Almenn útbreiðsla rafrænna skilríkja

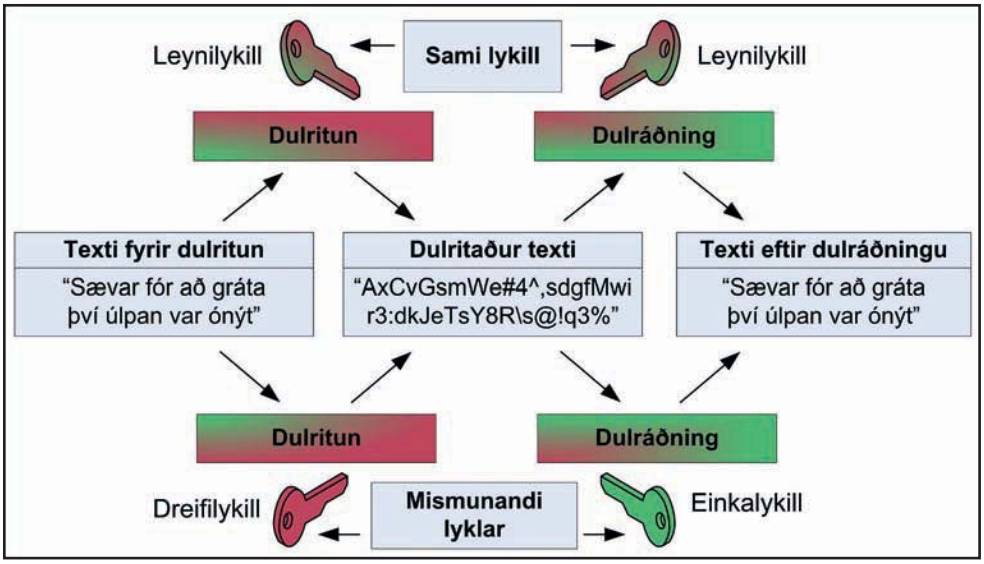
Um nokkurt skeið hafa Samtök banka og verðbréfafyrirtækja (SBV) og fjármálaráðuneytið (FJR) unnið saman að mótun almenns dreifilyklaskipulags á Íslandi. Í samstarfinu er lögð áhersla á almenna útbreiðslu og notkun rafrænna skilríkja til auðkenningar og undirskrifta. Markmiðið er að byggja upp gagnsætt grunnkerfi til afnota fyrir alla sem bjóða almenningi og fyrirtækjum þjónustu. Tilgangurinn er jafnframt að skapa forsendur fyrir trausti við rafræn samskipti á Íslandi og í alþjóðlegu umhverfi. Stefnt er að því að dreifing rafrænna skilríkja á snjallkortum til almennings og lögaðila hefjist árið 2007. Með rafrænu skilríkjunum geta aðilar undirritað skjöl og skuldbindingar með rafrænum hætti og munu spara tíma og fjármuni. Því fleiri rafrænar þjónustur sem nýta skilríkin þeim mun auðveldara verður líf einstaklinga og starfsmanna fyrirtækja. Gulu miðarnir með aðgangsorðum munu hverfa því með einni auðkenningu opnast flestar dyr í rafrænum heimum.

Í greininni verður fjallað um notkun rafrænna skilríkja og skýrðir tæknilegir þættir sem varða skilríkin og beitingu þeirra. Þá er samstarfsverkefni ríkis og banka í uppbyggingu á almennri notkun rafrænna skilríkja á Íslandi kynnt stuttlega.

Dreifilyklaskipulag

Allt frá tímum Rómverja hafa menn leitað tæknilegra leiða til að leyna viðkvæmum upplýsingum fyrir þeim sem ekki eiga að hafa aðgang að þeim. Ein leið er sú að aðilar sem eiga að hafa aðgang að upplýsingunum eigi sameiginlegt leyndarmál sem aðrir vita ekki um. Slíkt leyndarmál er þá nokkurs konar leynilykill að upplýsingunum. Gögnin eru dulrituð þannig að einungis er hægt að opna þau með leynilyklinum. Sá sem dulritar gögnin og allir sem þurfa að dulráða gögnin verða að varðveita leynilykilinn með öruggum hætti. Ef þörf er á því að vernda önnur gögn fyrir öðrum aðilum þá þarf til þess annan leynilykil sem miðlað er til réttra aðila. Þetta kallast samhverf dulritun.

Leynilyklaskipulag sem þetta getur hentað vel þegar um fáa aðila er að ræða, en verður fljótt óviðráðanlegt þegar handhöfum lykla fjölgar því að allir aðilar þurfa að varðveita leynilykla allra annarra sem þeir eiga samskipti við. Traust í slíku skipulagi er því byggt á veikum grunni þar sem leynilyklum er dreift milli allra og verndun þeirra á ábyrgð margra. Dæmi um slíka leynilykla er aðgangsorð í innskráningu á tölvukerfi.



