INNIHALD
RAFRÆNNA SKILRÍKJA

Samræmt innihald rafrænna skilríkja
sem gefin eru út á Íslandi

Útgáfa 01-04-00
30. nóvember 2006

Þetta skjal er samkomulag sérfræðinga ríkis og banka um samræmt innihald rafrænna skilríkja.

Breytingasaga

Útgáfudagur	Útgáfa	Lýsing	Ábyrgðaraðili
12.3.2006	01-00-00	Fyrsta útgáfa – takmörkuð dreifing.	AFAx
13.3.2006	01-01-00	Útgáfa til allra meðlima samstarfshóps sérfræðinga ríkis og SBV. Leiðréttingar á dæmum í töflum. Viðbætur á skilgreiningu á Qualified certificate statement.	AFAx
9.8.2006	01-02-00	Útgáfa eftir breytingar á töflu yfir kröfur til svæða þar sem kröfur eru nú settar fram um notkun og vægi. Samsvarandi breytingar voru gerðar í töflum með skilgreiningum á svæðum og töflum með dæmum.	AFAx
3.10.2006	01-02-03	Drög (vinnuútgáfa) fyrir afmarkaða dreifingu.	AFAx
3.11.2006	01-03-00	Útgáfa lögð fram í sérfræðihópi ríkis og banka til staðfestingar.	AFAx
23.11.2006	01-03-02	Vinnuskjal með samþykktum breytingum frá samráðsfundi sérfræðinga ríkis og banka þann 9.11.2006.	AFAx
30.11.2006	01-04-00	Lokaútgáfa til staðfestingar sem samkomulag hjá sérfræðingum ríkis og banka fyrir kl. 12:00 fimmtudaginn 30. nóvember 2006.	AFAx

Efnisyfirlit

1 Inngangur

Tilgangur skjalsins er að samræma kröfur til innihalds rafrænna skilríkja til að samræma notkun skilríkja á Íslandi. Skjalið lýsir innihaldi rafrænna skilríkja þar sem byggt er á alþjóðlegum stöðlum og viðmiðunum. Skjalið tilgreinir lágmarkskröfur en er ekki ætlað að vera tæmandi listi yfir möguleika á innihaldi rafrænna skilríkja.

Í þessu skjali er ekki sérstaklega fjallað um þau sjálfgefnu gildi sem þurfa að vera til staðar svo að rafræn skilríki virki, t.d.

- Public key
- Thumbprint algorithm
- Thumbprint

2 Tilvísanir

[1] Lög um rafrænar undirskriftir, nr. 28/2001, með síðari breytingum.

[2] Tilskipun Evrópuþingsins og ráðsins 1999/93/EB frá 13. desember 1999 um ramma bandalagsins varðandi rafrænar undirskriftir.

[3] ISO/IEC 9594-8:2001 | ITU-T Recommendation X.509: *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[4] IETF RFC 3280, apríl 2002: *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[5] IETF RFC 3739, mars 2004: *Internet X.509 Public Key Infrastructure Qualified Certificates Profile*.

[6] ETSI TS 101 862 v1.3.1 (2004-03): *Qualified Certificate Profile.*

[7] ETSI TS 102 280 v1.1.1 (2004-03): *X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons.*

[8] ISO/IEC 9834-1:2005 | ITU-T Recommendation X.660: *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: General Procedures and top arcs of the ANS.1 Object Identifier tree*.

[9] ETSI TS 102 176-1 v 1.2.1 (2005-07): *Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms*.

[10] IETF RFC 2616, júní 1999: *Hypertext Transfer Protocol -- HTTP/1.1*.

[11] IETF RFC 2255, desember 1997: *The LDAP URL Format.*

[12] IETF RFC 2560, júní 1999: *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*.

3 Meðmæli um innihald rafrænna skilríkja á Íslandi

Í þessum kafla er lýsing á innihaldi rafrænna skilríkja sem gefin eru út á Íslandi til áskrifenda sem hafa lögsögu á Íslandi. Lýsingin á við um innihald rótarskilríkja, milliskilríkja og endaskilríkja. Lýsingin gildir fyrir einkaskilríki (þar sem vottorðshafinn er einstaklingur sem jafnframt er áskrifandi skilríkjanna), starfsskilríki (þar sem vottorðshafi er einstaklingur í tengslum við fyrirtæki, stofnun eða félag sem er áskrifandi skilríkjanna), búnaðarskilríki (sem staðfesta að búnaður (hug- eða vélbúnaður) sé tengdur

áskrifanda skilríkjanna) og skipulagsheildarskilríki (sem staðfesta að svið, deild eða önnur skipulagsheild séu tengd fyrirtæki, stofnun eða félagi sem áskrifanda skilríkjanna).

