PSD2 og tæknistaðlarnir sem varða framtíðina

Hjálmar Stefán Brynjólfsson, lögfræðingur á sviði yfirlögfræðings

Í greininni Hvenær öðlast PSD2 gildi hér á landi?, sem birtist í Fjármálum í mars sl.[1], var fjallað almennt um eina af lykilspurningunum sem tengjast innleiðingu PSD2 tilskipunarinnar. Farið var í því sambandi yfir nokkur málefni sem hafa munu áhrif á innleiðinguna á komandi misserum. Jafnframt var komið lauslega inn á eina af mikilvægustu fylgigerðum tilskipunarinnar, sem í senn er fylgifiskur hennar og hryggjarstykki. Um er að ræða svokallaða framselda reglugerð framkvæmdastjórnarinnar (ESB) 2018/389 varðandi tæknilega eftirlitsstaðla um sterka sannvottun viðskiptavina og almenna og örugga opna staðla vegna samskipta[2], hér eftir nefnd til einföldunar tæknistaðlar um sterka auðkenningu og örugga upplýsingamiðlun[3] eða bara tæknistaðlarnir. Í þessari grein er ætlunin að fjalla nánar um þessa tæknistaðla[4] .

Það er til marks um þá miklu gerjun sem fylgir PSD2 um þessar mundir, að þegar fyrrnefnd grein var skrifuð, þ.e. í upphafi árs 2018, voru greinar á vegum Reiknistofu bankanna og í Viðskiptablaðinu eina efnið sem birst hafði opinberlega um efni tilskipunarinnar hér á landi. Á þeim stutta tíma sem liðinn er síðan hafa birst fleiri greinar[5] og skýrslur,[6] auk þess sem um málið hefur verið fjallað á námskeiði,[7] ráðstefnum[8] og í allmörgum lokaritgerðum háskólanema.[9] Í fyrrnefndu efni hefur m.a. verið komið inn á eftirlitshlutverk Fjármálaeftirlitsins gagnvart svonefndum „vottunaraðilum“ auk þess sem fjallað hefur verið um þörf fyrir frekari stöðlun vegna hins nýja landslags á greiðsluþjónustumarkaði. Þessi umræða er af hinu góða og mikilvægt að taka hana til nánari skoðunar. Þessi grein er hugsuð sem innlegg í umræðuna með sérstakri hliðsjón af tæknistöðlunum.

Víðtækt umboð EBA til að móta leikreglur

Aðdragandinn að gerð tæknistaðlanna um sterka auðkenningu og örugga upplýsingamiðlun er einn sá lengsti og umfangsmesti sem um getur.[10] Þessi einstaki aðdragandi

---

[1] *Sjá nánar hér: Hvenær öðlast PSD2 gildi hér á landi?*

[2] *Til áréttingar er tekið fram að tæknilegir staðlar (e. binding technical standards), eru tiltölulega ný tegund löggjafar sem unnið hefur verið að innan Evrópu frá því að reglugerðirnar um ESMA/EBA/EIOPA voru settar árið 2010. Slík löggjöf er mótuð innan evrópsku eftirlitsstofnananna en samþykkt og útgefin af hálfu framkvæmdastjórnar ESB. Endanlegar útgáfur tæknilegra staðla eru gefnar út í formi reglugerða af hálfu Evrópusambandsins. Tæknistaðlar er fyrst og fremst þjálla samheiti fyrir tæknilega staðla.*

[3] *Til þeirra tæknistaðla sem fjallað er um í þessari grein var vísað í fyrrnefndri grein Hvenær öðlast PSD2 gildi hér á landi? sem „tæknistaðlar um sterka auðkenningu og örugga upplýsingamiðlun“. Um tæknistaðlana hefur bæði verið fjallað sem tæknistaðla um „sterka sannvottun“ og „sterka auðkenningu“ hér á landi, en rétt er að geta þess að „sterk sannvottun“ felur efnislega í sér auðkenningu. Þá skal þess einnig getið að sá hluti tæknistaðlanna sem fjallar um „örugga opna staðla vegna samskipta“, sbr. heiti tæknistaðlanna, eru efnislega fyrst og fremst staðlar um auðkenningu þriðju aðila og miðlun upplýsinga milli banka og þeirra. Rétt er að geta þess að lokum að víðs vegar í umfjöllunum um umræddda tæknistaðla erlendis er hið óþjála heiti þeirra gjarnan einfaldað, t.a.m. með því að vísa til þeirra í formi skammstafana sem „RTS“ „the RTS“ eða jafnvel „RTS on SCA&CSC“.*

