Nr. 780 16. ágúst 2011

REGLUGERÐ

um rafrænar undirskriftir.

I. KAFLI
Gildissvið og skilgreiningar.

1. gr.
Gildissvið.

Reglugerð þessi tekur til upplýsinga sem fullgild vottorð skulu hafa að geyma, krafna til vottunaraðila sem gefa út fullgild vottorð, krafna til öruggs undirskriftarbúnaðar, tilhögunar skráningar, tilkynningar og upplýsingagjafar vottunaraðila og tilhögunar eftirlits með starfsemi vottunaraðila sem gefa út fullgild vottorð.

Rafræn undirskrift sem gerð er með fullgildu vottorði er ekki staðfesting á tímamarki undirritunar.

2. gr.
Skilgreiningar.

Merking eftirfarandi hugtaka í reglugerð þessari er sem hér segir:

Vottunarstefna: Safn af reglum sem skilgreina nothæfni vottorða á tilteknu notkunarsviði og/eða tæknilegum lausnum þar sem öryggiskröfur eru sambærilegar. Í vottunarstefnu kemur fram hvernig stefnt er að því að standa að útgáfu og meðferð rafrænna vottorða. Í vottunarstefnu eru einnig settar reglur um þær kröfur sem gerðar eru til öryggis og eftirlits.

Vottunaraðili: Aðili sem gefur út vottorð eða þriðji aðili sem starfar að útgáfu fullgildra vottorða á hans vegum og á hans ábyrgð, sbr. 17. gr. laga nr. 28/2001 um rafrænar undirskriftir eða veitir aðra þjónustu í tengslum við rafrænar undirskriftir.

Um skilgreiningar á hugtökum fer að öðru leyti eftir ákvæðum laga nr. 28/2001.

II. KAFLI
Um innihald fullgilds vottorðs.

3. gr.
Um innihald og upplýsingar fullgilds vottorðs.

Heimilt er að tilgreina að vottorð sé fullgilt, uppfylli vottorðið ákvæði 7. gr. laga nr. 28/2001 og sé gefið út af vottunaraðila sem uppfyllir ákvæði V. kafla laganna sem og skilyrði reglna sem settar eru á grundvelli laganna.

Í fullgildu vottorði ber að hafa læsilegt orðið *fullgilt*. Jafnframt skal vísa til þess að vottorðið uppfyllir ákvæði laga og reglna sem gilda um útgáfu fullgildra vottorða.

Vottorð teljast fullnægja kröfum þessarar greinar, uppfylli þau skilyrði staðla og annarra samþykktra kröfuskjala, sem talin eru upp í viðauka I við reglugerð þessa.

4. gr.
Kennitala og nafn undirritanda.

Í fullgildu vottorði útgefnu hér á landi skal, á sérstöku nafnasvæði vottorðsins, tilgreina fullt nafn undirritanda úr þjóðskrá eða dulnefni.

Í fullgildu vottorði útgefnu hér á landi skal, á sérstöku númerasvæði vottorðsins, tilgreina kennitölu undirritanda. Hafi undirritandi ekki lögheimili hér á landi skal tilgreina sambærilegt einkvæmt númer sem úthlutað er af þjóðskrá samkvæmt reglum sem um þá úthlutun gilda á hverjum tíma.

Noti undirritandi dulnefni í fullgildu vottorði skal koma skýrt fram í vottorðinu að um dulnefni sé að ræða. Vottunaraðili sannreynir deili á undirritanda sem notar dulnefni og tengingu hans við dulnefnið, sbr. nánar ákvæði 14. gr. þessarar reglugerðar.

5. gr.
Viðbótarupplýsingar.

Í fullgildu vottorði er unnt að veita frekari upplýsingar um undirritanda en þær sem tilgreindar eru í 4. gr., s.s. að vottorðið sé jafnframt starfsskilríki og tilgreina nánar stöðuumboð þess sem undirritar, eða nánari lýsingu á tegund þeirrar undirritunar sem heimilt er að gera með hlutaðeigandi vottorði. Um gildi undirskrifta samkvæmt þessari grein fer eftir almennum reglum um stöðuumboð og afturköllun þeirra.

