MAT Á FULLVISSUSTIGI AUÐKENNA

Sannvottun á auðkennum fyrir rafræna þjónustu

Mat á mismunandi útfærslu
á rafrænum auðkennum
og sannvottun í rafrænni þjónustu

ADMON
RÁÐGJÖF

Verkefni (*Project*):	Matsskýrsla Admon
Útgáfa (*Release*):	Önnur útgáfa
Dagsetning (*Date*):	27.06.2013

Höfundur (*Author*):	Arnaldur F. Axfjörð
Eigandi (*Owner*):	Admon ehf.
Viðskiptavinur (*Client*):	Almenn útgáfa.
Tilvísun (*Document Ref*):	Mat á fullvissustigi 02-00 2013-06-27.docx
Útgáfunúmer (*Version No*):	02-00

Breytingasaga (*Revision History*):

Útgáfudagur	Útgáfa	Lýsing	Ábyrgðaraðili
16.06.2013	01-00-00	Fyrsta útgáfa.	Arnaldur F. Axfjörð
26.06.2013	01-01-00	Leiðrétt fyrsta útgáfa.	Arnaldur F. Axfjörð
27.06.2013	02-00-00	Önnur útgáfa. Mat á veiku aðgangsorði í kafla 6.1. Aukið við skýringar.	Arnaldur F. Axfjörð

EFNISYFIRLIT

1 INNGANGUR

Í þessu skjali er mat sérfræðinga ráðgjafarfyrirtækisins Admon ehf. á mismunandi útfærslu á rafrænni auðkenningu og sannvottun í rafrænni þjónustu með hliðsjón af svokölluðu QAA matskerfi sem kennt er við STORK verkefnið[1]. STORK QAA kerfið[1] byggir á tillögu IDABC[2] um margþrepa tilhögun fyrir rafræna sannvottun[2], er í góðu samræmi við umgjörð *Liberty Alliance Project*[3] fyrir fullvissustig rafrænna auðkenna[3] og í samræmi við viðmið alríkisstjórnar Bandaríkjanna (tilmæli NIST800-63[4] og leiðbeiningar OMB M-04-04[5]) fyrir fullvissustig[4][5].

Efnistök skýrslunnar miða við lesendur sem eru sérfræðingar í rafrænum auðkennum og í útfærslu á útgáfu þeirra og notkun í rafrænni þjónustu yfir fjartengingar. Niðurstöður matsins ættu einnig að höfða til stjórnenda og annarra sem þurfa að taka ákvörðun um útfærslu á öryggi í rafrænni þjónustu. Einnig er það von skýrsluhöfunda að efni skýrslunnar veki áhuga þeirra sem vilja auka þekkingu sína á rafrænni auðkenningu og öryggisþáttum í sannvottun í rafrænni þjónustu.

Mat á fullvissustigum rafrænna auðkenna í þessari skýrslu er byggt á opinberum upplýsingum, meðal annars á vefsetrum útgefenda og annarra hagsmunaaðila. Farið var yfir lýsingar þeirra á ferlum við skráningu áskrifenda og afhendingu auðkennanna og á útfærslu á rafrænni sannvottun á notendum sem krefjendum réttinda til innskráningar. Einnig er byggt á fyrirliggjandi upplýsingum um kröfur til útgáfu og útgefenda, meðal annars í opinberum vottunarstefnuskjölum. Að auki er í sumum tilvikum byggt á sértækri þekkingu skýrsluhöfunda á fyrirkomulagi við skráningu og notkun rafrænu auðkennanna.

Niðurstöður matsins afmarkast því að miklu leyti af þeim gögnum sem eru aðgengileg og eru ekki réttari en þær upplýsingar sem byggt er á. Ef lesendur hafa athugasemdir eða ábendingar um rangfærslur er mikilvægt að þeir komi þeim á framfæri við Admon í tölvupóstfangi info@admon.is. Það er markmið Admon að þessi skýrsla verði endurútgefin, bætt og aukin eftir því sem þörf er á.

STORK QAA hefur verið notað síðan 2009 til að samræma gæðastig rafrænna auðkenna sem gefin eru út hjá þeim þjóðum sem tóku þátt í STORK verkefninu. Í STORK 2.0 framhaldsverkefninu sem nú er í gangi meðal 19 þjóða í Evrópu mun þetta líkan verða notað áfram. Fyrir liggja drög að endurskoðun á STORK QAA[6] sem tína til eftirfarandi annmarka sem talið er nauðsynlegt að taka á í framtíðinni:

- STORK QAA er afurð úr samstarfi í verkefninu en ekki tæknilegur staðall. Efnisleg atriði eru því í sumum tilvikum afmörkuð við samhengi STORK verkefnisins.

[1] STORK (*Secure Identity Across Borders Linked*) var verkefni í Upplýsingatækniáætlun Evrópusambandsins undir Samkeppnis- og nýsköpunaráætluninni (CIP) – ESB INFSO-ICT-PSP-224993. Verkefnið hófst í júní 2008 og því lauk í desember 2011. Nú er í gangi framhaldsverkefni sem kallast STORK 2.0. Sjá www.eid-stork.eu og www.eid-stork2.eu.

[2] IDABC (*Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens*) var vettvangur Evrópusambandsins fyrir samstarf þjóða í framþróun rafrænnar stjórnsýslu. Nýr vettvangur, ISA (*Interoperability Solutions for European Public Administrations*), tók við af IDABC í janúar 2010; sjá ec.europa.eu/isa/.

[3] *Liberty Alliance Project* var á árunum 2001 til 2010 samstarfsvettvangur fyrir uppbyggingu á stöðlum, viðmiðum, leiðbeiningum og bestu aðferðum fyrir framþróun rafrænna viðskipta með verndun á friðhelgi einstaklinga og öryggi persónulegra auðkenna að leiðarljósi. Sjá www.projectliberty.org. *Kantara Initiative* tók við af *Liberty Alliance Project*, sjá www.kantarainitiative.org.

[4] NIST (*National Institute of Standards and Technology*) er staðlaráð Bandaríkjanna. Sjá www.nist.gov.

[5] OMB (*Office of Management and Budget*) heyrir undir Skrifstofu Bandaríkjaforseta. Sjá www.whitehouse.gov/omb/.

- STORK QAA byggir á Evrópskum viðmiðum, til dæmis tilskipun Evrópuþingsins og ráðsins 1999/93/EB um rafrænar undirskriftir [7]. Þetta hefur í för með sér annmarka í notkun líkansins í alþjóðlegu samhengi og möguleg vandamál þegar regluverk Evrópusambandsins er þróað áfram.
- STORK QAA tekur ekki tillit til gæðaþátta eins og reglubundinnar endurskoðunar á gildi og réttleika þeirra gagna sem liggja til grundvallar fullvissustigi rafrænna auðkenna, né þátta í starfsemi sem lúta að færsluskráningu, hlítingu við persónuverndarkröfur og fjárhagslegan stöðugleika (þ.m.t. tryggingar)[6].

Það er álit skýrsluhöfunda að þessi atriði hafi ekki áhrif á mat á fullvissustigum rafrænna auðkenna í þessari skýrslu. Þau varða úrbætur í greiningarlíkani og samræmingu við viðmið sem hugsanlega verða sett í framtíðinni, meðal annars til að samstilla Evrópsk viðmið við alþjóðleg viðmið. STORK QAA fellur mjög vel að viðurkenndum viðmiðum í Bandaríkjunum og hefur nú þegar náð þeirri stöðu að vera grunnur í staðlagerð ISO/IEC[7] og endurskoðun á regluverki Evrópusambandsins[8]. Þegar nýir staðlar og endurskoðaðar kröfur hafa komið fram þarf að sjálfsögðu að meta hvort og hvaða áhrif það hefur á mat á fullvissustigum rafrænna auðkenna í þessari skýrslu.

Þessi skýrsla er að hluta til byggð á STORK skjalinu *D2.3 – Quality authenticator scheme*[1]. Lögð er áhersla á að þýða lykilhugtök og skýra þau nægilega vel til að lesendur geti sjálfir metið þær forsendur sem liggja til grundvallar STORK QAA líkaninu og því mati sem hér er sett fram. Í þeim tilgangi var leitað í ýmsar aðrar heimildir og skilgreiningar og leitast við að ná góðu samræmi í heildarmyndina.

Í kafla 2 er sett fram hugtakalíkan sem skýrir alla þætti skráningar, útgáfu og notkunar rafrænna auðkenna. Þar eru einnig settar fram skýringar á hugtökum og skammstöfunum sem notuð eru í skýrslunni.

Í kafla 3 er fjallað um STORK QAA fullvissustigin. Í kafla 4 eru síðan settar fram þær sundurgreindu kröfur sem liggja að baki.

Í kafla 5 er fjallað um sannvottun í tengslum við færsluaðgerðir til að draga fram þann mismun sem er á sannprófun á færsluaðgerðinni sjálfri og sannvottun á kennslum þess notanda sem biður um færsluaðgerðina.

Mat á auðkennum í almennri notkun er síðan sett fram í kafla 6. Þau rafrænu auðkenni sem lagt er mat á eru eftirfarandi:

1. Hefðbundið notandanafn og aðgangsorð
2. Veflykill ríkisskattstjóra
3. Íslykill Þjóðskrár Íslands
4. Innskráning í netbanka með Auðkennislykli
5. Innskráning í netbanka hjá Landsbankanum
6. Rafræn skilríki undir Íslandsrót
7. OCES-skilríki og NemID í Danmörku

[6] Það er þó rétt að hafa í huga að tilskipun Evrópuþingsins og ráðsins 1999/93/EB um rafrænar undirskriftir inniheldur meðal annars slíkar kröfur til starfsemi vottunarstöðva og útgáfu rafrænna skilríkja fyrir fullgildar rafrænar undirskriftir. Þessar kröfur eru útfærðar nánar í ETSI TS 101 456 tækniforskriftinni[8].

[7] Undir sameiginlegu staðlanefndinni JTC 1/SC 27 er verið að vinna frumvarp að alþjóðlegum staðli ISO/IEC 29115 *Information technology – Security techniques – Entity authentication assurance framework*. Þann 26. febrúar 2013 voru drög staðalsins gefin út til endanlegrar samþykktar. Staðallinn byggir á NIST 800-63-1[4].

[8] Fyrir liggur tillaga að reglugerð Evrópuþingsins og ráðsins um rafræna auðkenningu og traustþjónustu – COM(2012) 238/2.

8. BankID í Noregi

Í kafla 7 er fjallað um sjálfsmat þátttökuþjóða í STORK 2.0 verkefninu á þeim auðkennum sem hægt er að nota í grunngerð STORK til sannvottunar yfir landamæri í Evrópu.

Samantekt á niðurstöðum skýrslunnar er í kafla 8.

2 SKÝRINGAR Á HUGTÖKUM

Rafræn auðkenning og sannvottun á þeim í fjartengingu er tiltölulega nýleg fræðigrein, sérstaklega hér á landi. Orðanotkun er því nokkuð nýstárleg og getur verið flókin þar sem skilningur á lykilþáttum í útfærslu rafrænnar auðkenningar og sannvottunar byggir á afmörkuðum og vel skilgreindum hugtökum. Auk þess eru rafræn auðkenni margskonar og mismunandi þannig að góð og skýr skilgreining á þeim þáttum sem skipta máli er algjör forsenda þess að hægt sé að setja fram almenn viðmið sem umgjörð fyrir samanburð á fullvissustigi rafrænna auðkenna.

Í þessum kafla er fyrst fjallað um almennt hugtakalíkan fyrir sannvottun sem setur grunnhugtökin í samhengi. Þar á eftir er listi yfir hugtök og skilgreiningar þeirra. Í síðasta hlutanum er listi yfir skammstafanir sem notaðar eru í skýrslunni.

2.1 HUGTAKALÍKAN FYRIR SANNVOTTUN

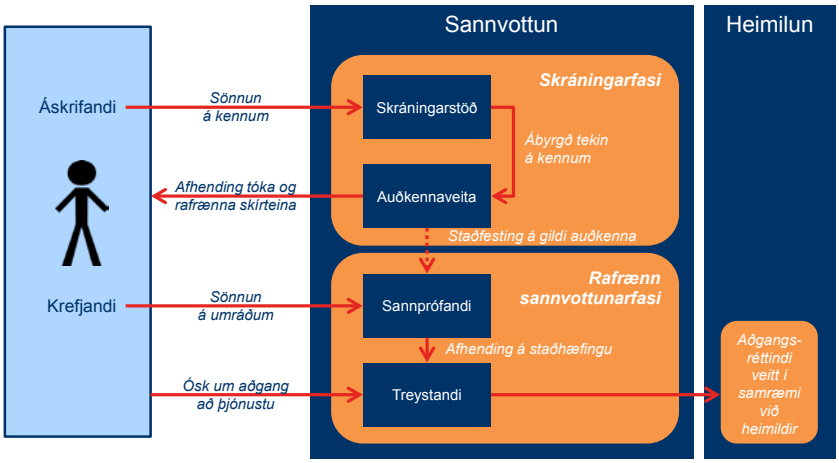
Á Mynd 1 er líkan fyrir viðmið í notkun hugtaka í tengslum við rafræna sannvottun.

Sannvottun á notanda krefst að lágmarki tveggja fasa, skráningarfasa og rafræns sannvottunarfasa:

1. **Skráningarfasi** þar sem notandinn fær *tóka* og/eða önnur auðkennagögn eins og notandanafn eða rafrænt vottorð til að nota á seinni stigum í sannvottun fyrir aðgang að rafrænni þjónustu. Skráningarfasinn er venjulega í eftirfarandi skrefum:
    a. *Sönnun á kennum* þar sem raunveruleg kenni umsækjanda (t.d. nafn og aldur) eru staðfest.
    b. Skráning og útgáfa á auðkennagögnum umsækjanda byggt á ábyrgð skráningarstöðvar á réttum kennum (*ábyrgð tekin á kennum*).
    c. Afhending á rafrænum auðkennum (*tóka* og/eða öðrum rafrænum auðkenningargögnum sem *rafrænum skírteinum*).
2. **Rafrænn sannvottunarfasi**, sem líka má nefna *sönnun á umráðum*, þar sem rafræn auðkenni *krefjandans* (handhafa rafrænu auðkennanna) eru sannprófuð.

Í kjölfarið getur veitandi rafrænnar þjónustu (sem *treystandi*) tekið afstöðu til þess hvort notandi sem krefst aðgangs (*krefjandi*) fær aðgangsréttindi inn á rafræna þjónustu í samræmi við heimildir (*heimilun*).

Lítum nánar á þessi ferli með hliðsjón af Mynd 1. Hugtök sem finna má á myndinni eru skáletruð.



Mynd 1: Hugtakalíkan fyrir sannvottun.

Við útgáfu rafrænna auðkenna þarf að skrá notandann og halda til haga sönnunum fyrir því hver hann er. Notandinn er því umsækjandi og *áskrifandi* í huga *skráningarstöðvar*. *Áskrifandinn* þarf síðan að taka ábyrgð á rafrænu auðkennunum eftir útgáfu þeirra og tryggja að hann einn hafi umráð yfir þeim.

Sönnun á kennum er það ferli sem staðfestir að auðkenni *áskrifanda* samsvari sannanlega kennum sem tengist raunverulegum einstaklingi, eins og nafni hans eða fæðingardegi. Eftir því sem kröfur um fullvissu eru meiri þarf umfangsmeiri og traustari aðgerðir til að staðfesta auðkenni notenda. *Sönnun á kennum* fer fram hjá *skráningarstöð*.

Skráningarstöðin er ábyrg fyrir því að sannprófa kenni áskrifandans, til dæmis með því að staðfesta persónuskilríki, ökuskírteini eða önnur pappírsgögn, staðfesta upplýsingar í opinberum gagnagrunnum og taka í kjölfarið ábyrgð á kennum áskrifandans gagnvart *auðkennaveitunni*[9] sem síðan gefur rafrænu auðkennin út.

Þegar *auðkennaveitan* hefur fengið staðfestingu frá *skráningarstöð* sem felur í sér ábyrgð á kennum *áskrifandans* afhendir *auðkennaveitan áskrifandanum tóka* sem nota má í rafrænu sannvottunarferli og gefur út auðkennagögn (stundum kallað *rafrænt skírteini*) sem þarf til að binda *tókann* við auðkenni *áskrifandans* eða við tiltekin kenni hans. Afhending rafrænna auðkennagagna og samsvarandi *tóka* þarf ekki að fara fram á sama tíma, svo fremi sem þess er gætt að tengsl *tókans* og auðkennagagnanna séu varðveitt.

Algengt er að *skráningarstöð* og *auðkennaveita* séu sami aðilinn þó ferlar þessara þjónustuþátta séu yfirleitt skýrt aðgreindir.

Dæmi: Rafræn skilríki og Ísland.is

Skráningarfasi

1. *Áskrifandi* mætir í útibú banka sem er *skráningarstöð* samkvæmt samningi við Auðkenni ehf.
2. *Áskrifandinn* leggur fram *sönnun á kennum* með skilríkjum með mynd, útgefnum af opinberum aðila.
3. Skráningarfulltrúi afritar framlögð skilríki og staðfestir upplýsingar um kennsl *áskrifandans* (mynd, nafn og kennitölu).
4. Skráningarfulltrúi staðfestir gagnvart *auðkennaveitunni* (Auðkenni ehf.) með rafrænni undirskrift sinni að *ábyrgð sé tekin á kennum* og að kröfur um skráningu séu uppfylltar.
5. Skráningarfulltrúinn *afhendir áskrifandanum* snjallkort (debetkort) með rafrænu skilríki(*) fyrir hönd *auðkennaveitunnar* (Auðkenni ehf.).
6. *Áskrifandinn* slær inn sinn hluta af PUK-númeri og slær síðan inn PIN-númer sem hann hefur valið sér. Skilríkið er þar með orðið virkt.
7. Skilríkið innheldur einkalykil í öruggum búnaði (*tóka*) og tilgreinir dreifilykil *áskrifandans*, nafn hans og kennitölu ásamt öðrum upplýsingum um notkunarsvið skilríkisins (*rafrænt skírteini*).
8. *Áskrifandinn* skrifar undir áskrifandasamning og tekur þar með ábyrgð á verndun einkalykilsins í rafræna skilríkinu.

Rafrænn sannvottunarfasi

1. *Krefjandinn* (sem er jafnframt *áskrifandi* skilríkjanna) velur að skrá sig inn á Mitt svæði hjá LÍN í gegnum Ísland.is með rafrænu skilríki.
2. Innskráningarþjónusta Íslands.is sem *sannprófandi* kallar eftir *sönnun á umráðum krefjandans* á einkalyklinum (*tókanum*) með því að senda stuttan textastreng til dulritunar.
3. *Krefjandinn sannar umráð* sín yfir einkalyklinum (*tókanum*) með því að dulrita textastrenginn með honum.
4. Með því að dulráða strenginn með dreifilykli krefjandans staðfestir Íslands.is að samstæður einkalykill hans (*tóki*) hafi verið notaður.
5. Innskráningarþjónusta Ísland.is *staðfestir gildi auðkennanna* með uppkalli til *auðkennaveitunnar* (Auðkenni ehf.).
6. LÍN sem *treystandi* fær *afhenta staðhæfingu* á sannvottun *krefjandans* í SAML skírteini frá innskráningarþjónustu Ísland.is.
7. LÍN sem *treystandi* tekur afstöðu til *óska krefjandans um aðgang að þjónustu* (Mínu svæði) og veitir honum aðgang í *samræmi við heimildir* hans sem notanda.

*Til einföldunar er hér gert ráð fyrir einu skilríki á debetkorti en í raun eru þar tvö skirlíki, eitt til auðkenningar og annað fyrir undirskriftir.

Sannprófandi er sá aðili sem sannprófar að notandinn sem *krefjandi* aðgangs hafi umráð og stjórn á *tókanum* og samsvarandi auðkennagögnum sem staðfesta kenni hans. *Sönnun á*

[9] Sem dæmi þá er ríkisskattstjóri auðkennaveita sem gefur út veflykil ríkisskattstjóra og bankarnir ásamt Auðkenni ehf. eru auðkennaveitur sem gefa út notendanöfn og lykilorð (bankarnir) og Auðkennislykil (Auðkenni ehf.). Auðkenni ehf. er einnig auðkennaveita fyrir útgáfu rafrænna skilríkja.

umráðum fer fram með því að notandinn sannvottar auðkenni sitt fyrir *sannprófandanum* með því að nota *tóka* og *rafrænt skírteini* sitt með tiltekinni rafrænni sannvottunaraðferð eða hætti (e. protocol). Í sumum tilvikum þarf *sannprófandi* að byggja sannprófun sína á *staðfestingu á gildi auðkenna* frá auðkennaveitunni sem gaf rafrænu auðkennin út, til dæmis ef þau hafa tilgreindan gildistíma. *Sannprófandinn* og *auðkennaveitan* geta verið sami aðilinn eða mismunandi aðilar sem vinna saman.

Treystandi er sá aðili sem þarf að geta treyst á kenni notanda sem krefst aðgangs að þjónustu hans. *Sannprófandi* og *treystandinn* geta verið sami aðilinn. Ef *sannprófandinn* og *treystandinn* eru sitt hvor aðilinn þá þarf *sannprófandinn* að afhenda *treystandanum* staðhæfingu í samræmi við niðurstöðu sannvottunarinnar (*afhending á staðhæfingu*). Rafræn afhending á slíkri staðhæfingu er stundum kölluð „rafræn staðhæfing á auðkennum“.

Treystandinn treystir á niðurstöðu rafrænu sannvottunarinnar þegar hann veitir síðan notandanum aðgang að rafrænni þjónustu. Þar með er krefjandanum *veitt aðgangsréttindi í samræmi við heimildir*.

2.2 SKILGREININGAR Á HUGTÖKUM

Eftifarandi skýringar eiga við um notkun hugtaka í þessari skýrslu. Samsvarandi þýðing á ensku eru skáletruð í sviga.

Aðgangsorð (*password*): Leynileg gögn, venjulega stafastrengur eða röð tákna, notað sem sannvottunargögn. Aðgangsorð er einungis þekkt hjá krefjanda og í þeim búnaði eða kerfi sem hann getur tengst til að sannvotta kennsl sín og fá aðgang.

Afhending á staðhæfingu (*assertion delivery*): Afhending á fullyrðingu frá sannprófanda til treystanda með upplýsingum um kenni áskrifanda og jafnvel sannprófaðar eigindir hans.

Auðkennagögn (*identity credentials*): Gögn gefin út af traustum aðila sem sett eru fram til að staðfesta fullyrðingu um auðkenni einstaklings. Oft eru auðkennagögn einfaldlega kölluð „auðkenni“. Rafræn auðkennagögn geta innihaldið auðkennatóka.

Auðkennatóki (*identity token*): Tóki sem notaður er til sannvottunar auðkenna.

Auðkennaveita (*credentials service provider; identity provider*): Þjónustuaðili sem gefur út einhvers konar rafræn auðkenni. Í dreifilyklaskipulagi er auðkennaveita rafrænna skilríkja kölluð vottunarstöð eða vottunaraðili, enda er undirritað vottorð stöðvarinnar innifalið í rafrænu skilríkjunum.

Auðkenni (*identity*): Samsafn einkenna eða eiginleika sem gerir í heild mögulegt að þekkja og aðgreina einstakling frá öðrum. Stundum notað sem stytting fyrir „auðkennagögn“.

Auðkenning (*identification*): Það að bera kennsl á einstakling með því að leggja fram sönnun til auðkennaveitu (til dæmis með skírteini eða skjölum) um að einstaklingurinn sé þekkjanlegur í einhverju samhengi með einkvæmum vísunum í kenni og/eða með viðbótarupplýsingum sem einkenna einstaklinginn. Staðfesting auðkennaveitunnar á þessum sönnunum er ekki hluti auðkenningar heldur hluti af sannvottun á kennum.

Ábyrgð tekin á kennum (*vouching for identity*): Að staðhæfa um auðkenni einstaklings byggt á sönnunum því til stuðnings.

Áskrifandi (*subscriber*): Einstaklingur eða lögaðili sem er áskrifandi hjá auðkennaveitu sem handhafi rafrænna auðkenna. Áskrifandinn[10] verður handhafi rafrænu auðkennanna eftir útgáfu þeirra og kemur fram sem krefjandi sem óskar eftir aðgangi að rafrænni þjónustu byggt á rafrænu auðkennunum.

Dreifilyklaskilríki (*public key certificate*): Rafrænt vottorð sem tilgreinir dreifilykil vottorðshafa (e. subject; sá sem vottaður er) og sem tengir dreifilykilinn við vottorðshafann á ótvíræðan hátt. Sjá einnig „rafrænt vottorð" og „rafræn skilríki".

Dreifilyklaskipulag (*public key infrastructure*): Það skipulag sem þarf til að framleiða og afhenda dulmálslykla og rafræn skilríki, viðhalda stöðuupplýsingum um skilríkin, gera afturköllunarlista aðgengilega og safnvista viðeigandi upplýsingar.

Eigind (*attribute*): Gögn sem tilgreina eiginleika sem tengjast einstaklingi eða lögaðila.

Fullgild rafræn undirskrift (*qualified electronic signature*): Útfærð (e. advanced) rafræn undirskrift sem er studd fullgildu skilríki og gerð með öruggum undirskriftarbúnaði. Fullgild rafræn undirskrift í skilningi laga nr. 28/2001 um rafrænar undirskriftir uppfyllir ætíð kröfu um réttaráhrif undirskriftar.

Fullgilding (*qualification*): Staðfesting, stundum með faglegri viðurkenningu (faggildingu), á hæfni einstaklings eða lögaðila til að gegna tilteknu hlutverki eða annast tiltekna starfsemi.

Fullgildur aðili (*qualified entity*): Aðili sem hefur fengið staðfestingu á hæfni sinni til að gegna tilteknu hlutverki eða annast tiltekna starfsemi. Vottunaraðilar sem fullnægja skilyrðum í V. kafla laga um rafrænar undirskriftir nr. 28/2001 teljast fullgildir aðilar.

Fullgilt skilríki (*qualified certificate*): Notað um skilríki sem inniheldur fullgilt vottorð.

Fullgilt vottorð (*qualified certificate*): Vottorð sem hefur að geyma upplýsingar sem kveðið er á um í 7. gr. laga um rafrænar undirskriftir, nr. 28/2001 og er gefið út af vottunarstöð (vottunaraðila) sem fullnægir skilyrðum V. kafla laganna.

Fullvissa (*assurance*): Annars vegar það traust sem borið er til þeirrar aðferðar sem notuð er til að ákvarða auðkenni þess einstaklings sem rafrænu skírteinin voru gefin út fyrir, og hins vegar það traust sem borið er til þess að sá einstaklingur sem notar rafrænu auðkennin sé sá einstaklingur sem þau voru gefin út fyrir.

Fullvissustig (*assurance level*): Mælikvarði fyrir fullvissu sem vísar til afleiðinga þess að villa sé í auðkenningu eða ef rafrænu auðkennin eru misnotuð.

Færslusannprófun (*transaction verification*): Sannprófun á því að innihaldi færslu hafi ekki verið breytt, til dæmis með sviksamlegum hætti. Færslusannprófun felst þannig ekki eingöngu í sannvottun á auðkennum krefjandans heldur einnig í sannprófun á heilleika færslunnar, með því að tryggja að færslunni hafi ekki verið breytt án vitundar krefjandans. Stundum er slík sannprófun kölluð „sannprófun á heilleika færslu" (e. transaction integrity verification).

Færslusannvottun (*transaction authentication*): Aðferð til að bera kennsl á krefjanda við aðgerð eða færslu frekar en að sannvotta hann við innskráningu eða við stofnun tengilotu.