Þessi meðmæli um innihald rafrænna skilríkja byggja á tæknilýsingu ETSI TS 102 280 [7] sem aftur byggir á ETSI TS 101 862 [6] og IETF viðmiðum RFC 3280 [4] og RFC 3739 [5] fyrir innihald X.509 v3 [3] skilríkja. Nota skal svæði rafrænna skilríkja á Íslandi á þann hátt sem tilgreint er í þessum gögnum, með þeim breytingum eða viðbótum sem koma fram í þessu skjali.

Eftirfarandi tafla sýnir þau svæði sem skilgreind eru í ETSI TS 102 280 [7]. Þessi upptalning er ekki tæmandi listi yfir möguleika á innihaldi rafrænna skilríkja.

Undirstöðusvæði	Stöðluð viðskeyti	Önnur svæði
• Version • Serial number • Signature • Issuer • Validity • Subject • Subject public key info	• Authority key identifier • Subject key identifier • Key usage • Private key usage period • Certificate policies • Policy mappings • Subject alternative name • Issuer alternative name • Subject directory attributes • Basic constraints • Name constraints • Policy constraints • Extended key usage • CRL distribution points • Inhibit any-policy • Freshest CRL	X.509 v2: • Issuer Unique Identifier • Subject Unique Identifier RFC 3280 Internet certificate ext. • Authority Information Access • Subject information access RFC 3739 certificate ext. • Biometric information • Qualified certificate statement

Í þessum kafla er einungis fjallað um þau svæði í skilríkjum sem eru skilgreind ítarlegar heldur en í áðurnefndum stöðlum og viðmiðunum, eða þar sem frávik er á skilgreiningunni. Þau svæði sem ekki er fjallað sérstaklega um hér skal nota á þann hátt sem tilgreint er í þeim viðmiðunarstöðlum sem byggt er á. Er þar sérstaklega vísað á ETSI TS 102 280 [7].

Lausnaraðilar sem þróa hugbúnað sem les skilríki og staðfestir gildi þeirra skulu miða við kröfur í X.509 staðlinum [3], sjá m.a. kafla 7.

Til að tryggja sem best samhæfni skilríkja til framtíðar er lögð áhersla á að miða við evrópska og alþjóðlega staðla og önnur almennt viðurkennd viðmið þegar innihald skilríkjanna er lagað að íslensku umhverfi.

3.1 Tilgreind svæði

Í töflunni hér fyrir neðan er yfirlit yfir þau svæði í skilríkjum sem fjallað er um í þessum kafla. Í töflunni eru tilgreindar kröfur til notkunar á svæðum með eftirfarandi merkingum:

Notkun:

M:	Skilyrt svæði – svæðið skal vera notað (e. mandatory).
O:	Valfrjáls notkun (e. optional).
- :	Ekki eru tilgreindar kröfur til notkunar svæðis.

Vægi:

C:	Mikilvægt (krítískt) svæði – svæðið skal vera merkt krítískt (e. critical).
X:	Svæðið má ekki merkja sem krítískt (e. critical).
(C):	Vottunarstöð má merkja svæðið krítískt (e. critical).
- :	Ekki eru tilgreindar kröfur til notkunar svæðis.

Svæði	Enda-skilríki		Milli-skilríki		Rótar-skilríki		Tilvísun í IETF RFC
	Notkun	Vægi	Notkun	Vægi	Notkun	Vægi	
Issuer	M	-	M	-	M	-	3280 4.1.2.4 [4]
Subject	M	-	M	-	M	-	3280 4.1.2.6 [4]
Authority key identifier	O	X	O	X	-	-	3280 4.2.1.1 [4]
Subject key identifier	O	X	M	X	M	X	3280 4.2.1.2 [4]
Key usage	M	C	M	C	M	C	3280 4.2.1.3 [4]
Certificate policies	M	X	O	X	O	X	3280 4.2.1.5 [4]
Subject alternative name	O	X	O	X	O	X	3280 4.2.1.7 [4]
Basic constraints	M	(C)	M	C	M	C	3280 4.2.1.10 [4]
Extended key usage	O	X	O	X	O	X	3280 4.2.1.13 [4]
CRL distribution points	M	X	M	X	-	X	3280 4.2.1.14 [4]
Authority Information Access	O	X	O	X	O	X	3280 4.2.2.1 [4]
Qualified certificate statement	O	(C)	-	X	-	X	3739 3.2.6 [5]

3.2 Skilgreining á gildum

Í eftirfarandi töflu er ítarleg skilgreining á notkun svæða í skilríkjum í íslensku umhverfi.

