Vottunarstefna Auðkennis
fyrir rafræn skilríki
gefin út undir Fullgildu auðkenni

Útgáfa 01-02-00
12. júní 2018

Breytingasaga

Útgáfudagur	Útgáfa	Lýsing	Ábyrgðaraðili
28.08.2008	01-00-00	Fyrsta útgáfa.	Logi Ragnarsson
27.11.2013	01-01-00	Útgáfa 1.1	Haraldur A. Bjarnason
12.06.18	01-02-00	Útgáfa 1.2	Haraldur A. Bjarnason

Efnisyfirlit

Breytingasaga ii
Réttindi 5
Formáli 5
Yfirlit 5
1 Gildissvið 6
2 Tilvísanir 6
3 Skilgreiningar og skammstafanir 7
3.1 Skilgreiningar 7
3.2 Skammstafanir 10
4 Almenn hugtök 10
4.1 Vottunarstöð 11
4.2 Vottunarþjónusta 11
4.3 Vottunarstefna og yfirlýsing um framkvæmd vottunar 12
4.3.1 Tilgangur 12
4.3.2 Sérhæfni skjala 12
4.3.3 Nálgun 13
4.3.4 Aðrar yfirlýsingar vottunarstöðvar 13
4.4 Áskrifandi og vottorðshafi 13
5 Almennt um vottunarkröfur 13
5.1 Yfirlit 13
5.2 Auðkenning 13
5.3 Notkunarsvið og nothæfi 14
5.4 Samræmi 15
5.4.1 Yfirlýsing um samræmi 15
5.4.2 Kröfur um samræmi 15
6 Skyldur og skuldbindingar 15
6.1 Skyldur Auðkennis 15
6.2 Skyldur áskrifenda 15
6.3 Upplýsingar fyrir treystendur 16
6.4 Skuldbindingar 16
7 Kröfur um framkvæmd vottunarstöðva 17
7.1 Yfirlýsing um framkvæmd vottunar 17
7.2 Dreifilyklaskipulag - lífsskeið lyklaumsjónar 17
7.2.1 Framleiðsla lykla Auðkennis 18
7.2.2 Geymsla, öryggisafritun og endurheimt lykla hjá Auðkenni 18
7.2.3 Dreifing Auðkennis á dreifilyklum 19
7.2.4 Vörsluafrit lykla 19
7.2.5 Notkun á einkalykli Auðkennis 19
7.2.6 Endalok lífskeiðs einkalykla Auðkennis 19
7.2.7 Umsjón dulmálsvélbúnaðar fyrir undirritun skilríkja á lífsskeiði hans 19
7.2.8 Umsjón Auðkennis með lyklum vottorðshafa 20
7.2.9 Undirbúningur á öruggum notendabúnaði 20
7.3 Dreifilyklaskipulag - lífsskeið skilríkjaumsjónar 20
7.3.1 Skráning vottorðshafa 20

7.3.2 Endurnýjun, uppfærsla og endurlyklun skilríkja 22
7.3.3 Framleiðsla skilríkja 22
7.3.4 Miðlun á skilmálum og skilyrðum 23
7.3.5 Miðlun skilríkja 23
7.3.6 Afturköllun og tímabundin ógilding skilríkja 24
7.4 Stjórnun og rekstur vottunarstöðvar Auðkennis 25
7.4.1 Stjórnun upplýsingaöryggis 25
7.4.2 Eignastjórnun 25
7.4.3 Mannauður og öryggi 26
7.4.4 Raunlægt öryggi og umhverfisöryggi 26
7.4.5 Stjórnun á samskiptum og rekstri 27
7.4.6 Aðgangsstýring 28
7.4.7 Öflun, þróun og viðhald upplýsingakerfa 29
7.4.8 Stjórnun á rekstrarsamfellu og umsjón með upplýsingaöryggisatvikum 29
7.4.9 Lokun þjónustu 30
7.4.10 Hlíting 31
7.4.11 Skráning upplýsinga 31
7.5 Skipulag 32

Réttindi

Auðkenni á öll réttindi varðandi þessa vottunarstefnu.

Formáli

Þessi vottunarstefna er samin á ábyrgð Auðkennis fyrir útgáfu á rafrænum skilríkjum til almennings undir milliskilríkinu Fullgilt auðkenni. Skjal þetta var samið með hliðsjón af kröfum í *Stefnumarkandi kröfur fyrir ISRS skilríki í rafrænni þjónustu* [1], sem samið var af SAM, sem er samstarfshópur fjármálaráðuneytisins og Auðkennis. SAM hópurinn starfaði í samræmi við *Samstarfssamning Auðkennis og fjármálaráðuneytisins um innleiðingu dreifilyklaskipulags og almenna notkun rafrænna skilríkja*, sem gilti frá 8. mars 2007 til 8. mars 2013.

Nánari upplýsingar um Auðkenni má fá á www.audkenni.is og almennar upplýsingar um rafræn skilríki má nálgast á www.skilriki.is.

Yfirlit

Ein helsta forsenda fyrir útbreiðslu rafrænnar þjónustu er sú 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.

Með tilkomu laga um rafrænar undirskriftir, nr. 28/2001 [2] og síðar reglugerðar um rafrænar undirskriftir nr. 780/2011 [3], laga um rafræn viðskipti og aðra rafræna þjónustu, nr. 30/2002 [5], og laga nr. 51/2003 um breytingu á stjórnsýslulögum, nr. 37/1993 [6] (rafræn stjórnsýsla), var lagður grundvöllur að rafrænum viðskiptum, þar með talið rafrænni stjórnsýslu, samhliða hefðbundnum aðferðum.

Notendur rafrænna skilríkja og allir þeir sem reiða sig á rafræn skilríki verða 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.

Vottunarstefna þessi setur fram þær kröfur sem Auðkenni fylgir við rekstur vottunarstöðvar Fullgilds auðkennis. Hún er aðgengileg þeim sem hyggjast nýta sér eða reiða sig á rafræn skilríki sem gefin eru út af vottunarstöðinni, til þess að þeir aðilar geti lagt mat á hversu mikið traust þeir vilja leggja á skilríkin.

Skilríki sem uppfylla kröfur þessarar vottunarstefnu geta verið fullgild vottorð í skilningi laga um rafrænar undirskriftir. Yfirlýsing um slíkt er sett fram í skilríkjunum, þegar við á.

1 Gildissvið

Auðkenni gefur út rafræn skilríki undirrituð af Fullgildu auðkenni í dreiflyklaskipulagi sem kallað er „PKI-Ísland“, í traustléni þar sem Íslandsrót er efst í stigveldinu og uppruni traustsins. Með dreiflyklaskipulagi er átt við það skipulag sem þarf til að framleiða lykla, skilríki og afturköllunarlista, dreifa þeim, hafa umsjón með þeim og safnvista.

Í þessu skjali, *Vottunarstefnu Auðkennis fyrir rafræn skilríki gefin út undir Fullgildu auðkenni*, eru tilgreindar lagalegar og tæknilegar kröfur sem Auðkenni uppfyllir við framleiðslu, útgáfu, notkun, geymslu, afturköllun og endurnýjun rafrænna skilríkja undir Fullgildu auðkenni. Þessar kröfur tryggja öryggi rafrænna skilríkja og veita þeim sem nota eða reiða sig á skilríkin vissu um að þeir geti lagt traust á þau. Vottunarstefnan er ekki samningur milli Auðkennis og þátttakenda í PKI-Ísland dreiflyklaskipulaginu, heldur einhliða yfirlýsing Auðkennis um hvaða kröfum verður fylgt til að tryggja öryggi kerfisins. Þessi Vottunarstefna nýtist því:

- Áskrifendum skilríkja til að meta hvernig öryggi kerfisins er tryggt, hvernig nota megi skilríkin og hverjar skyldur þeirra eru.
- Treystendum sem reiða sig á skilríkin til að meta hversu mikið traust má bera til skilríkjanna og þá undirritun sem framkvæmd er með þeim.

Skilríki sem gefin eru út í samræmi við þessa vottunarstefnu geta talist fullgild vottorð sbr. lög um rafrænar undirskriftir nr. 28/2001. Yfirlýsing um slíkt er sett fram í skilríkjunum, þegar við á.

2 Tilvísanir

Eftirfarandi skjöl innhalda ákvæði sem, með tilvísunum í texta þessarar vottunarstefnu, mynda ákvæði 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] Reglugerð um rafrænar undirskriftir, nr. 780/2011.

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

[5] Lög um rafræn viðskipti og aðra rafræna þjónustu, nr. 30/2002, með síðari breytingum.

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

[7] *TS 146:2013 Innihald almennra rafrænna skilríkja*. Staðlaráð Íslands, 2013.

[8] *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.

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

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

[11] 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).*

[12] 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).*

[13] 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).*

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

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

[16] ÍST ISO/IEC 27002:2005: *Upplýsingatækni – Öryggistækni: Starfsvenjur fyrir stjórnun upplýsingaöryggis.*

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

3 Skilgreiningar og skammstafanir

3.1 Skilgreiningar

Í neðangreindum lista eru skilgreiningar sem koma fram í vottunarstefnunni. 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 gildistími þeirra rennur út. Ekki er hægt að gera afturkölluð skilríki gild aftur.

Afturköllunarlisti skilríkja (*certificate revocation list*): Skrá yfir skilríki sem ekki eru 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.

