ÍSLANDSRÓT

Vottunarstefna Íslandsrótar

Útgáfa 01-00-00 19. maí 2008

Breytingasaga

Útgáfudagur	Útgáfa	Lýsing	Ábyrgðaraðili
19.05.2008	01-00-00	Fyrsta útgáfa.	Angantýr Einarsson

Efnisyfirlit

Réttindi

Fjármálaráðuneytið fyrir hönd ríkissjóðs á öll réttindi varðandi þessa vottunarstefnu.

Formáli

Þessi vottunarstefna er samin af fjármálaráðuneytinu vegna útgáfu rótarskilríkis (Íslandsrót) og milliskilríkja (undir skipulagi Íslandsrótar). Skjal þetta er samið með hliðsjón af kröfum í skjalinu *Stefnumarkandi kröfur fyrir ISRS skilríki í rafrænni þjónustu* [1], sem samið er af SAM, sem er samstarfshópur fjármálaráðuneytisins og Auðkennis. SAM hópurinn starfar á grundvelli Samstarfssamnings Auðkennis og fjármálaráðuneytisins um innleiðingu dreifilyklaskipulags og almenna notkun rafrænna skilríkja, sem undirritaður var 8. mars 2007.

Upplýsingar um Íslandsrót má fá á www.islandsrot.is og upplýsingar um rafræn skilríki má nálgast á www.skilriki.is.

Yfirlit

Ein helsta forsenda fyrir útbreiðslu rafrænnar þjónustu er að rafræn málsmeðferð njóti sama trausts og hin hefðbundna. Traustið felst í því að öryggi, trúnaður og festa við meðferð mála séu óháð því hvaða aðferð er notuð. Mikilvæg forsenda fyrir því trausti er að aðilar sem stunda rafræn viðskipti séu vottaðir og þær upplýsingar sem miðlað er séu varðveittar.

Í stefnu ríkisstjórnar Íslands um upplýsingasamfélagið „Auðlindir í allra þágu“, 2004-2007, er lögð rík áhersla á þróun rafrænnar stjórnsýslu, rafrænna viðskipta og rafrænna samskipta almennt í samfélaginu. Í stefnunni kemur fram sá vilji ríkisstjórnarinnar að notkun rafrænna skilríkja verði almenn og útbreidd á opnum og stöðluðum markaði fyrir rafræn skilríki.

Með tilkomu laga um rafrænar undirskriftir, nr. 28/2001 [2], laga um rafræn viðskipti og aðra rafræna þjónustu, nr. 30/2002, og laga nr. 51/2003 um breytingu á stjórnsýslulögum, nr. 37/1993 (rafræn stjórnsýsla) [4], var lagður grundvöllur að rafrænni stjórnsýslu og rafrænum viðskiptum samhliða hefðbundnum aðferðum.

Mikilvægur þáttur í útbreiðslu rafrænna skilríkja er að auðvelt og áreiðanlegt sé fyrir notendur að staðfesta heilleika rafrænna auðkenninga og undirskrifta. Tiltrú á heilleika upplýsinga byggir á því að traustur aðili sé tilbúinn til að „votta“ um það. Samkvæmt samstarfsverkefni fjármálaráðuneytisins og Auðkennis sér fjármálaráðuneytið um að stofna og stýra „vottunarrót“ fyrir Ísland. Þessi rót fékk nafnið „Íslandsrót“.

Íslandsrót er skilríki sem er gefið út af fjármálaráðuneytinu, fyrir fjármálaráðuneytið og í eigu þess. Íslandsrót er notuð til að gefa út milliskilríki. Í útgáfunni felst vottun eiganda Íslandsrótar, það er fjármálaráðuneytisins, á handhafa milliskilríkja. Milliskilríki eru síðan notuð til að gefa út önnur milliskilríki eða endaskilríki sem notuð eru í rafrænum samskiptum. Það er mögulegt að búa til traustskeðju með því að gefa út milliskilríki undir milliskilríki en það eru sömu þættir sem skipta máli í hverju þrepi fyrir sig. Það eru því í raun einungis þrjár gerðir skilríkja sem skipta máli í traustkeðju; rót, milliskilríki og endaskilríki. Rót, eins og Íslandsrót, er ekki notuð til að votta skilríki til endanotenda.

Notendur rafrænna skilríkja og allir sem reiða sig á rafræn skilríki verða einnig að treysta vottunarstöðinni sem gefur skilríkin út. Mikilvægur þáttur í að byggja upp traust á vottunarstöðinni er að þessir aðilar geti fullvissað sig um að vottunarstöðin viðhafi fagmannleg vinnubrögð og tryggi öryggi við framleiðslu, afhendingu og dreifingu skilríkja.

Í vottunarstefnunni koma fram þær kröfur og stefnureglur sem viðkomandi vottunarstöð skal uppfylla í starfsemi sinni. Hún á að vera aðgengileg þeim sem hyggjast nýta sér eða reiða sig á rafræn skilríki útgefin af vottunarstöðinni, til þess að þeir aðilar geti lagt mat á traustleika skilríkja. Vottunarstöð Íslandsrótar (hér eftir VÍR) mun stýra starfssemi Íslandsrótar, fyrir hönd fjármálaráðuneytisins og gefur út vottunarstefnu þessa.

1 Gildissvið

Íslandsrót er starfrækt af Vottunarstöð Íslandsrótar fyrir hönd fjármálaráðuneytisins og er uppruni trausts í dreifilyklaskipulagi. Með dreiflyklaskipulagi er átt við það skipulag sem þarf til að framleiða lykla, skilríki og afturköllunarlista ásamt dreifingu, umsjón og safnvista.

Vottunarstefnan tilgreinir þær kröfur sem VÍR þarf að uppfylla vegna útgáfu rafrænna skilríkja. Stefnan tilgreinir lagalegar og tæknilegar kröfur sem VÍR skal uppfylla vegna framleiðslu, útgáfu, notkun, geymslu, afturköllun og endurútgáfu Íslandsrótar og skilríkja sem hún gefur út. Kröfurnar eiga að tryggja öryggi Íslandsrótar og fullvissa notendur og þá sem reiða sig á milliskilríkin að þeir geti treyst þeim. Vottunarstefnan tilgreinir einnig þær kröfur sem gera þarf vegna útgáfu rótarskilríkis þ.e. Íslandsrótar og milliskilríkja undir skipulagi hennar.

Vottunarstefnan er einhliða yfirlýsing VÍR um hvaða stefnureglum er fylgt til að tryggja öryggi kerfisins. Þessi vottunarstefna felur því í sér að:

- Áskrifendur skilríkja geta metið hvernig öryggi kerfisins er tryggt, hvernig nota megi skilríki og hverjar skyldur þeirra eru.
- Þeir sem reiða sig á skilríki geta metið hversu mikið traust má bera til skilríkja og þá undirritun sem framkvæmd er með þeim.

Skipulag Íslandsrótar tekur mið að því að gefin verði út endaskilríki sem geta uppfyllt kröfur um fullgild vottorð í skilningi laga um rafrænar undirskriftir nr. 28/2001 [2].

2 Tilvísanir

Eftirfarandi skjöl innhalda skilyrði og ákvæði sem með tilvísunum í vottunarstefnu þessari mynda stefnureglur hennar.

[1] Stefnumarkandi kröfur fyrir ISRS skilríki í rafrænni þjónustu: Kröfur til vottunarstöðva sem gefa út dreifilyklaskilríki. Útgáfa 1.0 frá 5. maí 2008. Samstarfshópur fjármálaráðuneytisins og Auðkennis.

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

[3] Lög um persónuvernd og meðferð persónuupplýsinga, nr. 77/2000, með síðari breytingum.

[4] Stjórnsýslulög, nr. 37/1993, með síðari breytingum.

[5] *Innihald rafrænna skilríkja: Samræmt innihald rafrænna skilríkja sem gefin eru út á Íslandi*. Útgáfa 1.4 frá 30. nóvember 2006. Sérfræðingar ríkis og banka um samræmt innihald rafrænna skilríkja.

[6] *Lýsing á starfsemi skráningarstöðvar: Skráning á kennimarki viðfangs undir landaboga {joint-iso-itu-t(2) country(16) is(352)} fyrir Ísland. Póst- og fjarskiptastofnun, útgáfa 0.3.1 frá 2. maí 2007.*

[7] FIPS PUB 140-2 (2001): *Security Requirements for Cryptographic Modules*.

[8] ISO/IEC 15408 (hlutar 1 til 3): *Information technology – Security techniques – Evaluation criteria for IT security*.

[9] CEN Workshop Agreement 14167-2:2004: *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 2: Cryptographic Module for CSP Signing Operations with Backup – Protection Profile (CMCSOB-PP).*

[10] CEN Workshop Agreement 14167-3:2004: *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 3: Cryptographic Module for CSP Key Generation Services – Protection Profile (CMCKG-PP).*

[11] CEN Workshop Agreement 14167-4:2004: *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 4: Cryptographic Module for CSP Signing Operations – Protection Profile (CMCSO-PP).*

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

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

[14] ÍST ISO/IEC 17799:2005: *Upplýsingatækni – Öryggistækni: Starfsvenjur fyrir stjórnun upplýsingaöryggis.*

[15] ÍST ISO/IEC 27001:2005: *Upplýsingatækni – Öryggistækni: Stjórnkerfi upplýsinga - Kröfur.*

[16] ISO/IEC 20000: *Information technology: Service management.*

3 Skilgreiningar og skammstafanir

3.1 Skilgreiningar

Í neðangreindum lista eru skilgreiningar sem koma fram í vottunarstefnunni þessari. Samsvarandi orð á ensku eru skáletruð innan sviga.

Afturköllun skilríkja (*certificate revocation*): Óafturkræf aðgerð er felur í sér að skilríki eru gerð ógild áður en gildstími þeirra rennur út. Ekki er hægt að gera afturkölluð skilríki gild aftur.

Afturköllunarlisti skilríkja (*certificate revocation list*): Skrá yfir skilríki sem eru ekki lengur í gildi vegna þess að þau hafa verið afturkölluð (gerð ógild) áður en gildistími þeirra rennur út.

Áskrifandi skilríkja (*certificate subscriber*): Einstaklingur eða lögaðili sem er áskrifandi hjá vottunarstöð fyrir einn eða fleiri vottorðshafa. Áskrifandi getur jafnframt verið vottorðshafi í skilríkjum.

Búnaður (*device* eða *system*): Tæki eða kerfi. Búnaður getur verið hvort sem er vélbúnaður eða hugbúnaður.

Dreifilykill (*public key*): Dulmálslykill sem er ætlaður hvaða einindi (e. entity) sem er, til nota fyrir dulritunarsamskipti við eiganda samsvarandi einkalykils. Við tvílykla dulritun er dreifilykill bæði notaður til dulritunar og til að sannprófa rafræna undirskrift.

Dreifilyklaskilríki (*public key certificate*): Rafrænt vottorð sem tilgreinir dreifilykil vottorðshafa og sem tengir dreifilykilinn við vottorðshafann á ótvíræðan hátt. Sjá einnig „vottorð” og „skilríki”.

Dreifilyklaskipulag (*public key infrastructure*): Það skipulag sem þarf til að framleiða og afhenda lykla og skilríki, viðhalda stöðuupplýsingum um skilríkin, gera afturköllunarlista aðgengilega og safnvista viðeigandi upplýsingar. Dreifilyklaskipulag gerir notendum meðal annars kleift að hafa samskipti yfir almenn netkerfi eins og Internetið á öruggan hátt með því að nota par af dulmálslyklum, einkalykil og dreifilykil. Framleiðsla lyklanna ásamt tengingu þeirra við vottorðshafa er staðfest af aðila sem nýtur trausts.

Dulmálseining (*cryptographic module*): Vélbúnaðareining sem meðal annars framleiðir og varðveitir lykla og notar rafræna undirskrift.

Eigind (*attribute*): Gögn sem tengjast einindi (e. entity) sem tilgreina eiginleika sem tengist einindinu.

Einkalykill (*private key*): Leynilykill sem er ætlaður einum notanda, eiganda lykilsins. Í tvílykla dulritun, eins og í dreifilyklaskipulagi, er einkalykill bæði notaður til dulráðningar og til að búa til rafræna undirskrift.

Einkalykill vottunarstöðvar (*certification authority key*): Einkalykill sem tilheyrir vottunarstöð og sem notaður er til að undirrita skilríkin sem vottunarstöðin gefur út.

Endanotandi (*end user*): Áskrifendur og vottorðshafar kallast endanotendur þar sem skilríki þeirra eru á enda vottunarslóðar og verða því ekki notuð til að sannvotta önnur skilríki.

Endaskilríki (*end-entity certificate*): Skilríki endaaðila eða endaeinindar. Einindið getur verið persónutengt sem einka- eða starfsmannaskilríki. Endaskilríki geta einnig verið skilríki sem eru ekki tengd persónum s.s.. búnaði, tölvukerfi eða skipulagseiningu eins og félagi, sviði eða deild í fyrirtæki.

Fullgild rafræn undirskrift (*qualified electronic signature*): Útfærð (e. advanced) rafræn undirskrift sem er studd fullgildu skilríki og gerð með öruggum undirskriftarbúnaði (e. secure signature-creation device).

