YFIRLÝSING AUÐKENNIS UM FRAMKVÆMD VOTTUNAR FYRIR FULLGILD RAFRÆN SKILRÍKI GEFIN ÚT UNDIR FULLGILDU AUÐKENNI

Lýsing á framkvæmd vottunar
við útgáfu fullgildra endaskilríkja
hjá vottunarstöð Fullgilds auðkennis

Útgáfa 02-00-00
4. janúar 2012

Breytingasaga

Útgáfudagur	Útgáfa	Lýsing	Ábyrgðaraðili
4.01.2012	02-00-00	Útgáfa 2.0 gefin út.	HAB

Efnisyfirlit

Réttindi

Auðkenni á öll réttindi varðandi þessa yfirlýsingu um framkvæmd vottunar.

Formáli

Þetta skjal er yfirlýsing um framkvæmd vottunar hjá Auðkenni sem lýsir því hvernig vottunarstöð Fullgilds auðkennis uppfyllir kröfur sem tilgreindar eru í *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8].

Í skjalinu eru tilgreindar kröfur til fullgildra skilríkja sem gefin eru út til almennings. Sömu kröfur eru gerðar til skilríkja sem ætluð eru til auðkenningar og skilríkja sem ætluð eru til undirritunar með öruggum undirskriftarbúnaði en mismunandi notkunarskilmálar eru tilgreindir í skilríkjunum.

Skjal þetta lýsir framkvæmd við útgáfu endaskilríkja hjá vottunarstöð Fullgilds auðkennis, undir skipulagi Íslandsrótar. Vottunarstöð Fullgilds auðkennis verður hér eftir nefnd vottunarstöðin. Upplýsingar um útgáfu rafrænna skilríkja hjá Auðkenni má fá á audkenni.is og almennar upplýsingar um rafræn skilríki má nálgast á www.skilriki.is. Athugasemdir og ábendingar vegna skjalsins má senda til Auðkennis á netfangið audkenni@audkenni.is.

Yfirlit

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 vottunarstöðin fer að því að uppfylla kröfurnar.

1 Gildissvið

Þetta skjal byggir á *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8] og lýsir framkvæmd vottunar hjá vottunarstöðinni við útgáfu fullgildra rafrænna skilríkja til einstaklinga; bæði einkaskilríkja og starfsskilríkja. Fullgild skilríki uppfylla kröfur um fullgild vottorð í skilningi laga um rafrænar undirskriftir nr. 28/2001 [1].

Á vegum Evrópusambandsins hafa niðurstöður vinnustofa á vegum CEN (CEN Workshop Agreements, CWA) verið staðfestar sem fullnægjandi kröfur fyrir útgáfu fullgildra rafrænna skilríkja, sbr. ákvörðun 2003/511/EC. Af þeim sökum er horft til skjalanna CWA 14169, CWA 14167-1 og CWA 14167-2 auk viðeigandi ETSI staðla við samningu þessa skjals. Þetta skjal lýsir framkvæmd vottunar hjá vottunarstöðinni sem uppfyllir lagalegar kröfur og tæknilegar stefnureglur sem Vottunarstefna Íslandsrótar setur vegna útgáfu fullgildra endaskilríkja undir Íslandsrót. Kröfur Íslandsrótar eiga að tryggja öryggi Íslandsrótar og fullvissa notendur og þá sem reiða sig á milliskilríkin að þeir geti treyst þeim.

2 Tilvísanir

Eftirfarandi skjöl innhalda ákvæði sem, að því leyti sem vísað er til í þessu skjali, mynda ákvæði þess.

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

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

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

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

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

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

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

[8] *Vottunarstefna Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni*, útgáfa 01-00-00. Auðkenni, 28. ágúst 2008.

[9] *Stefnumarkandi kröfur fyrir ISRS skilríki í rafrænni þjónustu: Kröfur til vottunarstöðva sem gefa út dreifilyklaskilríki*, útgáfa 1.0. Samstarfshópur fjármálaráðuneytisins og Auðkennis, 5. maí 2008.

[10] *Öryggishandbók Auðkennis: Skipulag og stjórnun öryggismála Auðkennis*, útgáfa 1.2. Auðkenni, 14. júlí 2009.

[11] *Almennir skilmálar fyrir skilríki gefin út undir Fullgildu auðkenni*, útgáfa 1.0. Auðkenni, 15. nóvember 2011

[12] *Afturköllun skilríkja og afturköllunarmiðlun hjá Fullgildu auðkenni*, útgáfa 1.0. Auðkenni, 11. nóvember 2011.

[13] *Skráningarþjónusta hjá Fullgildu Auðkenni*, útgáfa 1.0. Auðkenni, 11. nóvember 2011.

[14] *Framleiðsla skilríkja hjá Fullgildu Auðkenni*, útgáfa 1.0. Auðkenni, 11. nóvember 2011.

[15] *Samningur um skráningarstöð Auðkennis – vegna útgáfu rafrænna skilríkja undir milliskilríki Auðkennis*, útgáfa 1.0. Auðkenni, júlí 2008.

Ef misræmi er í þessum gögnum þá gilda þær kröfur til vottunarstöðva sem skilgreindar eru í þessu skjali.

3 Skilgreiningar, skammstafanir og táknun

3.1 Skilgreiningar

Eftirfarandi orðskýringar eiga við í þessu skjali. Samsvarandi orð á ensku eru skáletruð í 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.

Dreifilyklaveldi (*PKI domain*): Safn óháðra þátta (þar með talið vottunarstöðvar, skráningarstöðvar, virkir notendur í dreifilyklaskipulagi o.fl.) sem starfa í samræmi við stefnumarkandi kröfur fyrir rafræn skilríki sem tilgreindar eru af þeirri reglustjórn sem tengist dreifilyklaskipulaginu.

Dulmálseining (*cryptographic module*): Vélbúnaðareining sem meðal annars framleiðir og varðveitir lykla og notar rafræna undirskrift. Dulmálseining er sérstakt tilvik af varbúnaði sem ætlaður er fyrir framleiðslu, varðveislu og notkun einkalykla í dreifilyklaskipulagi.

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

Eigindaskilríki (*attribute certificate*): Gagnaskipan sem inniheldur safn af eigindum fyrir endanotanda og aðrar upplýsingar, dulritað með einkalykli vottunarstöðvarinnar sem gaf skilríkin út.

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

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

Einkaskilríki: (*private certificate*) Persónuleg rafræn skilríki einstaklinga. Einkaskilríki staðfesta að áskrifandi skilríkja sé sá sem skilríkin tilgreina. Í einkaskilríkjum er áskrifandi skilríkja og vottorðshafi sami aðilinn.

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 [1] 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*): Milliskilríki eru undirskilríki sem gefin eru út af tryggilegri rót eða af öðru milliskilríki í þeim tilgangi að gefa út önnur milliskilríki eða endaskilríki. Milliskilríki liggja á milli endaskilríkja og rótarskilríkja í traustaslóð skilríkja. Endaskilríki, milliskilríki og rótarskilríki mynda þannig skilríkjakeðju sem treystandi kannar þegar hann staðfestir það traust sem hann getur borið til endaskilríkja.

Móttakandi skilríkja (*certificate recipient*): Sá sem tekur á móti skilríkjum í rafrænum samskiptum og getur þurft að staðfesta 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.

OCSP samskiptaháttur (*Online Certificate Status Protocol*): Samskiptaháttur til að kalla eftir upplýsingum um stöðu skilríkja yfir nettengingar.

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“.

PIN-lausnarlykill (*PIN unblocking key*): Lykill, oftast númer eða textastrengur, sem veitir aðgang að öruggum búnaði, til dæmis símakorti, greiðslukorti eða snjallkorti, þrátt fyrir að aðgangi með PIN-númeri hafi verið lokað. Stundum kallað „PUK-númer“.