Mynd 1: Munur á dulritun með leynilykli og vensluðu lyklapari.

Ein leið til að auðvelda verndun leynilykla felst í því að búa til tvo dulmálslykla sem eru tengdir á stærðfræðilegan hátt. Öðrum lyklinum, einkalykli, er haldið leyndum hjá eiganda sínum en öllum veitt aðgengi að öðrum lykli sem kallast dreifilykill. Skipulagið kallast dreifilyklaskipulag og dulritun með lyklaparinu er ósamhverf dulritun.

Hugmyndin að dreifilyklaskipulagi er einnig gömul en fyrst um miðjan 8. áratuginn voru

**Haraldur A. Bjarnason, sérfræðingur hjá fjármálaráðuneytinu.
Ragnar T. Jónasson, sérfræðingur hjá Landsbanka Íslands og fulltrúi starfshóps Auðkennis um dreifilyklaskipulag.
Arnaldur F. Axfjörð, ráðgjafi hjá Admon og verkefnisstjóri í samstarfi Samtaka banka og verðbréfafyrirtækja og fjármálaráðuneytisins.**

einnig gömul en fyrst um miðjan 8. áratuginn voru sett fram algrím sem gerðu dreifilyklaðulritun að fýsilegum kosti. Lyklarnir eru smíðaðir þannig að þótt annar lykillinn sé þekktur er ekki hægt að nýta þá vitneskju til að útfæra eða finna hinn lykilinn. Gögn sem dulrituð eru með öðrum lyklinum er einungis hægt að opna með hinum lyklinum. Lykillinn sem gögnin voru dulrituð með gagnast því ekki til þess að endurheimta gögnin. Mynd 1 sýnir á einfaldan hátt muninn á leynilykla- og dreifilyklaskipulagi.
Dreifilyklaskipulag byggist á rafrænum skilríkjum, dulritunartækni og vottunarþjónustu sem gefur út skilríki. Um það gilda jafnframt samræmdar kröfur og skilgreiningar.

Rafræn skilríki
Með tilkomu dreifilyklaskipulags er mögulegt að tengja gögn sem hafa verið sannprófuð af óháðum ytri aðila við tiltekinn einstakling og staðfesta rafrænt hver hann er. Rafræn skilríki innihalda dreifilykil viðkomandi einstaklings ásamt öðrum gögnum og eru undirrituð með einkalykli vottunarstöðvarinnar sem gefur út skilríkin. Þannig getur þjónustuveitandi staðfest auðkenningu eða rafræna undirritun einstaklings en forsenda slíkrar staðfestingar er að þjónustuveitandi treysti útgefanda skilríkjanna. Traust til útgefanda byggist aftur á móti á trausti til þess aðila sem gaf út milliskilríki hans. Þannig myndast slóð vottunar allt að svokölluðu traustsakkeri. Ef mikið er í húfi þá getur sá sem treystir á skilríkin rakið þessa slóð og staðfest að allir aðilar séu traustsins verðir. Á mynd 2 er sýnt dæmi um vottunarslóð.

Vottunarslóð myndar þannig keðju skilríkja, frá endaskilríkjum til eins eða fleiri milliskilríkja (eða útgáfuskilríkja) allt að traustsakkeri. Traustsakkeri getur verið rót skilríkjaútgáfu eða milliskilríki sem gefin eru út undir tiltekinni rót.

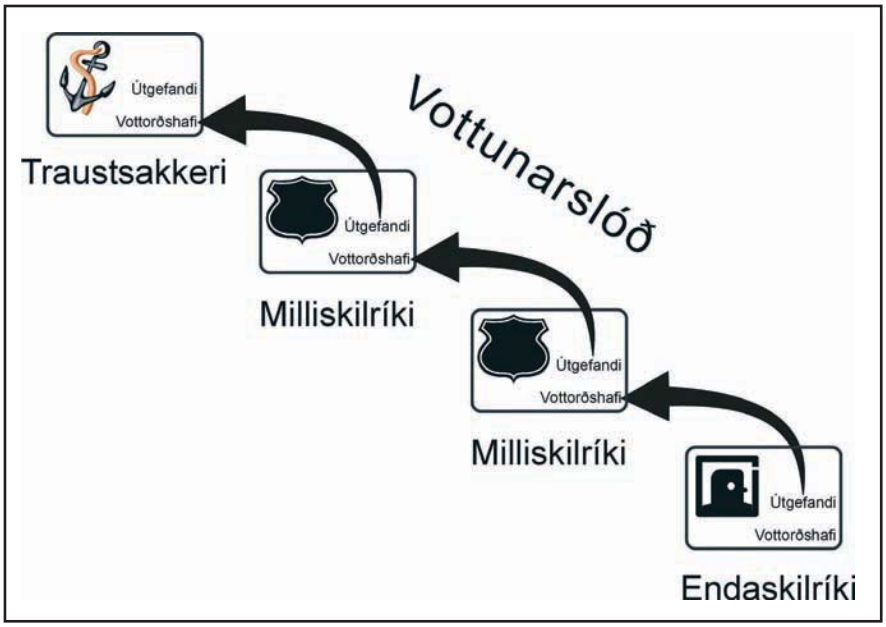
Rafræn skilríki eru útfærð sem stafrænn strengur sem er undirritaður með einkalykli vottunarstöðvar. Innihald skilríkja er skilgreint í alþjóðlega staðlinum ISO/IEC 9594-8, sem samsvarar ITU-T tilmælum X.509 fyrir skilríki af útgáfu 3 (venjulega tilgreint sem „X.509 v3 skilríki"). Fyrir undirritun vottunarstöðvar eru gögnin í skilríkjunum kóðuð með svokölluðum ASN.1 DER kóðunarreglum samkvæmt ITU-T tilmælum X.690. Mynd 3 sýnir svæði í X.509 v3 skilríkjum.