Fullgild skilríki (*qualified certificate*): Skilríki sem hafa að geyma upplýsingar sem kveðið er á um í 7. gr. laga um rafrænar undirskriftir, nr. 28/2001 [2] og er gefið út af vottunarstöð (vottunaraðila) sem fullnægir skilyrðum V. kafla laganna.

Hagsmunaaðili (*relying party* eða *verifier*): Notað um þá sem sannprófa skilríki eða treysta á þau. Sjá einnig hugtökin „treystandi“ og „sannprófandi“.

Íslandsrót: Rót sem er efst í stigveldi trausts í dreifilyklaskipulagi á Íslandi. Einkalykill Íslandsrótar er notaður til að undirrita önnur skilríki sem byggja á því trausti.

Kennimark viðfangs (*object identifier - OID*): Auðkenni í svæðinu „certificate policy” í skilríkjum sem tilgreinir tegund skilríkja og vísar til þeirrar vottunarstefnu sem gildir um útgáfu þeirra og notkun.

Lykill (*key*): Í umfjöllun um þætti dreifilyklaskipulags er oftast átt við dulmálslykil (e. cryptographic key). Bitastrengur af breytilegri lengd sem aðgerðir við dulritun eða dulráðningu ráðast af.

Lögaðili (*legal entity*): Stofnun eða félag sem viðurkennt er að geti átt réttindi og borið skyldur. Ríki, sveitarfélög, stofnanir og félög eru lögaðilar og hafa öll sínar kennitölur.

Lögbær fulltrúi (*agent*): Einstaklingur sem valinn er og samþykktur af yfirstjórn fyrirtækis sem tengiliður og sem hefur umboð til að koma fram fyrir hönd fyrirtækisins til að samþykkja og sækja um skilríki, og/eða hafa umsjón með skilríkjum fyrirtækisins.

Milliskilríki (*CA certificate*): Skilríki fyrir vottunarstöð gefin út af annarri vottunarstöð.

Móttakandi skilríkja (*certificate recipient*): Sá sem tekur á móti skilríkjum í rafrænum samskiptum og hefur staðfest það traust sem hann ber til dreifilykils vottorðshafa.

Notkunaraðgangsorð (*enabling password*): Aðgangsorð sem verndar einkalykil vottorðshafa. Þegar notkunaraðgangsorð er notað þarf vottorðshafinn að slá það inn þegar einkalykillinn er notaður. Þegar skilríki eru varðveitt í örgjörva snjallkorta er algengt að persónulegt kenninúmer (PIN) sé notað sem notkunaraðgangsorð.

Persónulegt kenninúmer (*personal identification number*): Stutt númer sem einstaklingur notar sem aðgangsorð að virkum búnaði, til dæmis símakorti, greiðslukorti eða rafrænum skilríkjum á snjallkorti. Persónulegt kenninúmer fyrir rafræn skilríki virkar sem notkunaraðgangsorð sem vottorðshafinn slær inn þegar einkalykillinn er notaður. Stundum kallað „PIN-númer“, „kenninúmer einstaklings“ eða „persónulegt innsláttarnúmer“.

Rafræn skilríki (*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. Í skilríkjum er dreifilykill vottorðshafa ásamt öðrum gögnum, dulritað með einkalykli vottunarstöðvar.

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

Rót (*root*): Upphaf trausts í tilteknu léni dreifilyklaskipulags. Rót er útfærð með skilríki sem kallast rótarskilríki.

Rótarlykill (*root key*): Einkalykill vottunarstöðvar sem er efst í tilteknu stigveldi trausts. Rótarlykillinn er notaður til að undirrita önnur skilríki sem byggja á því trausti.

Rótarskilríki (*root certificate*): Dreifilyklaskilríki sem eru efst í stigveldi trausts og gefin út af vottunarstöð til að undirrita önnur skilríki. Rótarskilríki eru undirrituð með einkalykli þess lyklapars sem tilheyrir sjálfu skilríkinu. Rótarskilríki eru því sjálfundirrituð.

Sjálfundirrituð skilríki (*self-signed certificate*): Skilríki (dreifilykill) sem eru undirrituð með eigin einkalykli. Dreifilykill skilríkjanna er því sjálfundirritaður dreifilykill. Skilríki vottunarstöðvar sem notuð eru til að sannvotta útgefin skilríki eru sjálfundirrituð, sjá einnig skilgreiningu á rótarskilríki.

Sannprófandi (*verifier*): Viðtakandi skilríkja sem sannprófar þau og/eða rafræna undirskrift sem er staðfest með þeim. Stundum kallaður „hagsmunaaðili“.

Sannprófunargögn (*signature verification data*): Gögn, svo sem kótar eða dreifilykill dulritunar, sem notuð eru til að sannreyna rafræna undirskrift.

Skilríki (*certificate*): Í umfjöllun um þætti dreifilyklaskipulags er átt við rafræn skilríki nema annað sé skýrt af samhengi í texta. Stundum er orðið „vottorð” samheiti fyrir „skilríki”.

Skráningarstöð (*registration authority*): Aðili sem er ábyrgur fyrir auðkenningu og sannvottun á vottorðshafa en undirritar ekki skilríki né heldur gefur þau út. Skráningarstöð getur tekið að sér þannig verkefni fyrir hönd vottunarstöðvar.

Stigveldi trausts (*trust hierarchy*): Skipulag rótar og milliskilríkja þar sem traust á tilteknum skilríkjum byggir á trausti til þeirra skilríkja sem notuð voru til að undirrita þau og sem eru ofar í skipaninni (nær rótinni).

Stofnaðgangsorð (*activation code*): Aðgangsorð sem vottunarstöð úthlutar vottorðshafa til að búa til eða stofna skilríkin og mynda lyklapar. Vottorðshafinn þarf ekki að nota stofnaðgangsorðið aftur.

Tímabundin ógilding (*suspension*): Aðgerð sem felur í sér að vottunarstöð skráir skilríki sem ógild í afmarkaðan tíma. Vottunarstöð getur gert skilríkin virk að nýju með því að breyta stöðu þeirra þannig að þau séu ekki lengur ógild.

Treystandi (*relying party*): Viðtakandi skilríkja sem treystir á þau og/eða rafræna undirskrift sem er staðfest með þeim. Stundum kallaður „treystir“, „hagsmunaaðili“, „notandi vottorðs” eða „notandi skilríkja”.

Tvískipt stjórnun (*dual control*): Öryggisverklag sem krefst samvinnu tveggja einstaklinga til að fá aðgang að vernduðum gögnum, skrám, búnaði eða kerfum.

Undirskriftarbúnaður (*signature-creation device*): Hugbúnaður eða vélbúnaður sem notaður er til að mynda rafræna undirskrift með hjálp undirskriftargagna.

Undirskriftargögn (*signature-creation data*): Einstök gögn, svo sem kótar eða einkalykill dulritunar, sem undirritandi notar til að mynda rafræna undirskrift.

Vottorð (*certificate*): Í umfjöllun um þætti dreifilyklaskipulags er orðið „vottorð” oft samheiti fyrir „skilríki”.

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

Vottunarstefna (*certificate policy*): Safn af reglum sem skilgreina nothæfni skilríkja á tilteknu notkunarsviði þar sem öryggiskröfur eru samskonar. Í vottunarstefnu kemur fram hvernig stefnt er að því að standa að útgáfu og meðferð rafrænna skilríkja. Í vottunarstefnu eru líka settar reglur um þær kröfur sem gerðar eru til öryggis og eftirlits.

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

Vottunarþjónusta (*certification service provider*): Aðili sem veitir hagsmunaaðilum alhliða þjónustu varðandi þætti dreifilyklaskipulags.

Yfirlýsing um framkvæmd vottunar (*certification practice statement*): Formleg yfirlýsing vottunarstöðvar um starfsvenjur og framkvæmd við útgáfu og viðhald skilríkja. Yfirlýsing um vottunarframkvæmd lýsir ferlum og reglum skilríkjaútgefanda sem uppfylla kröfur í tiltekinni vottunarstefnu.

Öruggur notendabúnaður (*secure user device*): Búnaður sem geymir einkalykil vottorðshafa, verndar hann gegn ógnum og framkvæmir undirritun eða dulritun fyrir vottorðshafann. Öruggur notendabúnaður sem ætlaður er fyrir rafræna undirritun og sem uppfyllir kröfur sem kveðið er á um í 8. gr. laga um rafrænar undirskriftir, nr. 28/2001 [2] kallast „öruggur undirskriftarbúnaður“.

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]. Öruggur undirskriftarbúnaður er sérstakt tilvik af öruggum notendabúnaði sem ætlaður er fyrir rafrænar undirskriftir.

3.2 Skammstafanir

Eftirfarandi eru algengar skammstafanir í enskum texta um dreifilyklaskipulag. Skýringar á ensku eru skáletraðar í sviga.

CA Vottunarstöð (***C**ertification **A**uthority*).

CSP Vottunarþjónusta (***C**ertification **S**ervice **P**rovider*).

CRL Afturköllunarlisti (***C**ertificate **R**evocation **L**ist*).

ISRS **Ís**lensk **r**afræn **s**kilríki - skilríki í rafrænni þjónustu á Íslandi sem uppfylla samræmdar kröfur í samstarfsverkefni ríkis, banka og sparisjóða.

PIN Persónulegt kenninúmer (***P**ersonal **I**dentification **N**umber*).

4 Almenn hugtök

Meginflokkar rafrænna skilríkja í dreyfilyklaskipulagi eru rótarskilríki, milliskilríki og endaaskilríki. Rótarskilríki eru sjálfundirrituð og gefin út af áskrifandanum sjálfum og er uppruni trausts í opnu dreifilyklaskipulagi. Milliskilríki eru gefin út til vottunarstöðva og staðfesta að vottunarstöðin sé sú sem skilríkin tilgreina og að skilríkin tengist þeim sem lögaðila. Vottunarstöðvar milliskilríkja gefa síðan annað hvort út önnur milliskilríki eða endaaskilríki til almennings og lögaðila.

Þessi vottunarstefna fjallar um kröfur og stefnureglur vegna útgáfu rótarskilríkis og annarra skilríkja gefin út af rótarskilríkinu.

Dreifilyklaskipulag er notað m. a. við miðlun upplýsinga milli tveggja aðila yfir opið samskiptanet, eins og Internetið, þar sem tiltekinn þriðji aðili, sem kallast vottunarstöð, nýtur trausts beggja aðila og ábyrgist sannprófun á auðkenni þeirra. Stefnumarkandi kröfur í skjali þessu lýsa tengslum milli þessara þriggja aðila.

VÍR er vottunarstöð sem myndar rót og gefur út skilríki í samræmi við kröfur stefnu þessarar. Meginmarkmiðið er að unnt sé að nota rafræna undirskrift á öruggan hátt. Traust áskrifenda skilríkja, notenda skilríkja, viðtakenda rafrænt undirritaðra skjala og annarra hagsmunaaðila byggir m.a. á vottunarstefnu þessari.

Í dreifilyklaskipulagi eru rafræn skilríki undirrituð með einkalykli vottunarstöðvar og þau innihalda dreifilykil vottorðshafa ásamt öðrum gögnum. Dreifilyklaskilríkin tengja þannig sannprófunargögn við það viðfang sem vottað er, hvort sem það er einstaklingur, búnaður í eigu lögaðila eða skilgreind deild innan fyrirtækis, stofnunar eða félags.

Í þessari vottunarstefnu er notað íslenska orðið „skilríki“ fyrir það hugtak sem á ensku er kallað „certificate“. Er það til samræmis við orðalag íslenskrar þýðingar á tilskipun Evrópuþingsins og ráðsins

1999/93/EB. Í lögum um rafrænar undirskriftir nr. 28/2001 [2] er íslenska orðið „vottorð“ notað fyrir enska hugtakið „certificate“. Orðin „vottorð“ og „skilríki“ hafa sömu merkingu í þessu skjali og eiga í öllum tilvikum við dreifilyklaskilríki nema annað sé tekið fram. Orðið „vottorðshafi“ er notað um handhafa skilríkja, sem á ensku er kallað „certificate subject“, enda er vísað til þess að handhafi er sá aðili sem er vottaður og auðkenndur sem slíkur í skilríkjum.