Birtingarskýrsla dreifilyklaskipulags (*PKI disclosure statement - PDS*): Skýrsla sem inniheldur upplýsingar um dreifilyklaskipulag, gerð í þeim tilgangi að birta upplýsingarnar þannig að þær séu auðskiljanlegar og aðgengilegar fyrir hinn almenna notanda sem þarf að leggja mat á það traust sem hann getur borið til skipulagsins.

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

Dreifilykill (*public key*): Dulmálslykill sem ætlaður er hvaða einindi (*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 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 varðveita 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 getur framleitt og varðveitt lykla og notað rafræna undirskrift.

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

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

Einkalykill vottunarstöðvar (*certification authority key*): Einkalykill sem tilheyrir vottunarstöð og notaður er 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.

Fullgild skilríki (*qualified certificate*): Skilríki sem hafa að geyma upplýsingar þær sem kveðið er á um í 7. gr. laga um rafrænar undirskriftir, nr. 28/2001 [2] og gefið er 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“.

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 (*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 hefur umboð til að koma fram fyrir hönd fyrirtækisins og samþykkja og sækja um skilríki, eða hafa umsjón með skilríkjum fyrirtækisins.

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

Móttakandi skilríkja (*certificate recipient*): Sá aðili 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 örgjörvakortum er algengt að persónulegt kenninúmer (PIN) sé notað sem notkunaraðgangsorð.

Persónulegt kenninúmer (*personal identification number - PIN*): Stutt númer sem einstaklingur notar sem aðgangsorð að virkum búnaði, til dæmis símakorti, greiðslukorti eða að rafrænum skilríkjum á örgjörvakorti. 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, stafrænt undirritað með einkalykli vottunarstöðvar.

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

Rót (*root*): Upphaf trausts í tilteknu léni dreifilyklaskipulags. Rót er útfærð með skilríkjum 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.

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

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

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 ábyrgur er fyrir auðkenningu og vottun á vottorðshafa en undirritar hvorki skilríki né heldur gefur þau út. Skráningarstöð getur tekið að sér þess háttar verkefni fyrir hönd vottunarstöðvar.

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

Stofnaðgangsorð (*activation code*): Aðgangsorð sem vottunarstöð úthlutar vottorðshafa í þeim tilgangi að búa til, eða stofna, skilríkin og mynda lyklapar. Vottorðshafinn þarf ekki að nota stofnaðgangsorðið aftur. Stundum kallað „virkjunarkóði“.

Tímabundin ógilding (*suspension*): Aðgerð sem felur í sér að vottunarstöð skráir skilríki 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 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.

Útfærð rafræn undirskrift (*advanced electronic signature*): Rafræn undirskrift sem a) tengist undirritanda einum, b) er til þess fallin að bera kennsl á undirritanda, c) er gerð með aðferð sem er eingöngu á forræði undirritanda og d) er tengd gögnum á þann hátt að hvers konar breyting á þeim eftir undirritun er greinileg.

Virkjunargögn (*activation data*): Gagnagildi, önnur en lyklar, sem þarf til að nota dulmálsbúnað. Virkjunargögn þarf að vernda. Virkjunargögn eru t.d. aðgangsorð (notkunaraðgangsorð), 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 nothæfi 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 einnig 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] og ákvæði IV. kafla reglugerðar um rafrænar undirskriftir, nr. 780/2011 [3]. Öruggur undirskriftarbúnaður er sérstakt tilvik af öruggum notendabúnaði sem ætlaður er fyrir fullgildar rafrænar undirskriftir.

3.2 Skammstafanir

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 sem uppfylla kröfur þessa skjals.
QCP	Fullgildar vottunarkröfur, fyrir fullgild skilríki (***Q**ualified **C**ertificate **P**olicy*).
SSCD	Öruggur undirskriftarbúnaður (***S**ecure **S**ignature-**C**reation **D**evice*).
PIN	Persónulegt kenninúmer (***P**ersonal **I**dentification **N**umber*).

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.

Þessi vottunarstefna fjallar um kröfur og stefnureglur vegna útgáfu endaskilríkja.

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

Auðkenni rekur vottunarstöðvar sem gefa út skilríki á almennum markaði í samræmi við þær kröfur sem fram koma í vottunarstefnum skilríkjanna. Meginmarkmið Auðkennis 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, lögaðili 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] og reglugerð um rafrænar undirskriftir nr. 780/2011 [3] er íslenska orðið „vottorð" notað fyrir enska hugtakið „certificate". Orðin „vottorð" og „skilríki" hafa almennt sömu merkingu í þessu skjali og eiga í öllum tilvikum við dreifilyklaskilríki, nema annað sé tekið fram. Orðið „vottorðshafi" er notað um réttan handhafa skilríkja, sem á ensku er kallað „certificate subject", enda er vísað til þess að réttur handhafi er sá aðili sem er vottaður og auðkenndur sem slíkur í skilríkjum.

4.1 Vottunarstöð

Eins og áður segir er vottunarstöð 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 því að veita þá þjónustu sem tilgreind er í kafla 4.2. Einkalykill vottunarstöðvar er notaður til að undirrita skilríkin og vottunarstöðin er auðkennd í skilríkjunum sem útgefandi. Auðkenni rekur vottunarstöð sem gefur út fullgild rafræn skilríki til almennings.

Í lögum um rafrænar undirskriftir nr. 28/2001 [2] og reglugerð um rafrænar undirskriftir nr. 780/2011 [3] er orðið „vottunaraðili" notað yfir þann aðila sem gefur út vottorð eða veitir aðra þjónustu í tengslum við rafrænar undirskriftir. Í þessari stefnu nær orðið vottunarstöð yfir vottunaraðila.

Vottunarstöð er heimilt að nota aðra aðila til að framkvæma hluta af vottunarþjónustunni, en ber þó ábyrgð á öllum þáttum sem varða notkun skilríkja og tryggir að þær kröfur sem tilgreindar eru í vottunarstefnu þessari séu ávallt uppfylltar.

4.2 Vottunarþjónusta

Starfsemi vottunarstöðvar skiptist í eftirfarandi þjónustuþætti:

Skráningarþjónusta: Sannprófar auðkenni og ef við á hvaða sértækar eigindir vottorðshafa sem er. Niðurstaða þessarar þjónustu er nýtt við framleiðslu skilríkja.

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

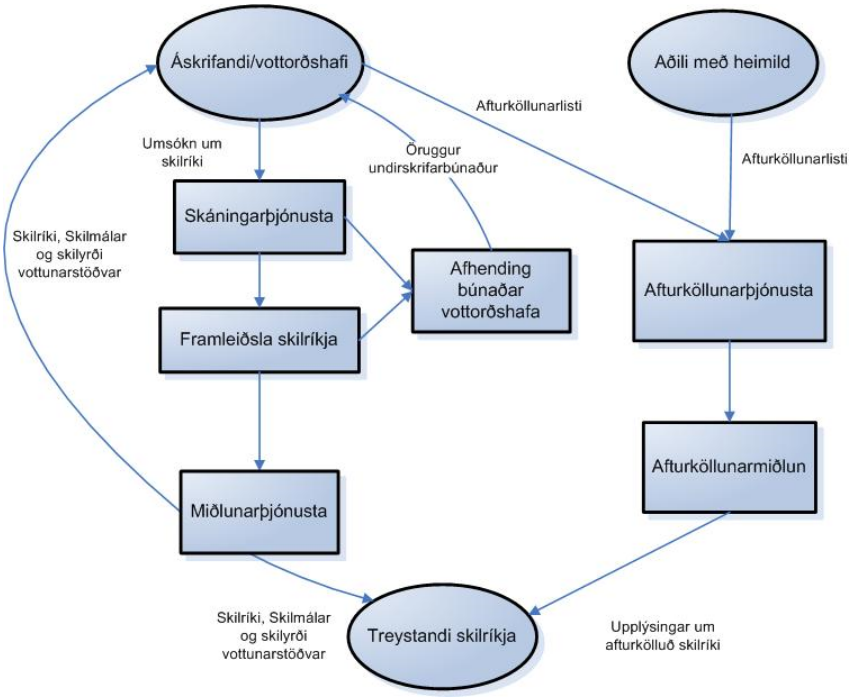
Miðlunarþjónusta: Miðlar skilríkjum til vottorðshafa og birtir skilríkin þannig að treystendur geti haft aðgang að þeim, að því gefnu að vottorðshafi samþykki það. Þessi þjónusta birtir einnig skilmála og skilyrði vottunarstöðvarinnar ásamt þeim reglum og upplýsingum um framkvæmd sem gefnar hafa verið út til áskrifenda og treystenda.

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

Stöðumiðlun: Veitir upplýsingar um stöðu skilríkja til treystenda. Þessi þjónusta getur verið miðlun í rauntíma eða byggð á upplýsingum sem eru uppfærðar reglulega, svo sem afturköllunarlistum.

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

Mynd 1 hér sýnir innbyrðis tengsl á milli þjónustuþáttanna.



Mynd 1: Skýringarmynd sem sýnir skiptingu vottunarþjónustu í þjónustuþætti.