Svæði	Endaskilríki	Milliskilríki	Rótarskilríki	RFC 3280 [4]
Issuer	Eftirfarandi eigindi skal nota til að auðkenna útgefanda skilríkjanna á einkvæman hátt: **countryName (C)=IS** **organizationName (O)**=*Nafn útgefanda endaskilríkjanna (nafn vottunarstöðvarinnar)* **serialNumber (SN)**=*Kennitala útgefanda skilríkjanna* Mælt er með að nota **commonName (CN)** eigindið. Gildi **commonName (CN)** er valfrjást og ekki tómur strengur. Það er valfrjálst að nota **organizationalUnitName (OU)** eigindið til að tilgreina nánar skipulagsheild innan vottunarstöðvar eða hlutverk skilríkja til frekari afmörkunar, en staðfesting á trausti vottunarslóðar mun ekki byggja á því. Ekki er takmörk á fjölda **organizationalUnitName (OU)** gilda í svæðinu.	Eftirfarandi eigindi skal nota til að auðkenna útgefanda skilríkjanna á einkvæman hátt: **countryName (C)=IS** **organizationName (O)**=*Nafn útgefanda milliskilríkjanna (nafn vottunarstöðvarinnar)* **serialNumber (SN)**=*Kennitala útgefanda skilríkjanna* Mælt er með að nota **commonName (CN)** eigindið. Gildi **commonName (CN)** er valfrjást og ekki tómur strengur. Það er valfrjálst að nota **organizationalUnitName (OU)** eigindið til að tilgreina nánar skipulagsheild innan vottunarstöðvar eða hlutverk skilríkja til frekari afmörkunar, en staðfesting á trausti vottunarslóðar mun ekki byggja á því. Ekki er takmörk á fjölda **organizationalUnitName (OU)** gilda í svæðinu.	Eftirfarandi eigindi skal nota til að auðkenna útgefanda skilríkjanna á einkvæman hátt: **countryName (C)=IS** **organizationName (O)**=*Nafn útgefanda rótarskilríkjanna (nafn vottunarstöðvarinnar)* **serialNumber (SN)**=*Kennitala útgefanda skilríkjanna* Útgefandi rótarskilríkja er jafnframt vottorðshafi skilríkjanna. Mælt er með að nota **commonName (CN)** eigindið. Gildi **commonName (CN)** er valfrjást og ekki tómur strengur. Í **commonName (CN)** má tilgreina að skilríkið sé rótarskilríki. Það er valfrjálst að nota **organizationalUnitName (OU)** eigindið til að tilgreina nánar skipulagsheild innan vottunarstöðvar til frekari afmörkunar, en staðfesting á trausti vottunarslóðar mun ekki byggja á því. Ekki er takmörk á fjölda **organizationalUnitName (OU)** gilda í svæðinu.	4.1.2.4
Subject	Eftirfarandi eigindi skal nota til að auðkenna vottorðshafa skilríkjanna á einkvæman hátt: **countryName (C)=IS** **organizationName (O)**=*Nafn áskrifanda skilríkjanna (ef annar en vottorðshafi)* **organizationalUnitName (OU)**=*Tegund skilríkis.* **serialNumber (SN)**=*Kennitala vottorðshafa***:***kennitala áskrifanda*	Eftirfarandi eigindi skal nota til að auðkenna vottorðshafa skilríkjanna á einkvæman hátt: **countryName (C)=IS** **organizationName (O)**=*Nafn áskrifanda milliskilríkjanna (nafn vottunarstöðvarinnar)* **serialNumber (SN)**=*Kennitala útgefanda skilríkjanna*	Eftirfarandi eigindi skal nota til að auðkenna vottorðshafa skilríkjanna á einkvæman hátt: **countryName (C)=IS** **organizationName (O)**=*Nafn áskrifanda milliskilríkjanna (nafn vottunarstöðvarinnar)* **serialNumber (SN)**=*Kennitala vottorðshafa (vottunarstöðvarinnar)*	4.1.2.6