4.1 Vottunarstöð

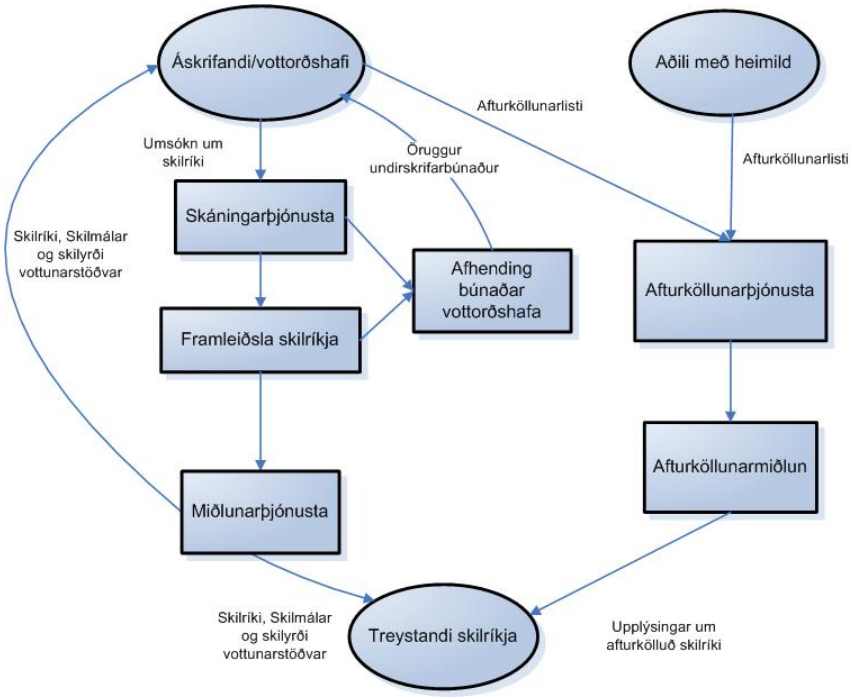
Vottunarstöð er sá aðili sem nýtur trausts notenda vottunarþjónustu, til dæmis áskrifenda skilríkja, vottorðshafa, viðtakenda rafrænt undirritaðra skjala og annarra hagsmunaaðila, til að framleiða og gefa út skilríki. Vottunarstöð er ábyrg fyrir að veita þá þjónustu sem tilgreind er í kafla 4.2. Einkalykill vottunarstöðvar er notaður til að undirrita skilríki og vottunarstöðin er auðkennd í skilríkjunum sem útgefandi. Íslandsrót er sjálfundirritað skilríki gefið út af VÍR. Íslandsrót er efst í stigveldi trausts og undirritar milliskilríki sem eru neðar í stigveldinu. VÍR er því vottunarstöð sem er útgefandi milliskilríkja.

Í lögum um rafrænar undirskriftir nr. 28/2001 [2] er orðið vottunaraðili notað yfir aðila sem gefur út vottorð eða veitir aðra þjónustu í tengslum við rafrænar undirskriftir. Í þessari stefnu nær orðið vottunarstöð yfir vottunaraðila. VÍR er vottunarstöð.

VÍR getur heimilað öðrum aðila að framkvæma hluta af vottunarþjónustunni en ber ábyrgð á öllum þáttum sem varða notkun skilríkja og skal tryggja að þær stefnureglur sem tilgreindar eru í vottunarstefnu þessari séu ávallt uppfylltar.

4.2 Vottunarþjónusta

Starfsemi vottunarstöðvar skiptist í eftirfarandi þætti:



Mynd 1. Skýringarmynd sem sýnir skiptingu vottunarþjónustu í þjónustuþætti.

Skráningarþjónusta: Sannprófar auðkenni og ef við á hvaða sértækar eigindir vottorðshafa sem er. Niðurstöðu þessarar þjónustu er miðlað til þjónustuþáttarins framleiðsla skilríkja.

Framleiðsla skilríkja: Býr til skilríki og undirritar skilríki sem byggjast á auðkenni og öðrum eigindum sem sannprófuð eru af skráningarþjónustunni.

Miðlunarþjónusta: Miðlar skilríkjum til vottorðshafa og birtir skilríkin til þess að hagsmunaaðilar geti haft aðgang að þeim ef vottorðshafi samþykkir. Þessi þjónusta birtir einnig skilmála og skilyrði vottunarstöðvarinnar ásamt þeim reglum og upplýsingum um framkvæmd sem gefnar hafa verið út til áskrifenda og hagsmunaaðila.

Afturköllunarþjónusta: Afgreiðir beiðnir og ábendingar varðandi afturköllun og segir til um hvaða aðgerðir séu nauðsynlegar. Afurð þessarar þjónustu er miðlað til hagsmunaaðila í gegnum afturköllunarmiðlun.

Afturköllunarmiðlun: Veitir upplýsingar um afturköllun skilríkja til hagsmunaaðila. Þessi þjónusta getur verið miðlun í rauntíma eða byggð á afturköllunarupplýsingum sem eru uppfærðar reglulega.

Afhending búnaðar vottorðshafa: Undirbýr undirskriftarbúnað eða annan öruggan notendabúnað og afhendir til vottorðshafa. Þessi þjónusta getur meðal annars falið í sér framleiðslu og afhendingu á lyklapari vottorðshafans, undirbúning á undirskriftareiningunni og stofnaðgangsorði og afhendingu til vottorðshafans.

4.3 Vottunarstefna og yfirlýsing um framkvæmd vottunar

Í þessum kafla er fjallað almennt um hlutverk vottunarstefnu og yfirlýsingar um framkvæmd vottunar.

4.3.1 Tilgangur

Í dreifilyklaskipulagi er tilgangur vottunarstefnu að segja til um hvaða kröfur vottunarstöð skuli uppfylla en tilgangur með yfirlýsingu um framkvæmd vottunar er að segja til um hvernig farið er að því að uppfylla kröfurnar hjá viðkomandi vottunarstöð, það er að segja þeir ferlar sem notaðir eru til að búa til og viðhalda skilríkjum hjá vottunarstöðinni. Í skilríkjunum er tilvísun á vottunarstefnuna, með kennimarki stefnunnar, þannig að móttakandi rafrænna skilríkja geti kynnt sér þær kröfur sem vottunarstöðin skal að lágmarki uppfylla.

Ef gerðar eru breytingar á vottunarstefnu sem hafa áhrif á nothæfi stefnunnar þá ætti að breyta kennimarki stefnunnar í skilríkjunum.

4.3.2 Sérhæfni skjala

Vottunarstefna er ekki eins ítarleg og yfirlýsing um framkvæmd vottunar. Yfirlýsing um framkvæmd vottunar er nákvæmari lýsing á framkvæmd vottunarstöðvar við útgáfu og aðra umsýslu skilríkja. Í yfirlýsingu um framkvæmd vottunar er skilgreint hvernig tiltekin vottunarstöð uppfyllir þær kröfur um tækni, skipulag og verklag sem tilgreindar eru í vottunarstefnu..

Í sumum tilvikum getur verið viðeigandi fyrir vottunarstöð að lýsa ítarlegar í undirskjölum sérstökum ferlum sem nauðsynlegir eru til að fullgera þær framkvæmdir sem tilgreindar eru í yfirlýsingu um framkvæmd vottunar. Venjulega er litið á slík undirskjöl sem innri verklagsreglur sem skilgreina sérstakar aðgerðir og ábyrgðir innan starfseminnar. Þrátt fyrir að slík skjöl séu hluti af daglegri starfsemi vottunarstöðvar og þau rýnd af þar til bærum endurskoðendum þá geta þau fallið utan afmörkunar á vottunarstefnu og yfirlýsingu um framkvæmd vottunar. Dæmi um slík undirskjöl eru ítarlegar lýsingar á ferlum með staðsetningum, aðgangsskrám og aðgangsferlum.

4.3.3 Nálgun

Nálgun vottunarstefnu er umtalsvert ólík nálgun yfirlýsingar um framkvæmd vottunar. Vottunarstefna er óháð sérstökum smáatriðum í rekstrarumhverfi vottunarstöðvar en yfirlýsing um framkvæmd vottunar er sniðin að skipulagi, rekstrarferlum, aðstöðu og tölvuumhverfi vottunarstöðvar. Notenda vottunarþjónustu getur skilgreint vottunarstefnu en yfirlýsing um vottunarframkvæmd er alltaf skilgreind af veitanda vottunarþjónustu.

4.3.4 Aðrar yfirlýsingar vottunarstöðvar

Vottunarstöð getur gefið út skilmála og skilyrði auk vottunarstefnu og yfirlýsingar um framkvæmd vottunar. Slíkir skilmálar og skilyrði eru venjulega almenns eðlis og varða almenna viðskiptahætti vegna útgáfu skilríkja og miðlun upplýsinga.

Birtingarskýrsla dreifilyklaskipulags er sá hluti skilmála og skilyrða vottunarstöðvar sem varða rekstur dreifilyklaskipulagsins og sem eðlilegt er að vottunarstöð birti bæði áskrifendum og treystendum rafrænna skilríkja.

4.4 Áskrifandi og vottorðshafi

Skilríki eru í sumum tilvikum gefin út til einstaklinga til eigin notkunar. Sá aðili sem óskar eftir skilríkjum getur þó verið annar en sá sem skilríkin vísa til. Til dæmis getur fyrirtæki þurft skilríki fyrir starfsmenn sína til að þeir geti haft rafræn samskipti í nafni fyrirtækisins. Í slíkum tilvikum er sá sem er áskrifandi hjá vottunarstöð annar en sá sem er vottorðshafi og tilgreindur í skilríkjum sem slíkur.

Til að aðgreina þær kröfur sem eiga við í hvoru tilviki er gerður greinarmunur í þessu skjali á hlutverki áskrifanda, sem gerir samning við vottunarstöðina um útgáfu skilríkja, og hlutverki vottorðshafa sem skilríkin auðkenna. Áskrifandinn ber ábyrgð gagnvart vottunarstöð á notkun þess einkalykils sem tengdur er dreifilyklaskilríkjum en vottorðshafinn er sá einstaklingur eða búnaður sem notar einkalykilinn og er sannvottaður með þeim skilríkjum sem tengjast honum.

Hugtakið vottorðshafi er notað þar sem sérstaklega er átt við þann sem skilríkin auðkenna en hugtakið áskrifandi er notað í öllum öðrum tilfellum, einnig þar sem mismunurinn er ekki skýr af merkingu texta.

5 Almennt um vottunarkröfur

5.1 Yfirlit

Þær kröfur sem eru skilgreindar í þessu skjali eru þær kröfur sem VÍR mun uppfylla vegna útgáfu á rafrænum skilríkjum í samræmi við það gildissvið sem lýst er í kafla 1. Skilríki sem eru gefin út í samræmi við þetta skjal innihalda auðkenningu á þessari vottunarstefnu og hagsmunaaðilar geta notað hana til að ákvarða hentugleika skilríkjanna og traust til þeirra við tiltekna notkun.

5.2 Auðkenning

Þessi vottunarstefna er auðkennd með kennimarki viðfangs (e. object identifier: OID) sem skráð er hjá Póst- og fjarskiptastofnun undir viðurkenndum og skráðum landaboga fyrir Ísland í samræmi við lýsingu á starfsemi skráningarstöðvar [6] og í samræmi við kröfur í ISO/IEC 9594-8|ITU-T Recommendation X.509 [13]. Þetta kennimark viðfangs er: {2 16 352 1 1 1 1}.

{joint-iso-itu-t(2) country(16) is(352) fyrirtæki-samtök-og-stofnanir(1) fjarmalaraduneyti(1) dreifilyklaskipulag-cp(1) íslandsrót(1)}

Öll skilríki sem gefin eru út í samræmi við þessa vottunarstefnu vísa til hennar með því að tilgreina viðkomandi kennimark viðfangs í svæðinu „Certificate policies“ í skilríkjunum. Með vísun í vottunarstefnuna með kennimarki viðfangs í skilríkjunum lýsir VÍR yfir að skilríkin uppfylli kröfur vottunarstefnunnar. VÍR mun einnig tilgreina kennimörk viðfangs í þeim skilmálum og skilyrðum sem hún birtir hagsmunaaðilum til að koma á framfæri yfirlýsingu um samræmi við kröfur þessa skjals.

5.3 Notkunarsvið og nothæfi

Í samræmi við vottunarstefnu þessa gefur VÍR út skilríki sem uppfylla eftirfarandi kröfur:

a) Skilríkin uppfylla kröfur 7. gr. laga um rafrænar undirskriftir nr. 28/2001 [2].

b) VÍR sem vottunarstöð uppfyllir kröfur V. kafla í lögum um rafrænar undirskriftir nr. 28/2001 [2].

c) Skilríkin eru eingöngu ætluð til notkunar með öruggum undirskriftarbúnaði sem uppfyllir kröfur 8. gr. laga um rafrænar undirskriftir nr. 28/2001 [2].

d) Skilríkin eru gefin út til vottunarstöðva auk skilríkja sem ætluð eru fyrir starfsemi Íslandsrótar.

5.4 Samræmi

5.4.1 Yfirlýsing um samræmi

VÍR lýsir því yfir að við útgáfu, dreifingu, birtingu og afturköllun skilríkja sem gefin eru út í samræmi við vottunarstefnu þessa, eru uppfyllt skilyrði sem taka mið af því að gefin verði út milliskilríki sem munu gefa út endaskilríki sem geta uppfyllt kröfur um fullgild vottorð í skilningi laga um rafrænar undirskriftir nr. 28/2001 [2].

Til þess að færa sönnur á að svo sé mun VÍR láta til þess bæra aðila gera úttekt sem sýnir fram á að útgáfa skilríkja hjá VÍR sé í samræmi við þær kröfur sem koma fram í þessari vottunarstefnu. Niðurstöður slíkrar úttektar munu verða gerðar aðgengilegar áskrifendum og hagsmunaðilum sem reiða sig á skilríkin. Slíka úttekt skal framkvæma reglulega. Sýni slík úttekt að VÍR uppfylli ekki þær kröfur sem vottunarstefna þessi setur mun VÍR þegar í stað hætta útgáfu skilríka, þar til kröfurnar eru uppfylltar.

5.4.2 Kröfur um samræmi

VÍR uppfyllir kröfur í kafla 6.1. og hefur innleitt stýringar sem uppfylla kröfurnar, þar með talið þá valkosti sem eiga við í kafla 7.