[10] Í dreifilyklaskipulagi er áskrifandi sá sem gerir samning við útgefanda rafrænna skilríkja og vottorðshafi sá sem vottaður er í skilríkjunum. Hér er eingöngu miðað við útgáfu hefðbundinna einkaskilríkja þar sem áskrifandi og vottorðshafi er sami einstaklingurinn. En þegar gefin eru út starfsskilríki sem vottar starfsmann fyrirtækis þá er áskrifandinn sá lögaðili sem skilríkin eru gefin út fyrir (fyrirtækið sem starfsmaðurinn starfar hjá) en starfsmaðurinn sem er vottaður er vottorðshafinn. Þegar um búnaðar- eða skipulagsskilríki er að ræða er í raun engin vottorðshafi í þeim skilningi, enda er það búnaður annars vegar og skipulagsheild hins vegar sem er vottað í skilríkinu.

Hart skilríki (*hard certificate*): Snjallkort eða annar öruggur vélbúnaður sem inniheldur rafrænt skilríki ásamt dulmálslykli.

Heimilun (*authorisation*): Það að heimila eitthvað, eins og aðgangsréttindi að kerfum og gögnum.

Kenni (*identity*): Samheiti fyrir auðkenni. Getur vísað til stakra einkenna eða eiginleika sem eru þættir í auðkenni einstaklings.

Krefjandi (*claimant*): Sá aðili sem þarf að auðkenna með því að beita samskiptahætti sannvottunar.

Mjúkt skilríki (*soft certificate*): Rafrænt skilríki sem er gefið út og afhent án sérstaks vélbúnaðar. Mjúkt skilríki er gjarnan dulmálslykill sem vistaður á diski í tölvu eða á öðrum almennum miðli. Venjulega eru mjúk skilríki umlukin aðgangslagi þannig að ekki sé hægt að beita dulmálslyklinum nema með notkunaraðgangsorði eða PIN-númeri.

Rafræn sannvottun (*electronic authentication*): Ferlið við að byggja upp traust á auðkennum notanda sem sett eru fram á rafrænan hátt gagnvart upplýsingakerfi.

Rafræn undirskrift (*electronic signature*): Gögn í rafrænu formi sem fylgja eða tengjast rökrænt öðrum rafrænum gögnum og eru notuð til að sannprófa frá hverjum hin síðarnefndu gögn stafa.

Rafrænn sannvottunarfasi (*electronic authentication phase*): Sá fasi sannvottunar á notanda þar sem rafræn auðkenni hans sem krefjanda eru sannprófuð. Hinn fasinn er skráningarfasi þar sem notandinn fær tóka og/eða önnur auðkennagögn til að nota síðar sem krefjandi.

Rafrænt auðkenni (*electronic identity credentials*): Rafræn gögn og/eða tóki sem gefin eru út af traustum ytri aðila sem ætluð eru til að staðfesta fullyrðingu um auðkenni einstaklings.

Rafrænt sannvottunarferli (*electronic authentication process*): Ferli rafrænnar sannvottunar. Sjá hugtakið „rafræn sannvottun“.

Rafrænt skilríki (*electronic certificate; electronic credentials*): Í flestum tilvikum samheiti fyrir rafrænt vottorð en getur einnig innihaldið tóka og notendabúnað sem gerir mögulegt að beita vottorðinu á öruggan hátt. Dæmi um slíkt er örgjörvi á snjallkorti (til dæmis debetkorti) sem inniheldur mörg rafræn vottorð og einkalykla sem varðveittir er í öruggum búnaði með dulritunarvirkni.

Rafrænt skírteini (*electronic credentials*): Rafræn gögn og/eða tóki sem gefin eru út af traustum ytri aðila sem ætluð eru til að staðfesta fullyrðingu um auðkenni, heimild, réttindi eða aðrar staðreyndir. Ef rafræn skírteini staðfesta auðkenni einstaklings eru þau rafrænt auðkenni. Rafrænu gögnin geta hvort sem er verið í fórum áskrifandans eða varðveitt á rafrænan hátt hjá auðkennaveitunni sem staðfestir tengslin á milli tóka áskrifandans og auðkenna hans.

Rafrænt vottorð (*electronic certificate*): Vottorð á rafrænu formi sem tengir sannprófunargögn við vottorðshafa og staðfestir hver hann er. Í umfjöllun um þætti dreifilyklaskipulags er oftast átt við dreifilyklaskilríki sem inniheldur dreifilykil vottorðshafa ásamt öðrum gögnum, dulritað með einkalykli vottunarstöðvar.

Raunveruleg kenni (*real-world identity*): Þau kenni sem vísa til raunverulegra einkenna eða eiginleika, eins og nafn, aldur eða lífkenni, en ekki rafrænnar framsetningar á kennum.

Samskiptaháttur (*protocol*): Reglur sem ákvarða hegðun viðfanga eða hluta þegar þeir skiptast á boðum. Stundum kallað „samskiptareglur“ eða „aðgerðarlýsing“.

Samskiptaháttur sannvottunar (*authentication protocol*): Skilgreind röð skeyta á milli krefjanda og sannprófanda sem sýna fram á að krefjandinn hafi umráð og stjórn á gildum tóka til að staðfesta auðkenni sín og, ef óskað er, til að sýna krefjandanum fram á að hann sé í samskiptum við ætlaðan sannprófanda. Lýsir þannig aðferð við sannvottun.

Sannprófandi (*verifier*): Aðli sem sannprófar auðkenni krefjandans með því að sannprófa umráð og stjórn krefjandans á þeim tóka sem notaður er í samskiptahætti fyrir sannvottun.

Sannprófun (*verification*): Það ferli eða það atvik að staðfesta sannleika eða gildi einhvers.

Sannvottun (*authentication*): Staðfesting á upplýsingum sem settar eru fram sem fullyrðingar (til dæmis safn eiginda) með tilgreindu eða þekktu stigi trúverðugleika.

Sannvottunaraðferð (*authentication mechanism*): Aðferð sem notuð er til að sannvotta upplýsingar um auðkenni eða eigindi sem settar eru fram sem fullyrðingar.

Sannvottunarháttur (*authentication protocol*): Sama og „samskiptaháttur sannvottunar“.

Sannvottunartóki (*authentication token*): Tóki sem notaður er til sannvottunar.

Skírteini (*credential*): Gögn sem gefin eru út af traustum ytri aðila sem ætluð eru til að staðfesta fullyrðingu um auðkenni, heimild, réttindi eða aðrar staðreyndir.

Skráningarstöð (*registration authority*): Traustur aðili sem er ábyrgur fyrir auðkenningu og sannvottun á áskrifanda en gefur ekki út rafræn auðkenni. Skráningarstöð staðfestir og tekur ábyrgð á kennum eða eigindum áskrifanda gagnvart auðkennaveitu. Skráningarstöðin getur verið hluti af starfsemi auðkennaveitu eða sjálfstæður aðili sem hefur tengsl við auðkennaveitu.

Skráningarfasi (*registration phase*): Sá fasi sannvottunar á notanda þar sem raunveruleg kenni notandans sem áskrifanda eru staðfest og hann fær afhent tóka og/eða önnur auðkennagögn sem rafræn auðkenni. Hinn fasinn er rafrænn sannvottunarfasi þar sem rafræn auðkenni krefjandans (það er að segja, notandans sem krefjanda) eru sannprófuð.

Staðfesting á gildi auðkenna (*credential validation*): Staðfesting auðkennaveitunnar sem gaf auðkennagögnin út á gildi auðkennanna gagnvart sannprófanda.

Staðhæfing (*assertion*): Fullyrðing frá sannprófanda til treystanda sem inniheldur upplýsingar um kenni áskrifanda. Staðhæfingar geta einnig innihaldið sannprófaðar eigindir (e. verified attribute).

Staðlað skilríki (*nomalized certificate*): Skilríki sem uppfyllir staðlaðar vottunarkröfur (e. normalized certificate policy). Staðlaðar vottunarkröfur jafngilda fullgildum vottunarkröfum (e. qualified certificate policy) að öllu leyti nema að ekki er gerð krafa um beitingu skilríkjanna í öruggum notendabúnaði.

Stafræn undirskrift (*digital signature*): Í þessu skjali er stafræn undirskrift það sama og rafræn undirskrift. Oft er hugtakið stafræn undirskrift notað um dulmálsfræðilega vörpun gagna, til dæmis til að staðfesta yfirráð yfir einkadulmálslykli í rafrænni sannvottun, en hugtakið rafræn undirskrift er til aðgreiningar notað um beitingu á stafrænni undirskrift í skilgreindri útfærslu sem staðfestir samþykki undirritanda á gögnunum þannig að ekki er hægt að hrekja það.

Sterkt aðgangsorð (*strong password*): Aðgangsorð með upplýsingaóreiðu (e. information entropy) sem jafngildir að minnsta kosti 60 stafa aðgangsorði í tvílotukerfi. Aðgangsorð með

táknum úr útvíkkaða ASCII stafasettinu (innheldur 218 tákn) þarf að vera að minnsta kosti 8 tákn til að teljast sterkt aðgangsorð.

Sönnun á kennum (*identity proofing*): Ferlið fyrir söfnun og sannprófun á upplýsingum um einstakling hjá auðkennaveitu og skráningarstöð í þeim tilgangi að gefa rafræn auðkenni út fyrir einstaklinginn.

Sönnun á umráðum (*proof of possession*): Sönnun á því að krefjandinn ráði yfir tilteknum tóka og/eða auðkennagögnum til rafrænnar sannvottunar.

Tóki (*token*): Eitthvað sem krefjandi hefur umráð yfir og stjórn á sem nota má til að sannvotta auðkenni hans, til dæmis einkalykill, dulmálsbúnaður eða aðgangsorð.

Treystandi (*relying party*): Aðli sem treystir á rafræn auðkenni áskrifandans eða staðhæfingu sannprófanda á kennum krefjanda, til dæmis til að framkvæma færslu eða heimila aðgang að upplýsingum eða kerfum.

Umráð og stjórn á tóka (*possession and control of a token*): Sú hæfni að geta virkjað og notað tókann í sannvottunarsamskiptum.

Upplýsingaóreiða (*information entropy*): Mæling á óvissu í upplýsingum eða upplýsingaboðum sem byggir á kennisetningum Shannon[11]. Upplýsingaóreiða er notuð til að mæla styrkleika aðgangsorða með vísun til lengdar tvílotustrengs með sömu óvissu. Upplýsingaóreiða segir þannig til um hversu erfitt er að giska á aðgangsorð eða finna út á annan hátt hvert það er.

Út-úr-leið aðferð (*out-of-band method*): Aðferð til staðfestingar sem notar tengingu eða önnur samskipti sem eru óháð þeirri meginleið sem notuð er í samskiptum notanda við þjónustuveituna. Dæmi um slíka aðferð er að biðja notanda sem tengdur er þjónustuveitu yfir Internetið um staðfestingu við innskráningu með SMS-skeyti úr farsíma hans, sem fer yfir farsímakerfið óháð Internettengingu notandans við þjónustuveituna.

Veikt aðgangsorð (*weak password*): Aðgangsorð með upplýsingaóreiðu sem jafngildir minna en 60 stafa aðgangsorði í tvílotukerfi. Aðgangsorð með táknum úr útvíkkaða ASCII stafasettinu (inniheldur 218 tákn) sem er styttra en 8 tákn er yfirleitt talið veikt aðgangsorð.

Viðurkenndur útgefandi (*accredited issuer*): Aðili sem er viðurkenndur eða faggildur í samræmi við staðlaðar og/eða opinberar kröfur.

Vottorðshafi (*certificate subject*): Einstaklingur, lögaðili, skipulagseining eða búnaður sem auðkenndur er í skilríkjum sem handhafi þess lyklapars, einkalykils og dreifilykils, sem tilgreint er í skilríkjunum. Í þessu skjali er vottorðshafi áskrifandi sem fær lyklapar í eigin nafni.

Vottunarstöð (*certification authority*): Aðili sem nýtur trausts hagsmunaaðila til að framleiða, undirrita og gefa út skilríki. Stundum kallað „vottunaraðili“.

Vottunarþjónusta (*certification service provider*): Vottunarstöð sem veitir alhliða þjónustu sem getur innifalið skráningu og sannvottun á kennum áskrifenda, framleiðslu og afhendingu tóka og annarra auðkennagagna og staðfestingu á gildi rafrænna auðkenna gagnvart treystendum.

[11] Claude E. Shannon skrifaði grein árið 1948, *A Mathematical Theory of Communication*, sem lagði grunninn að fræðilegum bakgrunni óreiðu í upplýsingum.

Öruggur undirskriftarbúnaður (*secure signature-creation device*): Búnaður fyrir rafræna undirritun sem uppfyllir kröfur sem kveðið er á um í 8. gr. laga um rafrænar undirskriftir, nr. 28/2001.

2.3 SKAMMSTAFANIR

Eftirfarandi skammstafanir eru notaðar í þessari skýrslu. Skýringar á ensku eru skáletraðar í sviga.

Skammstafanir notaðar fyrir gæðaþætti í STORK QAA líkaninu:

AM Sannvottunaraðferð (***A**uthentication **M**echanism*).

EA Rafrænn sannvottunarfasi (***E**lectronic **A**uthentication Phase*).

IC Skírteinaútgáfa (***I**ssuing **C**redentials*).

ID Auðkenningarferli (***Id**entification Procedure*).

IE Útgáfuaðili (***I**ssuing **E**ntity*).

RC Traustleiki skírteina (***R**obustness of the **C**redential*).

RP Skráningarfasi (***R**egistration **P**hase*).

Aðrar skammstafanir:

EAL Fullvissuþrep úr mati (***E**valuation **A**ssurance **L**evel*). Matsþrep á upplýsingatæknibúnaði eða kerfi sem tilgreint er eftir mat á öryggi samkvæmt alþjóðlega staðlinum *Common Criteria*. EAL matsþrep segir ekki til um öryggi búnaðar eða kerfis heldur á hvaða matsþrepi kerfið eða búnaðurinn var metinn.

IDABC ***I**nteroperable **D**elivery of European eGovernment Services to public **A**dministrations, **B**usinesses and **C**itizens*. Vettvangur Evrópusambandsins fyrir samstarf þjóða í framþróun rafrænnar stjórnsýslu þar til ISA tók við í janúar 2010.

ISA ***I**nteroperability **S**olutions for European Public **A**dministrations*. Vettvangur Evrópusambandsins fyrir samstarf þjóða um samvirkni í rafrænni stjórnsýslu. Tók við af IDABC í janúar 2010.

ISO Alþjóðlegu staðlasamtökin (e. The International Organization for Standardization). ISO er í raun ekki skammstöfun heldur tekið upp af samtökunum sem skammheiti, byggt á gríska orðinu *isos* sem þýðir „jafn“.

NIST ***N**ational **I**nstitute of **S**tandards and **T**echnology*. Staðlaráð Bandaríkjanna.

OCES ***O**ffentlige **C**ertifikater til **E**lektronisk **S**ervice*. Staðall fyrir opinber rafræn skilríki í Danmörku.

QAA Gæði fullvissu sannvottunar (***Q**uality **A**uthentication **A**ssurance*).

STORK Stór verkefni í Upplýsingatækniáætlun Evrópusambandsins undir Samkeppnis- og nýsköpunaráætluninni um rafræn auðkenni yfir landamæri (***S**ecure Iden**t**ity Acr**o**ss Bo**r**ders Lin**k**ed*). Fyrra verkefnið, STORK, var í gangi frá júní 2008 til desember 2011 en síðara verkefnið, STORK 2.0, hófst í apríl 2012 og stendur í þrjú ár.

3 STORK QAA FULLVISSUSTIG

Viðmið fyrir fullvissustig eru forsenda fyrir mati á ásættanlegri auðkenningu og samhæfingu á milli aðila. Þess vegna er sameiginleg skilgreining á fullvissustigum mikilvæg fyrir samskipti og þjónustu, hvort sem er innan Íslands eða yfir landamæri ríkja, til dæmis á innri markaði Evrópusambandsins.

STORK (*Secure Identity Across Borders Linked*)[12] var samstarfsverkefni 18 Evrópuþjóða um uppbyggingu á kerfi fyrir samvirkni rafrænna auðkenna á milli landa. Ein af megin afurðum verkefnisins var samkomulag allra þátttakenda um svokölluð fullvissustig rafrænna auðkenna og skilgreiningu á undirliggjandi kröfum. Skilgreiningin var gefin út í skjalinu *D2.3 – Quality authenticator scheme*[1] og er venjulega vísað til hennar sem „STORK QAA“ [13].

Í STORK QAA eru sett fram fjögur fullvissustig, svokölluð QAA-stig 1 til 4. STORK QAA fullvissustigunum er raðað eftir því hversu alvarleg áhrif verða af skaða ef óréttmætur aðgangur er veittur vegna mistaka við sannvottun á auðkennum. Því meiri sem skaðinn yrði því meira traust þarf að vera á staðfestum auðkennum notandans hjá þeim sem veitir aðgang að þjónustu eða gögnum. STORK QAA fullvissustigin eru skilgreind þannig:

STORK QAA	LÝSING	ÁHRIF AF SKAÐA
QAA 1	Engin eða lágmarks fullvissa.	Mjög lítil eða hverfandi áhrif.
QAA 2	Lítil fullvissa.	Lítil áhrif.
QAA 3	Veruleg fullvissa.	Veruleg áhrif.
QAA 4	Mikil fullvissa.	Mikil áhrif.

Tafla 1: Fullvissustig STORK QAA.

STORK QAA 1 er lægsta fullvissustig; tiltrú á staðhæfðum auðkennum er annað hvort engin eða í lágmarki. Auðkenningargögn eru samþykkt án nokkurrar sannprófunar. Ef áskrifandinn gefur upp tölvupóstfang þá er einungis staðfest hvort það er virkt póstfang. Þetta fullvissustig er viðeigandi þegar neikvæðar afleiðingar af rangri sannvottun eru mjög veigalitlar eða hverfandi. Fullvissustig QAA 1 hentar í rafrænni þjónustu þar sem litlar eða engar öryggisráðstafanir eru gerðar.

STORK QAA 2 skilgreinir það stig sem rafræn þjónusta þarf að nota þegar áhrif skaða af sviksamri beitingu raunverulegra auðkenna eru lítil. Þrátt fyrir að áskrifandinn þurfi ekki að mæta í eigin persónu við skráningu þá þarf að sannprófa raunveruleg auðkenni hans og sá aðili sem gefur út tóka, til dæmis aðgangsorð eða leynilykil, verður að falla undir sérstakt samkomulag við opinberan aðila. Ferlar við afhendingu auðkennatóka þurfa að vera ítarlegir

[12] STORK verkefnið var styrkt af Upplýsingatækniáætlun Evrópusambandsins undir Samkeppnis- og nýsköpunaráætluninni ((CIP) – ESB INFSO-ICT-PSP-224993). Verkefnið hófst á miðju ári 2008 og lauk í lok árs 2011. Heildarfjármagn verkefnisins var rúmir 4 milljarðar króna. Sjá nánar á vefslóðinni www.eid-stork.eu.
[13] STORK 2.0 er nýtt verkefni 19 þjóða í Evrópu sem byggir á afurðum í STORK verkefninu. STORK 2.0 hófst í apríl 2012 og stendur í þrjú ár. Áætlaður kostnaður við STORK 2.0 er rúmir 3 milljarðar króna. Í STORK 2.0 er byggt áfram á STORK QAA fullvissustigum.

og þannig að afhendingin sé örugg. Nota þarf nægilega trausta tilhögun við rafræna sannvottun á krefjanda þegar hann óskar eftir aðgangi að rafrænni þjónustu.

STORK QAA 3 skilgreinir það stig sem notað er af þjónustu sem gæti orðið fyrir verulegum skaða ef auðkenni eru misnotuð. Skráning á auðkennum fer fram með aðferðum sem staðfesta á skýran hátt og með mikilli vissu hver áskrifandinn er. Útgefendur auðkenna eru undir eftirliti eða viðurkenndir (e. accredited) af hinu opinbera. Rafrænu skírteinin sem eru afhent eru í það minnsta vottorð undirrituð af útgefanda, samanber rafræn skilríki. Rafrænu auðkennin eru send áskrifandanum í ábyrgðarpósti á staðfest lögheimili hans eða afhent rafrænt og virkjuð eftir staðfestingu áskrifandans með rafrænni undirskrift eða með einkaaðgangsorði sem hann fékk við skráningu þegar hann staðfesti kenni sín í eigin persónu. Fyrirkomulag við rafræna sannvottun fjartengdra notenda eru traustar.

STORK QAA 4 er hæsta fullvissustigið og á við þá þjónustu þar sem skaði af misnotkun auðkenna gæti haft mikil áhrif. Við skráningu þarf áskrifandinn annað hvort að koma minnst einu sinni í eigin persónu (það er að segja, í fyrsta skipti en ekki fyrir endurnýjun síðar) eða það þarf að hitta hann í eigin persónu til að staðfesta kenni hans (sem dæmi, ef beiðni um skilríki er lögð inn yfir Internetið, skilríkin síðan send heim til áskrifandans og afhent í hendur hans eftir að kennsl eru borin á hann í eigin persónu). Eða, þegar skráning fer fram yfir fjarskiptatengingu, þá þarf að staðfesta kenni áskrifandans með traustri rafrænni undirskrift hans. Fullvissustigi QAA 4 er fullnægt ef kröfur í lögum nr. 28/2001 um rafrænar undirskriftir[9][14] eru uppfylltar. Jafnframt þarf auðkennaveitan að vera fullgildur vottunaraðili samkvæmt kröfum í V. kafla í lögum nr. 28/2001. Skilríkin eru svokölluð hörð skilríki, fullgild vottorð í öruggum undirskriftarbúnaði samkvæmt lögum nr. 28/2001 um rafrænar undirskriftir[15]. Notuð er eins traust tilhögun og möguleg er við rafræna sannvottun þegar skilríkjunum er beitt.

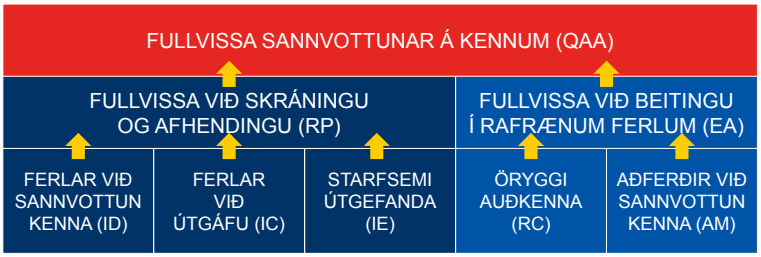
[14] V. kafli í lögum nr. 28/2001 um rafrænar undirskriftir uppfyllir viðauka II í tilskipun Evrópuþingsins og ráðsins 1999/93/EB um rafrænar undirskriftir[7]. Tilskipunin skilur smáatriði í útfærslu á sannprófun kenna eftir fyrir lagasetningu í hverju landi.

[15] 7. gr. laga nr. 28/2001 um rafrænar undirskriftir uppfyllir Viðauka I í tilskipun Evrópuþingsins og ráðsins 1999/93/EB um rafrænar undirskriftir[7].

4 KRÖFUR STORK QAA FULLVISSUSTIGA

Í STORK QAA skjalinu *D2.3 – Quality authenticator scheme*[1] er ítarleg lýsing á sundurgreindum kröfum sem liggja á bak við QAA fullvissustigin. Í þessum kafla er lýsing á nálguninni sett fram í þeim tilgangi að styðja umfjöllun um styrkleika mismunandi rafrænna auðkenna í kafla 6 og mat á STORK QAA fullvissustigi þeirra.

Fullvissustig sannvottunar á kennum (STORK QAA) eru skilgreind í tveimur þrepum eins og sýnt er á Mynd 2. Kröfur QAA fullvissustiganna fjögurra eru samsettar úr kröfum í skráningu og afhendingu annars vegar (RP) og kröfum í rafrænni sannvottun við beitingu rafrænna auðkenna hins vegar (EA). Hvor þessara meginþátta er samsettur úr undirþáttum. Í heild eru þessi undirþættir fimm þar sem þrír mynda skipulagslegar kröfur í skráningu og afhendingu (ID, IC og IE mynda RP) og tveir mynda tæknilegar kröfur við beitingu í rafrænum ferlum í sannvottunarfasanum (RC og AM mynda EA - sjá Mynd 2). Fyrir hvern af þessum fimm undirþáttum eru tilgreindar gæðakröfur sem vísa til fullvissustiga frá QAA 1 til QAA 4.



Mynd 2: Þættir sem hafa áhrif á fullvissustig sannvottunar.

Þegar öryggislegur styrkleiki tiltekinna rafrænna auðkenna er metinn þá ræður lægsta gæðastig meðal þessara fimm undirþátta því heildar QAA fullvissustigi sem auðkennin geta veitt. Það er því veikasti hlekkurinn sem takmarkar það traust sem hægt er að bera til rafrænnar sannvottunar með tilteknum rafrænum auðkennum.

4.1 FULLVISSA VIÐ SKRÁNINGU OG AFHENDINGU

Fullvissa við skráningu og afhendingu auðkenna ræðst í fyrsta lagi af öryggi ferla við sannvottun á kennum þess sem fær rafrænu auðkennin (sannvottun áskrifanda). Þar skiptir máli hvort þess er krafist að sá sem er sannvottaður mæti á staðinn, hvernig kenni hans eru staðfest og hversu mikil vissa er fyrir því að um réttan einstakling sé að ræða.

Í öðru lagi ræðst fullvissustigið af öryggi ferla við útgáfu auðkennanna. Þar skiptir máli hvernig auðkennin eru afhent eða send til áskrifandans og hvort auðkennin og tengd gögn og búnaður eru afhent í einu lagi eða skipt í hluta sem miðlað er eftir ólíkum leiðum.

Í þriðja lagi ræðst fullvissustigið af öryggi í starfsemi útgefandans við framleiðslu og útgáfu auðkennanna, það er hvort hann uppfyllir tiltekin viðmið og hvort starfsemin er tekin út, viðurkennd með fullgildinu, vottuð eða á annan hátt staðfest af traustum ytri aðila.

4.1.1 Gæði verklags við auðkenningu

Þetta er það fyrirkomulag sem er á auðkenningu áskrifandans áður en sannvottunartóki er gefinn út. Það stig sem auðkenningarferlið nær er háð nokkrum þáttum:

(i) Viðvera áskrifandans í eigin persónu á einhverjum tímapunkti í auðkenningarferlinu.

a. Viðveru áskrifandans í eigin persónu til að auðkenna hann er yfirhöfuð ekki krafist. Með öðrum orðum þá er aldrei raunverulegur fundur með áskrifandanum.

b. Viðveru áskrifandans í eigin persónu til að auðkenna hann er krafist við skráningu. Þetta þarf að ske að minnsta kosti einu sinni (það þarf hugsanlega ekki viðveru við endurnýjun).

c. Viðveru áskrifandans í eigin persónu til að auðkenna hann er krafist þegar honum eru afhent rafrænu auðkennin (sem dæmi þá getur áskrifandinn skráð sig yfir Internetið en þarf að vera viðstaddur til að taka við auðkennunum). Þetta þarf að ske að minnsta kosti einu sinni (það þarf hugsanlega ekki við endurnýjun).

(ii) Gæði staðhæfinga um auðkenni áskrifandans:

a. Stök staðhæfing út frá gögnum sem tengjast áskrifandanum sem þurfa ekki endilega að vera þekkt af honum einum (til dæmis nafn hans eða fæðingardagur). Þetta þarf ekki að skila ótvíræðri auðkenningu.

b. Margföld staðhæfing út frá gögnum sem tengjast áskrifandanum sem þurfa ekki endilega að vera þekkt af honum einum (til dæmis nafn hans, fæðingardagur og lögheimili). Þetta þarf að skila ótvíræðri auðkenningu.

c. Staðhæfingar sem vísa að minnsta kosti til sértækra gagna sem einungis áskrifandinn er talin þekkja (til dæmis númer ökuskírteinis eða vegabréfs) og sem hægt er að sannprófa í einhverri opinberri skrá. Þetta skilar ótvíræðri auðkenningu.