[4] *Tæknistaðlarnir eru aðgengilegir hér: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389.*

[5] *Sjá til að mynda greinar um PSD2 í veftímariti Kjarnans: https://kjarninn.is/frettir/2018-06-14-nyjar-tegundir-greidsluthjonustu-vaentanlegar/, https://kjarninn.is/frettir/2018-06-28-nyjar-leidir-litid-notadar-i-greidslumidlun/, https://kjarninn.is/skodun/2018-06-04-althjodavaeddur-heimur-skellur-islandi/, https://kjarninn.is/skodun/2018-05-01-ny-stada-taekifaeri-til-hagraedingar/ og https://kjarninn.is/skodun/2018-06-27-munu-bankar-hverfa-eins-og-hljomplotuverslanir/. Þá hefur Seðlabanki Íslands nýlega fjallað um PSD2 innleiðinguna í tímariti sínu Fjármálainnviðir: https://www.sedlabanki.is/utgefid-efni/rit-og-skyrslur/rit/2018/06/14/Fjarmalainnvidir-2018/*

[6] *Fjallað er um skýrslu Íslandsstofu um málið í greininni https://kjarninn.is/frettir/2018-06-28-nyjar-leidir-litid-notadar-i-greidslumidlun/, en skýrslan sjálf er aðgengileg hér: https://www.islandsstofa.is/frettir/banka-og-millifaerslukostnadur-islenskra-utflutningsfyrirtaekja.*

[7] *Um tilskipunina og breytingar vegna PSD2 var fjallað á námskeiði á vegum Endurmenntunar í vor: http://www.endurmenntun.is/namskeid/stakt-namskeid?courseID=117H18.*

[8] *Um málið var til að mynda fjallað á Lagadeginum 2018: http://www.lagadagur.is/dagskrá-2018/, svo og á ráðstefnu á vegum Reiknistofu bankanna: https://www.rb.is/radstefna-2018/.*

[9] *Fjallað var um PSD2 tilskipunina í alls fjórum lokaritgerðum nemenda á háskólastigi sl. vor, þar af þremur á sviði viðskipta- og hagfræði. Ritgerðirnar eru aðgengilegar á vef Skemmunnar.*

[10] *Við lok árs 2015 birti EBA samráðsskjal (e. discussion paper) um málefni sem vörðuðu reglusmíðina og bárust stofnuninni 118 svarbréf frá evrópskum bönkum og hagsmunasamtökum við þeim tillögum sem þar voru kynntar. Í kjölfar þess birti EBA í ágúst 2016 umræðuskjal sem 224 aðilar veittu umsögn um og af þeim eru 147 birtar á vefsíðu EBA. Svo sterk viðbrögð við drögum að tæknilegum stöðlum eru einsdæmi. Jafnvel umdeildustu tæknistaðlar sem tengjast öðrum móðurgerðum á fjármálamarkaði fá nokkra tugi umsagna, en að á þriðja hundrað umsagna berist í slíku ferli er einstakt. Þessu til viðbótar tók það langan tíma og allnokkur bréfaskipti milli framkvæmdastjórnar ESB og EBA að ljúka við endanlega útgáfu tæknistaðlanna. Þannig sendi EBA framkvæmdastjórninni lokadrögin í febrúar 2017 og fékk svarbréf frá framkvæmdastjórninni í maí 2017 með breyttri útgáfu tæknistaðlanna. Í kjölfar þess sendi EBA framkvæmdastjórninni álit á breytingunum í júní 2017 og bréf til ítrekunar í janúar 2018. Framkvæmdastjórn ESB svaraði þeim skjölum í febrúar 2018. Endanleg útgáfa þeirra var svo birt í formi reglugerðar í mars síðastliðnum. Hingað til hafa á bankamarkaði ekki tíðkast sérstök bréfasamskipti á milli EBA og framkvæmdastjórnar ESB til að fullklára tæknilega staðla.*