Rafrænar undirskriftir
Rafræn undirskrift er dæmi um tengingu rafrænna upplýsinga við tiltekinn einstakling. Undirskriftin er framkvæmd með tiltölulega einfaldri stærðfræðilegri aðgerð í eftirfarandi skrefum:
1. Rafræn gögn til undirritunar eru birt notanda en slík birting er forsenda þess að aðgerðin geti talist lagalega bindandi.
2. Rafrænu gögnin eru tætt (e. hash) með einkvæmri stærðfræðilegri aðgerð sem minnkar þau niður í viðráðanlegan streng af tiltekinni lengd. Þessi strengur kallast tætigildi.
3. Framkvæmd er dulritun á strengnum með einkalykli sem varðveittur er í skilríkjunum og verður þá til undirskriftarstrengur.

Á mynd 4 eru sýndar aðgerðir við undirritun skjals með rafrænum skilríkjum.

Rafræn undirritun gagna í dreifilyklaskipulagi hefur marga kosti. Hægt er að sannreyna hver hefur undirritað gögnin og skuldbundið sig samkvæmt þeim. Einnig er mögulegt að staðfesta heilleika (e. integrity) gagna, þ.e. að þeim hafi ekki verið breytt né þau skemmst frá undirritun. Þá má tryggja að uppruni þeirra og efnislegt innihald sé ekki hrekjanlegt, það er staðfesta óhrekjanleika (e. non-repudiation) þeirra.
Staðfesting á rafrænni undirskrift
Forsenda þess að þjónustuveitandi geti sannprófað rafræna undirskrift er sem fyrr segir að hann treysti útgefanda skilríkjanna og staðfesti gildi þeirra. Staðfestingin er framkvæmd í eftirfarandi skrefum:
1. Þjónustuveitandi kannar skilríkjakeðjuna og staðfestir traust á henni.
2. Þjónustuveitandi staðfestir gildi skilríkjanna.
3. Þjónustuveitandi tekur upprunalegan texta, tætir hann með sömu einkvæmu stærðfræðilegu aðgerðinni (t.d. SHA) og undirritandinn og fær þá streng af tiltekinni lengd (tætigildi).
4. Þjónustuveitandi tekur undirskriftina, dulræður hana með dreifilykli úr skilríkjum undirritanda og fær þá nýjan streng.
5. Þjónustuveitandi tekur þessa tvo strengi og ber þá saman.

Ef samanburðurinn leiðir í ljós að strengirnir eru eins staðfestir það að undirritandi undirritaði sannanlega gögnin og að gögnunum hefur ekki verið



Mynd 2: Dæmi um vottunarslóð.

breytt frá því að þau voru undirrituð. Þetta er sýnt á mynd 4.

Skilríki á snjallkortum

Einkalykil notanda er hægt að varðveita í rafrænum skilríkjum á marga vegu. Í svokölluðum mjúkum skilríkjum er einkalykillinn varðveittur sem tölvuskrá á tölvu notandans. Þegar einkalykillinn er varðveittur á hörðum miðli þá er talað um hörð skilríki. Dæmi um harða miðla eru USB-tókar, SIM símakort og snjallkort. Vandasamt getur verið að tryggja örugga varðveislu á einkalyklum á einmenningstölvum notenda en hins vegar er auðveldara að útfæra einkalykla á hörðum miðlum þannig að verndun þeirra sé ásættanleg. Það gildir t.d. um rafræn skilríki á snjallkortum.

Útfærsla skilríkja á snjallkortum byggist bæði á vélbúnaði (kortinu og lesara) og hugbúnaði notanda (reklum fyrir snjallkort og lesara og undirskriftarbúnaði). Til að hægt sé að beita skilríkjum á snjallkortum þarf notandinn því að hafa bæði hug- og vélbúnað uppsettan á tölvu sinni. Á mynd 5 kemur fram hvaða staðlar og viðmið eru í samskiptum milli snjallkorta og vefþjóna, í gegnum lesara, rekil og vafra.