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.

Reglustjórn (*policy authority*): Stofnun eða nefnd sem velur eða þróar vottunarstefnu og heldur henni við.

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

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”.

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

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.

Starfsskilríki: Skilríki starfsmanna fyrirtækja og stofnana. Starfsskilríki staðfesta að vottorðshafi sé sá sem skilríkin tilgreina og að skilríkin séu tengd þeim lögaðila sem kemur fram í skilríkjunum. Í starfsskilríkjum er lögaðilinn, t.d. fyrirtæki eða stofnun, áskrifandi skilríkjanna og starfsmaðurinn vottorðshafi.

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.

Virkjunargögn (*activation data*): Gagnagildi, önnur en lyklar, sem þarf til að nota dulmálsbúnað. Virkjunargögn þarf að vernda. Virkjunargögn eru t.d. lykilorð (notkunarlykilorð), PIN, lyklahluti eða lífkenni.

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 [1] 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 [1]. Öruggur undirskriftarbúnaður er sérstakt tilvik af öruggum notendabúnaði sem ætlaður er fyrir rafrænar undirskriftir.

3.2 Skammstafanir

CP Vottunarstefna (***C**ertificate **P**olicy*).

CPS Yfirlýsing um framkvæmd vottunar (***C**ertification **P**ractice **S**tatement*).

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

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

ISRS **Ís**lensk **r**afræn **s**kilríki - skilríki í rafrænni þjónustu sem uppfylla kröfur þessa skjals.

OCSP OCSP samskiptaháttur (IETF RFC). OCSP er notað til að kalla eftir upplýsingum um stöðu skilríkja yfir nettengingar (***O**nline **C**ertificate **S**tatus **P**rotocol*).

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

PKI Dreifilyklaskipulag (***P**ublic **K**ey **I**nfrastructure*).

PUK PIN-lausnarlykill (***P**IN **U**nblocking **K**ey*).

4 Almenn hugtök

Meginflokkar rafrænna skilríkja í dreifilyklaskipulagi eru rótarskilríki, milliskilríki og endaskilríki. 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 endaskilríki til almennings og lögaðila.

Fjallað er um almenn hugtök í kafla 4 í *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8].

4.1 Vottunarstöð

Fjallað er um hugtakið „vottunarstöð“ í kafla 4.1 í *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8].

4.2 Vottunarþjónusta

Í þessu skjali er starfsemi vottunarstöðvar skipt í eftirfarandi þætti:

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 Yfirlýsing um framkvæmd vottunar

Fjallað er um mismunandi tilgang og útfærslu á vottunarstefnu annars vegar og yfirlýsingu um framkvæmd vottunar hins vegar í kafla 4.3 í *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8].

4.4 Áskrifandi og vottorðshafi

Í þessu skjali er gerður greinarmunur á hlutverki áskrifanda, sem gerir samning við vottunarstöðina um útgáfu skilríkja, og hlutverki vottorðshafa sem skilríkin auðkenna. Fjallað er um mismun á áskrifanda og vottorðshafa í kafla 4.3 í *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8].

5 Almennt um vottunarkröfur

5.1 Yfirlit

Í þessu skjali er lýsing á framkvæmd vottunarstöðvarinnar við vottun vegna útgáfu á fullgildum rafrænum skilríkjum gefnum út undir milliskilríkinu Fullgilt auðkenni.

5.2 Auðkenning

Þessi yfirlýsing um framkvæmd vottunar er auðkennd með kennimarki viðfangs (e. object identifier: OID). Auðkenni hefur fengið úthlutað númeri frá Póst- og fjarskiptastofnun undir viðurkenndum og skráðum landaboga fyrir Ísland í samræmi við *Lýsingu á starfsemi skráningarstöðvar* [3]. Kennimark þessa skjals er: {2 16 352 1 2 1 1 5 1}.

{joint-iso-itu-t(2) country(16) is(352) companies-organizations-and-institutes(1) audkenni(2) pki(1) public-pki(1) cps-fa(5) version(1)}

Þessi yfirlýsing um framkvæmd vottunar uppfyllir kröfur í *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8] sem er með kennimark viðfangs {2 16 352 1 2 1 1 1 1}.

5.3 Notkunarsvið og nothæfi

Í samræmi við *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8] lýsir þetta skjal útgáfu vottunarstöðvarinnar á fullgildum skilríkjum sem uppfylla eftirfarandi kröfur:

a) Skilríkin uppfylla 7. gr. laga um rafrænar undirskriftir nr. 28/2001 [1] og II. kafla reglugerðar nr. 780/2011 um rafrænar undirskriftir.

Töluliðir 7. gr.	**Aðferð vottunarstöðvarinnar**
1. tl., sbr. 3. gr. reglugerðar.	Í skilríkjunum er læsilegur eftirfarandi texti: „This certificate is intended for signing. This certificate is issued as a qualified certificate in accordance with act 28/2001 and Directive 99/93/EC.“ Í reglugerð nr. 780/2011 um rafrænar undirskriftir er til viðbótar gerð krafa um að í skilríkjunum beri að hafa læsilegt orðið fullgilt, sbr. 2. mgr. 3. gr. Þar er jafnframt tilgreint í 3. mgr. að skilríki „teljast fullnægja kröfum þessarar greinar, uppfylli þau skilyrði staðla og annarra samþykktra kröfuskjala, sem talin eru upp í viðauka I“. Í viðauka I er um innihald fullgildra vottorða vísað á ETSI TS 101 862 sem er grunnurinn að baki skjalsins *Innihald rafrænna skilríkja: Samræmt innihald rafrænna skilríkja sem gefin eru út á Íslandi* [4]. Innihaldsskjal þetta er fyrirmynd allrar skilríkjaútgáfu vottunarstöðvarinnar.
2. tl.	Í skilríkjunum eru eftirfarandi upplýsingar um Auðkenni og vottunarstöðina tilgreindar í svæði útgefanda (issuer): CN = Fullgilt audkenni OU = Utgefandi fullgildra skilrikja O = Audkenni hf. SERIALNUMBER = 5210002790 C = IS
3. tl., sbr. 4. gr. reglugerðar.	Í skilríkjunum eru eftirfarandi upplýsingar um skilríkjahafa í svæði undirritanda (subject): CN = [Nafn eins og það kemur fyrir í þjóðskrá] SERIALNUMBER = [kennitala skilríkjahafa]:[kennitala áskrifanda] C = IS Ef skilríki er starfsskilríki er kennitala áskrifanda önnur en kennitala skilríkjahafa, oftast er áskrifandinn þá fyrirtæki sem skilríkjahafinn vinnur hjá. Fullt nafn skilríkjahafa eru tekin beint úr þjóðskrá og því eru ekki notuð dulnefni í skilríkjum vottunarstöðvarinnar.
4. tl.	Í skilríkjunum koma fram upplýsingar um þær tegundir skilríkja sem vottunarstöðin gefur út: Auðkenning og undirritun. Eins er þar greint á milli einkaskilríkja og starfsskilríkja.
5. tl., sbr. 6. gr. reglugerðar.	Í skilríkjunum er dreifilykill sem tengdur er einkalykli sem er á forræði skilríkjahafa.
6. tl., sbr. 7. gr. reglugerðar.	Sérstök svæði eru í skilríkjunum sem tilgreina frá hvaða tíma þau gilda og hvenær þau renna úr gildi.
7. tl., sbr. 8. gr. reglugerðar.	Öll skilríki sem vottunarstöðin gefur út bera með sér einkvæman auðkenniskóta.
8. tl., sbr. 9. gr. reglugerðar.	Skilríkin eru undirrituð með einkalykli vottunarstöðvarinnar.
9. tl., sbr. 10. gr.	Í skilríkjunum eru engar takmarkanir gerðar á gildissviði eða fjárhæð viðskipta sem

reglugerðar.	unnt er að nota vottorðið til.

b) Vottunarstöðin uppfyllir kröfur V. kafla í lögum um rafræna undirskriftir nr. 28/2001 [1].