6. gr.
Sannprófun á fullgildri rafrænni undirskrift.

Í fullgildu vottorði skulu vera sannprófunargögn sem svara til undirskriftargagna sem undirritandi hefur forræði yfir og sem notuð eru til að sannreyna rafræna undirskrift hans.

7. gr.
Gildistími vottorða og afturköllun.

Í fullgildu vottorði skal koma fram upphaf og lok gildistíma vottorðsins. Um afturköllunarþjónustu vottunaraðila fer samkvæmt ákvæðum III. kafla í reglugerð þessari.

8. gr.
Auðkenniskóti vottorðs.

Öll fullgild vottorð skulu hafa einkvæmt númer sem er auðkenniskóti vottorðsins þannig að með því sé ávallt hægt að bera kennsl á vottorðið.

9. gr.
Upplýsingar um vottunaraðila.

Til að unnt sé að sannreyna að fullgilt vottorð stafi frá vottunaraðila skal í vottorðinu koma fram útfærð rafræn undirskrift útgefanda þess.

10. gr.
Takmarkanir á notkun fullgildra vottorða.

Fullgild vottorð eru án takmarkana við rafrænar undirskriftir nema slíkar takmarkanir hafi verið gerðar sérstaklega

Vottunaraðili sem vill setja takmarkanir á gildissvið fullgildra vottorða eða fjárhæð viðskipta sem unnt er að nota vottorðið til, skal setja upplýsingar um slíkar takmarkanir í vottorðið.

III. KAFLI
Kröfur til vottunaraðila, skráningar- og afturköllunarþjónusta, o.fl.

11. gr.
Kröfur til vottunaraðila sem gefa út fullgild vottorð.

Vottunaraðili sem gefur út fullgild vottorð skal í starfsemi sinni tryggja örugga og áreiðanlega útgáfu fullgildra vottorða og haga starfsemi sinni að öllu leyti í samræmi við ákvæði laga nr. 28/2001 og reglur sem settar eru á grundvelli þeirra.

Vottunaraðila ber að viðhafa vandaðar stjórnunar- og starfsaðferðir. Í því skyni skal hann m.a. útbúa gæða- og öryggishandbók þar sem settar eru fram verklagsreglur og vinnulýsingar fyrir starfsemina.

Þá skal vottunaraðili útbúa þjálfunaráætlun til að tryggja að starfsmenn er starfa á ábyrgð vottunaraðila við útgáfu fullgildra vottorða, búi yfir nægjanlegri hæfni og hljóti viðeigandi þjálfun í samræmi við verkefna- og ábyrgðarsvið þeirra.

Vottunaraðili skal tryggja að eigið fé og fjármögnun á skuldbindingum hans varðandi starfsemina, sé fullnægjandi, þannig að tekið sé mið af:

a. Áætlaðri stærð viðskiptamannahóps og tekjustreymi starfseminnar,
b. hvort takmarkanir séu varðandi notkun fullgildra vottorða,
c. áætlaðri bótaskyldu vottunaraðila.

Vottunaraðili skal framkvæma reglulega innri úttektir í samræmi við gæða- og öryggisstjórnunarreglur sem hann notar í starfsemi sinni.

Vottunaraðili skal vegna c-liðar 4. mgr. þessarar greinar leggja fram upplýsingar um hver sé áætluð heildarfjárhæð skaðabóta, hvort einhver takmörkun sé gerð varðandi lágmarksábyrgð vottunaraðila í hverju einstöku tjónstilviki fyrir sig og hvort aflað hafi verið starfsábyrgðartryggingar vegna starfseminnar. Upplýsingar samkvæmt þessari málsgrein svo og breytingar á þeim skulu sendar Neytendastofu.

12. gr.

Kerfi og búnaður.

Vottunaraðili skal í starfsemi sinni nota áreiðanleg kerfi og búnað sem eru varin gegn breytingum og tryggja öryggi dulritunar og tæknilegt öryggi.

Ákvæðum 1. mgr. telst fullnægt ef vottunaraðili notar kerfi og búnað sem viðurkennd eru skv. 9. gr. laga nr. 28/2001.