6 Skyldur og skuldbindingar

6.1 Skyldur VÍR

VÍR sér til þess að kröfurnar sem tilgreindar eru í kafla 7 séu uppfylltar og að útfærsla vottunarstefnu þessarar sem auðkennd er skilríkjunum sé í samræmi við það (sjá kafla 5.4.2).

VÍR ber ábyrgð á að samræmi sé í þeim starfsreglum sem lýst er í þessari vottunarstefnu jafnvel þó VÍR ákveði að fela undirverktaka hluta starfseminnar.

VÍR gefur út yfirlýsingu um framkvæmd vottunar sem uppfyllir þessa vottunarstefnu . VÍR framkvæmir vottunarþjónustu í samræmi við yfirlýsingu um framkvæmd vottunar.

6.2 Skyldur áskrifenda

VÍR gerir samning við áskrifanda skilríkja (sjá kafla 7.3.1 og 7.3.4) sem skuldbindur áskrifandann til að standa við eftirfarandi kröfur:

a) Að réttar og fullnægjandi upplýsingar séu gefnar til vottunarstöðvar samkvæmt vottunarstefnunni ,sérstaklega tengdar skráningu.

b) Að varðveita og nota eigið lyklapar með þeim takmörkunum sem VÍR tilkynnir áskrifanda (sjá kafla 7.3.4).

c) Að gera eðlilegar og raunhæfar ráðstafanir til að koma í veg fyrir óheimila notkun á einkalykli vottorðshafa, koma í veg fyrir að hann glatist eða að honum sé breytt.

d) Ef áskrifandinn eða vottorðshafinn framleiðir lykla vottorðshafa:

   i. Að lyklar vottorðshafa séu framleiddir með algrími sem er almennt viðurkennt fyrir þá notkun á vottaða lyklinum sem tilgreind er í vottunarstefnu VÍR.

ii. Að lengd lykils og algrím sem notað er séu almennt viðurkennd fyrir þá notkun á vottaða lyklinum á gildistíma skilríkjanna sem tilgreind er í vottunarstefnu VÍR.

iii. Að einkalykill vottorðshafa sé alfarið á forræði vottorðshafa.

e) Að nota einkalykil vottorðshafa einungis til undirskriftar eða dulráðningar í öruggum notendabúnaði.

f) Ef lyklapar vottorðshafa er framleitt af áskrifanda eða vottorðshafa skal framleiða lyklapar vottorðshafans sem ætlað er fyrir undirskrift eða dulráðningu í þeim örugga notendabúnaði sem notaður er fyrir undirskrift eða dulráðningu.

g) Að tilkynna án tafar til vottunarstöðvar ef eitthvert eftirtalinna atvika koma upp á meðan skilríkin eru gild samkvæmt gildistíma sem fram kemur í skilríkjunum:

i. Einkalykill vottorðshafa hefur glatast eða verið stolið.

ii. Vottorðshafi ræður ekki lengur einn yfir einkalykli sínum vegna uppljóstrunar á notkunaraðgangsorði eða af öðrum ástæðum.

iii. Ónákvæmni eða breytingar á innihaldi skilríkja samkvæmt tilkynningum til áskrifanda.

h) Að hætta samstundis og til frambúðar notkun einkalykils vottorðshafa ef lyklinum hefur verið stofnað í hættu.

i) Að koma í veg fyrir að vottorðshafi noti skilríki ef upplýst er að vottunarstöðin sem gaf út skilríkin hafi orðið fyrir öryggisbresti.

6.3 Upplýsingar fyrir hagsmunaaðila

Til þess að hagsmunaðili geti á eðlilega hátt reitt sig á tiltekin skilríki munu skilmálar og skilyrði sem VÍR birtir hagsmunaaðilum (sjá kafla 7.3.4) innihalda viðvörun um að hann skuli;

a) staðfesta gildi, tímabundna ógildingu eða afturköllun á mótteknum skilríkjunum með nýjustu upplýsingum um afturköllunarstöðu eins og þær eru birtar hagsmunaaðilum (sjá kafla 7.3.4) og

b) taka tillit til allra takmarkana á notkun skilríkja eins og þær eru birtar hagsmunaaðilum annað hvort í skilríkjunum eða í skilmálum og skilyrðum sem látin eru í té samkvæmt kröfum í kafla 7.3.4 og

c) gera aðrar þær ráðstafanir sem lýst er í samningum eða annarsstaðar.

6.4 Skuldbindingar

Ábyrgð gagnvart áskrifendum og hagsmunaaðilum

VÍR er bótaskylt vegna tjóns hjá þeim sem með réttu reiða sig á skilríkin svo fremi að tjónið sé tilkomið vegna eftirtalinna atriða:

a) upplýsingar í skilríkjunum voru ekki réttar á þeim tíma sem skilríkin voru gefin út,

b) skilríkin innihalda ekki þær upplýsingar sem krafist er í kafla 7.3.3,

c) misbrestur verður á afturköllun skilríkjanna, sjá kafla 7.3.6,

d) upplýsingar skortir eða upplýsingar eru rangar um afturköllun skilríkjanna, gildistíma eða takmarkanir varðandi notkun eða fjárupphæðir, sjá kafla 7.3.3 og 7.3.6,

e) ákvæði í kafla 7.3.1 um skráningu eru ekki virt.

Ofangreind skaðabótaábyrgð gildir einungis ef sýnt þykir að tjónið hafi orðið vegna ásetnings eða gáleysis starfsmanna VÍR.

Ábyrgð VÍR tekur ekki til nokkurs konar óbeins, tilviljanakennds eða afleidds tjóns, þar með talið en ekki einskorðað við hvers konar missi á hagnaði, missi afnota, eða refsikenndra bóta eða viðurlaga sem orsakast af eða standa í sambandi við notkun, afhendingu, leyfi, virkni eða óvirkni skilríkis eða hvers konar framkvæmda, aðgerða eða þjónustu sem boðin er fram eða áformuð í tengslum við það.

VÍR getur afmarkað skyldur sínar við samningsaðila sína.

7 Kröfur um framkvæmd vottunarstöðva

VÍR viðhefur stýringar sem uppfylla kröfur samkvæmt þessum kafla.

Í þessum kafla eru kröfur um skráningu, framleiðslu og dreifingu skilríkja, afturköllunarþjónustu, afturköllunarmiðlun og afhendingu búnaðar vottorðshafa (sjá kafla 4.2).

Kröfunum er lýst með öryggismarkmiðum sem fylgt er eftir með ítarlegri stefnureglum um stýringar til að uppfylla þessi markmið.

7.1 Yfirlýsing um framkvæmd vottunar

VÍR gefur út yfirlýsingu um framkvæmd og verklag.

Sérstaklega uppfyllir VÍR eftirfarandi kröfur:

a) Tilgreinir í yfirlýsingu um framkvæmd vottunar hvernig kröfum í vottunarstefnu þessari verður fullnægt.

b) Tilgreinir í yfirlýsingu um framkvæmd vottunar skyldur allra lögaðila sem styðja starfsemi vottunarstöðvarinnar, þar á meðal viðeigandi stefnureglur og framkvæmd.

c) Veitir áskrifendum og hagsmunaaðilum aðgang að yfirlýsingu um framkvæmd vottunar og öðrum viðeigandi skjölum að því marki sem nauðsynlegt er til að meta samræmi við vottunarstefnuna. VÍR þarf ekki að hafa aðgengileg öll atriði varðandi framkvæmd vottunarinnar.

d) Birtir skilmála og skilyrði sem varða notkun skilríkja, eins og tilgreint er í kafla 7.3.4, öllum áskrifendum og væntanlegum hagsmunaaðilum.

e) Stjórnendur VÍR bera tilgreinda ábyrgð á yfirlýsingu um framkvæmd vottunar og hafa endanlegt vald til að samþykkja hana.

f) Yfirstjórn VÍR er ábyrg fyrir því að framkvæmd vottunar sé á öllum tímum í samræmi við viðeigandi stefnureglur í þessu skjali.

g) Skilgreinir úttektarferli fyrir framkvæmd vottunar sem felur m.a. í sér ábyrgð á viðhaldi yfirlýsingu um framkvæmd vottunar.

h) Tilkynnir um fyrirhugaðar breytingar á yfirlýsingu um framkvæmd vottunar með nægilegum fyrirvara og veitir áskrifendum og hagsmunaaðilum aðgang að nýrri yfirlýsingu um framkvæmd vottunar, í samræmi við c)-lið hér fyrir ofan, tafarlaust eftir að hún hefur verið samþykkt af stjórnendum VÍR sem tilgreindir eru í e)-lið.

i) Skjalfestir þau algrím og þær færibreytur sem notaðar eru.

7.2 Dreifilyklaskipulag - lífsferill lyklaumsjónar

Meðhöndlun lykla hjá VÍR er í samræmi við ETSI TS 102 176-1 [12] sem inniheldur lista yfir viðurkennd dulmálsalgrím ásamt kröfum um færibreytur þeirra.

7.2.1 Framleiðsla einkalykla vottunarstöðva

Framleiðsla skilríkja

VÍR framleiðir rótarlykla og aðra einkalykla sína, sem notaðir eru til að undirrita skilríki, í stýrðu umhverfi. Í því skyni mun VÍR sérstaklega uppfylla eftirfarandi kröfur:

a) Einkalyklar VÍR eru framleiddir í raunlægt (e. physically) öruggu umhverfi (sjá kafla 7.4.4) af einstaklingum í trúnaðarstöðum (sjá kafla 7.4.3) með tvískiptri stjórnun (e. dual control), að lágmarki. Fjöldi þeirra einstaklinga sem hafa heimild til að framleiða einkalykla er haldið í lágmarki.

b) Einkalyklar VÍR eru framleiddir í búnaði sem

   i. uppfyllir að lágmarki kröfur stigs 3 (e. level 3) í FIPS 140-2 [7], eða

   ii. uppfyllir kröfur CWA 14167-2 [9], CWA 14167-3 [10] eða CWA 14167-4 [11], eða

iii. er áreiðanlegt kerfi sem staðfest er að uppfylli að lágmarki EAL 4 í samræmi við ISO/IEC 15408 [8], eða jafngilt öryggisviðmið. Þetta skal vera hluti af öryggismarkmiði eða verndunarsniðum sem uppfylla kröfur þessa skjals og sem byggja á áhættugreiningu þar sem tekið er tillit til raunlægra öryggisráðstafana auk annarra öryggisráðstafana sem eru ekki tæknilegar.

c) Einkalyklar VÍR eru framleiddir með algrími sem er viðurkennt fyrir undirritun vottunarstöðvar á skilríkjum samkvæmt ETSI TS 102 176-1 [12].

d) Lengd og algrím fyrir undirskriftarlykil VÍR er í samræmi við viðurkenndar venjur við undirritun vottunarstöðvar á skilríkjum, sbr. ETSI TS 102 176-1 [12].

e) VÍR framleiðir nýtt lyklapar fyrir undirritun skilríkja og gerir nauðsynlegar ráðstafanir til að koma í veg fyrir truflun á starfsemi þeirra sem gætu treyst á undirskriftarlykilinn tímanlega áður en gildistími gildandi undirskriftarlykils rennur út.

7.2.2 Geymsla, öryggisafritun og endurheimt lykla hjá vottunarstöðvum

Framleiðsla skilríkja

VÍR tryggir að einkalyklar þess haldist leyndir og að heilleiki þeirra varðveitist með því m.a. að uppfylla eftirfarandi kröfur:

a) Einkalyklar VÍR fyrir undirritun skilríkja eru varðveittir og notaðir í dulmálseiningu sem:

i. uppfyllir að lágmarki kröfur stigs 3 (e. Level 3) í FIPS 140-2 [7], eða

ii. uppfyllir kröfur CWA 14167-2 [9], CWA 14167-3 [10] eða CWA 14167-4 [11], eða

iii. er áreiðanlegt kerfi sem staðfest er að uppfylli að lágmarki EAL 4 í samræmi við ISO/IEC 15408 [8], eða jafngilt öryggisviðmið. Þetta skal vera hluti af öryggismarkmiði eða verndunarsniðum sem uppfylla kröfur þessa skjals og sem byggja á áhættugreiningu þar sem tekið er tillit til raunlægra öryggisráðstafana auk annarra öryggisráðstafana sem eru ekki tæknilegar.

b) Ef einkalykill VÍR fyrir undirritun er færður á milli öruggs dulmálsbúnaðar er einkalykilinn verndaður með jafn traustum hætti og dulmálsbúnaðurinn veitir, samanber kröfur í a).

c) Vistun öryggisafritun og endurheimt á einkalykli VÍR fyrir undirritun er framkvæmt í raunlægt (e. physically) öruggu umhverfi (sjá kafla 7.4.4) af einstaklingum sem gegna trúnaðarhlutverki í vottunarstöðinni í að minnsta kosti tvískiptri stjórnun (sjá kafla 7.4.3). Fjölda þeirra einstaklinga sem hafa heimild til að framkvæma þessa aðgerð er haldið í lágmarki og í samræmi við verklag hjá VÍR.

d) VÍR beitir sambærilegum öryggisstýringum við meðhöndlun öryggisafrita af einkalyklum VÍR og beitt er fyrir einkalykla í notkun.

e) Aðgangsstýringum er beitt til að koma í veg fyrir að lyklar, sem geymdir eru í sérstökum vélbúnaði fyrir meðhöndlun þeirra, séu aðgengilegir utan vélbúnaðarins.

