user Signing Certificate – eSeal QCP-1

| 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 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-semanticId-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 | http://cdp.islandsrot.is/skilriki/FA2021.p7b | |
| Certificate Policies | Policy Identifier = 2.16.352.1.2.1.1.2 0.4.0.194112.1.1 2.16.352.1.2.13.2 | https://repo.audkenni.is/cps Notice text: eSeal - Advanced |
| 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 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 0.4.0.2042.1.2 2.16.352.1.2.14.1 | https://repo.audkenni.is/cps Notice text: Equipment Authentication |
| Key Usage | Digital Signature, Key Encipherment, nonRepudiation | |
| CRLDistributionpoints | URI: http://crl.audkenni.is/FA2021/latest.crl | |
| SubjectKeyIdentifier | SHA-1 hash of the public key | |
| Authority Information Access | | |
| Oscp | http://ocsp.audkenni.is | |
| CertificateAuthorityIssuer | http://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 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) | <SSN 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 0.4.0.194112.1.2 2.16.352.1.2.12.1 | https://repo.audkenni.is/cps Notice text: App on Smartphone - Qualified |
| CRLDistributionpoints | 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 | http://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 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) | <SSN 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 |
| CRLDistributionpoints | URI: http://crl.audkenni.is/FA2021/latest.crl | |
| SubjectKeyIdentifier | SHA-1 hash of the public key | |
| Key Usage | DigitalSignature, KeyEncipherment | |
| Extended Key Usage | Client Authentication | |
| Authority Information Access | | |
| Oscp | http://ocsp.audkenni.is | |
| CertificateAuthorityIssuer | http://cdp.islandsrot.is/skilriki/FA2021.p7b | |

Non-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) | <SSN 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 2.16.352.1.2.12.2 | https://repo.audkenni.is/cps |
| CRLDistributionpoints | URI: http://crl.audkenni.is/FA2021/latest.crl | |
| Key Usage | nonrepudiation | |
| 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 | http://cdp.islandsrot.is/skilriki/FA2021.p7b | |

Non-Qualified 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) | <SSN 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 2.16.352.1.2.12.2 | https://repo.audkenni.is/cps Notice text: App on Smartphone - Non-Qualified |
| CRLDisributionpoints | URI: http://crl.audkenni.is/FA2021/latest.crl | |
| Key Usage | DigitalSignature, KeyEncipherment | |
| Extended Key Usage | Client Authentication | |
| 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 | http://cdp.islandsrot.is/skilriki/FA2021.p7b | |

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 |
|---------------------|---|--|-----------|
| ResponseStatus | # | 0 for success or error number | M |
| ResponseBytes | | | O |
| ResponseType | Id-pkix-ocsp-basic | Basic OCSP Response | M |
| BasicOCSPResponse | | | M |
| ResponseData | | | M |
| Version | 1 | Version of response format | M |
| Responder ID | CN = ocspp.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 |

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 audkenni 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 | 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 | | | 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 Numer | | | |

| Name | Format | Description | Necessity |
|----------------------------|--|-------------|-----------|
| Authority Key Identifier | | | |
| Issuing Distribution Point | URL=http://crl.audkenni.is/FA2021/latest.crl | | |

Note that revokedCertificates may be empty.

Expired certificates are not removed from the CRL.

None of the Extensions are marked as critical.