Vottunaraðili skal grípa til aðgerða til að hindra möguleika á fölsun fullgildra vottorða. Vottunaraðili sem útbýr undirskriftargögn skal tryggja leynd við framleiðsluna.

13. gr.

Skráningar- og afturköllunarþjónusta.

Vottunaraðili sem gefur út fullgild vottorð skal koma á fót og starfrækja hraðvirkt og öruggt kerfi fyrir skráningu og afturköllun á fullgildum vottorðum. Upplýsingar um afturkölluð fullgild vottorð skal uppfæra eigi sjaldnar en daglega.

Vottunaraðili skal tryggja að unnt sé að sjá nákvæmlega hvenær vottorð tók gildi, hvenær það var afturkallað og hvenær það var skráð á afturköllunarlista.

Vottunaraðili skal jafnframt skrá og hafa aðgengilegar upplýsingar um takmarkanir á gildi fullgildra vottorða, s.s. takmarkanir á gildissviði og fjárhæð viðskipta sem unnt er að nota vottorðið til, séu slíkar takmarkanir fyrir hendi.

14. gr.

Kennsl borin á undirritanda.

Vottunaraðili sem gefur út fullgild vottorð, eða aðili sem starfar á hans ábyrgð og í umboði hans, skal við upphaf viðskipta sannreyna deili á undirritanda og aðrar frekari upplýsingar um hann sem skylt er að skrá samkvæmt reglugerð þessari.

Undirritandi skal við fyrstu afhendingu fullgilds vottorðs hjá vottunaraðila, eða þeim sem starfar í hans umboði við afhendingu fullgildra vottorða, sanna á sér deili með framvísun:

a. Vegabréfs; eða
b. ökuskírteinis; eða
c. nafnskírteinis sem útgefið er af Þjóðskrá Íslands.

15. gr.

Geymsla upplýsinga.

Vottunaraðili skal nota áreiðanleg kerfi við geymslu á fullgildum vottorðum þannig að:

a. Enginn geti gert breytingar eða viðbætur á fullgildum vottorðum nema þeir sem til þess hafa sérstaka heimild,
b. unnt sé að athuga hvort upplýsingar eru réttar,
c. fullgilt vottorð sé eingöngu aðgengilegt almenningi ef undirritandi hefur samþykkt það sérstaklega, og
d. hugsanlegar tæknilegar breytingar, sem geta stefnt öryggiskröfum í hættu, séu sýnilegar þeim sem starfrækja kerfið.

Fullgild vottorð skulu geymd þannig að unnt sé að sannprófa þau. Vottunaraðilanum er ekki heimilt að geyma eða afrita undirskriftargögn undirritanda.

Vottunaraðili skal varðveita afrit fullgildra persónuskilríkja, sem framvísað er samkvæmt 14. gr., á öruggan og aðgengilegan hátt.

Varðveisluskylda gagna um einstaklinga og lögaðila, sem auðkenndir hafa verið vegna útgáfu fullgildra vottorða, er 20 ár frá því að fullgilt vottorð er fellt úr gildi. Nánar um varðveislu og skilaskyldu gagna fer að öðru leyti eftir lögum sem gilda um varðveislu slíkra gagna á hverjum tíma.

16. gr.

Vottunarstefna.

Vottunaraðili skal birta vottunarstefnu á aðgengilegan hátt, þar með taldar allar upplýsingar um framkvæmd og tilhögun auðkenningar einstaklinga og lögaðila sem fram fer á hans vegum, vegna útgáfu fullgildra vottorða.

Í vottunarstefnu vottunaraðila skal koma fram með hvaða hætti hann notar kerfi sem uppfyllir ákvæði 15. gr. og hvernig hann tryggir varðveislu gagna þannig að ávallt sé unnt að sannprófa gögn fullgildra vottorða, einkum til þess að mögulegt sé að leggja fram sönnunargögn um vottun í málarekstri fyrir dómstólum.

Auk þess skal í vottunarstefnu koma fram hvernig varðveislu gagna skuli háttað ef nýr aðili tekur yfir rekstur vottunaraðila eða önnur ófyrirséð atvik koma til, s.s. að starfseminni er hætt eða rekstur stöðvast á annan hátt.