Útbreiðsla snjallkortalesara hefur fram að þessu verið takmörkuð en á síðustu misserum hefur orðið bylting í þessum málum og nú orðið eru fartölvur frá fjölmörgum framleiðendum með innbyggða kortalesara. Nýlegar tölur frá innflytjendum fartölva á Íslandi benda til þess að nokkur þúsund tölvur hér á landi séu með innbyggða lesara. Auk þess eru fáanlegir ódýrir lesarar sem tengdir eru með USB-tengi. Að öllum líkindum verður þróunin hröð á næstu mánuðum, eins og reyndin var með USB-tengi fyrir nokkrum árum.

Nú eru snjallkortaframleiðendur fjölmargir og misjafnt er hvernig kortin og skipanasett fyrir þau eru uppbyggð. Tæknin er ung og viðmiðunarstaðlar enn í þróun. Margir framleiðendur byggja þó á tæknilegum stöðlum eins og ISO 7816 seríunni.

Stjórnvöld og kortaframleiðendur í Evrópu hafa síðustu misseri gert átak í þessum efnum, m.a. unnið að stöðlun korta og hugbúnaðar tengdum þeim. Mest munar þar um European Citizen Card kortastaðalinn (ECC), nánar tiltekið IAS-hluta hans, og ISO 24727 staðalinn fyrir millibúnað (e. middleware). IAS stendur fyrir auðkenningu (e. identification), sannvottun (e. authentication) og undirskrift (e. signature). Stefnt er að því að öll kort sem byggjast á ECC IAS staðlinum geti átt samskipti við hvers konar hugbúnað sem er samhæfður ISO 24727.

Þótt enn liggi ekki fyrir staðfesting frá stærstu hugbúnaðarframleiðendum um stuðning við ISO 24727 í stýrikerfum eins og Windows eða MacOS má telja fullvíst að hann verði kominn á árið 2007. Bæði Windows og MacOS styðja nú þegar kort frá flestum framleiðendum sem eru leiðandi í mótun þessara staðla og munu líklegast fylgja þróun þeirra á kortum.

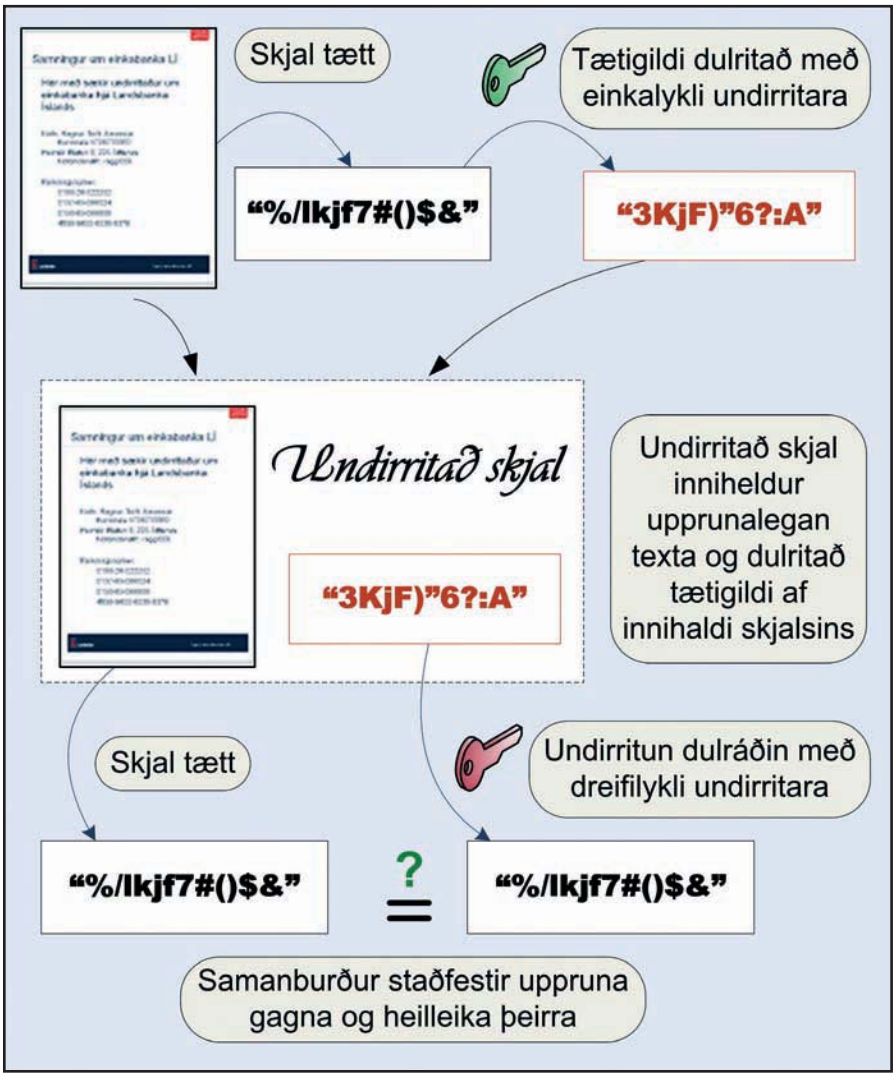
Snjallkort eru auðveld og þægileg í notkun. Þegar notandi er á vefsíðu sem krefur hann um skilríki stingur hann snjallkortinu í lesarann, velur skilríkin í glugga sem opnast og slær inn PIN-númer sem opnar aðgang að einkalyklinum. Auðkenning eða undirskrift er framkvæmd með lyklinum á kortinu og því engin hætta á því að tölvuþrjótur geti náð lyklinum og falsað slíka vottun.