7.2.3 Dreifing VÍR á dreifilyklum

Framleiðsla og miðlunarþjónusta

VÍR tryggir að heilleiki og áreiðanleiki dreifilykilsins sem notaður er til að sannvotta undirskrift skilríkja og tengdra færibreyta sé viðhaldið við dreifingu til hagsmunaaðila.

Sérstaklega mun VÍR tryggja að:

a) Dreifilykill VÍR, sem notaður er til að sannvotta undirskrift skilríkja, sé aðgengilegur hagsmunaaðilum á þann hátt að hagsmunaaðilar geti fullvissað sig um heilleika hans og fengið uppruna hans sannvottaðan.

7.2.4 Vörsluafrit lykla

a) VÍR varðveitir ekki einkalykla vottorðshafa.

7.2.5 Notkun á einkalykli vottunarstöðva

VÍR tryggir að eigin einkalyklar séu ekki notaðir á óviðeigandi hátt.

Framleiðsla skilríkja

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

a) VÍR sér til þess að eigin einkalyklar sem notaðir eru til undirritunar á skilríkjum, eins og tilgreint er í kafla 7.3.3, eða til undirritunar á stöðuupplýsingum um skilríki séu ekki notaðir í öðrum tilgangi.

b) VÍR sér til þess að undirskriftarlyklar skilríkja séu aðeins notaðir í raunlægt (e. physically) öruggum húsakynnum samkvæmt 7.4.4.

7.2.6 Endalok lífskeiðs einkalykla vottunarstöðva

Einkalyklar VÍR hafa tiltekinn gildistíma. VÍR sér til þess að einkalykill sem notaður er til undirritunar á skilríkjum sé ekki notaður eftir að gildistími hans er liðinn.

Framleiðsla skilríkja

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

a) Notkun samsvarandi einkalykils VÍR afmarkast við þá notkun sem samræmist því tætialgrími, því undirskriftaralgrími og þeirri lengd undirskriftarlykla sem notuð eru í framleiðsluskilríkinu samanber viðurkenndar venjur í 7.2.1 d).

b) Eftir að gildistíma lýkur mun VÍR annað hvort eyðileggja einkalykilinn eða geyma hann þannig að ekki sé hægt að nota hann aftur.

7.2.7 Umsjón dulmálsvélbúnaðar fyrir undirritun skilríkja á lífsskeiði hans

VÍR meðhöndlar og varðveitir dulmálsvélbúnað samkvæmt kröfum í kafla 7.4 á lífsskeiði dulmálsbúnaðarins.

Framleiðsla skilríkja

Sérstaklega mun VÍR tryggja að:

a) dulmálsvélbúnaður fyrir undirritun skilríkja og stöðuupplýsinga sé hvorki misnotaður né honum stofnað í hættu þegar hann er í flutningi.

b) dulmálsvélbúnaður fyrir undirritun skilríkja og stöðuupplýsinga sé hvorki misnotaður né honum stofnað í hættu þegar hann er í geymslu.

c) meðferð á undirskriftarlyklum VÍR í dulmálsvélbúnaði, þar með talin uppsetning, gangsetning, afritun og endurreisn eftir áfall, sé í samstilltri stjórnun að minnsta kosti tveggja einstaklinga sem hafa hvor sitt trúnaðarhlutverk í vottunarstöðinni.

d) dulmálsvélbúnaður fyrir undirritun skilríkja og stöðuupplýsinga virki ávallt rétt.

e) undirskriftarlyklum sem varðveittir eru í dulmálsvélbúnaði og sem ætlaðir eru til undirritunar á skilríkjum og stöðuupplýsingum, sé eytt ef dulmálsvélbúnaðurinn er tekinn varanlega úr notkun.

7.2.8 Umsjón VÍR með lyklum vottorðshafa

VÍR sér til þess að lyklar vottorðshafa framleiddir af VÍR, séu framleiddir á öruggan hátt og að leynd yfir einkalykli vottorðshafa sé tryggð.

Framleiðsla skilríkja

Lyklar vottorðshafa framleiddir hjá VÍR eru:

a) framleiddir með algrími sem er í samræmi við viðurkenndar venjur fyrir þá notkun skilríkjanna á gildistíma þeirra sem tilgreind er í vottunarstefnu þessari, samanber ETSI TS 102 176-1 [12].

b) af þeirri lengd og fyrir notkun með þeim dreifilyklaalgrímum sem eru í samræmi við viðurkenndar venjur fyrir þá notkun skilríkjanna á gildistíma þeirra sem tilgreind er í þessari vottunarstefnu, samanber ETSI TS 102 176-1 [12].

c) framleiddir og varðveittir á öruggan hátt áður en þeir eru afhentir vottorðshafa. VÍR eyðir afritum af einkalykli vottorðshafa þegar honum hefur verið komið fyrir í öruggum notendabúnaði.

d) afhentir þannig að trausti til lyklanna sé ekki stofnað í hættu og þannig að einkalykill vottorðshafa sé alfarið á forræði vottorðshafa eftir að hann hefur verið afhentur.

e) Ef afrit af lyklum vottorðshafa verður ekki varðveitt hjá VÍR eða öðrum réttmætum aðila eftir afhendingu til vottorðshafa, samanber 7.2.4, munu einungis vottorðshafinn, eða áskrifandinn hafa aðgang að einkalyklinum. Í slíkum tilvikum mun öllum afritum af lyklum vottorðshafa hjá VÍR vera eytt.

7.2.9 Undirbúningur á öruggum notendabúnaði eða öruggum undirskriftarbúnaði

VÍR mun tryggja öruggan frágang og afhendingu á öruggum notendabúnaði þegar notendabúnaður er afhentur vottorðshafa.

Afhending búnaðar vottorðshafa

a) Frágangur á öruggum notendabúnaði er undir öruggu eftirliti VÍR.

b) Öruggur notendabúnaðar er geymdur á öruggum stað og honum dreift á öruggan hátt.

c) Öruggt eftirlit er haft með því þegar öruggur notendabúnaður er gerður óvirkur eða virkjaður aftur.

d) Notkunaraðgangsorð sem fylgja öruggum notendabúnaði eru undirbúin á öruggan hátt og dreift aðskilið frá notendabúnaði.

7.3 Dreifilyklaskipulag - lífsskeið skilríkjaumsjónar

7.3.1 Skráning vottorðshafa

VÍR tryggir að gögn til að bera kennsl á áskrifanda skilríkja og vottorðshafa auk áreiðanleika nafna þeirra og tilheyrandi upplýsinga, séu könnuð með viðeigandi hætti. VÍR tryggir einnig að umsóknir um skilríki séu réttar, innihaldi þær upplýsingar sem krafist er og séu byggðar á gildu umboði þegar það á við.

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

Skráningarþjónusta

a) Áður en VÍR gerir samning við áskrifanda skilríkja er áskrifandinn upplýstur um skilmála og skilyrði fyrir notkun skilríkjanna samanber kafla 7.3.4.

b) VÍR miðlar upplýsingum samkvæmt a)-lið þannig að heilleiki þeirra sé varanlega tryggður. Upplýsingunum er miðlað á skýru og einföldu máli.

c) Vottunarstöðin skal afla annað hvort beinna sannana eða vitnisburðar frá viðeigandi og réttmætum aðilum um auðkenni (eins og nafn) og, ef við á, um tilteknar eigindir vottorðshafa. Framlögð gögn geta verið hvort sem er rafræn skjöl eða á pappír. Staðfesting á auðkenni vottorðshafa skal staðfesta með viðeigandi aðferðum um leið og skráning fer fram og í samræmi við lög.

d) Allar upplýsingar sem nauðsynlegar eru til að staðfesta auðkenni vottorðshafa eru skjalfestar, og sérhver einkenni vottorðshafa ef það á við, þar með talið tilvísanir í gögn sem notuð eru til staðfestingar og þær takmarkanir sem kunna að vera á gildi þeirra.

e) Framlögð gögn skulu færa sönnur á eftirfarandi:

   i. Fullt nafn lögaðila (sem vottorðshafa) með vísun í viðurkennda skráningu, t.d. fyrirtækjaskrá, eða önnur einkenni sem hægt er að nota til að aðgreina lögaðilann frá öðrum.

   ii. Fullt nafn, kennitölu og stöðu áskrifanda skilríkja.

   iii. Fullt nafn, kennitölu og fæðingastað lögbærs fulltrúa vottorðshafa samkvæmt þjóðskrá.

iv. Tengsl lögbærs fulltrúa vottorðshafa við áskrifanda skilríkja.

v. Heimild lögbærs fulltrúa áskrifanda til að sækja um skilríki fyrir hönd vottorðshafa.

f) VÍR skjalfestir allar ofangreindar upplýsingar sem nauðsynlegar eru til að staðfesta auðkenni vottorðshafa og lögbærra fulltrúa, þar með talið tilvísanir í gögn sem notuð eru til staðfestingar og þær takmarkanir sem kunna að vera á gildi þeirra.

g) Áskrifandi skilríkja skal gefa upp lögheimili, tölvupóstfang eða aðrar upplýsingar um hvernig unnt sé að hafa samband við hann.

h) VÍR varðveitir undirritað samkomulag við áskrifanda skilríkja sem meðal annars felur í sér:

i. Samkomulag um skyldur áskrifanda skilríkja (sjá kafla 6.2).

ii. Samkomulag við áskrifanda skilríkja um notkun á öruggum undirritunarbúnaði (sjá kafla 7.2.2.a).

iii. Samþykki áskrifanda fyrir því að VÍR varðveiti upplýsingar sem notaðar eru við skráningu, afhendingu búnaðar til vottorðshafa og afturköllun (sjá kafla 7.4.11). Einnig samþykki fyrir varðveislu á auðkenni og öðrum einkennum sem sett eru í skilríkin og miðlun þessara upplýsinga til annarra aðila með sömu skilyrðum og uppfylla skal þegar VÍR hættir starfsemi.

iv. Hvort, og þá með hvaða skilyrðum, áskrifandi skilríkja getur krafist útgáfu skilríkja og vottorðshafi samþykkt útgáfu skilríkjanna.

v. Staðfestingu á því að upplýsingar í skilríkjunum séu réttar.

i) VÍR varðveitir upplýsingar sem skráðar eru skv. fyrirmælum í þessum kafla eins lengi og nauðsynlegt er svo unnt sé að veita sönnun á vottun, meðal annars fyrir dómstólum. VÍR upplýsir áskrifendur skilríkja um hvaða upplýsingar verða geymdar og hversu lengi.

j) Þegar lyklapar vottorðshafa er ekki framleitt af VÍR staðfestir VÍR samkvæmt verklagi fyrir umsókn skilríkja:

i. að vottorðshafi hafi undir höndum þann einkalykil sem samsvarar þeim dreifilykli sem vottaður er.

ii. að sá dreifilykill sem vottaður er sé hluti af lyklapari sem framleitt er í öruggum notendabúnaði.

k) VÍR sér til þess að lögum um persónuvernd og meðferð persónuupplýsinga nr. 77/2000 [3] sé framfylgt í skráningarferlinu, þar á meðal notkun gervinafns ef við á.

l) Við staðfestingu á auðkenni mun VÍR takmarka varðveislu auðkenningargagna við það sem nauðsynlegt er fyrir ætlaða notkun skilríkjanna.

7.3.2 Endurnýjun, uppfærsla og endurlyklun skilríkja

VÍR tryggir að beiðni um útgáfu skilríkja til vottorðshafa sem hefur áður verið skráður hjá VÍR, sé byggð á réttum og fullnægjandi upplýsingum og sé byggð á tilhlýðilegri heimild, t.d. gildu umboði. Þetta á við um endurnýjun skilríkja, endurlyklun eftir afturköllun eða þegar gildistími skilríkjanna er að renna út, eða uppfærslu vegna breytinga á eigindum vottorðshafa.

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

Skráningarþjónusta

a) VÍR sækir staðfestingu á tilvist og gildi þeirra skilríkja sem beðið er um endurnýjun á, og að þær upplýsingar sem lágu til grundvallar sannprófun á auðkenni og eigindum vottorðshafa séu enn réttar.

b) Ef breytingar verða á skilmálum eða skilyrðum VÍR mun VÍR miðla þeim til áskrifanda skilríkjanna og gera samkomulag í samræmi við kafla 7.3.1 a), b) og h).

c) Ef nöfn eða aðrar eigindir sem vottaðar eru hafa breyst eða ef skilríkin hafa verið afturkölluð mun vottunarstöðin sannprófa, skrá og ganga frá samkomulagi við áskrifanda skilríkjanna í samræmi við kafla 7.3.1.

d) VÍR skal ekki gefa út ný skilríki með eldri dreifilykli vottorðshafa nema staðfest sé að dulritunaröryggi hans sé nægjanlegt fram yfir gildistíma nýju skilríkjanna og að engar vísbendingar séu um að trausti einkalykils vottorðshafans hafi verið stofnað í hættu.

7.3.3 Framleiðsla skilríkja

Útgáfa skilríkja hjá VÍR er framkvæmd á öruggan hátt og áreiðanleika þeirra viðhaldið.