17. gr.

Um ábyrgð vottunaraðila.

Um ábyrgð vottunaraðila fer samkvæmt ákvæðum VI. kafla laga nr. 28/2001.

18. gr.

Upplýsingar um skilmála, meðferð kvartana o.fl.

Vottunaraðili skal veita viðskiptavinum, sem gera samning um útgáfu fullgilds vottorðs, skriflega og með varanlegum hætti upplýsingar í samræmi við ákvæði 15. gr. laga nr. 28/2001.

Vottunaraðili sem býður upp á meðferð kvartana og úrlausn deilumála utan dómstóla skal birta málsmeðferðarreglur á aðgengilegan hátt. Neytendastofa skal staðfesta málsmeðferðarreglur og gæta að því að þar sé fylgt meginreglum um aðila sem vinna að úrlausn deilumála utan dómstóla.

IV. KAFLI
Öruggur undirskriftarbúnaður.

19. gr.

Grunnkröfur um öryggi undirskriftarbúnaðar, leynd og vörn gagna.

Fullgild rafræn undirritun er því aðeins gild sé hún gerð með öruggum undirskriftarbúnaði sem uppfyllir grunnkröfur laga nr. 28/2001 og studd fullgildu vottorði.

Öruggur undirskriftarbúnaður skal tryggja að undirskriftargögnin:

a. Geti eingöngu komið einu sinni fram,
b. verði með hliðsjón af eðlilegum öryggiskröfum ekki brotin upp, og
c. séu varin með fullnægjandi hætti gegn notkun annarra en undirritanda.

Öruggur undirskriftarbúnaður skal einnig tryggja leynd undirskriftargagnanna með fullnægjandi hætti og að rafræn undirskrift sé varin gegn fölsun.

Ekki skal vera unnt að nota öruggan undirskriftarbúnað til að breyta þeim gögnum sem undirrita á, eða hindra að undirritandi geti séð gögnin fyrir undirritun.

20. gr.

Staðlar og önnur kröfuskjöl.

Undirskriftarbúnaður telst fyrirfram ávallt öruggur samkvæmt ákvæðum þessarar greinar ef hann er í samræmi við staðla og önnur kröfuskjöl sem framkvæmdastjórn Evrópusambandsins hefur ályktað um og gefið út tilvísanir til og birtar eru í Stjórnartíðindum Evrópusambandsins. Lista yfir nöfn staðla og önnur kröfuskjöl er að finna í viðauka við reglugerð þessa. Ráðherra uppfærir listann að tillögu Neytendastofu.

21. gr.
Viðurkenning á undirskriftarbúnaði.

Kröfum til undirskriftarbúnaðar samkvæmt 19. og 20. gr. reglugerðar þessarar telst fullnægt þegar hann hefur fengið staðfestingu frá þar til bærum aðila um að hann uppfylli kröfur 8. gr. laga nr. 28/2001, sbr. a- og b-lið 1. mgr. 9. gr. sömu laga.

Um skilyrði fyrir tilnefningu þar til bærs aðila samkvæmt þessari grein gilda viðmiðanir sem kveðið er á um í ákvörðun framkvæmdastjórnar ESB nr. 2000/709/EB um lágmarksviðmiðanir sem aðildarríkin skulu taka tillit til þegar þau tilnefna aðila í samræmi við 4. mgr. 3. gr. tilskipunar Evrópuþingsins og ráðsins 1999/93/EB um ramma bandalagsins varðandi rafrænar undirskriftir. Ráðherra getur auk þess kveðið nánar á um þá aðila sem veitt geta staðfestingu samkvæmt þessari grein.

Neytendastofa kannar upplýsingar um og staðfestingar á að úttekt og vottun undirskriftarbúnaðar uppfylli grunnkröfur, staðla og önnur samþykkt kröfuskjöl í samræmi við ákvæði þessarar reglugerðar og hafi verið gerð af þar til bærum aðila sem uppfyllir skilyrði þessarar greinar. Neytendastofa getur óskað eftir gögnum og upplýsingum sem hún telur nauðsynlegar til þess að leggja mat á hæfni, hæfi og sjálfstæði aðila sem annast frumúttektir og reglulegar úttektir samkvæmt ákvæðum þessarar reglugerðar.

