FRAMKVÆMDARREGLUGERÐ FRAMKVÆMDASTJÓRNARINNAR (ESB) 2015/1502 **2019/EES/101/09**

frá 8. september 2015

um að ákvarða lágmarkstækniforskriftir og -ferla varðandi fullvissustig fyrir rafrænar auðkenningarleiðir skv. 3. mgr. 8. gr. reglugerðar Evrópuþingsins og ráðsins (ESB) nr. 910/2014 um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti á innri markaðinum (*)

FRAMKVÆMDASTJÓRN EVRÓPUSAMBANDSINS HEFUR,

með hliðsjón af sáttmálanum um starfshætti Evrópusambandsins,

með hliðsjón af reglugerð Evrópuþingsins og ráðsins (ESB) nr. 910/2014 frá 23. júlí 2014 um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti á innri markaðinum og um niðurfellingu á tilskipun 1999/93/EB ([1]), einkum 3. mgr. 8. gr.,

og að teknu tilliti til eftirfarandi:

1) Í 8. gr. reglugerðar (ESB) nr. 910/2014 er kveðið á um að rafræn auðkenningarskipan, sem er tilkynnt skv. 1. mgr. 9. gr., þurfi að tilgreina fullvissustigin „lágt“, „verulegt“ og „hátt“ fyrir rafrænar auðkenningarleiðir sem gefnar eru út undir þeirri skipan.

2) Brýnt er að ákvarða lágmarkstækniforskriftir, -staðla og -ferla til að tryggja að sameiginlegur skilningur ríki um einstök atriði fullvissustiganna og tryggja samvirkni við vörpun á landsbundnum fullvissustigum tilkynntra rafrænna auðkenningarskipana við fullvissustigin skv. 8. gr. eins og kveðið er á um í b-lið 4. mgr. 12. gr. reglugerðar (ESB) nr. 910/2014.

3) Tekið hefur verið tillit til staðals ISO/IEC 29115 í sambandi við forskriftir og ferla sem sett eru fram í þessari framkvæmdargerð, þar sem hann er mikilvægasti alþjóðlegi staðallinn sem er fyrir hendi á sviði fullvissustiga fyrir rafrænar auðkenningarleiðir. Efni reglugerðar (ESB) nr. 910/2014 er þó frábrugðið þeim alþjóðlega staðli, einkum að því er varðar kröfur um sönnun og sannprófun á kennslum og einnig það með hvaða hætti tekið er tillit til mismunarins milli auðkennisfyrirkomulags aðildarríkja og þeirra tækja sem eru fyrir hendi í ESB með sama markmið. Því ætti viðaukinn, enda þótt hann sé byggður á þessum alþjóðlega staðli, ekki að vísa til tiltekins innihalds í staðli ISO/IEC 29115.

4) Þessi reglugerð hefur verið þróuð út frá árangurstengdri nálgun sem talin er eiga best við, sem endurspeglast líka í skilgreiningunum sem notaðar eru til að lýsa heitum og hugtökum. Í þeim er tekið tillit til markmiðs reglugerðar (ESB) nr. 910/2014 að því er varðar fullvissustig rafrænna auðkenningarleiða. Því ætti að taka ítrasta tillit til stóra tilraunaverkefnisins STORK, þ.m.t. forskrifta sem hafa verið þróaðar innan þess, sem og til skilgreininga og hugtaka í staðlinum ISO/IEC 29115, við ákvörðun forskrifta og ferla sem settar eru fram í þessari framkvæmdargerð.

5) Áreiðanlegar heimildir geta verið á margs konar formi, allt eftir því í hvaða samhengi sannprófa þarf þátt í sönnunargagni um kennsl einhvers, s.s. skrár, skjöl, stofnanir o.fl. Áreiðanlegar heimildir geta verið mismunandi eftir aðildarríkjum, jafnvel í svipuðu samhengi.

6) Kröfur um sönnun og sannprófun á kennslum ættu að taka tillit til mismunandi kerfa og starfsvenja, en tryggja jafnframt nægilega fullvissu til að skapa nauðsynlegt traust. Af þeim sökum ætti viðurkenning ferla, sem voru áður notaðir í öðrum tilgangi en við útgáfu rafrænna auðkenningarleiða, að vera háð staðfestingu á því að ferlarnir uppfylli kröfurnar sem gert er ráð fyrir um samsvarandi fullvissustig.

(*) Þessi ESB-gerð birtist í Stjtíð. ESB L 235, 9.9.2015, bls. 7. Hennar var getið í ákvörðun sameiginlegu EES-nefndarinnar nr. 242/2019 frá 27. september 2019 um breytingu á XI. viðauka (Rafræn fjarskipti, hljóð- og myndmiðlun og upplýsingasamfélagið) við EES-samninginn (bíður birtingar).

([1]) Stjtíð. ESB L 257, 28.8.2014, bls. 73.

7) Yfirleitt eru notaðir tilteknir sannvottunarþættir, s.s. leyndarmál sem miðlað er, hlutkenndur búnaður og líkamlegar eigindir. Þó ætti að hvetja til notkunar á fleiri sannvottunarþáttum, einkum úr ólíkum flokkum þátta, til að auka öryggi sannvottunarferlisins.

8) Reglugerð þessi ætti ekki að hafa áhrif á rétt lögaðila til fyrirsvars. Viðaukinn ætti þó að innihalda kröfur um tengingu milli rafrænna auðkenningarleiða einstaklinga og lögaðila.

