Nefndarálit

Öryggisstefna fyrir rafræna stjórnsýslu á Íslandi.

Tillaga um aðgerðir til að hrinda dreifilyklastefnu í framkvæmd.

Nefnd um skipulag dreifilykla í rafrænum viðskiptum
Nóvember 2001

Efni skýrslu

1. Samantekt 3

2. Inngangur 6

3. Greining KPMG 7

4. Norðurlönd 10

5. Tillögur og ályktanir nefndarinnar 12

6. Ákvörðunaratriði við útfærslu dreifilyklaskipulags 17

Viðaukar

1. Erindisbréf nefndarinnar 20

2. Dreifilyklaskipulag – Nokkur meginhugtök og grundvallaratriði 21
(úr athugasemdum við frumvarp til laga um rafrænar undirskriftir 2001)

3. Kröfur vegna rafrænna kennsla, vottunar og undirskrifta 24
– lausleg íslensk þýðing á viðaukum A og B úr útboði sænska ríkisins haustið 2001.

4. Samanburður á formi vottorða í Noregi og Svíþjóð 35

5. Orðaskýringar 40

6. Helstu heimildir 41

Fylgiskjal

Skýrsla KPMG, maí 2001

Samantekt

1.1. Inngangur

Ein helsta forsenda fyrir útbreiðslu rafrænnar stjórnsýslu er sú að rafræn málsmeðferð njóti sama trausts og hin hefðbundna. Því á að mega treysta að öryggi, trúnaður og festa við meðferð mála séu sambærileg óháð því hvaða aðferð er notuð.

Rafrænar undirskriftir byggðar á dreifilyklaskipulagi munu verða þýðingarmikill þáttur í því að byggja upp slíkt traust. Með tilkomu laga um rafrænar undirskriftir, nr. 28/2001, og væntanlegri endurskoðun stjórnsýslulaga er lagður grundvöllur að rafrænni stjórnsýslu samhliða hefðbundnum aðferðum. Stefna ber að því að allir landsmenn geti á komandi árum aflað sér skilríkja og annars búnaðar til fullgildra rafrænna undirskrifta og dulritunar með viðunandi kjörum.

Þróun tæknilausna fyrir rafrænar undirskriftir og búnað til stuðnings við dreifilyklakerfi er afar hröð samhliða því sem markaðssetning þeirra er öflug. Í ljósi þess hve tæknin þróast ört, og þegar ennfremur er litið til þess að útbreiðsla til almennings mun taka nokkurn tíma, virðist ekki ráðlegt að velja nú þegar og kaupa fyrir alla landsmenn einhverja háþróaða tæknilega lausn, til dæmis byggða á gjörvakortum. Álitlegra virðist til skamms tíma að taka í notkun einfaldari lausnir sem geta tryggt fullnægjandi öryggi við marga þætti í rafrænni opinberri þjónustu. Sömu eða hliðstæðar lausnir myndu nýtast við rafræn viðskipti af ýmsu tagi.

Þessi skoðun nefndarinnar er meðal annars byggð á nær samhljóða áliti sérfræðinga norrænna stjórnvalda eins og lesa má í tilvitnuðum skjölum.

1.2. Meginatriði öryggisstefnu til langs tíma

1. – Útbreiðsla – almenn notkun
Stefna ber að því að notkun rafrænna skilríkja verði almenn og útbreidd. Þegar litið er til reynslu annarra þjóða af notkun gjörvakorta í samskiptum hins opinbera og almennings, þar sem ætlast er til að einstaklingar kaupi þau, er skemmst frá því að segja að margar slíkar tilraunir hafa misheppnast. Ætla má að þröskuldar séu í veginum bæði hvað varðar verð og fyrirhöfn. Undan því verður þó ekki skotist að háu öryggisstigi hlýtur að fylgja visst umstang tengt því að bera kennsl á menn með viðhlítandi hætti og koma skilríkjum í réttar hendur. Leita þarf nýstárlegra leiða til að örva notkun og útbreiðslu rafrænna undirskrifta meðal almennings og í atvinnulífinu.

2. – Markaðslausnir – virk samkeppni. Fjölhæf rafræn skilríki.
Stefna ber að því að almenningur geti notað rafræn skilríki sín í samskiptum við ríkið án tillits til þess hver gaf þau út, svo framarlega sem þau uppfylla sett skilyrði. Þetta verði tryggt með því að setja fram kröfur um innihald og form vottorða og reglur um meðferð þeirra, sem uppfylla þurfi til þess að þau verði tekin gild í samskiptum við opinberar stofnanir. Kröfurnar eigi sér stoð í evrópskum og alþjóðlegum stöðlum og teknar verði til fyrirmyndar þær kröfur

sem aðrar norrænar þjóðir gera, t.d. Svíar.[1] Kröfurnar má setja fram annað hvort í rammasamningum eða reglugerð, sem þyrfti þá að eiga sér stoð í lögum.

3. – Viðeigandi öryggisstig, viðunandi kostnaður.
Algeng mistök við innleiðingu öryggiskerfa, svo sem dreifilykla, eru að ákveða tiltekið öryggisstig fyrir fram og velja síðan lausn sem látin er gilda fyrir allan reksturinn. Engin ein lausn er til sem dugir alls staðar. Því ber nauðsyn til að stofnanir láti fara fram áhættugreiningu fyrir hvern þátt starfseminnar og velji síðan viðeigandi öryggislausnir með tilliti til ásættanlegs kostnaðar og niðurstaðna úr greiningu.
Fjármögnun kerfisins þarf að ganga upp, helst þannig að kostnaður þátttakenda verði í hlutfalli við það hagræði sem þeir hafa af því að taka upp rafræn samskipti. Í Svíþjóð er í undirbúningi kerfi þar sem reiknað er með að ríkið muni fá inni með sín vottorð hjá öðrum, sem hagsmuni geti haft af því að afhenda fólki rafræn skilríki, svo sem bönkum, félagssamtökum o.fl. Ríkisstofnanir greiði vottunarmiðstöðvum gjald fyrir sannvottun vegna samskipta þegar skjöl berast undirrituð með slíkum skilríkjum. Þannig verði rafræn skilríki einstaklinga nothæf til margs konar afgreiðslu og samskipta.

1.3. Aðgerðaáætlun

Nefndin minnir á að undirbúningur og innleiðing dreifilyklaskipulags tekur langan tíma og gerir kröfu til markvissra vinnubragða. Því er nauðsynlegt að það starf sem hófst með skipan dreifilyklanefndar haldi áfram af fullum þunga og án tafar. Nefndin leggur til eftirfarandi aðgerðaáætlun í fjórum liðum miðað við næstu tvö ár. Áður en þeim tíma lýkur liggi fyrir endurskoðuð áætlun er líti lengra fram í tímann.

Í fyrsta lagi verði opinberum stofnunum sem fyrst séð fyrir aðgangi að hugbúnaðarlausn eða lausnum fyrir rafrænar undirskriftir.
Slíkur aðgangur gæti t.d. fengist þannig að einhverri stórri stofnun sem þörf hefur fyrir víðtæk gagnvirk samskipti við bæði einstaklinga og atvinnulíf, ellegar nokkrum stofnunum í samvinnu, verði fengið það hlutverk að afla tilboða í slíka lausn og stjórna rekstri hennar. Frá upphafi verði leitað eftir stöðluðum markaðslausnum samanber tillögur í kafla 5.1. Það yrði mjög hvetjandi fyrir framgang málsins ef fljótlega tækist að koma af stað verkefnum þar sem sömu skilríkin myndu nýtast til fleiri aðgerða en einnar (Dæmi: tilkynningar til hlutafélagaskrár, tollafgreiðsla og skil á skattaupplýsingum).

Í öðru lagi verði gerðar ráðstafanir til þess að opinberar stofnanir geti svo fljótt sem auðið er veitt almenningi þjónustu á grundvelli skilríkja á gjörvakortum sem aðrir hafa gefið út (til dæmis viðskiptabankar, félagssamtök og fleiri). Slík ráðstöfun myndi stuðla mjög að útbreiðslu rafrænna skilríkja meðal almennings.

Í þriðja lagi verði séð fyrir öflugri leiðbeiningaþjónustu fyrir opinberar stofnanir sem taka vilja upp dreifilyklalausnir. Meðal annars verði þeim veitt aðstoð og ráðgjöf vegna áhættugreiningar.

[1] Sjá viðauka 4 og 5

Í fjórða lagi verði komið á verkefnisstjórn um rafrænar undirskriftir í ríkiskerfinu, er fari með samræmingar- og kynningarhlutverk, og hafi samráð við markaðinn og atvinnulífið um stöðlun og annað sem máli skiptir fyrir lipra verkan kerfisins.

Nú þegar verði hafin vinna við skilgreiningu krafna um form og innihald vottunarstefnu með hliðsjón af fyrirliggjandi fyrirmyndum frá t.d. Danmörku og Svíþjóð og að teknu tilliti til viðurkenndra staðla. Skilgreining á svæðum í vottorðum[2] verði hluti af þessu verki. Leita þarf aðstoðar sérfræðinga við þetta, að líkindum erlendis frá.

[2] Sjá viðauka 4.

2. Inngangur

Í apríl 2000 lagði forsætisráðherra fyrir ríkisstjórn aðgerðaáætlun þar sem rafræn viðskipti og rafræn stjórnsýsla eru gerð að forgangsverkefni, einu af fjórum, við framkvæmd stefnunnar um upplýsingasamfélagið hér á landi. Meðal annars er gert ráð fyrir að rafrænni afgreiðslu verði beitt hvarvetna þar sem henni verður við komið í stjórnsýslunni samhliða hefðbundnum afgreiðsluháttum. Unnið er að tilraunaverkefni með rafræn innkaup opinberra stofnana. Upp hafa verið tekin rafræn skil á virðisaukaskatti, rafræn skil á staðgreiðslu skatta og tryggingagjaldi eru á döfinni. Um 60% framtalsskyldra einstaklinga og 85% lögaðila hafa skilað framtölum sínum á rarfrænan hátt árið 2001. Rafræn atkvæðagreiðsla hefur farið fram í Reykjavík. Mörg verkefni eru ráðgerð í heilbrigðiskerfinu. Tollalög gera ráð fyrir að frá síðustu áramótum sé öllum tollskjölum skilað á rafrænu formi.

Eitt af því sem hamlað hefur þessari þróun er óvissa um réttarstöðu rafrænna skjala. Annað er ónógt traust á þeim kerfum sem í notkun eru. Þær aðferðir sem öruggastar eru taldar eru jafnframt kostnaðarsamar fyrir almenna notendur.

Vorið 2001 voru samþykkt á Alþingi lög um rafrænar undirskriftir[3] þar sem innleidd eru hér á landi ákvæði tilskipunar ESB 1999/93/EC um tiltekinn ramma fyrir rafrænar undirskriftir á Evrópska efnahagssvæðinu. Jafnframt hefur forsætisráðherra skipað nefnd til að kanna hvort og þá eftir atvikum hvaða lagabreytinga sé þörf til að stjórnsýslan geti áfram þróast rafrænt á æskilegan hátt. Skal hún einnig undirbúa þær lagabreytingar er hún telur nauðsynlegar.

Sú aðferð sem almennt er horft til varðandi rafrænar undirskriftir, hvort sem er í viðskiptalífinu eða opinberri þjónustu, er byggð á tveggja lykla dulritunarkerfi þar sem annar lykillinn er einkalykill (private key) en hinn dreifilykill (public key). Notkun rafrænna undirskrifta með dreifilyklum er, að uppfylltum tilteknum kröfum um skipulag og rekstur slíkra kerfa, talin tryggja með fullnægjandi hætti eftirtalin þrjú öryggisatriði í samskiptum með rafræn gögn:

- ✓ Tryggja heilleika gagna. Ef skeyti er rafrænt undirritað getur móttakandi þess gengið úr skugga um að það hafi skilað sér í heild sinni og að innihaldi þess hafi ekki verið breytt á leiðinni til hans.
- ✓ Staðfesta uppruna. Ef skeyti er rafrænt undirritað getur móttakandi þess fengið staðfestingu á uppruna þess því undirritunin tryggir að óviðkomandi aðili geti ekki sent skeyti í annars nafni án heimildar.
- ✓ Koma í veg fyrir afneitun. Með rafrænni undirritun má tryggja að hvorki sendandi þess né móttakandi geti ranglega neitað því að hafa sent það eða móttekið.

Fjármálaráðuneytið hefur tekist á hendur forgöngu um samstarf að gerð dreifilyklaskipulags fyrir íslenska stjórnkerfið. Árið 2001 var veitt fjárupphæð af fjárlagalið upplýsingasamfélagsins til að greina þörfina og gera tillögur að slíku skipulagi. Nefnd sú er hér skilar áliti var skipuð 24. janúar sl. Sjá erindisbréf í viðauka nr. 1

[3] Lög um rafrænar undirskriftir nr. 28/2001.

3. Greining KPMG

Ráðgjafafyrirtækið KPMG hefur samkvæmt samningi við fjármálaráðuneytið dags. 13. mars 2001 framkvæmt þarfagreiningu vegna dreifilyklaskipulags fyrir íslenskar ríkisstofnanir. Jafnframt skyldi kannað hvernig samsvarandi mál eru á vegi stödd í Hollandi, Kanada og Svíþjóð.

Skýrsla KPMG, sem skilað var samkvæmt samningi í lok maímánaðar, er 70 síður alls, í 6 köflum ásamt 5 viðaukum. 1. kafli er yfirlit fyrir stjórnendur, 2. kafli er formáli með lýsingu á aðferðum og aðstæðum. 3. kafli er þarfagreining, 4. kafli fjallar um nálgun að rafrænni stjórnsýslu í Kanada, Hollandi og Svíþjóð, 5. kafli um áform og aðgerðir sömu landa varðandi dreifilyklaskipulag. Í 6. kafla eru niðurstöður og tillögur um frekari aðgerðir. Viðauki A er tafla yfir stofnanir og einstaklinga sem rætt var við. Viðauki B er heimildaskrá. Viðauki C fjallar um skipulag yfirstjórnar dreifilyklakerfis kanadíska ríkisins. Viðauki D er almenn kynning á dreifilyklaskipulagi. Viðauki E hefur að geyma skýringar orða og hugtaka.

3.1 Þarfir stofnana

Þarfagreiningin er byggð á viðtölum við 17 stofnanir og fyrirtæki, og voru ríkisstofnanir í meirihluta. KPMG dregur þessar ályktanir af viðtölunum:

- ✓ Nær allar ríkisstofnanir hafa komið auga á leiðir til að nota Internettækni í starfsemi sinni. Flestar þeirra hafa reyndar tekið hana í notkun að einhverju leyti. Helstu markmið eru að auka rekstrarhagkvæmni og bæta gæði þjónustunnar.
- ✓ Hvort sem um er að ræða samskipti innan ríkisgeirans, milli ríkis og fyrirtækja eða ríkis og einstaklinga er þörf fyrir eftirtalda fjóra öryggisþætti í mismunandi mæli, leynd, staðfestingu á heilleika gagna, staðfestingu á uppruna og að verjast afneitun. Þörfin er breytileg, en á þriggja þrepa kvarða mælist þó ávallt þörfin fyrir einhvern einn þáttinn vera mikil og fyrir einhvern annan í meðallagi[4].
- ✓ Því nær allar stofnanir sem rætt var við telja stafræn vottorð vera heppilegustu lausnina á öryggisþörfum sínum, enda hyggjast þær flestar taka upp þess konar kerfi fyrr eða síðar.