V. KAFLI
Skráning, eftirlitsgjald og eftirlit með vottunaraðilum sem gefa út fullgild vottorð.

22. gr.
Skráning.

Vottunaraðili sem hyggst gefa út fullgild vottorð skal senda tilkynningu um starfsemi sína til Neytendastofu.

Tilkynningu um starfsemi vottunaraðila skulu fylgja öll gögn og upplýsingar sem Neytendastofa telur nauðsynlegar vegna eftirlitsins. Upphafstilkynningu skulu ávallt að lágmarki fylgja eftirtalin gögn:

1. Formlegar upplýsingar um tilkynnanda:
   - 1.1 Skráningarvottorð hlutafélagaskrár eða hlutaðeigandi skráningaraðila félagsins.
   - 1.2 Afrit af samþykktum félagsins og upplýsingar um stjórn þess.
2. Upplýsingar um fjárhagslegan grundvöll fyrir starfsemi:
   - 2.1 Yfirlýsing endurskoðanda þar sem m.a. kemur fram að áætlanir og gögn sýni að nægjanlegt fjármagn sé til staðar. Eftirtalin gögn skulu m.a. lögð fram til að styðja þetta:
     - 2.1.1 Stofnefnahagsreikningur og ársreikningar undangenginna tveggja ára ef þeir liggja fyrir.
     - 2.1.2 Rekstraráætlun ársins.
     - 2.1.3 Lýsing á fjármögnun til lengri tíma þar sem fram kemur hvernig tryggja eigi tekjustreymi til að standa undir þeirri starfsemi sem tilkynnt er, a.m.k. til næstu 3-5 ára, sem og aðrar nauðsynlegar upplýsingar um viðskiptaáætlun vottunaraðila.
     - 2.1.4 Afrit af starfsábyrgðartryggingu.
3. Skipulag starfseminnar:
   - 3.1 Yfirlýsing um framkvæmd vottunar.
   - 3.2 Vottunarstefna.
   - 3.3 Öryggisstefna.
   - 3.4 Afrit af áskriftarsamningi við undirritendur og upplýsingar um takmarkanir á notkun fullgildra vottorða, ef við á.
   - 3.5 Upplýsingar um stjórnunar- og starfsaðferðir, þar sem fram kemur hvernig tryggja eigi vandaða stjórnunarhætti, og skipulag starfseminnar, þ.m.t upplýsingar um öryggismál og með hvaða hætti rekstrarsamfella sé tryggð í starfseminni. Framangreindum upplýsingum skal fylgja yfirlit um gæða- og öryggisstjórnunarkerfi starfseminnar s.s. gæðahandbók með helstu verklagsreglum og vinnulýsingum og öðrum skjölum er máli skipta varðandi stjórnunar- og starfsaðferðir vottunaraðilans.

3.6 Þjálfunaráætlun þar sem finna má m.a. grunnkröfur til menntunar starfsmanna og upplýsingar um það með hvaða hætti vottunaraðili aflar staðfestingar á hæfni starfsmanna.

4. Kerfi og búnaður:

4.1 Kerfis- og búnaðarlýsingar.

4.1.1 Kröfur og verklagsreglur um það hvernig kennsl eru borin á undirritanda.

4.2.1 Upplýsingar um örugg geymslukerfi og sannprófun gagna.

4.2 Yfirlit og upptalning á stöðlum og önnur kröfuskjöl sem farið er eftir.

4.3 Upplýsingar um innra eftirlit.

4.4 Staðfesting þar til bærs aðila um að kröfum til öruggs undirskriftarbúnaðar teljist fullnægt, sbr. 8. og 9. gr. laga nr. 28/2001.

Vottunaraðili skal senda Neytendastofu án tafar upplýsingar um allar breytingar varðandi starfsemina og aðrar uppfærslur á gögnum samkvæmt 2.1.4 og 3.-4. tölul. 2. mgr. þessarar greinar.