(iii) Staðfesting þeirra staðhæfinga sem áskrifandi lætur í té um kenni sín, samkvæmt eftirfarandi tilfellum:

a. Staðfesting takmarkast við sannprófun á tölvupóstfangi, ef það er gefið upp. Annars fer engin sannprófun fram.

b. Staðfesting á staðhæfingu er gerð með því að bera saman staðhæfinguna sem veitt er við upplýsingar frá opinberum aðila eða við gagnagrunna með auðkennagögnum frá hlutlausum og traustum heimildum eins og bönkum, tryggingarfyrirtækjum eða opinberri stofnun.

c. Staðfestingin þarf að vera undirrituð með stafrænni undirskrift (sem þarf þó ekki að vera fullgild).

d. Staðfestingin krefst þess að sýnd séu raunlæg persónuskilríki gefin út af opinberum aðilum eins og nafnskírteini, vegabréf eða ökuskírteini sem hafi að minnsta kosti ljósmynd og/eða handritaða undirskrift.

e. Staðfestingin krefst þess að staðhæfingin sé undirrituð með stafrænni undirskrift sem er sannprófuð af vottunarþjónustu áður en tókinn eða auðkennagögnin (e. credentials) eru gefin út.

Í eftirfarandi töflu eru sýnd stigin fyrir gæði verklags við auðkenningu (ID1-ID4). Þau samsvara því hversu miklar kröfur þau uppfylla.

Kröfur		Gæðastig verklags við auðkenningu (ID)			
		ID1	ID2	ID3	ID4
Viðvera	Ekki krafist, þ.e.a.s. af tegund (i.a). Skráning er yfir Internetið.				
Gæði staðhæfingar	Að minnsta kosti af tegund (ii.a).	●			
Staðfesting staðhæfingar	Að minnsta kosti af tegund (iii.a).				
Viðvera	Ekki krafist, af tegund (i.a).				
Gæði staðhæfingar	Að minnsta kosti af tegund (ii.b).	●	●		
Staðfesting staðhæfingar	Af tegund (iii.b).				
Viðvera	Krafist, af tegund (i.b).				
Gæði staðhæfingar	Að minnsta kosti af tegund (ii.b).	●	●	●	
Staðfesting staðhæfingar	Að minnsta kosti af tegund (iii.c)				
Viðvera	Ekki krafist, þ.e.a.s. af tegund (i.a). Skráning er yfir Internetið.				
Gæði staðhæfingar	Af tegund (ii.c).	●	●	●	
Staðfesting staðhæfingar	Að minnsta kosti af tegund (iii.d)				
Viðvera	Krafist, að minnsta kosti af tegund (i.b).				
Gæði staðhæfingar	Af tegund (ii.c).	●	●	●	●
Staðfesting staðhæfingar	Að minnsta kosti af tegund (iii.d)				

Tafla 2: Gæðastig verklags við auðkenningu.

4.1.2 Gæði ferla við útgáfu auðkenna

Annar skráningarþáttanna varðar ferlið við útgáfu auðkennatóka og/eða auðkennagagna. Gæði útgáfuferlisins er háð því hvort afhending er í viðurvist áskrifanda, um tölvupóstkerfi eða landpóstflutning og hvort tókinn er afhentur sem ein upplýsingaeining eða sem aðskildir hlutir sem sameina þarf síðar.

Því meiri sem gæðin eru í verklagi við útgáfu því sterkari verða tengslin á milli þeirra auðkenna sem áskrifandinn setur fram við skráningu og raunverulegra auðkenna hans í rafrænni sannvottun á seinni stigum. Hæsta stig (afmarkað við útgáfuferlið) næst þegar afhending fer fram í viðurvist áskrifandans. Athugið að til að ná hæsta stigi í skráningarfasanum þarf afhending í eigin persónu að tengjast hæsta stigi auðkenningarferlisins; þetta gerir þá kröfu að auðkenni móttakandans séu staðfest með persónuskilríkjum gefnum út af opinberum aðila (staðfestingin fari fram annað hvort hjá útgefanda eða með sannvottaðri afhendingu á öðrum tilgreindum stað).

Eftirfarandi tafla skilgreinir lágmarkskröfur fyrir hvert stig útgáfuferilsins (IC1-IC4).

Kröfur	Gæðastig útgáfuferlis auðkenna (IC)			
	IC1	IC2	IC3	IC4
Auðkennagögnin eru fengin án nokkurrar sannprófunar.	●			
Auðkennagögnin eru fengin með léttvægri sannprófun á persónukennum áskrifandans (t.d. nafni hans og/eða lögheimili). Eftirfarandi dæmi sýna þessa tegund af útgáfu auðkennagagna: • Notendanafn og aðgangsorð eru send út í tveimur aðgreindum póstsendingum þar sem að minnsta kosti önnur sendingin er um landpóst (ekki tölvupóst) á lögheimili áskrifandans samkvæmt þjóðskrá. • Auðkennagögnunum er hlaðið niður af áskrifandanum eftir skráningarferlið. Niðurhalið fer fram með því að senda tengil á tölvupóstfang sem áskrifandinn gaf upp við skráningu; í þessu tilviki þarf að vera tímatakmörkun á virkni tengilsins (t.d. 24 klst.).	●	●		
Auðkennagögnin eru fengin með miðlungs sannprófun á persónukennum áskrifandands (t.d. nafni og/eða lögheimili). Eftirfarandi dæmi sýna þessa tegund af útgáfu auðkennagagna: • Auðkennagögnin eru send út með ábyrgðarpósti eftir að búið er að staðfesta að lögheimili áskrifandans er í samræmi við þjóðskrá. • Auðkennagögnunum er hlaðið niður af Internetinu eftir að áskrifandinn hefur undirritað staðhæfingarbeiðnina með fullgildri rafrænni undirskrift samkvæmt lögum nr. 28/2001 um rafrænar undirskriftir[9] og sem staðfest er af vottunarþjónustu. Auðkennin eru mynduð af vottunarþjónustunni um leið og staðfesting hefur fengist og hlaðið niður í vafra áskrifandans. • Auðkennagögnunum er hlaðið strax niður af áskrifandanum eftir að hann slær inn einkaaðgangsorð sem honum var afhent í eigin persónu þegar auðkenning sem er að minnsta kosti af stigi 3 fór fram (Tafla 2 - ID3).	●	●	●	
Auðkennagögnin eru fengin með sterkri sannprófun á persónukennum áskrifandans. Eftirfarandi dæmi sýna þessa tegund af útgáfu auðkenningagagna: • Auðkennagögnin eru afhent áskrifandanum í eigin persónu eftir staðfestingu á kennum. • Auðkennagögnin eru send til áskrifandans og virkjuð eftir staðfestingu á kennum hans (t.d. með skráningu í viðurvist áskrifandans).	●	●	●	●

Tafla 3: Gæðastig útgáfuferlis.

4.1.3 Gæði útgefanda auðkenna

Þriðja atriðið sem hefur áhrif á gæði fullvissu í skráningarfasa eru gæði þess aðila sem gefur út auðkennagögnin (vottorð, aðgangsorð, tóka). Útgefendur rafrænna auðkenna geta verið hvort sem er opinberir aðilar eða einkaaðilar. Slíkur útgáfuaðili gæti verið hefðbundin auðkennaveita sem gefur út einhverskonar aðgangsorð sem leyndarmál eða vottunarstöð sem gefur út undirrituð rafræn vottorð, til dæmis rafræn skilríki.

Gerður er greinarmunur á aðilum sem eru fullgildir samkvæmt kröfum til vottunaraðila sem gefa út fullgild vottorð í V. kafla í lögum nr. 28/2001 um rafrænar undirskriftir[9] og þeim sem eru það ekki. Einungis þeir sem teljast fullgildir geta boðið hæsta stig fullvissu.

Meðal þeirra sem ekki teljast fullgildir er gerður greinarmunur á þeim sem eru með fyrirkomulag sem er viðurkennt, undir eftirliti eða fullgilt af hinu opinbera og þeirra sem eru með tilhögun sem fellur ekki undir opinbert eftirlit, samþykki né fullgildingu (til dæmis fjármálafyrirtæki).

Eftirfarandi tafla skilgreinir lágmarkskröfur fyrir hvert stig útgefanda.

Kröfur	Gæðastig útgefanda auðkenna (IE)			
	IE1	IE2	IE3	IE4
Ekkert fyrirkomulag á samkomulagi við hið opinbera (engar opinberar kröfur, ekkert eftirlit, engin fullgilding).	●			
Með samning um uppfylltar kröfur við opinberan aðila.	●	●		
Með fullgildingu eða undir eftirliti hins opinbera.	●	●	●	
Fullgildur sem útgefandi fullgildra vottorða samkvæmt kröfum í V. kafla í lögum nr. 28/2001 um rafrænar undirskriftir[9].	●	●	●	●

Tafla 4: Kröfur um gæði útgefanda auðkenna.

4.1.4 Fullvissustig fyrir skráningarfasann

Í töflunni hér fyrir neðan eru teknir saman gæðaþættirnir þrír í fullvissustig fyrir allt skráningarferlið (RP1-RP4).

	Fullvissustig fyrir skráningarfasa (RP)			
	RP1	RP2	RP3	RP4
Gæði verklags við auðkenningu (Tafla 2)	ID1	ID2	ID3	ID4
Gæði ferlis við útgáfu auðkennagagna (Tafla 3)	IC1	IC2	IC3	IC4
Gæði útgefanda auðkennagagna (Tafla 4)	IE1	IE2	IE3	IE4

Tafla 5: Samsett gæðastig skráningarfasa.

Heildarstig fyrir skráningarfasann samanstendur af gæðastigum skráningarþáttanna þriggja. Almenna reglan er að stig heildar skráningarferlis getur ekki verið hærra en það stig sem krafist er af sérhverjum þáttanna þriggja.

4.2 FULLVISSA VIÐ BEITINGU Í RAFRÆNUM FERLUM

Í rafrænnum sannvottunarfasa er gildi sönnunargagnanna um kenni sem krefjandinn lætur í té (auðkennatóki og önnur auðkennagögn) sannprófað. Fullvissa við beitingu rafrænna auðkenna ræðst annars vegar af öryggi auðkennanna sjálfra og hins vegar af öryggisstigi aðferða við sannvottun þeirra. Gæði þessa fasa er háð þáttum eins og tegund auðkennatóka sem notaður

er, samskiptahætti sem notaður er í sannvottunarathuguninni og tilhögun við miðlun á niðustöðu fjar-sannvottunarinnar til krefjandans.

4.2.1 Tegundir og traustleiki auðkenna

Fyrsti þátturinn sem hefur áhrif á gæði fullvissu í rafræna sannvottunarfasanum er tegund rafræna auðkennatókans sem er notaður sem sönnun á umráðum. Gæðastig tókanna getur verið mjög mismunandi. Veflyklar og önnur aðgangsorð sem byggja á fáum bókstöfum eða tölustöfum teljast veik auðkenni[16] en fullgild rafræn skilríki[17] á hörðum miðli, eins og öruggum örgjörva, eru talin hafa mestan styrk auðkenna.

Helstu tegundir tóka eru eftirfarandi:

Notandanafn og aðgangsorð eða PIN: Stafastrengur sem gert er ráð fyrir að krefjandi leggi á minnið og haldi leyndum. Þessi tegund tóka er notuð fyrir þjónustu þar sem áhætta er lítil. Notandanafn getur verið annað hvort valið af krefjandanum eða ákveðið af þjónustuaðilanum. Almennt er notandanafn ekki leyndarmál svo það hefur ekki áhrif á sannvottunarstigið. Hins vegar er styrkleiki aðgangsorða eða PIN númera mismunandi eftir því hvort þjónustuveitandinn býr þau til sjálfvirkt, og þá jafnvel handahófskennt, eða hvort krefjandinn velur þau sjálfur við skráningu[18]. Aðgangsorð eru oft flokkuð í sterk aðgangsorð annars vegar og veik aðgangsorð hins vegar. Mörkin eru venjulega miðuð við upplýsingaóreiðu (e. information entropy) 60 stafa (bita) aðgangsorðs í tvílotukerfi. Aðgangsorð með handahófskenndum táknum úr útvíkkaða ASCII stafasettinu (sem innheldur 218 tákn) þarf að vera að minnsta kosti 8 stafir til að teljast sterkt aðgangsorð. Margir aðrir þættir geta haft áhrif á styrk aðgangsorðs, til dæmis ítarlegri kröfur sem útiloka endurtekningu á táknum, útilokun á orðum í orðasöfnum, útilokun á samsvörun við nafn eða kennitölu og læsing á innskráningu eftir tiltekinn fjölda innskráningartilrauna.

Aðgangsorðalisti: Listi yfir aðgangsorð (pappírslisti) sem er í raun einkatóki krefjandans. Inniheldur aðgangsorð (oft PIN) sem tengist gjarnan stöðuaðgangsorði (e. static password) eða PIN númeri í sannvottunarkerfi þjónustuaðila.

Tæki fyrir einskiptis aðgangsorð: Einkatæki sem myndar einskiptis aðgangsorð sem er einungis í gildi fyrir eina sannvottunarlotu. Í tilteknum tilvikum er einskiptis aðgangsorð myndað sem tímastimpill með því að beita dulmálsalgrími til að binda saman tímasetningu og leynifræ (e. secret seed) sem varðveitt er í tækinu. Í öðrum tilvikum bindur sérhæfður lesbúnaður saman samstæðan lykil sem varðveittur er í einkatækinu (til dæmis snjallkorti) og einskiptis bitastreng. Bitastrengurinn getur verið tímasetning, teljari í lesbúnaðnum eða, ef

[16] Það er ekki til nein nákvæm viðurkennd skilgreining á því hvenær aðgangsorð telst sterkt. Algengt er að miðað sé við að upplýsingaóreiða (e. information entropy) aðgangsorðs þurfi að samsvara streng í tvílotukerfi sem sé að lágmarki 60 bitar til að aðgangsorðið geti talist sterkt. Bandaríska staðlaráðið NIST leggur til að miðað sé við 80 bita lengd að lágmarki. Sjá meðal annars viðauka A í NIST staðli 800-63[4].

[17] Hér er notað hugtakið „fullgild skilríki" um rafræn vottorð sem uppfylla kröfur í lögum um rafrænar undirskriftir nr. 28/2001, þó svo þau séu hugsanlega ætluð til rafrænna auðkenninga en ekki fyrir fullgildar rafrænar undirskriftir.

[18] Í NIST 800-63 staðlinum[4] er sett fram einföld reikniregla út frá líkindafræði fyrir styrk aðgangsorða sem krefjandinn velur algjörlega sjálfur án nokkurra takmarkana – miðað við enskumælandi krefjanda. Í þeim tilvikum velur fólk gjarnan heil orð eða setningar. Samkvæmt þessari reiknireglu NIST þá skilar fyrsta tákn fjórum bitum í tvílotukerfi, næstu sjö skila tveimur bitum hvert og næstu tákn eftir það, upp að 20. tákni, skilar 1,5 bitum hvert. Hvert tákn eftir 21. tákn skila 1 bita hvert. 8 stafa aðgangsorð jafngildir þá 18 bita aðgangsorði í tvílotukerfi en ekki 52 bita aðgangsorði sem er tilfellið þegar val tákna (úr 95 tákna ASCII stafrófi) er algjörlega handahófskennt. Ef enskumælandi fær að velja sjálfur aðgangsorðið, og ekki eru gerðar kröfur um samsetningu tákna (e. composition rule) þá þarf lengd aðgangsorðsins að vera 44 stafir til að ná 60 bita óreiðu. Með því að bæta við kröfum um samsetningu til að tryggja að notuð séu tölur, sértákn og/eða bæði há- og lágstafir má stytta lengdina í 38 stafi.

tækið hefur takkaborð, áskorun frá sannprófandanum. Einskiptis aðgangsorð sem myndað er birtist venjulega á skjá á lesbúnaðnum og er miðlað til fjarþjónustunnar (til dæmis slegið inn á vefgátt þjónustunnar, hlaðið upp í vefgáttina sjálfkrafa eða sent sem SMS).

Mjúkt skilríki: Dulmálslykill sem gjarnan er vistaður á diski í tölvu, í USB-kubbi eða í öðrum miðli. Sannvottun er gerð með því að sanna umráð og stjórn á lyklinum. Venjulega er mjúka skilríkið dulritað með lykli sem tengist aðgangsorði (kallað notkunaraðgangorð) sem einungis notandinn þekkir; þess vegna þarf aðgangsorðið (t.d. PIN) til að virkja dulmálslykilinn og beita skilríkinu.

Fullgilt mjúkt skilríki eða sambærilegt: Mjúkt skilríki með tæknilega eiginleika sem uppfylla kröfurnar í 7. gr. laga nr. 28/2001 um rafrænar undirskriftir[9]. Undir þessa skilgreiningu falla einnig þau mjúku skilríki sem eru gefin út af opinberum aðilum með nákvæmlega sömu ferlum og fullgild skilríki; svokölluð stöðluð skilríki.

Hart skilríki: Snjallkort eða sambærilegir miðlar sem innhalda varinn dulmálslykil. Sannvottun er gerð með því að sanna umráð og stjórn á lyklinum.

Fullgilt hart skilríki eða sambærilegt: Hart skilríki með tæknilega eiginleika sem uppfylla kröfurnar í 7. gr. laga nr. 28/2001 um rafrænar undirskriftir.

Eftirfarandi tafla sýnir vörpun á tegundum tóka yfir í gæðastig. Kröfur til styrkleika tókanna byggja á því hversu vel þeir eru varðir gegn uppljóstrun eða fjölföldun, á notkun á mörgum mismunandi leiðum í beitingu þeirra og á lögum nr. 28/2001 um rafrænar undirskriftir.

Kröfur	Gæðastig tegunda og traustleika auðkenna (RC)			
	RC1	RC2	RC3	RC4
Tóki byggður á aðgangsorði eða PIN-númeri sem valið er af krefjandanum eða myndað sjálfvirkt. Uppfyllir ekki almenn viðmið fyrir sterk aðgangorð eða PIN-númer (til dæmis ekki nægilega langt, ekki blanda af bókstöfum, táknum og tölustöfum, endurnýtt o.s.fr.) og þess vegna veikt gagnvart ágiskunum eða orðalistaárásum.	●			
Tóki byggður á aðgangsorði eða PIN-númeri sem valið er af krefjandanum eða myndað sjálfvirkt. Uppfyllir almenn viðmið fyrir sterk aðgangorð eða PIN-númer (til dæmis nægilega langt, blanda af bókstöfum, táknum og tölustöfum, ekki endurnýtt o.s.fr.) og þess vegna ekki veikt gagnvart ágiskunum eða orðalistaárásum.	●	●		
Mjúk skilríki eða búnaðartóki fyrir einskiptis aðgangsorð.	●	●	●	
Fullgild mjúk skilríki samkvæmt 7. gr. laga nr. 28/2001 um rafrænar undirskriftir[9].	●	●	●	
Hörð skilríki.	●	●	●	
Fullgild hörð skilríki samkvæmt 7. gr. laga nr. 28/2001 um rafrænar undirskriftir[9].	●	●	●	●

Tafla 6: Tegundir og traustleiki auðkenna.

Ef skilríki eru fullgild vottorð samkvæmt kröfum í lögum nr. 28/2001 um rafrænar undirskriftir[9] þá er sönnunin sterkari (hærra fullvissustig) en þegar um er að ræða önnur vottorð vegna þess að fullgild vottorð eru sannprófuð í ferli sem er undir strangara eftirliti. Jafnframt

ætti notkun dulritunaralgríma við beitingu fullgildra skilríkja að geta veitt nægilega vernd gegn fölsun með þeirri tækni sem til er í dag (sjá einnig kröfur viðvíkjandi öruggum undirskriftarbúnaði í 8. gr. í lögum nr. 28/2001 um rafrænar undirskriftir[19]).

4.2.2 Öryggi tilhögunar við sannvottun

Það traust sem hægt er að bera til fyrirkomulags á fjar-sannvottun er háð öryggislegu þoli sannvottunarinnar. Hér er áreiðanleiki við sannvottun metinn með hliðsjón af alvarlegustu ógn sem er við sannvottun, sem er stuldur á auðkennum. Afbrotamaður þarf í flestum tilvikum að komast yfir upplýsingar eða gögn sem nota má til að auðkenna einstakling til að geta villt á sér heimildir. Það er hægt að nota margar mismunandi leiðir til þess, meðal annars að ná upplýsingum úr aflóga tölvubúnaði sem hefur verið hent án þess að hreinsa diska og minni nægilega vel, með því að leita í opinberum skrám, á Internetinu eða með því að vafra um samfélagsvefi eins og Fésbók (Facebook) eða MySpace í leit að persónulegum upplýsingum sem notendur hafa sett inn.

Þessar tegundir árása eru í grundvallaratriðum það sem kallað er félagslegt handlag (e. social engineering) sem er alvarleg tegund afbrota sem nýtir það að notandandinn er veikasti hlekkurinn í öryggiskeðjunni. Í þessari greiningu er áherslan á ógnir af árásum sem beinast einungis að sannvottunarsamskiptunum sjálfum. Þannig er hægt að stela auðkennum með röð árása á sannvottunarferlið. Eftirfarandi er listi yfir slíkar árásir.

1) **Ágiskun** (e. guessing) er einföld árás þar sem illvilja aðili reynir að giska á leyndarmál sem notað er í samskiptum (til dæmis aðgangsorð, PIN-númer eða dulritunarlykil). Þessi árás skilar árangri þegar leyndarmálið er veikt, til dæmis einfalt aðgangsorð sem auðvelt er að giska á með orðalistum.

2) **Hlerun** (e. eavesdropping) er árás þar sem fylgst er með boðum sem fara um samskiptarás sem sannvottunarsamskiptin flæða meðal annars um. Oftast eru boðin vistuð í þeim tilgangi að greina þau nánar til að gera aðrar árásir síðar. Hlerun er gjarnan notuð þannig til að reyna að fanga tóka til að geta þóst vera krefjandinn.

3) **Lotustuldur** (e. hijacking) er árás sem felst í því að taka yfir (eða stela) samskiptalotu sem þegar hefur verið sannvottuð til að safna viðkvæmum upplýsingum. Í sannvottun getur lotustuldur verið hvort sem er á lotu krefjandans við treystandann (þjónustuveitu), lotu krefjandans við sannprófanda (sem sannprófar kennsl krefjandans) eða á lotu á milli þjónustuveitunnar og sannprófanda sem miðla á milli sín staðhæfingum um kenni og staðfestingum á þeim.

4) **Endursending** (e. replay) er aðferð við árás þar sem illvilja aðili endurtekur skeytasamskipti eða seinkar samskiptum sem áður hefur verið gripið inn í til að fá aðgang að viðkvæmum upplýsingum.

5) **Maður-í-milli**[20] (e. man-in-the-middle) er virk hlerun þar sem árásaraðilinn kemur upp margþættum tengingum við fórnarlömb sín og miðlar boðum á milli þeirra þannig að þeir haldi að þeir séu að tala beint við hvorn annan yfir einkasamband þegar sam-

[19] 8. gr. í lögum nr. 28/2001 um rafrænar undirskriftir uppfyllir kröfur í Viðauka III í tilskipun Evrópuþingsins og ráðsins 1999/93/EB um rafrænar undirskriftir[7].

[20] Maður-í-vafra (e. man-in-the-browser) árás er sérstök tegund af maður-í-milli árás sem nýtir sér veikleika í öryggi vefvafrans til að breyta upplýsingum sem fara á milli notandans og vefsíðu þjónustuaðilans. Notkun á öruggum samskiptum (eins og SSL dulritun) kemur ekki í veg fyrir maður-í-vafra árásir. Algengt er að nota svokallaðar „út-úr-leið" aðferðir (e. out-of-band) þegar þörf er á staðfestingu á aðgerðum eða færslum til að verjast maður-í-vafra árásum, til dæmis við millifærslu á fjármunum. Dæmi um slíka aðferð er að biðja um staðfestingu notandans með SMS-skeyti úr farsíma hans.

skiptunum er í raun stjórnað alfarið af árásaraðilanum. Árásaraðilinn verður að geta gripið inn í öll boðskipti á milli fórnarlambanna og skotið inn nýjum boðum.

Það er beint samband á milli fullvissustigs sannvottunarsamskiptanna og hversu þolin rafrænu auðkennin eru gagnvart þessum tegundum árása. Þetta þol gegn árásunum er þó alltaf metið með hliðsjón af tæknistigi þar sem árásir og varnir þróast samhliða í tíma. Þess vegna eru aðferðir við fjar-sannvottun flokkaðir í eftirfarandi töflu eftir staðfestu öryggi þeirra eða staðfestu óöryggi gagnvart þessum tilgreindu árásum eða veikleikum þeirra fyrir þeim, sem hægt er að færa sönnur á miðað við núverandi tæknistig.

Staðfest öryggi er erfitt hugtak. Það getur falið í sér þol byggt á reynslu, til dæmis þegar um er að ræða tilhögun sem hefur verið notuð um langan tíma án þess að vitað sé um öryggisbrest. Á hinn bóginn getur staðfest öryggi þýtt að öryggið sé formlega staðfest með rannsóknum og prófunum. Hafa ber í huga að erfitt getur reynst að skynja sumar tegundir árása, eins og lotustuld og maður-í-milli árás. Þegar tilgreint er að tilhögun hafi varnir (eða sterkar varnir) gegn árás þá er það með hliðsjón af núverandi tæknistigi.

Af þessum ástæðum er einungis hægt að lýsa efsta gæðastigi, stigi 4, formlega. Hin gæðastigin þurfa að byggja á öryggislegu sjálfsmati (e. security self-assessment). Bent er á EAL matsþrepin í „*Common Criteria*“[10] til leiðbeiningar við ákvörðun á öðrum gæðastigum.

Eftirfarandi tafla tekur saman kröfurnar fyrir fullvissustig tilhögunar við sannvottun.

Kröfur	Gæðastig öryggis í tilhögun við sannvottun (AM)			
	AM1	AM2	AM3	AM4
Tilhögun sannvottunar sem veitir litla eða enga vörn gegn ofangreindum árásum.	●			
Tilhögun sannvottunar sem veitir einhverja vörn gegn ofangreindum árásum.	●	●		
Tilhögun sannvottunar sem veitir vörn gegn flestum af ofangreindum árásum.	●	●	●	
Viðurkennd örugg tilhögun sannvottunar sem veitir vörn gegn öllum af ofangreindum árásum. Sambærilegt við EAL4+ eða hærra í „*Common Criteria*“[10].	●	●	●	●

Tafla 7: Gæðastig tilhögunar við sannvottun.

Hægt er að minnka ógnir af ofangreindum árásum með því að bæta við ótengdum aðgerðum í sannvottunarfasanum, eins og út-úr-leið staðfestingum og staðfestingu á endabúnaði krefjandans (e. device profiling). Út-úr-leið staðfestingar, til dæmis með staðfestingu í farsíma með SMS skeyti, geta komið í veg fyrir að maður-í-milli árásir nái að villa fyrir krefjandanum og þjónustuveitunni og takmarka einnig möguleika á árás með endursendingu skeyta. Staðfesting á búnaði með samanburði við þann búnað sem krefjandinn hefur notað áður getur gert erfiðara að gera árásir með ágiskunum eða lotustuld. Með því að tengja slíkar aðferðir saman er mögulegt að verjast öllum ógnum sem tilgreindar eru hér fyrir ofan að einhverju marki. Hversu öflug slík tilhögun getur orðið er háð því hvernig staðið er að skráningu viðbótargagna (eins og á farsímanúmeri eða auðkennum búnaðar) og hvernig kerfisleg útfærsla er. Þar gilda sömu lögmál og fyrir fullvissustig rafrænna auðkenna í heild.

4.2.3 Fullvissustig fyrir rafræna sannvottunarfasann

Í töflunni hér fyrir neðan eru teknir saman gæðaþættirnir tveir sem ákvarða fullvissustig fyrir rafræna sannvottunarferlið (EA1-EA4).