Svæði	Endaskilríki	Milliskilríki	Rótarskilríki	RFC 3280 [4]
	Mælt er með að nota **commonName (CN)** eigindið. Gildi **commonName (CN)** má ekki vera tómur strengur, en er að öðru leiti valfrjást. Gildi **commonName (CN)** er oft heiti vottorðshafa. Fyrsta **organizationalUnitName (OU) eigindi** svæðisins skal skilgreina tegund skilríkis. Þetta **organizationalUnitName (OU)** skal hafa eitt af eftirfarandi gildum (eftir því sem við á): einkaskilriki, starfsskilriki, bunadarskilriki, skipulagsheildarskilriki. Mælt er með að nota annað **organizationalUnitName (OU)** sem lýsir hlutverki skilríkisins. Í þeim tilvikum þar sem ekki er önnur aðgreining í Issuer og Subject svæðunum skal nota þriðja OU til aðgreiningar. Svæðin Issuer og Subject skulu ekki vera eins í tveimur sklríkjum. Ekki eru takmörk á fjölda **organizationalUnitName (OU)** gilda í svæðinu, en staðfesting á trausti vottunarslóðar mun ekki byggja á þeim. Hafa ber í huga að við úrvinnslu skilríkjanna er óvíst að aðilar skoði fleiri en tvö fyrstu gildin í **organizationalUnitName (OU)**. Í eigindinu **organizationName (O)** er tómur strengur ef vottorðshafi og áskrifandi skilríkjanna er sami aðili. Annars er nafn áskrifanda í **organizationName (O)**. Ef **organizationName (O)** er ekki með tóman streng þá er gildið í eigindinni **serialNumber (SN)** kennitala vottorðshafa og kennitala áskrifanda aðgreint með bókstafnum „**:**” án stafbila. Kennitölurnar eru 10 tölustafir án stafbila, eins og þær eru í opinberum skrám. Tvípunktur kemur aðeins fyrir ef	Mælt er með að nota **commonName (CN)** eigindið. Gildi **commonName (CN)** má ekki vera tómur strengur, en er að öðru leiti valfrjást Vottunarstöðin er bæði áskrifandi milliskilríkja og vottorðshafi. Það er valfrjálst að nota **organizationalUnitName (OU)** eigindið til að tilgreina skipulagsheild innan vottunarstöðvar eða hlutverk skilríkja til frekari afmörkunar, eða til að tilgreina tegund skilríkja og/eða nánari lýsingu á tilgangi þeirra. Staðfesting á trausti vottunarslóðar mun ekki byggja á því.	Mælt er með að nota **commonName (CN)** eigindið. Gildi **commonName (CN)** má ekki vera tómur strengur, en er að öðru leiti valfrjást. Í **commonName (CN)** má tilgreina að skilríkið sé rótarskilríki. Vottunarstöðin er bæði áskrifandi rótarskilríkja og vottorðshafi. Vottunarstöðin er einnig útgefandi. Það er valfrjálst að nota **organizationalUnitName (OU)** eigindið til að tilgreina skipulagsheild innan vottunarstöðvar til frekari afmörkunar, eða til að tilgreina tegund skilríkja og/eða nánari lýsingu á tilgangi þeirra. Staðfesting á trausti vottunarslóðar mun ekki byggja á því.	

Svæði	Endaskilríki	Milliskilríki	Rótarskilríki	RFC 3280 [4]
	organizationName (O) er ekki tómt. Það er valfrjálst að nota **EmailAddress (E)** eigindið fyrir netpóstfang vottorðshafa.			
Authority key identifier	Inniheldur tilvísun sem nota má til að bera kennsl á þann dreifilykil vottunarstöðvar sem tengist einkalyklinum sem notaður var til að undirrita viðkomandi skilríki. Oft notað þegar vottunarstöðin hefur marga undirritunarlykla.	Sjá End Entity.	Ekki notað.	4.2.1.1
Subject key identifier	Ekki notað.	Inniheldur tilvísun sem nota má til að bera kennsl á þau skilríki sem innihalda tiltekinn dreifilykil.	Sjá milliskilríki.	4.2.1.2
Key usage	Með vísun í töflu í kafla 5.4.3 í ETSI TS 102 280 [7]: D) Digital Signature, Key Encipherment A) Non-Repudiation Miðað er við að skilríkin byggi á tveimur lyklapörum (e. dual key). Gerð A er eingöngu notuð í tengslum við undirritanir skjala og gagna. Gerð D er notuð til auðkenningar og dulritunar. (Sjá einnig kafla 4.2.1.3 í RFC 3280 [4]).	Certificate Signing, Off-line CRL Signing, CRL Signing (06)	Sjá milliskilríki.	4.2.1.3
Certificate policies	Fylgir kröfum í kafla 4.2.1.5 RFC 3280 [4] og kafla 3.2.3 í RFC 3739 [5]. Skilríki sem fullyrt er að séu fullgild skilríki skulu uppfylla kröfur í ETSI TS 101 862. Nota skal auðkenni viðfangs (Object IDentifier - OID) að minnsta kosti einnar vottunarstefnu sem skilgreinir kröfur til framkvæmdar vottunarstöðvar við útgáfu skilríkjanna. Valfrjálst er að nota viðbótar tilvísanir í vottunarstefnuna, en þess verður að gæta að valfrjálsar tilvísanir breyti ekki skilgreiningum vottunarstefnunnar. Auðkenni vottunarstefnu (OID) skal vera út	Ekki notað.	Ekki notað.	4.2.1.5