kallaði fram viðbrögð frá haghöfum og stjórnvöldum sem eru fáséð, en skiljanleg af tveimur ástæðum: Í fyrsta lagi í ljósi þeirra hagsmuna sem eru í húfi, en líkt og bent hefur verið á kunna þær breytingar sem PSD2 hefur í för með sér að leiða til þess að tekjur viðskiptabanka í Evrópu dragist saman um allt að 25%. Þetta eru gríðarmiklir hagsmunir sem hafa áhrif á að minnsta kosti þrenns konar aðila: banka, kortafyrirtæki og fjártæknifyrirtæki. Innan vébanda þeirra er fjöldi fyrirtækja á Evrópuvísu sem velta fyrir sér hvernig breytingarnar hafa áhrif á starfsemi hvers og eins.

Í öðru lagi má færa rök fyrir því að viðbrögðin hafi verið skiljanleg þar sem EBA var veitt nokkuð rúmt umboð til að móta leikreglur á greiðsluþjónustumarkaði við mótun draganna að tæknistöðlunum. Þannig eru meginreglur um efni tæknistaðlanna ekki ítarlegar í tilskipuninni sem tæknistaðlarnir byggjast á. EBA hefur jafnframt haft nokkuð frjálsar hendur við mótun tæknistaðlanna í þeim skilningi að við gerð þeirra er ekki stuðst við alþjóðlega staðla eða viðmið í jafn ríkum mæli og tíðkast á öðrum sviðum löggjafar á fjármálamarkaði. Þannig fela viðamestu móðurgerðirnar á bankamarkaði, svo sem CRD IV/CRR eða BRRD, í sér efni sem eru alþjóðlega viðurkenndar leikreglur á markaði eftir víðtækt samráð alþjóðlegra stofnana, svo sem Basel-nefndarinnar eða alþjóðlega fjármálastöðugleikaráðsins (e. Financial Stability Board - FSB).

Vísbendingar um að umboðið sem PSD2 tilskipunin veitir EBA vegna tæknistaðlanna sé nokkuð rúmt má m.a. ráða af 36. gr., 97. gr. og 1. og 2. mgr. 98. gr. tilskipunarinnar sem fjalla um afhendingu gagna frá lánastofnunum og hvenær beita skuli sterkri auðkenningu. Þannig kveður 36. gr. á um skyldu EES-ríkja til að tryggja að greiðslustofnanir hafi aðgang að greiðslureikningum lánastofnana á hlutlægan hátt og án mismununar. Lánastofnun ber skylda til að rökstyðja með fullnægjandi hætti ef hún neitar greiðslustofnun um slíkan aðgang. Tilskipunin útfærir þessa skyldu ekki með nákvæmari hætti en svo, að með þessum tveimur setningum er nokkurn veginn búið að endursegja efni 36. gr. tilskipunarinnar í heild sinni. EBA er hins vegar eftirlátið að útlista nánar hvað felst í þessum skyldum og útfæra framkvæmd ákvæðisins, þ.e. afhendingu gagna og upplýsinga, með því að búa til tæknistaðlana.

Að sama skapi er í 97. gr. tilskipunarinnar einungis að finna ákvæði um það hvenær skuli beita sterkri auðkenningu. Það er þegar viðskiptavinur „kveikir“ greiðslu, fer inn á greiðslureikning í gegnum netið eða framkvæmir hverja þá aðgerð í gegnum fjarskipti sem kann að hafa í för með sér hættu á greiðslusvikum. Þessu til viðbótar mælir ákvæðið fyrir um að greiðsluþjónustuveitendur þurfi að hafa til staðar fullnægjandi öryggisráðstafanir til að tryggja trúnað og vernda heilleika þeirra skírteina (e. credentials) sem notendur greiðsluþjónustu þurfa að reiða sig á. Fyrir utan nokkur ákvæði sem varða sérstaklega samskipti banka við þjónustuveitendur vegna greiðsluvirkjunar (PISP) og þjónustuveitendur vegna reikningsupplýsinga (AISP) er efni 97. gr. þar með upp talið.