	Fullvissustig fyrir rafrænan sannvottunarfasa (EA)			
	EA1	EA2	EA3	EA4
Tegund og traustleiki auðkennatóka (Tafla 6)	RC1	RC2	RC3	RC4
Öryggi tilhögunar við sannvottun (Tafla 7)	AM1-3	AM1-3	AM1-3	AM4

Tafla 8: Samsett gæðastig fyrir rafrænan sannvottunarfasa.

Eins og kom fram í síðasta kafla þá getur reynst erfitt að setja formleg viðmið fyrir staðfest öryggi, nema fyrir gæðastig AM4 með vísun í öruggan búnað sem uppfyllir matsþrep EAL4+ í „*Common Criteria*“[10]. Þar sem hin gæðastigin byggja á öryggislegu sjálfsmati þá er það látið liggja á milli hluta í samsettu gæðastigi í þessari töflu.

Þegar þörf er á því að meta hvort gæðastig er AM1, AM2 eða AM3 þá þarf að greina hversu þolin samvottunarsamskiptin eru gagnvart sérhverri tegund árása sem fjallað er um á bls. 25. Við slíkt mat verður að taka tillit til þeirra tæknilegu lausna sem úfærðar eru til að skynja og verjast árásunum og vega raunhæfar líkur á skaða, í ljósi reynslu og rannsókna.

4.3 STORK FULLVISSUSTIG

Tafla 9 sýnir hvernig STORK QAA fullvissustigin leiða af fullvissu við skráningu og afhendingu annars vegar (skipulagslegir þættir RP1-RP4[21]) og við beitingu í rafrænum sannvottunarferlum hinsvegar (tæknilegir þættir: EA1-EA4[22]).

STORK QAA FULLVISSUSTIG		Fullvissustig fyrir rafrænan sannvottunarfasa			
		EA1	EA2	EA3	EA4
Fullvissustig fyrir skráningarfasa	RP1	QAA 1	QAA 1	QAA 1	QAA 1
	RP2	QAA 1	QAA 2	QAA 2	QAA 2
	RP3	QAA 1	QAA 2	QAA 3	QAA 3
	RP4	QAA 1	QAA 2	QAA 3	QAA 4

Tafla 9: STORK QAA fullvissustig.

[21] RP vísar til skráningarfasa (e. registration phase). RP byggir á gæðastigi fyrir sannvottun á auðkennum (ID, e. identification), útgáfu auðkenna (IC, e. issuing of credentials) og fyrir styrk útgefanda (IE, e. issuing entity).
[22] EA vísar til rafrænnar sannvottunar (e. electronic authentication). EA byggir á gæðastigi fyrir öryggi auðkenna (RC, e. robustness of credential) og fyrir aðferðir við sannvottun (AM, e. authentication mechanism).

Styrkur hvers auðkennis sem verið er að meta ræðst af styrk skráningarfasa og sannvottunarfasa og ræður lægsta mat á undirþáttum því hvaða heildarmat auðkennið fær. Öryggi er aldrei betra en veikasti hlekkur öryggiskeðjunnar.

5 SANNPRÓFUN Á FÆRSLUAÐGERÐ

Það fer vaxandi að nota sértækar öryggisaðferðir í tengslum við færslur eða aðrar aðgerðir sem krefjandi vill framkvæma í kerfi þjónustuveitu. Bankar um allan heim hafa verið leiðandi í því að taka upp slíkar aðferðir til að verjast maður-í-milli árásum, þar með talið maður-í-vafra árásum, sem ógna öryggi í fjármagnsfærslum á milli reikninga og öðrum aðgerðum sem fela í sér skuldbindingu viðskiptavina þeirra.

Ástæðan er sú að undanfarin ár hefur orðið mikil aukning á maður-í-milli árásum þar sem illvilja aðilar reyna að komast á milli notandans og þjónustuveitunnar til að villa um fyrir báðum aðilum. Með slíkum árásum er krefjandinn látinn halda að hann sé að framkvæma þá færslu eða aðgerð sem hann ætlar, en þjónustuveitunni eru sendar aðrar upplýsingar sem hún gerir ráð fyrir að komi frá krefjandanum. Þannig má til dæmis breyta upphæð og reikningsnúmeri í beiðni um fjármagnsfærslu í netbanka. Hefðbundnar aðferðir við sannvottun á auðkennum krefjandans koma ekki í veg fyrir skaða af slíkum árásum.

5.1 VARNIR GEGN SVIKSAMLEGUM BREYTINGUM Á FÆRSLUGÖGNUM

Almennt má skipta vörnum í rafrænni þjónustu í tvennt. Í fyrsta lagi eru varnir gegn uppljóstrun upplýsinga sem einungis krefjandinn á að hafa aðgang að. Hins vegar eru varnir gegn sviksamlegum breytingum á færslum eða aðgerðum sem krefjandinn vill framkvæma. Varnir gegn uppljóstrun byggja á því að krefjandinn fái ekki réttindi til aðgangs að upplýsingunum fyrr en búið er að staðfesta auðkenni hans með fullvissu sem er af ásættanlegu stigi miðað við viðkvæmni gagnanna.

Varnir gegn sviksamlegum breytingum á færslugögnum, til dæmis með maður-í-milli árásum illvilja aðila, byggja hins vegar á því að sannprófa uppruna og heilleika færslugagnanna. Þannig er leitast við að hafa fullvissu fyrir því að krefjandinn vilji framkvæma þá færslu eða aðgerð sem hann óskar eftir, og að sú beiðni sem þjónustuveitandinn móttekur sé sú sem krefjandinn sendi. Slíkar aðferðir eru kallaðar færslusannprófun og felast í því að sannprófa að hinu eiginlega innihaldi færslu hafi ekki verið breytt með maður-í-milli eða maður-í-vafra árás.

Ekki má rugla færslusannprófun við hugtakið færslusannvottun. Færslusannvottun merkir einfaldlega aðferð til að sannvotta auðkenni krefjanda sem biður um færsluaðgerð. Færslusannvottun innifelur ekki sannprófun á heilleika færslugagnanna sjálfra. Í raun er færslusannvottun því ekki annað en sannvottun á auðkennum sem fer fram á þeim tímapunkti þegar krefjandi vill framkvæma færslu eða aðgerð.

Algengt er að þjónustuveitendur útfæri færslusannvottun undir því yfirskyni að auka öryggi við færslur og aðgerðir. Staðreyndin er hins vegar sú að slíkar aðferðir auka ekki öryggi við færslur eða aðgerðir, umfram það að sýna að krefjandi geti ennþá staðfest auðkenni sín þegar hann vill framkvæma færslu eða aðgerð. Færslusannvottun sem byggir á út-úr-leið aðferð, til dæmis með SMS skeytum, eykur vissulega líkur á því hver krefjandinn er, þar sem hann þarf að hafa stjórn á þeim endabúnaði sem notaður er í út-úr-leið aðferðinni (til dæmis farsímanum), en hún staðfestir ekki heilleika færslunnar.

Á sama hátt er ekki nægilegt að staðfesta heilleika færslugagna til að hafa ásættanlega fullvissu fyrir því að krefjandinn standi á bak við þær skuldbindingar sem felast í færslunni – að þær séu óhrekjanlegar. Það þarf líka að vera ásættanleg fullvissa fyrir því að krefjandinn sé í

raun sá sem hann segist vera, og sú fullvissa verður að tengjast á tryggan hátt sannprófuninni á heilleika færslugagnanna.

Það þarf því bæði fullvissu fyrir því hver vill framkvæma færsluna og fullvissu fyrir því hvaða færslu á að framkvæma. Ef fullvissustig auðkenningar á krefjandanum er ekki ásættanlegt takmarkar það þá fullvissu sem getur verið um færsluna sjálfa.

Af þessu er ljóst að útfærsla á færslusannprófun til að tryggja ásættanlegt öryggi í færslum og aðgerðum dregur ekki úr kröfum til fullvissustigs þeirra rafrænu auðkenna sem sannvottun á krefjandanum byggja á.

Algengt er að færslusannprófun sé annað hvort útfærð með út-úr-leið aðferð, til dæmis með staðfestingarkóta með SMS skeyti úr farsíma krefjandans, eða með öruggum dulritunarbúnaði þar sem færslugögnin eru rafrænt undirrituð.

5.2 FÆRSLUSANNPRÓFUN MEÐ ÚT-ÚR-LEIÐ AÐFERÐ

Til að út-úr-leið aðferð veiti ásættanlega vissu fyrir því hver færslugögnin eru þarf að birta færslugögn í endabúnaði sem tengist þeirri aðferð, til dæmis í farsíma ef sú leið er notuð. Ein leið er að kerfi þjónustuveitandans sendi SMS skeyti með færslugögnum í farsímanúmer sem krefjandinn hefur gefið upp þannig að hann geti lesið færslugögnin og samþykkt með staðfestingarkóta. Það dugir ekki að beita öryggisspurningum eða öryggiskótum eingöngu ef krefjandinn fær ekki að sjá þau færslugögn sem beðið er um staðfestingu á.

Öryggi í út-úr-leið aðferð yfir farsímatengingar byggir á því að skráning á farsímanúmeri fari fram á öruggan hátt og sé vernduð í kerfum þjónustuveitunnar. Ef illvilja aðili getur komist inn í skrána og breytt farsímanúmerinu, eða yfirtekið það á einhvern hátt, þá getur hann villt á sér heimildir þegar kemur að staðfestingu á færslugögnum. Öryggiskótar sem notkunaraðgangsorð fyrir endabúnað í út-úr-leið aðferð geta komið í veg fyrir slíka sviksemi.

Það er áhyggjuefni að það eru þekktar aðferðir með spillihugbúnaði í farsímum sem gera illvilja aðilum kleyft að komast inn í út-úr-leið SMS-skeytasamskipti. Slíkar árásir eru kallaðar maður-í-farsímanum árásir (e. man-in-the-mobile)[23].

5.3 FÆRSLUSANNPRÓFUN MEÐ RAFRÆNNI UNDIRSKRIFT

Rafrænt skilríki í öruggum búnaði, til dæmis í sérbyggðum örgjörva á snjallkorti, býður upp á mikilvæg verkfæri til að útfæra varnir gegn maður-í-milli árásum. Þar sem skilríkið inniheldur dulmálsfræðilegan búnað og leynilykil er mögulegt að dulrita gögn með rafrænni undirskrift krefjandans þannig að móttakandi geti staðfest að gögnunum hafi ekki verið breytt eftir undirritun. Á sama hátt getur þjónustuveita, sem hefur útfært rafrænt skilríki og öruggan dulmálsbúnað í sínum kerfum, dulritað gögn þannig að krefjandinn sem móttakandi getur staðfesta að gögnunum hafi ekki verið breytt frá því þau voru undirrituð af kerfi þjónustuveitunnar. Rafræn undirskrift á færslugögnum gefur þannig kost á öflugri færslusannprófun sem um leið er færslusannvottun á auðkennum krefjandans.

Til að verjast maður-í-milli árásum þarf krefjandinn að koma í veg fyrir að árásaraðilinn geti komist á milli lyklaborðsins sem notað er til að slá inn notkunaraðgangsorðið (PIN-númerið) og örugga búnaðarins (t.d. örgjörva) sem varðveitir leynilykilinn og beitir honum til

[23] Sem dæmi um maður-í-farsímanum árás (e. man-in-the-mobile – MitMo) má nefna ZitMo (Zeus-in-the-Mobile) sem er spillihugbúnaður sem ferðast í gegnum Zeus-sýkta tölvu yfir í farsíma. ZitMo sýkir meðal annars Windows Mobile, Android, Symbian og Blackberry farsíma. SpitMo (Spy-eye-in-the-Mobile) er annar spillihugbúnaður sem svipar til ZitMo.

dulritunar. Hefðbundið lyklaborð við tölvu með snjallkortalesara veitir töluverða vernd gegn maður-í-milli árásum almennt þar sem árásaraðilinn er á milli í samskiptunum við veituna en getur ekki komist inn í samskiptin á milli lyklaborðsins og örugga örgjörvans.

Hins vegar er erfitt að verjast maður-í-vafra árásum þar sem árásaraðilinn hefur komið tólum sínum fyrir inn í tölvu krefjandans og hefur stjórn á vafranum sem notaður er til samskipta við þjónustuveituna. Ein leið er að nota örugga snjallkortalesara með innbyggðu lyklaborði.

Á sama hátt þarf tölvukerfi þjónustuveitunnar að innihalda örugg kerfi sem geta tryggt að illvilja aðili geti ekki beitt leynilykli þjónustuveitunnar til að undirrita gögnin. Ef útfærslan á báðum endum útilokar þannig að maður-á-milli (og þar með talið maður-í-vafra) geti beitt dulritunarlyklunum þá er hægt að sannprófa heilleika samskiptanna og þar með staðfesta á óhrekjanlegan hátt að færslugögnin séu rétt og að þeim hafi ekki verið breytt.

Það er hins vegar hindrun að öruggir lesarar með innbyggðum lyklaborðum eru mun dýrari en einfaldari lyklaborðslausir lesarar. Það er því ekki raunhæft að ætla notendum almennt að vera með annað en einfaldan lesara. Í þeim tilvikum þarf þá einnig að huga að öðrum aðferðum til að tryggja ásættanlega sannprófun á færsluaðgerðum, eins og út-úr-leið aðferðum.

Undanfarin ár hefur verið mikil uppbygging á lausnum þar sem rafræn skilríki eru sett í farsíma. Þegar þörf er á sannvottun á krefjanda sem óskar eftir aðgangi að þjónustuveitu, eða þegar þörf er á sannprófun á færslugögnum, þá er skilríki farsímans notað til að dulrita gögn sem send eru yfir farsímakerfið. Rafræn skilríki á farsíma sameina þannig virkni rafrænna skilríkja í dulmálsbúnaði og út-úr-leið aðferða til sannvottunar. En maður-í-farsímanum árásir geta haft áhrif á öryggi slíkra lausn.

6 MAT Á AUÐKENNUM Í ALMENNRI NOTKUN

Nokkrar gerðir rafrænna auðkenna eru í almennri notkun á Íslandi til að stýra aðgangi yfir Internetið að rafrænni þjónustu. Algengast er að sannvottun hjá þjónustuveitum byggi á notandanafni og aðgangsorði. Veflykill ríkisskattstjóra er einnig orðinn töluvert almennur og virkar sem aðgangsorð inn á þjónustuveitur á vegum hins opinbera og þjónustusetur nokkurra félagasamtaka. Auðkennislykillinn, sem er búnaður sem kallar fram einskiptis aðgangsorð, er notaður ásamt notandanafni og aðgangsorði fyrir innskráningu í netbanka fjármálafyrirtækja, nema hjá Landsbankanum. Rafræn skilríki undir Íslandsrót eru rafræn vottorð sem hafa verið vaxandi undanfarin misseri sem auðkenni fyrir innskráningu í rafræna þjónustu. Rafræn skilríki eru almenn rafræn auðkenni og eru notuð fyrir innskráningu hvort sem er hjá hinu opinbera eða hjá einkaaðilum.

Í þessum kafla er lagt mat á fullvissustig þessara rafrænu auðkenna. Jafnframt er lagt mat á styrk svokallaðra OCES-skilríkja í Danmörku og NemID útfærslu á beitingu þeirra og á BankID auðkenna í Noregi í þeim tilgangi að hafa samanburð á íslenskum rafrænum auðkennum og auðkennum í nágrannalöndum sem sumir þekkja vel.

Þau rafrænu auðkenni sem lagt er mat á eru því eftirfarandi:

1. Hefðbundið notandanafn og aðgangsorð
2. Veflykill ríkisskattstjóra
3. Íslykill Þjóðskrár Íslands
4. Innskráning í netbanka með Auðkennislykli
5. Innskráning í netbanka hjá Landsbankanum
6. Rafræn skilríki undir Íslandsrót
7. OCES-skilríki og NemID í Danmörku
8. BankID í Noregi

Í skýrslunni eru rafræn auðkenni metin fyrst og fremst sem almenn auðkenni, til afnota fyrir einstaklinga í samfélaginu gagnvart mörgum þjónustuveitum. Í sumum tilvikum er þó um afmörkuð eða lokuð kerfi að ræða, eins og í tilviki hefðbundins notandanafns og aðgangsorðs sem í flestum tilvikum er rafrænt auðkenni inn á tiltekna þjónustuveitu og í tilviki Auðkennislykilsins sem er lokað kerfi fjármálafyrirtækja á Íslandi.

6.1 HEFÐBUNDIÐ NOTANDANAFN OG AÐGANGSORÐ

Yfirleitt er notandanafni úthlutað af þjónustuveitunni. Aðgangsorði er ýmist úthlutað af þjónustuveitunni eða það valið af notandanum sjálfum. Flestar þjónustuveitur auka fullvissuna með því að senda tölvupóst á uppgefið tölvupóstfang sem inniheldur tengil með vefslóð til að staðfesta skráningu.

Notendanöfn eru almennt ekki leyndarmál og hafa ekki mikið gildi fyrir sannvottun umfram það að vísa til aðgangsorðs, sem er hin eiginlegi aðgangstóki. Notendanöfn hafa því ekki áhrif á fullvissustigið.

Í mati á fullvissustigum hér fyrir neðan er tekið mið af algengustu notkun á notandanafni og aðgangsorði. Gert er ráð fyrir að skráning fari alfarið fram yfir Internetið og að auðkennaveitan, sem gert er ráð fyrir að sé sami aðili og þjónustuveitan sem krefjandinn vill fá aðgang að, geri ekki kröfu um aðra staðfestingu frá áskrifandanum sjálfum þegar hann virkjar

aðgangsorðið en að hann geti svarað tölvupósti á tiltekið tölvupóstfang sem hann sjálfur gefur upp við skráningu.

Eins og algengast er þá er gert ráð fyrir að notendur velji sjálfir aðgangsorðið. Þá inniheldur það gjarnan heilt orð eða samsetning úr orðum, þó það geti í sumum tilvikum líka innihaldið tölustafi og tákn. Upplýsingaóreiða slíkra aðgangsorða er umtalsvert lægri en ef val tákna er handahófskennt því auðveldara er að giska á röð stafa útfrá orðalistum.

Það er einnig gert ráð fyrir því hér að útgefandinn sé opinber aðili sem uppfyllir tilgreindar opinberar kröfur eða einkaaðili sem uppfyllir kröfur sem settar eru fram af opinberum aðila.

Miðað við þessar forsendur hefur hefðbundið notandanafn og aðgangsorð fullvissustig QAA 1.

Hefðbundið notandanafn og aðgangsorð			
Gæðaþættir	**Gæðastig**	**Fullvissustig fasa**	**Fullvissustig auðkenna**
Verklag við auðkenningu	ID2	RP2	QAA1
Útgáfuferli auðkenna	IC2		
Útgefandi auðkenna	IE2		
Tegund og traustleiki auðkenna	RC1	EA1	
Öryggi í tilhögun við sannvottun	AM3		

Tafla 10: Fullvissustig fyrir hefðbundið notandanafn og aðgangsorð.

Fullvissustig fyrir skráningarfasann er **RP2** og fullvissustig fyrir rafræna sannvottunarfasann er **EA1**.

Hefðbundið notandanafn og aðgangsorð getur farið upp í QAA 2 ef gerð er krafa um sterkt aðgangsorð. En hefðbundið notandanafn og aðgangsorð getur ekki haft hærra fullvissustig en QAA 2.

Þrátt fyrir að aðgangsorð sé sterkt geta eftirfarandi þættir komið í veg fyrir að fullvissustigið nái hærra en QAA 1:

- Auðkenning er ekki ótvíræð (til dæmis ekki gefin upp kennitala).
- Uppgefin kenni eru ekki staðfest í opinberum skrám eða í öðrum viðurkenndum gagnagrunnum.
- Engin sannprófun fer fram á auðkenningargögnum, ekki einu sinni í tölvupósti.
- Kröfur til auðkennaveitunnar liggja ekki fyrir eða hún uppfyllir ekki opinberar kröfur.
- Samskipti við þjónustuveituna eru ekki dulrituð eða varin á annan hátt.

Forsendur matsins eru í köflunum hér á eftir.

6.1.1 Gæði verklags við auðkenningu

Viðveru áskrifandans í eigin persónu er yfirhöfuð ekki krafist á neinum tímapunkti í auðkenningarferlinu (sjá (i.a) í kafla 4.1.1). Staðhæfing um auðkenni áskrifandans við skráningu byggir oftast á kennitölu og nafni sem skilar ótvíræðri auðkenningu, það er að segja að aðeins

einn einstaklingur kemur til greina samkvæmt uppgefinni kennitölu (sjá (ii.b)). Staðfesting á staðhæfingum eru gerðar með því að notandinn gefur upp tölvupóstfang við skráningu og þarf að hafa aðgang að því pósthólfi til að geta staðfest skráninguna og í sumum tilvikum er kennitölu jafnframt flett upp í þjóðskrá til að staðfesta staðhæfingu um kennitölu og tengt nafn (sjá (iii.b)).

Gæðastig verklags við auðkenningu fyrir hefðbundið notandanafn og aðgangsorð er þá **ID2**.

Ef áskrifandi er ekki beðinn um kennitölu eða önnur ótvíræð kenni þá ná gæði staðhæfinga ekki upp fyrir (ii.a). Auðkenningin er þá ekki ótvíræð og gæðastigið fellur niður í ID1.

Ef uppgefnum kennum er ekki flett upp í þjóðskrá eða öðrum traustum gagnagrunnum og staðhæfing takmarkast þannig við tölvupóstfang sem áskrifandinn gefur upp, þá nær staðfestingin ekki upp fyrir (iii.a). Gæðastigið verður þá ekki hærra en ID1.

Auðkenning fyrir hefðbundin aðgangsorð geta náð gæðastigi ID3 ef krafist er viðveru áskrifandans í eigin persónu við skráningu en þá þarf að fylgja því staðfesting á kennum áskrifandans með stafrænni undirskrift. Einnig getur gæðastigið náð ID3 ef skráningarstöðin staðfestir og skráir raunlæg persónuskilríki á traustan hátt, þrátt fyrir að áskrifandinn sé ekki viðstaddur í eigin persónu. Ef við það bætist að áskrifandinn mæti í eigin persónu í skráningu og fái aðgangsorðið afhent samfara því (eða það búið til), þá getur auðkenning fyrir hefðbundin aðgangsorð náð gæðastigi ID4.

Hér á landi er nokkuð um það að aðgangsorð séu afhent í netbanka notandans. Þá er auðkenning notandans byggð á fullvissustigi innskráningar í netbanka sem er QAA 2[24], þrátt fyrir að Auðkennislykillinn sé notaður. Þetta ræðst af því að Auðkennislykillinn er lokað kerfi sem er ekki með fullgildingu né undir eftirlit hins opinbera (sjá umfjöllun um innskráningu með Auðkennislykli í kafla 6.4). Sú aðferð hækkar því ekki gæðastig verklags við auðkenningu fyrir hefðbundið notandanafn og aðgangsorð úr ID2.

6.1.2 Gæði ferla við útgáfu auðkenna

Þar sem skráning er staðfest með því að áskrifandinn tengist þjónustuveitunni með tengli sem barst á tölvupóstfang sem hann gaf sjálfur upp við skráningu, og virkjar þannig aðgangsorðið, þá nær gæðastig útgáfuferlis auðkennanna **IC2**.

Ef engin slík sannvottun fer fram, þá er gæðastigið IC1.

Hægt er að ná gæðastigi IC3 fyrir hefðbundin aðgangsorð ef áskrifandinn undirritar staðhæfingarbeiðni (með ótvíræðum kennum hans) með fullgildri rafrænni undirskrift eða ef hann fær einkaaðgangsorð afhent í eigin persónu til að virkja aðgangsorðið yfir Internetið.

Hefðbundin aðgangsorð geta náð gæðastigi IC4 ef aðgangsorðið er afhent áskrifandanum í eigin persónu (eða það búið til) samfara sannvottun á opinberum persónuskilríkjum.

Það er vert að hafa í huga að ef aðgangsorð er afhent í netbanka notandans þá hækkar það ekki gæðastig útgáfuferils auðkennanna úr IC2, þar sem fullvissustig innskráningar í netbanka er QAA 2 fyrir öðrum aðilum en bönkum og sparisjóðum.

[24] Innskráning með notandanafni og aðgangsorði í netbanka Landsbankans gefur einungis fullvissustig QAA 1. Þjónustuveitan sem treystandi á rafrænu auðkennin getur ekki vitað í hvaða netbanka aðgangsorðið var sótt. Því má rökstyðja að ef aðgangsorði er miðlað í netbanka þá geti gæðastig við auðkenningu og útgáfu ekki farið upp fyrir ID1 og IC1. En í þessari skýrslu er gert ráð fyrir að fullvissustig í innskráningu í netbanka sé QAA 2.

6.1.3 Gæði útgefanda auðkenna

Notendur rafrænnar þjónustu leggja oft mikið traust á starfsemi þjónustuveitunnar, meðal annars í aðgangsstjórnun og verndun gagna. Algengt er að þjónustuveitur veiti aðgang að notendamiðuðum þjónustusíðum, eins og „mínum síðum“, án þess að fyrir liggi hvaða kröfur þjónustuveitan (sem auðkennaveita og útgefandi aðgangsorða) uppfyllir í rekstri sínum og starfsumhverfi.

Ef slíkar kröfur liggja hins vegar fyrir og byggja á einhverskonar samningi við opinberan aðila eða vísar í opinberar kröfur, eða ef um opinbera þjónustuveitu er að ræða sem birtir kröfurnar sem hún uppfyllir, þá er gæðastig útgefanda auðkennanna **IE2**.

Ef auðkennaveitan er einkaaðili sem hefur ekki staðfestingu á því að hún uppfylli opinberar kröfur eða samning við opinberan aðila nær gæðastig útgefandans ekki upp fyrir IE1.

Útgefandi aðgangsorða sem rafrænna auðkenna getur náð gæðastigi IE3 ef starfsemi hans fellur undir eftirlit hins opinbera.

6.1.4 Fullvissustig fyrir skráningarfasann

Ef við tökum saman gæðastig þáttanna þriggja í skráningarfasanum þá er fullvissustig fyrir skráningarfasa fyrir hefðbundið notandanafn og aðgangsorð **RP2**.

Fullvissustig skráningarfasans fellur í RP1 ef auðkenning er ekki ótvíræð eða ef staðhæfing er ekki staðfest með uppflettingu í opinberum eða öðrum traustum gagnagrunnum (ID1). Sama á við ef engin sannvottun fer fram áður en aðgangsorðið er virkjað (IC1).

Ef útgefandi er einkaaðila og kröfur til hans sem auðkennaveitu liggja ekki fyrir eða hann uppfyllir ekki opinberar kröfur þá fellur fullvissustig skráningarfasans í RP1.

Hefðbundin aðgangsorð geta náð fullvissustigi RP3 ef ítrustu kröfur um verklag, útgáfu og styrk útgefanda eru uppfylltar.

Útgáfa aðgangsorða í gegnum netbanka notandans hækkar ekki fullvissustig skráningarfasans úr RP2.

6.1.5 Tegundir og traustleiki auðkenna

Veikt aðgangsorð er af gæðastigi **RC1** fyrir tegund og traustleika auðkenna[25].

Ef aðgangsorðið telst vera sterkt þá hækkar gæðastigið í RC2.

Hefðbundið aðgangsorð sem rafrænt auðkenni, án annarra ráðstafana[26], getur ekki undir neinum kringumstæðum haft hærra gæðastig en RC2.

6.1.6 Öryggi tilhögunar við sannvottun

Tengingar við rafræna sannvottun með aðgangsorði eru oftast hjúpaðar með dulritun (svokallað HTTPS með SSL/TLS samskiptahætti). Það veitir tiltekna vörn gegn flestum þekktum árásum með hlerun, lotustuldi eða maður-í-milli.