Svæði	Endaskilríki	Milliskilríki	Rótarskilríki	RFC 3280 [4]
	frá boga (e. arc) sem tilheyrir Íslandi og úthlutað í samræmi við X.660 [8].			
Subject alternative name	Fylgir kröfum í kafla 4.2.1.7 í RFC 3280 [4]. Notað til að bæta viðbótar auðkenningu við skilríkin. Valfrjálst svæði; ef svæðið er notað má það ekki vera tómt.	Fylgir kröfum í kafla 4.2.1.7 í RFC 3280 [4]. Notað til að bæta viðbótar auðkenningu við skilríkin. Valfrjálst svæði; ef svæðið er notað má það ekki vera tómt.	Ekki notað.	4.2.1.7
Basic constraints	Subject Type=End Entity: **cA=FALSE** Path Length Constraint=None: **pathLenConstraint=***Tómur strengur*	Subject Type=CA: **cA=TRUE** Path Length Constraint=0: **pathLenConstraint=0**	Subject Type=CA: **cA=TRUE** Path Length Constraint=1: **pathLenConstraint=1**	4.2.1.10
Extended key usage	Valfrjálst svæði sem tilgreinir tilgang skilríkjanna; notist eingöngu í endaskilríkjum. Ef sett eru inn eigin gildi þá skulu þau hafa OID sem úthlutað er í samræmi við X.660 [8]. Ef „Key usage" svæðið tilgreinir notkun skilríkjanna fyrir „Non-Repudiation" (gerð A) þá skal ekki nota þetta svæði.	Ekki notað.	Ekki notað.	4.2.1.13
CRL distribution point	Hér skal setja vísanir í afturköllunarlista (CRL) með CRL og/eða LDAP vísunum. Þetta svæði verður að vera til staðar og má ekki vera tómt (sjá kafla 5.1.14 í ETSI TS 102 280[7]) Svæðið skal innihalda að minnsta kosti eina vísun í afturköllunarlista lista (CRL). Að minnsta kosti ein af vísunum skal nota annað hvort HTTP (http://) í samræmi við RFC 2616 [10] eða LDAP (ldap://) í samræmi við RFC 2255 [11].	Sjá End Entity.	Ekki notað.	4.2.1.14
Authority Information Access	Notað til að gefa OCSP biðlara (Online Certificate Status Protocol) til kynna hvar upplýsingar um stöðu skilríkja eru (URI vísun). Þetta svæði skal nota í samræmi við RFC 2560 [12] og kafli 4.2.2.1 í RFC 3280 [4].	Ekki notað.	Ekki notað.	4.2.2.1

Svæði	Endaskilríki	Milliskilríki	Rótarskilríki	RFC 3280 [4]
Qualified certificate statement	Skilríki sem fullyrt er að séu fullgild skilríki skulu uppfylla kröfur í ETSI TS 101 862 [6]. Öll fullgild skilríki sem gefin eru út eftir 30. júní 2005 skulu hafa auðkenni í þessu svæði fyrir vottunarstefnu (OID) sem tilgreinir að skilríkin séu gefin út í samræmi við kröfur til fullgildra skilríkja sem kveðið er á um í lögum um rafrænar undirskriftir [1]. Þar sem sett eru takmörk í vottunarstefnu fyrir útgáfu á fullgildum skilríkjum á fjárupphæð í viðskiptafærslum þá skal tilgreina auðkenni fyrir takmörkun fjárhæðar með OID og tilgreina þá fjárhæð sem upphæðin takmarkast við. Sjá nánar í kafla 5.2.2 í ETSI TS 101 862 [6]. Ef vottunarstöðin fullyrðir að einkalykill fullgildra skilríkja, sem tengist dreifilykli skilríkjanna, sé varðveittur í öruggum undirskriftarbúnaði sem fullnægir skilyrðum sem kveðið er á um í 8. og 9. gr. laga um rafrænar undirskriftir [1] þá skal tilgreina auðkenni fyrir þá fullyrðingu með OID. Auðkenni viðfangs (OID) skulu vera út frá boga (e. arc) sem tilheyrir Íslandi og þeim úthlutað í samræmi við X.660 [8].	Ekki notað.	Ekki notað.	

3.3 Dæmi um notkun svæða

Í eftirfarandi töflum eru dæmi um notkun þeirra svæða í skilríkjum sem skilgreind eru í þessu skjali.