Þá kom fram í viðræðum við nokkra íslenska banka að hjá þeim er í undirbúningi að gefa út gjörvakort (smart cards) fyrir alla sína viðskiptavini. Bent er á að þetta gæti haft þýðingu fyrir ríkið þar sem vista mætti einkalykla og rafræn vottorð á slíkum kortum. Í viðtölum kom fram að bankarnir virtust reiðubúnir til samstarfs við ríkið á þeim vettvangi. Ennfremur bendir KPMG á að ríkisstofnanir virðist ekki hafa á móti því að nota rafræn vottorð gefin út af einkafyrirtæki, enda séu greiðslukort bankanna tekin gild í daglegum samskiptum sem persónuskilríki nánast hvar sem er hér á landi þó að þau gildi ekki formlega sem slík.

[4] Sjá Skýrslu KPMG bls. 13 og 14.

3.2. Staðan í grannlöndum

Það var hluti af verkefni KPMG að kynna sér dreifilyklaskipulag í þremur löndum, Hollandi. Kanada og Svíþjóð. Löndin voru valin af dreifilyklanefnd. Rætt var við þrjá erlenda aðila auk þess sem farið var yfir fáanleg gögn, t.d. á veraldarvefnum. Í ljós kemur að Kanada er lang lengst á veg komið, á að giska tveimur árum á undan hinum. Dreifilyklaskipulag fyrir ríkið lá fyrir haustið 1998. Skilgreind eru fjögur ábyrgðarsvið fyrir undirskriftir og fjögur fyrir dulritun. Upp eru talin 17 frumherjaverkefni sem hafin eru. Svo virðist sem mörg þeirra verkefna sem hafin eru í Kanada séu áþekk þeim sem menn hyggjast fara út í hér. Megi því ætla að dreifilyklaskipulag gæti hentað íslenskri stjórnsýslu.

Svíar og Hollendingar hafa skilgreint dreifilyklaskipulag hvorir með sínum hætti en eru mun skemmra á veg komin en Kanada. Í báðum löndunum hafa stjórnvöld komist að þeirri niðurstöðu að dreifilyklatækni sé sú lausn sem þurfi til að fullnægja þörfum stjórnkerfisins í öryggismálum.

Í Kanada og Hollandi hefur samræmdri skipan verið komið á, þar sem tekið er á skipulagsmálum, tæknilausnum og lögfræðilegum atriðum fyrir ríkið í heild. Ætlast er til að ríkisstofnanir noti þetta skipulag enda tryggir það gagnkvæma virkni innan stjórnsýslunnar. Í báðum þessum löndum verður rótarlykill að öryggiskerfinu framleiddur og varðveittur á vegum hins opinbera. Í Svíþjóð er notað einfaldara líkan. Allar þjóðirnar þrjár hafa málefni dreifilyklakerfa mjög ofarlega á lista yfir mikilvægustu forsendur rafrænnar stjórnsýslu. Allar hafa þær skipað formlega yfirstjórn eða stýrinefnd dreifilyklaskipulags ríkisins.

Nefndin hefur komist að þeirri niðustöðu að könnun KPMG á stöðu mála í Svíþjóð hafi ekki gefið fyllilega rétta mynd. Sjá 4. kafla, Norðurlönd.

3.3 Niðurstöður KPMG

Í þessum kafla eru helstu niðurstöður skýrslu KPMG birtar í lauslegri þýðingu. Fyrst almennar athugasemdir.

Tímasetning. Það var niðurstaða KPMG að íslenska ríkið hafi þörf fyrir dreifilyklaskipulag til stuðnings verkefnum í rafrænni stjórnsýslu. Þó að ekki hafi verið leidd í ljós brýn þörf fyrir skjótar lausnir eru mörg verkefni á döfinni þar sem dreifilyklaskipulag gæti átt við. Að skilgreina það og hleypa af stokkunum er tímafrekt. Því ætti það verk að hefjast án tafar svo unnt verði að sinna þörfum ríkisstofnana um leið og þær gera vart við sig. Samræmt dreifilyklaskipulag sem komið væri á í tæka tíð myndi draga úr þeirri hættu að til verði einangraðar „eyjar“ með ósamþýðanlegum dreiflyklakerfum þar sem þurfa myndi sín skilríkin fyrir hvert viðfangsefni.

Uppbygging þekkingar. Nauðsyn ber til að innan ríkisins byggist upp þekking á dreifilyklakerfum og notkun þeirra. Dreifilyklatækni er flókin og þekking er lítil í landinu á þróun hennar og beitingu. Það myndi stórlega auka líkurnar á farsælli framkvæmd ef hið opinbera kæmi sér upp vissri sérþekkingu bæði á skipulags- tækni- og lagahlið dreiflyklakerfanna.

Alþjóðlegir samráðshópar. Bent er á að Ísland sé ekki eina landið sem stendur í því um þessar mundir að innleiða dreifilyklaskipulag. Til séu alþjóðlegir samráðshópar stjórnvalda, til dæmis á vegum Bandaríksjastjórnar, þar sem með þátttöku fengist aðgangur að dýrmætri þekkingu og reynslu.

KPMG lagði fram áætlun um næstu skref og aðgerðir í fjórum liðum:

- ✓ **Skilgreining mismunandi leiða til að útfæra dreifilyklaskipulag.** Að því marki sé unnt að fara nokkrar leiðir. Skilning á kostum og göllum hverrar um sig má öðlast með því að skilgreina og bera saman þær leiðir sem helst koma til álita við okkar kringumstæður.

- ✓ **Ákvörðun um hvaða leið farin skuli.** Í þessu skrefi ætti að velja þá leið sem talin er hagkvæmust og líklegust til árangurs.

- ✓ **Uppbygging fyrstu útgáfu traust- og stjórnunarlíkans.** Traust- og stjórnunarlíkan dreifilyklaskipulags lýsir stöðu og hlutverki hinna ýmsu þátta kerfisins. Það ætti að taka mið af skipulagi stjórnsýslunnar og vera sniðið að upplýsinga- og fjarskiptakerfum ríkisins. Traustlíkanið á að lýsa því hvernig eftirliti er háttað með dreifilyklakerfinu og því haldið í traustverðu ástandi.

- ✓ **Uppsetning dreifilyklaskipulags og gagnsetning fyrstu verkefna.** Ráðlegt sé að mati KPMG að koma dreiflyklaskipulagi á í áföngum og hefja verkið með nokkrum frumherjaverkefnum þar sem líkur á árangri séu góðar. Í þessum verkefnum ætti að flétta dreifilyklakerfið saman við heildarskipulag örygggismála hjá viðkomandi stofnunum. Við framkvæmd frumherjaverkefna muni verða til verðmæt reynsla og þekking til að byggja á skipulag dreifilyklamála í öllu stjórnkerfi ríkisins.

-

4. Norðurlönd

Þar sem í ljós kom að greining KPMG á stöðu mála í Svíþjóð var ekki fullnægjandi ákvað nefndin að skoða stöðuna betur og taka þá Danmörku og Noreg með í samanburðinn. Helstu heimildir sem skoðaðar hafa verið eru:

- *Frá Danmörku:* Digital forvaltning. Finansministeriet, maí 2001.
- *Frá Noregi:* Uten penn og blekk. Bruk av digitale signaturer i elektronisk samhandling med og i forvaltningen. NOU 2001:10, mars 2001.
- *Frá Svíþjóð:* Elektronisk identifiering 2001. Förfrågningsunderlag F:168 (með fylgiskjölum).

Auk þess allmörg rit sem talin eru upp í heimildaskrá og viðtal formanns nefndarinnar við Dag Osterman, sérfræðing hjá ríkisskattstjóra Svíþjóðar.

Margt er líkt með áætlunum frændþjóðanna um innleiðingu dreifilyklaskipulags í stjórnsýslunni. Má með nokkrum sanni segja að við blasi norræn eða að minnsta kosti skandinavísk leið þegar áætlanir eru bornar saman.

Í öllum löndunum hafa fyrir 2-3 árum verið sett af stað tilrauna- og frumherjaverkefni með tiltölulega takmörkuðu umfangi til að safna reynslu. Sjá t.d. matsskýrslu um árangur í Danmörku.[5] Það vekur athygli að útbreiðsla rafrænna skilríkja er enn sem komið er mjög takmörkuð og að öll þessi þróun tekur langan tíma.

Allir leggja áherslu á markaðslausnir þar sem ríkið setur þó fram kröfur um form vottorða og helstu atriði í vottunarstefnu, einkum í því skyni að tryggja eftir föngum að ríkisstofnanir geti tekið við og unnið úr vottorðum útgefnum af mismunandi vottunarmiðstöðvum. Kröfur þessar eru byggðar á evrópskum stöðlum og alþjóðlegum samþykktum um útfærslu staðla (prófílum).[6]

Ennfremur er það samhljóða niðurstaða í öllum þremur löndunum (skýrslur skrifaðar 2000 og 2001)[7] að fullgildar undirskriftir séu ekki á dagskrá til almennrar útbreiðslu á næstunni (t.d. næstu tvö árin). Helsta ástæðan er sú að það öryggisstig sem krafist er náist ekki nema með gjörvakortum, en þau séu enn sem komið er af ýmsum ástæðum óraunhæfur kostur til handa almenningi. Bent er á að fjölmörg erindi milli ríkisins og landsmanna megi inna af hendi með rafrænum hætti þó notað sé lægra öryggisstig. Allur undirbúningur er þó miðaður við að taka upp fullgildar undirskriftir þegar það verður tímabært. Sem stendur er horft um það bil tvö ár fram í tímann. Er ætlunin að á þeim tíma verði úrbreiðsla rafrænna skilríkja aukin verulega og jarðvegurinn undirbúinn undir almenna notkun.

Lögð er áhersla á að verkefni stofnana séu misjöfn og að áhættugreining verði að fara fram áður en ákvörðun sé tekin um öryggislausnir. Í skýrslu danska UT-

[5] [Evaluering]
[6] [RFC 2459]; [TS 101 862].
[7] DK: [Dig-forvalt] 7. kafli bls. 2; NO: [NOU2001: 10] kafli 9.7 bls.14; SE: [F:168], 1.5 bls. 5.

öryggisráðsins er bent á að of stífar öryggiskröfur kosti bæði tíma og fyrirhöfn, og ennfremur að ein tiltekin öryggislausn eigi sjaldnast við öll verkefni sem stofnun þarf að fást við.

Í sömu skýrslu er einnig bent á nokkur mikilvæg stjórnunarleg ákvörðunaratriði sem mörg hver eiga eins við hér á landi. Dreifilyklanefnd hefur gert sumar ábendingar hennar að sínum (sjá 5. kafla).

Minnst er á krossvottun milli útgefenda skilríkja víðar en á einum stað, en í óljósum orðum. Sennilega er ekki alls staðar átt við krossvottun heldur þann möguleika fyrir ríkisstofnanir að geta tekið gild vottorð frá mismunandi útgefendum. Svíar hafa ekki í hyggju að setja á stofn eigin vottunarmiðstöð (statens CA) í þessum áfanga, en útiloka ekki að það kunni að verða gert í framtíðinni. Í Noregi hefur fyrirkomulag þessara mála ekki verið ákveðið.

Nefndin telur líklegt að með stöðlun af því tagi sem að ofan getur megi, að minnsta kosti á meðan útgefendur vottorða eru fáir, finna rekstrarform þar sem komast megi hjá krossvottun. Í Svíþjóð er stefnt að slíkri lausn.

Það kemur víða fram í þessari skýrslu að nefndin hefur umfram aðra leitað heimilda í sænskum gögnum. Meðal annars er viðauki 3 tekinn úr sænskum útboðsgögnum vegna rafrænna skilríkja.
Hugmynd Svía um útbreiðslu skilríkja meðal almennings er einnig að mati nefndarinnar afar athyglisverð. Hún er í stuttu máli fólgin í því að hinir og þessir sem „eiga“ hóp viðskiptavina, svo sem bankar, stéttarfélög og önnur félagasamtök, einnig Internet- og símafyrirtæki, sem gefi út rafræn skilríki hvort sem er, sjái sér hag í því að bjóða aðgang að upplýsingakerfum ríkisins sem aukaþjónustu. Um þessa þjónustu verði á grundvelli útboða gerðir rammasamningar sem í raun jafngilda vottunarstefnu.

Ríkið hyggst svo greiða samningsaðilum sínum þjónustugjald fyrir uppflettingu í skrám um gild vottorð (eða lokunarskrám). Gangi þetta eftir verður í raun ekki nema ein tegund vottorða í gangi í samskiptum ríkisins og almennings (og fyrirtækja) þó að útgefendur verði margir.

Tvö skilyrði þurfa að vera uppfyllt ef einstaklingur eða fyrirtæki vill verða þátttakandi í dreifilyklaskipulagi sænska ríkisins:

- Þjónustuveitandi hans (certification service provider, CSP) þarf að hafa rammasamning við ríkið, og
- Vottorðið sé á skilgreindu formi ríkisins.

5. Tillögur og ályktanir nefndarinnar

Greining KPMG (sjá fylgiskjal 1) hefur sýnt fram á þörf fyrir dreifilyklaskipulag til að styrkja öryggi í meðferð gagna allvíða í stjórnsýslu ríkisins. Til sömu niðurstöðu leiðir skoðun á tillögum og framkvæmd tilraunaverkefna í grannlöndum okkar, til dæmis Danmörku og Svíþjóð. Greining hefur ekki farið fram hérlendis á hagkvæmni, kostnaði eða tíma, en vitað er um nokkur verkefni sem sterkar líkur benda til að dreifilyklalausnir myndu henta vel.

> ***Nefndin telur brýnt*** að standa rétt að skilgreiningu og innleiðingu slíks skipulags enda þarf frá upphafi að liggja fyrir traust á því til jafns við hefðbundin ferli. Jafnframt beri að hraða undirbúningi svo að þær framfarir í rafrænni stjórnsýslu sem byggjast á traustum öryggisráðstöfunum þurfi ekki að tefjast, eða menn grípi til óstaðlaðra og ósamhæfðra lausna.
>
> ***Nefndin álítur vænlegt***, og er það meginstoð tillagna hennar, að taka til fyrirmyndar þá „skandinavísku leið“ sem lýst er í skýrslu þessari og tilvitnuðum gögnum. Með því að tileinka sér þá reynslu sem safnast hefur má koma í veg fyrir mistök. Með því að taka upp, breyttu breytanda, þær aðferðir og vinnubrögð sem sérfræðingar þriggja þjóða virðast sammála um getur íslensk stjórnsýsla náð upp að verulegu leyti því forskoti sem flest grannríki okkar hafa nú.

Til að ná þessum markmiðum er eftirfarandi lagt til:

5.1. Staðlaðar markaðslausnir

Margar leiðir eru til þess að innleiða dreifilyklaskipulag og ekki auðséð í fljótu bragði hver þeirra sé heppilegust fyrir íslenska ríkið. Meðal atriða sem meta þarf eru til dæmis notkunarsvið skilríkja, ákvörðun öryggisstigs, áhrif gildandi laga og kostnaður fyrir ríkið og viðskiptavini þess. Nánar er fjallað um nokkur þessara ákvörðunaratriða í kafla 6. Þá er það matsatriði hvert skuli vera hlutverk markaðarins þar sem vottun og útgáfa rafrænna vottorða ásamt sölu á ýmsum sérhæfðum búnaði er orðinn umtalsverður iðnaður. Hér verður drepið á tvær lausnir, sína á hvorum kanti þess litrófs sem í boði er, en síðan gerð tillaga um staðlaða markaðslausn.

Það sem kalla mætti hreina markaðslausn felst í því að ríkið gefur stofnunum ekki önnur fyrirmæli en að þær skuli nota dreifilykla í samræmi við útkomu úr áhættugreiningu. Stofnanir semja hver við sinn seljanda um útgáfu og viðhald vottorða, vottun og skráahald. Dreifilyklastefna seljanda lausnarinnar er tengd opinberum traustverðugleika stofnunar með samningi.