Greinar í V. kafla	**Aðferð vottunarstöðvarinnar**
10. gr.	Vottunarstöðin uppfyllir kröfur laganna til starfseminnar með því að innleiða og fylgja skilvirku stjórnkerfi upplýsingaöryggis sem lýst er í *Öryggishandbók Auðkennis* [10]. Þar má meðal annars finna yfirlit yfir þær stjórnunar- og starfsaðferðir sem fylgt er við framleiðslu, afhendingu og umsýslu með fullgildum rafrænum skilríkjum og þjálfunaráætlun Auðkennis. Nægilegt fjármagn til starfsemi vottunarstöðvarinnar er sótt í gegnum gjaldskrá félagsins en að baki Auðkenni standa jafnframt traust og öflug og fjárhagslega burðug félög.
11. gr.	Vísað er til c) liðar hér fyrir neðan til þess að svara því hvernig vottunarstöðin uppfyllir kröfur laganna til kerfis og búnaðar.
12. gr.	Um skráningar- og afturköllunarþjónustu vottunarstöðvarinnar er fjallað í eftirfarandi skjölum: *Skráningarþjónusta hjá Fullgildu auðkenni* [13] og *Afturköllun skilríkja og afturköllunarmiðlun hjá Fullgildu auðkenni* [12], sbr. og nánari umfjöllun í kafla 7.3.
13. gr.	Lýsingu á því hvernig kennsl eru borin á skilríkjahafa má finna í skjalinu *Skráningarþjónusta hjá Fullgildu auðkenni* [13], sbr. og umfjöllun í kafla 7.3.1.
14. gr.	Lýsingu á varðveislu upplýsinga hjá vottunarstöðinni má finna í kafla 7.
15. gr.	Skilmálar við notkun skilríkjanna eru tilgreindir í áskriftarsamningum og skráningarfulltrúum ber að upplýsa skilríkjahafa um innihald þeirra við afhendingu skilríkjanna. Sama gildir um upplýsingar um meðferð kvartana og úrlausn deilumála. Áskriftarsamningarnir eru aðgengilegir á netinu og eru sendir til kynningar hverjum þeim sem óskar eftir því. Vottunarstöðin rekur engin valfrjáls faggildingarkerfi.

c) Skilríkin eru eingöngu ætluð fyrir notkun með öruggum undirskriftarbúnaði sem uppfyllir kröfur í 8. gr. laga um rafræna undirskriftir nr. 28/2001 [1].

Skilríkin sem vottunarstöðin gefur út og einkalyklar vottorðshafa, eru ávallt varðveitt á örgjörvum sem hafa staðist EAL4+ eða sambærilega vottun. Búnaðurinn er ávallt keyptur frá traustum og öruggum aðilum og hefur verið tekinn út og staðfestur meðal annars af Visa International og MasterCard bæði hvað varðar örgjörva og stýrikerfi í þeirri samsetningu sem Auðkenni notar.

d) Skilríkin eru gefin út til almennings.

Skilríki vottunarstöðvarinnar eru gefin út til allra sem þess óska og skráðir eru með kennitölu í þjóðskrá. Engar aðrar takmarkanir eru á því hverjir geta orðið skilríkjahafar en misjafnt getur verið hvernig skilríkin eru afhent þessum aðilum.

Skilríki sem gefin eru út í samræmi við *Vottunarstefnu Auðkennis fyrir fullgild skilríki gefin út undir Fullgildu auðkenni* [8], má nota til rafrænnar undirskriftar sem uppfyllir lagakröfur um undirskrift í tengslum við rafræn gögn á sama hátt og eiginhandarundirskrift uppfyllir lagakröfur í tengslum við pappírsgögn, sbr. 1. mgr. 4. gr. laga 28/2001 um rafrænar undirskriftir [1].

5.4 Samræmi

5.4.1 Yfirlýsing um samræmi

Framkvæmd vottunar hjá vottunarstöðinni við útgáfu, dreifingu, birtingu og afturköllun rafrænna skilríkja sem lýst er í þessu skjali er í samræmi við kröfur í *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir*

Fullgildu auðkenni [8] og uppfyllir öll skilyrði sem gerð eru til fullgildra rafrænna skilríkja í lögum um rafrænar undirskriftir nr. 28/2001 [1] og í *Stefnumarkandi kröfum fyrir ISRS skilríki í rafrænni þjónustu* [9].

Starfsemi vottunarstöðvar Fullgilds auðkennis hefur verið tilkynnt til Neytendastofu sem hefur eftirlit með starfsemi vottunarstöðvarinnar sbr. lög um rafrænar undirskriftir nr. 28/2001 [1].

Reglulega lætur Auðkenni til þess bæra aðila gera úttektir sem sýna fram á að útgáfa vottunarstöðvarinnar á rafrænum skilríkjum gefnum út undir Fullgildu auðkenni sé í samræmi við *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8]. Niðurstöður úttekta eru aðgengilegar áskrifendum og hagsmunaðilum á vefsetri Auðkennis. Vottunarstöðin mun þó ekki birta opinberlega upplýsingar sem geta stofnað öryggi kerfa vottunarstöðvarinnar í hættu.

5.4.2 Kröfur um samræmi

Í köflum 6.1 og 7 verður sýnt fram á það með hvaða hætti vottunarstöðin uppfyllir skyldur sínar samkvæmt kafla 6.1 í *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8] og hefur innleitt stýringar sem uppfylla kröfurnar, þar með talið þá valkosti sem eiga við í þeim reglum sem innleiddar eru, eins og tilgreint er í kafla 7.

6 Skyldur og skuldbindingar

6.1 Skyldur vottunarstöðvarinnar

Vottunarstöðin hefur innleitt stjórnkerfi upplýsingaöryggis sem tekur mið af ISO 27001 staðlinum [7] og sem samræmist kröfum í *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8] um framkvæmd, stjórnun og rekstur vottunarstöðvarinnar. Stjórnkerfi upplýsingaöryggisins samastendur af *Öryggishandbók Auðkennis* [10] og færsluskrám og vísar í önnur skjöl sem uppfylla stefnu Auðkennis um upplýsingaöryggi. Vottunarstöðin ber ábyrgð á samræmi við vottunarstefnuna jafnvel að því marki sem vottunarstöðin hefur kosið að fela undirverktökum hluta starfseminnar.

Þessi lýsing á framkvæmd vottunar hjá vottunarstöðinni er í samræmi við *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8] og styður vottunarstöðina í því að uppfylla allar skyldur sínar.

6.2 Skyldur áskrifenda

Auðkenni gerir samninga við áskrifendur skilríkja fyrir vottunarstöðina. Samningarnir innihalda m.a. þær kröfur sem eru settar fram í kafla 6.2, 7.3.1 og 7.3.4 í *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8]. Auk þess setur vottunarstöðin fram almenna skilmála. Umrædd skjöl eru birt á vef Auðkennis, www.audkenni.is og auk þess á vefsvæðinu islandsrot.is. Sé misræmi í skjölum eftir staðsetningum gildir sú útgáfa sem birt er á audkenni.is.

6.3 Upplýsingar fyrir treystendur

Upplýsingar fyrir treystendur má finna á vef Auðkennis og skilriki.is. Á vef Auðkennis og vef Íslandsrótar, www.islandsrot.is, eru birtir *Almennir skilmálar fyrir skilríki gefin út undir Fullgildu auðkenni* [11] sem innihalda m.a. skilmála og skilyrði vottunarstöðvarinnar gagnvart treystendum.