Dæmi um persónutengd skilríki - einkaskilríki og starfsskilríki

Svæði	Notkun (M=Mandatory O=Optional)	Tilgreind gildi	Athugasemdir – forskrift viðmiðana
Issuer	M	**CN = Stjornarrad Islands, vefskilrikjautgafa** **OU = Utgefandi vefskilrikja** **SN = 5501692829** **O = Fjarmalaraduneyti** **C = IS**	**OU** er valfrjálst. Mælt er með að hafa **OU** sem lýsir hlutverki milliskilríkjanna. Nota má eins mörg **OU** og þörf er á.
Subject	M	**CN = Jon Jonsson** **OU = starfsskilriki** **OU = Rafraen skilriki til vefafgreidslu** **SN = 2202705579:5302677559** **O = Fyrirtaeki hf.** **E = jon.jonsson@len.is** **C = IS**	Fyrsta **OU** svæðisins skilgreinir tegund skilríkja. Annað **OU** lýsir hlutverki skilríkjanna. Þar sem ekki er önnur aðgreining í Issuer og Subject svæðunum skal nota þriðja OU. Svæðin Issuer og Subject skulu ekki vera eins í tveimur sklríkjum. Það er valfrjálst að nota eins mörg **OU** og þörf er á. Í eigindinu **O** er nafn áskrifanda **skilríkjanna**. Í einkaskilríkjum er tómur strengur í **O**. **SN** inniheldur kennitölu vottorðshafa og : (tvípunktur) kennitala áskrifanda ef **O** er fyllt út. Engin bil eru leyfð. Tvípunktur kemur aðeins ef **O** er útfyllt. **E** er valfrjálst eigindi.
Key usage	M	**D) Digital Signature, Key Encipherment**	Gert er ráð fyrir að skilríkin innihaldi tvö

Svæði	Notkun (M=Mandatory O=Optional)	Tilgreind gildi	Athugasemdir – forskrift viðmiðana
		A) Non-Repudiation	vottorð, þ.e. séu með tvenn lyklapör (e. dual key). Vottorð af gerð A eru eingöngu notuð í tengslum við undirritanir skjala og gagna. Vottorð af gerð D eru notuð til auðkenningar og dulritunar.
Certificate policies	M	**[1]Certificate Policy:** **Policy Identifier=1.3.6.1.4.1.1513.100.1.1** **[1,1]Policy Qualifier Info:** **Policy Qualifier Id=CPS** **Qualifier:** **https://www.skilriki.is/em** **[1,2]Policy Qualifier Info:** **Policy Qualifier Id=User Notice** **Qualifier:** **Notice Text=This certificate is primarily intended to use in eGovernment in Iceland**	Auðkenni vottunarstefnu (OID) er hér út frá boga (e. arc) sem tilheyrir varnarmálaráðuneyti Bandaríkjanna og er úthlutað til almennra fyrirtækja í samræmi við X.660 [8]. Við framsetningu gagna í svæðinu er mikilvægt að fylgja RFC 3280 kafla 4.2.1.5 [4].
Subject alternative name	O	**Other Name:** **Principal Name=nr1234@fyrirtaeki.is**	Fylgir kröfum í kafla 4.2.1.7 í RFC 3280 [4]. Notað til að bæta viðbótar auðkenningu við skilríkin. Valfrjálst svæði; ef svæðið er notað má það ekki vera tómt.
Basic constraints	M	**Subject Type=End Entity** **Path Length Constraint=None**	Skilgreinir að þessi skilríki séu endaskilríki. Þessi skilgreining tryggir að ekki er hægt að nota skilríkin til að undirrita önnur skilríki.
Extended key usage	O	**Client Authentication (1.3.6.1.5.5.7.3.2)** **Secure Email (1.3.6.1.5.5.7.3.4)** **Encrypting File System (1.3.6.1.4.1.311.10.3.4)** **Smart Card Logon (1.3.6.1.4.1.311.20.2.2)**	Valfrjálst svæði sem er eingöngu notað í endaskilríkjum. Skráð OID vísa á skilgreiningu á notkun skilgríkjanna.

Svæði	Notkun (M=Mandatory O=Optional)	Tilgreind gildi	Athugasemdir – forskrift viðmiðana
CRL distribution points	M	**[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://crl.xxx.com/ FjarmalaraduneytiVefafgreidsluskilriki/LatestCRL.crl**	Svæðið skal að minnsta kosti innihalda eina aðferð til að fletta upp á stöðu skilríkjanna.
Authority Information Access	O	**OCSP;URI:http://ocsp.midlari.is/**	Vísar á OCSP biðlara með URI vísun í upplýsingar um stöðu skilríkjann.