- Kostir: Frjáls markaður, fyrirhöfn stofnunar í lágmarki, miðstýring í lágmarki.
- Gallar: Hætt við að margs konar skilríki verði í gangi, hver um sig með takmarkað gildissvið. Verðskrár vottunarfyrirtækja ráða kostnaði að mestu leyti. Sérstakar ráðstafanir verður að gera vegna samskipta stofnana innbyrðis, til dæmis að semja við eitt fyrirtæki um þjónustu fyrir allar ríkisstofnanir, sem þá er hætt við að verði allsráðandi á markaðinum. Óvíst hvernig við stæðum varðandi samskipti við yfirvöld í öðrum löndum.

Hrein ríkislausn væri þannig að hið opinbera kæmi á fót heildstæðu skipulagi með vottunarstöðvum, aðstöðu til útgáfu skilríkja, eigin rótarlykli, öryggis- og eftirlitskerfi ásamt öllu öðru sem til þarf.

- Kostir: Full yfirráð yfir öllum þáttum. Ríkið óháð fyrirtækjum sem koma og fara.
- Gallar: Mikil fyrirhöfn við rekstur, engin trygging fyrir samhæfingu við markaðinn.

Þriðja leiðin, sem kalla má staðlaða markaðslausn, felst í því að ríkið setur fram kröfur um helstu atriði vottunarstefnu og framkvæmd hennar ásamt formi vottorða. Kröfurnar eru í samræmi við þær útfærslur evrópskra og alþjóðlegra staðla sem tíðkast í grannlöndum okkar, þannig að víðtæk samræming næst.

Kröfurnar eru settar fram í rammasamningum eða með reglugerð. Ríkisstofnanir geta skipt við hvern þann seljanda þjónustu sem hefur gert rammasamning eða getur staðfest að hann fari að viðkomandi reglugerð ef það fyrirkomulag verður ofan á. Samkomulag er gert við markaðinn um skiptingu kostnaðar.
Þessi leið hefur verið valin af sænska ríkinu, og verða rammasamningar undirritaðir um miðjan nóvember. Af tiltækum gögnum má ráða að bæði Danir og Norðmenn ætli að fara svipaðar leiðir.

- Kostir: Stöðluð lausn, tiltölulega einföld útfærsla, margvísleg not af sömu skilríkjum, t.d. fyrir einstaklinga.

> ***Nefndin leggur til*** að síðasttalda leiðin verði farin hér. Í viðauka 3 er birt lausleg þýðing á kröfum sænska ríkisins eins og þær koma fram í útboðslýsingu. Ennfremur er samanburð á innihaldi vottorða í Svíþjóð og Noregi að finna í viðauka 4. Að teknum ákvörðunum um útfærslu leggur nefndin til að sem fyrst verði hafist handa við að útfæra kröfur íslenska ríkisins í þessum anda. Um vottunarstefnu og framkvæmd hennar verði ennfremur tekið tillit til staðlanna ETSI TS 101 456 og RFC 2527. Um innihald og form vottorða samkvæmt X.509 V3 verði tekið tillit til staðlanna RFC 3039 og ETSI TS 101 862.

Með þessu vinnst tvennt: Opinn markaður með víðtækum möguleikum á samnýtingu vottorða og að reglurnar verða í samræmi við ákvæði laga og tilskipana um fullgildar undirskriftir. Nefndin telur miklar líkur á að almenn samstaða geti náðst um þessa leið hér á landi, einkum þegar tekið er tillit til þess að notkun rafrænna undirskrifta hefur ekki náð neinni útbreiðslu enn sem komið er.

5.2. Framsækin markmið, raunsæir áfangar

Þróun tæknilausna fyrir rafrænar undirskriftir og búnað til stuðnings við dreifilyklakerfi er afar hröð samhliða því sem markaðssetning þeira er öflug. Staðlar til að tryggja viðunandi samvirkni og þar með nýtingu fjárfestingar í búnaði eru í þróun. Lesarar fyrir gjörvakort gætu mjög fljótlega orðið staðalbúnaður á nýjum tölvum, til dæmis í rammasamningum ríkisins. Útbreiðsla slíkra tækja meðal almennings mun fyrirsjáanlega taka lengri tíma. Hins vegar er þess að gæta að aðferðir við að bera kennsl á fólk eru líka í þróun. Í því sambandi má nefna manngreinitækni (biometric), svo sem búnað til að skynja fingraför. Rafrænar undirskriftir með vottuðum fingraförum hafa verið notaðar í tilraunaverkefnum, m.a. í Hollandi.
Talið er að eina örugga leiðin til að varðveita fullgild vottorð sé gjörvakort eða annar slíkur „harður miðill“, sem vottorðshafi beri á sér[8]. Búnaður til að lesa gjörvakort er enn lítt útbreiddur. Í ljósi þess sem að ofan segir virðist veruleg áhætta fylgja því að kaupa nú þegar einhverja háþróaða tæknilega lausn, til dæmis byggða á gjörvakortum, fyrir alla landsmenn.

> ***Nefndin telur álitlegra*** til skemmri tíma að leggja áherslu á einfaldari lausnir sem þó myndu tryggja fullnægjandi öryggi við mjög marga þætti í rafrænni opinberri þjónustu. Sömu eða hliðstæðar lausnir myndu nýtast samhliða við rafræn viðskipti af ýmsu tagi.

Þetta þýðir engan veginn að vikið sé frá þeirri stefnu að innleiða og styðja fullgildar rafrænar undirskriftir. Allur undirbúningur ætti að miðast við að ríkisstofnanir geti notað þær í samskiptum við atvinnulíf og almenning jafnskjótt og eftirspurn skapast. Eftirspurn frá almenningi kann að skapast vegna útbreiðslu vottorða sem gefin væru út í öðru skyni, svo sem til samskipta við rafræna bankaþjónustu.

> ***Nefndin leggur til*** að ríkisstofnanir undirbúi sig á markvissan hátt undir að geta átt samskipti við atvinnulíf og almenning með stuðningi rafrænna vottorða, meðal annars á „hörðum miðlum“.

Þegar litið er til reynslu annarra þjóða af notkun gjörvakorta í samskiptum hins opinbera og almennings þar sem ætlast er til að einstaklingar kaupi eða útvegi sér kort er skemmst frá því að segja að flestar slíkar tilraunir hafa misheppnast. Ætla má að þröskuldar séu í veginum bæði hvað varðar verð og fyrirhöfn. Undan því verður þó ekki skotist að háu öryggisstigi hlýtur að fylgja visst umstang tengt því að bera kennsl á menn með viðunadi öryggi og koma skilríkjum í réttar hendur.

> ***Nefndin leggur til*** að leitað verði nýstárlegra leiða til að örva notkun og útbreiðslu dreifilykla meðal almennings og í atvinnulífinu. Meðal þess sem til greina kemur er að leita eftir samstarfi við aðra hugsanlega stórnotendur rafrænna skilríkja, svo sem viðskiptabanka, stéttarfélög o.fl. Fram kemur í skýrslu KPMG[9] að afstaða að minnsta kosti sumra banka til slíkrar samvinnu sé jákvæð.

[8] Sjá 4. kafla.
[9] Skýrsla KPMG bls. 45

5.3. Frumherjaverkefni

Fjármögnun kerfisins þarf að ganga upp, helst þannig að kostnaður þátttakenda verið í samræmi við tilkostnað þeirra. Það yrði mjög hvetjandi fyrir útbreiðslu rafrænna skilríkja ef fljótlega tækist að koma af stað verkefnum þar sem sömu skilríkin myndu nýtast til fleiri aðgerða en einnar (Dæmi: tilkynningar til hlutafélagaskrár, tollafgreiðsla og skil á skattaupplýsingum).

> ***Nefndin leggur til*** að opinberum stofnunum verði sem fyrst séð fyrir aðgangi að hugbúnaðarlausn eða lausnum fyrir rafrænar undirskriftir (vottorð á mjúkum miðlum). Slíkur aðgangur gæti t.d. fengist þannig að einhverri stórri stofnun sem þörf hefur fyrir víðtæk gagnvirk samskipti við bæði einstaklinga og atvinnulíf, ellegar nokkrum stofnunum í samvinnu, verði fengið það hlutverk að afla tilboða í slíka lausn og stjórna rekstri hennar. Frá upphafi verði svo sem unnt er miðað við staðlaðar markaðslausnir sbr. kafla 5.1.

5.4. Stjórnun innleiðingarferlis

Reynsla annarra þjóða sýnir að innleiðingarferli dreifilyklaskipulags er tímafrekt. Því telur nefndin nauðsynlegt að þróunarferlið haldi áfram þegar eftir að starfi hennar lýkur. Huga þarf að yfirstjórn þessara mála til framtíðar, en víða í grannlöndum okkar hefur verið sett á fót sameiginleg yfirstjórn sem ber ábyrgð á dreifilyklaskipulaginu, heldur því við og samræmir aðgerðir stjórnvalda.

> ***Nefndin leggur því til*** að sem fyrst verði komið á verkefnisstjórn um rafrænar undirskriftir í ríkiskerfinu, er fari með samræmingar- og kynningarhlutverk, og hafi samráð við markaðinn og atvinnulífið um stöðlun og annað sem máli skiptir fyrir lipra verkan kerfisins.

5.5 Leiðbeiningarþjónusta

Ferlið er býsna flókið og þekking á þýðingu þess af skornum skammti bæði í stjórnsýslunni og hvarvetna í þjóðfélaginu. Því þarf að halda uppi öflugu kynningarstarfi, bæði meðal stjórnenda ríkisstofnana og almennings.

> ***Nefndin leggur því til*** að höfð verði uppi af hálfu ríkisins, gjarnan í samstarfi við aðra sem hagsmuna eiga að gæta, öflug leiðbeiningaþjónusta fyrir opinberar stofnanir sem taka vilja upp dreifilyklalausnir. Meðal annars fái þær aðstoð og ráðgjöf vegna áhættugreiningar. Leiðbeiningum og upplýsingum verði einnig komið á framfæri við almenning.

5.6. Áhættugreining og ákvörðun öryggisstigs

Algeng mistök við innleiðingu öryggiskerfa, svo sem dreifilykla, eru að ákveða tiltekið öryggisstig fyrir fram og velja síðan lausn sem gilda á fyrir allan reksturinn. Engin ein lausn er til sem dugir alls staðar. Því ber nauðsyn til að stofnanir láti fara fram áhættugreiningu fyrir hvern þátt starfseminnar og velji síðan viðeigandi öryggislausnir fyrir hvern rekstrarþátt með tilliti til niðurstaðna úr greiningu. Eftirfarandi þrjú öryggisstig eru almennt viðurkennd.

- ***Hátt öryggisstig*** svarar til þeirra krafna sem gerðar eru til fullgildra rafrænna undirskrifta í lögum um rafrænar undirskriftir nr. 28/2001. Í Noregi, Danmörku og Svíþjóð líta menn svo á að kröfur um fullgildar undirskriftir verði ekki uppfylltar nema skilríki séu varðveitt á gjörvakortum

eða öðrum hörðum miðlum sem menn beri á sér.

- ***Meðalhátt öryggisstig*** miðast við útfærða rafræna undirskrift í skilningi laganna. Við þetta stig er jafnan heimilt að vista lykla á vinnustöð eða disklingi að því gefnu að kerfislausnir séu viðhafðar sem tryggi að þeir liggi ekki á lausu. Við hverja undirskrift ber að nota tilheyrandi PIN-númer. Talið er að þetta öryggisstig sé fullnægjandi við fjöldamargar afgreiðslur og samskipti hjá ríkisstofnunum.

- ***Lágt öryggisstig***, til dæmis aðrar gerðir vottorða, auðkenni sem byggist á leyniorðum eða PIN-númerum eingöngu (SSL og slíkar lausnir).

Nefndin telur að við innleiðingu nýrra verkefna varðandi þjónustu hins opinbera ætti í öllum tilvikum þegar um er að ræða persónuupplýsingar eða viðkvæmar upplýsingar um fyrirtæki að miða við hátt eða meðalhátt öryggisstig.

6. Ákvörðunaratriði við útfærslu dreifilyklaskipulags

Þótt farið sé að stöðlum eru allmörg atriði sem skilgreina þarf og álitamál um útfærslu. Sum atriði eru tæknilegs eðlis og krefjast sérfræðiþekkingar á stöðlum og hugbúnaði, önnur af þeim toga að stjórnendur þurfa að taka afstöðu til þeirra. Hér á eftir verður bent á nokkur þessara atriða án þess að tæmandi sé talið. Nefndin tekur ekki afstöðu til einstakra álitamála en bendir á að því flóknari sem gerð kerfisins er og því meiri lagskipting, þeim mun erfiðari verður framkvæmd og eftirlit.

6.1. Tæknileg atriði

6.1.1. Form vottorða

Við samanburð á formi vottorða[10] í Noregi og Svíþjóð kemur í ljós munur á skilgreiningu örfárra svæða. Koma þar til tæknileg álitamál sem leita verður til sérfræðinga um úrlausn á, en miklu varðar að velja kosti sem njóta almennrar viðurkenningar.

Einnig kemur fram munur á notkun þátta í „subject“-svæðinu, þ.e. vottorðshafa. Þar þarf meðal annars að taka ákvörðun um það hvort nota eigi fullt nafn samkvæmt þjóðskrá eða heimila að millinafni sé sleppt (nota „commonName“), hvort til greina komi að nota eitthvert annað númer en kennitölu og hvort heimila eigi dulnefni.

6.1.2. Fjöldi vottorða í skilríkjum

Einstök vottorð eru sérhæfð og til vel skilgreindra nota. Ef miðað er við persónuskilríki, svo dæmi sé tekið, gera norsku tillögurnar ráð fyrir þremur vottorðum í hverjum skilríkjum:

- fyrir afneitunarvörn (non-repudiation)
- fyrir kennsl (authentication)
- fyrir dulritun texta og lykla (data encipherment, key encipherment).

Sænska skilgreiningin gerir ráð fyrir tveimur vottorðum, semsé að tveimur þeim síðastnefndu verði steypt saman í eitt. Sjá nánar í fylgiskjali 4.

6.2. Stjórnunarleg atriði

6.2.1. Gildissvið og tegundir skilríkja

Nokkrar tegundir skilríkja hafa verið skilgreindar í dreifilyklaskipulagi grannþjóðanna. Meðal ákvörðunaratriða er það hvort og þá hvernig þau skuli notuð. Eftirtalin afbrigði eru nefnd í tilvitnuðum gögnum, og er nokkur munur milli landa:

- Persónuskilríki einstaklinga, með nafni og kennitölu ásamt tilheyrandi vottorðum og dulritunarlyklum.
- Starfsmannaskilríki þar sem einstaklingurinn er tengdur stofnun þeirri eða fyrirtæki sem veitir honum vinnu. Eigindir (attribute) í vottorði gefa til kynna á hvern hátt hann má skuldbinda vinnuveitandann.

[10] Sjá viðauka 5, Orðaskýringar, varðandi merkingarmun á orðunum „vottorð“ og „skilríki“ í þessari skýrslu.

- Skilríki fyrirtækis eða stofnunar; afbrigði eru skilríki fyrir stimpil stofnunar.
- Skilríki fyrir starfsréttindi eða stöðu (læknir, ráðuneytisstjóri).
- Skilríki fyrir netþjón. Mjög stór hluti þeirra skilríkja sem gefin hafa verið út í heiminum til þessa eru væntanlega netþjónaskilríki (secure server).

UT-öryggisráðið danska hefur bent á[11] að hugsanlega megi fækka afbrigðum skilríkja með því að tengja notkun þeirra og meðfylgjandi ábyrgð í „rafheimum“ við skipurit stofnunar og starfslýsingu viðkomandi einstaklings í „pappírsheimum“, enda séu upplýsingar um hvort tveggja greiðlega aðgengilegar, til dæmis á vef stofnunarinnar.