9) Viðurkenna ætti mikilvægi upplýsingaöryggis- og þjónustustjórnkerfa, sem og mikilvægi þess að nota viðurkenndar aðferðir og beita þeim meginreglum, sem eru innbyggðar í staðla á borð við ISO/IEC 27000- og ISO/IEC 20000-raðirnar.

10) Einnig ætti að taka tillit til góðra starfsvenja í tengslum við fullvissustig í aðildarríkjunum.

11) Öryggisvottun í upplýsingatækni sem byggist á alþjóðlegum stöðlum er mikilvægt tæki til að sannreyna að vörur uppfylli öryggiskröfur þessarar framkvæmdargerðar.

12) Nefndin, sem um getur í 48. gr. reglugerðar (ESB) nr. 910/2014, skilaði ekki áliti innan þeirra tímamarka sem formaður hennar setti.

SAMÞYKKT REGLUGERÐ ÞESSA:

1. gr.

1. Fullvissustigin „lágt“, „verulegt“ og „hátt“ fyrir rafrænar auðkenningarleiðir sem gefnar eru út undir tilkynntri, rafrænni auðkenningarskipan skulu ákvörðuð á grundvelli þeirra forskrifta og ferla sem tilgreind eru í viðaukanum.

2. Nota skal forskriftirnar og ferlana sem tilgreind eru í viðaukanum til að tilgreina fullvissustig rafrænna auðkenningarleiða, sem gefnar eru út undir tilkynntri, rafrænni auðkenningarskipan, með því að ákvarða áreiðanleika og gæði eftirfarandi þátta:

a) skráningar, eins og fram kemur í lið 2.1 í viðaukanum við þessa reglugerð skv. a-lið 3. mgr. 8. gr. reglugerðar (ESB) nr. 910/2014,

b) stjórnunar rafrænna auðkenningarleiða, eins og fram kemur í lið 2.2 í viðaukanum við þessa reglugerð skv. b- og f-lið 3. mgr. 8. gr. reglugerðar (ESB) nr. 910/2014,

c) sannvottunar, eins og fram kemur í lið 2.3 í viðaukanum við þessa reglugerð skv. c-lið 3. mgr. 8. gr. reglugerðar (ESB) nr. 910/2014,

d) stjórnunar og skipulags, eins og fram kemur í lið 2.4 í viðaukanum við þessa reglugerð skv. d- og e-lið 3. mgr. 8. gr. reglugerðar (ESB) nr. 910/2014.

3. Ef rafræn auðkenningarleið, sem er gefin út undir tilkynntri, rafrænni auðkenningarskipan, uppfyllir kröfu sem tilgreind er fyrir hærra fullvissustig skal líta svo á að hún uppfylli sambærilega kröfu fyrir lægra fullvissustig.

4. Ef annað er ekki tekið fram í viðeigandi hluta viðaukans skal öllum þáttum, sem taldir eru upp í viðaukanum fyrir tiltekið fullvissustig rafrænnar auðkenningarleiðar sem gefin er út undir tilkynntri, rafrænni auðkenningarskipan, vera fullnægt til að hún teljist samsvara því fullvissustigi sem gert er tilkall til.

2. gr.

Reglugerð þessi öðlast gildi á tuttugasta degi eftir að hún birtist í *Stjórnartíðindum Evrópusambandsins*.

Reglugerð þessi er bindandi í heild sinni og gildir í öllum aðildarríkjunum án frekari lögfestingar.

Gjört í Brussel 8. september 2015.

Fyrir hönd framkvæmdastjórnarinnar,

Jean-Claude JUNCKER

forseti.

———

VIÐAUKI

Tækniforskriftir og ferlar varðandi fullvissustigin „lágt“, „verulegt“ og „hátt“ fyrir rafrænar auðkenningarleiðir sem gefnar eru út undir tilkynntri, rafrænni auðkenningarskipan

1. **Gildandi skilgreiningar**

Í þessum viðauka er merking eftirfarandi hugtaka sem hér segir:

1) „áreiðanleg heimild“: hvers konar heimild, óháð því á hvaða formi hún er, sem treysta má að veiti nákvæm gögn, upplýsingar og/eða sönnunargögn sem nota má til að sanna kennsl einhvers,

2) „sannvottunarþáttur“: þáttur sem staðfest er að tengist aðila og fellur undir einhvern af eftirfarandi flokkum:

   a) „sannvottunarþáttur sem byggist á umráðum“: sannvottunarþáttur sem viðkomandi þarf að geta sýnt fram á að hann hafi umráð yfir,

   b) „sannvottunarþáttur sem byggist á vitneskju“: sannvottunarþáttur sem viðkomandi þarf að geta sýnt fram á að hann hafi vitneskju um,

   c) „eðlislægur sannvottunarþáttur“: sannvottunarþáttur sem byggist á líkamlegri eigind einstaklings, þar sem einstaklingurinn þarf að sýna fram á að hann hafi til að bera þessa líkamlegu eigind,

3) „kvik sannvottun“: rafrænt ferli sem felur í sér leið til að skapa, með notkun dulritunar eða annarrar tækni, þegar krafist er, rafræna sönnun fyrir því að viðkomandi aðili hafi stjórn á eða umráð yfir auðkenningargögnunum og sem breytist við hverja sannvottunaraðgerð milli viðkomandi aðila og kerfisins sem sannprófar kennsl hans,

4) „stjórnkerfi upplýsingaöryggis“: röð aðferða og ferla sem ætlað er að stjórna áhættu í tengslum við upplýsingaöryggi þannig að hún sé viðunandi.