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 fylgir, en tilgangur með yfirlýsingu um framkvæmd vottunar er hins vegar að segja til um hvernig farið er að því að fylgja kröfunum hjá viðkomandi vottunarstöð, það er að segja þeir ferlar sem notaðir eru til að búa til og viðhalda skilríkjum hjá vottunarstöðinni. Í skilríkjunum er vísað á vottunarstefnuna, með kennimarki stefnunnar, þannig að móttakandi rafrænna skilríkja geti kynnt sér þær kröfur sem vottunarstöðin fylgir.

Ef gerðar eru breytingar á vottunarstefnunni sem áhrif hafa á nothæfi stefnunnar ætti um leið 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 fylgir þeim kröfum um tækni, skipulag og verklag sem tilgreindar eru í vottunarstefnunni.

Í sumum tilvikum getur verið viðeigandi fyrir vottunarstöð að lýsa með ítarlegri hætti í undirskjölum, sérstökum ferlum sem nauðsynlegir eru svo mögulegt sé 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.

Allar vottunarstöðvar gefa út vottunarstefnu sem lýsa gildissviði og öryggisstigi skilríkja. Vottunarstefnur vottunarstöðva geta þannig verið fleiri en ein, ef gefin eru út skilríki með mismunandi gildissviði eða

öryggisstigi. Yfirlýsing um framkvæmd vottunar mun því vísa til krafna í tilgreindri vottunarstefnu vottunarstöðvar og í skilríkjunum er vísað á þá tilteknu vottunarstefnu.

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 aftur á móti sniðin að skipulagi, rekstrarferlum, aðstöðu og tölvuumhverfi vottunarstöðvar.

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 alla jafna almenns eðlis og varða almenna viðskiptahætti vegna útgáfu skilríkja og miðlunar upplýsinga.

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

4.4 Áskrifandi og vottorðshafi

Þegar skilríki eru gefin út til einstaklinga til eigin notkunar (einkaskilríki) þá er einstaklingurinn bæði áskrifandi og vottorðshafi. Sá aðili sem óskar eftir skilríkjum getur þó verið annar en sá sem skilríkin vísa til. Til að mynda getur fyrirtæki þurft skilríki fyrir starfsmenn sína eða búnað þannig að þeir geti haft rafræn samskipti í nafni fyrirtækisins (starfsskilríki, búnaðarskilríki). Í slíkum tilvikum er sá sem er áskrifandi hjá vottunarstöð annar en sá sem er vottorðshafi og tilgreindur í skilríkjunum sem slíkur.

Svo að mögulegt sé 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 vottaður 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 skilgreindar eru í vottunarstefnunni eru kröfur sem Auðkenni fylgir við útgáfu á rafrænum skilríkjum hjá vottunarstöð Fullgilds auðkennis. Skilríki sem gefin eru út í samræmi við vottunarstefnuna innihalda auðkenningu á stefnunni 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 (*object identifier: OID*) sem skráð er hjá Póst- og fjarskiptastofnun undir viðurkenndum og skráðum landaboga fyrir Ísland. Skráningin er í samræmi við *Lýsingu á starfsemi skráningarstöðvar* [8] og í samræmi við kröfur í ISO/IEC 9594-8|ITU-T Recommendation X.509 [15]. Þetta kennimark vottunarstefnunnar er:

{joint-iso-itu-t(2) country(16) is(352) fyrirtæki-samtök-og-stofnanir(1) audkenni(2) pki(1) public-pki(1) cp-fa(1) version(2)}

Þetta kennimark má einnig rita {2 16 352 1 2 1 1 1 2}. Öll rafræn skilríki sem gefin eru út á grundvelli þessarar vottunarstefnu vísa til hennar með því að tilgreina þetta kennimark í svæðinu „Certificate policies" í skilríkjunum. Með vísun í kennimark þessarar vottunarstefnu í skilríkjunum lýsir Auðkenni því yfir að skilríkin uppfylla kröfur vottunarstefnunnar.

5.3 Notkunarsvið og nothæfi

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

5.3.1 Rafræn skilríki

Rafræn skilríki sem Auðkenni gefur út undir Fullgildu Auðkenni uppfylla eftirfarandi kröfur:

a) Auðkenni sem vottunarstöð vinnur í samræmi við þær kröfur sem settar eru fram í V. kafla laga um rafrænar undirskriftir nr. 28/2001 [2] og III. kafla reglugerðar um rafrænar undirskriftir nr. 780/2011 [3].

b) Skilríkin eru gefin út á almennum markaði.

5.3.2 Fullgild skilríki án öruggs undirskriftarbúnaðar

Þegar yfirlýsing um slíkt er sett í skilríkin, uppfylla fullgild skilríki á almennum undirskriftarbúnaði eftirfarandi kröfur:

a) Skilríkin uppfylla kröfur 7. gr. laga um rafrænar undirskriftir nr. 28/2001 [2] og ákvæði II. kafla reglugerðar um rafrænar undirskriftir nr. 780/2011 [3].

b) Auðkenni sem vottunarstöð fullnægir þeim kröfum sem settar eru fram í V. kafla laga um rafrænar undirskriftir nr. 28/2001 [2] og III. kafla reglugerðar um rafrænar undirskriftir nr. 780/2011 [3].

c) Skilríkin eru gefin út á almennum markaði.

Fullgild rafræn skilríki sem Auðkenni gefur út má nota til rafrænnar undirskriftar sem ekki má hafna að njóti réttaráhrifa og séu viðurkennd sem sönnun í málarekstri, sbr. 2. mgr. 4. gr. laga 28/2001 [2] og eru í samræmi við kröfur til fullgildra skilríkja sem auðkenndar eru sem „QCP public" í *Stefnumarkandi kröfum fyrir ISRS skilríki í rafrænni þjónustu [1]*.

5.3.3 Fullgild skilríki á öruggum undirskriftarbúnaði

Þegar yfirlýsing um slíkt er sett í skilríkin, uppfylla fullgild skilríki sem gefin eru út á öruggum undirskriftarbúnaði eftirfarandi kröfur:

a) Skilríkin uppfylla kröfur 7. gr. laga um rafrænar undirskriftir nr. 28/2001 [2] og ákvæði II. kafla reglugerðar um rafrænar undirskriftir nr. 780/2011 [3].

b) Auðkenni sem vottunarstöð fullnægir þeim kröfum sem settar eru fram í V. kafla laga um rafrænar undirskriftir nr. 28/2001 [2] og III. kafla reglugerðar um rafrænar undirskriftir nr. 780/2011 [3].

c) Skilríkin eru eingöngu ætluð fyrir notkun með öruggum undirskriftarbúnaði sem fullnægir kröfum í 8. gr. laga um rafrænar undirskriftir nr. 28/2001 [2] og ákvæði IV. kafla reglugerðar um rafrænar undirskriftir nr. 780/2011 [3].

d) Skilríkin eru gefin út á almennum markaði.

Fullgild rafræn skilríki sem Auðkenni gefur út á öruggum undirskriftarbúnaði fullnægja því lagakröfum um réttaráhrif rafrænna undirskrifta, sbr. 1. mgr. 4. gr. laga um rafrænar undirskriftir nr. 28/2001 [3] og eru í samræmi við kröfur til fullgildra skilríkja sem auðkenndar eru sem „QCP public + SSCD" í *Stefnumarkandi kröfum fyrir ISRS skilríki í rafrænni þjónustu* [1].

5.4 Samræmi

5.4.1 Yfirlýsing um samræmi

Auðkenni lýsir því yfir að við útgáfu, dreifingu, birtingu og afturköllun fullgildra skilríkja sem gefin eru út í samræmi við vottunarstefnu þessa, eru uppfyllt öll skilyrði sem gerð eru til fullgildra rafrænna skilríkja í lögum um rafrænar undirskriftir nr. 28/2001 [2], reglugerð um rafrænar undirskriftir nr. 780/2011 [3] og *Stefnumarkandi kröfum fyrir ISRS skilríki í rafrænni þjónustu* [1].

Til þess að færa sönnur á að svo sé lætur Auðkenni til þess bæra aðila, framkvæma úttekt sem sýna skal fram á að framkvæmd Auðkennis við útgáfu skilríkja sé í samræmi við þær kröfur sem settar eru fram í þessari vottunarstefnu. Niðurstöður slíkrar úttektar verða gerðar aðgengilegar áskrifendum og hagsmunaðilum sem reiða sig á skilríkin. Slík úttekt verður framkvæmd reglulega. Sýni slík úttekt fram á að Auðkenni uppfylli ekki þær kröfur sem vottunarstefna þessi setur mun Auðkenni þegar í stað hætta útgáfu skilríka, þar til samræmi við kröfurnar er tryggt á ný.

5.4.2 Kröfur um samræmi

Auðkenni uppfyllir skyldur sínar samkvæmt kafla 6.1 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 Auðkennis

Auðkenni sér til þess að kröfum þeim sem tilgreindar eru í vottunarstefnu þessari sé fylgt, einnig þar sem undirverktakar taka að sér hluta starfseminnar.

Á vegum Auðkennis starfa skráningarstöðvar sem sjá um framkvæmd og tilhögun auðkenningar einstaklinga og lögaðila vegna útgáfu fullgildra skilríkja hjá Auðkenni. Nánar er fjallað um störf skráningarstöðva í yfirlýsingu um framkvæmd vottunar.

Auðkenni gefur út yfirlýsingu um framkvæmd vottunar sem lýsir fylgni við kröfur þessarar vottunarstefnu. Auðkenni ber ábyrgð á allri vottunarþjónustu í samræmi við yfirlýsingu sína um framkvæmd vottunar.