6.2.2. Móttaka og sending stafrænt undirritaðra sendinga.

Stofnun sem taka vill á móti boði með stafrænni undirskrift sendanda verður að birta á áberandi hátt upplýsingar um það með hvaða hætti senda skuli slíka sendingu. Hér skiptir máli hvernig stofnunin kýs að sannvotta undirskriftina. Ef ekki eru skilgreindar og settar upp sjálfvirkar aðferðir til sannvottunar verður að vera til opinbert tölvupóstfang til að senda á öll undirskrifuð boð. Þennan póst þarf svo sérstakur starfsmaður að fara yfir, sannvotta (oftast að fá sannvottaðar) undirskriftirnar, og senda áfram til rétts viðtakanda innan stofnunar, svo framarlega sem sannvottun tekst. Takist sannvottun ekki verður að bregðast á fyrirfram ákveðinn hátt við því gagnvart sendanda.

6.2.3. Móttaka dulritaðra sendinga.

Þegar dulrituð sending berst er það að jafnaði vegna þess að sendandinn telur að efninu beri að halda leyndu. Sé ekki svo er dulritunin eingöngu til tafa og óþurftar. Á móttökustað ber að beina sjónum að því hvernig staðið er að dulráðningu dulritaðra boða, - og hver skuli gera það. Taka þarf afstöðu til þess hvort stofnunin skuli koma sér upp einum lykli til að dulráða öll móttekin boð eða hvort það skuli gert með lyklum starfsmanna eftir atvikum. Sameiginlegur dulráðningarlykill hefur þann kost að hvaða starfsmaður sem er getur ráðið móttekin boð hafi hann á annað borð aðgang að varðveislustað þeirra. Í hinu tilvikinu getur reynst ómögulegt að ráða tiltekin boð ef starfsmaður er hættur eða fjarstaddur.

Margt mælir með því að boð sem stofnun fær send séu dulrituð með sameiginlegum lykli sem allir starfsmenn geti notað. Sé það ekki gert verður að vera fyrir hendi tækni til að endurheimta lykilinn (key recovery).
Allavega ætti það að vera almenn regla að ekki séu notuð sömu lyklapör til dulritunar boða og stafrænna undirskrifta.

6.2.4. Líftími undirskrifta.

Liður í hverri áhættugreiningu ætti að vera skilgreining á því hversu lengi rafrænt undirskrifuð skjöl þurfi að vera virk í þeim skilningi að unnt sé að sannvotta undirskriftina. Sannvottun undirskriftar er framkvæmd með hjálp þekkts algríms á grundvelli stafræns vottorðs, sem jafnframt þarf að vera unnt að sannvotta. Núgildandi danskar leiðbeiningar mæla með að miða líftímann við fyringarreglur bókhaldslaga (5 ár þar í landi) og eitt ár til viðbótar í öryggisskyni.

[11] [IT-sikk] kafli 3.3.

Margir véfengja það að svo langur varðveislutími virkra skjala sé nauðsynlegur. Áhættugreining ætti að leiða það í ljós hve langur hann þarf að vera í hverju tilviki. Benda má á að þær stofnanir sem nota rafræn skjalavörslukerfi gætu í staðinn gert ráðstafanir til að merkja sérstaklega að skjal hafi verið rafrænt undirskrifað og undirskriftin sannvottuð við móttöku.

6.2.5. Meðferð dulritaðra skjala innan stofnunar

Taka þarf ákvörðun um það hvort dulritunar er þörf í skjalageymslum stofnunar. Greining á styrk annarra aðgangstakmarkana gæti leitt til þeirrar niðurstöðu að dulritun bæti ekki gagnaleyndina að því marki sem réttlæti óhjákvæmileg óþægindi og kostnað. Þá er bent á að taka þarf tillit til lögbundins hlutverks Þjóðskjalasafns sem ráðgjafa um skjalavörslu.

Viðauki 1.

Erindisbréf

24. janúar 2001
Tilvísun: FJR00110077/032/JG/--

Fjármálaráðuneytið skipar yður hér með í nefnd til að gera tillögur að dreifilyklaskipulagi *(Public key infrastructure, PKI)* fyrir ríkið í heild og leggja meginlínur um það hvernig notkun rafrænna undirskrifta skuli hagað í ríkiskerfinu. Meginmarkmið skal vera að leggja drög að fullnægjandi og traustverðu dreifilyklakerfi er noti fáanlegar markaðslausnir og viðurkennda staðla, en kostnaði og umstangi verði haldið í lágmarki bæði fyrir ríkið, atvinnulífið og borgarana. Meðal annars skal nefndin

- kanna hvar sé þörf fyrir rafrænar undirskriftir og dulritun hjá ríkisstofnunum vegna verkefna á sviði rafrænna viðskipta og rafrænnar stjórnsýslu,
- gera grein fyrir þeim öryggiskröfum sem gera þarf bæði innan ríksikerfisins og út á við til að tryggja áreiðanleika og traust í rafrænum samskiptum,
- gera drög að kostnaðar- og framkvæmdaáætlun við að koma upp dreifilyklaskipulagi fyrir ríkið og kanna grundvöll fyrir útboði á búnaði og þjónustu vegna slíks kerfis,
- kanna grundvöll fyrir samstarfi við aðra hugsanlega stórnotendur rafrænna skírteina, til dæmis viðskiptabankana, um aðgerðir til að auðvelda almenningi afnot af þeim kerfum sem byggð verða upp. Meðal annars er hér átt við hugsanlega samnýtingu rafrænna skírteina.

Eftirtaldir eru skipaðir í nefndina: Jóhann Gunnarsson, tilnefndur formaður af fjármálaráðuneyti, Angantýr Einarsson, tilnefndur af fjármálaráðuneyti, Benedikt Bogason, tilnefndur af dómsmálaráðuneyti, Daði Einarsson, tilnefndur af heilbrigðisráðuneyti, Guðmundur Ásmundsson, tilnefndur af Samtökum atvinnulífsins, Ingi Örn Geirsson, tilnefndur af Sambandi banka og verðbréfafyrirtækja, Jónína S. Lárusdóttir, tilnefnd af iðnaðar- og viðskiptaráðuneytum, Stefán Jón Friðriksson, tilnefndur af Verslunarráði Íslands.

Nefndin skal hefja störf nú þegar og ljúka störfum fyrir lok júlí 2001. Nefndin getur keypt sérfræðiaðstoð og stofnað til útgjalda í þágu verkefnisins í samráði við ráðuneytið. Nefndin þiggur þóknun fyrir störf sín, ákvarðaða af þóknananefnd eftir tillögu ráðuneytisins.

F.h.r.

Viðauki 2.

Þessi viðauki er tekinn beint úr athugasemdum við frumvarp til laga um rafrænar undirskriftir er lagt var fyrir Alþingi vorið 2001. Nefndin bendir ennfremmur á rit Ríkisendurskoðunar „Rafræn viðskipti“ gefið út í október 2000, þar sem fjallað er um rafrænar undirskriftir og dulritun á greinargóðan hátt. Sjá vef Ríkisendurskoðunar, http://www.rikisend.althingi.is.

Dreifilyklaskipulag –Nokkur meginhugtök og grundvallaratriði.

3.1. Hvað er rafræn undirskrift?

3.1.1. Rafræn undirskrift í víðri merkingu.

Rafræn undirskrift (e. electronic signature) er almennt og tæknilega hlutlaust hugtak sem vísar til samansafns allra hugsanlegra aðferða sem hægt er að nota til að undirrita rafrænar upplýsingar. Þessar aðferðir geta t.d. verið undirritun í tölvupósti, skönnuð eiginhandarundirritun, vefsíðufang, líffræðileg kennimerki eins og skönnun á fingri eða auga og stafrænar undirskriftir byggðar á rafrænum lyklum og vottorðum.

3.1.2. Rafræn undirskrift í þrengri merkingu.

Nú er almennt ekki talað um rafrænar undirskriftir í svo víðtækum skilningi sem hér að ofan. Yfirleitt er átt við undirskrift í rafrænu formi sem er hluti af eða skýrt tengd rafrænum gögnum sem notuð er til að sannprófa uppruna gagnanna. Í eiginlegum skilningi er rafræn undirskrift í því fólgin að tiltekinn búnaður eða aðferð eru notuð til þess að dulrita efni sendingar, í heild eða að hluta, og dulráðning sendingarinnar sannprófar rétt efni sendingar, uppruna hennar og sendanda.

Frá tæknilegu sjónarhorni er rafræn undirskrift hins vegar tilteknar rafrænar upplýsingar. Þessar upplýsingar eru eins og aðrar rafrænar upplýsingar táknaðar með rafhleðslum og eyðum í minni tölvu sem eftir atvikum er hægt að flytja til annarrar tölvu með sendingu rafboða og gera þannig aðgengilegar öðrum.

Langflestar þeirra aðferða sem notaðar eru til að mynda undirskriftir núna eru stafrænar. Stafræn undirskrift (e. digital signature) er hugtak sem er notað um tiltekna tækni til að búa til rafrænar undirskriftir. Þá eru notuð svokölluð dreifilyklakerfi (e. Public Key Infrastructure) til að undirrita upplýsingar. Þessi aðferð er sú algengasta og hefur bæði ýtt undir tæknilega þróun, og víðtæk viðbrögð í lagasetningu. Í eiginlegri merkingu er stafræn undirskrift dulritun stafrænna upplýsinga með einkalykli (e. private key). Þá er unnt að staðfesta hver eigandi einkalykilsins sé og heilleika skilaboðanna með notkun á samsvarandi dreifilykli (e. public key) og vottorði vottunaraðila á dreifilyklinum. Stafræn undirskrift er hins vegar frá tæknilegu sjónarhorni samsafn af ritstafatáknum (e. alphanumeric) sem gert er með algóritma við dulritun.

Hugtakið rafræn undirskrift er víðtækara en stafræn undirskrift þar sem hið fyrrnefnda vísar ekki til ákveðinnar tækni við undirskrift, eins og hið síðarnefnda gerir. Í löggjöf eru núna hugtökin stafræn undirskrift og rafræn undirskrift notuð jöfnum höndum. Þó hefur þróunin verið sú undanfarið að almennt er notað hugtakið rafræn undirskrift, enda samrýmist það betur þeirri stefnu við lagasetningu að hafa tæknilegt hlutleysi að leiðarljósi til að hamla ekki gegn þróun. Í ákvæðum frumvarps þessa verður hugtakið rafræn undirskrift notuð og er þá vísað til hugtaksins í þrengri merkingu.

3.2. Dulritun og stafrænar undirskriftir.

Í öllum nútímaaðferðum er notast við dulritun til að búa til og sannreyna rafrænar undirskriftir. Með hvers konar dulritun er upplýsingum komið þannig fyrir að þær eru eingöngu skiljanlegar þeim sem hefur undir höndum viðeigandi dulmálslykil. Stafrænar undirskriftir grundvallast í stuttu máli á þeirri hugmynd að persónuleg staðfesting sé send með þeim hætti að viðtakandi geti sannreynt að hún stafi frá tilteknum aðila en jafnframt þannig að viðtakanda sé ekki unnt að senda gögn áfram og gefa til kynna að hann sé hinn upprunalegi sendandi.

Ein algengasta aðferðin við að búa til rafrænar undirskriftir er með svokölluðu dreifilyklakerfi. Þá er notuð tiltekinn algóritmi (e. algorithm) sem býr til mismunandi en skylda lykla, sem kallaðir eru dreifilykill og einkalykill, með því að margfalda tvær stórar og mismunandi prímtölur. Annar lykillinn er notaður til að umrita undirskriftina í dulmál, þ.e. dulrita (e. encipher), en hinn er notaður til að lesa úr dulmálinu þ.e. dulráða (e. decipher) og sannprófa undirskriftina.

Notendur slíkra undirskrifta fá útgefna til sín ofangreinda tvo lykla, þ.e. einkalykil og dreifilykil. Gert er ráð fyrir að dreifilyklinum sé dreift með því að senda hann með þeim gögnum sem undirrituð eru hverju sinni eða láta hann í vörslur þriðja aðila sem síðan veitir aðgang að honum, t.d. á netinu. Einkalyklinum verður eigandinn að halda leyndum. Einkalykillinn getur verið geymdur á margan hátt, t.d. á snjallkorti, símakorti eða í minni tölvu.

Þegar sendandi undirritar gögn eða einhvers konar upplýsingar afmarkar hann fyrst það efni sem hann ætlar að staðfesta með undirskriftinni. Að því loknu skipar hann tölvunni að tæta upplýsingarnar sem skapar tiltekið tætigildi. Tölvan dulkóðar síðan tætigildið með einkalykli sendanda, þannig að út komi hin rafræna undirskrift. Það tryggir að móttakandi sé viss um að sendandi hafi sent skeytið, þar sem eingöngu er unnt að dulráða sendinguna með dreifilykli sendanda.

Við tætingu er notaður algóritmi, sem virkar eingöngu í aðra áttina, þ.e. ekki er unnt að afbrengla tætigildið til þess að sjá upplýsingarnar sem hafa verið tættar. Því eru læsileg gögn (ódulrituð og ekki tætt) send með rafrænu undirskriftinni.

Ef sendandinn ákveður að dulrita gögnin með dreifilykli móttakanda er aðeins hægt að dulráða gögnin með einkalykli móttakandans. Innihaldið er því dulritað á þann hátt að enginn annar en móttakandinn sem hefur einkalykilinn getur lesið þau.

Tölva móttakandans tekur við skeytinu og notar dreifilykil sendandans til að leysa úr dulritun undirskriftarinnar með því að finna tætigildi hennar. Því næst eru gögnin tætt með sama algóritmanum og sendandi notaði við tætinguna. Loks ber móttakandi tætigildin saman. Ef gögnunum hefur verið breytt í sendingunni eru tætigildin ekki hin sömu.

3.3. Vottun á rafrænum undirskriftum – vottunaraðilar.

Vottunaraðili er sérstakur þriðji aðili í samskiptum milli undirritanda og móttakanda sem báðir treysta. Hann vottar að dreifilykillinn stafi í raun frá undirritanda og móttakandi geti þannig treyst rafrænu undirskriftinni. Þetta ferli gerir það að verkum að aðili getur verið viss um að sendandi sé sá sem hann segist vera.

Í frumvarpi þessu eru settar reglur um tiltölulega nýja gerð af þjónustu, þ.e. starfsemi vottunaraðila. Til að tryggja eftirfylgni við reglur frumvarpsins er sett á fót sérstakt eftirlit sem Löggildingarstofa mun rækja. Þá mun Persónuvernd hafa eftirlit með því að vottunaraðilar hagi meðferð persónuupplýsinga í samræmi við 5. gr. frumvarpsins og laga nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga.

3.4. Vottorð.

Þegar undirritandi sendir undirrituð gögn getur hann sent vottorð með sem hefur að geyma dreifilykilinn hans og upplýsingar um undirritanda. Þannig er hægt að tengja tiltekna persónu við dreifilykilinn.

Almennt eru í vottorði upplýsingar um það hver undirritandi er og gildistíma undirskriftar. Auk þess er mögulegt að nota vottorð við mismunandi viðskipti og vista þar viðeigandi upplýsingar, t.d. um virðisaukaskattsnúmer, umboð undirritanda, sérstök leyfi og takmarkanir gildissviðs vottorðsins.

Til eru margir staðlar um það hvaða upplýsingar má eða hægt er að gefa í vottorði og hvernig þær skuli settar fram, t.d. alþjóðlegi staðallinn X.509. Í frumvarpinu eru settar reglur um það hvað skuli koma fram í svokölluðu fullgildu vottorði, en þær eiga sér ekki hliðstæðu í gildandi staðli.