6.4 Skuldbindingar

Upplýsingar um ábyrgð og skuldbindingar vottunarstöðvarinnar gagnvart áskrifendum og treystendum er að finna í *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8] auk almennra skilmála og áskriftarsamninga vottunarstöðvarinnar sem aðgengilegir eru á vef Auðkennis.

7 Lýsing á framkvæmd vottunarstöðvarinnar

Vottunarstöðin hefur byggt upp stjórnkerfi upplýsingaöryggis sem tekur mið af ISO 27001 [7].

7.1 Yfirlýsing um framkvæmd vottunar

Auðkenni ber ábyrgð á starfssemi vottunarstöðvarinnar og hefur gert ráðstafanir til þess að tryggja samfelldan rekstur hennar.

Yfirlýsing þessi er aðgengileg áskrifendum og treystendum skilríkja gefnum út undir Fullgildu auðkenni á vefsíðu Auðkennis til þess að unnt sé að meta samræmi vottunarframkvæmdarinnar við vottunarstefnuna. Auk þess er birt á vef Auðkennis skilmálar og skilyrði sem varða notkun fullgildra skilríkja gefnum út undir Fullgildu auðkenni.

Þessi framkvæmdarlýsing er samþykkt og henni viðhaldið af vottunarstöðinni. Auðkenni ber ábyrgð á því að framkvæmd vottunar hjá vottunarstöðinni sé á öllum tímum í samræmi við *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8]. Tilkynnt er um nýjar útgáfur af skjali þessu á vef Auðkennis, www.audkenni.is.

Vottunarstöðin hefur skilgreint úttektarferli fyrir framkvæmd vottunar sem nánar er lýst í verklagsreglum *Öryggishandbókar Auðkennis* [10].

7.2 Dreifilyklaskipulag - lífsskeið lyklaumsjónar

Meðhöndlun lykla hjá vottunarstöðinni tekur mið af ETSI TS 102 176-1 [6] sem inniheldur lista yfir viðurkennd dulmálsalgrím ásamt kröfum um færibreytur þeirra.

7.2.1 Framleiðsla einkalykla vottunarstöðvarinnar

Umhverfi fyrir framleiðslu einkalykla vottunarstöðvarinnar er raunlægt öruggt og stýrt undir öryggisstjórnkerfi Auðkennis sem lýst er í verklagsreglum *Öryggishandbókar Auðkennis* [10]. Þar eru skilgreindar sértækar kröfur um varðveislu eigna vottunarstöðvarinnar, stefnureglur í aðgangsstjórnun og almennar kröfur í stjórnun aðgangs og réttinda hjá vottunarstöðinni. Þar er einnig skilgreint verklag og útfærsla fyrir aðgangsstjórnun, þar á meðal ábyrgð, hlutverk og skipta stjórnun við framkvæmd aðgerða.

Nánari grein er gerð fyrir því hvernig vottunarstöðin framleiðir einkalykla sína á öruggan hátt í stýrðri lyklaathöfn í skjalinu *Framleiðsla skilríkja hjá Fullgildu auðkenni* [14]. Einkalyklar vottunarstöðvarinnar eru framleiddir og varðveittir í öruggri HSM dulmálseiningu sem er áreiðanlegt kerfi sem staðfest er að uppfylli að lágmarki EAL 4+ í samræmi við ISO/IEC 15408 [5].

Vottunarstöðin notar SHA-1 tætifallsalgrím og RSA dulmálsalgrím í framleiðslu og meðhöndlun lykla. Lengd undirskriftarlykils milliskilríkisins „Fullgilt auðkenni“ er 2048 bitar og lengd einkalykla endaskilríkja er 2048 bitar. Við val á lengd lykla er unnið eftir verklagsreglu um eftirlit með úreldingu tækniþátta. Tekið er mið af tækniforskrift í skjalinu ETSI TS 102 176-1 [6].

Gildistími milliskilríkisins „Fullgilt auðkenni“ er 15 ár. Auðkenni mun framleiða nýtt lyklapar tímanlega áður en gildistímanum lýkur þannig að ekki verði truflun á starfssemi þeirra sem treysta á undirskriftarlykilinn eins og nánar er skilgreint í verklagsreglu um endurnýjun milliskilríkis, undirbúning og tímamörk. Gildistími endaskilríkja gefnum út undir Fullgilt auðkenni er allt að 5 ár.

7.2.2 Geymsla, öryggisafritun og endurheimt lykla hjá vottunarstöðvum

Einkalyklar vottunarstöðvarinnar eru varðveittir í öruggri HSM dulmálseiningu (e. hardware security module) sem er sérhannaður til að tryggja heilleika og öryggi gagna og er áreiðanlegt kerfi sem staðfest er að uppfylli EAL 4+ í samræmi við ISO/IEC 15408 [5].

Samrit einkalykla vottunarstöðvarinnar tryggir endurheimt á einkalykli. Öll meðhöndlun á skilríki og einkalyklum vottunarstöðvarinnar til undirritunar fer fram í raunlægt öruggu umhverfi sem uppfyllir verklagsreglur öryggisstjórnkerfis Auðkennis. Beitt er sambærilegum stýringum fyrir öll samrit.

Sérstakar ráðstafanir eru gerðar í aðgangsstýringum, m.a. með tvískiptri stjórnun, til að koma í veg fyrir að einkalyklar vottunarstöðvarinnar séu aðgengilegir utan öruggs vélbúnaðar eins og nánar er lýst í skjalinu *Framleiðsla skilríkja hjá Fullgildu auðkenni* [14]. Fjöldi þeirra einstaklinga sem hafa heimild til að framkvæma þessar aðgerðir er haldið í lágmarki.

7.2.3 Dreifing vottunarstöðva á dreifilyklum

Dreifilykill vottunarstöðvarinnar sem notaður er til að sannvotta undirskrift vottunarstöðvarinnar á endaskilríkjum er aðgengilegur á vef Auðkennis, www. audkenni.is. Jafnframt er dreifilyklinum dreift með endaskilríkjunum. Undirskrift með einkalykli Íslandsrótar á samsettum dreifilyklinum og meðfylgjandi rafrænu skilríki, vottar heilleika dreifilykilsins og tengingu hans við einkalykil vottunarstöðvarinnar.

7.2.4 Vörsluafrit lykla

Vottunarstöðin varðveitir vörsluafrit sinna eigin einkalykla, sbr. kafla 7.2.2, en hvorki einkalykla vottorðshafa né annarra utanaðkomandi aðila.

7.2.5 Notkun á einkalykli vottunarstöðvarinnar

Vottunarstöðin notar einkalykla sína eingöngu til þess að undirrita skilríki og stöðuupplýsingar um skilríki og tryggir rétta notkun með tvískiptri stjórnun við skráningu aðgerða sem heimilaðar hafa verið.

Undirskriftarlyklar skilríkja vottunarstöðvarinnar eru eingöngu notaðir í raunlægt (e. physically) öruggum húsakynnum sem uppfylla kröfur verklagsreglna í öryggisstjórnkerfi Auðkennis.

7.2.6 Endalok lífsskeiðs einkalykla vottunarstöðvarinnar

Allir einkalyklar Auðkennis sem notaðir eru til undirritunar á skilríkjum og hafa sama gildistíma, notast við sömu algrími og eru af sömu lengd, sem tilgreind er í kafla 7.2.1.

Eftir að gildistími einkalykla vottunarstöðvarinnar lýkur mun vottunarstöðin eyðileggja öll eintök lyklanna með því að eyða rafrænum gögnum á dulmálsvélbúnaði sem hýsir einkalyklana og endursetja geymslumiðla vélbúnaðarins með viðurkenndum frumstillingaraðferðum þannig að ekki verði mögulegt að nota eða uppgötva einkalyklana. Nánar er fjallað um eyðingu einkalykla vottunarstöðva hjá Auðkenni í verklagsreglum *Öryggishandbókar Auðkennis* [10].