6.2 Skyldur áskrifenda

Auðkenni gerir samning við áskrifanda skilríkja (sjá k)-lið kafla 7.3.1) sem skuldbindur áskrifandann til að standa við eftirfarandi skuldbindingar. Ef vottorðshafi og áskrifandi eru sitt hvor aðilinn skal áskrifandinn gera vottorðshafann meðvitaðan um þær skuldbindingar sem eiga við vottorðshafann:

a) Að réttar og fullnægjandi upplýsingar séu gefnar til Auðkennis í samræmi við þessa vottunarstefnu, sérstaklega varðandi skráningu áskrifandans.

b) Að varðveita og nota eigið lyklapar með þeim heimildum og takmörkunum sem Auðkenni tilkynnir áskrifanda.

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

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

e) Að tilkynna án tafar til Auðkennis eða aðila er Auðkenni tilgreinir, ef eitthvert eftirtalinna atvika koma upp, á gildistíma skilríkjanna:

   i. Einkalykill vottorðshafa hefur glatast, honum verið stolið eða á annan hátt stofnað í hættu, eða

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

iii. vottorðshafi hefur ekki lengur tengsl við áskrifanda skilríkja, eða

iv. ónákvæmni eða breytingar eru á innihaldi skilríkja, samkvæmt tilkynningum til áskrifanda eða vottorðshafa.

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

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

6.3 Upplýsingar fyrir treystendur

Til þess að treystendur geti á eðlilegan hátt reitt sig á fullgild skilríki munu skilmálar og skilyrði sem Auðkenni birtir treystendum innihalda viðvörun um að þeir skuli;

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

b) taka tillit til allra takmarkana á notkun fullgildra skilríkja eins og þær eru birtar treystendum annað hvort í skilríkjunum eða í skilmálum, og

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

6.4 Skuldbindingar

Ábyrgð gagnvart áskrifendum og treystendum

Auðkenni sem útgefandi fullgildra skilríkja á öruggum undirskriftarbúnaði er bótaskylt í samræmi við VI. kafla laga um rafrænar undirskriftir nr. 28/2001 [2]. 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 7. gr. laga um rafrænar undirskriftir nr. 28/2001 [2].

c) Skilríki hafi ekki verið réttilega skráð í afturköllunarlista skv. 12. gr. laga um rafrænar undirskriftir nr. 28/2001 [2].

d) Að vottorðshafi hafi við útgáfu skilríkja ekki haft undir höndum einkalykla sem svara til þeirra dreifilykla sem koma fram í skilríkjunum.

e) Að hver einstakur einkalykill vottorðshafa svari ekki einvörðungu til paraðs dreifilykils vottorðshafans og að dreifilykillinn svari ekki einvörðungu til paraðs einkalykils vottorðshafans, þegar Auðkenni býr lyklapörin til.

Ofangreind skaðabótaábyrgð gildir einungis um fullgild skilríki á öruggum undirskriftarbúnaði ef sýnt þykir að tjónið hafi orðið vegna ásetnings eða vegna gáleysis starfsmanna Auðkennis og fellur niður ef notkun skilríkjanna er andstæð takmörkunum á gildissviði þeirra eða fjárhæð viðskipta, að því marki sem mögulegt er að kynna sér slíkar takmarkanir.

Ábyrgð Auðkennis 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.

Auðkenni kaupir og viðheldur tryggingu fyrir hugsanlegum skaðabótakröfum á vottunar- og skráningarstöðvar hvort heldur er frá samningsbundnum viðskiptavinum (áskrifendum) eða treystendum. Tryggingarfjárhæðin er ákvörðuð með hliðsjón af umfangi rekstrar Auðkennis hverju sinni.

Sérstakar skyldur vegna verndunar trúnaðarupplýsinga

Auðkenni flokkar upplýsingar sem varðveittar eru hjá félaginu á eftirfarandi hátt með tilliti til trúnaðar:

a) Aðrar upplýsingar en þær sem skráðar eru í skilríki og afturköllunarlista eru trúnaðarupplýsingar.

b) Upplýsingar sem skráðar eru í skilríki og afturköllunarlista eru opinberar upplýsingar. Persónugreinanlegar upplýsingar í skilríkjum eru birtar þar með samþykki áskrifanda.

Auðkenni tryggir:

c) Að trúnaðarupplýsingar séu verndaðar og þær verði ekki notaðar til annars en þess sem nauðsynlegt er fyrir rekstur vottunarstöðvar Auðkennis.

d) Að persónuupplýsingar séu verndaðar og ekki notaðar umfram það sem nauðsynlegt er fyrir rekstur Auðkennis í samræmi við lög um persónuvernd og meðferð persónuupplýsinga nr. 77/2000 [4].

7 Kröfur um framkvæmd vottunarstöðva

Við útgáfu á rafrænum skilríkjum fylgir Auðkenni þeim kröfum sem settar eru fram í þessum kafla.

Í þessum kafla eru kröfur um skráningarþjónustu, framleiðslu skilríkja, miðlunarþjónustu, afturköllunarþjónustu, stöðumiðlun og afhendingu búnaðar vottorðshafa. Kröfur er varða tiltekna þjónustuþætti Auðkennis eru settar í samsvarandi undirkafla. Ef ekki er tilgreint hvaða þjónustu átt er við, eða ef undirkaflinn heitir „Almennar kröfur“, þá eiga kröfurnar við almenna starfsemi vottunarstöðvar Auðkennis.

Kröfunum er lýst með öryggismarkmiðum sem síðan er fylgt eftir með ítarlegri kröfum um stýringar til að uppfylla öryggismarkmiðin.

7.1 Yfirlýsing um framkvæmd vottunar

Auðkenni gefur út yfirlýsingu um framkvæmd og verklag sem kallast *Yfirlýsing Auðkennis um framkvæmd vottunar fyrir skilríki gefin út undir Fullgildu auðkenni*.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

a) Tilgreinir í yfirlýsingu um framkvæmd vottunar hvernig kröfum í vottunarstefnu þessari er fylgt.

b) Tilgreinir í yfirlýsingu um framkvæmd vottunar skyldur samstarfsaðila Auðkennis þar á meðal viðeigandi stefnureglur og framkvæmdir.

c) Veitir áskrifendum og treystendum aðgang að yfirlýsingu um framkvæmd vottunar og öðrum viðeigandi skjölum að því marki sem nauðsynlegt er svo mögulegt sé að meta samræmi við vottunarstefnuna. Auðkenni mun ekki opinbera öll atriði varðandi framkvæmd vottunar.

d) Birtir skilmála og skilyrði er varða notkun rafrænna skilríkja eins og tilgreint er í kafla 7.3.4 fyrir öllum áskrifendum og væntanlegum treystendum.

e) Reglustjórn Auðkennis ber ábyrgð á yfirlýsingu um framkvæmd vottunar og hefur endanlegt vald til að samþykkja hana.

f) Reglustjórn Auðkennis er ábyrg fyrir því að framkvæmd vottunar sé á öllum tímum í samræmi við þessa vottunarstefnu.

g) Skilgreinir úttektarferli fyrir framkvæmd vottunar sem felur meðal annars í sér ábyrgð á viðhaldi yfirlýsingar um framkvæmdina.

h) Tilkynnir um fyrirhugaðar breytingar á yfirlýsingu um framkvæmd vottunar með nægum fyrirvara. Áskrifendum og treystendum verður veittur aðgangur að nýrri yfirlýsingu um framkvæmd vottunar, eftir að hún hefur verið samþykkt af reglustjórn Auðkennis. Takmarkanir verða á aðgengi að nýrri yfirlýsingu um framkvæmd vottunar í samræmi við c)-lið hér fyrir ofan.

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

7.2 Dreifilyklaskipulag - lífsskeið lyklaumsjónar

Meðhöndlun lykla hjá Auðkenni tekur mið af ETSI TS 102 176-1 [14] sem inniheldur lista yfir viðurkennd dulmálsalgrím ásamt kröfum um færibreytur þeirra.