Eins og fram hefur komið er hægt að dreifa vottorði með ýmsu móti, t.d. með því að birta það í þar til gerðum rafrænum skrám sem eru gerðar opinberar. Yfirleitt sendir sá sem undirritar rafræn gögn vottorðið með opinbera lyklinum með gögnunum sem hann undirritar.

Undirritandi getur gefið mismunandi upplýsingar um sig. Hann getur t.d. komið fram í eigin nafni, undir dulnefni eða sem fyrirsvarsmaður einhvers annars, t.d. fyrirtækis. Vottorð sem gefið er út til undirritanda vegna umboðs hans eða stöðu nefnast „stöðuvottorð“. Í slíku vottorði þarf ekki að koma fram nafn undirritanda heldur staða hans, t.d. að hann sé framkvæmdastjóri tiltekins

fyrirtækis. Vottorð geta einnig verið gefin út til einstaklinga á grundvelli starfsheitis þeirra, t.d. lækna eða endurskoðenda. Slík vottorð kallast „starfsheitisvottorð“. Í sumum tilvikum er ekki nauðsynlegt að vita nákvæmlega hver undirritandi er, en mikilvægt að fá upplýsingar um starfsheiti hans eða stöðu. Í þeim tilvikum geta stöðu- eða starfsheitisvottorð verið fullnægjandi.

Í vottorðinu ábyrgist vottunaraðilinn að það sé tiltekin persóna sem hafi forræði yfir viðkomandi einkalykli. Vottunaraðilinn undirritar þau vottorð sem hann gefur út með einkalykli sínum. Með þessu er tryggt að ekki sé unnt að breyta upplýsingum í vottorði. Þurfi að breyta slíkum upplýsingum þarf að afturkalla vottorðið og gefa út nýtt. Að sama skapi getur móttakandi treyst því að vottunaraðilinn sé raunverulega sá sem hann segist vera, ef unnt er að nota dreifilykil vottunaraðila til að dulráða vottorð sem hann hefur undirritað með einkalykli sínum. Dreifilykill þessi getur síðan verið vottaður af öðrum vottunaraðila. Þetta er grundvallaratriði í dreifilyklakerfi, þ.e. byggð er upp keðja af vottorðum sem endar í svokallaðri rót. Með þessu er reynt að tryggja að í keðjunni sé alltaf aðili sem sá sem reiðir sig á vottorð telur sig geta treyst.

Til eru margar tegundir vottorða sem endurspegla mismunandi öryggisstig. Þannig getur vottunaraðili gefið út vottorð með lágu öryggisstigi, þar sem einungis er krafist að undirritandi láti í té gilt tölvupóstfang. Hins vegar getur verið krafist persónulegrar nærveru undirritanda og viðurkenndra persónuskilríkja áður en vottorð er gefið út sem telst uppfylla strangar öryggiskröfur. Eins og áður er getið er í frumvarpi þessu að meginstefnu til fjallað um fullgild vottorð sem uppfylla tilteknar strangar öryggiskröfur.

3.5. Vottunarstefna og vottunarframkvæmd.

Í vottunarstefnu (e. Certification Policy) kemur fram hvernig stefnt er að því að standa að útgáfu og meðferð stafrænna vottorða. Í vottunarstefnu eru líka settar reglur um þær kröfur sem gerðar eru í þjónustunni til öryggis og eftirlits.

Vottunarframkvæmd segir fyrir um hvernig vottunaraðili framkvæmir útgáfu vottorða. Vottunaraðili gefur gjarnan út skriflegar upplýsingar um þessa framkvæmd (Yfirlýsing um framkvæmd vottunarstefnu, e. Certification Practice Statement) þar sem fram koma upplýsingar um hvernig vottunaraðilinn framkvæmir vottunarstefnu sína.

3.6. Vandamál við notkun rafrænna undirskrifta.

Hafa verður í huga að tæknileg þróun á sviði rafrænna undirskrifta er mjög hröð og að rafræn undirskrift sem telst örugg núna verður kannski ekki örugg gegn fölsun síðar. Því getur reynst erfitt að sanna að undirskrift, byggð á vottorði sem fallið er úr gildi, stafi frá undirritanda. Þetta getur haft áhrif á sönnunarmat rafrænna undirskrifta vegna samninga sem hafa langan gildistíma. Í slíkum tilvikum er nauðsynlegt að skrá í upphafi með hvaða hætti kennsl voru borin á undirritanda þegar samningurinn var gerður. Þá verða kerfi og búnaður aðila á þessu sviði að vera í stöðugri endurskoðun.

Viðauki 3.

Lausleg íslensk þýðing á völdum köflum úr viðaukum A og B úr útboði sænska ríkisins haustið 2001. Ekki er ábyrgst að númer kafla og málsgreina séu eins og í frumriti.
Til frekari skoðunar á útfærslu staðalkrafna er bent á viðauka C í sænska útboðinu á eftirfarandi vefstað: http://it-upphandling.statskontoret.se/Uhw/
Smellið á eftirfrandi atriði í hliðarvalreit vinstra megin:
- Aktuella upphandlingar
- Pågående upphandlingar
- Elektronisk identifiering 2001.

Veljið síðan Bilaga C úr ramma hægra megin á skjánum.

Kröfur vegna rafrænna kennsla, vottunar og undirskrifta.

Útboð F:168, viðauki A

Skýring: Kröfur í útboðslýsingunni eru ýmist **Skall** eða **Bör**. Þar sem stendur **Skall** við kröfu þarf hún skilyrðislaust að vera uppfyllt eigi tilboðið að koma til greina. **Bör** virðist vera umsemjanlegt. Við höfum þýtt Skall með **skal** og Bör annaðhvort með **ber** eða **ætti að** (ábyrgjumst ekki 100% nákvæmni).

Almennar kröfur. Rafræn kennsl

2 Almennar kröfur

2.1 Samningur – Almennt

2.11

Rammasamningur

Rammasamningur Statskontoret byggist á megintexta, almennum þjónustuskilyrðum, almennum skilyrðum fyrir ráðgjafaþjónustu og fylgiskjölum. Þær afurðir og þjónustur sem leiða af rammasamningi afhendist skv. þessum skilyrðum. Tilboðsgjafi skal í öllum aðalatriðum samþykkja rammasamninginn í heild. Í þeim tilvikum sem tilboðsgjafi leggur til breytingar á megintexta eða í almennum skilyrðum skulu breytingarnar settar upp sem tillögur að nýjum atriðum. Í þeim tilvikum þar sem tilboðsgjafi leggur fram sína eigin almennu skilmála mun Statskontoret ekki telja sig bundið af neinum ákvæðum þeirra.

1.1.2 Samband

Þessi krafa á við hluta A, borgaraskilríki (medoborgarcertificat).
Það ættu að vera greinileg tengsl milli rammasamnings, tilgreindra skilríkja og vottunarstefnu tilboðsgjafa, sem á að tryggja að skilríkin séu útfærð skv. kröfum þessa útboðs. Gerið grein fyrir þessum tengslum.

1.1.3 Eftirlit með afhendingu

Tilboðsgjafi skal samþykkja að utanaðkomandi eftirlitsaðili annist eftirlit með afhendingu til að sannreyna að tilboðsgjafi standi við skyldur sínar samkvæmt samningi, hvort heldur sem viðskiptavinur eða Statskonteret fer fram á það. Kostnaður við eftirlit skal borinn af viðskiptavininum nema tilboðsgjafinn vanræki verkkefni sitt á stórfelldan hátt.

1.2 Rafræn viðskipti (e-handel)

Með rafrænum viðskiptum er hér aðallega átt við eftirfarandi:
- einfalda pöntun á þeirri þjónustu og vörum sem eru skýrt skilgreindar í rammasamningi
- endurteknar pantanir á þeim afurðum sem skilgreind eru í undirliggjandi samningi um afhendingu
- yfirfærslu á pöntunarstaðfestingu með tölvupósti
- yfirfærslu upplýsinga um afhendingu, fylgiskjölum o.s.frv. með tölvupósti
- yfirfærslu upplýsinga um vöru viðkomandi afhendingar
- notendaþjónusta (help desk), villumeldingar og svörun í gegnum www og tölvupóst

Pöntunarform, auðkenni pöntunar og ógreiddir reikningar ættu að vera aðgengilegir á vefsetri tilboðsgjafa.

1.1.1 Rafræn viðskipti á interneti

R-verlsun í Rammasamningi ætti að vera möguleg í gegnum internetið í síauknum og vaxandi mæli.

2.3 Menntun

2.3.1 Menntun

Á samningstímanum skal tilboðsgjafi uppfylla kröfur þess sem pantar varðandi menntun og upplýsingagjöf varðandi þjónustu og vörur sem í boði eru.

2.3.2 Kennslugögn

Öll kennslugögn og upplýsingaefni ættu að vera á sænsku

2.3.3 Tungumál

Námskeið og upplýsingar eiga að vera á sænsku

2.3.4 Fræðsla

Gerið í stuttu máli grein fyrir þeirri fræðslu sem í boði eru ásamt upplýsingum um hver annast þá fræðslu.

2.4 Samverkun o.fl.

2.4.1 Samverkun milli tilboðsgjafa

Þessi krafa á við hluta A, boragaraskilríki.
Almenningur á aðeins að þurfa skilríki frá einum tilboðsgjafa rammasamnings til að auðkenna sig gagnvart öllum rafrænum þjónustum hins opinbera á internetinu. Til að uppfylla þessa kröfu þurfa allar opinberar stofnanir sem bjóða upp á rafræna þjónustu á internetinu annaðhvort að gera samning við alla tilboðsgjafa ellegar að allir tilboðsgjafar rammasamnings vinni þannig saman að stofnum sem ber traust til eins tilboðsgjafa geti einnig borið traust til allra hinna. Þegar fram í sækir er reiknað með að samvinnuútfærslan muni verða notuð, sjá hugsanlegar leiðir til útfærslu í fskj. H.

Tilboðsgjafa ber að hafa samvinnu við aðra tilboðsgjafa um ráðstafanir til þess að hver stofnum þurfi einungis að gera samning við einn tilboðsgjafa rammasamnings til að fá aðgang að öllum þeim upplýsingum sem nauðsynlegar eru til að hægt sé að treysta skilríkjum gefnum út af hverjum tilboðsgjafanna sem er.
Greið grein fyrir:

- hvernig sú lausn sem í boði er uppfylli slíka samvinnu milli tilboðsgjafa
- hvernig tilboðsgjafinn ætlar að stuðla að því að slík samvinna komist á
- hugsanleg vandkvæði eða annmarkar á því að slík samvinna geti gengið.

2.4.2 Samstarfsaðilar

Lýsið samstarfsaðilum ef einhverjir eru og þeim samningum sem í gildi eru eru við þá.
Gerið grein fyrir í hvaða tilvikum þið munuð nota samstarfsaðila/undirverktaka

1.3.3 Útbreiðsla

Þessi krafa gildir einungis í Hluta A, borgaraskilríki

1.3.3.1 Útbreiðsla

Tilboðsgjafa ber með hjálp þeirrar þjónustu sem hann veitir að stuðla að því að rafrænar þjónusta hins opinbera komist fljótt í gagnið. Gerið grein fyrir:

- hvernig tilboðsgjafinn hyggst vinna að þessu, þróunaráætlunum, fyrirliggjandi reynslu af vinnu með og í tengslum við almenning og fyrirtæki, ásamt því hvernig nýta megi þetta í þeim tilgangi að ná þeirri útbreiðslu sem óskað er eftir
- Hversu margir einstaklingar hafa fengið vottorð nú þegar sem uppfylla þær kröfur sem settar eru fram í þessum spurningalista?

- Hversu langur er afhendingartími fyrir almennan borgara sem þiggur boð um vottorð þar til hann getur byrjað að nota það?
- Afkastageta tilboðsgjafans við framleiðslu á skilríkjum.

5.1.1.1 Búnaður

Tilboðsgjafa ber að ráða yfir nauðsynlegum búnaði og skipulagi til að dreifa án tafar skilríkjum til einstaklinga óháð búsetu viðkomandi.
Gerið grein fyrir því hvort þannig sé ástatt með tiltekna landshluta eða þjóðfélagshópa að tilboðsgjafi hafi takmarkaða getu til að afhenda þeim skilríki án tafar.

Útboð F:168, viðauki B
Tæknilegar kröfur. Rafræn kennsl

2 Umfang, afmörkun og samspil
2.1 PKI

Tilboðsgjafi skal afhenda lausn sem byggir á brenglun með einka- og dreifilykli eða s.k. Public Key Infrastructure (PKI)

5.2 Samvinnuvettvangur

Tilboðsgjafi skal vera reiðubúinn að taka þátt í samvinnu við aðra tilboðsgjafa og stofnanir undir stjórn einnar stofnunar.

2.2.1 Notendaráð

Tilboðsgjafa ber að koma upp samráðshópi notenda. Notendaráð skal vera einn af þeim starfsþáttum sem tilboðsgjafi kemur upp til að vinna með viðskiptavinum sínum varðandi framþróun og viðhald þeirra þjónustu sem í boði er skv. Rammasamningi.

2.2.2 Notendaráð – viðhaldsaðgerðir

Notendaráði ber að taka þátt í viðhaldsaðgerðum skv. samningi og skal kalla ráðið saman í tengslum við allar stærri breytingar á þjónustu eða forritum, þó ekki sjaldnar en tvisvar á ári.

3. Kröfur til skilríkja og þjónustu
3.1 Tegundir skilríkja

Til þess að geta komið upp PKI þurfa stofnanir að minnsta kosti 3 mismunandi gerðir skilríkja:
- Borgaraskilríki
- Netþjónaskilríki
- Skilríki til nota fyrir rafræna undirskriftir hjá stofnunum (stimpil)

3.1.1 Borgaraskilríki

Tilboðsgjafi skal bjóða borgaraskilríki skv. 3.8.1

2.1.2 Netþjónaskilríki

Tilboðsgjafa ber að bjóða upp á netþjónaskiríki skv. 3.8.2

2.1.3 Rafræn undirskriftarskilríki hjá opinberum stofnunum

Tilboðsgjafa ber að bjóða rafræn undirskriftaskilríki (stimpilskilríki) skv. 3.8.3. Gerið grein fyrir með hvaða hætti það gæti gerst.

2.2 Grundvallar öryggiskröfur til skilríkja
2.1.1 Borgaraskilríki
2.1.1.1 Ein skilríki fyrir brenglun og önnur fyrir undirskrift

Tilboðsgjafi skal útvega einstaklingum tvenn skilríki; ein fyrir brenglun og önnur fyrir undirskrift. Gildissvið viðkomandi skilríkja og samsvarandi einkalykils skal koma fram í því svæði vottorðs er kallast “KeyUsage”. Sjá skilgreiningu 3.8.1

2.1.1.2 Hver skilríki skulu vera bundin tilteknum einstaklingi

Viðkomandi ilríki skal aðeins tiltekinn einstaklingur geta notað.
Tilboðsgjafi skal ábyrgjast að:

- samningur sé gerður við skilríkjahafa
- skilríkjahafi sé uppfræddur um skyldur og áhhættu samfara meðhöndlun skilríkja og einkalykla
- skilríkjahafi fái einkalykla afhenta undir ströngu eftirliti
- Skilríkjahafa sé útvegað forrit og búnað sem stuðlar að vernd einkalykils og þess tölvuumhverfis þar sem einkalykill er notaður.
- Skilríkjahafi fái aðgang að raunhæfum aðferðum til að loka skilríkjum á hraðvirkan hátt

7.1.1.1 Hver skilríki gera kleift að auðkenna réttan aðila

Það þýðir að tilboðsgjafi skal:

- bera kennsl á einstaklinginn skv. 3.4.1
- útbúa skilríki með kennitölu eða öðru einkvæmu auðkenni sem viðkomandi þjónusta tilboðsgjafa getur túlkað yfir í kennitölu jafn skjótt, öruggt og snurðulaust eins og ef kennitala væri í skírteini
- Framkvæma reglulega afstemmingu gagnvart opinberum skrám, t.d. þjóðskrá, gagnvart afskráningu o.þ.h. og loka skilríkjum hafi viðkomandi opinberar upplýsingar breyst.