7.2.7 Umsjón dulmálsvélbúnaðar fyrir undirritun skilríkja á lífsskeiði hans

Vottunarstöðin viðhefur stjórnkerfi upplýsingaöryggis sem tryggir rétta virkni, örugga meðhöndlun og varðveislu dulmálsvélbúnaðar fyrir undirritun skilríkja og stöðuupplýsinga á lífsskeiði hans. Þetta stjórnkerfi upplýsingaöryggis er skjalfest í verklagsreglum *Öryggishandbókar Auðkennis* [10]. Öll meðferð á undirskriftarlyklum í dulmálsvélbúnaði er í samstilltri stjórn að minnsta kosti tveggja einstaklinga sem hafa hvor sitt trúnaðarhlutverk hjá vottunarstöðinni, eins og nánar er lýst í skjalinu *Framleiðsla skilríkja hjá Fullgildu auðkenni* [14]. Sama gildir um kröfur til búnaðar og lýsingu á dulmálsvélbúnaði vottunarstöðvarinnar.

Ef dulmálsvélbúnaður er tekinn varanlega úr notkun er undirskriftarlyklum eytt og búnaðurinn eyðilagður í ígildi lyklaathafnar þar sem vélbúnaðurinn er annað hvort tættur eða frumstilltur með aðferðum sem veita jafnmikið öryggi gagnvart undirskriftarlyklum og tæting.

7.2.8 Umsjón vottunarstöðva með lyklum vottorðshafa

Þegar vottunarstöðin framleiðir lykla vottorðshafa tryggir vottunarstöðin að leynd sé yfir einkalyklum og að lyklar séu framleiddir á öruggan hátt með notkun SHA-1 tætifallsalgríms og RSA dulmálsalgríms. Einkalyklar endaskilríkja sem gefin eru út undir milliskilríkinu Fullgilt auðkenni eru 2048 bitar að lengd og tekið er mið af tækniforskrift í skjalinu ETSI TS 102 176-1 [6]. Eftir framleiðslu er einkalyklum vottorðshafa komið fyrir á öruggum undirskriftarbúnaði sem samanstendur annars vegar af örgjörva sem vottaður er EAL 5+ í samræmi við ISO/IEC 15408 [5] og hins vegar stýrikerfi og sérsniðnum hugbúnaði fyrir dreifilyklameðhöndlun í öruggu umhverfi, sbr. nánari umfjöllun í *Framleiðslu skilríkja hjá Fullgildu auðkenni* [14].

Afrit af lyklum vottorðshafa er ekki varðveitt hjá vottunarstöðinni eftir að þeir eru afhentir vottorðshafa. Við afhendingu er þess gætt að trausti til lyklanna sé ekki stofnað í hættu. Eftir afhendingu til vottorðshafa mun einungis vottorðshafinn hafa aðgang að einkalyklinum.

7.2.9 Undirbúningur á öruggum undirskriftarbúnaði

Öruggur undirskriftarbúnaður kemur frágenginn frá framleiðanda búnaðarins ekki er því um virkjun eða óvirkjun hans að ræða. Meðhöndlun, varðveisla og dreifing á öruggum undirskriftarbúnaði hjá vottunarstöðinni er undir öruggu eftirliti öryggisstjórnkerfis Auðkennis, sem nánar er lýst í *Öryggishandbók Auðkennis* [10]. Dreifingu á öruggum undirskriftarbúnaði og tengdum virkjunargögnum er lýst í *Skráningarþjónustu hjá Fullgildu auðkenni* [13]. Virkjunargögn (PUK númer, þ.e. PIN-lausnarlykill) eru útbúin með öruggum hætti. Þau eru tvískipt og þeim er dreift til skilríkjahafa eftir tveimur mismunandi leiðum, aðskilið frá lyklaparinu. PIN notkunaraðgangsorð myndast við framleiðslu skilríkjanna og er slembitala sem ekki er varðveitt hjá vottunarstöðinni. Við virkjun skilríkjanna er PIN-lausnarlykill notaður af vottorðshafa til að endursetja PIN notkunaraðgangsorðið.

7.3 Dreifilyklaskipulag - lífsskeið skilríkjaumsjónar

7.3.1 Skráning vottorðshafa

Vottunarstöðin sér til þess að áskrifandi skilríkja sé upplýstur um almenna skilmála og skilyrði áður en gerður er samningur við hann, meðal annars þá skyldu áskrifanda að upplýsa vottorðshafa um skyldur vottorðshafans. Viðeigandi áskriftarsamningar eru aðgengilegir á vef Auðkennis, www.audkenni.is.

Vottunarstöðin kannar gögn skilríkjahafa með viðeigandi hætti og tryggir að umsóknir um skilríki séu réttar, innihaldi þær upplýsingar sem krafist er og séu byggðar á gildu umboði þegar það á við eins og nánar er lýst í *Skráningarþjónustu hjá Fullgildu auðkenni* [13].

Vottunarstöðin staðfestir og skjalfestir auðkenni vottorðshafa og önnur eigindi hans með viðeigandi aðferðum um leið og skráning fer fram. Sama gildir um staðfestingu á samþykki vottorðshafa fyrir útgáfu á skilríki í tengslum við áskrifanda. Allar upplýsingar sem nauðsynlegar eru til að staðfesta auðkenni vottorðshafa og lögbærs fulltrúa áskrifanda eru skráðar í *Skráningarþjónustu hjá Fullgildu auðkenni* [13].

Vottunarstöðin varðveitir upplýsingar sem varða umsókn og skráningu, þar með talið upplýsingar sem áskrifandi lætur í té, þar til að liðnum 10 árum frá andláti áskrifanda. Vottunarstöðin mun við skráningarferlið og varðveislu upplýsinganna fylgja í hvívetna lögum um persónuvernd og meðferð persónuupplýsinga nr. 77/2000 [2].

Bankar og sparisjóðir gegna meðal annarra hlutverki skráningarstöðva og hafa undirgengist skyldur skráningarstöðva með undirritun *Samnings um skráningarstöð Auðkennis* [15].

7.3.2 Endurnýjun, uppfærsla og endurlyklun skilríkja

Þetta er ekki hluti af framkvæmd vottunar fyrir fullgild rafræn skilríki hjá vottunarstöðinni.

7.3.3 Framleiðsla skilríkja

Innihald skilríkja sem vottunarstöðin gefur út er í samræmi við 7. gr. laga um rafrænar undirskriftir [1] og skjalið *Innihald rafrænna skilríkja* [4], sbr. umfjöllun í kafla 5.3. Skilríkin eru varðveitt á öruggum undirskriftarbúnaði, sbr. kafla 7.2.9 og einkalykillinn er framleiddur í öruggu umhverfi, sbr. kafla 7.2.8.

Útgáfu skilríkja og undirbúningi öruggs undirskriftarbúnaðar er lýst í skjalinu *Framleiðsla skilríkja hjá Fullgildu auðkenni* [14]. Ekki er um endurnýjun, uppfærslu eða endurlyklun skilríkja að ræða hjá vottunarstöðinni.

Vottunarstöðin sér til þess að auðkennandi nafn (e. distinguished name) sem notað er í fullgildum rafrænum skilríkjum gefnum út hjá vottunarstöðinni verður aldrei notað til að auðkenna annan aðila með því að hafa einkvæmt raðnúmer hluta af auðkennandi nafni.

Verndun á trúnaði og heilleika skráningargagna sem verða til hjá vottunarstöðinni er hluti af öryggisstjórnkerfi Auðkennis. Auðkenni fylgir í hvívetna lögum um persónuvernd og meðferð persónuupplýsinga nr. 77/2000 [2].