7.2.1 Framleiðsla lykla Auðkennis

Framleiðsla skilríkja

Auðkenni framleiðir einkalykla sína, sem notaðir eru til að undirrita skilríki, í stýrðu umhverfi. Í því skyni mun Auðkenni uppfylla eftirfarandi kröfur:

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

a) Einkalyklar Auðkennis eru framleiddir í raunlægt (*physically*) öruggu umhverfi (sjá kafla 7.4.4) af einstaklingum í trúnaðarstöðum (sjá kafla 7.4.3) með tvískiptri stjórnun, að lágmarki. Fjölda þeirra einstaklinga sem hafa heimild til að framleiða einkalykla er haldið í lágmarki og í samræmi við verklag hjá vottunarstöðinni.

b) Einkalyklar Auðkennis eru framleiddir í dulmálseiningu sem:

   i. uppfyllir að lágmarki kröfurnar í FIPS 140-2 [9] stig 3 (*level 3*), eða

   ii. uppfyllir kröfurnar í CWA 14167-2 [11], CWA 14167-3 [12] eða CWA 14167-4 [13], eða

   iii. er áreiðanlegt kerfi sem staðfest er að uppfylli að lágmarki EAL 4 í samræmi við ISO/IEC 15408 [10], eða jafngilt öryggisviðmið. Kerfið er hluti af öryggismarkmiði eða verndunarsniðum sem uppfylla kröfurnar í þessu skjali og byggja á áhættugreiningu þar sem tekið er mið af raunlægum öryggisráðstöfunum auk annarra öryggisráðstafana sem ekki eru tæknilegar.

c) Einkalyklar Auðkennis eru framleiddir með algrími sem er í samræmi við viðurkenndar venjur fyrir undirritun vottunarstöðvar á skilríkjum samkvæmt ETSI TS 102 176-1 [14].

d) Lengd og algrím fyrir undirskriftarlykil Auðkennis er eins og í samræmi við viðurkenndar venjur fyrir undirritun vottunarstöðvar á skilríkjum, sbr. ETSI TS 102 176-1 [14].

e) Auðkenni framleiðir nýtt lyklapar fyrir undirritun skilríkja og gerir allar 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 Auðkenni

Framleiðsla skilríkja

Auðkenni tryggir að einkalyklar þess haldist leyndir og að heilleiki þeirra varðveitist.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

a) Einkalyklar Auðkennis fyrir undirritun skilríkja eru varðveittir í dulmálseiningu sem:

   i. uppfyllir að lágmarki kröfurnar í FIPS 140-2 [9] stig 3 (*level 3*), eða

   ii. uppfyllir kröfurnar í CWA 14167-2 [11], CWA 14167-3 [12] eða CWA 14167-4 [13], eða

   iii. er áreiðanlegt kerfi sem staðfest er að uppfylli að lágmarki EAL 4 í samræmi við ISO/IEC 15408 [10], eða jafngilt öryggisviðmið. Kerfið er hluti af öryggismarkmiði eða verndunarsniðum sem uppfylla kröfurnar í þessu skjali og byggja á áhættugreiningu þar sem tekið er mið af raunlægum öryggisráðstöfunum auk annarra öryggisráðstafana sem ekki eru tæknilegar.

b) Ef einkalykill Auðkennis fyrir undirritun er utan undirskriftarbúnaðar er einkalykilinn verndaður á þann hátt sem veitir sömu verndun og fæst með dulmálsbúnaðinum, samanber kröfur í a).

c) Vistun, öryggisafritun og endurheimt á einkalykli Auðkennis fyrir undirritun er framkvæmt í raunlægt öruggu umhverfi (sjá kafla 7.4.4) af einstaklingum í trúnaðarstöðum (sjá kafla 7.4.3) með tvískiptri stjórnun, að lágmarki. Fjölda þeirra einstaklinga sem hafa heimild til að framkvæma þessa aðgerð er haldið í lágmarki.

d) Auðkenni beitir sambærilegum öryggisstýringum við meðhöndlun öryggisafrita af einkalyklum Auðkennis fyrir undirritun og beitt er við meðhöndlun lykla 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 Auðkennis á dreifilyklum

Framleiðsla og miðlunarþjónusta

Auðkenni tryggir að heilleika og áreiðanleika dreifilykilsins, sem notaður er til að sannprófa undirskrift skilríkja, og tengdra færibreyta sé viðhaldið við dreifingu til treystenda.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

a) Dreifilykill Auðkennis, sem notaður er til að sannprófa undirskrift skilríkja, er aðgengilegur treystendum á þann hátt að treystendur geti fullvissað sig um heilleika hans og fengið uppruna hans sannvottaðan.

7.2.4 Vörsluafrit lykla

a) Einkalykill vottorðshafans er ekki geymdur hjá Auðkenni á þann hátt að hægt sé að nota hann sem afrit til dulráðningar.

b) Auðkenni varðveitir ekki afrit af lykli vottorðshafa.

7.2.5 Notkun á einkalykli Auðkennis

Auðkenni sér til þess að einkalyklar vottunarstöðvarinnar séu ekki notaðir á óviðeigandi hátt.

Framleiðsla skilríkja

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

a) Auðkenni sér til þess að einkalyklar vottunarstöðvarinnar 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) Auðkenni sér til þess að undirskriftarlyklar skilríkja séu aðeins notaðir í raunlægt öruggum húsakynnum samkvæmt 7.4.4.

7.2.6 Endalok lífskeiðs einkalykla Auðkennis

Einkalykill Auðkennis sem notaður er til undirritunar á skilríkjum hefur tiltekinn gildistíma. Auðkenni mun ekki nota einkalykillinn eftir að gildistími hans er liðinn.

Framleiðsla skilríkja

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

a) Notkun samsvarandi einkalykils Auðkennis afmarkast við þá notkun sem samræmist því tætialgrími, því undirskriftaralgrími og þeirri lengd undirskriftarlykla sem notuð eru í framleiðsluskilríkinu og samræmist viðurkenndum venjum, samanber d)-lið kafla 7.2.1.

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

7.2.7 Umsjón dulmálsvélbúnaðar fyrir undirritun skilríkja á lífsskeiði hans

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

Framleiðsla skilríkja

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

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

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

c) Að meðferð á undirskriftarlyklum Auðkennis í dulmálsvélbúnaði, þar með talin uppsetning, gangsetning, afritun og endurreisn eftir áfall, sé í samstilltri stjórnun að lágmarki tveggja einstaklinga í trúnaðarstöðum.

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

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

7.2.8 Umsjón Auðkennis með lyklum vottorðshafa

Auðkenni sér til þess að lyklar vottorðshafa séu framleiddir á öruggan hátt og að leynd yfir einkalykli vottorðshafa verði ávallt tryggð.

Framleiðsla skilríkja

Þegar lyklar vottorðshafa eru framleiddir hjá vottunarstöðinni þá uppfyllir Auðkenni sérstaklega eftirfarandi kröfur:

a) Lyklar vottorðshafa eru framleiddir með algrími sem er í samræmi við viðurkenndar venjur fyrir þá notkun skilríkjanna sem tilgreind er í vottunarstefnu þessari, samanber ETSI TS 102 176-1 [14].

b) Lyklar vottorðshafa eru af þeirri lengd og fyrir notkun með þeim dreifilyklaalgrímum sem eru í samræmi við viðurkenndar venjur fyrir þá notkun, sem tilgreind er í vottunarstefnu þessari, samanber ETSI TS 102 176-1 [14].

c) Lyklar vottorðshafa eru framleiddir og varðveittir á öruggan hátt áður en þeir eru afhentir vottorðshafa.

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

e) Afrit af lyklum vottorðshafa verður ekki varðveitt hjá Auðkenni eða hjá öðrum aðila eftir afhendingu til vottorðshafa, samanber 7.2.4. Ef afrit af lyklum vottorðshafa verða til hjá vottunarstöðinni þá er þeim eytt.

7.2.9 Undirbúningur á öruggum notendabúnaði

Auðkenni afhendir öruggan notendabúnað til vottorðshafa og sér til þess að frágangur og afhending séu framkvæmd á öruggan hátt.

Afhending búnaðar vottorðshafa

Auðkenni uppfyllir sérstaklega eftirfarandi kröfur við afhendingu á öruggum notendabúnaði til vottorðshafa:

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

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) Virkjunargögn tengd öruggum notendabúnaði, eru útbúin á öruggan hátt og þeim dreift aðskilið frá notendabúnaði.

7.3 Dreifilyklaskipulag - lífsskeið skilríkjaumsjónar

7.3.1 Skráning vottorðshafa

Auðkenni sér til þess að þau gögn sem eiga að bera kennsl á áskrifanda skilríkja og vottorðshafa séu könnuð með viðeigandi hætti og að nöfn áskrifenda og vottorðshafa ásamt öðrum upplýsingum séu rétt færð inn. Auðkenni sér til þess að umsóknir um skilríki séu réttar, innihaldi allar upplýsingar sem krafist er og að umsóknir séu byggðar á gildu umboði þegar það á við.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

Skráningarþjónusta

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

b) Þegar vottorðshafi er annar en áskrifandi skilríkja er hann upplýstur um skyldur sínar í samræmi við kafla 6.2.

c) Auðkenni miðlar upplýsingum samkvæmt a) og b) liðum þannig að heilleiki þeirra sé varanlega tryggður. Upplýsingunum er miðlað á skýru og einföldu máli.

d) Auðkenni vottorðshafa eru staðfest um leið og skráning fer fram. Auðkenni aflar annað hvort beinna sannana eða vitnisburðar frá viðeigandi og réttmætum aðilum um auðkenni (eins og nafn),og ef við á, tiltekin eigindi vottorðshafa. Framlögð gögn geta verið hvort sem er rafræn skjöl eða skjöl á pappír.

e) Framlögð gögn um auðkenni vottorðshafa (t.d. nafn hans), eða önnur einkenni vottorðshafans eins og tengsl við lögaðila, eru annað hvort borin saman við einstaklinginn í eigin persónu eða staðfest á óbeinan hátt með aðferðum sem veita sömu fullvissu og nærvera einstaklingsins á skráningarstöð. Nafn og kennitölu vottorðshafa skal staðfesta með framvísun á vegabréfi, ökuskírteini eða nafnskírteini þegar vottorðshafi mætir á skráningarstöð í eigin persónu.

f) Við útgáfu einkaskilríkja eru eftirfarandi auðkenni vottorðshafa staðfest:

   i. Fullt nafn og kennitala vottorðshafa samkvæmt þjóðskrá.

g) Við útgáfu starfsskilríkja eða annarra skilríkja þar sem vottorðshafi er einstaklingur sem auðkenndur er í tengslum við lögpersónu, fyrirtæki, stofnun eða félag (sem áskrifanda skilríkja) eru eftirfarandi auðkenni og einkenni staðfest:

   i. Fullt nafn og kennitala vottorðshafa samkvæmt þjóðskrá.

   ii. Fullt nafn, kennitala og lagaleg staða áskrifanda skilríkja (t.d. fyrirtæki, deild í fyrirtæki eða opinber stofnun).

   iii. Fullt nafn og kennitala lögbærs fulltrúa áskrifanda skilríkja samkvæmt þjóðskrá og lagaleg staða hans.

   iv. Tengsl vottorðshafa og lögbærs fulltrúa við áskrifanda skilríkja.