Dæmi um skilríki sem ekki tengjast persónu - búnaðarskilríki og skiplagsheildarskilríki

Svæði	Notkun (M=Mandatory O=Optional)	Tilgreint gildi	Athugasemdir – forskrift viðmiðana
Issuer	M	**CN = Bunadarskilriki** **OU = Utgefandi bunadarskilrikja** **SN = 5501692829** **O = Fjarmalaraduneyti** **C = IS**	**OU** er valfrjálst. Mælt er með að hafa **OU** sem lýsir hlutverki milliskilríkjanna. Nota má eins mörg **OU** og þörf er á.
Subject	M	**CN = Mottaka VSK skyrslna** **OU = bunadarskilriki** **OU = Utgefandi bunadarskilrikja** **SN = 5402696029** **O = Rikisskattstjori** **E = vsk@rsk.is** **C = IS**	**CN** inniheldur hér heiti búnaðarins (hug- eða vélbúnaðar) sem skilríkin votta. Auðkenni búnaðar getur verið IP tala eða lén. Í skipulagsheildarskilríkjum inniheldur **CN** heiti deildar eða fyrirtækis sem vottað er. Fyrsta **OU** svæðisins skilgreinir tegund skilríkja. Annað **OU** lýsir hlutverki skilríkjanna. Það er valfrjálst að nota eins mörg **OU** og þörf er á. Í eigindinu **O** er nafn áskrifanda skilríkjanna, sem er sá aðili sem ber ábyrgð á búnaðinum eða skipulagsheildinni. Í skilríkjum sem tengjast ekki persónu þarf að fylla út **O**. **SN** inniheldur kennitölu vottorðshafa. Engin bil eru leyfð. **E** er valfrjálst eigindi.
Key usage	M	**D) Digital Signature, Key Encipherment** **A) Non-Repudiation**	Gert er ráð fyrir að skilríkin innihaldi tvö vottorð, þ.e. séu með tvenn lyklapör (e. dual key). Vottorð af gerð A eru eingöngu notuð í

Svæði	Notkun (M=Mandatory O=Optional)	Tilgreint gildi	Athugasemdir – forskrift viðmiðana
			tengslum við undirritanir skjala og gagna. Vottorð af gerð D eru notuð til auðkenningar og dulritunar.
Certificate policies	M	**[1]Certificate Policy:** **Policy Identifier=1.3.6.1.4.1.1513.100.1.1** **[1,1]Policy Qualifier Info:** **Policy Qualifier Id=CPS** **Qualifier:** **https://www.skilriki.is/em** **[1,2]Policy Qualifier Info:** **Policy Qualifier Id=User Notice** **Qualifier:** **Notice Text=This certificate is primarily intended to use in eGovernment in Iceland**	Auðkenni vottunarstefnu (OID) er hér út frá boga (e. arc) sem tilheyrir varnarmálaráðuneyti Bandaríkjanna og er úthlutað til almennra fyrirtækja í samræmi við X.660 [8]. Við framsetningu gagna í svæðinu er mikilvægt að fylgja RFC 3280 kafla 4.2.1.5 [4].
Basic constraints	M	**Subject Type=End Entity** **Path Length Constraint=None**	Skilgreinir að þessi skilríki séu endaskilríki. Þessi skilgreining tryggir ekki er hægt að nota skilríkið til að undirrita önnur skilríki.
Extended key usage	O	**Client Authentication (1.3.6.1.5.5.7.3.2)** **Secure Email (1.3.6.1.5.5.7.3.4)** **Encrypting File System (1.3.6.1.4.1.311.10.3.4)** **Smart Card Logon (1.3.6.1.4.1.311.20.2.2)**	Valfrjálst svæði sem er eingöngu notað í endaskilríkjum. Skráð OID vísa á skilgreiningu á notkun skilríkjanna.
CRL distribution points	M	**[1]CRL Distribution Point** **Distribution Point Name:** **Full Name: URL=http://crl.xxx.com/ FjarmalaraduneytiVefafgreidsluskilriki/LatestCRL.crl**	Svæðið skal að minnsta kosti innihalda eina aðferð til að fletta upp á stöðu skilríkjanna.
Authority Information Access	O	**OCSP;URI:http://ocsp.midlari.is/**	Vísar á OCSP biðlara með URI vísun í upplýsingar um stöðu skilríkjanna.

Dæmi um milliskilríki (e. CA certificate)