2. **Tækniforskriftir og ferlar**

Nota skal þá þætti tækniforskrifta og ferla, sem eru tilgreindir í þessum viðauka, til að ákvarða hvernig beita skuli kröfum og viðmiðunum í 8. gr. reglugerðar (ESB) nr. 910/2014 að því er varðar rafrænar auðkenningarleiðir sem eru gefnar út undir rafrænni auðkenningarskipan.

2.1. *Skráning (e. enrolment)*

2.1.1. Umsókn og skráning

Fullvissustig	Nauðsynlegir þættir
Lágt	1. Tryggt er að umsækjandinn geri sér ljóst hvaða skilmálar og skilyrði tengjast notkun rafrænu auðkenningarleiðarinnar. 2. Tryggt er að umsækjandinn geri sér ljóst hvaða öryggisráðstöfunum mælt er með í sambandi við rafrænu auðkenningarleiðina. 3. Viðeigandi kennigögnum (e. identity data), sem krafist er til sönnunar og sannprófunar á kennslum, er safnað.
Verulegt	Sama og fyrir stigið „lágt“.
Hátt	Sama og fyrir stigið „lágt“.

2.1.2. Sönnun og sannprófun á kennslum (einstaklingur)

Fullvissustig	Nauðsynlegir þættir
Lágt	1. Gera má ráð fyrir því að viðkomandi hafi umráð yfir sönnunargagni sem aðildarríkið, þar sem sótt er um rafræna auðkenningarleið, viðurkennir og sem stendur fyrir þau kennsl sem tilkall er gert til. 2. Gera má ráð fyrir að sönnunargagnið sé ósvikið eða að það sé til samkvæmt áreiðanlegri heimild og það virðist vera gilt. 3. Vitað er, samkvæmt áreiðanlegri heimild, að kennslin, sem tilkall er gert til, eru til og gera má ráð fyrir því að sá sem gerir tilkall til þeirra sé réttur aðili.
Verulegt	Stigið „lágt“ og að auki þarf einu af atriðunum, sem talin eru upp í 1.–4. lið, að vera fullnægt: 1. Sannprófað hefur verið að viðkomandi hafi umráð yfir sönnunargagni, sem aðildarríkið, þar sem sótt er um rafræna auðkenningarleið, viðurkennir og sem stendur fyrir þau kennsl sem tilkall er gert til og sönnunargagnið er athugað til að ákvarða að það sé ósvikið, eða vitað er, samkvæmt áreiðanlegri heimild, að það sé til og að það tengist raunverulegum einstaklingi og gerðar hafa verið ráðstafanir til að lágmarka hættu á að kennsl einstaklings séu önnur en þau sem hann gerir tilkall til, t.d. með tilliti til hættunnar á að sönnunargagn týnist, því sé stolið, það hafi verið ógilt tímabundið, afturkallað eða sé útrunnið eða 2. framvísað er persónuskilríkjum í skráningarferli í aðildarríkinu þar sem skilríkin voru gefin út og þau virðist eiga við einstaklinginn sem framvísar þeim og gerðar hafa verið ráðstafanir til að lágmarka hættu á að kennsl einstaklings séu önnur en þau sem hann gerir tilkall til, t.d. með tilliti til hættunnar á að skilríki týnist, þeim sé stolið, þau hafi verið ógilt tímabundið, afturkölluð eða séu útrunnin eða 3. ef ferlar, sem opinber aðili eða einkaaðili í sama aðildarríki hefur áður notað í öðrum tilgangi en að gefa út rafræna auðkenningarleið, veita jafna vissu og þeir sem settir eru fram í lið 2.1.2 fyrir fullvissustigið „verulegt“ þarf aðilinn sem ber ábyrgð á skráningu ekki að endurtaka þessa fyrri ferla, að því tilskildu að samræmismatsstofa, sem um getur í 13. mgr. 2. gr. reglugerðar Evrópuþingsins og ráðsins (EB) nr. 765/2008[1], eða jafngildur aðili staðfesti að slík vissa teljist jöfn eða 4. ef rafrænar auðkenningarleiðir eru gefnar út á grundvelli gildrar tilkynntrar, rafrænnar auðkenningarleiðar með fullvissustigið „verulegt“ eða „hátt“, og að teknu tilliti til hættunnar á breytingu á auðkenningargögnum aðila, er þess ekki krafist að ferli til sönnunar og sannprófunar á kennslum séu endurtekin. Hafi rafræna auðkenningarleiðin sem liggur til grundvallar ekki verið tilkynnt þarf samræmismatsstofa, sem um getur í 13. mgr. 2. gr. reglugerðar (EB) nr. 765/2008, eða jafngildur aðili að staðfesta fullvissustigið „verulegt“ eða „hátt“.