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

i) Ef annar aðili en vottorðshafinn er áskrifandi skilríkjanna hjá Auðkenni skal færa sönnur á að áskrifandinn hafi heimild vottorðshafa til að sækja um skilríki fyrir hönd vottorðshafans.

j) Áskrifandi skilríkja skal gefa upp lögheimili, tölvupóstfang eða aðrar upplýsingar sem gefa til kynna hvernig unnt sé að hafa samband við hann.

k) Auðkenni skjalfestir undirritað samkomulag við áskrifanda skilríkja, þar með talið:

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

   ii. Samkomulag við áskrifanda skilríkja um notkun á öruggum notendabúnaði ef vottunarstöðin krefst þess að slíkur búnaður sé notaður.

   iii. Samþykki áskrifanda fyrir varðveislu Auðkennis á upplýsingum sem notaðar eru við skráningu, afhendingu búnaðar hvort sem er til vottorðshafa eða áskrifanda skilríkja og við afturköllun (sjá kafla 7.4.11). Einnig samþykki fyrir varðveislu á auðkenni og sérhverjum eigindum sem sett eru í skilríkin og miðlun þessara upplýsinga til annarra aðila með þeim skilyrðum sem krafist er í þessari vottunarstefnu ef Auðkenni hættir starfsemi.

   iv. Hvort, og þá með hvaða skilyrðum, áskrifandi skilríkja krefst útgáfu skilríkja og vottorðshafi samþykkir útgáfu skilríkjanna.

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

l) Auðkenni varðveitir upplýsingar sem tilgreindar eru í þessum kafla eins lengi og nauðsynlegt er í þeim tilgangi að veita sönnun á vottun fyrir dómstólum þar sem Auðkenni hefur staðfestu. Auðkenni upplýsir áskrifendur skilríkja um hvaða upplýsingar verða geymdar og hversu lengi.

m) Auðkenni krefst ekki sönnunar á auðkenni umfram það sem nauðsynlegt er til að uppfylla þær þarfir sem notkun skilríkjanna miðast við.

7.3.2 Endurnýjun, uppfærsla og endurlyklun skilríkja

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

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

Skráningarþjónusta

a) Auðkenni staðfestir að þau skilríki sem beðið er um endurnýjun á séu til, að þau séu gild, og að þær upplýsingar sem lágu til grundvallar sannprófun á auðkenni og eigindum vottorðshafa séu enn réttar.

b) Ef einhverjar breytingar verða á skilmálum eða skilyrðum Auðkennis mun Auðkenni miðla þeim til áskrifanda skilríkjanna og gera samkomulag í samræmi við kafla 7.3.1.

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

d) Auðkenni gefur ekki út ný skilríki með dreifilykli vottorðshafa sem áður var vottaður nema staðfest sé að dulritunaröryggi skilríkjanna sé enn nægjanlegt yfir gildistíma nýju skilríkjanna og að engar vísbendingar séu um að trausti til einkalykils vottorðshafans hafi verið stofnað í hættu.

7.3.3 Framleiðsla skilríkja

Auðkenni sér til þess að útgáfa rafrænna skilríkja, ekki síst fullgildra, sé framkvæmd á öruggan hátt til að viðhalda áreiðanleika þeirra.

Innihald skilríkja er í samræmi við viðmið í *Innihald rafrænna skilríkja* [7].

Framleiðsla skilríkja

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

a) Skilríkin skulu innihalda eftirfarandi:
   i. Þegar skilríkin eru gefin út sem fullgild: Vísbendingu um að skilríkin séu gefin út sem fullgild skilríki.
   ii. Auðkenni vottunarstöðvar og þess lands þar sem vottunarstöð Auðkennis hefur lögfestu.
   iii. Nafn vottorðshafa eða gervinafn sem skal auðkennt sem slíkt.
   iv. Ef fyrirhuguð notkun skilríkjanna er þannig þá skal gera ráðstafanir fyrir sérstök eigindi fyrir undirritanda.
   v. Dreifilykil sem samsvarar einkalykli vottorðshafans.
   vi. Upphaf og enda gildistíma skilríkjanna.
   vii. Raðnúmer skilríkjanna.
   viii. Rafræna undirskrift vottunarstöðvarinnar sem gefur skilríkin út.
   ix. Útfærða rafræna undirskrift vottunarstöðvarinnar sem gefur skilríkin út.
   x. Takmörkun á notagildi skilríkjanna, ef það á við.
   xi. Takmörkun á upphæð þeirra fjárfærslu sem nota má skilríkin fyrir, ef það á við.

b) Auðkenni gerir ráðstafanir til að koma í veg fyrir fölsun á skilríkjum og ábyrgist trúnað við framleiðslu einkalykils vottorðshafa ef hann er framleiddur hjá vottunarstöðinni.

c) Auðkenni sér til þess að útgáfa skilríkjanna sé tengd á öruggan hátt við tilsvarandi skráningu, endurnýjun, uppfærslu eða endurlyklun skilríkja, þar með talið ráðstafanir vegna dreifilykla sem framleiddir eru hjá vottorðshafa.

d) Við framleiðslu lyklapars vottorðshafa, sjá kafla 7.2.8, mun Auðkenni uppfylla eftirfarandi kröfur:

   i. Skjalfesta verklagsreglur fyrir framleiðslu og afhendingu á lyklapari vottorðshafa sem tryggir að útgáfa skilríkjanna er tengd framleiðslu lyklaparsins á öruggan hátt.

   ii. Afhenda skráðum vottorðshafa einkalykilinn á öruggan hátt.

   iii. Afhenda skráðum vottorðshafa öruggan notendabúnað eða undirskriftarbúnað sem inniheldur einkalykil vottorðshafans á öruggan hátt.

e) Auðkenni sér til þess að auðkennandi nafn (*distinguished name*) sem notað er í skilríkjum sé ekki notað til að auðkenna annan aðila.

f) Auðkenni verndar trúnað og heilleika skráningargagna, sérstaklega þegar þeim er miðlað til áskrifenda og vottorðshafa og þegar þeim er miðlað á milli dreifðra kerfishluta vottunarstöðvarinnar.

g) Auðkenni nýtir sér ytri skráningarstöðvar og sannprófar að samskipti með skráningargögn séu einungis við viðurkenndar skráningarstöðvar þar sem auðkenni þeirra er vottað.

7.3.4 Miðlun á skilmálum og skilyrðum

Auðkenni sér til þess að skilmálar og skilyrði séu aðgengileg fyrir áskrifendur og treystendur.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

a) Auðkenni hefur eftirfarandi skilmála og skilyrði sem varða notkun skilríkjanna aðgengilega fyrir áskrifendur og treystendur sem reiða sig á skilríkin:

   i. Vottunarstefnu þessa.

   ii. Takmarkanir í 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 treystandi geti á raunhæfan hátt reitt sig á skilríkin (sjá kafla 6.3).

   v. Takmarkanir á skaðabótaskyldu, þar með talið þá afmörkun á notkun eða tilgangi skilríkjanna sem Auðkenni 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 fyrir meðhöndlun kvartana og sáttagerð í deilumálum.

   ix. Viðeigandi lagaumhverfi.

   x. Hvort vottunarstöð Auðkennis hefur verið metin með hliðsjón af samræmi við þessa vottunarstefnu, og þá hvernig.

b) Auðkenni miðlar upplýsingum í a)-lið á varanlegan hátt þannig að heilleiki þeirra er tryggður yfir tíma. Upplýsingunum er miðlað á skýru og einföldu máli.