Þessu til viðbótar er í 1. mgr. 98. gr. nánast einungis að finna útlistun á því hvaða efni á að fjalla um í tæknistöðlunum og í hvaða röð, á meðan 2. mgr. 98. gr. tilgreinir þau markmið sem EBA á að ná fram og taka mið af við gerð tæknistaðlanna.

Þannig má í rétt tæplega þremur málsgreinum endursegja grundvöll tæknistaðlanna úr móðurgerðinni, þessara sömu tæknistaðla sem mæla fyrir um samræmingu öryggisráðstafana innan alls Evrópska efnahagssvæðisins vegna auðkenningar í tengslum við greiðslur, svo og miðlun upplýsinga frá bönkum til þriðju aðila[11].

Tæknistaðlar um sterka auðkenningu og örugga upplýsingamiðlun í hnotskurn

Tæknistaðlarnir skiptast í sex kafla sem fela í sér alls 37 ákvæði. Að auki fylgir þeim viðauki með töflu sem inniheldur viðmið varðandi tíðni vegna sviksamra greiðslufærslna. Tæknistaðlarnir öðlast gildi 14. september 2019 og frá og með þeim tímapunkti á afhending gagna frá bönkum til þriðju aðila að geta átt sér stað innan Evrópska efnahagssvæðisins. Sex mánuðum fyrir þann tímapunkt (þ.e. 14. mars 2019) ber bönkum að koma sér upp prófunarumhverfi til að veita þriðju aðilum tækifæri til að tengjast þeim sérhæfðu forritaskilum (e. dedicated interface) sem þeir koma sér upp.

Staðlarnir snerta greiðsluþjónustuveitendur með ólíkum hætti eftir því hvar þeir eru í greiðslukeðjunni. Þannig þurfa lánastofnanir að huga að öllum ákvæðum staðlanna og geta orðið fyrir miklum áhrifum vegna þess

---

[11] Rétt er að geta þess að til viðbótar við þær almennu forskriftir vegna sterkrar auðkenningar og öruggrar upplýsingamiðlunar í tengslum við tæknistaðlana sem fjallað er um í þessari grein, er í tilskipuninni einnig að finna almenn skilyrði sem þjónustuveitendur vegna greiðsluvirkjunar (PISP) og þjónustuveitendur vegna reikningsupplýsinga (AISP) þurfa að uppfylla til að mega virkja greiðslur eða veita upplýsingar um reikninga. Slík almenn skilyrði er að finna í 66. - 67. gr. tilskipunarinnar en í þeim felst m.a. að þeir þurfi skýlaust samþykki (e. explicit consent) neytenda, auk þess sem óheimilt er að vista eða óska eftir viðkvæmum greiðslugögnum (e. sensitive payment data). Fleira mætti tína til, en slík skilyrði verða öll lögfest við innleiðingu PSD2 tilskipunarinnar.

hluta þeirra sem snýr að miðlun upplýsinga til og samskipta við þriðju aðila. Hins vegar verða greiðslustofnanir sem þegar beita sterkri auðkenningu og eru ekki að brjóta sér leið inn á greiðslumarkaðinn sem PISP eða AISP væntanlega fyrir litlum áhrifum vegna tæknistaðlanna.

Í I. kafla tæknistaðlanna eru almenn ákvæði sem m.a. fela í sér kröfu um að unnt sé að vakta greiðslufærslur (e. transaction monitoring) (2. gr.) og þar er einnig fjallað um endurskoðun vegna öryggisráðstafana. Í VI. og síðasta kafla tæknistaðlanna er gildistökuákvæði sem þegar hefur verið endursagt. Fjallað er stuttlega um aðra kafla tæknistaðlanna, og tæpt á helstu ákvæðum hvers kafla, hér að neðan. Ómögulegt er að endursegja allar reglur tæknistaðlanna í grein sem þessari, enda er markmiðið fyrst og fremst að draga fram nokkur áhugaverð ákvæði til að skapa frekari umræðu um þær kröfur og skilyrði sem felast í tæknistöðlunum.