Fullvissustig	Nauðsynlegir þættir
Hátt	Fullnægja þarf kröfum annað hvort 1. eða 2. liðar: 1. Stigið „verulegt“ og að auki þarf einu af atriðunum, sem talin eru upp í a- til c-lið, að vera fullnægt: a) Ef sannprófað hefur verið að viðkomandi hafi umráð yfir sönnunargagni um kennsl með ljósmynd eða lífkenniupplýsingum, sem aðildarríkið, þar sem sótt er um rafræna auðkenningarleið, viðurkennir og sem stendur fyrir þau kennsl sem tilkall er gert til, er sönnunargagnið athugað til að ákvarða að það sé gilt samkvæmt áreiðanlegri heimild og kennslin, sem umsækjandinn gerir tilkall til, eru staðfest með því að bera eitt eða fleiri líkamleg einkenni hans saman við áreiðanlega heimild eða b) ef ferlar, sem opinber aðili eða einkaaðili í sama aðildarríki hefur áður notað í öðrum tilgangi en að gefa út rafræna auðkenningarleið, veita jafna vissu og þeir sem settir eru fram í lið 2.1.2 fyrir fullvissustigið „hátt“ þarf aðilinn sem ber ábyrgð á skráningu ekki að endurtaka þessa fyrri ferla, að því tilskildu að samræmismatsstofa, sem um getur í 13. mgr. 2. gr. reglugerðar (EB) nr. 765/2008, eða jafngildur aðili staðfesti að slík vissa teljist jöfn og gerðar eru ráðstafanir til að sýna fram á að niðurstöður þessara fyrri ferla séu enn gildar eða c) ef rafrænar auðkenningarleiðir eru gefnar út á grundvelli gildrar tilkynntrar, rafrænnar auðkenningarleiðar með fullvissustigið „hátt“, og með tilliti til hættunnar á breytingu á auðkenningargögnum aðila, er þess ekki krafist að ferli til sönnunar og sannprófunar á kennslum séu endurtekin. Hafi rafræna auðkenningarleiðin sem liggur til grundvallar ekki verið tilkynnt þarf samræmismatsstofa, sem um getur í 13. mgr. 2. gr. reglugerðar (EB) nr. 765/2008, eða jafngildur aðili að staðfesta fullvissustigið „hátt“ og gerðar eru ráðstafanir til að sýna fram á að niðurstöður þessa fyrra útgáfuferlis tilkynntrar, rafrænnar auðkenningarleiðar séu enn gildar. EÐA 2. Ef umsækjandinn framvísar ekki viðurkenndu sönnunargagni um kennsl með ljósmynd eða lífkenniupplýsingum er beitt nákvæmlega sömu verklagsreglum til að afla slíks sönnunargagns um kennsl með ljósmynd eða lífkenniupplýsingum og notaðar eru á landsvísu í aðildarríkinu þar sem stofnunin er sem ber ábyrgð á skráningu.

([1]) Reglugerð Evrópuþingsins og ráðsins (EB) nr. 765/2008 frá 9. júlí 2008 um kröfur varðandi faggildingu og markaðseftirlit í tengslum við markaðssetningu á vörum og um niðurfellingu reglugerðar (EBE) nr. 339/93 (Stjtíð. ESB L 218, 13.8.2008, bls. 30).

2.1.3. Sönnun og sannprófun á kennslum (lögaðili)

Fullvissustig	Nauðsynlegir þættir
Lágt	1. Sýnt er fram á að kennslin, sem lögaðilinn gerir tilkall til, eru hans á grundvelli sönnunargagns, sem aðildarríkið, þar sem sótt er um rafræna auðkenningarleið, viðurkennir.

Fullvissustig	Nauðsynlegir þættir
	2. Sönnunargagnið virðist vera gilt og gera má ráð fyrir að það sé ósvikið eða að það sé til samkvæmt áreiðanlegri heimild, ef lögaðilann er að finna í öruggu heimildinni af frjálsum vilja og það stjórnast af samkomulagi milli lögaðilans og öruggu heimildarinnar. 3. Samkvæmt öruggri heimild er ekki vitað til þess að staða lögaðilans sé slík að hún komi í veg fyrir að hann komi fram sem sá lögaðili.
Verulegt	Stigið „lágt“ og að auki þarf einu af atriðunum, sem talin eru upp í 1.–3. lið, að vera fullnægt: 1. Sýnt er fram á að kennslin, sem lögaðilinn gerir tilkall til, eru hans á grundvelli sönnunargagns, sem aðildarríkið, þar sem sótt er um rafræna auðkenningarleið, viðurkennir, þ.m.t. nafn lögaðilans, félagsform og (ef við á) skráningarnúmer hans og sönnunargagnið er athugað til að ákvarða hvort það er ósvikið eða hvort vitað er að það sé til samkvæmt áreiðanlegri heimild, ef lögaðila er að finna í öruggu heimildinni vegna þess að honum er það skylt til að geta starfað innan síns geira og gerðar hafa verið ráðstafanir til að lágmarka hættu á að kennsl lögaðila séu önnur en þau sem hann gerir tilkall til, t.d. með tilliti til hættunnar á að skjöl týnist, þeim sé stolið, þau hafi verið ógilt tímabundið, afturkölluð eða séu útrunnin eða 2. ef ferlar, sem opinber aðili eða einkaaðili í sama aðildarríki hefur áður notað í öðrum tilgangi en að gefa út rafræna auðkenningarleið, veita jafna vissu og þeir sem settir eru fram í lið 2.1.3 fyrir fullvissustigið „verulegt“ þarf aðilinn sem ber ábyrgð á skráningu ekki að endurtaka þessa fyrri ferla, að því tilskildu að samræmismatsstofa, sem um getur í 13. mgr. 2. gr. reglugerðar (EB) nr. 765/2008, eða jafngildur aðili staðfesti að slík vissa teljist jöfn eða 3. ef rafrænar auðkenningarleiðir eru gefnar út á grundvelli gildrar tilkynntrar, rafrænnar auðkenningarleiðar með fullvissustigið „verulegt“ eða „hátt“ er þess ekki krafist að ferli til sönnunar og sannprófunar á kennslum séu endurtekin. Hafi rafræna auðkenningarleiðin sem liggur til grundvallar ekki verið tilkynnt þarf samræmismatsstofa, sem um getur í 13. mgr. 2. gr. reglugerðar (EB) nr. 765/2008, eða jafngildur aðili að staðfesta fullvissustigið „verulegt“ eða „hátt“.
Hátt	Stigið „verulegt“ og að auki þarf einu af atriðunum, sem talin eru upp í 1.–3. lið, að vera fullnægt: 1. Sýnt er fram á að kennslin, sem lögaðilinn gerir tilkall til, eru hans á grundvelli sönnunargagns, sem aðildarríkið, þar sem sótt er um rafræna auðkenningarleið, viðurkennir, þ.m.t. nafn lögaðilans, félagsform og a.m.k. eitt einkvæmt kennimark sem stendur fyrir lögaðilann, sem notað er í viðkomandi aðildarríki og sönnunargagnið er athugað til að ákvarða að það sé gilt samkvæmt áreiðanlegri heimild eða