7.3.5 Miðlun skilríkja

Auðkenni hefur skilríkin aðgengileg fyrir áskrifendur, vottorðshafa og treystendur sem reiða sig á skilríkin.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

Miðlunarþjónusta

a) Þegar skilríki hafa verið framleidd eru þau aðgengileg, í heild sinni og nákvæmlega, fyrir áskrifandann eða vottorðshafann sem skilríkin eru gefin út fyrir.

b) Skilríki verða ekki aðgengileg fyrir treystendur sem reiða sig á skilríkin fyrr en samþykki vottorðshafans liggur fyrir.

c) Auðkenni hefur skilmála og skilyrði sem varða notkun skilríkjanna aðgengileg fyrir treystendur sem reiða sig á skilríkin.

d) Upplýsingarnar sem tilgreindar eru í b) og c) lið eru aðgengilegar allan sólarhringinn sjö daga vikunnar um allan heim. Ef bilun verður í kerfi eða búnaði sem Auðkenni hefur ekki stjórn á, þá gerir Auðkenni 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

Auðkenni afturkallar rafræn skilríki svo fljótt sem auðið er ef beiðni um um afturköllun er staðfest og kemur frá aðila sem hefur heimild til þess að biðja um afturköllun.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

Afturköllunarþjónusta

a) Auðkenni hefur skjalfestar verklagsreglur fyrir afturköllun á skilríkjum sem hluta af yfirlýsingu um framkvæmd vottunar. Þessar verklagsreglur innihalda meðal annars eftirfarandi atriði:

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

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

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

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

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

   vi. Hámarkstíma 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. Þessi hámarks tími skal vera 24 klst.

b) Auðkenni afgreiðir tilkynningar og beiðnir sem tengjast afturköllun 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) Auðkenni staðfestir hvort tilkynningar og beiðnir sem tengjast afturköllun eru með heimild og af réttum uppruna. Slíkar tilkynningar og beiðnir eru staðfestar í samræmi við verklagsreglur Auðkennis.

d) Auðkenni má ógilda skilríki tímabundið á meðan afturköllun er staðfest og skal sjá til þess að skilríki séu ekki ógilt af þessum ástæðum lengur en nauðsynlegt er til að staðfesta stöðu þess.

e) Auðkenni tilkynnir vottorðshafa og áskrifanda þeirra skilríkja sem hafa verið afturkölluð eða ógild tímabundið 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 Auðkenni birtir eru gefnir út ekki sjaldnar en með 24 klst. millibili.

h) Ef einungis afturköllunarlistar (CRL) eða breytingarlistar (e. delta CRL) eru notaðir til að veita upplýsingar um afturköllunarstöðu þá uppfylla þeir eftirfarandi:

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

   ii. Heimilt er að gefa út nýjan afturköllunarlista áður en komið er að tilgreindum útgáfutíma.

   iii. Afturköllunarlistinn er undirritaður af vottunarstöð Auðkennis eða af öðrum aðila sem Auðkenni tilgreinir.

i) Afturköllunarlistar eru í samræmi við kröfur í ISO/IEC 9594-8|ITU-T X.509 [15].

j) Afturköllunarþjónusta Auðkennis er aðgengileg allan sólarhringinn sjö daga vikunnar. Ef rof verður á afturköllunarþjónustu af ástæðum sem Auðkenni hefur ekki stjórn á þá reynir Auðkenni eftir fremsta megni að

sjá til þess að þjónustan sé aðgengileg aftur innan þeirra tímamarka sem tilgreind eru í yfirlýsingu um framkvæmd vottunar.

Stöðumiðlun

k) Upplýsingar um stöðu skilríkja eru aðgengilegar allan sólarhringinn sjö daga vikunnar um allan heim. Ef rof verður á stöðumiðlun af ástæðum sem Auðkenni hefur ekki stjórn á þá reynir Auðkenni 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) Auðkenni verndar heilleika upplýsinga um stöðu skilríkja og áreiðanleika uppruna þeirra.

m) Stöðumiðlun inniheldur upplýsingar um stöðu skilríkjanna að minnsta kosti þar til gildistími þeirra rennur út.

7.4 Stjórnun og rekstur vottunarstöðvar Auðkennis

7.4.1 Stjórnun upplýsingaöryggis

Auðkenni viðhefur verklagsreglur í stjórnun og rekstri vottunarstöðvarinnar sem eru fullnægjandi með hliðsjón af starfsemi og í samræmi við ÍST ISO/IEC 27002 [16].

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

Almennar kröfur til vottunarstöðva

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

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

d) Auðkenni hefur á að skipa skilvirku stjórnkerfi upplýsingaöryggis í samræmi við líkan sem gefið er í ÍST ISO/IEC 27001 [17]. Stjórnkerfi upplýsingaöryggis Auðkennis fullnægir þeim kröfum sem settar eru í ÍST ISO/IEC 27001 [17] fyrir þá vottunarþjónustu sem Auðkenni veitir. Varðandi starfsvenjur fyrir stjórnun upplýsingaöryggis er tekið mið af ÍST ISO/IEC 27002 [16].

e) Auðkenni viðhefur ætíð nauðsynlegt skipulag á upplýsingaöryggi til að stjórna öryggi í starfsemi vottunarstöðvarinnar. Stjórnendur Auðkennis samþykkja allar breytingar sem hafa áhrif á það öryggisstig sem veitt er.

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

g) Auðkenni sért til þess að öryggi upplýsinga sé viðhaldið þegar ábyrgð á starfsþáttum Auðkennis er útvistað til annars fyrirtækis eða aðila.

7.4.2 Eignastjórnun

Auðkenni heldur uppi viðeigandi vernd fyrir eignir og upplýsingar fyrirtækisins.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

Almennar kröfur til vottunarstöðva

a) Auðkenni heldur eignaskrá yfir allar upplýsingaeignir og tiltekur verndarstig fyrir þessar eignir í samræmi við áhættugreiningu.

7.4.3 Mannauður og öryggi

Aðferðir Auðkennis við starfsmannahald og ráðningu eru ætíð þannig að þær auka og styðja áreiðanleika starfseminnar.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

Almennar kröfur til vottunarstöðva

a) Auðkenni mun ávallt hafa 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) Auðkenni beitir viðeigandi viðurlögum við brotum starfsmanna á stefnureglum eða verklagsreglum vottunarstöðvarinnar.

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

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

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

Skráning, framleiðsla skilríkja, afhending búnaðar vottorðshafa, afturköllunarþjónusta

f) Stjórnendur Auðkennis hafa sérfræðiþekkingu 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 Auðkennis í trúnaðarstarfi eru lausir við stríðandi hagsmuni sem gætu skaðað hlutleysi í starfseminni.

h) Trúnaðarstörf eru meðal annars eftirfarandi ábyrgðarstörf:

   i. Öryggisstjórar: Bera heildarábyrgð á stjórnun á framkvæmd 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 áreiðanlegra 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 áreiðanlegum kerfum vottunarstöðvarinnar.

i) Starfsmenn Auðkennis sem gegna trúnaðarstörfum eru skipaðir formlega í það hlutverk.

j) Einstaklingar sem hafa verið dæmdir fyrir alvarlega glæpi eða önnur brot sem áhrif geta haft á getu þeirra til að gegna trúnaðarstarfi fyrir Auðkenni eru ekki skipaðir í trúnaðar- eða stjórnunarstöðu. Starfsmenn sinna ekki trúnaðarstörfum eða hafa réttindi sem slíkir fyrr en nauðsynlegum athugunum er lokið. Auðkenni aflar samþykkis viðkomandi starfsmanns áður en slíkar athuganir eru gerðar.

7.4.4 Raunlægt öryggi og umhverfisöryggi

Raunlægum aðgangi að mikilvægri þjónustu vottunarstöðvar Auðkennis er stýrt með það að markmiði að halda raunlægri áhættu fyrir eignir Auðkennis í lágmarki.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

Almennar kröfur til vottunarstöðva

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

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

c) Auðkenni 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 varið er með raunlægum vörunum gegn hættu vegna aðgangs óviðkomandi aðila án heimilda, að búnaði, kerfum eða gögnum.

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

f) Raunlægar varnir byggja á skýrt skilgreindum öryggismærum (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) Auðkenni viðhefur öryggisstýringar sem vernda stoðkerfi húsrýma, kerfisbúnað og aðstöðu fyrir upplýsingavinnslu. Öryggis- og umhverfisstefna Auðkennis 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 endurreisnar á starfsemi eftir stóráföll.

h) Auðkenni viðhefur stýringar sem koma í veg fyrir að búnaður, upplýsingar, miðlar og hugbúnaður sem tengist þjónustu vottunarstöðvar Auðkennis sé fjarlægður úr aðstöðu vottunarstöðvarinnar án heimildar.

7.4.5 Stjórnun á samskiptum og rekstri

Auðkenni sér til þess að rekstur á búnaði og kerfum vottunarstöðvar sé öruggur og samkvæmt viðurkenndum aðferðum sem eru eins og best verður á kosið, þannig að áhætta á bilunum eða óhöppum sé í lágmarki.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

Almennar kröfur til vottunarstöðva

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

b) Auðkenni reynir að lágmarka skaða vegna öryggisatvika og bilana með verklagsreglum um tilkynningar og viðbrögð við atvikum.

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

d) Verklagsreglur Auðkennis fyrir umsjón gagnamiðla vernda þá gegn úreldingu og hrörnun yfir það tímabil sem viðhalda þarf skrám.

e) Auðkenni 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) Auðkenni hefur eftirlit með rýmdarþörf og viðheldur áætlun um framtíðarþarfir í þeim tilgangi að sjá til þess að vinnsluafl og geymslurými sé ávallt nægilegt.

Tilkynningar á atvikum og viðbrögð

h) Auðkenni mun bregðast strax við atvikum og takmarka 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) Auðkenni viðhefur 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 Auðkennis er aðgreindur frá almennum rekstri. Öryggisstjóri ber ábyrgð á öryggisrekstri sem 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.

   Öryggisstjóri Auðkennis 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 Auðkennis er takmarkaður við einstaklinga með réttar heimildir.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

Almennar kröfur til vottunarstöðva

a) Auðkenni útfærir virkar varnir (m.a. eldveggi) sem 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 ekki eru trygg.