3.2.1.4

Gefið upp tegund auðkennis sem notað verður í skírteini, kennitölu eða annað einkvæmt auðkenni.

4.1.1.1 Kennsl og undirskrift útfærist með aðferðum sem skilríkjahafi einn stjórnar

Tilboðsgjafi skal útvega skilríkjahafa:

- hjálpartól, t.d. forrit og aðferðir, til að tryggja öryggi þegar hann notar skilríkin til kennsla, undirskrifta eða brenglunar gagna skv. 3.6.2
- sérstakan lykil fyrir undirskrift
- sérstakt PIN fyrir hvern lykil

4.1.1.1 Undirskrift er bundin öðrum rafrænum gögnum á þann hátt að upp komist hvort þeim hafi verið spillt

Tilboðsgjafi skal sjá skilríkjahafa fyrir hjálpartólum svo hann geti undirritað skjöl rafrænt og sannvottað rafrænar undirskriftir.

4.1.1.2 Unnt þarf að vera að skiptast á brengluðum gögnum

Tilboðsgjafi skal sjá skilríkjahafa fyrir hjálpartólum sem gera honum kleift að brengla gögn sem ekki eru ætluð fyrir augu allra.

3.2.1.7

Tilboðsgjafi skal ekki útfæra “mjúk” skilríki með lengri gildistíma en 2 ár.

3.2.1.8

Tilboðsgjafi skal ekki útfæra “hörð” skilríki til lengri tíma en 5 ára.

3.2.1.9

Lyklar skilríkjahafa skulu vera byggðir upp með RSA með 1.024 bitum

4.1.2 Netþjónavottorð

4.1.2.1 Eitt vottorð fyrir kennsl/brenglun

Tilboðsgjafi skal útvega stofnun eitt vottorð fyrir kennsl/brenglun. Gildissvið þeirra og viðkomandi einkalykils skal koma fram í því svæði vottorðsins er nefnist “keyUsage”. Sjá skilgreiningu 3.8.2

2.2.2.2 Hvert vottorð er bundið einum og aðeins einum netþjóni

Einkalykill sem tilheyrir vottorðinu skal vera aðgengilegur tilteknum netþjóni og engum öðrum.

Tilboðsgjafi skal beita eftirfarandi vinnureglum:

- gera samning við vottorðshafa
- upplýsa vottorðshafa um kröfur og áhættu samfara meðhöndlun skilríkja og einkalykla
- einkalykill skal afhentur undir ströngu eftirliti
- vottorðshafi hafi greiðan aðgang að aðferðum til að loka vottorði á skjótan hátt

2.1.1.3 Hvert vottorð gerir það kleift að auðkenna réttan netþjón stofnunar.

Þetta þýðir að tilboðsgjafi skal:

- sjá til þess að lyklar og vottorð séu einungis afhent þar til bærum fulltrúa viðkomandi stofnunar.
- skrá kennitölu stofnunar í vottorðið.

4.1.1 Rafræn undirskriftarskilríki stofnunar

Bjóði tilboðsgjafi skilríki til rafrænnar undirskriftar (stimpils) stofnunar gilda eftirfarandi kröfur

4.1.1.1 Eitt vottorð fyrir undirritun

Tilboðsgjafi skal útvega stofnun eitt eða fleiri vottorð fyir undirskriftir. Tilgangurinn með vottorðinu og tilheyrandi einkalykli skal koma fram í svæðinu “KeyUsage”. Sjá skilgreiningu 3.8.3

4.1.1.2 Sérhvert vottorð er aðeins bundið einni stofnun eða tilteknu starfssviði stofnunar.

Einkalykill tilheyrandi slíku vottorði skal ekkivera aðgengilegur öðrum en þeirri tilteknu stofnun eða því tiltekna starfssviði.

Tilboðsgjafi skal setja verkferla þannig að:

- samningur sé gerður við vottorðshafa
- vottorðshafi sé upplýstur um kröfur og áhættu við meðhöndlun vottorðs og einkalykils því tilheyrandi
- einkalykill sé afhentur undir ströngu eftirliti
- vottorðshafi hafi greiðan aðgang að aðferðum til að gera vottorð óvirkt á fljótlegan hátt.

8.1.1.1 Hvert vottorð gerir kleift að bera kennsl á rétta stofnun eða tiltekið starfssvið viðkomandi stofnunar

Þettta þýðir að tilboðsgjafis skal:

- sjá til þess að lykill og vottorð séu eingöngu afhent þar til bærum fulltrúa viðkomandi stofnunar.
- skrá kennitölu stofnunar í vottorðið.

3.1.1 Fullgild rafræn undirskrift

Tilboðsgjafa ber að geta afhent vottorð og búnað til öruggra undirskrifta sem fullnægi skilyrðum um fullgilda rafræna undirskrift skv. lögum (SFS 2000:832) um fullgildar rafrænar undirskriftir.

3.1.2 Kröfur um vottunarstefnu

Grundvöllur þeirra krafna sem settar eru varðandi umsýslu og verklag tilboðsgjafa varðandi starfrækslu vottunarmiðstöðvar (CA) er sá staðall fyrir vottorðastefnu sem þróaður hefur verið innan evrópsku staðlanefndarinnar ETSI: “Policy requirement for certifaction authorities issuing qualified certificates”. ETSI TS 101 456, hér eftir nefnt ETSI-stefnan. ETSI-stefnan er notuð hér í víðu samhengi, þ.e.a.s. jafnvel fyrir vottortð sem ekki eru fullgild. ETSI-stefnuna er einnig heimilt að nota fyrir vottorð sem fylgja lyklum til að bera kennsl á eða yfirfæra brenglunarlykla.

Tilboðsgjafi ætti að uppfylla kröfur ETSI-stefnunnar í starfrækslu vottunarstöðva sinna.

3.2.5.1

Tilboðsgjafi skal láta fylgja með tilboði þær aðgerðir sem mynda vottunarstefnu og yfirlýsingu um framkvæmd vottunarstefnu fyrir vottorð sem vísað er til í svæði vottorðsins fyrir OID (certificatePolicy)

2.1.4.2 Kröfur um endurskoðun.

Endurskoðun á því að hve miklu leyti starfsemi vottunarstöðva (CA) tilboðsgjafa sé í samræmi við útgefna skilmála skal eiga sér stað á minnst 36 mánaða fresti og vera framkvæmd af óháðum þar til bærum eftirlitsaðila. Þess skal gætt að:

Niðurstöður séu aðgengilegar að ósk hvers þess sem treysta þarf vottun

- Áætlanir séu gerðar um aðgerðir til úrbóta ef misbrestir finnast.

3.1 Kröfur til vottunarstöðva

2.2.1 Gæðaviðmiðun

Tilboðsgjafi skal hafa í frammi viðurkenndar og reyndar aðferðir, verkferla og starfsreglur til að tryggja vönduð vinnubrögð.

2.2.2

Tilboðsgjafa ber að viðhafa í vottunarstöð sinni gæðakerfi skv. EN/ISO- vottun eða hliðstætt vel skilgreint gæðakerfi eða skjalfesta áætlun sem uppfyllir þessa kröfu.

2.2.3 Öryggisviðmiðanir

Tilboðsgjafa ber í vottunarstöð sinni að hafa kerfi til stjórnunar á öryggi upplýsingakerfa samsvarandi ISO/IEC 17799:2000.

Tilboðsgjafa ber í vottunarstöð sinni að fylga FA22, þ.e.a.s. fyrirmælum sem "Overstyrelsen for civil beredskap, OCB" gefur út um grundvallaröryggi fyrir þjóðfélagslega mikilvæg tölvukerfi hjá hinu opinbera (ÖCBFS 1998:1).

3.3.3.1

Sérhver tilboðsgjafi sem býður í þessa þjónustu þarf að vera meðvitaður um að boðnar lausnir kunna að verða notaðar við þjóðfélagslega mikilvæga starfsemi þar sem sérstakar kröfur eru gerðar. Tilboðsgjafi skal geta skuldbundið sig til að halda uppi samningsbundnu öryggisstigi samkvæmt sérstökum "öryggisverndarsamningi".

2.2.4 Kröfur um framleiðslu

3.3.4.1 Lyklar vottunarmiðstöðvar (CA-lyklar, CA-keys)

Framleiðsla lykla ætti í höfuðatriðum að fylga ETSI-stefnu kafla 7.2. Kafli 7.2.9 á einungis við þegar lyklar eru innbyggðir í sérstakan vélbúnað.

3.3.4.2

Tilboðsgjafa ber að vinna skv. viðteknum aðferðum við meðhöndlun einkalykils vottunarmiðstöðvarinnar, sem m.a. felur í sér:

- Að CA-lykill sé RSA lykill með 2048 bitum
- Að CA-lykill sé í gildi í 5 ár að hámarki.
- Að þegar vottunarmiðstöð skiptir út einkalykli sé það gert með sannreyndum og vel skjöluðum aðferðum (key rollover).
- Að skilríki vottunarmiðstöðvar séu í gildi í 10 ár að hámarki.

4.1.1 Færsla dagbókar

Tilboðsgjafa ber í rekstri vottunarmiðstöðvar að færa í dagbók (logga) öll mikilvæg atvik er snúa að öryggi skv. Kafla 7.4.11 í ETSI-stefnunni.

4.1.2 Útgáfa og aðgangur að upplýsingum

Tilboðsgjafi skal sjá til þess að eftirfarandi skjöl og upplýsingar verði aðgengileg:

- ✓ vottunarstefna og önnur skjöl sem lýsa vinnubrögðum vottunarmiðstöðvarinnar
- ✓ upplýsingar um ógildingu vottorða, skv. kröfum undir lið 3.5.1

✓ vottorð vottunarmiðstöðvarinnar

3.3.6.1

Tilboðsgjafi skal ekki birta vottorð sem innihalda kennitölur í opinberum skrám.

3.3.6.2

Tilboðsgjafi skal vera reiðubúinn að aðstoða með fljótvirkum hætti við allar þær aðgerðir sem krafist er í lögum, reglugerðum, dómsúrskurðum eða með öðrum stjórnvaldsákvörðunum.

4.1.3 Varðveisla

Tilboðsgjafi skal skjala alla þætti líftíma vottorðs þannig að rekjanleiki haldist.
Skjölun á líftíma vottorðs ber að framkvæma þannig að hún:

- sé aðgengileg, án viðbótarkostnaðar, að minnsta kost þeir hlutar sem kaupandi þarf á að halda
- sé rýnd og endurskoðuð reglulega
- sé viðhaldið með útgáfustýringum
- sé grisjuð reglulega skv. áætlun sem sett er upp í samráði við kaupanda.
- sé varðveitt hjá tilboðsgjafa

3.3.7.1

Tilboðsgjafi skal geta afhent varðveitt efni í lesanlegu formi á umsömdum geymslutíma

3.3.7.2

Tilboðsgjafi ætti að geta afhent skv. beiðni gögn til opinberra aðila til varðveislu þar

3.3.7.3

Komi til þess að tilboðsgjafi hætti starfsemi vottunarmiðstöðvar ætti varðveitt skjölun að afhendast skv. kafla 3.7.

5.1 Kröfur um umsóknir og afhendingu

Tilboðsgjafi skal í þeim tilfellum sem kaupandi framleiðir sjálfur sína lykla, hafa eftirlit með að kaupandi noti einkalykil samsvarandi dreiflyklinum sem er í vottorði hans.

5.1.1 Borgaraskilríki

Tilboðsgjafi skal sjá til þess að þegar um er að ræða vottorð ætlað einstaklingi:

1. sé einstaklingurinn greinilega auðkenndur skv. opinberum persónuupplýsingum, beint með kennitölu eða með öðru einkvæmu auðkenni.
2. séu þær upplýsingar sem nota þarf um einstaklinginn sannreyndar gagnvart opinberum skrám (t.d. SPAR)
3. séu vottorð og tilheyrandi einkalyklar afhent á þann hátt að einstaklingur geti hvorki nálgast þau né notað nema áður hafi verið borin kennsl á hann með skilríkjum samþykktum af SIS eða á annan hátt í samræmi við kröfur SIS um persónuauðkenningu
4. séu vottorð og tilheyrandi einkalyklar afhent á þann hátt að einstaklingur geti ekki notað þau fyrr en eftir að hann hefur undirritað samning við tilboðsgjafa með rafrænum hætti eða skrifað undir á hefðbundinn hátt (sjá atriði 3.4.4)
5. séu „virkjunargögn“ (t.d. PIN) og vottorð/lyklar afhent vottunarhafa eftir aðskildum dreifileiðum (tölvupósti, bréf eða SMS osfrv).

5.1.1.1 Borgaraskilríki með einkvæmu auðkenni

Í þeim tilfellum þar sem lausn tilboðsgjafa reiknar ekki með kennitölu í boragaraskilríkjum heldur vísar í hana með einkvæðum lykli skal tilboðsgjafi:

- Stinga upp á einkvæmum auðkennum sem komi í stað kennitölu í vottorðum þannig að sjálfvirk uppfletting á réttri kennitölu verði svo hraðvirk, örugg og sveigjanleg sem unnt er. Statskontoret mun leita eftir samræmdum lausnum á slíkum auðkennum og setja nánari reglur í rammasamningi.
- Koma með tillögur um samskiptareglur, skilgreiningar og rútínu, sem opinberar stofnanir þurfa til að sækja rétta kennitölu þannig að sjálfvirk uppfletting kennitölu verði verði svo hraðvirk, örugg og sveigjanleg sem unnt er. Statskontoret mun leita eftir samræmdum lausnum fyrir samskiptalausnir, skilgreiningar og rútínur og setja nánari reglur í rammasamning.
- Viðhalda lista yfir tengsl milli einkvæms auðkennis og kennitölu

- Hafa aðgengilega þjónustu þar sem opinberar stofnanir geta sótt á rauntíma rétta kennitölu til einkvæðrar auðkenningar með álíka auðveldum hætti og þær sækja upplýsingar um lokuð vottorð.

1.4.1 Netþjónavottorð

Bjóði tilboðsgjafi netþjónavottorð gilda eftirfarandi kröfur:
Tilboðsgjafi skal sjá til þess að eftirfarandi gildi um vottorð sem ætlað er til að auðkenna netþjón í opinberri stofnun:

1. netþjónn sé greinilega auðkenndur með léni (DNS host name)
2. aðgengilegar upplýsingar um netþjóninn séu sannreyndar gagnvart lénaskrá
3. vottorð og tilheyrandi einkalyklar séu afhent á þann hátt að einstaklingur geti ekki haft aðgengi eða geti notað það í netþjóni án þess að borin hafi verið kennsl á hann sem fullgildan fulltrúa viðkomandi stofnunar á þann hátt sem SIS telur fullnægjandi eða á annan þann hátt sem samsvarar kröfum SIS til auðkenningar
4. vottorð og tilheyrandi einkalykar séu afhentir á þann hátt að þau verði ekki notuð í netþjón fyrr en eftir að þar til bær fulltrúi stofnunar hefur móttekið upplýsingar um hvernig og til hvers megi nota vottorð og lykla, og hefur undirritað samning við tilboðsgjafa með rafrænum hætti eða skrifað undir hann á hefðbundinn hátt

4.1.1 Rafræn undirskrift stofnunar

Bjóði tilboðsgjafi vottorð fyrir rafræna stofnunarundirskrift gilda eftirfarandi kröfur:
Tilboðsgjafinn skal sjá til þess að eftirfarandi gildi um vottorð sem ætlað er sem rafrænn stimpill/undirskrift stofnunar:

1. stofnun sé greinilega auðkennd með stofnunarnúmeri
2. Þær upplýsingar sem á þarf að halda um stofnunina séu sannreyndar á móti opinberri stofnanaskrá
3. vottorð og tilheyrandi einkalyklar séu afhent á þann hátt að einstaklingur geti ekki haft aðgengi eða geti notað það án þess að borin hafi verið kennsl á hann sem fullgildan fulltrúa viðkomandi stofnunar á hátt sem SIS telur fuillnægjandi, eða á annan þann hátt sem samsvarar kröfum SIS til auðkenningar
4. vottorð og tilheyrandi einkalykar séu afhent á þann hátt að þau verði ekki notuð fyrr en eftir að þar til bær fulltrúi stofnunarinnar hefur móttekið upplýsingar um hvernig og til hvers megi nota vottorð og lykla, og hefur undirritað samning við tilboðsgjafa með rafrænum hætti eða skrifað undir hann á hefðbundinn hátt

4.1.1 Kröfur um samning við vottorðshafa

Tilboðsgjafi skal gera samning við vottorðshafa og upplýsa hann á skýran og auðskilinn hátt um samninginn og innihald hans ásamt hugsanlegum takmörkunum á notkun vottorðsins.