Stilling vefþjóna fyrir auðkenningu

Tiltölulega einfalt er að stilla vefþjóna þannig að þeir krefjist sannvottunar með rafrænum skilríkjum. Í Apache er bætt við fáeinum línum og enn einfaldara er að stilla Microsoft IIS eins og sjá má á mynd 6.

Vefþjónninn þarf auk þess að þekkja skilríkjakeðjur sem hann treystir og því þarf að skrá þær sérstaklega.

Rafræn skilríki geta meðal annars innihaldið kennitölu. Hægt er að nýta hvers konar forritakóða til að lesa kennitöluna úr skilríkjunum og nýta til að stýra aðgangi notanda. Á mynd 7 er dæmi um .ASP-kóða á einfaldri vefsíðu sem les kennitölu úr skilríkjum útgefnum af fjármálaráðuneytinu og birtir á skjá.



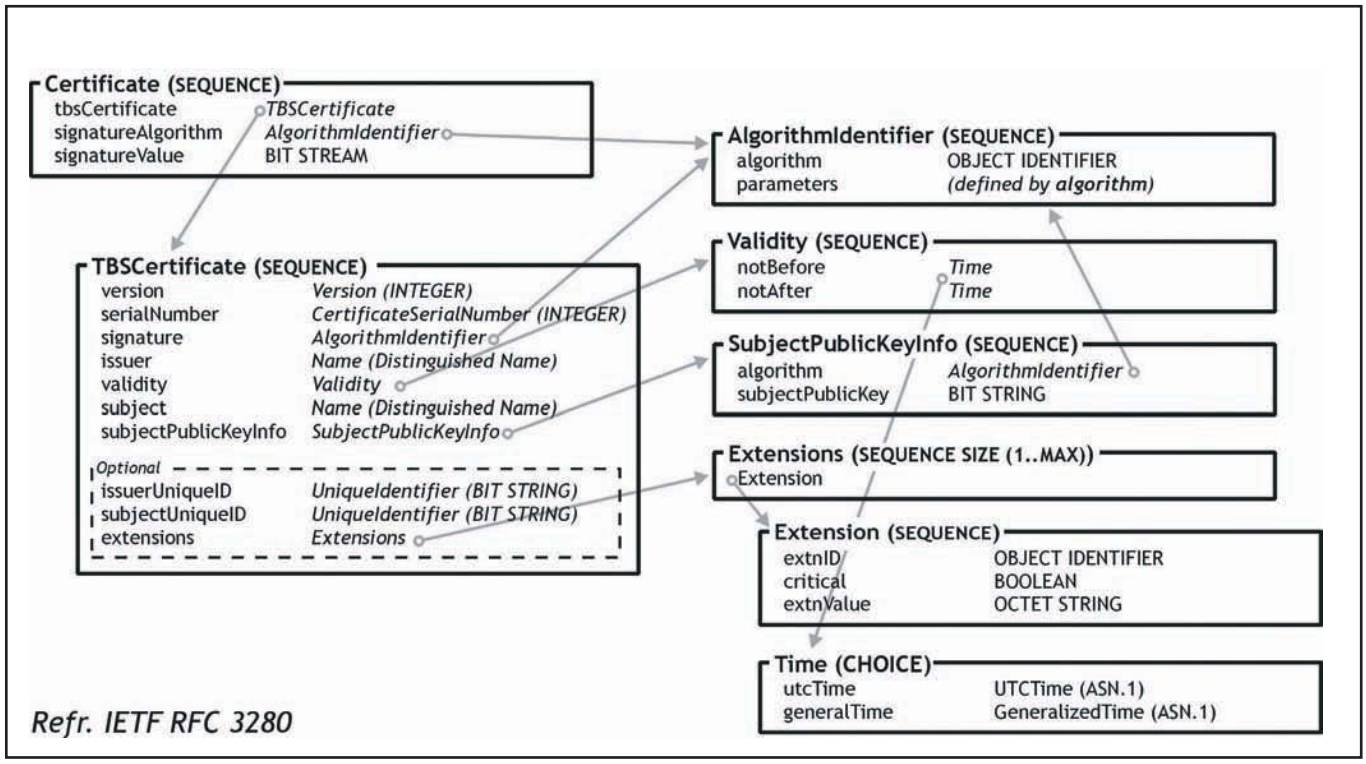
Mynd 4: Undirritun skjals með rafrænum skilríkjum og staðfesting á uppruna og heilleika skjalsins.