Fullvissustig	Nauðsynlegir þættir
	2. ef ferlar, sem opinber aðili eða einkaaðili í sama aðildarríki hefur áður notað í öðrum tilgangi en að gefa út rafræna auðkenningarleið, veita jafna vissu og þeir sem settir eru fram í lið 2.1.3 fyrir fullvissustigið „hátt“ þarf aðilinn sem ber ábyrgð á skráningu ekki að endurtaka þessa fyrri ferla, að því tilskildu að samræmismatsstofa, sem um getur í 13. mgr. 2. gr. reglugerðar (EB) nr. 765/2008, eða jafngildur aðili staðfesti að slík vissa teljist jöfn og gerðar eru ráðstafanir til að sýna fram á að niðurstöður þessa fyrra ferlis séu enn gildar eða 3. ef rafrænar auðkenningarleiðir eru gefnar út á grundvelli gildrar tilkynntrar, rafrænnar auðkenningarleiðar með fullvissustigið „hátt“ er þess ekki krafist að ferli til sönnunar og sannprófunar á kennslum séu endurtekin. Hafi rafræna auðkenningarleiðin sem liggur til grundvallar ekki verið tilkynnt þarf samræmismatsstofa, sem um getur í 13. mgr. 2. gr. reglugerðar (EB) nr. 765/2008, eða jafngildur aðili að staðfesta fullvissustigið „hátt“ og gerðar eru ráðstafanir til að sýna fram á að niðurstöður þessa fyrra útgáfuferlis tilkynntrar, rafrænnar auðkenningarleiðar séu enn gildar.

2.1.4. Tenging milli rafrænna auðkenningarleiða einstaklinga og lögaðila

Eftirfarandi skilyrði gilda um tengingu milli rafrænnar auðkenningarleiðar einstaklings og rafrænnar auðkenningarleiðar lögaðila (hér á eftir nefnd „tenging“):

1) Hægt skal vera að ógilda tímabundið og/eða afturkalla tengingu. Stjórna skal vistferli tengingar (t.d. virkjun, tímabundinni ógildingu, endurnýjun, afturköllun) samkvæmt verklagsreglum sem eru viðurkenndar á landsvísu.

2) Einstaklingur, sem er með rafræna auðkenningarleið sína tengda rafrænni auðkenningarleið lögaðila, getur framselt öðrum einstaklingi notkun tengingarinnar á grundvelli verklagsreglna sem eru viðurkenndar á landsvísu. Þó skal einstaklingurinn sem framselur tenginguna áfram vera ábyrgur.

3) Tenging skal fara fram á eftirfarandi hátt:

Fullvissustig	Nauðsynlegir þættir
Lágt	1. Sannprófað er að sönnun á kennslum einstaklingsins sem kemur fram fyrir hönd lögaðilans hefur farið fram á stiginu „lágt“ eða hærra. 2. Tengingunni hefur verið komið á á grundvelli verklagsreglna sem eru viðurkenndar á landsvísu. 3. Samkvæmt öruggri heimild er ekki vitað til þess að staða einstaklingsins sé slík að hún komi í veg fyrir að hann komi fram fyrir hönd lögaðilans.
Verulegt	3. liður stigsins „lágt“ og að auki: 1. Sannprófað er að sönnun á kennslum einstaklingsins sem kemur fram fyrir hönd lögaðilans hefur farið fram á stiginu „verulegt“ eða „hátt“.

Fullvissustig	Nauðsynlegir þættir
	2. Tengingunni hefur verið komið á á grundvelli verklagsreglna sem eru viðurkenndar á landsvísu sem leiddi til þess að tengingin var skráð í áreiðanlega heimild. 3. Tengingin hefur verið sannprófuð á grundvelli upplýsinga frá áreiðanlegri heimild.
Hátt	3. liður stigsins „lágt“ og í 2. liður stigsins „verulegt“ og að auki: 1. Sannprófað er að sönnun á kennslum einstaklingsins sem kemur fram fyrir hönd lögaðilans hefur farið fram á stiginu „hátt“. 2. Tengingin hefur verið sannprófuð á grundvelli einkvæms kennimarks, sem stendur fyrir lögaðilann og notað er í viðkomandi aðildarríki, og á grundvelli upplýsinga sem með einkvæmum hætti standa fyrir einstaklinginn og koma frá áreiðanlegri heimild.