Hluta af rekstri vottunarstöðvarinnar er útvistað. Skráningarstöðvar hafa undirgengist skyldur sínar með undirritun *Samnings um skráningarstöð Auðkennis* [15]. Staðfesting á auðkenni viðurkenndra skráningarfulltrúa skráningarstöðva í samskiptum við vottunarstöðina er með rafrænu skilríki.

7.3.4 Miðlun á skilmálum og skilyrðum

Vottunarstöðin leggur fram upplýsingar um skilmála og skilyrði fyrir áskrifendur og treystendur skilríkja á vef Auðkennis, www.audkenni.is. Þar eru meðal annars, auk yfirlýsingar þessarar, *Vottunarstefna Auðkennis fyrir*

fullgild rafræn skilríki gefin út undir Fullgildu auðkenni [8] og *Almennir skilmálar fyrir skilríki gefin út undir Fullgildu auðkenni* [11]. Skilmálarnir lýsa meðal annars lagaumhverfi vottunarstöðvarinnar, varðveislutíma persónuupplýsinga sem safnast hjá vottunarstöðinni og ferli vegna kvartana og úrlausn deilumála. Þar má einnig finna upplýsingar um hvernig skuli staðfesta gildi rafrænna skilríkja og hvernig vottunarstöðin hefur verið metin með hliðsjón af samræmi við *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni* [8].

Trygging á heilleika upplýsinga er hluti af öryggisstjórnkerfi Auðkennis sem lýst er í *Öryggishandbók Auðkennis* [10].

7.3.5 Miðlun skilríkja

Vottunarstöðin mun gera dreifilykla endaskilríkja aðgengilega fyrir almenning á vef Auðkennis, dreifilyklar.www.audkenni.is að því marki sem áskrifendur og vottorðshafar samþykkja slíka birtingu. Unnið er að tæknilegri útfærslu sem tryggir vernd persónuupplýsinga.

Skilríkin eru aðgengileg í heild sinni fyrir vottorðshafann á örgjörvum debetkorta.

Almennir skilmálar vottunarstöðvarinnar eru birtir á vef Auðkennis og jafnframt á vefnum islandsrot.is.

7.3.6 Afturköllun og tímabundin ógilding skilríkja

Verklagsreglur fyrir afturköllun á skilríkjum eru í skjalinu *Afturköllun skilríkja og afturköllunarmiðlun* [12].

Breytingar á upplýsingum um afturköllunarstöðu eru aðgengilegar innan 24 klst. frá því að tilkynning eða beiðni um afturköllun er móttekin hjá vottunarstöðinni og upplýsingarnar eru aðgengilegar þar til annað tveggja gerist, að stöðu skilríkjanna er breytt þannig að þau eiga ekki lengur að vera á afturköllunarlista eða að gildistími skilríkjanna rennur út. Tekið er á móti tilkynningum og beiðnum allan sólarhringinn í þjónustuveri Auðkennis og hjá útgefendum debetkorta.

Upplýsingar um afturkölluð skilríki sem vottunarstöðin hefur undirritað, eru gefnar út ekki sjaldnar en með 24 klst. millibili og eru aðgengilegar á vef Auðkennis, www.audkenni.is. Ef vefur Auðkennis verður ekki aðgengilegur mun Auðkenni tryggja að upplýsingar um stöðu skilríkja séu aðgengilegar aftur með öðrum hætti eins fljótt og auðið er frá því að Auðkenni fær vitneskju um tap á aðgengi. Afturköllunarþjónustan er rekin í tvöföldu kerfi í stýrðu umhverfi í aðskildum vélarsölum. Þjónustan er aðgengileg allan sólarhringinn allan ársins hring. Til þess að tryggja aðgengi að þjónustunni er hún vöktuð og brugðist er skjótt við áföllum. Nánar er fjallað um verklagsreglur stjórnkerfisins í *Öryggishandbók Auðkennis* [10].

Afturköllunarlisti fyrir skilríki sem vottunarstöðin hefur undirritað er aðgengilegur á eftirfarandi vefslóð:

http://crl.audkenni.is/fullgiltaudkenni/latest.crl.

Stöðuupplýsingar fyrir endaskilríki eru einnig aðgengilegar yfir nettenginu með OCSP samskiptahætti á slóðinni

http://ocsp.audkenni.is.

Stöðuupplýsingar sem Auðkenni veitir með OCSP samskiptahætti eru byggðar á rauntímaupplýsingum, upplýsingar í afturköllunarlistum (CRL) geta verið allt að 24 tíma gamlar.

Afturköllunarlistar sem vottunarstöðin gefur út og svör frá stöðumiðlunarþjónum vottunarstöðvarinnar eru undirrituð af einkalykli stöðvarinnar. Með því móti er heilleiki upplýsingana tryggður og staðfesta má uppruna þeirra.

7.4 Stjórnun og rekstur vottunarstöðva

7.4.1 Stjórnun upplýsingaöryggis

Auðkenni ber ábyrgð á öllum þáttum þeirrar vottunarþjónustu sem vottunarstöðin rekur. Ábyrgðin nær einnig til útvistaðrar starfsemi. Allir undirverktakar verða að undirgangast kröfur vottunarstöðvarinnar til upplýsingaöryggis og eru skyldugir til þess að útfæra allar kröfur sem gerðar eru til vottunarþjónustu. Þetta er framkvæmt með samningum þar sem kröfur Auðkennis til upplýsingaöryggis koma fram og eftirlit er haft með því að kröfunum sé fylgt.

Til þess að tryggja skilvirkni hefur Auðkenni komið á gæða- og öryggiskerfi í samræmi við alþjóðlega staðla fyrir gæðastjórnun og upplýsingaöryggi og þá vottunarþjónustu sem fyrirtækið veitir. Við gerð gæða- og öryggiskerfis hjá Auðkenni hefur verið stuðst við ISO 9001 og ISO 27001 staðlana. Öryggisráð Auðkennis sem skipað er starfsmönnum og stjórnendum hjá Auðkenni hefur umsjón með rekstri þess hluta stjórnkerfisins sem snýr að upplýsingaöryggi. Ráðið ber ábyrgð á því að skilgreina stefnu í upplýsingaöryggi og að dreifa henni til allra starfsmanna, ásamt því að viðhalda skriflegum verkferlum, verklýsingum og öðrum nauðsynlegum skjölum til þess að reka vottunarþjónustu Auðkennis á öruggan og hagkvæman hátt. Öryggisráð er jafnframt ábyrgt fyrir því að allar breytingar sem haft geta áhrif á öryggi vottunarþjónustunnar verði rýndar, samþykktar og unnar samkvæmt formlegu breytingastjórnunarferli.

Vottunarstöðin framkvæmir reglulega áhættumat til þess að meta áhættur sem stefnt geta rekstri stöðvarinnar í hættu. Vottunarstöðin hefur skilgreint hvað telst ásættanleg áhætta og gerir ráðstafanir til þess að meðhöndla áhættu sem talin er óásættanleg. Áhættumat vottunarstöðvarinnar er staðfest af öryggisráði og afgangsáhætta samþykkt af framkvæmdastjóra.

7.4.2 Flokkun og stjórnun verðmæta

Auðkenni viðheldur skrá yfir öll verðmæti sem þörf er á fyrir vottunarþjónustu fyrirtækisins, þar á meðal þessa vottunarstöð. Verðmætaskráin er notuð sem grundvöllur fyrir áhættumat. Öll verðmæti eru flokkuð samkvæmt mikilvægi þeirra í rekstri vottunarstöðvarinnar. Flokkunin gefur einnig til kynna hver þörfin er fyrir öryggisráðstafanir hvers verðmætis.