Mikilvægi rafrænna skilríkja

Rafræn skilríki nýtast á marga vegu, t.d. til að:

- Sannvotta og auðkenna sig gagnvart fyrirtækjum, stofnunum og einstaklingum.
- Undirrita umsóknir, skuldbindingar, skjöl og tölvupóst.
- Skrifa undir millifærslur í netbönkum.
- Samþykkja rafræn skjöl og reikninga (rafrænt samþykktarferli).
- Tryggja öryggi í fjarvinnu og um þráðlaus tölvunet.
- Tryggja öryggi tölvupósts.
- Dulrita samskipti.

Opinberir aðilar stefna að bættri þjónustu við almenning og fyrirtæki með því að gera þjónustu sem nú krefst auðkenningar aðila í eigin persónu, og jafnvel undirskriftar, sjálfvirka og aðgengilega yfir opin tölvunet. Þessar breytingar bæta verulega aðgengi að stjórnsýslu og spara almenningi og fyrirtækjum fjármuni og tíma. Íslenska ríkið notar rafræn skilríki nú þegar, svo sem við afgreiðslu tollskýrslna og við rafræn skil endurskoðenda og bókara á skattskýrslum. Skattframtöl frá atvinnumönnum hafa verið rafrænt undirrituð og dulrituð undanfarin níu ár, og er nú um 100.000 slíkum skilað árlega. Bankar og sparisjóðir hafa einnig unnið að innleiðingu dreifilyklaskipulags í sinni starfsemi. Þar hafa verkefni sem krefjast



Mynd 3: Innihald X.509 v3 skilríkja.

rafrænnar undirskriftar á millifærslum verið rekin um árabil. Af þessu má sjá að talsverð reynsla og þekking í þessum efnum hefur þegar safnast bæði hjá ríki og bönkum. Ljóst er að atvinnulífið í heild getur nýtt sér rafræn skilríki á ýmsan hátt og þannig bætt þjónustu við viðskiptavini sína.

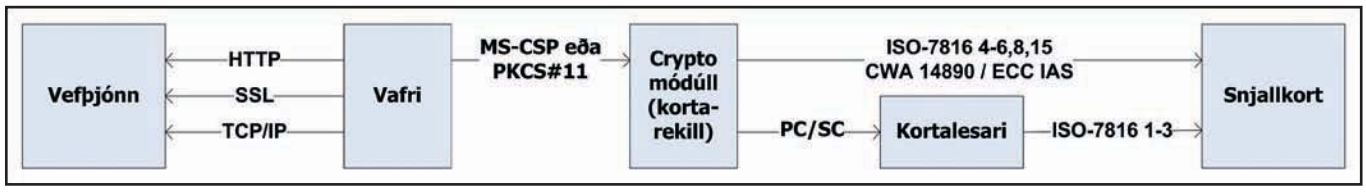
Skilríki eru ekki eingöngu notuð í viðskiptalegum tilgangi eða í samskiptum við opinbera aðila. Sem dæmi um aðra notkun má nefna að í nágrannalöndunum hefur verið komið upp öruggum spjallrásum þar sem notkun rafrænna skilríkja minnkar verulega líkurnar á að fólk geti villt á sér heimildir. Þetta er sérstaklega mikilvægt til að tryggja öryggi barna á Internetinu.

Samstarf um Íslandsrót

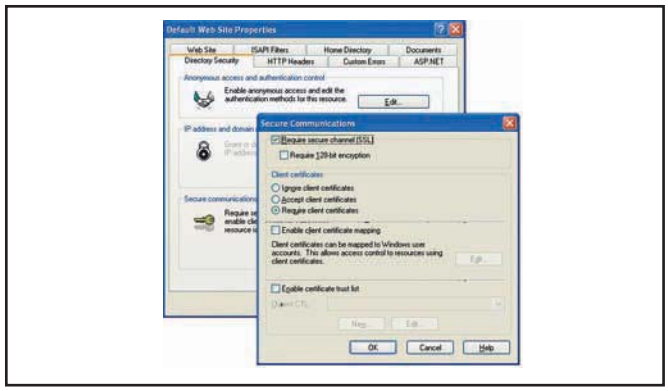
Markmið íslenska ríkisins er að koma upp vottunarrót fyrir Ísland, Íslandsrót, í þeim tilgangi að skapa sameiginlegt traust í dreifilyklaskipulagi fyrir íslenskt atvinnulíf og hið opinbera. Lögð er áhersla á trausta rót sem uppfyllir kröfur um útgáfu rafrænna skilríkja fyrir íslenskt samfélag. Jafnframt verður þess gætt að útgáfa rafrænna skilríkja undir Íslandsrót hlíti kröfum viðurkenndra staðla um rafræn skilríki í öðrum Evrópulöndum.