Gæðastig tilhögunar við sannvottun er því í flestum tilfellum **AM3**. Það er þó háð því að dulritunaraðferðir séu öflugar og að þjónustuveitan hafi viðurkennt SSL-skilríki af góðum styrk,

[25] Til að aðgangsorð geti talist sterkt þarf það að hafa upplýsingaóreiðu (e. information entropy) sem samsvarar 60 bita aðgangsorði í tvílotukerfi.
[26] Algengt er að nota annan tóka með aðgangsorði, eins og einskiptis aðgangsorð í RCA-lykli eða yfir SMS samskipti. Þá er mögulegt að ná gæðastigi RC3 fyrir slíkt samsett rafrænt auðkenni.

m.a. hvað varðar lengd dulritunarlykils. Ef slíkar ráðstafanir eru veikar fellur gæðastigið niður í AM2.

Ef samskipti við þjónustuveituna eru ekki dulrituð eða varin á annan áhrifaríkan hátt þá fellur gæðastigið niður í AM1.

6.1.7 Fullvissustig fyrir rafræna sannvottunarfasann

Ef við tökum saman gæðastig þáttanna tveggja í rafræna sannvottunarfasanum þá er fullvissustig hans **EA1**.

Hefðbundið aðgangsorð, þó það teljist sterkt, getur ekki náð hærra fullvissustigi fyrir rafræna sannvottunarfasann en EA2 vegna takmarkana í traustleika þess sem rafræns auðkennis.

Ef samskipti við þjónustuveituna eru ekki dulrituð þegar rafræna sannvottunin fer fram þá getur fullvissustig rafræna sannvottunarfasans ekki verið hærra en EA1.

6.2 VEFLYKILL RÍKISSKATTSTJÓRA

Ríkisskattstjóri gefur út veflykla sem tengjast kennitölum[27]. Með veflyklinum er hægt að skrá sig inn á þjónustuvef ríkisskattstjóra og þaðan er aðgangur að upplýsingum frá nokkrum öðrum stofnunum, meðal annars úr Ökutækjaskrá Umferðastofu og frá Tryggingastofnun.

Veflykill ríkisskattstjóra hefur undanfarin ár verið megin innskráningarleið Ísland.is og margra opinberra stofnana. Eftir að Íslykill Þjóðskrár Íslands kom til sögunnar í apríl 2013 er ekki hægt að nota veflykil ríkisskattstjóra til innskráningar á Ísland.is. Innskráningarþjónusta Ísland.is styður þó enn veflykil ríkisskattstjóra fyrir aðra aðila.

Þegar stofnanir leyfa innskráningu á þjónustuveitur sínar með veflykli ríkisskattstjóra byggt á innskráningarþjónustu Ísland.is sannvottar Ísland.is tengsl veflyklanna við kennitölu og önnur eigindi krefjanda úr þjóðskrá. Innskráningarþjónustan sendir síðan staðhæfingu um auðkenni krefjandans til þjónustuveitunnar sem getur þá ákveðið að heimila krefjandanum aðgang að þjónustu sinni. Við sannvottunina leitar Ísland.is staðfestingar hjá ríkisskattstjóra á þeirri staðhæfingu að veflykillinn tilheyri þeirri kennitölu sem notuð er sem notandanafn við innskráningu.

Þjónustuveita ríkisskattstjóra notar ekki innskráningarþjónustu Ísland.is. Rafræn sannvottun á krefjanda fer fram í innri kerfum ríkisskattstjóra þar sem upplýsingar um kenni notandans eru sóttar í innri skrár.

Fyrir fullan aðgang að gögnum og upplýsingum einstaklinga leyfir ríkisskattstjóri ekki aðra veflykla en svokallaða varanlega aðalveflykla sem áskrifendur velja á vefsetri ríkisskattstjóra, skattur.is, eða sem ríkisskattstjóri hefur sent áskrifendum í netbanka.

Aðalveflykillinn er gefinn út fyrir alla einstaklinga 16 ára og eldri sem eru framteljendur á skattgrunnskrá. Aðalveflykillinn hefur ótakmarkaðan gildistíma og er ekki endurnýjaður.

Við upphaf útgáfu á veflyklum ríkisskattstjóra voru þeir sendir með skattframtölum í pósti á lögheimili einstaklinga. Til að sá veflykill yrði varanlegur þurfti að breyta honum á vefsetri ríkisskattstjóra, eða fá varanlegan veflykil sendan í netbanka einstaklingsins.

Ef veflykill glatast er nýr lykill gefinn út og sendur í netbanka viðkomandi einstaklings eða í pósti á lögheimili hans. Nægir þar að hafa samband við ríkisskattstjóra í síma eða með tölvu-

[27] Sjá vefslóðina www.rsk.is/atvinnurekstur/rafraen-skil/veflyklar-og-rafraen-skilriki/#tab1.

pósti til að biðja um nýjan veflykil. Einnig eru veflyklar afhentir í afgreiðslu ríkisskattstjóra gegn framvísun opinberra persónuskilríkja.

Veflykill ríkisskattstjóra er í raun hefðbundið aðgangsorð sem tengist kennitölu krefjanda sem notað er sem notandanafn við innskráningu.

Varanlegur aðalveflykill ríkisskattstjóra hefur fullvissustig QAA 1.

Veflykill ríkisskattstjóra			
Gæðaþættir	**Gæðastig**	**Fullvissustig fasa**	**Fullvissustig auðkenna**
Verklag við auðkenningu	ID2	RP2	QAA1
Útgáfuferli auðkenna	IC2		
Útgefandi auðkenna	IE2		
Tegund og traustleiki auðkenna	RC1	EA1	
Öryggi í tilhögun við sannvottun	AM3		

Tafla 11: Fullvissustig fyrir veflykil ríkisskattstjóra.

Fullvissustig fyrir skráningarfasann er **RP2** og fullvissustig fyrir rafræna sannvottunarfasann er **EA1**.

Það er veikleiki við veflykla ríkisskattstjóra að handhafar þeirra átta sig sumum tilvikum ekki á því að veflykillinn er hugsaður sem rafrænt persónukenni. Eitthvað er um það að handhafar veflykilsins láni öðrum hann til að sinna erindum sínum í rafrænni þjónustu. Þar með getur ekki verið nein vissa fyrir því hver krefjandinn (notandinn) raunverulega er.

Forsendur matsins eru í köflunum hér á eftir.

6.2.1 Gæði verklags við auðkenningu

Viðveru áskrifandans í eigin persónu er yfirhöfuð ekki krafist á neinum tímapunkti í auðkenningarferlinu (sjá (i.a) í kafla 4.1.1). Staðhæfing um auðkenni áskrifandans við skráningu byggir á kennitölu og nafni sem skilar ótvíræðri auðkenningu, það er að segja að aðeins einn einstaklingur kemur til greina samkvæmt uppgefinni kennitölu (sjá (ii.b)). Staðfesting á staðhæfingum eru gerðar með því að fletta kennitölu upp í þjóðskrá til að staðfesta staðhæfingu um kennitölu og tengt nafn (sjá (iii.b)).

Gæðastig verklags við auðkenningu fyrir veflykil ríkisskattstjóra er þá **ID2**.

Veikasta mögulega fyrirkomulagið, það að panta veflykil í síma eða með tölvupósti og gefa upp nafn og kennitölu, ræður gæðastiginu þar sem ekki er gerður greinarmunur á veflyklunum þegar þeim er beitt við innskráningu eftir því fyrirkomulagi sem var á auðkenningunni. Ef einungis væri mögulegt að sækja veflyklana í afgreiðslu gegn framvísun persónuskilríkja getur gæðastigið farið í ID4.

Þegar veflykill ríkisskattstjóra er afhentur í netbanka er auðkenning notandans byggð á fullvissustigi innskráningar í netbankann sem er QAA 2, þrátt fyrir að Auðkennislykillinn sé notaður[28]. Þetta ræðst af því að Auðkennislykillinn er lokað kerfi sem er ekki með fullgildingu né undir eftirlit hins opinbera (sjá umfjöllun um innskráningu með

[28] Innskráning með notandanafni og aðgangsorði í netbanka Landsbankans gefur einungis fullvissustig QAA 1.

Auðkennislykli í kafla 6.4). Sú aðferð hækkar því ekki gæðastig verklags við auðkenningu fyrir veflykil ríkisskattstjóra úr ID2.

6.2.2 Gæði ferla við útgáfu auðkenna

Varanlegur aðalveflykill ríkisskattstjóra er gefinn út á þrjá mismunandi vegu:

a) Veflykill sendur á lögheimili áskrifandans sem staðfest er með uppflettingu á kennitölu í þjóðskrá og veflykillinn notaður til að velja nýjan varanlegan aðalveflykil á vefsetri ríkisskattstjóra (IC2).

b) Varanlegur aðalveflykill myndaður sjálfkrafa hjá ríkisskattstjóra og sendur í netbanka áskrifandans samkvæmt beiðni hans í síma eða í tölvupósti. Áskrifandi getur breytt veflyklinum á vefsetri ríkisskattstjóra (IC2).

c) Veflykill afhentur í afgreiðslu ríkisskattstjóra gegn framvísun opinberra persónuskilríkja og hann notaður til að velja nýjan varanlegan aðalveflykil á vefsetri ríkisskattstjóra (IC3).

Veikasta ferlið ræður gæðastiginu þar sem ekki er gerður greinarmunur á veflyklum eftir útgáfuferli. Gæðastig útgáfuferlis varanlegs aðalveflykils ríkisskattstjóra er því **IC2**.

Það er vert að hafa í huga að ef veflykill ríkisskattstjóra er afhentur í netbanka notandans þá hækkar það ekki gæðastig útgáfuferils auðkennanna úr IC2, þar sem fullvissustig innskráningar í netbanka er QAA 2 fyrir öðrum aðilum en bönkum og sparisjóðum[29]. Þetta ræðst af því að Auðkennislykillinn er lokað kerfi sem er ekki með fullgildingu né undir eftirlit hins opinbera (sjá umfjöllun um innskráningu með Auðkennislykli í kafla 6.4).

6.2.3 Gæði útgefanda auðkenna

Ríkisskattstjóri er opinber aðili sem gefur út og á veflyklana. Starfsemi ríkisskattstjóra sem útgefandi rafrænna auðkenna er í samræmi við þær kröfur sem varða starfsemi stofnunarinnar sem ríkisskattstjóraembætti. Útgáfan er ekki fullgild á neinn hátt sem auðkennaútgáfa og er ekki háð eftirliti hins opinbera, enda liggja ekki fyrir neinar opinberar kröfur sem lúta að starfsemi ríkisskattstjóra sem auðkennaveitu.

Gæðastig ríkisskattstjóra sem útgefanda veflyklanna sem rafrænna auðkenna er því **IE2**.

6.2.4 Fullvissustig fyrir skráningarfasann

Ef við tökum saman gæðastig þáttanna þriggja í skráningarfasanum þá er fullvissustig skráningarfasa fyrir veflykil ríkisskattstjóra **RP2**.

6.2.5 Tegundir og traustleiki auðkenna

Lágmarkskröfur til lengdar veflykilsins eru 6 bókstafir og/eða tölur. Ekki eru leyfð sértákn né íslenskir bókstafir og ekki er gerður greinarmunur á lág- og hástöfum. Fjöldi mögulegra tákna er því 36. Veflykillinn er því í raun veikt aðgangsorð sem nær ekki hærra óreiðustigi (e. information entropy) en sem samsvarar 31 bita í tvílotukerfi, ef aðgangsorðið er algjörlega handahófskennd.

Veflyklar ríkisskattstjóra eru hins vegar valdir af notendum og gjarnan heil orð eða samsett orð, mynduð úr mjög takmörkuðu stafrófi tákna. Í slíkum tilvikum verður óreiðan mun minni. Samkvæmt einfaldri reiknireglu NIST fyrir aðgangsorð sem eru valin af notandanum (sjá

[29] Innskráning með notandanafni og aðgangsorði í netbanka Landsbankans gefur einungis fullvissustig QAA 1.

viðauka A í NIST 800-63 staðlinum[4]) skilar fyrsta tákn fjögurra bita óreiðu og næstu fimm tákn skila tveimur bitum hvert. Þetta gefur samtals 14 bita óreiðu fyrir veflykil ríkisskattstjóra.

Ef tekið er tillit til þess að reikniregla NIST miðar við enska tungu eingöngu þá má rökstyðja að óreiðan sé eitthvað hærri ef orðaforðinn er úr mörgum tungumálum. Stafrófið leyfir eingöngu enska stafi svo það hækkar ekki óreiðu í fyrsta stafa en getur hækkað óreiðuna í hinum fimm stöfunum umfram viðmið í reiknireglunni. Ef við gerum ráð fyrir að annar til sjötti stafur skili þremur bitum hver þá hækkar óreiðan í 19 bita. Raunveruleg óreiða er því væntanlega á milli 19 og 31 bita.

Varanlegur aðalveflykill ríkisskattstjóra telst því vera af gæðastigi **RC1** fyrir tegund og traustleika rafrænna auðkenna.

Ef kröfur um lengd og óreiðustig veflykilsins væru auknar þannig að hann yrði sterkt aðgangsorð þá gæti veflykillinn náð gæðastigi RC2. Aðgangsorð sem rafrænt auðkenni, og þar með veflykill sem aðgangsorð með kennitölu sem notandanafn, getur ekki undir neinum kringumstæðum haft hærra RC gæðastig.

6.2.6 Öryggi tilhögunar við sannvottun

Hægt er að nota veflykil ríkisskattstjóra til innskráningar beint á vefsetri ríkisskattstjóra skattur.is og í gegnum innskráningarþjónustu Ísland.is. Í báðum þessum tilvikum eru tengingar við rafræna sannvottun hjúpaðar með dulritun (svokallað HTTPS með SSL/TLS samskiptahætti). Það veitir tiltekna vörn gegn flestum þekktum árásum með hlerun, lotustuldi eða maður-í-milli. Notaðar eru öflugar dulritunaraðferðir og viðurkennd skilríki til auðkenningar þeirra kerfa sem tengjast í sannvottunarferlinu.

Gæðastig tilhögunar við sannvottun er því **AM3**.

6.2.7 Fullvissustig fyrir rafræna sannvottunarfasann

Ef við tökum saman gæðastig þáttanna tveggja í rafræna sannvottunarfasanum þá er fullvissustig hans **EA1**.

6.3 ÍSLYKILL ÞJÓÐSKRÁR ÍSLANDS

Þann 12. apríl 2013 hóf Þjóðskrá Íslands útgáfu á nýjum veflykli – Íslykli – sem leysir veflykil ríkisskattstjóra af hólmi í innskráningarþjónustu Ísland.is[30]. Íslykill, eins og veflykill ríkisskattstjóra, er í raun hefðbundið aðgangsorð fyrir innskráningu sem tengt er kennitölu sem notandanafni.

Umtalsverð bót verður með tilkomu nýja Íslykilsins. Gerð er krafa um 10 stafa aðgangsorð sem sé blanda af bókstöfum, tölum og táknum. Íslykill er talinn sterkt aðgangsorð.

Íslykill er í boði fyrir alla einstaklinga óháð aldri. Fyrirhugað er að veita einkafyrirtækjum aðgang að innskráningarþjónustu Ísland.is með tilkomu Íslykilsins. Einnig hefur verið boðað að fljótlega verði hægt að veita öðrum umboð til að sinna sínum málum, en sú útfærsla er ekki útskýrð nánar í þeim gögnum sem tiltæk eru.

Ekki er lengur hægt að skrá sig inn á innskráningarþjónustu Ísland.is með veflykli ríkisskattstjóra. Allir handhafar veflykla ríkisskattstjóra verða því að sækja um Íslykil eða nota rafræn

[30] Sjá www.islykill.is.

skilríki til að komast inn á Ísland.is. Þegar Íslykillinn er síðan notaður í fyrsta sinn til innskráningar þarf að skrá farsímanúmer og netfang.

Hægt er að panta Íslykil á vefsetri Ísland.is eða í afgreiðslu Þjóðskrár Íslands gegn framvísun persónuskilríkja. Virkjunaraðgangsorð (bráðabirgða Íslykill) er afhent í netbanka umsækjandans eða sent í bréfpósti á lögheimili hans. Við fyrstu innskráningu á Ísland.is þarf krefjandinn að velja sér varanlegan Íslykil. Einnig virðist af gögnum frá Þjóðskrá Íslands vera gert ráð fyrir að afhenda aðgangsorðið í afgreiðslu Þjóðskrár Íslands í tengslum við sannvottun með framvísun persónuskilríkja.

Ekki þarf að skrá sig inn á vefsetur Ísland.is til að panta Íslykilinn heldur er nóg að gefa upp kennitölu og þá er virkjunaraðgangsorðið (bráðabirgða Íslykill) sent í netbanka þess sem kennitalan vísar til.

Íslykill Þjóðskrá Íslands hefur fullvissustig QAA 2.

Íslykill Þjóðskrár Íslands			
Gæðaþættir	**Gæðastig**	**Fullvissustig fasa**	**Fullvissustig auðkenna**
Verklag við auðkenningu	ID2	RP2	QAA2
Útgáfuferli auðkenna	IC2		
Útgefandi auðkenna	IE2		
Tegund og traustleiki auðkenna	RC2	EA2	
Öryggi í tilhögun við sannvottun	AM3		

Tafla 12: Fullvissustig fyrir Íslykil Þjóðskrár Íslands.

Fullvissustig fyrir skráningarfasann er **RP2** og fullvissustig fyrir rafræna sannvottunarfasann er **EA2**.

Í kafla 6.2 er bent á veikleika við veflykla ríkisskattstjóra þar sem handhafar átta sig í sumum tilvikum ekki á því að veflykillinn er hugsaður sem rafrænt persónukenni. Þetta er að óbreyttu einnig veikleiki Íslykilsins, meðal annars vegna þess að honum svipar til veflykils ríkisskattstjóra í útfærslu og notkun og mun því væntanlega verða notaður á svipaðan hátt. Ef ekki eru gerðar sérstakar ráðstafanir til að breyta hugarfari fólks þá getur ekki verið nein vissa fyrir því hver krefjandinn (notandinn) raunverulega er. Það þarf því að tryggja að borin sé virðing fyrir því að aðgangsorðið er leyndarmál hvers einstaklings og hefur ekki gildi sem persónulegt rafrænt auðkenni nema það sé virt. Annars getur orðið erfitt að rökstyðja að Íslykillinn hafi hærra fullvissustig en QAA 1.

Þjóðskrá Íslands hefur tilkynnt að fyrirhugað sé að efla Íslykilinn með því að tengja hann við „út-úr-leið“ einskiptis-aðgangsorð yfir farsímakerfið í farsíma krefjandans[31]. Sú styrking eingöngu mun hins vegar ekki hækka fullvissustig Íslykilsins úr QAA 2 þar sem fullvissustig skráningarfasans er einungis RP2. Til að fullvissustig Íslykilsins hækki í QAA 3 er því nauðsynlegt að hækka gæðastig verklags við auðkenningu, gæðastig ferla við útgáfu auðkenna og gæðastig útgefanda Íslykilsins í að minnsta kosti ID3, IC3 og IE3.

Það er hægt að hækka gæði verklags við auðkenningu (ID) og gæði ferla við útgáfu (IC) með því að gera þá kröfu að Íslykill sé annað hvort sóttur í afgreiðslu gegn sannvottun með fram-

[31] Sjá www.islykill.is.

vísun á persónuskilríkjum útgefnum af opinberum aðila eða að hann sé sóttur rafrænt með beitingu rafrænna skilríkja undir Íslandsrót, sem hafa fullvissustig QAA 4. Það þarf líka að hafa í huga að þar sem Aukennislykill fjármálafyrirtækja er lokað kerfi sem byggir ekki á öryggiskröfum sem staðfestar eru af opinberum aðila þá mun fullvissustig skráningarfasans falla í RP2 ef Íslykill er afhentur í netbanka, þrátt fyrir að sótt sé um hann með rafrænum skilríkjum undir Íslandsrót.

Til að gæði Þjóðskrár Íslands sem útgefanda Íslykils nái IE3, sem er eitt af skilyrðum fyrir því að Íslykillinn nái fullvissustigi QAA 3, þá þarf stofnunin að fá opinbera fullgildingu á starfsemi sinni sem útgefandi rafrænna auðkenna eða vera undir eftirliti opinbers aðila.

Forsendur matsins eru í köflunum hér á eftir.

6.3.1 Gæði verklags við auðkenningu

Á sama hátt og fyrir veflykil ríkisskattstjóra þá er viðveru áskrifandans í eigin persónu yfirhöfuð ekki krafist á neinum tímapunkti í auðkenningarferlinu (sjá (i.a) í kafla 4.1.1). Staðhæfing um auðkenni áskrifandans við skráningu byggir á kennitölu og nafni sem skilar ótvíræðri auðkenningu, það er að segja að aðeins einn einstaklingur kemur til greina samkvæmt uppgefinni kennitölu (sjá (ii.b)). Staðfesting á staðhæfingum eru gerðar með því að fletta kennitölu upp í þjóðskrá til að staðfesta staðhæfingu um kennitölu og tengt nafn (sjá (iii.b)).

Gæðastig verklags við auðkenningu fyrir Íslykil Þjóðskrár Íslands er þá **ID2**.

Veikasta mögulega fyrirkomulagið ræður gæðastiginu þar sem ekki er gerður greinarmunur á Íslyklum eftir því fyrirkomulagi sem var á auðkenningunni.

Ef einungis væri mögulegt að sækja Íslykil í afgreiðslu gegn framvísun persónuskilríkja eða með innskráningu með rafrænum skilríkjum undir Íslandsrót, getur gæðastigið farið í ID4.

Hver sem er getur beðið um Íslykil á tiltekna kennitölu, og er bráðabirgða Íslykill þá sendur í netbanka þess sem kennitalan vísar til. Það er því fullvissustig innskráningar í netbanka sem segir til um gæðastig verklags við auðkenningu. Fullvissustig innskráningar í netbanka er QAA 2, þrátt fyrir að Auðkennislykillinn sé notaður. Þetta ræðst af því að Auðkennislykillinn er lokað kerfi sem er ekki með fullgildingu né undir eftirlit hins opinbera (sjá umfjöllun um innskráningu með Auðkennislykli í kafla 6.4). Sú aðferð hækkar því ekki gæðastig verklags við auðkenningu fyrir Íslykilinn úr ID2.

Ef Íslykill er sóttur í netbanka Landsbankans þá er rafræna sannvottunin eingöngu byggð á hefðbundnu notandanafni og veiku aðgangsorði sem veitir einungis fullvissustig QAA 1, sama hvort traustið er innan lokaðs kerfis (traust milli Landsbankans og viðskiptavina þeirra) eða innan almenns opins umhverfis (og þá sérstaklega traust milli Þjóðskrár Íslands og viðskiptavina Landsbankans).

Það er athugunarvert að skráning á tölvupóstfangi og farsímanúmer fer ekki fram fyrr en eftir afhendingu aðgangsorðsins (Íslykilsins) og hefur því ekki áhrif á fullvissustig skráningarfasans. Vissa fyrir því hverjum farsímanúmerið og tölvupóstfangið tilheyrir getur ekki verið meiri en fullvissustig Íslykilsins sem notaður var við innskráningu þegar farsímanúmerið og tölvupóstfangið var gefið upp. Notkun sértækra aðgerða sem byggja á þessum gögnum munu því ekki hækka gæðastig verklags við auðkenningu úr ID2, þó slíkt geti hækkað fullvissustig fyrir rafræna sannvottunarfasann (EA) með því að nota út-úr-leið aðferð.

6.3.2 Gæði ferla við útgáfu auðkenna

Íslykill Þjóðskrár Íslands er afhentur á fjóra mismunandi vegu:

a) Í netbanka áskrifandans eftir að Íslykillinn er pantaður á Ísland.is (IC2).

b) Í bréfpósti á lögheimili áskrifandans eftir að Íslykillinn er pantaður á Ísland.is (IC2).

c) Í afgreiðslu Þjóðskrár Íslands gegn framvísun á persónuskilrikjum (IC3).

d) Á „Mínum síðum“ Ísland.is eftir innskráningu með rafrænum skilríkjum (IC4).

Veikasta ferlið ræður gæðastiginu þar sem ekki er gerður greinarmunur á Íslyklum eftir útgáfuferli. Það má rökstyðja að afhending með almennum bréfpósti nái ekki gæðastigi IC2. Hins vegar sendir Þjóðskrá Íslands Íslykilinn á lögheimili áskrifandans eftir að lögheimilið hefur verið staðfest með uppflettingu í þjóðskrá svo sannvottunin nær því að teljast léttvæg frekar en engin. Gæðastig útgáfuferlis Íslykils Þjóðskrár Íslands er því **IC2**.

Svokallaður styrktur Íslykill mun byggja á SMS samskiptum í viðbót við aðgangsorðið (hefðbundinn Íslykil). Þar sem skráning á farsímanúmer fer ekki fram fyrr en eftir afhendingu aðgangsorðsins (Íslykilsins) þá er gæðastig útgáfuferils styrkta Íslykilsins ekki hærra en gæðastig Íslykilsins sjálfs, það er IC2. Útgáfan byggir þá á vissu fyrir því hverjum farsímanúmerið tilheyrir, en hún getur ekki verið meiri en fullvissustig Íslykilsins sem notaður var við innskráningu þegar farsímanúmerið var gefið upp. Hins vegar getur styrktur Íslykill hækkað fullvissustig fyrir rafræna sannvottunarfasann (EA) þar sem hann byggir á út-úr-leið aðferð.

Það er vert að hafa í huga að ef Íslykillinn er afhentur í netbanka notandans þá hækkar það ekki gæðastig útgáfuferils auðkennanna úr IC2, þar sem fullvissustig innskráningar í netbanka er QAA 2 fyrir öðrum aðilum en bönkum og sparisjóðum[32]. Þetta ræðst af því að Auðkennislykillinn er lokað kerfi sem er ekki með fullgildingu né undir eftirlit hins opinbera (sjá umfjöllun um innskráningu með Auðkennislykli í kafla 6.4), og af lágu fullvissustigi við rafræna sannvottun hjá Landsbankanum með hefðbundnu aðgagnsorði eingöngu.

6.3.3 Gæði útgefanda auðkenna

Þjóðskrá Íslands er opinber aðili sem gefur út og á Íslykil. Starfsemi Þjóðskrár Íslands sem útgefandi rafrænna auðkenna hefur ekki verið fullgild á neinn hátt og er ekki háð eftirliti hins opinbera, enda liggja ekki fyrir neinar opinberar kröfur sem lúta að starfsemi Þjóðskrár Íslands sem auðkennaveitu fyrir Íslykilinn.

Gæðastig Þjóðskrár Íslands sem útgefanda Íslykla sem rafrænna auðkenna er því **IE2**.

6.3.4 Fullvissustig fyrir skráningarfasann

Ef við tökum saman gæðastig þáttanna þriggja í skráningarfasanum þá er fullvissustig skráningarfasa fyrir Íslykil Þjóðskrár Íslands **RP2**.

6.3.5 Tegundir og traustleiki auðkenna

Lágmarkskröfur til lengdar Íslykils eru 10 stafir og getur hann verið blanda af bókstöfum, tölum og táknum úr stafrófi sem inniheldur íslenska stafi. Gerð er krafa um notkun tákna í viðbót við bókstafi og/eða tölur en ekki er gerður greinarmunur á stórum og litlum bókstöfum. Íslykill nær því að hámarki óreiðustigi (e. information entropy) sem samsvarar 77 bitum í

[32] Innskráning með notandanafni og aðgangsorði í netbanka Landsbankans gefur einungis fullvissustig QAA 1.

tvílotukerfi[33], ef samsetning strengsins er algjörlega handahófskennd. Þetta er meira en tvöfallt hærra óreiðustig en núverandi veflykill ríkisskattstjóra nær.