2.2. *Stjórnun rafrænna auðkenningarleiða*

2.2.1. Eiginleikar og útfærsla rafrænna auðkenningarleiða

Fullvissustig	Nauðsynlegir þættir
Lágt	1. Rafræna auðkenningarleiðin notar a.m.k. einn sannvottunarþátt. 2. Útfærsla rafrænu auðkenningarleiðarinnar er þannig að útgefandinn gerir eðlilegar ráðstafanir til að ganga úr skugga um að hún sé einungis notuð undir stjórn þess aðila sem hún tilheyrir eða aðeins hann hafi umráð yfir henni.
Verulegt	1. Rafræna auðkenningarleiðin notar a.m.k. tvo sannvottunarþætti úr mismunandi flokkum. 2. Útfærsla rafrænu auðkenningarleiðarinnar er þannig að gera má ráð fyrir því að hún sé einungis notuð undir stjórn þess aðila sem hún tilheyrir eða aðeins hann hafi umráð yfir henni.
Hátt	Stigið „verulegt“ og að auki: 1. Rafræna auðkenningarleiðin veitir vernd gegn gerð afrits og fikti (e. tampering) og gegn árásarmönnum með mikla árásargetu. 2. Útfærsla rafrænu auðkenningarleiðarinnar er þannig að sá aðili sem hún tilheyrir getur með áreiðanlegum hætti verndað hana gegn því að aðrir noti hana.

2.2.2. Útgáfa, afhending og virkjun

Fullvissustig	Nauðsynlegir þættir
Lágt	Eftir að rafræna auðkenningarleiðin er gefin út er hún afhent með fyrirkomulagi sem er þannig að gera má ráð fyrir að hún berist aðeins þeim aðila sem hún er ætluð.
Verulegt	Eftir að rafræna auðkenningarleiðin er gefin út er hún afhent með fyrirkomulagi sem er þannig að gera má ráð fyrir að hún sé aðeins látin í hendur þeim aðila sem hún tilheyrir.
Hátt	Virkjunarferlið sannprófar að rafræna auðkenningarleiðin hafi aðeins verið látin í hendur þeim aðila sem hún tilheyrir.

2.2.3. Tímabundin ógilding, afturköllun og endurvirkjun

Fullvissustig	Nauðsynlegir þættir
Lágt	1. Hægt er að ógilda tímabundið og/eða afturkalla rafræna auðkenningarleið tímanlega og á skilvirkan hátt. 2. Fyrir hendi eru ráðstafanir til að koma í veg fyrir óheimila tímabundna ógildingu, afturköllun og/eða endurvirkjun. 3. Endurvirkjun skal aðeins fara fram ef sömu kröfum um fullvissu og settar voru fyrir tímabundnu ógildinguna eða afturköllunina er enn fullnægt.
Verulegt	Sama og fyrir stigið „lágt“.
Hátt	Sama og fyrir stigið „lágt“.

2.2.4. Endurnýjun og útskipti

Fullvissustig	Nauðsynlegir þættir
Lágt	Með tilliti til hættunnar á breytingu á auðkenningargögnum aðila þurfa endurnýjun eða útskipti að fullnægja sömu kröfum um fullvissu og upphafleg sönnun og sannprófun á kennslum eða byggjast á gildri, rafrænni auðkenningarleið með sama eða hærra fullvissustig.
Verulegt	Sama og fyrir stigið „lágt“.
Hátt	Stigið „lágt“ og að auki: Ef endurnýjun eða útskipti byggjast á gildri, rafrænni auðkenningarleið eru kennigögnin sannprófuð hjá áreiðanlegri heimild.

2.3. *Sannvottun*

Í þessum lið er áhersla lögð á ógnir í tengslum við notkun á sannvottunarferlinu og taldar upp kröfur fyrir hvert fullvissustig. Í þessum lið er gengið út frá því að eftirlitsráðstafanir séu í réttu hlutfalli við áhættu á tilteknu stigi.

2.3.1. Sannvottunarferli

Í eftirfarandi töflu eru settar fram kröfur fyrir hvert fullvissustig að því er varðar sannvottunarferlið sem notað er þegar einstaklingurinn eða lögaðilinn notar rafrænu auðkenningarleiðina til að staðfesta kennsl sín við treystanda.

Fullvissustig	Nauðsynlegir þættir
Lágt	1. Áður en auðkenningargögn aðila eru látin af hendi eru rafræna auðkenningarleiðin og gildi hennar sannprófuð með áreiðanlegum hætti. 2. Ef auðkenningargögn aðila eru vistuð sem hluti af sannvottunarferlinu eru þær upplýsingar varðar til að vernda þær gegn tapi og gegn því að þeim sé stofnað í hættu, þ.m.t. með greiningu utan nettengingar (e. analysis offline). 3. Sannvottunarferlið framkvæmir öryggiseftirlit til að sannprófa rafrænu auðkenningarleiðina, þannig að mjög ólíklegt er að aðgerðir á borð við ágiskun, hlerun, endursendingu eða misnotkun (e. manipulation) samskipta af hálfu árásaraðila með aukna grunngetu til árása geti spillt sannvottunarferlunum.