7.4.3 Mannauður og öryggi

Vottunarstöðin hefur á að skipa starfsfólki sem hefur þá þekkingu sem þörf er. Þekking starfsmanna miðast við að geta tryggt öruggan rekstur vottunarþjónustunnar og veitt viðskiptavinum alla nauðsynlega þjónustu. Stjórnendur hjá Auðkenni hafa þekkingu og reynslu á rafrænum skilríkjum og nauðsynlegum verkferlum í tengslum við starfsmenn og áhættumat.

Við ráðningu starfsmanna hjá Auðkenni er framkvæmd bakgrunnskönnun til þess að tryggja að ekki veljist aðilar til starfa sem gætu haft stríðandi hagsmuni við rekstur vottunarstöðvarinnar eða hafa verið dæmdir fyrir stórfellda glæpi eða aðrar sakir sem gætu haft áhrif á starfshæfni viðkomandi. Starfsmenn eru formlega skipaðir í skilgreind trúnaðarhlutverk og staðfesta hver fyrir sig að þeir muni fylgja öllum verkferlum sem skilgreindir hafa verið í tengslum við stjórnkerfi upplýsingaöryggis. Brot á stefnu Auðkennis í tengslum við rekstur vottunarþjónustunnar eru rannsökuð sérstaklega samkvæmt formlegu stigvaxandi agaferli sem starfsmönnum hefur verið kynnt.

Skilgreind hafa verið hlutverk öryggisstjóra, kerfisstjóra, kerfisumsjónarmanns og eftirlitsaðila kerfa og eru hlutverkin framkvæmd af starfsmönnum sem eru á ábyrgð vottunarstöðvarinnar. Starfslýsingar þessara hlutverka eru skilgreindar í öryggishandbók Auðkennis ásamt öðrum hlutverkum sem mikilvæg eru fyrir rekstur vottunarþjónustu Auðkennis og fela í sér kröfur um aðskilnað starfa að því marki sem það er nauðsynlegt.

7.4.4 Raunlægt öryggi og umhverfisöryggi

Vottunarstöðin hefur gert sérstakar ráðstafanir til þess að koma í veg fyrir óheimilaðan aðgang að húsnæði og búnaði vottunarstöðvarinnar ásamt því að gera ráðstafanir til þess að draga úr eða koma í veg fyrir truflanir á rekstri þjónustunnar. Eins eru gerðar sérstakar ráðstafanir til þess að koma í veg fyrir þjófnað á upplýsingum eða búnaði sem notaður er hjá vottunarstöðinni.

Auðkenni hefur gert allar ráðstafanir sem nauðsynlegar eru, í tengslum við framleiðslu skilríkja, búnað og afturköllun, til þess að:

a) tryggja öryggi húsnæðis;

b) engir starfsmenn verði skildir einir eftir á vernduðum svæðum;

c) verja það svæði sem notað er við framleiðslu skilríkja með raunlægu öryggi;

d) koma upp raunlægu öryggi gegn innbrotum, rafmagnstruflunum, þjófnaði, bruna o.þ.h;

e) koma í veg fyrir að búnaður, upplýsingar, miðlar eða hugbúnaður verði færð út úr húsnæðinu án heimildar.

7.4.5 Stjórnun á samskiptum og rekstri

Vottunarstöð Fullgilds auðkennis er aðskilin frá annarri starfsemi Auðkennis og virkt eftirlit með vottunarþjónustunni er tryggt með skipulögðu verklagi á meðan þjónustan er í rekstri. Verklagsreglur hafa verið skilgreindar og innleiddar fyrir öll hlutverk hjá vottunarstöðinni.

Vottunarstöðin hefur skilgreint verklag fyrir tilkynningar og meðhöndlun atvika sem haft hafa áhrif á þjónustu vottunarstöðvarinnar. Auðkenni mun bregðast við öllum atvikum á skipulegan hátt til þess að draga úr tjóni sem brot á öryggi getur valdið. Öll atvik eru skráð eins fljótt að mögulegt er.

Allir miðlar sem notaðir eru hjá vottunarstöðinni eru meðhöndlaðir á öruggan hátt og í samræmi við flokkun þeirra. Miðlarnir eru varðir gegn skemmdum og óheimilli notkun og gerðar hafa verið ráðstafanir til þess að koma í veg fyrir tap á upplýsingum vegna úreldingar eða öldrunar miðla innan þess tíma sem krafist er að gögn verði geymd. Öllum miðlum sem innihalda viðkvæmar upplýsingar er eytt á öruggan hátt þegar þeirra er ekki lengur þörf.

Rýmdaráætlanir eru framkvæmdar reglulega með því að fylgjast með nýtingu búnaðar í þeim tilgangi að geta metið framtíðarþörf og til þess að bregðast við með nægum fyrirvara. Ráðstafanir eru gerðar til þess að koma í veg fyrir að spillihugbúnaður geti skaðað réttleika þjónustunnar hjá vottunarstöðinni. Reglulega eru eftirlitsdagbækur rýndar til þess að finna ummerki um óheimila starfsemi.

Aðilar sem koma að framkvæmd öruggisaðgerða eru skipaðir sérstaklega í þau hlutverk eða ábyrgð skilgreint í starfslýsingu viðkomandi starfsmanns. Í hlutverkalýsingum er m.a. skilgreind helstu viðfangsefni, ábyrgð ásamt kröfum um þekkingu og hæfni. Öryggisstjóri ber ábyrgð á innleiðingu, viðhaldi og þróun öryggismála hjá Auðkenni. Framkvæmd lyklaathafna á vegum Auðkennis og skjöl tengd þeim eru rýnd fyrir og eftir lyklaathöfn af ytri endurskoðanda.

7.4.6 Aðgangsstýring

Hjá vottunarstöðinni gilda strangar reglur um aðgang starfsmanna að kerfum stöðvarinnar. Séð er til þess að ákveðin hlutverk eru aðskilin þannig að hvert hlutverk hefur aðeins þann aðgang sem hefur verið skilgreindur fyrir það hlutverk. Engir notendur geta notað kerfi vottunarstöðvarinnar án þess að hafa heimilaðan aðgang. Formlegir verkferlar sjá til þess að umsjón með notendum er skilvirk sem tryggir að aðgangur notenda er réttur hverju sinni og gott eftirlit með þeim. Starfsmenn eru ábyrgir fyrir þeim aðgerðum sem þeir framkvæma á tölvukerfum vottunarstöðvarinnar og eftirlitsdagbækur eru geymdar til að staðfesta aðgerðir starfsmanna.

Búnaður sem notaður er hjá vottunarstöðinni er staðsettur í öruggu húsnæði ásamt því að uppsetning búnaðarins eru reglulega skoðuð til að staðfesta rétta virkni. Öll innri netkerfi vottunarstöðvarinnar eru varin sérstaklega gagnvart innbrotum. Vottunarstöðin hefur komið upp eftirlitskerfi með viðvörunum um óeðlilegar aðgerðir við útgáfu skilríkja þannig að starfsmenn geti brugðist við með hraði. Fylgst er með öllum tilraunum til breytinga, viðbóta eða eyðingar skilríkja við miðlun þeirra.

Öll viðkvæm gögn eru varin gagnvart óleyfilegum aðgangi eða breytingum. Viðkvæm gögn sem flutt eru eftir netkerfum eru dulrituð til að tryggja öryggi þeirra. Þegar geymslumiðlar eru endurnotaðir er séð til þess að eldri gögn séu ekki aðgengileg.

Allar breytingar á stöðu skilríkja eru aðgangsstýrðar. Vottunarstöðin hefur komið upp eftirlitskerfi með viðvörunum um óeðlilegar aðgerðir við afturköllun skilríkja þannig að starfsmenn geti brugðist við með hraði.