Innihald skilríkja er í samræmi við viðmið í *Innihald rafrænna skilríkja* [5].

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

Framleiðsla skilríkja

a) Skilríkin innihalda eftirfarandi:
   i. Auðkenni vottunarstöðvar og þess lands þar sem vottunarstöðin er skráð.
   ii. Nafn vottorðshafa eða gervinafn sem skal auðkennt sem slíkt.
   iii. Sérstök eigindi vottorðshafa ef fyrirhuguð notkun skilríkjanna þarfnast þess.
   iv. Dreifilykil sem samsvarar einkalykli vottorðshafans.
   v. Upphaf og enda gildistíma skilríkjanna.
   vi. Raðnúmer skilríkjanna.
   vii. Rafræna undirskrift vottunarstöðvarinnar sem gefur skilríkin út.
   viii. Takmörkun á notagildi skilríkjanna, þegar það á við.
b) VÍR gerir ráðstafanir til að koma í veg fyrir fölsun á skilríkjum og ábyrgist trúnað við framleiðslu einkalykils vottorðshafa þegar hann er framleiddur hjá vottunarstöðinni.
c) Útgáfa skilríkja er tryggilega tengd tilsvarandi skráningu, endurnýjun, uppfærslu eða endurlyklun skilríkja, þar með talið ráðstafanir vegna dreifilykla sem framleiddir eru hjá vottorðshafa.
d) Þegar lyklapar vottorðshafa er framleitt hjá VÍR:
   i. Fylgir VÍR verklagsreglum sem tryggja örugg tengsl útgáfu skilríkjanna við framleiðslu lyklaparsins.
   ii. Afhendir VÍR vottorðshafa öruggan notendabúnað eða undirskriftarbúnað sem inniheldur einkalykil vottorðshafans á öruggan hátt.
e) VÍR tryggir að sértækt nafn (*distinguished name*) sem notað er í skilríkjum verður aldrei notað til að auðkenna annan aðila.
f) Trúnaður og heilleiki skráningargagna er verndaður, sérstaklega þegar þeim er miðlað til áskrifenda og vottorðshafa eða þegar þeim er miðlað á milli dreifðra kerfishluta vottunarstöðvar.
g) Þegar rekstri skráningarstöðvar er útvistað tryggir VÍR að samskipti með skráningargögn séu einungis við viðurkenndar skráningarstöðvar með því að staðfesta auðkenni þeirra .

7.3.4 Miðlun á skilmálum og skilyrðum

Skilmálar og skilyrði eru aðgengileg fyrir áskrifendur og treystendur.

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

a) VÍR hefur eftirfarandi skilmála og skilyrði sem varða notkun skilríkjanna aðgengilega fyrir áskrifendur og hagsmunaaðila sem reiða sig á skilríkin:
   i. Vottunarstefnu þessa.
   ii. Takmarkanir á notkun skilríkjanna.
   iii. Skyldur áskrifanda eins og þær eru skilgreindar í kafla 6.2.
   iv. Upplýsingar um það hvernig skuli staðfesta gildi skilríkjanna, þar með talið hvernig skuli kanna stöðu skilríkjanna þannig að hagsmunaaðili geti reitt sig á skilríkin (sjá kafla 6.3).
   v. Takmarkanir á skaðabótaskyldu, þar með talið þá afmörkun á notkun eða tilgangi skilríkjanna sem vottunarstöðin tilgreinir í tengslum við bótaskyldu sína.
   vi. Varðveislutíma skráningarupplýsinga (sjá kafla 7.3.1).

vii. Varðveislutíma færsluskráa vottunarstöðvarinnar (sjá kafla 7.4.11).

viii. Ferli vegna kvartana og sátta í deilumálum.

ix. Tilvísun í viðeigandi lagaumhverfi.

x. Hvort vottunarstöðin hefur verið metin með hliðsjón af samræmi við tilgreinda vottunarstefnu, og þá hvernig.

b) VÍR miðlar upplýsingum sem fram koma í a)-lið þannig að heilleiki þeirra sé varanlega tryggður. Upplýsingunum er miðlað á skýru og einföldu máli.

7.3.5 Miðlun skilríkja

VÍR hefur skilríkin aðgengileg fyrir áskrifendur, vottorðshafa og hagsmunaaðila sem reiða sig á skilríkin. Í þeim tilgangi veitir VÍR eftirfarandi þjónustu:

Miðlunarþjónusta

a) Að lokinni framleiðslu skilríkja og eftir staðfestingu á innihaldi þeirra eru þau aðgengileg fyrir áskrifandann eða vottorðshafann sem skilríkin eru gefin út fyrir.

b) Að fengnu samþykki vottorðshafans eru skilríki aðgengileg fyrir hagsmunaðila.

c) Skilmálar og skilyrði sem varða notkun skilríkjanna eru aðgengileg fyrir treystendur skilríkjanna.

d) Það skal vera auðvelt að finna þá skilmála og þau skilyrði sem eiga við tiltekin skilríki.

e) Upplýsingar sem tilgreindar eru í b) og c) lið verða ætíð aðgengilegar, allan sólarhringinn sjö daga vikunnar um allan heim. Ef bilun verður í kerfi eða búnaði sem vottunarstöðin hefur ekki stjórn á, skal vottunarstöðin gera ráðstafanir til að þessar upplýsingar séu gerðar aðgengilegar innan tímamarka sem tilgreind eru í yfirlýsingu vottunarstöðvar um framkvæmd vottunar.

7.3.6 Afturköllun og tímabundin ógilding skilríkja

VÍR afturkallar skilríki svo fljótt sem auðið er ef beiðni um afturköllun er staðfest og kemur frá aðila sem hefur heimild til þess að biðja um afturköllun. VÍR rekur í því skyni eftirfarandi þjónustu:

Afturköllunarþjónusta

a) Í yfirlýsingu VÍR um framkvæmd vottunar eru settar fram skjalfestar verklagsreglur fyrir afturköllun á skilríkjum. Þessar verklagsreglur innihalda meðal annars eftirfarandi:

i. Hver hafi heimild til að leggja fram tilkynningar og beiðnir um afturköllun.

ii. Hvernig heimilt sé að leggja fram tilkynningar og beiðnir um afturköllun.

iii. Þær kröfur sem vottunarstöðin gerir um frekari staðfestingar á tilkynningum og beiðnum um afturköllun.

iv. Hvort og þá af hvaða ástæðum heimilt sé að ógilda skilríki tímabundið.

v. Þær aðferðir sem notaðar eru til að dreifa upplýsingum um afturköllunarstöðu.

vi. Þann tíma sem líður frá móttöku á tilkynningu eða beiðni um afturköllun þar til breytingar á upplýsingum um afturköllunarstöðu eru aðgengilegar fyrir alla þá sem reiða sig á skilríkin.

b) VÍR afgreiðir tilkynningar og beiðnir vegna afturköllunar um leið og þær eru mótteknar; (t.d. vegna brests á öryggi einkalykils vottorðshafans, dauðsfalls vottorðshafans, óvæntra breytinga á tengslum milli áskrifanda og vottorðshafa og vegna riftunar samnings).

c) VÍR staðfestir að tilkynningar og beiðnir vegna afturköllunar komi frá aðila með réttar heimildir. Slíkar tilkynningar og beiðnir eru staðfestar í samræmi við verklagsreglur VÍR.

d) VÍR getur ógilt skilríki tímabundið á meðan afturköllun er staðfest og sér þá til þess að skilríki sé ekki ógilt af þessum ástæðum lengur en nauðsynlegt er til að staðfesta stöðu þess.

e) Vottorðshafa og áskrifanda þeirra skilríkja sem hafa verið afturkölluð eða ógilt tímabundið er tilkynnt um breytingu á stöðu þeirra.

f) Þegar afturköllun skilríkja hefur verið staðfest (þ.e. þegar ekki er bara um tímabundna ógildingu að ræða) eru skilríkin ekki gerð gild aftur.

g) Afturköllunarlistar (CRL), þar með talið breytingarlistar (e. delta CRL), sem VÍR birtir eru gefnir út að hámarki með 5 ára millibili.

h) Einungis afturköllunarlistar (CRL) eða breytingarlistar (e. delta CRL) eru notaðir til að veita upplýsingar um afturköllunarstöðu og gildir um þá eftirfarandi:

vii. Í sérhverjum afturköllunarlista kemur fram hvenær afturköllunarlisti verður gefinn út næst.

viii. Nýr afturköllunarlisti getur verið gefinn út áður en komið er að tilgreindum útgáfutíma.

ix. Afturköllunarlistinn er undirritaður af vottunarstöðinni eða af öðrum aðila sem vottunarstöðin tilgreinir.

i) Afturköllunarlistar VÍR eru í samræmi við kröfur í ISO/IEC 9594-8|ITU-T X.509 [13].

j) Afturköllunarþjónusta VÍR er aðgengileg allan sólarhringinn sjö daga vikunnar. Ef rof verður á afturköllunarþjónustu af ástæðum sem VÍR hefur ekki stjórn á þá reynir VÍR af fremsta megni að sjá til þess að þjónustan sé aðgengileg aftur innan þeirra tímamarka sem tilgreind eru í yfirlýsingu um framkvæmd vottunar.

Afturköllunarmiðlun

k) Upplýsingar um afturköllunarstöðu skilríkja verða aðgengilegar allan sólarhringinn sjö daga vikunnar um allan heim. Ef rof verður á afturköllunarmiðlun af ástæðum sem VÍR hefur ekki stjórn á þá reynir VÍR af fremsta megni að sjá til þess að upplýsingar um stöðu skilríkja séu aðgengilegar aftur innan þeirra tímamarka sem tilgreind eru í yfirlýsingu vottunarstöðvarinnar um framkvæmd vottunar.

l) VÍR verndar heilleika upplýsinga um stöðu skilríkja og áreiðanleika uppruna þeirra.

m) Upplýsingar um afturköllunarstöðu skilríkjanna innihalda upplýsingar um stöðu skilríkjanna að minnsta kosti þar til gildistími þeirra rennur út.

7.4 Stjórnun og rekstur vottunarstöðva

7.4.1 Stjórnun upplýsingaöryggis

Verklagsreglur VÍR um stjórnun og rekstur eru fullnægjandi með hliðsjón af starfsemi og í samræmi við ÍST ISO/IEC 17799 [14].

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

Almennar kröfur til vottunarstöðva

a) VÍR framkvæmir áhættumat til að meta rekstraráhættu og ákvarða nauðsynlegar öryggiskröfur og verkferla í rekstri. Áhættumatið er rýnt reglulega og endurskoðað þegar það er nauðsynlegt.

b) VÍR er ábyrgt fyrir öllum þáttum vottunarþjónustunnar, einnig þeim hlutum þjónustunnar sem útvistað er til ytri aðila. VÍR skilgreinir ábyrgð ytri aðila ítarlega og gerir ráðstafanir til að skuldbinda þá til að innleiða sérhverjar þær stýringar sem VÍR krefst. VÍR er ábyrgt fyrir birtingu upplýsinga um hlutverk allra aðila í yfirlýsingu um framkvæmd vottunar.

c) Stjórnendur VÍR hafa forystu um upplýsingaöryggi með því að samþykkja stefnu um upplýsingaöryggi og skipa háttsetta stýrinefnd til að viðhalda henni og sjá til þess að hún sé birt og kynnt öllum starfsmönnum og viðeigandi ytri aðilum.

d) VÍR hefur á að skipa skilvirku stjórnkerfi upplýsingaöryggis í samræmi við líkan sem gefið er í ÍST ISO/IEC 27001[15]. Stjórnkerfi upplýsingaöryggis VÍR fullnægir þeim kröfum sem settar eru í ÍST ISO/IEC 27001 [15] fyrir þá vottunarþjónustu sem VÍR veitir. Stefnureglur fyrir stjórnun upplýsingaöryggis taka mið af ÍST ISO/IEC 17799[14].

e) VÍR viðhefur ætíð nauðsynlegt skipulag á upplýsingaöryggi til að stýra öryggginu. Allar breytingar sem hafa áhrif á öryggisstig skulu samþykktar af öryggisráði VÍR.

f) VÍR hefur skjalfest, innleitt og mun viðhalda öryggisstýringum og rekstrarferlum fyrir aðstöðu vottunarstöðvarinnar, kerfi og upplýsingaeignir sem vottunarþjónustan byggir á.

g) VÍR viðheldur öryggi upplýsinga þegar ábyrgð á starfsþáttum VÍR er útvistað til annars fyrirtækis eða aðila.

7.4.2 Eignastjórnun

VÍR verndar eignir og upplýsingar fyrirtækisins. VÍR heldur eignaskrá yfir allar upplýsingar og tiltekur verndarstig fyrir þessar eignir í samræmi við áhættugreiningu.

7.4.3 Mannauður og öryggi

Aðferðir VÍR við mönnun hlutverka í VÍR eru ætíð þannig að þær auki og styðji áreiðanleika starfseminnar.