Svæði	Notkun (M=Mandatory O=Optional)	Tilgreint gildi	Athugasemdir – forskrift viðmiðana
Issuer	M	**CN = Stjornarrad Islands, rotarskilriki** **OU = Rotarskilriki** **SN = 5501692829** **O = Fjarmalaraduneyti** **C = IS**	**CN** inniheldur sýnilegt nafn þeirrar vottunarstöðvar gefur út skilríkin og sem í þessu tilfelli á rótina. Tilgreinir hér jafnframt tegund skilríkjanna. **OU** er valfrjálst. Mælt er með að hafa **OU** sem lýsir hlutverki rótarskilríkjanna. **O** er hér eigandi rótarinnar.
Subject	M	**CN = Stjornarrad Islands, vefskilrikjautgafa** **OU = Utgefandi vefskilrikja** **SN = 5501692829** **O = Fjarmalaraduneyti** **C = IS**	**CN** inniheldur sýnilegt nafn þeirrar vottunarstöðvar sem milliskilríkin eru gefin út fyrir. Tilgreinir hér jafnframt skipulagsheildina vefskilríkjaútgáfa. **OU** er valfrjálst. Mælt er með að nota **OU** til að lýsir hlutverki milliskilríkjanna. **O** er vottunarstöðin sem milliskilríkin eru gefin út fyrir. **SN** inniheldur kennitölu útgefanda Engin bil eru leyfð.
Authority key identifier	O	**KeyID=42 e3 01 99 8e 1e 74 f6 4d ad b0 ed 4e 25 06 c8 da 91 bb b2**	Authority key identifier auðkenni er notað af ýmsum hugbúnaði til að finna næsta dreifilykil (skilríki) fyrir ofan í skilríkjakeðjunni. Nánari lýsingu á gildi svæðisins er að finna í RFC 3280 kafla 4.2.1.1 [4].
Subject key identifier	O	**f0 19 2c 2a 0a de 3f c9 55 36 60 16 b2 d6 cf 71 8f 90 a0 eb**	Subject key identifier auðkenni er notað af ýmsum hugbúnaði til að finna skilríki sem innihalda tiltekinn dreifilykil, í þessu tilfelli skilríki sem milliskilríkið hefur gefið út

Svæði	Notkun (M=Mandatory O=Optional)	Tilgreint gildi	Athugasemdir – forskrift viðmiðana
			(þ.e. skilríki sem eru einu stigi neðar í skilríkja keðjunni). Sjá nánar í RFC 3280 kafla 4.2.1.2 [4].
Key usage	M	**Certificate Signing, Off-line CRL Signing, CRL Signing (06)**	Skilgreinir að skilríkin eru notuð til að gefa út skilríki og undirrita afturköllunarlista. Sjá ETSI TS 102 280 [7].
Subject alternative name	O	**Directory Address:** **CN=PrivateLabel2-119**	Notað í milliskilríkjum til að geyma innri tilvísanir sem útgefandi skilríkjanna vill koma að í skilríkjunum, t.d. netföng, IP tölur, Lén eða innri tilvísanir. Sjá ETSI TS 102 280 kafla 5.4.7 [7] og RFC 3280 kafla 4.2.1.7 [4].
Basic constraints	M	**Subject Type=CA** **Path Length Constraint=0**	Skilgreinir að skilríkið er gefið út sem milliskilríki (CA). Þetta svæði verður að vera í millskilríkjum.
CRL distribution points	M	**[1]CRL Distribution Point** **Distribution Point Name:** **Full Name:** **URL=http://crl.xxx.com/offlineca/FjarmalaraduneytiStjornarradIslandsrotarskilriki.crl**	Hér er vísun í afturköllunarlista (CRL) með URL.

Dæmi um rótarskilríki (e. root certificate)

Svæði	Notkun (M=Mandatory O=Optional)	Tilgreint gildi	Athugasemdir – forskrift viðmiðana
Issuer	M	**CN = Stjornarrad Islands, rotarskilriki** **OU = Rotarskilriki (valfrjálst)** **SN = 5501692829** **O = Fjarmalaraduneyti** **C = IS**	**CN** inniheldur sýnilegt nafn eiganda rótarinnar út á við. Mælt er með að hafa **OU** sem lýsir hlutverki rótarskilríkisins. **O** er hér eigandi rótarinnar
Subject	M	**CN = Stjornarrad Islands, rotarskilriki** **OU = Rotarskilriki (valfrjálst)** **SN = 5501692829** **O = Fjarmalaraduneyti** **C = IS**	Þar sem um rót er að ræða er skilríkið undirritað af sjálfu sér (e. self-signed).
Subject key identifier	O	**f0 19 2c 2a 0a de 3f c9 55 36 60 16 b2 d6 cf 71 8f 90 a0 eb**	Subject key identifier auðkenni er notað af ýmsum hugbúnaði til að finna skilríki sem innihalda tiltekinn dreifilykil, í þessu tilfelli skilríki sem hafa verið undirrituð af rótarlyklinum (þ.e. skilríki sem eru einu stigi neðar í skilríkja keðjunni). Sjá nánar í RFC 3280 kafla 4.2.1.2 [4].
Key usage	M	**Certificate Signing, Off-line CRL Signing, CRL Signing (06)**	Skilgreinir að rótin er eingöngu notuð til að gefa út skilríki og undirrita afturköllunarlista. Sjá ETSI TS 102 280 [7].
Basic constraints	M	**Subject Type=CA** **Path Length Constraint=1**	Þarf að skilgreina þannig að hugbúnaður viti að þetta sé CA.