Mynd 8 sýnir framsetningu í Windows-umhverfi á skilríkjum sem gefin eru út af núverandi rót ríkisins en áætlað er að Íslandsrót sinni þeim þörfum sem þar er sinnt nú.

Ríkið hefur frumkvæði að því, í tengslum við evrópskt og alþjóðlegt samstarf, að Íslandsrót komist í alþjóðlega dreifingu (e. federation) þar sem það á við. Í því felst að skilríkin þekkist og njóti viðeigandi trausts. Unnið er að



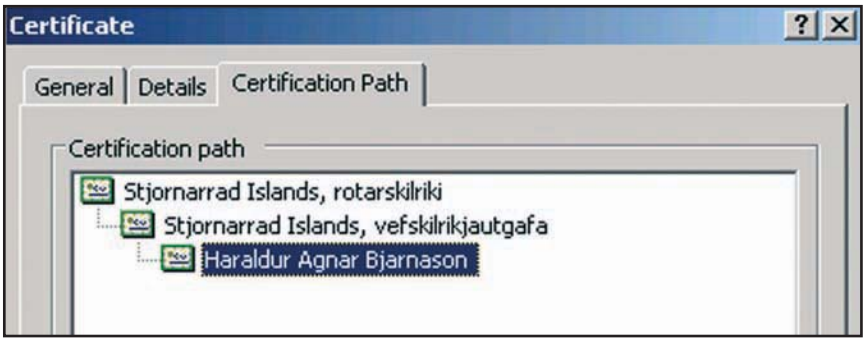
Mynd 5: Staðlar og viðmið í samskiptum milli snjallkorts og vefþjóns.



Mynd 6: Stillingar í Microsoft IIS netþjóni til að krefjast sannvottunar með skilríkjum.

```
<%@ Language=VBScript %>
<html>
<title>Skilríki - Demo</title>
<body>
<h3>Sækja kennitölu úr skilríki</h3>
<%
If Len(Request.ClientCertificate("Subject")) = 0 Then
  Response.Write("Ekkert skilríki fannst")
else
  'Sækja kennitölu úr subject
  pos = InStr(Request.ClientCertificate("Subject"), "OU = ID - ")
  kt = Mid(Request.ClientCertificate("Subject"),pos+11,10)
  Response.Write("<br/><b>Kennitala:</b><br/>")
  Response.Write(kt)
  Response.write("<br/>")
End if
%>
</body>
</html>
```

Mynd 7: Dæmi um einfaldan .ASP-kóða sem les kennitölu úr skilríki og birtir á skjá.



Mynd 8. Vottunarslóð á rafrænu skilríki undir núverandi rót ríkisins

skilgreiningu á kröfum fyrir Íslandsrót sem lagðar verða til grundvallar stefnu rótarinnar.

Tækninefnd um dreifilyklaskipulag

Stofnuð hefur verið tækninefnd undir Fagstaðlaráði í upplýsingatækni (FUT) hjá Staðlaráði Íslands. Tækninefndin verður óháður vettvangur fyrir hagsmunaðila rafrænna skilríkja á Íslandi.