7.4.7 Öflun, þróun og viðhald upplýsingakerfa

Vottunarstöðin gerir greiningu á kröfum til öryggis þegar nýrra kerfa er aflað eða eldri kerfum er breytt. Þessar kröfur eiga við hvort sem vottunarstöðin sér sjálf um þróun eða útvistar henni til ytri aðila. Breytingastjórn er beitt þegar gerðar eru breytingar á kerfum.

7.4.8 Stjórnun á rekstrarsamfellu og umsjón með upplýsingaöryggisatvikum

Vottunarstöðin hefur skilgreint neyðaráætlun til þess að bregðast við ófyrirséðum áföllum. Afritun og endurheimt er aðeins framkvæmd af tilgreindum starfsmönnum í trúnaðarhlutverkum og afrit eru geymd á öruggum stað til þess að auðvelda endurheimt kerfa á skilvirkan hátt. Gripið er til aðgerða ef óviðkomandi:

a) komast yfir eða talið er að hafi komist yfir einkalykil vottunarstöðvarinnar. Það er talið neyðarástand sem takast verður á með neyðaráætlun og ráðstafanir gerðar til þess að lágmarka líkur á að það endurtaki sig.

b) gerir óheimila breytingu á afturköllunarstöðu. Þá mun vottunarstöðin láta alla hlutaðeigandi aðila vita af því að vottunarstöðin kunni að vera óstarfhæf.

c) hefur komist yfir algrím eða stillingar vottunarstöðvarinnar eða ef það verður ófullnægjandi fyrir áframhaldandi notkun. Þá mun vottunarstöðin láta alla viðkomandi aðila vita af stöðunni og afturkalla öll skilríki sem atvikið hafði áhrif á.

7.4.9 Lokun þjónustu

Ef starfsemi vottunarstöðvarinnar verður hætt mun Auðkenni framkvæma eftirfarandi aðgerðir:

a) upplýsa alla hagsmunaaðila um stöðvun starfseminnar og hætta notkun á og eyða einkalykli þjónustunnar;

b) Auðkenni viðheldur tryggingu sem nægir til þess að standa straum af kostnaði í tengslum við stöðvun vottunarstöðvarinnar;

c) Vottunarstöðin hefur skilgreint verklag sem nær yfir nauðsynlegar aðgerðir vegna stöðvunar vottunarþjónustunnar. Þetta felur meðal annars í sér tilkynningu til allra hagsmunaaðila, flutning á skyldum til annars aðila og meðhöndlun á afturköllunarstöðu virkra skilríkja sem hafa verið gefin út.

7.4.10 Hlíting

Vottunarstöðin viðheldur lista yfir allar lagalegar kröfur gagnvart rekstri vottunarþjónustunnar. Gerðar eru ráðstafanir til þess að hlíta þeim kröfum sem gilda um vottunarþjónustuna t.d. með reglulegu eftirliti.

Vottunarstöðin tryggir með skriflegum verklagsreglum að lögum um persónuvernd sé fylgt varðandi skráningu upplýsinga, leynd þeirra og aðgangsstýringu. Einnig er tryggt að einstaklingar sem nýta þjónustu vottunarstöðvarinnar séu upplýstir um tilgang skráningarinnar og að þeir hafi veitt heimild fyrir skráningunni. Gerðar eru ráðstafanir til þess að koma í veg fyrir ólöglega meðhöndlun, tap, eyðingu eða breytingar á persónuupplýsingum. Vottunarstöðin lætur ekki af hendi upplýsingar sem einstaklingar hafa látið henni í té vegna vottunarþjónustu nema með heimild viðkomandi einstaklings eða dómsúrskurði.

7.4.11 Skráning upplýsinga

Vottunarstöðin viðheldur leynd og réttleika skráninga um fullgild skilríki með sérstökum ráðstöfunum og í samræmi við almennar viðskiptavenjur. Upplýsingar um fullgild skilríki eru geymdar í þann tíma sem krafist er samkvæmt lögum eða reglugerðum um vottunarþjónustu. Skráningarnar eru aðeins gerðar aðgengilegar að gengnum dómsúrskurði eða ef þörf er á vegna sönnunarbyrði í dómsmálum. Skilríkjahafi getur fengið aðgang að skráningunni og tengdum upplýsingum, sama gildir um áskrifanda eftir því sem við á, að teknu tilliti til ákvæða laga um persónuvernd.

Allar mikilvægar aðgerðir í vottunarþjónustu eru skráðar samkvæmt GPS klukku.

Vottunarstöðin hefur skilgreint hvaða aðgerðir talið sé nauðsynlegt að skrá í dagbók, skráðar eru allar aðgerðir sem tengjast skráningu fullgildra skilríkja, þar með talin endurnýjun þeirra. Jafnframt viðheldur vottunarstöðin ferilskrá yfir allar aðgerðir sem tengjast lífsskeiði einkalykla vottunarstöðvarinnar, skilríkja áskrifenda og annarra lykla sem eru í umsjón vottunarstöðvarinnar. Ferilskrá er haldin um frágang á öruggum undirskriftarbúnaði skilríkjahafa, að því marki sem það er framkvæmt hjá vottunarstöðinni. Eftirfarandi upplýsingar eru varðveittar tengdar skráningu á fullgildum skilríkjum:

a. Nafn og kennitala umsækjanda og skilríkjahafa.

b. tegund skjala sem umsækjandi notar til að styðja umsókn sína, þegar það á við;

c. geymslustaður afrita umsókna og skilríkja þar með talið undirritaður áskriftarsamningur;

d. sérstakar samþykktir áskrifanda;

e. auðkenni þess aðila sem samþykkir umsókn;

f. nafn skráningarfulltrúa og skráningarstöðvar.

Allar beiðnir um afturköllun ásamt niðurstöðum afturköllunar eru skráðar í dagbækur. Gerðar eru ráðstafanir til þess að koma í veg fyrir eyðingu dagbóka fyrir aðgerðir vottunarstöðvarinnar.

7.5 Skipulag

Starfssemi vottunarstöðvarinnar fellur undir stjórnskipulag Auðkennis. Auðkenni er einkahlutfélag og eigandi vottunarstöðvarinnar og milliskilríkisins „Fullgilt auðkenni“.

Auðkenni hefur starfað síðan 2000 og er leiðandi á þeim markaði fyrir öryggislausnir í rafrænum samskiptum. Félagið er í samstarfi við öfluga ytri aðila ýmist sem viðskiptavinur eða veitandi þjónustu. Í undangengnum köflum hefur því verið lýst hvernig vottunarþjónustan starfar eftir óhlutdrægum stefnureglum og verklagi sem byggir á stjórnkerfi fyrir gæði og upplýsingaöryggi, og býður þjónustu sína öllum umsækjendum sem þess óska og hafa íslenska kennitölu. Þar hefur því einnig verið lýst hvenær samningar eru gerðir og hvernig skilmálum og skilyrðum er miðlað, þar á meðal hvernig unnið er úr kvörtunum sem berast á borð félagsins. Í undangengnum köflum hefur verklagi við ferilkönnun starfsmanna verið lýst, m.a. með tilliti til óhæðis og bærni til sjálfstæðrar ákvarðanatöku um rekstur þjónustuþátta, þar á meðal afturköllun og ákvörðun um að hefja eða stöðva framleiðslu einstakra skilríkjategunda.

Neytendastofa, eftirlitsaðili vottunarstöðvarinnar, er reglulega upplýst um fjárhagslegan styrk félagsins, tryggingar og aðra slíka þætti. Það er á valdi stofnunarinnar að stöðva útgáfu fullgildra rafrænna skilríkja, telji stofnunin að vottunarstöðin uppfylli ekki ákvæði um fjárhagslegan styrk.

AUÐKENNI
Digitally signed by Auðkenni búnaðarskilríki
Date: 2012.01.05 16:42:03 Z