Fullvissustig	Nauðsynlegir þættir
Verulegt	Stigið „lágt“ og að auki: 1. Áður en auðkenningargögn aðila eru látin af hendi eru rafræna auðkenningarleiðin og gildi hennar sannprófuð með áreiðanlegum hætti með hjálp kvikrar sannvottunar. 2. Sannvottunarferlið framkvæmir öryggiseftirlit til að sannprófa rafrænu auðkenningarleiðina, þannig að mjög ólíklegt er að aðgerðir á borð við ágiskun, hlerun, endursendingu eða misnotkun samskipta af hálfu árásaraðila með meðalgetu til árása geti spillt sannvottunarferlunum.
Hátt	Stigið „verulegt“ og að auki: Sannvottunarferlið framkvæmir öryggiseftirlit til að sannprófa rafrænu auðkenningarleiðina, þannig að mjög ólíklegt er að aðgerðir á borð við ágiskun, hlerun, endursendingu eða misnotkun samskipta af hálfu árásaraðila með mikla getu til árása geti spillt sannvottunarferlunum.

2.4. *Stjórnun og skipulag*

Allir þátttakendur, sem veita þjónustu í tengslum við rafræna auðkenningu yfir landamæri („veitendur“) skulu hafa yfir að ráða skjalfestum starfsvenjum fyrir stjórnun upplýsingaöryggis, stefnum, aðferðum við áhættustýringu og öðrum viðurkenndum eftirlitsráðstöfunum til þess að veita viðeigandi stjórnunarstofnunum fyrir rafrænar auðkenningarskipanir í viðkomandi aðildarríkjum tryggingu fyrir því að skilvirkar starfsvenjur séu fyrir hendi. Í öllum lið 2.4 er gengið út frá því að allar kröfur/þættir séu í réttu hlutfalli við áhættu á tilteknu stigi.

2.4.1. Almenn ákvæði

Fullvissustig	Nauðsynlegir þættir
Lágt	1. Veitendur hvers konar rekstrarþjónustu, sem fellur undir þessa reglugerð, eru opinbert yfirvald eða lögaðili, sem er viðurkenndur sem slíkur samkvæmt landslögum aðildarríkis, hefur staðfest skipulag og er rekstrarhæfur að fullu að því er varðar alla þætti sem skipta máli fyrir veitingu þjónustunnar. 2. Veitendur fullnægja öllum lagalegum kröfum sem til þeirra eru gerðar í sambandi við starfrækslu og veitingu þjónustunnar, þ.m.t. um það hvers konar upplýsinga er heimilt að leita, hvernig sönnum á kennslum fer fram, hvaða upplýsingar má varðveita og hversu lengi. 3. Veitendur geta sýnt fram á getu sína til að taka á sig áhættu samfara skaðabótaábyrgð og að þeir ráði yfir nægilegu fjármagni til áframhaldandi starfsemi og veitingar þjónustunnar. 4. Veitendur bera ábyrgð á að allar skyldur, sem er útvistað til annarrar stofnunar, séu uppfylltar og að stefnu skipaninnar sé framfylgt, eins og hefðu þeir sjálfir sinnt verkefnunum. 5. Rafrænar auðkenningarskipanir, sem eru ekki stofnaðar samkvæmt landslögum, skulu hafa skilvirka áætlun sem lýsir því hvernig staðið yrði að niðurlagningu starfsemi. Slík áætlun skal taka til þess þegar þjónusta er lögð af með skipulegum hætti eða hún heldur áfram á vegum annars veitanda, hvernig viðkomandi yfirvöldum og endanlegum notendum er tilkynnt um það, ásamt því að innihalda ítarlegar upplýsingar um hvernig skrár verða verndaðar, varðveittar og þeim eytt í samræmi við stefnu skipaninnar.
Verulegt	Sama og fyrir stigið „lágt“.
Hátt	Sama og fyrir stigið „lágt“.

2.4.2. Birtar tilkynningar og upplýsingar til notenda

Fullvissustig	Nauðsynlegir þættir
Lágt	1. Fyrir hendi er birt skilgreining á þjónustunni þar sem fram koma allir viðeigandi skilmálar, skilyrði og gjöld, þ.m.t. allar takmarkanir á notkun hennar. Skilgreining á þjónustunni skal innihalda stefnu varðandi friðhelgi einkalífsins. 2. Innleiða skal viðeigandi stefnu og ferla til að tryggja að notendum þjónustunnar séu veittar upplýsingar tímanlega og með áreiðanlegum hætti um allar breytingar á skilgreiningu þjónustunnar og á öllum gildandi skilmálum, skilyrðum og stefnu varðandi friðhelgi einkalífsins fyrir hina tilteknu þjónustu. 3. Innleiða skal viðeigandi stefnur og ferla til að sjá til þess að beiðnum um upplýsingar sé svarað með fullnægjandi og réttum hætti.
Verulegt	Sama og fyrir stigið „lágt“.
Hátt	Sama og fyrir stigið „lágt“.