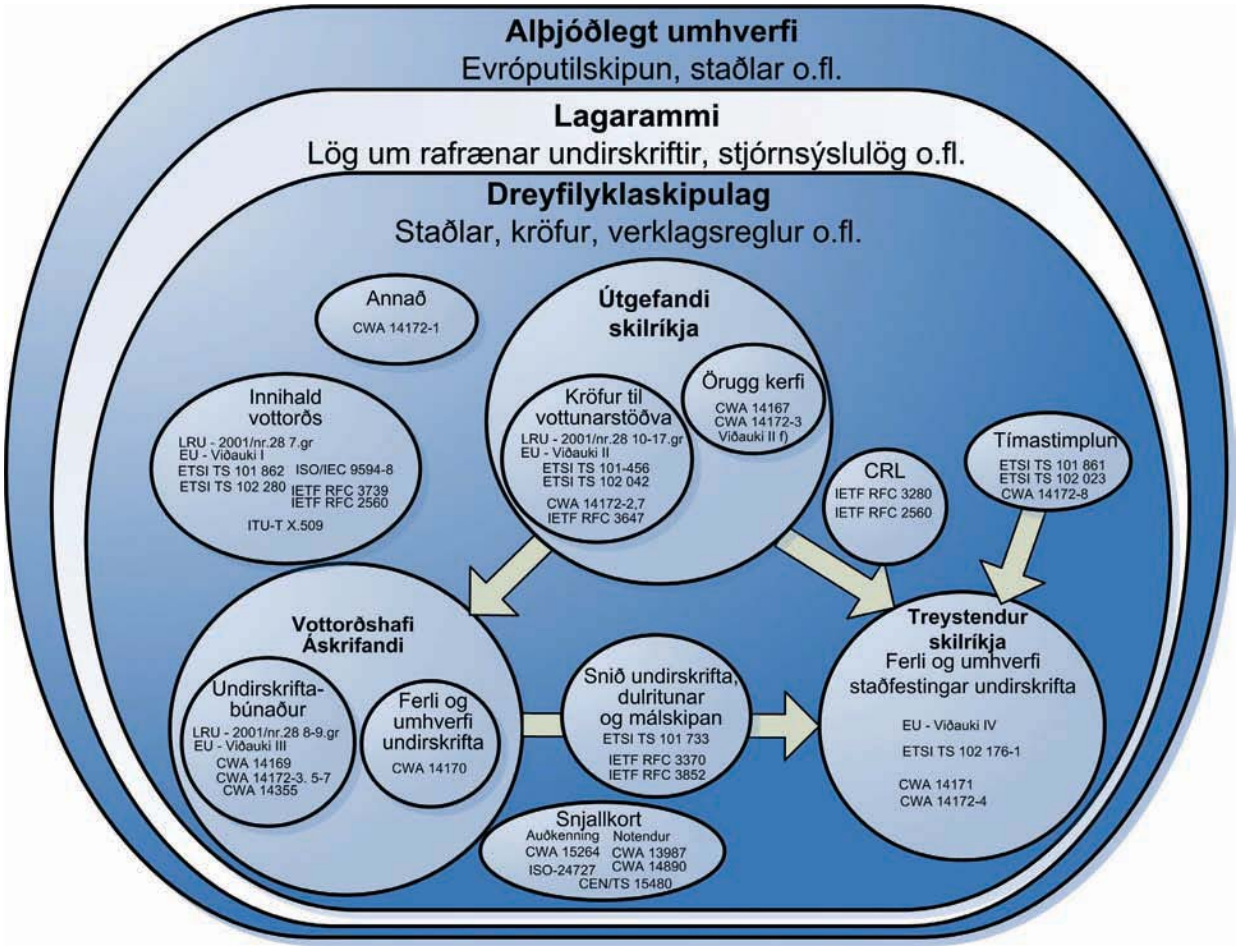
Mynd 9 sýnir umhverfi rafrænna skilríkja á Íslandi í þremur lögum. Ysta lagið markast af alþjóðlega umhverfinu þar sem staðlar og reglugerðir eru í gildi, m.a. tilskipanir Evrópuráðsins. Í öðru lagi markast umhverfið af innlendum lagaramma þar sem lög um rafrænar undirskriftir vega þyngst. Innan þess er þriðja lagið, dreifilyklaskipulag, þar sem útbúnar eru íslenskar kröfur og verklagsreglur byggðar á alþjóðlegum stöðlum og viðmiðunum og innlendum lögum. Starf tækninefndarinnar er að ná sátt um útfærslu á uppbyggingu íslenska umhverfisins. Tækninefndin verður vettvangur þar sem allir áhugasamir fá tækifæri til að koma skoðunum sínum og athugasemdum á framfæri.

Lokaorð

Veigamikill þáttur í því að neytendur treysti skilríkjum og sjái sér hag í að nýta þau í samskiptum við ríki og banka er að atvinnulífið í heild taki þátt í uppbyggingu kerfisins með hvers kyns þjónustu sem byggist á skilríkjunum. Þá þarf að sjá til þess að góð sátt sé um umhverfi rafrænna skilríkja og skilgreiningar á dreifilyklaskipulagi fyrir íslenskt atvinnulíf og almenning. Þess vegna hafa bankar og ríki lagt áherslu á opnar skilgreiningar á dreifilyklaskipulagi og á tæknilegum þáttum sem skipta máli fyrir samvirkni. Samtök banka og verðbréfafyrirtækja og fjármálaráðuneytið hafa sett fram eftirfarandi áherslur í samstarfsverkefninu:

- Samræma, eins og kostur er, notkun rafrænna skilríkja í lausnum sem boðnar eru.
- Einfalda grunngerð sem notendur og lausnaraðilar þurfa að byggja á.
- Fjarlægja tæknilegar og viðskiptalegar hindranir á útbreiðslu rafrænna skilríkja.

Almenn útbreiðsla rafrænna skilríkja mun fela í sér byltingu í samskiptum á Netinu. Með þeim mun skapast traust þar sem notendur munu með öruggum hætti geta auðkennt sig gagnvart öðrum og skrifað rafrænt undir skjöl og skuldbindingar. Samhliða almennri útbreiðslu mun framboð á rafrænni þjónustu margfaldast sem skilar sér í auknu hagræði fyrir þjónustuveitendur, fyrirtæki og almenning.



Mynd 9. Umhverfi rafrænna skilríkja á Íslandi.