Hins vegar velur notandinn Íslykilinn og notar gjarnan heil orð eða samsett orð ásamt táknum og tölum. Í slíkum tilvikum verður óreiðan mun minni. Samkvæmt reikniregla NIST fyrir aðgangsorð sem eru valin af notandanum (sjá viðauka A í NIST 800-63 staðlinum[4]) skilar fyrsta tákn fjórum bitum og næstu sjö tákn skila tveimur bitum hvert. Síðustu tvö táknin skila 1,5 bita hvort. Þetta gefur samtals 21 bita óreiðu miðað við forsendur NIST. Það myndi teljast frekar veikt aðgangsorð.

Reikniregla NIST miðar við enska tungu. Íslenska stafrófið inniheldur tíu bókstafi umfram bókstafi úr enska stafrófinu. Því má rökstyðja að óreiða í fyrsta tákni sé fimm bitar í stað fjögurra. Aukinn fjöldi orða sem felst í notkun á íslenskum orðum getur hækkað óreiðuna í hinum níu stöfunum umfram reikninregluna. Ef við gerum ráð fyrir að annar til áttundi stafur skili þremur bitum hver og síðustu tveir stafur skili tveimur bitum hver þá hækkar óreiðan í 30 bita.

Íslykill þarf einnig að innihalda tákn, önnur en bókstafi og tölustafi, sem hækkar óreiðuna um allt að 6 bitum samkvæmt rökum í viðauka A í NIST 800-63 staðlinum[4]. Raunveruleg óreiða er því væntanlega á milli 36 og 77 bitar.

Þrátt fyrir þetta verður Íslykill að teljast sterkt aðgangsorð í hefðbundnum skilningi, en þó með þeim fyrirvara sem umfjöllunin hér á undan setur.

Íslykill Þjóðskrár Íslands telst því vera af gæðastigi **RC2** fyrir tegund og traustleika rafrænna auðkenna.

Ef Þjóðskrá Íslands tengir Íslykil við einskiptis aðgangsorð sem útfært er „út-úr-leið“, til dæmis með búnaðartóka eða með staðfestingu frá farsíma krefjandans með SMS skeyti[34], þá getur gæðastigið farið í RC3. Íslykill Þjóðskrár Íslands, þó hann tengist einskiptis aðgangsorði yfir farsímakerfið, getur ekki undir neinum kringumstæðum haft hærra gæðastig en RC3.

6.3.6 Öryggi tilhögunar við sannvottun

Tengingar við rafræna sannvottun með Íslykli eru hjúpaðar með dulritun (svokallað HTTPS með SSL/TLS samskiptahætti) og staðfestingar eru útfærðar með SAML samskiptahætti. Það veitir tiltekna vörn gegn flestum þekktum árásum með hlerun, lotustuldi eða maður-í-milli. Notaðar eru öflugar dulritunaraðferðir og viðurkennd skilríki til auðkenningar þeirra kerfa sem tengjast í sannvottunarferlinu.

Gæðastig tilhögunar við sannvottun er því **AM3**.

Styrktur Íslykill sem byggir á einskiptis aðgangsorði sem sent er með SMS eflir varnir gegn lotustuldi og maður-í-milli árásum en hækkar ekki gæðastig tilhögunar við sannvottun upp fyrir AM3.

6.3.7 Fullvissustig fyrir rafræna sannvottunarfasann

Ef við tökum saman gæðastig þáttanna tveggja í rafræna sannvottunarfasanum þá er fullvissustig hans **EA2**.

[33] Hér er gert ráð fyrir 218 mögulegum táknum í stafrófi.
[34] Á vefsetri Ísland.is kemur fram að fyrirhugað sé að styrkja Íslykilinn með sex stafa tölu sem send er með SMS til notanda á farsímanúmer sem hann gefur upp á vefsetrinu við staðfestingu á Íslyklinum.

Ef Íslykill er tengdur einskiptis aðgangsorði sem útfært er „út-úr-leið“, þá getur gæðastig fyrir tegund og styrkleika rafrænu auðkennanna farið í RC3 og þar með fer fullvissutig fyrir rafræna sannvottun í EA3. Styrktur Íslykill nær því fullvissustigi EA3 fyrir rafræna sannvottunarfasann.

6.4 INNSKRÁNING Í NETBANKA MEÐ AUÐKENNISLYKLI

Fjármálafyrirtæki reka sérstaka sannvottunarþjónustu sem byggir á tóka fyrir einskiptis aðgangsorð, kallað Auðkennislykill[35]. Auðkennislykill banka og sparisjóða er miðlægt öryggiskerfi sem kallar fram tölur sem eru kerfislega tengdar við notandann. Talan sem kölluð er fram er í raun svokallað „einskiptis-aðgangsorð“ (e. one-time-password) þar sem hún er bara notuð einu sinni. Auðkennislykillinn er viðbót við hefðbundið sterkt aðgangsorð í innskráningu og er notaður hjá sumum bönkum og sparisjóðum sem færslusannvottun til að staðfesta auðkenni fyrir aðgerðir í netbanka.

Til að fá aðgang að netbanka þarf notandanafn, sterkt aðgangsorð og einskiptis aðgangsorð sem kallað er fram í tókanum (Auðkennislyklinum) sem er búnaður sem notandinn fær afhentan við skráningu. Rafræna sannvottunin byggir því meðal annars á staðfestingu miðlægs kerfis hjá Auðkenni á tengslum einskiptis aðgangsorðsins við kenni krefjandans.

Hægt er að kalla fram auðkennistöluna yfir SMS í farsíma í stað þess að nota tókabúnað notandans.

Auðkennislykillinn er lokað kerfi þar sem allir innan kerfisins (það er að segja, allir bankar og sparisjóðir) treysta fyrirkomulaginu í samræmi við formlegt samkomulag.

Innskráning í netbanka með Auðkennislykli sem lokað kerfi hefur fullvissustig QAA 3.

Innskráning í netbanka með Auðkennislykli			
Gæðaþættir	**Gæðastig**	**Fullvissustig fasa**	**Fullvissustig auðkenna**
Verklag við auðkenningu	ID4	RP3	QAA3
Útgáfuferli auðkenna	IC4		
Útgefandi auðkenna	IE3		
Tegund og traustleiki auðkenna	RC3	EA3	
Öryggi í tilhögun við sannvottun	AM3		

Tafla 13: Fullvissustig fyrir innskráningu í netbanka með Auðkennislykli.

Fullvissustig fyrir skráningarfasann er **RP3** og fullvissustig fyrir rafræna sannvottunarfasann er **EA3**.

Ef nota á Auðkennislykilinn til innskráningar af öðrum þjónustuaðilum en bönkunum og sparisjóðum þannig að hann sé opið kerfi fyrir almenning þá fellur fullvissustig fyrir skráningarfasann í RP2 (gæði útgefanda fellur í IE2) og heildar fullvissutigið fellur í QAA 2, nema til komi formlegar og opinberar kröfur eða opinbert eftirlit með útgefanda. Þetta snýst um það traust sem ytri aðilar, sem ekki eru þátttakendur í samstarfi um Auðkennislykilinn, geta borið

[35] Sjá nánari upplýsingar á vefsetrinu www.audkenni.is/vorur/aklyklar.cfm.

til útgefandans og þar af leiðandi til fullvissu sannvottunar við innskráningu í netbanka með Auðkennislykli. Þegar skaði af misnotkun rafrænna auðkenna getur verið verulegur þarf traust almennings á útgefanda að byggja á opinberri fullgildingu og/eða eftirliti opinbers aðila.

Forsendur matsins eru í köflunum hér á eftir.

Það er athyglisvert að Landsbankinn hefur einn banka hætt að nota Auðkennislykilinn. Í kafla 6.5 er innskráning í netbanka hjá Landsbankanum því metin sérstaklega.

6.4.1 Gæði verklags við auðkenningu

Í dag eru Auðkennislyklar (tókarnir) einungis afhentir áskrifendum í útibúum bankanna gegn framvísun opinberra persónuskilríkja. Þetta á við hvort sem verið er að afhenda fyrsta lykil eða nýjan lykil í stað annars sem hefur bilað eða tínst.

Öllum fjármálafyrirtækjum ber að framkvæma könnun á áreiðanleika viðskiptamanna sinna sem lið í aðgerðum til verndar gegn peningaþvætti og fjármögnun hryðjuverka (samanber Leiðbeinandi tilmæli Fjármálaeftirlitsins nr. 3/2011) sem felur í sér að viðskiptamenn fjármálafyrirtækja séu viðstaddir í eigin persónu til að sanna á sér deili. Tekið er afrit af persónuskilríkjum, númer þeirra skráð og kenni notandans staðfest með uppflettingu í gögnum frá þjóðskrá. Sannvottun við skráningu er því mjög formföst og ítarleg.

Þegar nýr viðskiptamaður stofnar netbanka er áreiðanleiki hans kannaður þar sem hann er viðstaddur í bankanum. Þá fær hann afhent aðgangsorð og Auðkennislykil. Ef viðskiptamaðurinn þarf nýjan lykil þá þarf hann að mæta í útibú bankans. Ef áreiðanleiki hans hefur verið kannaður áður, þá þarf hann samt að framvísa opinberum persónuskilríkjum sem eru þá borin saman við skírteinagrunn bankans og staðfest af þjónustufulltrúa. Annars er framkvæmd könnun á áreiðanleika viðskiptamannsins.

Viðveru áskrifandans er því krafist bæði þegar hann stofnar netbanka og fær aðgangsorð og Auðkennislykil og þegar hann endurnýjar Auðkennislykilinn (sjá (i.c) í kafla 4.1.1). Staðhæfingar um auðkenni hans eru margar og innihalda sértæk gögn (sjá (ii.c)) og þær eru staðfestar með raunlægum opinberum persónuskilríkjum með mynd (sjá (iii.d)).

Gæðastig verklags við auðkenningu fyrir Auðkennislykilinn er því **ID4**.

6.4.2 Gæði ferla við útgáfu auðkenna

Auðkennislykillinn er einungis afhentur áskrifandanum í eigin persónu. Til að virkja Auðkennislykilinn þarf áskrifandinn að skrá sig inn á netbankann með notandanafni og aðgangsorði og kalla fram eina tölu eða tvær tölur í röð á lyklinum (misjafnt eftir bönkum). Forskráðar upplýsingar um lykilinn, m.a. raðnúmer hans, sem skráð eru af bankanum við afhendingu tryggja þannig að einungis sá lykill sem gefinn er út fyrir áskrifandann getur orðið virkur í netbanka hans.

Þetta samsvarar því að áskrifandinn fari í gegnum sterka sannvottun og fái á sama tíma einka-aðgangsorð sem hann notar til að virkja auðkennagögnin (tókann).

Gæðastig ferla við útgáfu Auðkennislykilsins er því **IC4**.

6.4.3 Gæði útgefanda auðkenna

Þar sem Auðkennislykillinn er útfærður í lokuðu kerfi í þeim skilning að fullt traust ríkir á milli þeirra sem gefa út lykilinn, þeirra sem reka sannvottunarþjónustuna og þeirra sem treysta

á rafrænu auðkennin þá telst útgefandinn hafa fullgildingu gagnvart fjármálafyrirtækjum og viðskiptavinum þeirra.

Gæðastig Auðkennis hf. og bankanna sem útgefanda Auðkennislyklanna sem rafrænna auðkenna í lokuðu kerfi er því **IE3**.

Þess ber að geta að ef nota á Auðkennislykilinn almennt fyrir innskráningu á opnum markaði, til dæmis hjá þjónustuveitu sem ekki er aðili að samkomulaginu á milli Auðkennis og bankanna, þá fellur gæðastig útgefanda í IE2 nema útgefandi hafi fullgildingu með samningi um kröfur við opinberan aðila, eða ef hann er undir eftirliti opinbers aðila.

6.4.4 Fullvissustig fyrir skráningarfasann

Ef við tökum saman gæðastig þáttanna þriggja í skráningarfasanum þá er fullvissustig skráningarfasa fyrir innskráningu í netbanka með Auðkennislyklinum **RP3**.

Fullvissustig fyrir skráningarfasann fellur í RP2 ef nota á Auðkennislykilinn almennt í opnu kerfi, nema útgefandi falli undir opinberar kröfur.

6.4.5 Tegundir og traustleiki auðkenna

Með Auðkennislykli sem búnaðartóka fyrir einskiptis aðgangsorð í viðbót við hefðbundið notandanafn og aðgangsorð er gæðastig þess **RC3** fyrir tegund og traustleika rafrænna auðkenna.

6.4.6 Öryggi tilhögunar við sannvottun

Auðkennislykillinn ásamt aðgangsorði veitir mjög góða vörn gegn árás með ágiskun. Þegar auðkennistölu og aðgangsorði er miðlað yfir tengingar við rafræna sannvottun, og þegar kallað er eftir staðfestingu með tölu úr Auðkennislyklinum, þá eru samskiptin hjúpuð með dulritun (HTTPS). Það veitir tiltekna vörn gegn flestum þekktum árásum með hlerun, lotustuldi eða maður-í-milli. Notaðar eru öflugar dulritunaraðferðir og viðurkennd skilríki til auðkenningar þeirra kerfa sem tengjast í sannvottunarferlinu.

Gæðastig tilhögunar við sannvottun er því **AM3**.

6.4.7 Fullvissustig fyrir rafræna sannvottunarfasann

Ef við tökum saman gæðastig þáttanna tveggja í rafræna sannvottunarfasanum þá er fullvissustig hans fyrir innskráningu í netbanka með Auðkennislykli **EA3**.

6.5 INNSKRÁNING Í NETBANKA HJÁ LANDSBANKANUM

Undir lok ársins 2012 tók Landsbankinn einn banka upp nýtt öryggiskerfi sem útfærir breytilegar kröfur til sannvottunar vegna aðgerða byggt á áhættuflokkun aðgerðanna og greiningu á hegðun notenda í netbankanum. Kerfið notar áhættubyggða sannvottun (e. risk-based authentication), byggir á margþrepa ráðstöfunum eftir áhættu og eðli aðgerða og notar margþætta greiningu á notkun notandans á netbankanum. Á sama tíma tilkynnti Landsbankinn að fyrirtækið myndi ekki nota Auðkennislykilinn fyrir innskráningu í netbankann en að áfram yrði mögulegt að skrá sig inn með rafrænum skilríkjum.

Eftir þessa breytingu geta notendur netbanka Landsbankans skráð sig inn með notandanafni og aðgangsorði eingöngu – án þess að nota Auðkennislykilinn eins og er krafist að lágmarki hjá öðrum bönkum og sparisjóðum. Slík innskráning opnar aðgang að „Síðunum mínum“ í

netbanka viðskiptavina Landsbankans og þar með að öllum þeim upplýsingum sem þar liggja varðandi reikninga viðskiptavinarins, lán, verðbréfaeignir, fjárhagsfærslur á innlánsreikningum og kreditkortum, tengslaupplýsingar og ýmis rafræn skjöl sem hafa verið send til birtingar í netbankanum. Nýja öryggiskerfið bregst hins vegar við þegar viðskiptavinurinn vill framkvæma aðgerðir, eins og millifærslu á fjármunum, sem eru flokkaðar sem hærra áhættustig.

Þessi breyting lækkar fullvissustig sannvottunar við innskráningu verulega frá því sem hún er við innskráningu með Auðkennislykli. Illvilja aðili sem nær að finna út aðgangsorðið og nær þannig að brjótast inn getur komist inn á persónutengjanlegar og viðskiptatengdar upplýsingar í netbankanum. Þessar upplýsingar getur hann síðan notað til að undirbúa alvarlegri árás á netbankann, eða jafnvel aðra þjónustuveitu, byggða á þeim upplýsingum.

Landsbankinn segir að gerð sé krafa um sterkt aðgangsorð. Miðað við þær kröfur sem Landsbankinn setur fram er hins vegar ljóst að aðgangsorðið er á mörkum þess að geta talist sterkt miðað við hefðbundin viðmið (60 bita óreiðu). Fullvissustig við innskráningu er því að mörgu leyti sambærilegt við hefðbundið notandanafn og veikt aðgangsorð – sjá kafla 6.1.

Innskráning í netbanka hjá Landsbankanum hefur fullvissustig QAA 1.

Innskráning í netbanka hjá Landsbankanum			
Gæðaþættir	**Gæðastig**	**Fullvissustig fasa**	**Fullvissustig auðkenna**
Verklag við auðkenningu	ID4	RP2	QAA1
Útgáfuferli auðkenna	IC4		
Útgefandi auðkenna	IE2		
Tegund og traustleiki auðkenna	RC1	EA1	
Öryggi í tilhögun við sannvottun	AM3		

Tafla 14: Fullvissustig fyrir innskráningu í netbanka hjá Landsbankanum.

Fullvissustig fyrir skráningarfasann er **RP2** og fullvissustig fyrir rafræna sannvottunarfasann er **EA1**.

Með því að auka kröfur sínar til styrkleika aðgangsorðsins gæti gæðastig fyrir tegund og traustleika auðkenna hækkað í RC2, og þar með myndi fullvissustigið hækka í QAA 2.

Það er mikilvægt að hafa í huga að færslusannvottun (sjá kafla 5) sem byggir á upplýsingum sem gefnar eru í netbanka eftir innskráningu með rafrænum auðkennum af fullvissustigi QAA 2 hækkar ekki fullvissustigið umfram það. Þetta þýðir að þó Landsbankinn noti út-úr-leið aðferðir eins og SMS-skeyti í farsíma krefjandans til að framkvæma færslusannvottun þegar krefjandinn biður um tiltekna aðgerð þá er fullvissa þess hver einstaklingurinn er ekki meiri en hún var við innskráningu krefjandans þegar farsímanúmerið var skráð í kerfi Landsbankans. Sama á við þegar öryggiskerfið setur fram spurningu sem notandinn verður að svara með fyrirframskráðu svari, þá næst ekki meiri fullvissa en var fyrir hendi þegar notandinn skráði svarið upprunalega í netbankanum.

Annað gildir ef skráningarferlar fyrir farsímanúmer og þau leyndarmál notandans sem notuð eru við færslusannvottun hafa hærra fullvissustig. Slík gögn eru í raun sjálfstæð skírteini og tókar sem afhent eru eftir sannvottun á raunverulegum auðkennum áskrifandans og þannig að

tiltekin fullvissa sé fyrir því að réttur áskrifandi hafi fengið tókann í hendur og geti þar með einn beitt honum síðar sem krefjandi um færsluaðgerð. Ef nægilega strangar kröfur eru uppfylltar við skráningu og útgáfu tókans þá má ná meiri fullvissu við færslusannvottun en var við innskráningu krefjandans inn á netbankann í upphafi tengilotunnar.

Þetta á einnig við um færslusannprófun þar sem heilleiki og uppruni færslugagna er staðfestur samhliða sannvottun á krefjandanum (sjá kafla 5) því fullvissa um auðkenni krefjandans er í raun óháð staðfestingu á færslugögnunum.

Greining á hegðun notenda er annar þáttur sem nýja öryggiskerfi Landsbankans byggir á. Þannig má bregðast við frávikum í notkun netbankans með því að hækka áhættustig og staðfesta auðkenni, og jafnvel færslugögn, áður en lengra er haldið. Slíkar aðferðir geta aukið vissu fyrir því hver einstaklingurinn er, en það fer þó eftir því, eins og fyrr segir, hvernig gengið var frá skráningu á farsímanúmerum og þeim leyndarmálum sem byggt er á í slíkri viðbótar-sannvottun.

Hitt er svo annað mál að öryggiskerfi sem byggja á áhættuflokkun aðgerða og margþættri greiningu á notkun á þjónustuveitu eru mjög mikilvæg viðbót við aðrar aðferðir við sannvottun á einstaklingum yfir fjartengingar. Þau geta aukið verulega varnir gegn maður-í-vafra árásum sem eru sífellt að verða meiri ógn. Slík kerfi minnka hins vegar ekki kröfur til fullvissu í rafrænni sannvottun. Þau geta verið nauðsynleg viðbót við rafræna sannvottun af háu fullvissustigi í þeim tilvikum þar sem mikið er í húfi í færslum og aðgerðum í rafrænni þjónustu, eins og í netbönkum.

Forsendur matsins eru í köflunum hér á eftir.

6.5.1 Gæði verklags við auðkenningu

Gæði verklags við auðkenningu við skráningu er það sama hjá Landsbankanum og hjá öðrum bönkum og sparisjóðum vegna Auðkennislykilsins. Viðveru viðskiptavinar er krafist við stofnun viðskipta og áreiðanleikakönnun gerð í samræmi við kröfur um vernd gegn peningaþvætti og fjármögnun hryðjuverka.

Gæðastig verklags við auðkenningu fyrir aðgangsorð í netbanka Landsbankans er því **ID4**.

6.5.2 Gæði ferla við útgáfu auðkenna

Útgáfa aðgangsorða fer fram við stofnun netbanka í viðurvist viðskiptavinarins.

Gæðastig ferla við útgáfu aðgangsorðs fyrir netbanka Landsbankans er því **IC4**.

6.5.3 Gæði útgefanda auðkenna

Útgáfa aðgangsorðsins er á vegum Landsbankans sem útgáfuaðila. Landsbankinn uppfyllir ekki opinberar kröfur í útgáfunni en byggir útgáfuna á viðurkenndum viðmiðum og takmarkar notkun aðgangsorðsins við sína eigin viðskiptavini. Landsbankinn telst því uppfylla kröfur innan samkomulags við alla hagsmunaaðila. Það er þó ekki hægt að segja að aðgangsorðið sé útgefið í víðtæku lokuðu kerfi undir fullgildingu eða eftirliti ytri aðila, eins og er í tilviki útgáfu á Auðkennislykli þar sem allir hagsmunaaðilar hafa komið sér saman um sameiginlegar kröfur.

Gæðastig Landsbankans sem útgefanda aðgangsorðs sem rafrænna auðkenna er því **IE2**.

6.5.4 Fullvissustig fyrir skráningarfasann

Ef við tökum saman gæðastig þáttanna þriggja í skráningarfasanum þá er fullvissustig skráningarfasa fyrir innskráningu í netbanka hjá Landsbankanum **RP2**.

6.5.5 Tegundir og traustleiki auðkenna

Lágmarkskröfur til lengdar aðgangsorðs fyrir innskráningu í netbanka Landsbankans eru 8 stafir. Aðgangsorðið má ekki innihald önnur tákn en bókstafi og tölustafi og má ekki innhalda íslenska stafi. Ekki er gerður greinarmunur á lágstöfum og hástöfum. Sértækar reglur koma í veg fyrir að aðgangsorðið innihaldi eingöngu bókstafi og að það byrji á tölustaf. Sami stafur má ekki koma fyrir oftar en tvisvar.

Aðgangsorðið nær því að hámarki óreiðustigi (e. information entropy) sem samsvarar 41 bitum í tvílotukerfi[36], ef samsetning strengsins er algjörlega handahófskennd. Samkvæmt bæði viðmiðum NIST[4] (80 bita óreiða) og almennt viðurkenndu viðmiði (60 bita óreiða) telst aðgangsorðið því veikt.

Notandinn velur sjálfur aðgangsorðið fyrir innskráningu í netbanka Landsbankans og notar gjarnan heil orð eða samsett orð ásamt tölum. Í slíkum tilvikum verður óreiðan mun minni. Samkvæmt reiknireglu NIST fyrir aðgangsorð sem eru valin af notandanum (sjá viðauka A í NIST 800-63 staðlinum[4]) skilar fyrsta tákn fjórum bitum og næstu sjö tákn skila tveimur bitum hvert. Þetta gefur samtals 18 bita óreiðu miðað við forsendur NIST. Ef tekið er tillit til þess að reikniregla NIST miðar við enska tungu eingöngu þá má rökstyðja að óreiðan sé eitthvað hærri ef orðaforðinn er úr mörgum tungumálum. Stafrófið leyfir eingöngu enska stafi svo það hækkar ekki óreiðu í fyrsta stafa en getur hækkað óreiðuna í hinum sjö stöfunum umfram viðmið í reiknireglunni. Ef við gerum ráð fyrir að annar til áttundi stafur skili þremur bitum hver þá hækkar óreiðan í 25 bita. Raunveruleg óreiða er því væntanlega á milli 25 og 41 bita.

Kröfur Landsbankans um aðgangsorð fyrir innskráningu í netbanka tryggja því strangt til tekið ekki sterkt aðgangsorð.

Gæðastig fyrir tegund og traustleika aðgangsorðsins sem auðkennis er því **RC1**.

6.5.6 Öryggi tilhögunar við sannvottun

Landsbankinn notar svokallaða EV SSL öryggisviðmið[37] í tengingum notenda við netbankann. Samskipti við rafræna sannvottun eru því hjúpuð með dulritun auk þess sem auðkenning netbankans (rafrænt auðkenningarskilríki þjónustuveitu) uppfyllir sérstakar kröfur frá CA/Browser Forum[38]. Þetta veitir tiltekna vörn gegn flestum þekktum árásum með hlerun, lotustuldi, endursendingu eða maður-í-milli.

Gæðastig tilhögunar við sannvottun er því **AM3**.

6.5.7 Fullvissustig fyrir rafræna sannvottunarfasann

Ef við tökum saman gæðastig þáttanna tveggja í rafræna sannvottunarfasanum þá er fullvissustig hans fyrir innskráningu í netbanka hjá Landsbankanum **EA1**.

[36] Hér er gert ráð fyrir 36 mögulegum táknum í stafrófi (öllum bókstöfum í enska stafrófinu og tölustöfum).
[37] *Extended Validation Secure Socket Layer*.
[38] CA/Browser Forum (*The Certification Authority Browser Forum*) eru samtök vottunaraðila og framleiðenda vefvafra. CA/Browser Forum hefur gefið út leiðbeiningar um útgáfu og umsjón EV SSL skilríkja. Útgefendur sem vilja gefa út EV SSL skilríki þurfa að standast úttekt á hlítingu við kröfurnar í leiðbeiningunum.

6.6 RAFRÆN SKILRÍKI UNDIR ÍSLANDSRÓT

Rafræn skilríki gefin út undir Íslandsrót byggja á dreifilyklaskipulagi (e. public key infrastructure – PKI) sem ríkið hefur sett upp í samvinnu við fjármálarfyrirtækin[39]. Uppruni traustsins er Íslandsrót sem er í eigu ríkisins. Fjármála- efnahagsráðuneytið fyrir hönd ríkisins rekur vottunarstöð Íslandsrótar[40] og tryggir trúverðugleika rótarinnar. Útgáfa Íslandsrótar er samkvæmt Vottunarstefnu Íslandsrótar[11].

Rafrænu skilríkin eru gefin út í örgjörvum snjallkorta, meðal annars á debetkortum allra banka og sparisjóða. Skilríkin innihalda í raun fjögur vottorð þar sem tvö þeirra eru skilríki útgefenda, annað sjálfundirrituð Íslandsrót og hitt útgáfuskilríki Auðkennis „Fullgilt audkenni“ sem undirritað er rafrænt af Íslandsrót[41].

Í örgjörvanum eru einnig tvö endaskilríki. Annað þeirra er ætlað fyrir rafrænar undirskriftir og uppfyllir kröfur laga nr. 28/2001 um rafrænar undirskriftir[9] en hitt endaskilríkið er ætlað fyrir auðkenningar. Þau eru venjulega kölluð „auðkenningarskilríki“ og „undirskriftarskilríki“. Endaskilríkin eru bæði framleidd og afhend á sama hátt og uppfylla þannig sömu kröfur að öllu leyti, nema hvað auðkenningarskilríkið er ekki ætlað til undirskrifta og fellur því ekki undir lög nr. 28/2001 um rafrænar undirskriftir. Endaskilríkin eru gefin út í samræmi við kröfur í Vottunarstefnu Auðkennis[12]. Einkalyklar endaskilríkjanna, sem notaðir eru til að beita skilríkjunum, eru vistaðir í öruggum búnaði í örgjörva snjallkortsins.

Auðkenni sem útgefandi rafrænna skilríkja er undir eftirliti Neytendastofu.