3.4.4.1

Í samningi tilboðsgjafa og vottorðshafa ber að taka fram:

b. að vottorðshafi varðveiti lykla í því umhverfi sem fyrir er mælt
c. að vottorðshafi noti viðeigandi hugbúnað við undirskrift og kennsl
d. að vottorðshafi geri viðeigandi ráðstafanir til þess að aðeins hann/hún hafi aðgang að sínum einkalyklum
e. að vottorðshafi skipti út aðgangsorði við fyrstu hentugleika ef upphaflegt aðgangsorð er fengið frá vottunarmiðstöð
f. að vottorðshafi fari tafarlaust fram á ógildingu vottorðs vakni einhver grunur um misnotkun eða þvíumlíkt
g. að vottorðshafi upplýsi vottunarmiðstöð tafarlaust ef innihald vottorðs er ekki lengur í gildi eða því hefur verið breytt.
h. Að vottorðshafi verndi sérhvern einkalykil með sérstöku PIN númeri

Leggið fram uppkast að samningi sem inniheldur ofangreinda punkta.

4.8.1 Endurnýjun vottorðs.

Tilboðsgjafa ber að bjóða endurnýjun vottorðs í samræmi við þær reglur sem lýst er í ETSI-stefnunni í kafla 7.3.2

4.8.2 Afhendingartímar

Tilboðsgjafa ber að afhenda vottorðshafa vottorð og þau hjálpartól sem nauðsynleg eru til að hægt sé að ná sambandi við rafrænar þjónustur hins opinbera sem fyrst eftir að umsókn berst. Gerið grein fyrir afhendingartímum fyrir viðkomandi afurðir og þjónustu.

4.8.3 Varnaraðgerðir gegn því að einkalykill komist í hendur annarra

Tilboðsgjafi ábyrgjast að engir einkalyklar í hans vörslu verði afritaðir og varðveittir (s.k. “key escrow”) til síðari nota.

3.4.7.1

Ef tilboðsgjafi framleiðir einkalykla viðkomandi skírteinishafa ber honum að verja þá þannig að þeir komist ekki fyrir augu eða í hendur annarra. Gerið grein fyrir því hvernig það er tryggt.

3.4.7.2

Tilboðsgjafa ber að bjóða þann valkost að afhenda einkalykil innbbyggðan í vélbúnað (hardware-based)

3.4.7.3

Tilboðsgjafa ber að geta boðið hópum einstaklinga rafræna skilríkjameðferð byggða á gjörvakortum með eiginleikum skv. 3.6.3 fari stofnun fram á slíkt.

Gerið grein fyrir:

- Er hægt að útbúa gjörvakort þannig að yfirborð þess sé hægt að nota sem persónuskilríki samkvæmt kröfum SIS?

1.1.1 Kröfur til þjónustu og virkni

3.5.1 Lokunarþjónusta

Tilboðsgjafi skal hafa aðgengilegar lokunarupplýsingar fyrir öll lokuð vottorð með CRL skv. X.509 eða skv. OCSP-samskiptastaðli.

3.5.1.1

Tilboðsgjafa ber að hafa tiltækar lokunarupplýsingar skv. OCSP-samskiptastaðli

3.5.1.2

Tilboðsgjafa ber að hafa tiltæka lokunarþjónustu sem meðal annars tekur á móti lokunarbeiðnum allan sólarhringinn, kl. 00-24, 7 daga í viku með svartíma undir 10 mínútum jafnvel á mestu álagstímum.

3.5.1.3

Tilboðsgjafa ber að sjá til þess að lokunarupplýsingar sem haldið er til haga skv. 3.5.1 séu uppfærðar að minnsta kosti einu sinni á klst. allan sólarhringinn.

3.5.1.4

Aðferðir tilboðsgjafa til að birta upplýsingar um ógild vottorð skulu vera á mjög aðgengilegu formi. Gerið grein fyrir útfærslu.

3.5.1.5

Tilboðsgjafa ber að bera vottorðið reglulega saman við opinberar skrám (t.d. þjóðskrá) og loka vottorði sem inniheldur rangar upplýsingar. Gerið grein fyrir hversu oft slíkar afstemmingar verða gerðar.

3.5.2 Notendaþjónusta

Tilboðsgjafinn skal bjóða vottorðshöfum notendaþjónustu á sænsku.

3.5.2.1

Tilboðsgjafa ber að bjóða notendaþjónustu sem inniheldur uppsetningaraðstoð, skilgreiningaraðstoð, ásamt aðstoð við önnur álitamál sem upp koma varðandi þá þjónustu og vörur sem tilboðsgjafi selur.

Gerið grein fyrir hvernig notendaþjónustan er byggð upp, fjölda starfsmanna, staðsetningu, samskiptaleiðum ásamt skipuriti og gæðaeftirliti.

3.5.2.2

Tilboðsgjafinn skal bjóða aðgang að notendaþjónustu að lágmarki milli kl. 7.00- 22.00 á svartíma undir 10 mínútum jafnvel á mesta álagstíma.

3.5.3 Tímastimplanir

Tilboðsgjafa ber að bjóða upp á þá aðgerð að tímastimpla með eftirfarandi eiginleika:

- Styður tímastimplun með RSA-undirskrift
- Getur framkallað tímastimplunar- "token" skv. ósk, í samræmi við. PKIX
- Útbýr fyrir hvert nýtt tímastimplunar-"token" nýtt gildi með tíma og auðkenni.
- Tímastimplar eingöngu tætigildi (hash-value) viðkomandi skeytis.
- Notar sérstakan lykil sem er ætlaður eingöngu í það hlutverk að undirrita sérhvert tímastimplunar-"token".
- Er hægt að sannreyna að útreiknað tætigildi sé í samræmi við það tætialgrím sem notað er
- Getur bætt viðbótarupplýsingum í tímastimplunar-"token" sé þess óskað

Gerið grein fyrir hvenær og að hve miklu marki er hægt að uppfylla þessar kröfur.

7.1 Kröfur til vörunnar

7.1.1 Almennar kröfur

Eftirfarandi kröfur gilda þar sem við á fyrir allar vörur

Vörur tilboðsgjafa sem þurfa kann að setja upp í umhverfi vottunarhafa skulu:

- Vera á sænsku
- Vera í eftirfarandi tölvuumhverfi
  - Microsoft Windows ME/95/98
  - Microsoft Windows NT4
  - Microsoft Windows 2000
  - Apple Mac OS
  - Linux
- Afhendast með nauðsynlegum upplýsingum á sænsku

3.6.1.1

Gerið grein fyrir þeim kröfum sem að öðru leyti eru gerðar til hugbúnaðar og vélbúnaðar hjá vottorðshöfum til þess að boðnar lausnir virki.

6.1.1 Lyklameðhöndlun, kennsl og undirritun

Þær kröfur sem skilgreindar eru hér eiga við þá almennu virkni sem notandi þarf til að meðhöndla vottorð og lykla, t.d. viðbótarbúnað í vefrýni. Kröfurnar gilda án tillits til þess hvaða geymslumiðill er notaður fyrir einkalykil.

Virkni lausnar ber að uppfyll aeftirtalin skilyrði:

- Vera hreyfanleg, gera vottorðshafa mögulegt að vinna á mismunandi vinnustöðvum
- Sjá til þess að ekki sé unnt að nota lykla til annarra hluta en þeir eru ætlaðir til
- Sjá til þess að einkalyklar séu aðgangsvarðir með notkun PIN-kóða eða manngreiniaðferðum (biometrics [Tölvuorðasafn]).
- Styður notkun PIN númers að lágmarki 5 stafa langt.
- Styður notkun mismunandi PIN númera fyrir mismunandi lykla (kennsl/brenglun og undirskrift)
- Alltaf geta krafist upplýsinga um lokun skilríkja
- Geta meðhöndlað ósamhverfa lykla af gerðinni RSA með að lágmarki 1024 bita lyklalengd
- Sjá til þess að lykilorð, PIN númer og einkalyklar afmáist af öllum bráðabirgðageymslustöðum strax að lokinni notkun
- Virka með:
  - Internet Explorer 4.01 eða nýrra
  - Netscape 4 og nýrra
- Styðja SSL/TLS, Secure Socket Layer og Transport Layer Security
  -Triple-DES brenglun

- Styðja RSA vottun
- Krefjast þess að PIN sé slegið inn við hverja undirskrift
- Geta framleitt undirskrift skv. PKCS #7 v1.5; Cryptographic Message Syntax Standard og skv. RFC 2630; Cryptographic Message Syntax
- Geta framkallað fjölundirskriftir
- Styðja tætialgrímið SHA-1

9.1.1 Geymslumiðill í vélbúnaði (átt er við görvakort eða hliðstætt)

Bjóði tilboðsgjafi upp á geymslumiðil í vélbúnaði gildir eftirfarandi:
Geymslumiðillinn ætti að:

- Hafa notendaminni að lágmarki 16 Kbyte
- styðja PKCS#15 fyrir skilgreiningar á því hvernig lyklar, vottoð o.s.frv. er geymt
- geta meðhöndlað RSA lykla með 1024 bita lengd
- geta geymt að lágmarki 3 RSA lykla
- geta geymt að lágmarki 3 X-509 vottorð
- geta varið einkalykla gegn óheimilli notkun með því að krefjast innsláttar PIN
- leyfa mismunandi einkalykla varða með mismunandi PIN
- leyfa útskipti á PIN númeri eftir að rétt PIN númer hefur verið gefið upp
- Læsa geymslumiðli eftir skilgreinanlegan fjölda innsláttar með röngu PIN númeri
- Gera mögulegt að opna geymslumiðil aftur eftir að rétt PUK hefur verið gefið upp
- Styðja PIN lengd að lágmarki 5 stafi
- Koma í veg fyrir að hægt sé að lesa einkalykil eða að breyta honum
- Afhendast með þeim forritum og vélbúnaði sem þarf til að tengjast tölvubúnaði vottorðshafans.

21.1.1 Umhverfi notandans

Tilboðsgjafi skal bjóða aðferðir til verndar umhverfi notandans, svo sem:

- Staðbundinn eldvegg
- Vírusvörn
- Skeljavörn

3.7 Lokun þjónustu vottunarmiðstöðvar

Komi til að rekstur vottunarmiðstöðvar leggist niður ber að fylgja vinnureglum skv. ETSI kafla 7.4.9

3.8 Form skírteinis

3.8.1 Borgaraskírteini

3.8.1.1 Form

Vottorðið ætti að fylgja RFC 3039
Gerið grein fyrir hugsanlegum frávikum frá RFC 3039

3.8.1.2

Öll sértákn í sænska stafrófinu ber að vera hægt að meðhöndla í vottorðinu

3.8.1.3

Þær skilgreiningar sem settar eru fram í dálkinum Athugasemdir í töflunum hér að neðan eru allar í flokkinum „ber að “sé annað ekki tilgreint.
Ef lokunarupplýsingar eru meðhöndlaðar í gegnum CRL X.509 er skylt að nota svæðið CRLDistributionPoints.
Ef lokunarupplýsingar eru meðhöndlaðar í gegn um OCSP er skylt að nota svæðið AuthorityInfoAccess.

(Hér fyrir neðan kemur tafla með lýsingu á svæðum í vottorði. Hana er að finna í viðauka 4)

Viðauki 4.

Samanburður á formi vottorða samkvæmt kröfum ríkisins í Noregi og Svíþjóð

Persónuskilríki (einstaklingsvottorð)

Noregur (NO): Offentlig personsertifikat; Svíþjóð (SE): Statens ID-certifikat

NO: Persónuskilríki skulu byggð á RFC 2459 og skilgreiningum fyrir fullgld vottorð (væntanlega RFC 3039)
SE: Skal vera í samræmi við RFC 3039. Byggt á skilgreiningum fyrir fullgilt skírteini ásamt atriðum úr sænskum staðli til að gera sniðið skýrara

NO:Þrjú vottorð í persónuskilríkjum:
- Vottorð fyrir afneitunarvörn (rafræna udirskrift) með bita fyrir non-repudiation settan í svæðinu keyUsage.
- Vottorð fyrir sannvottun með bitann fyrir authentication settan í svæðinu keyUsage.
- Vottorð fyrir dulritun og sendingu setulykla (session keys) með bitana keyEncipherment og/eða dataEncipherment setta í svæðinu keyUsage.

SE: Tvö vottorð. Síðari tvö vottorðin sbr. Noreg í einu lagi. Bitarnir digitalSignature og keyEncipherment verði báðir settir í svæðinu keyUsage.