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

d) Auðkenni sér til þess að aðgangur að upplýsingum og notendakerfum sé takmarkaður í samræmi við stefnu um aðgangsstýringu og að kerfi Auðkennis 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 vottaðir áður en þeir nota mikilvægan notendahugbúnað fyrir umsjón með skilríkjum.

f) Starfsmenn Auðkennis eru ábyrgir fyrir gerðum sínum, og skulu halda atburðaskrá (sjá kafla 7.4.11).

g) Viðkvæm gögn, eins og skráningargögn, eru vernduð þannig að ekki er unnt að afhjúpa þau (til dæmis skrár sem búið er að eyða) þegar aflagður gagnageymslubúnaður er aðgengilegur notendum sem hafa ekki heimild.

Framleiðsla skilríkja

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

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

Miðlun

j) Notendakerfi fyrir miðlunarþjónustu stýrir aðgangi til að koma í veg fyrir tilraunir til að bæta við eða eyða skilríkjum og breyta öðrum tengdum upplýsingum.

Afturköllunarþjónusta

k) Auðkenni býr yfir sívakandi eftirlits- og viðvörunarkerfum til að hægt sé að skynja, skrá og bregðast tímanlega við sérhverri óheimilli eða óeðlilegri tilraun til að fá aðgang að tilföngum.

Stöðumiðlun

l) Notendakerfi fyrir stöðumiðlun 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

Auðkenni notar áreiðanleg kerfi og búnað sem varinn er fyrir breytingum. Kerfi og búnaður hafa fullnægjandi verndarsnið í samræmi við ISO/IEC 15408 [10] eða samsvarandi kröfur.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

a) Auðkenni sér til þess að greindar séu öryggiskröfur fyrir hönnun og kröfulýsingu í sérhverju kerfisþróunarverkefni á vegum vottunarstöðvar Auðkennis, eða fyrir þess hönd, til að öryggi sé innbyggt í upplýsingakerfin.

b) Auðkenni hefur skjalfest stjórnkerfi fyrir útgáfu, breytingar og neyðaruppfærslur rekstrarkerfa og búnaðar.

7.4.8 Stjórnun á rekstrarsamfellu og umsjón með upplýsingaöryggisatvikum

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

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

Almennar kröfur til vottunarstöðva

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

Öryggisafritun kerfisgagna vottunarstöðvarinnar og endurheimt

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

c) Öryggisafritun og endurheimt eru framkvæmd af einstaklingi í trúnaðarstarfi eins og tilgreint er í kafla 7.4.3.

Einkalykli vottunarstöðvar stofnað í hættu

d) Áætlun Auðkennis um rekstrarsamfellu (eða neyðaráætlun) tekur á öryggisbresti eða gruni um slíkan brest varðandi einkalykla vottunarstöðvarinnar sem alvarlegu áfalli og eru undirbúnir ferlar til staðar.

e) Eftir alvarlegt áfall gerir Auðkenni ráðstafanir til að koma í veg fyrir að áfallið endurtaki sig.

Stöðumiðlun

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

   i. Upplýsa eftirfarandi aðila um öryggisbrestinn: Alla áskrifendur og aðra samningsbundna aðila og aðra samstarfsaðila sem vottunarstöðin er í samstarfi við, þar með talið þá sem treysta á öryggi í starfsemi vottunarstöðvarinnar og aðrar vottunarstöðvar. Þessar upplýsingar eru jafnframt gerðar aðgengilegar fyrir aðra aðila sem treysta á öryggi í starfsemi vottunarstöðvarinnar.

   ii. Gefa til kynna að skilríki og upplýsingar um stöðu þeirra sem gefin hafa verið út með lykli vottunarstöðvarinnar gætu verið ógild.

Öryggisbrestur í algrími

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

   i. Upplýsa alla áskrifendur og þá samningsbundnu aðila sem treysta á öryggi í starfsemi Auðkennis og aðra aðila sem Auðkenni er í samstarfi við. Þessar upplýsingar eru jafnframt gerðar aðgengilegar fyrir aðra aðila sem treysta á öryggi í starfsemi Auðkennis.

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

7.4.9 Lokun þjónustu

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

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

Almennar kröfur til vottunarstöðva

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

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

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

   iii. Framkvæma nauðsynlegar aðgerðir til að yfirfæra skuldbindingar varðandi viðhald skráningarupplýsinga (sjá kafla 7.3.1), upplýsinga um afturköllunarstöðu (sjá kafla 7.3.6) og geymslu á atburðarskráningu (sjá kafla 7.4.11) í þann tíma sem tilgreindur er til áskrifenda og treystenda (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) Auðkenni hefur ávallt aðgang að fjármagni til að uppfylla ofangreindar lágmarkskröfur þó svo að til gjaldþrots komi eða ef Auðkenni verður af öðrum ástæðum ófært um að bera þann kostnað.

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

   i. Tilkynningar til allra aðila sem stöðvunin snertir.

   ii. Yfirfærsla skuldbindinga Auðkennis 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

Auðkenni hlítir öllum þeim kröfum sem gerðar eru til fyrirtækisins í lögum.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

Almennar kröfur til vottunarstöðva

a) Auðkenni uppfyllir allar lögboðnar kröfur sem við eiga um verndun skráa frá glötun, eyðileggingu og fölsun. Sum skjöl gæti þurft að varðveita á öruggan hátt til að uppfylla lögboðnar kröfur jafnframt því að styðja við grundvallar viðskiptahætti (sjá kafla 7.4.11).

b) Auðkenni fer, við meðferð persónuupplýsinga, að lögum nr. 77/2000 um persónuvernd og meðferð persónuupplýsinga [4].

c) Auðkenni gerir viðeigandi tæknilegar og skipulagslegar ráðstafanir gegn óheimilli eða ólöglegri vinnslu persónuupplýsinga og gegn glötun eða eyðileggingu á eða skemmd á persónuupplýsingum.

d) Upplýsingar sem áskrifendur leggja fram til vottunarstöðvar Auðkennis eru varðaveittar með öruggum hætti og þær eru ekki birtar nema með samþykki áskrifandans, með dómsúrskurði eða með öðrum lagaheimildum.

7.4.11 Skráning upplýsinga

Auðkenni sér til þess að allar viðkomandi upplýsingar varðandi vottunarþjónustu (þar með talið skráningarupplýsingar og upplýsingar varðandi atburði í umhverfi, lyklaumsjón og skilríkjaumsjón) eru skráðar og varðveittar yfir viðeigandi tímabil, sérstaklega í þeim tilgangi að geta fært sönnur á vottun í málarekstri fyrir dómstólum.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

Almennar kröfur til vottunarstöðva

a) Trúnaði og heilleika bæði virkra og safnvistaðra skráa varðandi skilríkjaútgáfu er viðhaldið.

b) Skrár varðandi skilríki eru safnvistaðar í heild sinni og undir trúnaði í samræmi við almennar viðskiptavenjur.

c) Skrár varðandi skilríki eru gerðar tiltækar ef þess er krafist í þeim tilgangi 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 það tímabil sem tilgreint er í skilmálum og skilyrðum í samningum (sjá kafla 7.3.4) til að veita sannanir til að styðja rafrænar undirskriftir í samræmi við þau lög sem um ræðir.

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

g) Auðkenni tilgreinir hvaða sérstöku atburði skuli skrá í atburðaskrá og hvernig.

Skráning

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

i) Auðkenni sér til þess að allar skráningarupplýsingar, þar með talið eftirfarandi, eru skráðar:

   i. Tegund þeirra skjala sem umsækjandi lagði 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 samningi 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) Auðkenni sér til þess að friðhelgi upplýsinga um vottorðshafa er viðhaldið.

Framleiðsla skilríkja

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

l) Auðkenni skráir alla atburði sem tengjast lífsskeiði skilríkja.

Afhending búnaðar vottorðshafa

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

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

Afturköllunarþjónusta

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

7.5 Skipulag

Auðkenni sér til þess að starfsemi vottunarstöðva sem félagið rekur sé áreiðanleg.

Sérstaklega uppfyllir Auðkenni eftirfarandi kröfur:

Almennar kröfur til vottunarstöðva

a) Auðkenni vinnur eftir óhlutdrægum stefnureglum og verklagi.

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

c) Auðkenni er löglega skráð fyrirtæki.

d) Auðkenni hefur nægjanlegar tryggingar til að bera skaðabótakröfur vegna starfsemi sinnar eða athafna.

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

f) Auðkenni sér til þess að til séu stefnureglur og verkferlar til að leysa úr kvörtunum sem berast og deilum sem koma upp við viðskiptavini eða aðra aðila um veitingu á rafrænni traustþjónustu eða vegna annarra skyldra mála.

g) Auðkenni skjalfestir með viðeigandi hætti það samkomulag eða þá samninga sem byggt er á þeim tilvikum þegar þjónusta hennar kallar á framlag undirverktaka, útvistunaraðila eða annarra ytri aðila.

h) Auðkenni hefur stjórnkerfi fyrir gæði og upplýsingaöryggi sem er viðeigandi fyrir þá vottunarþjónustu sem í boði er.

Framleiðsla skilríkja, afturköllunarþjónusta

i) Sá hluti Auðkennis sem sér um framleiðslu skilríkja og afturköllunarþjónustu er óháður öðrum fyrirtækjum hvað varðar ákvarðanir sem tengjast stofnun, veitingu, viðhaldi 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 Auðkenni veitir.

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