Rafræna sannvottunin byggir á nokkrum þáttum í dreifilyklaskipulaginu, meðal annars staðfestingu á umráðum krefjandans yfir leynilykli (einkalykli) sem byggir á dulritun. Rafrænu skilríkin eru því margþætt; þau eru vottorð, þau eru undirskriftarbúnaður, þau eru dulritunarbúnaður og þau eru örugg hirsla fyrir svokallaðan einkalykil, sem er leynilykill notaður sem dulmálslykill bæði í sannvottun og við rafræna undirskrift.

Rafræn skilríki undir Íslandsrót hafa fullvissustig QAA 4.

Rafræn skilríki undir Íslandsrót			
Gæðaþættir	**Gæðastig**	**Fullvissustig fasa**	**Fullvissustig auðkenna**
Verklag við auðkenningu	ID4	RP4	QAA4
Útgáfuferli auðkenna	IC4		
Útgefandi auðkenna	IE4		
Tegund og traustleiki auðkenna	RC4	EA4	
Öryggi í tilhögun við sannvottun	AM4		

Tafla 15: Fullvissustig fyrir rafræn skilríki undir Íslandsrót.

Fullvissustig fyrir skráningarfasann er **RP4** og fullvissustig fyrir rafræna sannvottunarfasann er **EA4**.

[39] Verkefnið PKI Ísland (PKI-IS) byggði á samstarfssamningi til 6 ára sem undirritaður var 8. mars 2007. Sjá upplýsingar um dreifilyklaskipulagið, rafræn skilríki og notkun þeirra á www.skilriki.is.
[40] Sjá www.islandsrot.is.
[41] Undir Íslandsrót er einungis eitt milliskilríki sem heitir „Fullgilt audkenni“ og er það í eigu Auðkennis ehf. Milliskilríkið „Fullgilt audkenni“ undirritar þau skilríki sem gefin eru út í dag og votta einstaklinga, til dæmis rafræn skilríki á debetkortum banka og sparisjóða. Sjá nánar á www.audkenni.is/rafraenskilriki/.

Forsendur matsins eru í köflunum hér á eftir.

6.6.1 Gæði verklags við auðkenningu

Rafræn skilríki eru einungis afhent á skráningarstöðvum eftir ítarlega sannvottun á áskrifandanum í eigin persónu. Einungis skráningarfulltrúar sem hafa fengið sérstaka þjálfun annast afhendingu rafrænna skilríkja. Skráningarstöðvar eru í flestum útibúum banka og sparisjóða á Íslandi.

Þeir ferlar sem notaðir eru uppfylla kröfur í lögum nr. 28/2001 um rafrænar undirskriftir[9]. Við sannvottun er tekið afrit af opinberum persónuskilríkjum og skráð raðnúmer þeirra og kenni áskrifandans staðfest með uppflettingu í gögnum frá þjóðskrá. Skráningarfulltrúi staðfestir skráningu með aðgerðum og rafrænni undirskrift í sérstöku skráningarstöðvarkerfi.

Þessir ferlar uppfylla einnig kröfur um aðgerðir gegn peningaþvætti og fjármögnun hryðjuverka sbr. Leiðbeinandi tilmæli Fjármálaeftirlitsins nr. 3/2011).

Viðveru áskrifandans er því krafist (sjá (i.c) í kafla 4.1.1). Staðhæfingar um auðkenni hans eru margföld, skila ótvíræðri auðkenningu og innihalda sértæk gögn (sjá (ii.c)) og þær eru staðfestar með raunlægum opinberum persónuskilríkjum með mynd auk þess að vera undirrituð rafrænt af skráningarfulltrúa (sjá (iii.d) og (iii.e)).

Gæðastig verklags við auðkenningu fyrir rafræn skilríki undir Íslandsrót er því **ID4**.

6.6.2 Gæði ferla við útgáfu auðkenna

Rafræn skilríki eru afhent áskrifandanum í eigin persónu og virkjuð eftir staðfestingu á kennum að honum viðstöddum.

Gæðastig ferla við útgáfu rafrænna skilríkja undir Íslandsrót er því **IC4**.

6.6.3 Gæði útgefanda auðkenna

Auðkenni ehf. sem vottunarstöð rafrænna skilríkja er fullgildur útgefandi fullgildra vottorða samkvæmt kröfum í V. kafla í lögum nr. 28/2001 um rafrænar undirskriftir[9] og starfar undir eftirliti Neytendastofu.

Gæðastig Auðkennis hf. sem útgefanda rafrænna skilríkja undir Íslandsrót sem rafrænna auðkenna er því **IE4**.

6.6.4 Fullvissustig fyrir skráningarfasann

Ef við tökum saman gæðastig þáttanna þriggja í skráningarfasanum þá er fullvissustig skráningarfasa fyrir rafræn skilríki undir Íslandrót **RP4**.

6.6.5 Tegundir og traustleiki auðkenna

Rafræn skilríki undir Íslandsrót eru fullgild vottorð sem uppfylla kröfur í 7. gr. laga nr. 28/2001 um rafrænar undirskriftir[9]. Auðkenningarskilríkin, sem eru ekki ætluð til rafrænna undirskrifta, eru hörð skilríki sem uppfylla að öllu leyti sömu kröfur og eru framleidd og gefin út með nákvæmlega sömu framkvæmdakröfum og ferlum og undirskriftarskilríkin.

Gæðastig rafrænna auðkenningarskilríkja undir Íslandsrót er því **RC4,** fyrir tegund og traustleika rafrænna auðkenna.

6.6.6 Öryggi tilhögunar við sannvottun

Við rafræna sannvottun, til að staðfesta að krefjandi hafi umráð og stjórn á skilríkinu, þá sendir þjónustuveitan táknstreng inn í örgjörva snjallkortsins sem er dulritaður þar með einkalyklinum. Notkun einkalykilsins er ræst með því að notandinn slær inn auðkenningar-PIN (4 tölustafir) fyrir skilríkið. Dulritaða strenginn er einungis hægt að dulráða með dreifilykli sem þjónustuveitan þekkir og tengist krefjandanum einum (það er einkvæmt stærðfræðilegt samband á milli einkalykils og samsvarandi dreifilykils). Þannig getur þjónustuveitan, sem krefjandinn biður um aðgang inn á, staðfest að einungis sá sem hefur umráð yfir einkalyklinum getur hafa dulritað táknstrenginn.

Auðkenningar-PIN sem krefjandinn notar til að beita einkalykli sínum fer ekki yfir samskiptatengingar við þjónustuveituna heldur einungis frá lyklaborði til örgjörvans. Auk þess eru öll samskipti yfir Internetið við sannvottun á rafrænum skilríkjum hjúpuð með dulritun (HTTPS).

Búnaðurinn (í örgjörvanum) sem verndar einkalykilinn og inniheldur dulmálsaðgerðir uppfyllir kröfur fyrir matsþrep EAL4+ í „*Common Criteria*“[10], sem eru samþykktar af Evrópuþinginu sem fullnægjandi fyrir öruggan undirskriftarbúnað fyrir fullgildar undirskriftir skv. lögum nr. 28/2001 um rafrænar undirskriftir[9] (þar sem lögin uppfylla kröfur í tilmælum Evrópuþingsins og ráðsins 1999/93/EB um ramma bandalagsins varðandi rafrænar undirskriftir[7]).

Rafræn skilríki undir Íslandsrót veita þannig öfluga vörn gegn öllum tilgreindum árásum í kafla 4.2.2. Þó ber að hafa í huga að maður-í-vafra árás getur komist á milli lyklaborðs og örgjörva nema snjallkortalesarinn sé öruggur búnaður með innbyggðu lyklaborði.

Gæðastig tilhögunar við sannvottun með rafrænum skilríkjum undir Íslandsrót er því **AM4**.

6.6.7 Fullvissustig fyrir rafræna sannvottunarfasann

Ef við tökum saman gæðastig þáttanna tveggja í rafræna sannvottunarfasanum þá er fullvissustig hans fyrir rafræn skilríki undir Íslandsrót **EA4**.

6.7 OCES-SKILRÍKI OG NEMID Í DANMÖRKU

Í Danmörku eru gefin út opinber rafræn skilríki fyrir rafræna þjónustu sem kölluð eru OCES-skilríki (d. Offentlige Certifikater til Elektronisk Service)[42]. Þessi skilríki má nota sem auðkenningarskilríki, undirskriftarskilríki eða dulritunarskilríki. Skilríkin eru gefin út undir vottunarstefnu Upplýsingatækni- og fjarskiptastofnunar Danmerkur (*IT & Telestyrelsen*)[43].

OCES skilríki eru ekki afhent áskrifendum heldur eru þau varðveitt í áreiðanlegu miðlægu kerfi sem rekið er af DanID sem er eitt af dóttufyrirtækjum Nets. Nets er í eigu nokkurra fjármálastofnana í Danmörku og Noregi og varð til við samruna fyrirtækjanna PBS Holding A/S í Danmörku og Nordito AS (móðurfélag fyrirtækisins BBS) í Noregi.

DanID Nets hefur síðan í júlí 2010 gefið út svokölluð NemID auðkenni sem almenna lausn fyrir innskráningu í netbanka, opinbera rafræna þjónustu og þjónustuveitur einkafyrirtækja[44]. Hugsunin á bak við NemID er ekki ósvipuð og á bak við Auðkennislykilinn þar sem notendur fá aðgangsorð ásamt tóka fyrir einskiptis-aðgangsorð til að nota samhliða. NemID tókinn er

[42] Sjá www.nets-danid.dk.
[43] Sjá til dæmis enska þýðingu *Certificate Policy for OCES Personal Certificates („Offentlige Certificater til Elekronisk Service")*, útgáfu 4 frá september 2009[13].
[44] Sjá www.nemid.nu.

pappírsspjald sem inniheldur 146 pör af tölum. Eftir að krefjandinn hefur slegið inn notandanafn (sem getur verið kennitala hans (CPR), útgefið NemID notandanafn eða sjálfvalið notandanafn) og aðgangsorð þá biður þjónustuveitan um 6 tölustafa NemID lykil sem samsvarar 4 stafa númeri sem birt er á vefsíðunni. Sérhvert talnapar er bara notað einu sinni. Þegar búið er að nota öll 146 pörin á spjaldinu fær áskrifandinn sent nýtt pappírsspjald.

Kröfur um aðgangsorð NemID eru svipaðar og fyrir veflykil ríkisskattstjóra. Aðgangsorðið má vera 6 stafir, bæði bókstafir og númer og það er ekki gerður greinarmunur á litlum og stórum bókstöfum. Hins vegar má nota ýmis sértákn þó ekki sé gerð krafa um þau.

NemID tengist OCES-skilríkjum sem gefin eru út af DanID og varðveitt í öruggum búnaði í miðlægu tölvukerfi. Krefjandinn kallar eftir því að skilríkjunum sínum sé beitt með því að nota aðgangsorðið og NemID-lykilinn. DanID tekur þannig yfir sannvottunina og dulritar táknstreng frá þjónustuveitunni með einkalykli krefjandans og sendir jafnframt dreifilykil hans til að þjónustuveitan geti dulráðið móttekinn streng og borið saman við upprunalegan táknstreng. Þetta er samskonar virkni og þegar rafræn skilríki undir Íslandsrót eru notuð í rafrænni sannvottun, en í NemID lausninni er það DanID sem beitir einkalykli krefjandans og staðfestir þannig kennsl hans gagnvart þjónustuveitunni.

NemID er notað á svipaðan hátt til að kalla eftir beitingu undirskriftarskilríkja hjá DanID fyrir hönd krefjanda við rafræna undirskrift.

Áskrifendur geta sótt um NemID yfir Internetið með því að gefa upp númer opinberra persónuskilríkja. Þeir geta einnig sótt um NemID virkjunargögn (NemID-spjald ásamt NemID notandanafni og tímabundnu aðgangsorði) í eigin persónu gegn framvísun persónuskilríkja. Ef persónuskilríkin eru opinber og með mynd geta þeir fengið virkjunargögnin afhent, en annars eru þau send í sitt hvoru lagi með landpósti (aðgangsorðið er ekki sent með NemID-spjaldinu og notandanafninu).

Nýlega hóf DanID að bjóða rafrænan auðkennislykil, svipaðan og Auðkennislykil íslensku bankanna, í stað NemID pappírsspjaldsins. Þar sem ferlar við auðkenningu og útgáfu eru þeir sömu, og aðferðir við rafræna sannvottun eru þær sömu, þá er það okkar mat að rafrænn tóki breyti ekki fullvissustigi NemID með OCES-skilríkjum.

NemID með OCES-skilríkjum hafa fullvissustig QAA 2.

OCES-skilríki og NemID í Danmörku			
Gæðaþættir	**Gæðastig**	**Fullvissustig fasa**	**Fullvissustig auðkenna**
Verklag við auðkenningu	ID2	RP2	QAA2
Útgáfuferli auðkenna	IC2		
Útgefandi auðkenna	IE3		
Tegund og traustleiki auðkenna	RC3	EA3	
Öryggi í tilhögun við sannvottun	AM3		

Tafla 16: Fullvissustig fyrir OCES-skilríki og NemID í Danmörku.

Fullvissustig fyrir skráningarfasann er **RP2** og fullvissustig fyrir rafræna sannvottunarfasann er **EA3**.

Forsendur matsins eru í köflunum hér á eftir.

6.7.1 Gæði verklags við auðkenningu

Til grundvallar er gerð sú krafa að auðkenni áskrifandans sé sannprófað í samræmi við kröfur í lögum um vernd gegn peningaþætti og fjármögnun hryðjuverka í Danmörku. En það er leyfilegt að slaka á kröfu um viðveru áskrifandans ef sannprófun á auðkenni hans fer fram með upplýsingum sem staðfesta auðkennin á jafn áreiðanlegan hátt. Þá er nægjanlegt að áskrifandinn vísi til persónuskilríkja eða annarra gagna sem hann hefur fengið í eigin persónu þar sem viðveru hans var krafist. Áskrifandi getur því sótt um NemID yfir Internetið með því að gefa upp nafn, lögheimili, kennitölu (CPR) og númer á opinberum persónuskilríkjum með mynd (m.a. ökuskírteini, vegabréf, nafnskírteini, Schengen ferðaskírteini og skírteini frá danskri fjármálastofnun), þar sem þau gögn eru síðan staðfest með uppflettingu í opinberum skrám. Í kjölfarið eru NemID-virkjunargögnin (ásamt NemID-spjaldi) sent í tveimur að-greindum póstsendingum á lögheimili áskrifandans.

Viðveru áskrifandans er því ekki krafist (sjá (i.a) í kafla 4.1.1). Staðhæfingar um auðkenni hans eru margföld, skila ótvíræðri auðkenningu og innihalda sértæk gögn (sjá (ii.c)) og þær eru staðfestar með uppflettingu í opinberum skrám (sjá (iii.b)).

Gæðastig verklags við auðkenningu fyrir NemID með OCES-skilríkjum er því **ID2**.

Það er athyglisvert að ef áskrifandi velur að mæta í eigin persónu til að sannvotta auðkenni sitt og fá virkjunargögn fyrir NemID afhent þá er krafist opinberra persónuskilríkja með mynd (sjá (i.c), (ii.c) og (iii.d)). Gæðastig slíkrar auðkenningar er ID4. Hins vegar ef framlögð persónuskilríki eru ekki með mynd þá eru virkjunargögnin ekki afhent heldur send á skráð lögheimili áskrifandans, sem gefur gæðastig ID2 (sjá (i.b), (ii.c) og (iii.b)). Þar sem ekki er gerður greinarmunur á NemID eftir því hvernig auðkenning fór fram þá miðast gæðastigið við veikustu ferla við auðkenningu.

6.7.2 Gæði ferla við útgáfu auðkenna

Algengast er að NemID auðkennin séu send með landpósti á lögheimili áskrifanda i í tveimur aðgreindum sendingum.

Gæðastig ferla við útgáfu NemID með OCES-skilríkjum er því **IC2**.

Það er athyglisvert að afhending og útgáfa á NemID fer fram á mismunandi hátt sem gefur mismunandi gæðastig. Ef áskrifandinn mætir í eigin persónu fyrir sannvottun á auðkennum sínum, leggur fram opinber persónuskilríki með mynd og fær virkjunargögnin afhent í sömu athöfn þá er gæðastigið IC4.

Það er einnig vert að vekja athygli á því að ef gæðastig auðkenningar á áskrifandanum væri ID3 og honum afhent NemID virkjunargögnin (NemID-spjald, tímabundið aðgangsorð og NemID-notandanafn) í eigin persónu þá væri gæðastig útgáfuferla IC3.

6.7.3 Gæði útgefanda auðkenna

DanID Nets er útgefandi NemID og OCES-skilríkja. OCES skilríkin eru gefin út undir vottunarstefnu Upplýsingatækni- og fjarskiptastofnunar Danmerkur (IT & Telestyrelsen). DanID er því útgefandi með fullgildingu og undir eftirliti hins opinbera. DanID er hins vegar ekki útgefandi fullgildra vottorða samkvæmt lögum um rafræn skilríki í Danmörku.

Gæðastig DanID Nets sem útgefanda NemID með OCES-skilríkjum sem rafrænna auðkenna er því **IE3**.

6.7.4 Fullvissustig fyrir skráningarfasann

Ef við tökum saman gæðastig þáttanna þriggja í skráningarfasanum þá er fullvissustig skráningarfasa fyrir rafræn skilríki undir Íslandrót **RP2**.

6.7.5 Tegundir og traustleiki auðkenna

Þar sem NemID með notandanafni, aðgangsorði og NemID-tölu er notað til að kalla eftir því að DanID beiti rafrænu OCES-skilríki krefjandans í rafrænni sannvottun þá ræðst traustleiki auðkennanna algjörlega af traustleika NemID (hefðbundið aðgangsorð með einskiptis-aðgangsorði). Styrkur rafrænu OCES-skilríkjanna bætir þannig ekki það fullvissustig sem NemID-spjaldið sem tóki fyrir einskiptis aðgangsorð í viðbót við hefðbundið notandanafn og aðgangsorð gefa.

Traustleikinn ræðst þannig algjörlega af því að rafræna auðkennið er einskiptis-aðgangsorð í viðbót við hefðbundið notandanafn og aðgangsorð.

Gæðastig NemID með OCES-skilríkjum er því **RC3** fyrir tegund og traustleika rafrænna auðkenna.

6.7.6 Öryggi tilhögunar við sannvottun

NemID talnalykill ásamt aðgangsorði veitir mjög góða vörn gegn árás með ágiskun. Þegar NemID-tölu og aðgangsorði er miðlað yfir tengingar við rafræna sannvottun þá eru samskiptin hjúpuð með dulritun (HTTPS). Ef tryggt er að notaðar séu öflugar dulritunaraðferðir og viðurkennd skilríki til auðkenningar þeirra kerfa sem tengjast í sannvottunarferlinu þá veitir það tiltekna vörn gegn flestum þekktum árásum með hlerun, lotustuldi eða maður-í-milli.

Í NemID er rafrænum OCES-skilríkjum beitt til viðbótar í sannvottuninni gagnvart þjónustuveitunni sem krefjandinn óskar aðgangs að. Gagnvart þjónustuveitunni, sem treystir á rafrænu auðkennin, þá er það DanID sem beitir OCES-skilríki krefjandans til að sannvotta auðkennin. En þar sem DanID treystir á rafræna sannvottun með NemID-spjaldi og aðgangsorði þá takmarkar það gæðastigið sem rafræna sannvottunin hefur.

Gæðastig tilhögunar við sannvottun er því **AM3**.

6.7.7 Fullvissustig fyrir rafræna sannvottunarfasann

Ef við tökum saman gæðastig þáttanna tveggja í rafræna sannvottunarfasanum þá er fullvissustig hans fyrir NemID með OCES-skilríkjum **EA3**.

6.8 BANKID Í NOREGI

BankID í Noregi fyrir einstaklinga byggir á rafrænum skilríkjum sem kallast „PersonBankID“. BankID er gefið út í sameiginlegu skipulagi norskra fjármálafyrirtækja[45]. Rafrænu skilríkin eru varðveitt miðlægt hjá Nets, sama fyrirtæki og stendur á bak við OCES skilríkin og DanID í Danmörku. Rafrænu skilríkin eru gefin út samkvæmt fullgildri vottunarstefnu Staðlaskrifstofu bankanna (Bankens Standardiseringskontor - BSK)[46] og uppfylla kröfur til fullgildra undirskrifta í norskum lögum um rafrænar undirskriftir. Þau má nota bæði til auðkenningar og til undirskrifta.

[45] Sjá www.bankid.no.
[46] Sjá *Norsk BankID sertifikatpolicy for banklagrede kvalifiserte sertifikater til personkunder (PersonBankID)*, útgáfu 1.6 frá september 2012[14].

Hægt er að beita rafrænu skilríkunum í hefðbundinni tölvu með vefvafra og með farsíma. Til að fá aðgang að miðlæga BankID skilríki krefjandans, til að beita því við innskráningu eða undirskrift, þarf að skrá sig inn með fæðingarnúmeri (kennitölu) áskrifandans sem notandanafni, kóta af öryggiskorti sem hann hefur fengið afhent frá bankanum sínum og aðgangsorði sem áskrifandinn velur sjálfur.

Hægt er að fá BankID í farsíma. Þá er leynilykill (einkalykill) geymdur á SIM-korti farsímans. Auðkenning krefjandans byggir á farsímanúmeri, fæðingardegi, leynilykli og PIN-númeri sem hann valdi sjálfur. Til að beita leynilyklinum þarf að slá inn PIN-númerið til að opna SIM-kortið. Leynilykillinn á SIM-kortinu er jafngilt afrit af þeim einkalykli sem tengist PersonBankID skilríkinu og varðveittur er miðlægt hjá Nets.

Öryggiskortin eru einskiptis aðgangsorð en bankarnir eru með mismunandi útfærslu á þeim. Sumir bankar nota prentað kort með kótum svipað og NemID byggir á, aðrir nota rafræna tóka og sumir nota snjallkort með kortalesara.

Kröfur um aðgangsorð BankID eru svipaðar og fyrir veflykil ríkisskattstjóra. Aðgangsorðið má vera 6 stafir, bæði bókstafir og númer og það er ekki gerður greinarmunur á litlum og stórum bókstöfum. Hins vegar má nota ýmis sértákn þó ekki sé gerð krafa um þau.

Í Noregi hafa verið samþykkt að kröfur til fjármálafyrirtækja um vernd gegn peningaþvætti og fjármögnun hryðjuverk þar sem allir viðskiptavinir þurfa að fara í gegnum áreiðanleikakönnun (þar sem þeir eru sannvottaður í eigin persónu) uppfylli kröfur um skráningu vegna fullgildra rafrænna skilríkja. Viðskiptavinirnir fá aðgang að netbanka í tengslum við þá áreiðanleikakönnun. Sú sannvottun sem fæst með innskráningu í netbanka gildir sem fullnægjandi tengsl við þann einstakling sem sannvottaður var við stofnun bankareikningsins. Það eru því einungis nýir viðskiptavinir sem þurfa að mæta í eigin persónu vegna skráningar fyrir BankID. Virkjunargögn fyrir rafrænu skilríkin eru síðan annað hvort send með landpósti í tveimur aðskildum sendingum eða afhent í netbanka viðskiptavinarins, eftir innskráningu með aðferðum sem byggja ekki á BankID.

BankID í Noregi hafa fullvissustig QAA 3.

BankID í Noregi			
Gæðaþættir	**Gæðastig**	**Fullvissustig fasa**	**Fullvissustig auðkenna**
Verklag við auðkenningu	ID3	RP3	QAA3
Útgáfuferli auðkenna	IC3		
Útgefandi auðkenna	IE4		
Tegund og traustleiki auðkenna	RC3	EA3	
Öryggi í tilhögun við sannvottun	AM3		

Tafla 17: Fullvissustig fyrir BankID í Noregi.

Fullvissustig fyrir skráningarfasann er **RP3** og fullvissustig fyrir rafræna sannvottunarfasann er **EA3**.

Fullvissustig fyrir rafræna sannvottunarfasann fyrir BankID á farsímum gæti talist EA4, en það dugir ekki til að hækka heildarfullvissustigið í QAA 4.

Það eru nokkur atriði sem eru athyglisverð í viðleitni Norðmanna til að koma á fullgildum rafrænum skilríkjum með útfærslu á BankID sem á að auðvelda bæði dreifingu skilríkjanna og notkun þeirra.

Í fyrsta lagi hafa þeir náð samkomulagi fjármálastofnana og ríkisins um fyrirkomulag skráningar sem miðar við kröfur um vernd gegn peningaþvætti og fjármögnun hryðjuverka. En þeir gæta ekki að veikum tengslum á milli rafrænu auðkennanna og skráningar áskrifenda (sem hugsanlega fór fram löngu fyrir virkjun rafrænu auðkennanna) þannig að fullvissustig fyrir skráningarfasann fellur í RP3. Auk þess verður ekki séð að kröfur í tilskipun Evrópuþingsins og ráðsins 1999/93/EB um rafrænar undirskriftir[7] sem varða færsluskráningu og varðveislu sannana fyrir skráningu vegna fullgildra rafrænna skilríkja séu að fullu uppfylltar. Þær kröfur eru umfram það sem krafist er í áreiðanleikakönnun vegna verndar gegn peningaþvætti og fjármögnun hryðjuverka. Þar með getur BankID ekki uppfyllt kröfur til fullvissustigs QAA 4, sem rafræn fullgild skilríki sem notuð eru til auðkenningar ættu að uppfylla.

Í öðru lagi eru skilríkin með einkalyklinum varðveitt hjá traustri vottunarstöð (Nets) en ekki afhent áskrifendum (reyndar er afrit af einkalyklinum sett í SIM-kort í BankID fyrir farsíma). Notkun skilríkjanna byggir þannig á sannvottun með aðgangsorði og einskiptis aðgangsorði (kóta), sem getur ekki veitt meiri fullvissu en sem nemur EA3 fyrir rafrænu sannvottunina. Þetta fyrirkomulag, og sambærilegt fyrirkomulag Dana í útfærslu á NemID byggt á OCES-skilríkjum, er gagnrýnt af mörgum sérfræðingum sem fullyrða að slíkt skipulag sem byggir á miðlægri vörslu og virkjun með lægra stigi af auðkenningu geti aldrei talist uppfylla kröfur um fullgild skilríki eða fullgildar undirskriftir.

Þetta á þó ekki við um BankID í farsímum þar sem notkun PersonBankID skilríkjanna byggir á sannvottun með einkalyklinum í SIM-kortinu.

Forsendur matsins eru í köflunum hér á eftir.

6.8.1 Gæði verklags við auðkenningu

Til grundvallar er gerð sú krafa að auðkenni áskrifandans sé sannprófað í samræmi við kröfur í lögum um vernd gegn peningaþætti og fjármögnun hryðjuverka í Noregi. Ef viðskiptavinur hefur á einhverjum tímapunkti farið í gegnum áreiðanleikakönnun samkvæmt þeim kröfum þá þarf hann ekki að mæta í eigin persónu við skráningu og afhendingu BankID auðkennanna.

Viðveru áskrifandans er því ekki krafist í beinum tengslum við afhendingu BankID eða virkjunargagna fyrir auðkennin (sjá (i.b) í kafla 4.1.1). Staðhæfingar um auðkenni hans eru margföld, skila ótvíræðri auðkenningu og innihalda sértæk gögn (sjá (ii.c)) og þær eru staðfestar með uppflettingu í opinberum skrám (sjá (iii.b)). Þrátt fyrir að það sé krafa að áskrifandi hafi sannvottað sig með persónuskilríkjum við áreiðanleikakönnunina þá er staðfestingin við skráningu ekki byggð á persónuskilríkjum heldur er hún háð því fullvissustigi sem er á auðkennum viðskiptavina í innskráningu í netbanka, án BankID. Það er því ekki hægt að flokka staðfestinguna sem (iii.d) í kafla 4.1.1.

Gæðastig verklags við auðkenningu fyrir BankID í Noregi er því **ID3**.