Skýring á birtingardálki.
M= mandatory Skylt að hafa;
O= optional Haft eftir vali

Grunnvottorð samkvæmt X.509 fyrir persónuskilríki			
Svæðisheiti	**Birting**	**Athugasemdir**	**Athugasemdir 2**
version	M	=2 (fyrir X.509 v.3)	
serialNumber	M	NO: RFC 2459 segir lítið annað en að númerið skuli vera í tölum og einkvæmt. Útgefandi er ábyrgur fyrir einkvæmni númera.	SE: Ekki enn ákveðið hvort farið verður að sænskum staðli (8bæti) eða látið opið
signature	M	Nota ber annað tveggja undirritunaralgríma: - md5WithRSAEncryption -sha-1WithRSAEncryption	
issuer	M	Nota ber eftirfarandi eigindir (attributes): - countryName (t.d. IS) - organizationName (Heiti úr fyrirtækjaskrá) - serialNumber (Kennitala útgefanda) - commonName (Heiti sem útgefandi er almennt þekktur undir) Þrjár fyrstnefndu eigindirnar eiga saman að nægja til að einkenna útgefanda með einkvæmum hætti og vera það sem í sniði fyrir fullgilda undirskrift er kallað “unmistakable identity”. Eigindin commonName skal vera það heiti sem útgefandi er almennt þekktur undir. (Dæmi: Eimskip)	
validity	M	Gildistími Frá-til samkv. RFC 2459	
subject	M	NO: Nota ber eftirfarandi eigindir (attributes): - countryName (t.d. IS) - serialNumber (Einkvæmt númer) - commonName (t.d. Árni Bjarnason). Þessar þrjár eigindir skulu skilgreina vottorðshafann, (einstaklinginn) á einkvæman hátt. Eigindin serialNumber er ekki kennitala mannsins heldurtalna- og stafaruna sem	SE: Nota skal eftirfarandi eigindir: - - countryName (t.d. IS) - surname (Kenninafn) - givenName (Nafn) - serialNumber (Kennitala) - commonName (t.d. Lars Wahlgren).

		afleidd er af kennitölunni og sem útgefandi vottorðsins getur breytt aftur í kennitölu. serialNumber verður í þessu vottorði “uniqueSubjectNumber”. Svæðið subject getur innihaldið aðrar eigindir, en þeirra á ekki að vera þörf til að bera kennsl áeinstaklinginn. commonName er fullt nafn, en unnt skal vera að sleppa millinöfnum sem ekki err óskað eftir að sjáist.	
subjectPublicKeyInfo	M	NO: Í vottorði fyrir kennsl eða afneitunarvörn skal þetta vera rsaEncryption. Í vottorði fyrir dulritun skal þetta vera rsaEncryption eða Diffie-HellmanKeyExchange	SE: Skal vera rsaEncryption
issuerUniqueIdentifier	---	Ekki notað	
subjectUniqueIdentifier	---	Ekki notað	

Stöðluð aukasvæði

Skylt að skoða: **Já** þýðir að nota verður þetta svæði til að vottorðið virki

Svæðisheiti	**Skylt að skoða**	**Birting**	**Athugasemdir**	**Athugasemdir 2**
authorityKeyIdentifier	Nei	M		
subjectKeyIdentifier	Nei	M		
keyUsage	Já	M	Upplýsingar um “keyUsage” skulu vera fyrir hendi. Ef valin er afneitunarvörn (non-repudiation) má ekki tilgreina neina aðra notkun	
privateKeyUsagePeriod		---	Ekki notað	
certificatePolicies	Nei	M		
policyMappings		---	Ekki notað	
subjectAltName	Nei	O	NO: Tvenns konar upplýsingar má birta hér: - Tölvupóstfang og – Fullt nafn samkvæmt þjóðskrá. Tölvupóstföng skulu skráð á IA5-formi	
issuerAltName		---	Ekki notað	
subjectDirectoryAttributes		---	Ekki notað	
basicConstraints		---	Ekki notað	
nameConstraints		---	Ekki notað	
policyConstraints		---	Ekki notað	
cRLDistributionPoints	Nei	M		
extKeyUsage		---	Ekki notað	

Sérstök aukasvæði

Svæðisheiti	**Skylt að skoða**	**Birting**	**Athugasemdir**	**Athugasemdir 2**
AuthorityInfoAccessSyntax	Nei	O		
biometricInfo	Nei	O		
qcStatements	Nei	O	NO: Mælt er með því að setja hér OID (Object identifier) fyrir yfirlýsingar frá útgefendum fullgildra skírteina	
cardNumber	Nei	O		

Starfsmannaskilríki

NO: Starfsmannaskilríki skulu byggð á RFC 2459 og skilgreiningum fyrir fullgld vottorð (væntanlega RFC 3039). Auk þess er tekið tillit til ákvæða í vottunarstefnu stjórnsýslunetsins. FSP-1
SE: Skal vera í samræmi við RFC 3039. Byggt á skilgreiningum fyrir fullgilt skírteini ásamt atriðum úr sænskum staðli til að gera sniðið skýrara.

NO: Vottorð í starfsmannaskilríkjum geta verið þrjú:
- Vottorð fyrir afneitunarvörn (rafræna udirskrift) með bita fyrir non-repudiation settan í svæðinu keyUsage.
- Vottorð fyrir sannvottun með bitann fyrir authentication settan í svæðinu keyUsage.
- Vottorð fyrir dulritun og sendingu setulykla (session keys) með bitana keyEncipherment og/eða dataEncipherment setta í svæðinu keyUsage.

Erfitt getur verið að meðhöndla 3 vottorð í vissum forritapökkum.
Starfsmannaskilríki hafa ekki að geyma kennitölu. Þau eru ekki ætluð sem einkvæm einkenni nema innan stofnunar eða fyrirtækis. Þá eru efasemdir uppi um að rétt sé að nota þessi skilríki fyrir einkaþarfir starfsmannsins.

Skýring á birtingardálki.
M= mandatory Skylt að hafa
O= optional Haft eftir vali

ASN-1Teg Absract syntax notation, staðlað framsetningarform.

Grunnvottorð samkvæmt X.509 fyrir starfsmannaskilríki				
Svæðisheiti	**Birting**	**ASN-1 Teg**	**Athugasemdir**	**Athugasemdir 2**
version	M		=2 (fyrir X.509 v.3)	
serialNumber	M		NO: RFC 2459 segir lítið annað en að númerið skuli vera í tölum og einkvæmt. Útgefandi er ábyrgur fyrir einkvæmni númera.	
signature	M		NO: Nota ber annað tveggja undirritunaralgríma: -md5WithRSAEncryption -sha-1WithRSAEncryption	SE: Nota ber -sha-1WithRSAEncryption
issuer	M	utf8String	Nota ber eftirfarandi eigindir (attributes): - countryName (t.d. IS) - organizationName (Heiti úr fyrirtækjaskrá) - organizationUnit (Sértækt fyrir SE) - serialNumber (Kennitala útgefanda) - commonName (Heiti sem útgefandi er almennt þekktur undir) countryName, organizationName og serialNumber eiga saman að nægja til að einkenna útgefanda með einkvæmum hætti og vera það sem í sniði fyrir fullgilda undirskrift er kallað “unmistakable identity”. Eigindin commonName skal vera það heit sem útgefandi er lamennt þekktur undir. (Dæmi: Eimskip) SE: commonName getur auk þess verið með auðkenni fyrir vottunarstefnu útgefandans.	
validity	M	UTCTime	Gildistími Frá-til samkv. RFC 2459	

subject	M	utf8String	NO: Nota ber eftirfarandi eigindir (attributes): - countryName (t.d. IS) - organizationName (Kennitala og heiti stofnunar í einu svæði) - commonName (t.d. Árni Bjarnason). - serialNumber (einkvæmt númer starfsmanns innan stofnunar) Þessar fjórar eigindir skulu skilgreina einstaklinginn á einkvæman hátt. Önnur eigindi eru heimil í svæðinu en þau skulu ekki vera nausðyunleg til að bera kennsl á starfsmanninn með einkvæmum hætti. Eigindina organizationUnitName má nota til að tákna deild eða stjórnunareiningu. commonName er fullt nafn, en unnt skal vera að sleppa millinöfnum sem ekki err óskað eftir að sjáist.	SE: Unnt skal vera að nota eftirfarandi eigindir: - - countryName (t.d. IS) - surname (Kenninafn) - givenName (Öll eiginnöfn) - serialNumber (Kennitala) - commonName (Eiginnafn sem notað er vanalega, t.d. Lars Wahlgren). - organizationName - organizationUnit - LocalityName surname, givenName og serialNumber skulu vera eins og í þjóðskrá
subjectPublicKeyInfo	M		NO: Í vottorði fyrir kennsl eða afneitunarvörn skal þetta vera rsaEncryption. Í vottorði fyrir dulritun skal þetta vera rsaEncryption eða Diffie-HellmanKeyExchange	SE: Skal vera rsaEncryption
issuerUniqueIdentifier	---		Ekki notað	
subjectUniqueIdentifier	---		Ekki notað	

Stöðluð aukasvæði

Skylt að skoða: **Já** þýðir að nota verður þetta svæði til að vottorðið virki

Svæðisheiti	**Skylt að skoða**	**Birting**	**Athugasemdir**	**Athugasemdir 2**
authorityKeyIdentifier	Nei	M	NO: Gerir mögulegt að auðkenna dreifilykilinn sem tilheyrir þeim einkalykli sem notaður er til að undirrita vottorðið.	
subjectKeyIdentifier	Nei	M	NO: Gerir mögulegt að auðkenna dreifilykilinn í vottorðinu	
keyUsage	Já	M	Upplýsingar um “keyUsage” skulu vera fyrir hendi (SE: Heimil notkun er digitalSignature, nonRepudiation og keyEncipherment). Ef valin er afneitunarvörn (non-repudiation) má ekki tilgreina neina aðra notkun	
privateKeyUsagePeriod		---	Ekki notað	
certificatePolicies	Nei	M	OID	
policyMappings		---	Ekki notað	
subjectAltName	Nei	O	NO: Mælt er með að birta hér: Tölvuóstfang skráð á IA5-formi SE: EF tölvupóstfang er birt hér skal það vera á forminu Rfc822Name (local-part@domain)	
issuerAltName		---	Ekki notað	
subjectDirectoryAttributes		---	Ekki notað	

basicConstraints		---	NO: Ekki notað SE: Notist eingöngu fyrir viðbótarupplýsingar um einstaklinginn, t.d. starfsheiti.
nameConstraints		---	Ekki notað
policyConstraints		---	Ekki notað
cRLDistributionPoints	Nei	M	
extKeyUsage		---	Ekki notað

Sérstök aukasvæði

Svæðisheiti	**Skylt að skoða**	**Birting**	**Athugasemdir**	**Athugasemdir 2**
AuthorityInfoAccessSyntax	Nei	O		
biometricInfo	Nei	O		
qcStatements	Nei	O	NO: Mælt er með því að setja hér OID (Object identifier) fyrir yfirlýsingar frá útgefendum fullgildra skírteina	
cardNumber	Nei	O		

Önnur skilríki

Fyrirtækisskilríki

NO: Virksomhedssertifikat er fyrir örugg samskipti milli stofnana og deilda innan stofnana (virksomheter og organisasjonsenheter) Geymir engar persónuupplýsingar.

SE: Stimpilskilríki (Certifikat för myndighets elektroniska stempel), fyrst og fremst ætlað til að undirrita gerðir sem stjórnvald sendir frá sér eða er ætlað til varðveislu. Þá er undirritað í nafni stjórnvalds en ekki einstaks starfsmanns.

Þessi skilríki eru mjög áþekk í formi hjá báðum og víkja ekki í stórum dráttum frá því sem lýst er að ofan nema í því sem sjálfsagt er, t.d. engar persónuupplýsingar í svæðinu subject.

Vefþjónsskilríki

SE: Vefþjónsskilríki (Servercertifikat) kallast þau skilríki sem helst eru notuð í vefþjónum til að setja upp örugga samskiptaleið milli biðlara og miðlara, oftast með samskiptaaðferðinni SSL.

Starfsréttindaskilríki

NO: Starfsréttindaskilríki (Professjonssertifikat) eru persónuskilríki sem tengja einstakling við tiltekin starfsréttindi, menntun og hugsanlega opinbera viðurkenningu á slíkum réttindum.

Viðauki 5. Orðaskýringar

Íslenska	Enska	Skýring
afturköllunarskrá	certification revocation list	Skrá yfir vottorð sem hafa verið afturkölluð (gerð ógild) áður en gildistími þeira rennur út.
heilleiki gagna	data integrity	Eiginleiki gagna sem felst í því að nákvæmni og samkvæmni haldast frá upphafi ferlis til enda.
rafræn undirskrift	digital signature	Rafræn undirskrift verður til við umritun skeytis með hjálp dulritunarkerfis þar sem lyklar eru notaðir til að ákvarða (1) hvort við umritunina var notaður einkalykill samsvarandi dreifilykli þess er undirritaði skeytið, og (2) hvort skeytinu hefur verið breytt eftir að það var umritað.
rótarvottorð (rótarskilríki)	root certificate	
sannvotta	authenticate	Sannprófa að einindi sé það sem það er sagt vera.
skilríki (skírteini)	certificate	Rafrænt vottorð eða sett af slíkum vottorðum sem vottorðshafi fær hjá vottunarmiðstöð ásamt búnaði til að nota það/þau.
skráningarmiðstöð	registration authority	
starfsheitisvottorð		Vottorð gefin út til einstaklinga á grundvelli starfsheitis þeirra, t.d. lækna eða endurskoðenda.
stöðuvottorð		Vottorð gefið út til undirritanda vegna umboðs hans eða stöðu.
vottorð	certificate	Vottorð á rafrænu formi sem tengir sannprófunargögn við undirritanda og staðfestir hver hann er. Hugtakið *„certificate“* eða *„sertifikat“* er notað í víðum skilningi í fyrirliggjandi erlendum textum. Í skjölum nefndarinnar er reynt að nota „vottorð“ um hvert einstakt, sértækt *„certificate“*, en „skilríki“ (hvorugkyn fleirtölu) um pakka, sem í væru vottorð, eitt eða fleiri, ásamt nauðsynlegum búnaði til að nota það/þau. Ef rétt er skilið sænska hugtakið *„statens e-id-handling“* þá eru það skilríki.
vottunarmiðstöð	certification authority	
vottunarstefna	certificate policy	Í vottunarstefnu kemur fram hvernig stefnt er að því að standa að útgáfu og meðferð stafrænna vottorða. Í vottunarstefnu eru líka settar reglur um þær kröfur sem gerðar eru í þjónustunni til öryggis og eftirlits.
yfirlýsing um framkvæmd vottunar	certification practice statement	Vottunarframkvæmd segir fyrir um hvernig vottunarstöð framkvæmir útgáfu og viðhald vottorða. Yfirlýsing um vottunarframkvæmd er skrifleg lýsing á þessari framkvæmd.
yfirstjórn dreifilyklaskipulags	policy authority, policy management authority	Stofnun eða nefnd sem velur eða þróar vottunarstefnu og heldur henni við.

Viðauki 6. Helstu heimildir

Danskar heimildir

[IT-sikk] Praktisk brug af kryptering og elektroniske signaturer. IT-sikkerhedsrådet, 2000. http://www.fsk.dk/fsk/publ/2000/praktiskbrug/samlet.htm
[Dig-forvalt] Digital forvaltning. Finansministeriet, maj 2001. http://www.fm.dk/udgivelser/publikationer/digitalforvaltning/download/digital_ren.html
Anbefaling af Specifikation for certifikater i FSK-projekter. Forum for digital signatur, 2001. http://www.fsk.dk/cgi-bin/doc-show.cgi?theme_id=7471&doc_id=35147&doc_type=29&leftmenu=3
[Evaluering] Sammenfattende evaluering af Forskningsministeriets pilotprojekter om Digital Signatur.
http://www.fsk.dk/fsk/div/digitalsignatur/DigitalSignaturEvaluering.pdf

Norskar heimildir

[NOU 2001:10] Uten penn og blekk . Bruk av digitale signaturer i elektronisk samhandling med og i forvaltningen..
http://odin.dep.no/aad/norsk/publ/utredninger/NOU/002001-020005/index-dok000-b-n-a.html
Døgnåpen forvaltning. Strategi og tiltak. Arbeids- og administrationsdepartementet 2001. http://odin.dep.no/aad/norsk/aktuelt/pressem/002001-990364/index-dok000-b-n-a.html

Sænskar heimildir

[F:168] Elektronisk identifiering 2001. Förfrågningsunderlag (með fylgiskjölum). Statskontoret 2001. http://it-upphandling.statskontoret.se/Uhw/
Hantering av certifikat och elektroniska signaturer inom statsförvaltningen. RSV Rapport 2001:15.
http://www.rsv.se/skatter/rapporter/rapport20001123/samsetrapport_09_27.html
Infrastruktur för Säker elektronisk överföring till, från och inom statsförvaltningen. Staskontoret 2000:7. http://www.statskontoret.se/pdf/200007.pdf
Elektroniska signaturer och elektronisk identifiering för myndigheders e-tjänster. Statskontoret 2000:40. http://www.statskontoret.se/pdf/200040.pdf

Staðlar og staðalútfærslur

[TS 101 456] ETSI TS 101 456. Policy requirements for certification authorities issuing qualified certificates.
[RFC 2459] RFC 2459. Internet X.509 Public Key Infrastructure Certificate and CRL Profile.
[RFC 3039] RFC 3039. Internet X.509 Public Key Infrastructure Qualified Certificate Profile.
[TS 101 862] ETSI TS 101 862. Qualified certificate profile.
.