2.4.3. Stjórnun upplýsingaöryggis

Fullvissustig	Nauðsynlegir þættir
Lágt	Fyrir hendi er skilvirkt stjórnkerfi upplýsingaöryggis til að stjórna og hafa eftirlit með áhættu í tengslum við upplýsingaöryggi.
Verulegt	Stigið „lágt“ og að auki: Stjórnkerfi upplýsingaöryggis fylgir sannreyndum kröfum eða meginreglum um stjórnun og eftirlit með áhættu í tengslum við upplýsingaöryggi.
Hátt	Sama og fyrir stigið „verulegt“.

2.4.4. Skráahald

Fullvissustig	Nauðsynlegir þættir
Lágt	1. Viðeigandi upplýsingar eru skráðar og þeim viðhaldið í skilvirku skráningarkerfi með tilliti til gildandi löggjafar og góðra starfsvenja að því er varðar persónuvernd og varðveislu gagna. 2. Upplýsingarnar eru varðveittar, að því marki sem það er heimilt samkvæmt landslögum eða öðru landsbundnu stjórnunarfyrirkomulagi, og verndaðar svo lengi sem þeirra er þörf vegna úttekta og rannsókna á öryggisrofi og vegna varðveislu, en að því loknu skal þeim eytt með öruggum hætti.
Verulegt	Sama og fyrir stigið „lágt“.
Hátt	Sama og fyrir stigið „lágt“.

2.4.5. Aðstaða og starfsfólk

Í eftirfarandi töflu er að finna kröfur að því er varðar aðstöðu og starfsfólk og, ef við á, undirverktaka sem sinna starfsskyldum sem falla undir reglugerð þessa. Samræmi við kröfur skal vera í réttu hlutfalli við þá áhættu sem tengist viðkomandi fullvissustigi.

Fullvissustig	Nauðsynlegir þættir
Lágt	1. Ferlar eru fyrir hendi, sem tryggja að starfsfólk og undirverktakar hafi fullnægjandi þjálfun, menntun og hæfi og reynslu sem nauðsynleg er til að sinna þeim hlutverkum sem þeir gegna. 2. Nægilegt starfsfólk og undirverktakar er fyrir hendi til að starfrækja og viðhalda þjónustunni með viðunandi hætti samkvæmt stefnum og ferlum sem gilda um hana. 3. Aðstaða sem er notuð við að veita þjónustuna er stöðugt vöktuð og vernduð gegn tjóni af völdum umhverfisatburða, óheimils aðgangs og annarra þátta, sem geta haft áhrif á öryggi þjónustunnar. 4. Aðstaða sem er notuð við að veita þjónustuna tryggir að aðgangur að svæðum þar sem persónuupplýsingar, dulritunarupplýsingar eða aðrar viðkvæmar upplýsingar eru geymdar eða unnið er með þær, sé takmarkaður við starfsfólk eða undirverktaka, sem til þess hafa heimild.
Verulegt	Sama og fyrir stigið „lágt“.
Hátt	Sama og fyrir stigið „lágt“.

2.4.6. Tæknilegar stýringar

Fullvissustig	Nauðsynlegir þættir
Lágt	1. Hæfilegar tæknilegar stýringar eru fyrir hendi til að stýra þeirri áhættu sem öryggi þjónustunnar er búin og standa vörð um leynd þeirra upplýsinga sem unnið er með, heilleika þeirra og aðgengileika. 2. Rafrænar samskiptarásir, sem eru notaðar til að skiptast á persónuupplýsingum eða viðkvæmum upplýsingum, eru verndaðar gegn hlerun, misnotkun og endursendingu. 3. Ef viðkvæmt dulritunarefni er notað við útgáfu á rafrænum auðkenningarleiðum og sannvottun er aðgangur að því takmarkaður við þær stöður og þá notkun sem krefst aðgangs. Tryggja skal að slíkt efni sé aldrei vistað varanlega sem venjulegur texti. 4. Ferlar eru fyrir hendi til að tryggja að öryggi sé viðhaldið til langs tíma og að geta sé fyrir hendi til að bregðast við breytingum á áhættustigum, atvikum og öryggisrofi. 5. Geymsla, flutningur og förgun allra miðla, sem innihalda persónuupplýsingar, dulritunar-upplýsingar eða aðrar viðkvæmar upplýsingar, fer fram með öruggum og tryggum hætti.
Verulegt	Sama og fyrir stigið „lágt“ og að auki: Ef viðkvæmt dulritunarefni er notað við útgáfu á rafrænum auðkenningarleiðum og sannvottun er það verndað gegn fikti (e. tampering).
Hátt	Sama og fyrir stigið „verulegt“.

2.4.7. Reglufylgni og úttekt

Fullvissustig	Nauðsynlegir þættir
Lágt	Fram fara reglubundnar innri úttektir sem ná yfir alla þætti sem skipta máli fyrir veitingu þjónustunnar til að tryggja að viðeigandi stefnu sé fylgt.

Fullvissustig	Nauðsynlegir þættir
Verulegt	Fram fara reglubundnar óháðar innri eða ytri úttektir sem ná yfir alla þætti sem skipta máli fyrir veitingu þjónustunnar til að tryggja að viðeigandi stefnu sé fylgt.
Hátt	1. Fram fara reglubundnar óháðar ytri úttektir sem ná yfir alla þætti sem skipta máli fyrir veitingu þjónustunnar til að tryggja að viðeigandi stefnu sé fylgt. 2. Skipan sem er undir beinni stjórn ríkisstofnunar sætir úttekt í samræmi við landslög.