6.8.2 Gæði ferla við útgáfu auðkenna

Kröfur í umgjörð norska ríkisins um rafrænar auðkenningar og óhrekjanleika[47] og þær kröfur sem varða útgáfu PersonBankID í vottunarstefnu BSK leyfa að virkjunargögn séu send með

[47] Sjá *Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon með og i offentlig sektor*[15].

landpósti á lögheimili áskrifanda í tveimur aðgreindum sendingum[48]. Þar sem skilríkin sjálf eru framleidd hjá traustum aðila (Nets) og varðveitt þar ásamt einkalyklinum þá má segja að rafrænu skírteining og tóki séu afhent með miðlungs sannprófun á kennslum áskrifandans, sérstaklega með vísun til þess að verklag við auðkenningu er af gæðastigi ID3.

Gæðastig ferla við útgáfu BankID í Noregi er því **IC3**.

6.8.3 Gæði útgefanda auðkenna

Bankarnir í Noregi gefa út BankID undir rót sem er gefin út af FNH; samtökum fjármálafyrirtækja í Noregi. Útgáfan uppfyllir opinberar kröfur til útgáfu fullgildra skilríkja og útgefendur eru undir eftirliti opinbers aðila.

Gæðastig bankanna sem útgefanda BankID sem rafrænna auðkenna er því **IE4**.

6.8.4 Fullvissustig fyrir skráningarfasann

Ef við tökum saman gæðastig þáttanna þriggja í skráningarfasanum þá er fullvissustig skráningarfasa fyrir BankID í Noregi **RP3**.

6.8.5 Tegundir og traustleiki auðkenna

BankID byggir á fullgildu skilríki sem uppfyllir kröfur í viðauka I í tilskipun Evrópuþingsins og ráðsins 1999/93/EB um rafrænar undirskriftir. En þar sem notandanafn, aðgangsorð og kóti af öryggiskorti er notað til að kalla eftir því að Nets beiti rafrænu PersonBankID-skilríki krefjandans í rafrænni sannvottun þá ræðst traustleiki auðkennanna algjörlega af traustleika aðgangsorðsins og kótans. Styrkur rafrænu PersonBankID-skilríkjanna bætir þannig ekki það fullvissustig sem öryggiskortið sem tóki fyrir einskiptis aðgangsorð til viðbótar við hefðbundið notandanafn og aðgangsorð gefa. Traustleikinn ræðst því algjörlega af því að rafræna auðkennið er í raun einskiptis-aðgangsorð í viðbót við hefðbundið notandanafn og aðgangsorð.

Gæðastig BankID í Noregi er **RC3** fyrir tegund og traustleika rafrænna auðkenna.

Hins vegar er sannvottun með leynilykli BankID í SIM-korti farsíma af gæðastigi RC4.

6.8.6 Öryggi tilhögunar við sannvottun

Kóti öryggiskortsins ásamt aðgangsorði veitir mjög góða vörn gegn árás með ágiskun. Þegar kóta og aðgangsorði er miðlað yfir tengingar við rafræna sannvottun þá eru samskiptin hjúpuð með dulritun (HTTPS). Ef tryggt er að notaðar séu öflugar dulritunaraðferðir og viðurkennd skilríki til auðkenningar þeirra kerfa sem tengjast í sannvottunarferlinu þá veitir það tiltekna vörn gegn flestum þekktum árásum með hlerun, lotustuldi eða maður-í-milli.

Í BankID er rafrænum PersonBankID-skilríkjum beitt til viðbótar í sannvottuninni gagnvart þjónustuveitunni sem krefjandinn óskar aðgangs að. Gagnvart þjónustuveitunni, sem treystir á rafrænu auðkennin, þá er það Nets sem beitir PersonBankID-skilríki krefjandans til að sannvotta auðkennin. En þar sem Nets treystir á rafræna sannvottun með kóta og aðgangsorði þá takmarkar það gæðastigið sem rafræna sannvottunin hefur.

Gæðastig tilhögunar við sannvottun er því **AM3**.

[48] Sjá kafla 6.4.1 í vottunarstefnuskjalinu *Norsk BankID sertifikatpolicy for banklagrede kvalifiserte sertifikater til personkunder (PersonBankID)*[14].

Ef SIM-kortið sem varðveitir leynilykilinn í BankID fyrir farsíma uppfyllir kröfur sem samsvara matsþrepi EAL4+ í „*Common Criteria*“[10], þar sem leynilyklinum er beitt til að sannvotta krefjandann, þá getur gæðastig tilhögunar við sannvottun verið AM4. En það hefur ekki fengist staðfest að SIM-kortið uppfylli slíkar kröfur.

6.8.7 Fullvissustig fyrir rafræna sannvottunarfasann

Ef við tökum saman gæðastig þáttanna tveggja í rafræna sannvottunarfasanum þá er fullvissustig hans fyrir BankID með PersonBankID-skilríkjum **EA3**.

BankID á farsíma gæti verið af fullvissustigi EA4, ef SIM-kortið uppfyllir kröfur um innihald og öryggisstig búnaðar. Það hefur ekki verið staðfest.

7 FLOKKUN STORK VERKEFNISINS Á AUÐKENNUM

Í STORK verkefninu var tekið saman mat á þeim rafrænu auðkennum sem notuð voru til sannvottunar yfir landamæri. Í STORK 2.0[49] hefur þessi listi verið uppfærður og inniheldur nú rafræn auðkenni frá 19 þjóðum. Eftirfarandi tafla sýnir sjálfsmat þeirra á þeim auðkennunum sem hægt er að nota í grunnkerfi STORK til auðkenningar á milli landanna[16].

Í gögnum STORK 2.0 er í sumum tilvikum gefin upp tvö eða fleiri STORK QAA fullvissustig fyrir tiltekin rafræn auðkenni. Ástæðan getur verið sú að um sé að ræða mismunandi útfærslur á auðkennunum, útgáfu þeirra og notkun sem gefa mismunandi fullvissustig, eða að sjálfsmatið hafi ekki staðfest afgerandi hvert fullvissustigið er.

Í þeim tilvikum þar sem sjálfsmat gefur tvö mismunandi STORK QAA fullvissustig ræður það lægra litamerkingunni. Grá merking táknar að fullvissustig hefur ekki verið metið ennþá þó fyrirhugað sé að nota auðkennin í STORK 2.0 verkefninu (sjá auðkenni í Spáni og í Tékklandi).

Land	Rafrænt auðkenni	Skýring	Fullvissustig STORK QAA
Austurríki	Bürgerkarte „e-card”	Snjallkort: Sjúkratryggingakort.	4
Austurríki	Bürgerkarte „ACOS”	Snjallkort: Greiðslukort, stúdentakort, starfsmannakort o.fl.	4
Austurríki	Handy-Signatur	Farsímaauðkenni (*Mobile eID*).	4
Belgía	BELPIC	Snjallkort: Nafnskírteini.	4
Belgía	Kids-ID	Snjallkort. Fyrir börn frá 6 ára aldri.	4
Belgía	Foreign Residence Card	Snjallkort: Fyrir útlendinga búsetta í Belgíu.	4
Bretland	Yorkshire Authentication Project	Mjúk skilríki.	3
Bretland	Yorkshire Authentication Project	Snjallkort.	4
Eistland	ID-kaart	Snjallkort: Nafnskírteini.	4
Eistland	Mobiil-ID	Farsímaauðkenni.	4
Eistland	Digi-ID	Snjallkort.	4
Finnland	FINEID	Snjallkort: Nafnskírteini og ferðaskírteini með fullgildum skilríkjum.	4
Frakkland	ChamberSign	Stafræn skilríki.	3
Grikkland	Y.A.P Digital Signature-Authentication Card	Snjallkort.	4

[49] Sjá www.eid-stork2.eu.

Land	Rafrænt auðkenni	Skýring	Fullvissustig STORK QAA
Grikkland	Y.A.P Soft Certificates for Digital Signature-Authentication	Mjúk skilríki.	3
Grikkland	Ermis – National Government Portal	Notandanafn og aðgangsorð.	1/2
Holland	DigiD PW	Notendanafn og aðgangsorð.	2
Holland	DigiD PW+SMS	Notandanafn, aðgangorð og SMS.	3
Holland	E-Herkenning PW	Notandanafn og aðgangsorð.	1/2
Holland	E-Herkenning SMS	Notandanafn, aðgangsorð og SMS.	3
Holland	E-Herkenning PKI	Rafræn skilríki.	4
Ísland	Debetkort –Fullgilt audkenni	Greiðslukort: Bæði auðkenningar- og undirritunarskilríki.	4
Ísland	Hvítkort – Fullgilt audkenni	Snjallkort: Einka- og starfsmannaskilríki, bæði fyrir auðkenningu og undirskriftir.	4
Ítalía	Carta d'identitá elettronica	Snjallkort: Nafnskírteini.	4
Ítalía	Carta Naxionale dei Servizi	Snjallkort: Nafnskírteini.	4
Litháen	eID	Snjallkort: Nafnskírteini.	4
Lúxemburg	LuxTrust smartcard	Snjallkort.	4
Lúxemburg	LuxTrust signing stick	USB-kubbur.	4
Lúxemburg	Signing Server Certificate	Bæði á farsímum og USB-kubbum.	4
Portúgal	Cartão de Cidadão	Snjallkort: Nafnskírteini.	4
Slóvakía		Nafnskírteini – í undirbúningi.	3
Slóvenía	SIGOV-CA		3 eða 4
Slóvenía	SIGEN-CA		3
Slóvenía	POSTArCA		3 eða 4
Slóvenía	HALCOM-CA		3 eða 4
Slóvenía	AC NLB	Fullgild skilríki.	3
Spánn	DNIe - Documento Nacional de Identidad Electrónico	Snjallkort: Nafnskírteini.	4
Spánn	80 mismunandi mjúk skilríki frá ýmsum aðilum	Mjúk skilríki, í sumum tilvikum sett í öruggan búnað (tóka).	3 eða 4

Land	Rafrænt auðkenni	Skýring	Fullvissustig STORK QAA
Spánn	FNMT-CERES - Fábrica Nacional de Moneda y Timbre		
Spánn	CATCert - Agència Catalana de Certificació		
Spánn	ACCV- Autoritat de Certificació de la Comunitat Valenciana		
Spánn	IZENPE – CA of the Government of the Basque Country		
Spánn	AC Camerfirma		
Spánn	ANF AC - Asociación Nacional de Fabricantes - Autoridad de Certificación		
Spánn	ANCERT - Agencia Notarial de Certificación Firma Profesional		
Spánn	ACA- Autoridad de Certificación de la Abogacía		
Spánn	Banesto		
Spánn	SCR- Servicio de Certificación de los Registradores		
Sviss	SuisseID	Snjallkort og USB-kubbur.	3 eða 4
Svíþjóð	Telia ID-card	Snjallkort.	3
Svíþjóð	Nordea e-legitimation	Snjallkort.	3
Svíþjóð	Handelsbanken BankID	Snjallkort.	3
Svíþjóð	Länsförsäkringar BankID	Mjúk skilríki.	3
Svíþjóð	Sparebanken Nöresund BankID	Mjúk skilríki.	3
Svíþjóð	Swedbank BankID	Mjúk skilríki, hörð skilríki og farsímaskilríki.	3
Svíþjóð	Ikano Bank BankID	Mjúk skilríki.	3
Svíþjóð	Skandia Banken BankID	Mjúk skilríki.	3
Svíþjóð	Danske Bank BankID	Mjúk skilríki.	3
Svíþjóð	Telia SEB	Mjúk og hörð skilríki.	3
Svíþjóð	Telia ICA Banken	Mjúk skilríki.	3

Land	Rafrænt auðkenni	Skýring	Fullvissustig STORK QAA
Svíþjóð	Sparebanken Syd	Mjúk skilríki	3
Tékkland	National eID cards	Snjallkort: Nafnskírteini – í undirbúningi.	
Tékkland	MojeID	Snjallkort: Sérstakt kort fyrir rafræna auðkenningu.	2/3
Tékkland	Commercial USB token or smartcard	Snjallkort og USB-kubbur með bæði auðkenningar- og undirskriftarskilríki.	4
Tyrkland	Turkish Electronic ID Card	Snjallkort: Nafnskírteini.	4
Þýskaland	Neuer Personalausweis	Snjallkort: Nafnskírteini.	4

Tafla 18: Fullvissustig rafrænna auðkenna í STORK 2.0 verkefninu.

Af þeim 19 þjóðum sem taka þátt í STORK 2.0 verkefninu eiga 15 þeirra rafræn auðkenni sem staðfest hefur verið að uppfylla fullvissustig QAA 4. Þetta eru Austurríki, Belgía, Bretland, Eistland, Grikkland, Holland, Ísland, Ítalía, Litháen, Luxemburg, Portúgal, Spánn, Tékkland, Tyrkland og Þýskaland. Slóvenía og Sviss eru einnig með auðkenni sem líklega verða staðfest sem rafræn auðkenni af fullvissustigi QAA 4 (ennþá gefið upp sem QAA „3 eða 4“). Einungis Frakkland og Svíþjóð eru ekki með rafræn auðkenni í STORK verkefninu af hærra fullvissustigi en QAA 3.

8 SAMANTEKT

Í þessari skýrslu er lagt mat á mismunandi útfærslu á rafrænum auðkennum og sannvottun í rafrænni þjónustu. Matið er gert með hliðsjón af STORK QAA matskerfi fyrir fullvissustig rafrænna auðkenna sem er í góðu samræmi við bandarísk viðmið byggð á NIST800-63 staðlinum. Þessi aðferð við mat á fullvissustigi rafrænna auðkenna er grunnur að nýjum alþjóðlegum staðli ISO/IEC 29115 sem er í samþykktarferli. Hún er einnig höfð til hliðsjónar við endurskoðun á regluverki Evrópusambandsins fyrir rafræna auðkenningu, undirskriftir og aðra traustþjónustu. Tillaga að nýrri reglugerð fyrir rafræna auðkenningu og traustþjónustu sem mun taka við af tilskipun Evrópuþingsins og ráðsins 1999/93/EB um rafrænar undirskriftir er í umsagnarferli og verður væntanlega staðfest á næstu mánuðum.

Tafla 19 sýnir niðurstöðu matsins á átta tegundum rafrænna auðkenna. Tvö af þessum auðkennum eru frá Danmörku og Noregi og eru metin í þeim tilgangi að hafa samanburð fyrir helstu tegundir auðkenna sem þekkt eru hér á landi.

Land	Rafrænt auðkenni	Skýring	Fullvissustig STORK QAA
--	Hefðbundið notandanafn og aðgangsorð – opinber aðili	Skráning yfir Internetið staðfest í tölvupósti. Veikt aðgangsorð valið af áskrifandanum.	1
Ísland	Veflykill ríkisskattstjóra	Varanlegur aðalveflykill.	1
Ísland	Íslykill Þjóðskrár Íslands	Veflykill gefinn út af Þjóðskrá Íslands.	2
Ísland	Auðkennislykill banka & sparisjóða	Innskráning í netbanka með Auðkennislykli. Lokað kerfi í eigu banka og sparisjóða.	3
Ísland	Notandanafn og aðgangsorð hjá Landsbankanum	Innskráning í netbanka hjá Landsbankanum án Auðkennislykils.	1
Ísland	Rafræn skilríki undir Íslandsrót	Fullgild skilríki gefin út af Auðkenni með milliskilríkinu Fullgilt audkenni.	4
Danmörk	OCES-skilríki og NemID	Miðlæg OCES-skilríki með NemID auðkenningu.	2
Noregur	BankID	Miðlæg fullgild PersonBankID skilríki með BankID auðkenningu.	3

Tafla 19: Samantekt á mati á fullvissustigi rafrænna auðkenna.

Hefðbundið notandanafn og aðgangsorð gefin út af opinberum aðila þar sem kröfur leyfa veikt aðgangsorð ná ekki hærra fullvissustigi en QAA 1. Það er þó mögulegt að ná fullvissustigi QAA 2 ef gerð er krafa um sterkt aðgangsorð, að öðrum kröfum uppfylltum. En hefðbundið notandanafn og aðgangsorð getur ekki náð hærra fullvissustigi en QAA 2.

Veflykill ríkisskattstjóra nær aðeins fullvissustigi STORK QAA 1. Það veikir jafnframt veflykilinn hversu algengt er að hann sé notaður sem aðgangslykill að þjónustu frekar en sem persónulegt rafrænt auðkenni, eins og við skil á skattframtölum einstaklinga þar sem einn fjölskyldumeðlimur gengur frá skilum fyrir aðra í fjölskyldunni með því að skrá sig inn með veflyklum þeirra. Í raun er mjög lítil vissa fyrir því hver raunverulega er að beita veflyklinum.

Innskráning í netbanka hjá Landsbankanum með notandanafni og aðgangsorði (án Auðkennislykilsins) nær einnig aðeins fullvissustigi STORK QAA 1. Ástæðan er sú að kröfur til aðgangsorða eru of litlar til að þau geti talist vera sterk aðgangsorð. Þar sem innskráningin veitir full réttindi inn á „Síðuna mína“ og þar með að öllum þeim upplýsingum sem þar liggja varðandi reikninga viðskiptavinarins. Innskráningin veitir meðal annars aðgang að aðgangsorðum og veflyklum annarra þjónustuveitna sem send eru í netbanka áskrifendanna og getur þannig minnkað fullvissu rafrænna auðkenna sem ætlunin er að hafi fullvissustig QAA 2 eða hærra.

Íslykill Þjóðskrár Íslands er með fullvissustig QAA 2. Þetta er sama fullvissustig og hefðbundið notandanafn og sterkt aðgangsorð hjá opinberri þjónustuveitu hafa, þar sem skráning er staðfest í tölvupósti og öll samskipti eru yfir dulritaðar tengingar.

Þjóðskrá Íslands hefur tilkynnt að síðar verði boðið upp á „styrktan“ Íslykil með því að tengja hann „út-úr-leið“ einskiptis-aðgangsorði yfir farsímakerfið. Það er hins vegar ljóst að sú styrking mun ekki hækka fullvissustigið úr QAA 2 nema gæðastig verklags við auðkenningu, gæðastig ferla við útgáfu auðkennanna og gæðastig Þjóðskrár Íslands sem útgefanda Íslykilsins verði líka hækkað í stig 3. Það þarf því að gera breytingar á skráningarþjónustu fyrir Íslykilinn miðað við það fyrirkomulag sem tilkynnt hefur verið á vefsíðum Þjóðskrár Íslands og útfæra viðbótarkröfur í verklagi við útgáfu og afhendingu Íslykilsins til að mögulegt sé að hækka fullvissustig hans í QAA 3 með „út-úr-leið“ aðferð. Þjóðskrá Íslands þarf einnig að öðlast opinbera fullgildingu sem útgefandi rafrænna auðkenna.

Innskráning í netbanka með Auðkennislykli fjármálafyrirtækja er af fullvissustigi QAA 3 sem lokað kerfi þar sem byggt er á trausti á milli fyrirtækjanna og viðskiptavina þeirra. Til að halda því fullvissustigi með Auðkennislykilinn sem almennt rafrænt auðkenni, notað af öðrum en þjónustuveitum fjármálafyrirtækja, þá þarf að efla styrk útgefandanna, Auðkennis ehf. og fjármálafyrirtækjanna, með staðfestri hlítingu við opinberar kröfur. Í raun geta ytri aðilar ekki treyst á fullvissu Auðkennislykilsins nema upp á stig QAA 2 þar sem forsendur fyrir almennu trausti á hlítingu við opinberar kröfur eru ekki til staðar. Aðrar auðkennaveitur (þjónustuveitur) sem senda aðgangsorð í netbanka geta því ekki gert ráð fyrir hærra fullvissustigi en QAA 2 við afhendingu aðgangsorðsins sem rafræns auðkennis, sem ræðst af þeirri fullvissu á auðkennum áskrifandans sem staðfest er við innskráningu með Auðkennislyklinum. Ef aðgangsorð er sótt í netbanka Landsbankans nær fullvissustigið ekki hærra en QAA 1.

NemID í Danmörku nær ekki fullvissustigi yfir QAA 2, þrátt fyrir að sannvottunaraðferðir byggi á OCES-skilríkjum sem uppfylla í sjálfu sér meiri kröfur. Ástæðan er sú að kröfur til verklags við auðkenningu áskrifandans og til ferla við útgáfu og afhendingar NemID auðkennanna eru ekki nægilegar til að NemID með OCES-skilríkjum nái QAA 3.

Í raun er svipað upp á tengingnum í Noregi þar sem BankID með PersonBankID skilríkjum nær ekki nema fullvissustigi QAA 3 vegna þess að kröfur til verklags við skráningu (sannvottun á áskrifanda og ferla við útgáfu og afhendingu) eru ekki nægilegar. PersonBankID er fullgilt skilríki og viðurkennt sem slíkt fyrir fullgildar rafrænar undirskriftir samkvæmt norskum lögum. Traustleiki BankID og öryggi tilhögunar við rafræna sannvottun krefjandans ræðst einnig af aðferðum við rafræna sannvottun við innskráningu með aðgangsorði og kóta af öryggiskorti sem nær ekki nema fullvissustigi QAA 3. Það þyrfti því að gera mun sterkari kröfur til bæði skráningar og rafrænnar sannvottunar til að BankID gæti náð fullvissustigi QAA 4.

Rafræn skilríki undir Íslandsrót eru einu rafrænu auðkennin sem metin eru í þessari skýrslu sem ná fullvissustigi STORK QAA 4.

Þær aðferðir sem STORK QAA byggir á og sem viðurkenndar eru bæði í Bandaríkjunum og í Evrópu vísa til þess að ef upplýsingar teljast á einhvern hátt viðkæmar þurfi að lágmarki að krefjast fullvissustigs QAA 2 við rafræna sannvottun til að veita aðgang að þeim. Það er því ljóst að veflykill ríkisskattstjóra er of veikt rafrænt auðkenni til að veita aðgang að viðkvæmum upplýsingum sem einhver trúnaður þarf að vera um. Það er því ekki ásættanlegt að hleypa krefjanda inn á vefsíður með persónutengjanlegum upplýsingum með veflykli ríkisskattstjóra.

Sama á við um hefðbundið notandanafn og aðgangsorð ef ekki er gerð krafa um sterkt aðgangsorð, miðað við aðrar forsendur í þessari skýrslu. Það er því umhugsunarefni þegar fyrirtæki og stofnanir veita aðgang að viðkvæmum upplýsingum, bæði persónutengjanlegum og sem varða viðskipti og þjónustu einstaklinga, með rafrænum auðkennum af fullvissustigi QAA 1.

Ef um persónutengjanlegar upplýsingar er að ræða þar sem mögulegur skaði af uppljóstrun er talinn vera miðlungs mikill ætti að krefjast fullvissustigs QAA 3. Nýr Íslykill Þjóðskrár Íslands sem ætlað er að hækka fullvissustig við innskráningu til að ásættanlegt sé að veita aðgang að persónutengjanlegum upplýsingum nær ekki fullvissustigi QAA 3. Það er því ekki ásættanlegt að nota almenn notendanöfn og aðgangsorð, veflykil ríkisskattstjóra eða nýja Íslykil Þjóðskrár Íslands til innskráningar á þjónustuveitu sem veitir aðgang að persónutengjanlegum upplýsingum, hvort sem það er þjónustuveita opinbers aðila eða einkaaðila.

Það er athyglisvert að NemID í Danmörku er, samkvæmt mati í þessari skýrslu, ekki ásættanlegt auðkenni fyrir innskráningu á þjónustuveitu þar sem veittur er aðgangur að upplýsingum sem eru persónutengjanlegar. NemID er hins vegar notað af opinberum vefsetrum í Danmörku til að veita aðgang að viðkvæmum persónuupplýsingum, meðal annars í heilbrigðisþjónustu.

Til að verja viðkvæmar persónuupplýsingar, eins og upplýsingar um kynþátt, stjórnmálaskoðanir, trúar- eða lífsskoðanir, kynhegðan, heilsuhagi og refsiverðan verknað, ætti ætíð að krefjast fullvissustigs QAA 4, enda er skaði af uppljóstrun slíkra upplýsinga skilgreindur í íslenskum lögum sem mikill. Hér á landi eru það eingöngu rafrænu skilríkin undir Íslandsrót sem hafa fullvissustig QAA 4.

TILVÍSANIR

[1] B. Hulsebosch, G. Lenzini og H. Eertink. *D2.3 – Quality authenticator scheme*. STORK-eID Consortium, 3. mars 2009.

[2] *eID Interoperability for PEGS: Proposal for a multi-level authentication mechanism and a mapping of existing authentication mechanisms*. IDABC, útgáfa 1.1, 5. september 2007.

[3] Russ Cutler ritstjóri. *Liberty Identity Assurance Framework. Liberty Alliance Project*, útgáfa 1.1, 2008.

[4] *Electronic Authentication Guideline: Recommendation of the National Institute of Standards and Technology (NIST Special Publication 800-63-1)*. NIST, desember 2011.

[5] *E-Authentication Guidance for Federal Agencies: Memorandum to the heads of all departments and agencies* (frá Joshua B. Bolten skrifstofustjóra). Skrifstofa reksturs og fjárhags (*Office of Management and Budget - OMB*) hjá Skrifstofu Bandaríkjaforseta (*Executive Office Of The President*), 16. desember 2003.

[6] *D3.2 – QAA Status Report*. Fyrstu drög að stöðuskýrslu STORK 2.0 verkefnisins dagsett 8. febrúar 2013. Sjá www.eid-stork2.eu.

[7] *Tilskipun Evrópuþingsins og ráðsins 1999/93/EB frá 13. desember 1999 um ramma bandalagsins varðandi rafrænar undirskriftir*. Íslensk þýðing 19. janúar 2000. Sjá http://www.utanrikisraduneyti.is/samningar/ees/, leitarorð „399L0093“.

[8] *ETSI TS 101 456 Electronic Signatures and Infrastructure (ESI); Policy requirements for certification authorities issuing qualified certificates*. ETSI, útgáfa 1.4.3, maí 2007.

[9] *Lög nr. 28/2001 um rafrænar undirskriftir* með síðari breytingum, samþykkt 7. maí 2001.

[10] *Common Criteria for Information Technology Security Evaluation - „The Common Criteria“*. Útgáfa 3.1. Sjá http://www.commoncriteriaportal.org/thecc.html.

[11] *Vottunarstefna Íslandsrótar*. Fjármálaráðuneytið, útgáfa 1.0, 19. maí 2008. Kennimark viðfangs {joint-iso-itu-t(2) country(16) is(352) fyrirtæki-samtök-og-stofnanir(1) fjarmalaraduneyti(1) dreifilyklaskipulag-cp(1) íslandsrót(1)}.

[12] *Vottunarstefna Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni*. Auðkenni, útgáfa 1.0, 28. ágúst 2008. Kennimark viðfangs {joint-iso-itu-t(2) country(16) is(352) fyrirtæki-samtök-og-stofnanir(1) audkenni(2) pki(1) public-pki(1) cp(1) cp-version(1)}.

[13] *Certificate Policy for OCES Personal Certificates („Offentlige Certifikater til Elektronik Service)*. Upplýsingatækni- og fjarskiptastofnun Danmörkur (IT & Telestyrelsen), útgáfa 4, september 2009. Kennimark viðfangs {1 2 208 stat(169) pki(1) cp(1) nq(1) person(1) ver(4)}.

[14] *Norsk BankID sertifikatpolicy for banklagrede kvalifiserte sertifikater til personkunder (PersonBankID)*. Bankenes Standardiseringskontor, útgáfa 1.6, september 2012. Kennimark viðfangs {joint-iso-itu-t(2) country(16) norway(578) organisasjon(1) bankenes-standardiseringskontor(16) policy(1) qualifiedCertificates(12) netcentric(1) 1}.

[15] *Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon með og i offentlig sektor*. Úrbóta- og stjórnsýsluráðuneyti Noregs, dagsett í apríl 2008.

[16] *STORK2.0 Member State's eIDs*. Vinnuskjal STORK 2.0 verkefnisins frá ágúst 2012. Sjá www.eid-stork2.eu.