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

Almennar kröfur

a) VÍR hefur á að skipa starfsmönnum sem búa yfir þeirri sérþekkingu, reynslu og hæfni sem nauðsynleg er vegna þeirrar þjónustu sem veitt er og sem er viðeigandi fyrir hlutverk starfsmannanna.

b) VÍR beitir viðeigandi viðurlögum vegna brota starfsmanna á stefnureglum eða verklagsreglum vottunarstöðvarinnar.

c) Hlutverk og ábyrgð er lúta að öryggi samkvæmt upplýsingaöryggisstefnu VÍR eru skjalfestar í starfslýsingum. Trúnaðarstörf, sem öryggi í starfsemi vottunarstöðvarinnar byggist á, eru skilgreind á skýran hátt.

d) Starfsmenn VÍR, bæði fastráðnir og tímabundnir starfsmenn, hafa starfslýsingu sem skilgreind er með hliðsjón af nauðsynlegum aðskilnaði á skyldum og takmörkun sérréttinda. Í starfslýsingu eru vegnar saman skyldur og þörf fyrir aðgangsstig að búnaði og aðstöðu, könnun á ferli einstaklingsins, þekking og skilningur á viðkomandi hlutverki. Þar sem við á er greint á milli almennra starfa og starfa sem eru sértæk fyrir VÍR. Starfslýsingar innihalda kröfur um færni og reynslu.

e) Starfsmenn skulu viðhafa verklag og ferli í stjórnun og rekstri sem eru í samræmi við verklagsreglur VÍR í stjórnun upplýsingaöryggis (sjá kafla 7.4.1).

Skráning, framleiðsla skilríkja, afhending búnaðar vottorðshafa, afturköllunarþjónusta

f) Stjórnendur VÍR hafa þekkingu á tækni við rafræna undirritun, þekkja öryggisverklag fyrir starfsmenn er bera öryggisábyrgð, og hafa fullnægjandi reynslu af upplýsingaöryggi og áhættumati til að sinna stjórnunarstarfi.

g) Allir starfsmenn VÍR í trúnaðarstarfi eru lausir við stríðandi hagsmuni sem gætu skaðað hlutleysi starfseminnar.

h) Trúnaðarstörf eru meðal annars eftirfarandi ábyrgðarstörf:

   i. Öryggisstjórar: Bera heildarábyrgð á stjórnun framkvæmdar öryggisaðgerða og samþykkja framleiðslu, afturköllun og ógildingu skilríkja.

   ii. Kerfisstjórar: Hafa heimild til að setja upp, stilla og viðhalda áreiðanlegum kerfum vottunarstöðvar fyrir skráningu, framleiðslu skilríkja, frágang búnaðar vottorðshafa og afturköllunarþjónustu.

   iii. Kerfisumsjónarmenn: Bera ábyrgð á daglegum rekstri kerfa vottunarstöðvar. Hafa heimild til að taka öryggisafrit og endurheimta afrituð gögn.

   iv. Eftirlitsaðilar kerfa: Hafa heimild til að skoða safnvistuð gögn og dagbókarfærslur í kerfum vottunarstöðvarinnar.

i) Starfsmenn VÍR sem gegna trúnaðarstörfum eru skipaðir formlega í það hlutverk af yfirmanni sem er ábyrgur fyrir öryggi.

j) Einstaklingar sem hafa verið dæmdir fyrir alvarleg brot eða fyrir önnur brot sem hafa áhrif á getu þeirra til að gegna trúnaðarstarfi eru ekki skipaðir í trúnaðar- eða stjórnunarstöðu. Starfsmenn sinna ekki trúnaðarstörfum

eða hafa réttindi sem slíkir fyrr en nauðsynlegum athugunum er lokið. VÍR aflar samþykkis viðkomandi starfsmanns áður en slík könnun er framkvæmd.

7.4.4 Raunlægt öryggi

VÍR sér til þess að raunlægum (e. physical) aðgangi að mikilvægri þjónustu sé stýrt og að raunlægri áhættu fyrir eignir VÍR sé haldið í lágmarki.

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

Almennar kröfur

a) Raunlægur aðgangur að aðstöðu þar sem framleiðsla skilríkja, frágangur búnaðar vottorðshafa og afturköllunarþjónusta fer fram er takmarkaður við einstaklinga með viðeigandi heimild.

b) VÍR viðhefur stýringar til að koma í veg fyrir tap, skemmdir eða vásetningu á eignum og truflun á atvinnustarfsemi.

c) VÍR viðhefur stýringar til að koma í veg fyrir vásetningu eða þjófnað á upplýsingum og upplýsingavinnslubúnaði.

Framleiðsla skilríkja, afhending búnaðar vottorðshafa, afturköllunarþjónusta

d) Búnaður þar sem framleiðsla skilríkja, frágangur búnaðar vottorðshafa (sjá kafla 7.2.9) og afturköllunarþjónusta fer fram er á öruggu svæði sem er raunlægt varið gegn hættu vegna aðgangs óviðkomandi án heimilda að búnaði, kerfum eða gögnum.

e) Sérhver einstaklingur sem fer inn á raunlægt örugg svæði er ávallt undir eftirliti einstaklings með viðeigandi heimild.

f) Raunlægar varnir byggja á skýrt skilgreindum öryggismærum (t.d. raunlægum hindrunum) umhverfis örugg svæði þar sem framleiðsla skilríkja, frágangur búnaðar vottorðshafa (sjá kafla 7.2.9) og afturköllunarþjónusta fer fram. Húsrými sem samnýtt er með öðru fyrirtæki eða starfsemi er haft utan þessara öryggismæra.

g) VÍR viðhefur öryggisstýringar til að vernda stoðkerfi húsrýma, kerfisbúnað og aðstöðu fyrir upplýsingavinnslu. Öryggisstefna VÍR fyrir þau kerfi þar sem framleiðsla skilríkja, frágangur búnaðar vottorðshafa (sjá kafla 7.2.9) og afturköllunarþjónusta fer fram tekur meðal annars til stjórnunar á raunlægum aðgangi, verndar gegn náttúruhamförum, eldvarna, rekstrartruflana í stoðkerfum húsrýma og veitna (til dæmis rafveitu, rafdreifingu og fjarskiptasamböndum), bresta í burðarvirki húsrýma, leka í lagnakerfum, þjófa- og innbrotsvarna og endurreisn á starfsemi eftir stóráföll.

h) VÍR viðhefur stýringar til að koma í veg fyrir að búnaður, upplýsingar, miðlar og hugbúnaður sem tengist þjónustu VÍR geti verið fjarlægður úr aðstöðu án heimildar.

7.4.5 Stjórnun samskipta og reksturs

VÍR tryggir að rekstur á búnaði og kerfum vottunarstöðvar sé öruggur og samkvæmt viðurkenndum bestu aðferðum, þannig að áhætta á bilunum eða óhöppum verði í lágmarki.

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

Almennar kröfur

a) VÍR verndar heilleika kerfa sinna gegn veirum, spillihugbúnaði og óheimilum hugbúnaði.

b) VÍR lágmarkar skaða vegna öryggisatvika og bilana með verklagsreglum um tilkynningar og viðbrögð við atvikum.

c) Gagnamiðlar sem notaðir eru af VÍR eru meðhöndlaðir á öruggan hátt til að vernda miðlana gegn skaða, þjófnaði og óheimilum aðgangi.

d) Verklagsreglur VÍR fyrir umsjón gagnamiðla vernda þá gegn úreldingu og hrörnun á því tímabili sem viðhalda þarf skrám.

e) VÍR skilgreinir, skjalfestir, innleiðir og notar ferla og lýsingar á ábyrgðarsviðum og hlutverkum fyrir þau stjórnunar- og trúnaðarstörf sem varða vottunarþjónustu.

Meðhöndlun gagnamiðla og öryggi

f) Allir gagnamiðlar eru meðhöndlaðir á öruggan hátt í samræmi við kröfur um flokkun upplýsinga (sjá kafla 7.4.2). Miðlum sem innihalda viðkvæm gögn er eytt á öruggan hátt þegar notkun þeirra er lokið.

Áætlanagerð vegna kerfa

g) VÍR hefur eftirlit með rýmdarþörf og hefur gert áætlun um framtíðarþarfir sem sjá til þess að vinnsluafl og geymslurými sé ávallt nægilegt.

Tilkynningar atvika og viðbrögð

h) VÍR mun bregðast strax við atvikum og takmarkar áhrif af öryggisbrestum með tímanlegum og samræmdum aðgerðum. Öll atvik verða tilkynnt eins fljótt og auðið er.

i) Úttektarferlar eru gerðir virkir við ræsingu kerfa, sbr. kafla 7.4.11, og ekki stöðvaðir fyrr en slökkt er á kerfum.

j) VÍR hefur eftirlit með eftirlitsskrám (e. audit logs) og eru þær yfirfarnar reglulega til að bera kennsl á sannanir fyrir spellvirkjum.

Framleiðsla skilríkja, afturköllunarþjónusta

Rekstrarferlar og ábyrgð

k) Öryggisrekstur VÍR er aðgreindur frá almennum rekstri í öryggisdeild. Ábyrgð á öryggisrekstri felur meðal annars í sér eftirfarandi þætti:

   i. Rekstrarferla og ábyrgð.

   ii. Skiplagningu öruggra kerfa og viðtöku þeirra.

   iii. Vernd gegn spillihugbúnaði.

   iv. Daglega umsjón.

   v. Stjórnun netkerfa.

   vi. Skilvirkt eftirlit með eftirlitsdagbókum, greiningu atvika og eftirfylgni úrbóta.

   vii. Meðhöndlun og öryggi gagnamiðla.

   viii. Höndlun gagna og hugbúnaðar.

   Öryggisdeild VÍR stýrir þessum ábyrgðarþáttum í öryggisrekstri. Rekstrarfólk sem hefur ekki sérþekkingu má framkvæma þessar öryggisaðgerðir undir eftirliti í samræmi við viðeigandi öryggisstefnu, starfslýsingar og skilgreiningu á ábyrgð.

7.4.6 Aðgangsstýring

Aðgangur að kerfum VÍR er takmarkaður við einstaklinga með heimildir þar að lútandi.

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

Almennar kröfur

Til þess að tryggja að aðgangur að kerfum VÍR takmarkist við einstaklinga með heimildir þar að lútandi skal VÍR m.a. hafa eftirfarandi varnir:

a) Virkar varnir (t.d. eldveggi) verja innra netkerfi vottunarstöðvarinnar frá ytri netkerfum sem ytri aðili hefur aðgang að.

b) Viðkvæm gögn, svo sem persónugreinanleg gögn, eru varin fyrir óheimilum aðgangi eða breytingum. Viðkvæm gögn eru vernduð þegar þeim er miðlað um netkerfi sem eru ekki trygg.

c) VÍR hefur skilvirka stjórnun á aðgangi notenda, þar með talið kerfisumsjónarmanna, kerfisstjóra og annarra notenda sem fá beinan aðgang að kerfinu, til að viðhalda kerfisöryggi. Í því felst m.a. umsjón með notendaaðgangi, eftirlit og tímanlegar breytingar og lokanir á aðgangi.

d) VÍR sér til þess að aðgangur að upplýsingum og notendakerfum sé takmarkaður í samræmi við stefnu um aðgangsstýringu og að kerfi VÍR veiti nægjanlegar stýringar á tölvuöryggi til að mögulegt sé að aðgreina þau trúnaðarstörf sem tilgreind eru í framkvæmdalýsingum, þar með talið aðgreining á hlutverkum í öryggisstjórnun og rekstri. Notkun á hjálparforritum kerfa er takmörkuð og undir strangri stýringu. Aðgangur er takmarkaður þannig að einungis er leyfður aðgangur að þeim tilföngum sem nauðsynlegt er til að notandinn geti sinnt því hlutverki sem honum er falið.

e) Starfsmenn eru auðkenndir og sannvottaðir áður en þeir nota mikilvægan notendahugbúnað tengdum umsjón skilríkjanna.

f) Starfsmenn VÍR eru ábyrgir gerða sinna og skulu halda atburðaskrá (sjá kafla 7.4.11).

g) Komið er í veg fyrir að unnt sé að afhjúpa viðkvæm gögn, eins og skráningargögn (til dæmis skrár sem búið er að eyða), þegar aflagður gagnageymslubúnaðar er aðgengilegur notendum án heimildar.

Framleiðsla skilríkja

h) VÍR sér til þess að netbúnaður í staðarneti (t.d. netbeinar og netskiptar) séu í raunlægt öruggu umhverfi og reglulega er farið yfir uppsetningar þeirra og stillingar til að staðfesta að öryggiskröfur séu uppfylltar.

i) Ráðstafanir eru gerðar með sívakandi eftirlits- og viðvörunarkerfum til hægt sé að skynja, skrá og bregðast tímanlega við sérhverri óheimilli eða óeðlilegri tilraun til að fá aðgang að aðstöðu og eignum VÍR.

Miðlun

j) Miðlunarþjónusta er aðgangsstýrð til að koma í veg fyrir tilraunir til að bæta við eða eyða skilríkjum og breyta öðrum tengdum upplýsingum.

Afturköllunarþjónusta

k) VÍR hefur stöðugt eftirlits- og viðvörunarkerfi til hægt sé að skynja, skrá og bregðast tímanlega við sérhverri óheimilli og/eða óeðlilegri tilraun til að fá aðgang að tilföngum.

Afturköllunarmiðlun

l) Upplýsingakerfi fyrir afturköllunarmiðlun skal stýra aðgangi til að koma í veg fyrir tilraunir til að breyta upplýsingum um stöðu skilríkja.