Vottunaraðili skal jafnframt afhenda allar þær upplýsingar og skýringar til Neytendastofu sem hún telur nauðsynlegar vegna eftirlitsins.

Neytendastofa getur samþykkt beiðni um að tiltekin gögn samkvæmt þessari grein skuli aðeins vera aðgengileg eftirlitinu á starfsstöð vottunaraðila ef um er að ræða mikilvæg trúnaðarskjöl sem leynt eiga að fara og af öryggisástæðum þykir ekki rétt að afhenda.

23. gr.

Eftirlitsgjald.

Vottunaraðili sem gefur út fullgild vottorð skal greiða gjald í samræmi við ákvæði laga hverju sinni til að standa straum af kostnaði vegna eftirlitsins.

24. gr.

Eftirlit Neytendastofu.

Neytendastofa hefur eftirlit með starfsemi vottunaraðila. Um eftirlit, málsmeðferð, stjórnvaldsúrræði og viðurlög fer nánar eftir ákvæðum laga nr. 28/2001. Neytendastofa getur krafist þess að fram fari endurskoðun á kerfi, búnaði og starfsskipulagi vottunaraðila sem gefa út fullgild vottorð. Neytendastofa tilnefnir þá aðila sem hafa heimild til að annast slíka endurskoðun. Vottunaraðili skal bera kostnað af slíkri endurskoðun.

VI. KAFLI

Gildistaka o.fl.

25. gr.

Reglugerð þessi er sett með stoð í 2. mgr. 7. gr., a-lið 1. mgr. 9. gr., 16. gr., 9. mgr. 18. gr. og 4. mgr. 19. gr. laga nr. 28/2001, um rafrænar undirskriftir og öðlast hún þegar gildi.

Efnahags- og viðskiptaráðuneytinu, 16. ágúst 2011.

F. h. r.

Helga Jónsdóttir.

Kjartan Gunnarsson.

VIÐAUKI

Tilvísun til staðla og annarra samþykktra kröfuskjala um innihald fullgildra vottorða og öruggan undirskriftarbúnað.

1. Staðlar og önnur samþykkt kröfuskjöl um innihald fullgildra vottorð.

1.1. ETSI TS 101 862 v1.3.1 (2004-03*): Sniðmát fullgilds vottorðs.* Á ensku: ETSI TS 101 862 v1.3.1 (2004-03): *Qualified Certificate Profile.*

2. Staðlar og önnur kröfuskjöl um vottunaraðila og almennt viðurkenndan og öruggan undirskriftarbúnað, sbr. ákvörðun framkvæmdastjórnar ESB nr. 2003/511/EB.

2.1. Almennt viðurkennd kröfuskjöl um örugg kerfi og vörur sem ekki er hægt að breyta og tryggja tæknilegt öryggi og öryggi dulkóðunar og sem fyrirfram telst uppfylla grunnkröfur:

2.1.1. CWA 14167-1 (March 2003): *Öryggiskröfur fyrir áreiðanleg kerfi sem annast vottorð fyrir rafrænar undirskriftir — Hluti 1: Öryggiskröfur*. Á ensku: CWA 14167-1 (March 2003): *security requirements for trustworthy systems managing certificates for electronic signatures — Part 1: System Security Requirements.*

2.1.2. CWA 14167-2 (March 2002): *Öryggiskröfur fyrir áreiðanleg kerfi sem annast vottorð fyrir rafrænar undirskriftir — Hluti 2: Dulmálseining fyrir undirskriftaaðgerðir vottunaraðila — Verndunarsnið (MCSO-PP).* Á ensku: 14167-2 (March 2002): *security requirements for trustworthy systems managing certificates for electronic signatures — Part 2: cryptographic module for CSP signing operations — Protection Profile (MCSO-PP).*

2.2. Almennt viðurkennd kröfuskjöl um öruggan undirskriftarbúnað sem fyrirfram telst uppfylla grunnkröfur:

2.2.1. CWA 14169 (March 2002): *Öruggur undirskriftarbúnaður*. Á ensku: CWA 14169 (March 2002): *secure signature-creation devices.*

———

B-deild – Útgáfud.: 17. ágúst 2011