7.4.7 Öflun, þróun og viðhald upplýsingakerfa

VÍR notar áreiðanleg kerfi og búnað sem eru varin fyrir breytingum. Kerfi og búnaður skulu vera í samræmi við ISO/IEC 15408 [8] eða samsvarandi. Í því skyni mun VÍR:

a) Sjá til þess að greindar séu öryggiskröfur fyrir hönnun og kröfulýsingu í sérhverju kerfisþróunarverkefni á vegum VÍR, eða fyrir þess hönd, til að staðfesta að öryggi sé innbyggt í upplýsingakerfin.

b) Hafa skjalfest stjórnkerfi fyrir útgáfu, breytingar og neyðaruppfærslur rekstrarkerfa og búnaðar, t.d. í samræmi við alþjóðlega staðalinn ISO/IEC 20000 *Information technology: Service management* [16].

7.4.8 Stjórnun á rekstrarsamfellu og umsjón með upplýsingaöryggisatvikum

VÍR sér til þess að rekstur sé endurreistur eins fljótt og auðið er ef alvarlegt áfall verður, meðal annars ef einkalykli vottunarstöðvarinnar hefur verið stofnað í hættu.

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

Almennar kröfur

a) VÍR skilgreinir og viðheldur áætlun um rekstrarsamfellu sem öðlast gildi þegar alvarlegt áfall verður.

Öryggisafritun kerfisgagna vottunarstöðvarinnar og endurheimt

b) VÍR afritar þau kerfisgögn sem nauðsynleg eru til að hefja að nýju starfsemi og vistar þau á öruggum stað þannig að VÍR geti hafið starfsemi vottunarþjónustu sinnar aftur tímanlega eftir óhapp eða hamfarir.

c) Öryggisafrit og endurheimt er framkvæmt af einstaklingi í trúnaðarstarfi eins og tilgreint er í kafla 7.4.3.

Einkalykli vottunarstöðvar stofnað í hættu

d) Áætlun VÍR um rekstrarsamfellu (eða neyðaráætlun) skilgreinir öryggisbrest eða grun um slíkan brest varðandi einkalykil vottunarstöðvarinnar sem alvarlegt áfall og eru undirbúnir ferlar til staðar.

e) Ef alvarlegt áfall verður mun VÍR, þar sem raunhæft er, gera ráðstafanir til að koma í veg fyrir að áfallið endurtaki sig.

Afturköllunarmiðlun

f) Ef öryggisbrestur verður mun VÍR m.a. framkvæma eftirfarandi:

   i. Upplýsa eftirfarandi aðila um öryggisbrestinn: Alla áskrifendur og aðra samningsbundna aðila auk samstarfsaðila sem vottunarstöðin er í samstarfi við, þar með talið þá sem treysta á öryggi í starfsemi vottunarstöðvarinnar og aðrar vottunarstöðvar. Jafnframt skal gera þessar upplýsingar aðgengilegar fyrir aðra aðila sem treysta á öryggi í starfsemi vottunarstöðvarinnar.

   ii. Gefa til kynna að skilríki og upplýsingar um afturköllunarstöðu sem gefin hafa verið út með einkalykli vottunarstöðvarinnar gætu verið ógild.

Öryggisbrestur í algrími

g) Ef einhver af þeim algrímum, eða tengdum færibreytum, sem VÍR eða áskrifendur þess nota verða ófullnægjandi fyrir áframhaldandi notkun þá mun VÍR:

   i. Upplýsa alla áskrifendur og þá samningsbundnu aðila sem treysta á öryggi í starfsemi VÍR og aðra aðila sem VÍR er í samstarfi við. Jafnframt gera þessar upplýsingar aðgengilegar fyrir aðra aðila sem treysta á öryggi í starfsemi VÍR.

   ii. Afturkalla öll skilríki sem algrímin eða tengdar færibreytur hafa áhrif á.

7.4.9 Lokun þjónustu

VÍR sér til þess að viðskiptavinir verði fyrir sem minnstum truflunum ef þjónusta og starfsemi er varanlega stöðvuð og að skrám sem þarf til að veita sönnun á vottun fyrir dómstólum sé viðhaldið áfram.

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

Almennar kröfur til vottunarstöðva

a) Áður en VÍR stöðvar þjónustu sína varanlega mun VÍR framkvæma eftirfarandi:

   i. Upplýsa eftirfarandi aðila um lokun þjónustu: Alla áskrifendur og aðra samningsbundna aðila auk samstarfsaðila sem vottunarstöðin er í samstarfi við, þar með talið þá sem treysta á öryggi i starfsemi vottunarstöðvarinnar og aðrar vottunarstöðvar. Jafnframt gera þessar upplýsingar aðgengilegar fyrir aðra aðila sem treysta á öryggi í starfsemi vottunarstöðvarinnar.

   ii. Fella niður allar heimildir undirverktaka til að framkvæma aðgerðir fyrir hönd VÍR í tengslum við útgáfu skilríkja.

   iii. Framkvæma nauðsynlegar aðgerðir til að yfirfæra skuldbindingar varðandi viðhald skráningarupplýsinga (sjá kafla 7.3.1) og geymslu á atburðarskráningu (sjá kafla 7.4.11) í þann tíma sem tilgreindur er til áskrifenda og hagsmunaaðila (sjá kafla 7.3.4).

   iv. Eyðileggja eða taka úr notkun þann búnað vottunarstöðvar sem mikilvægt er að sé ekki notaður eftir stöðvun, t.d. einkalykla vottunarstöðvar ef stöðvun er á útgáfu skilríkja, eins og skilgreint er í kafla 7.2.6.

b) VÍR hefur getu til þess að uppfylla ofangreindar lágmarkskröfur.

c) VÍR tilgreinir í yfirlýsingu um framkvæmd vottunar hvaða ráðstafanir verði gerðar varðandi stöðvun á þjónustu. Þessar ráðstafanir varða meðal annars eftirfarandi:

   i. Tilkynningar til allra aðila sem stöðvunin snertir.

   ii. Yfirfærsla skuldbindinga til annarra aðila.

   iii. Meðhöndlun á þjónustuþáttum sem nauðsynlegt er að halda úti eftir stöðvun, hugsanlega hjá þriðja aðila. Þetta getur meðal annars átt við um meðhöndlun á afturköllunarstöðu útgefinna skilríkja.

7.4.10 Hlíting

VÍR hlítir lagalegum kröfum

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

Almennar kröfur

a) VÍR hlítir öllum réttarreglum sem taka til verndunar skráa gegn glötun, eyðileggingu og fölsun. Verndun tiltekinna skjala getur hvoru tveggja verið vegna lögbundinna kvaða jafnt sem til stuðnings mikilvægrar starfsemi (sjá kafla 7.4.11).

b) Við meðferð persónuupplýsinga fer VÍR að lögum nr. 77/2000, um persónuvernd og meðferð persónuupplýsinga [3].

c) VÍR gerir viðeigandi tæknilegar og skipulagslegar ráðstafanir til að hindra óheimila eða ólöglega vinnslu persónuupplýsinga og gegn glötun eyðileggingu eða skemmd á persónuupplýsingum.

d) Upplýsingar sem áskrifendur leggja fram til VÍR eru varðveittar þannig að þær verði ekki birtar nema með samþykki notandans, með dómsúrskurði eða með öðrum heimildum skv. lögum.

7.4.11 Skráning upplýsinga

VÍR tryggir að allar viðkomandi upplýsingar varðandi vottunarþjónustu (þar með talið skráningarupplýsingar og upplýsingar varðandi atburði í umhverfi, lyklaumsjón og skilríkjaumsjón) séu skráðar og varðveittar yfir viðeigandi tímabil, sérstaklega í þeim tilgangi að geta fært sönnur á vottun í málarekstri.

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

Almennar kröfur

VÍR tryggir eftirfarandi við varðveislu og skráningu upplýsinga:

a) Trúnað og heilleika bæði virkra og safnvistaðra skráa tengdum skilríkjum.

b) Skrár tengdar skilríkjum eru safnvistaðar í heild sinni og undir trúnaði í samræmi við viðurkenndar viðskiptavenjur.

c) Skrár varðandi skilríki eru gerðar tiltækar ef þess er krafist til að veita sönnun á vottun í málarekstri fyrir dómstólum. Vottorðshafi, og áskrifandi skilríkja innan þeirra marka sem ákvarðast af kröfum um vernd persónuupplýsinga (sjá kafla 7.4.10), hafa aðgang að skráningarupplýsingum og öðrum upplýsingum sem varða vottorðshafann.

d) Nákvæm tímasetning, mikilvægra atburða hjá vottunarstöðinni varðandi umhverfi, lyklaumsjón og skilríkjaumsjón, er skráð.

e) Skjöl sem varða skilríki eru varðveitt yfir viðeigandi tímabil svo unnt sé að veita sannanir til að styðja rafrænar undirskriftir í samræmi við viðeigandi lög. Þetta tímabil er tilgreint í skilmálum og skilyrðum í samningum (sjá kafla 7.4.10).

f) Atburðir eru skráðir þannig að torvelt verði að eyða skráningunni eða eyðileggja innan þess tímabils sem varðveita skal skráninguna.

g) Tilgreiningu á því hvaða atburði skuli skrá í atburðaskrá og hvernig.

Skráning

h) VÍR sér til þess að þeir atburðir sem tengjast skráningu, þar með talið beiðni um endurnýjun skilríkja eða framlengingu á gildistíma þeirra, séu skráðir.

i) VÍR sér til þess að allar skráningarupplýsingar, þar með taldar eftirfarandi, séu skráðar:

   i. Tegund þeirra skjala sem áskrifandi leggur fram til að styðja skráningu.

   ii. Skráning á einræðum kennigögnum, tölum eða samsetningu á því (t.d. númer ökuskírteinis) á auðkenningarskjölum, ef við á.

iii. Geymslustaður afrita af umsóknum og auðkenningarskjölum, þar með talið undirritað samkomulag við áskrifanda (sjá kafla 7.3.1).

iv. Öll sérákvæði í samkomulagi við áskrifanda (til dæmis samþykki fyrir birtingu skilríkja og annarra upplýsinga, sjá kafla 7.3.1).

v. Auðkenni þess aðila sem samþykkir umsókn.

vi. Aðferð sem notuð er til að staðfesta gildi auðkenningarskjala, ef við á.

vii. Nafn vottunarstöðvar sem tekur á móti upplýsingum eða skráningarstöð sem sendir þær, ef við á.

j) VÍR skráir alla atburði sem tengjast lífsskeiði eigin einkalykla.

Framleiðsla skilríkja

k) VÍR skráir alla atburði sem tengjast lífsskeiði eigin einkalykla.

l) VÍR skráir alla atburði sem tengjast lífsskeiði skilríkja.

Afhending búnaðar vottorðshafa

m) VÍR skráir alla atburði sem tengjast lífsskeiði lykla í umsjón þess, þar með talið allra lykla vottorðshafa sem framleiddir eru af vottunarstöðinni.

n) VÍR skráir alla atburði sem tengjast frágangi á öruggum notendabúnaði, ef við á.

Afturköllunarþjónusta

o) VÍR skráir allar beiðnir og skýrslur um afturköllun, sem og aðgerðir í kjölfarið.

7.5 Skipulag

VÍR sér til þess að starfsemi vottunarstöðvarinnar sé áreiðanleg.

VÍR mun sérstaklega uppfylla eftirfarandi kröfur:

Almennar kröfur

VÍR uppfyllir eftirfarandi skilyrði m.a. svo starfsemi vottunarstöðvarinnar sé áreiðanleg.

a) Vinnur eftir óhlutdrægum stefnureglum og verklagi.

b) Býður þjónustu sína öllum umsækjendum með þarfir sem samræmast yfirlýstu starfssviði hennar.

c) Er skráður lögaðili.

d) Hefur nægjanlegar tryggingar vegna skaðabótakrafna vegna starfseminnar og/eða athafna.

e) Hefur styrk og fjárhagslegan stöðugleika til að starfa í samræmi við þessa vottunarstefnu.

f) Sér til þess að til séu reglur og verkferlar til að leysa úr kvörtunum sem berast og deilum sem koma upp við viðskiptavini eða aðra aðila um veitingu á vottunarþjónustu eða vegna annarra skyldra mála.

g) skjalfestir með viðeigandi hætti það samkomulag eða þá samninga sem byggt er á í þeim tilvikum þegar þjónustan þarf undirverktaka, útvistunararaðila eða aðra ytri aðila.

Framleiðsla skilríkja, afturköllunarþjónusta

h) Sá hluti VÍR sem sér um framleiðslu skilríkja og afturköllunarþjónustu er óháður öðrum skipulagsheildum hvað varðar ákvarðanir VÍR sem tengjast stofnun, veitingu, viðhald og lokun á þjónustu í samræmi við vottunarstefnu þessa. Stjórnendur, hærra settir starfsmenn og starfsmenn í trúnaðarstörfum eru lausir við hvaða hagsmuni sem varða viðskipti, fjárhag eða aðra þá hagsmuni sem gæti haft óhagstæð áhrif á traust á þeirri þjónustu sem VÍR veitir.

i) Sá hluti VÍR sem sér um framleiðslu skilríkja og afturköllunarþjónustu hefur skjalfest skipulag sem tryggir óhlutdrægni í rekstri.