II. kafli (4. – 9. gr.) Öryggisráðstafanir vegna sterkrar auðkenningar

Sterk auðkenning viðskipta (e. strong customer authentication) er annað af megin efnum tæknistaðlanna. Sterk auðkenning felur í sér að við auðkenningu greiðslunotanda er notast við tvo af eftirfarandi þremur þáttum til að sannvotta að greiðslunotandinn sé í raun hinn skráði notandi/handhafi viðkomandi greiðslumiðils: 1) það sem hann er (e. inherence), 2) það sem hann veit (e. knowledge) eða 3) það sem hann hefur (e. possession). Hver þáttur fyrir sig þarf að vera sjálfstæður, þ.e. ekki háður eða innifalinn í öðrum þáttum. Sterk auðkenning er ekki ný af nálinni í þeim skilningi að í viðmiðunarreglum EBA vegna öryggis netgreiðslna frá 2014 hefur verið lagt upp með að fullnægjandi öryggisráðstafanir náist aðeins með sterkri auðkenningu. Tína mætti til nokkurn fjölda dæma úr daglega lífinu þar sem nú þegar er unnið með tveggja þrepa nálgun til að tryggja öryggisráðstafanir við notkun upplýsingatækni, og væntanlega hafa sumir greiðslukortanotendur sem versla á netinu, eða framkvæma umfangsmikla greiðslu, orðið varir við auðkenningarkröfu ekki eingöngu með sannvottunarkóða (e. authentication code) heldur frekari auðkenningu t.d. í gegnum síma.

Það sem tæknistaðlarnir gera er því ekki að finna upp hjólið m.t.t. sterkrar auðkenningar heldur að tryggja samræmingu innan Evrópska efnahagssvæðisins vegna hennar. Til að mynda er hámarksfjöldi misheppnaðra tilrauna viðskiptavina til að auðkenna sig með sterkri auðkenningu 5 skipti, og hámarkstími án þess að aðhafast á greiðslureikningi í gegnum netið eru 5 mínútur (sbr. 4. mgr. 4. gr. tæknistaðlanna). Þá eru gerðar viðbótarkröfur varðandi öryggisráðstafanir ef greiðslur eru framkvæmdar með beintengingu (e. dynamic linking) milli greiðslureiknings og greiðslumiðils. Ákvæði 6. – 8. gr. tæknistaðlanna fjalla um sérstakar kröfur sem gerðar eru til hvers þáttar sterkrar auðkenningar fyrir sig, en 9. gr. hans fjallar um það hvernig skuli tryggja að hver þáttur fyrir sig sé sjálfstæður eða óháður hinum þáttunum.

III. kafli (10. – 21. gr.) Undanþágur frá beitingu sterkrar auðkenningar

Þriðji kafli tæknistaðlanna fjallar um undanþágur, þ.e. hvaða greiðslur eru undanþegnar því að beita þurfi sterkri auðkenningu á viðskiptamenn. Til undanþeginna greiðsla teljast:

- Snertilausar greiðslur í verslun ef upphæðin er undir 50 evrum (11. gr.)
- Greiðslur til aðila sem notandi skilgreinir sem traustan (e. trusted beneficiaries) (13. gr.)
- Endurteknar greiðslur sem allar eru hluti af röð greiðslna og eru af sömu upphæð til sama aðila (14. gr.)
- Millifærslur á milli reikninga í eigu sama aðila (15. gr.)
- Greiðslur með lágum upphæðum (16. gr.)
- Öruggar greiðslur fyrirtækja, þ.e. ekki neytenda (17. gr.)
- Greiðslur sem teljast öruggar á grundvelli áhættugreiningar (e. transaction risk analysis) (18.-21. gr.)

Af ofangreindum undanþágum eru þær greiðslur sem teljast öruggar á grundvelli áhættugreiningar þær sem mestar kröfur gilda um, enda þarf að vakta slíkar greiðslur sérstaklega auk þess sem í tengslum við þær mega ekki hafa átt sér stað svik sem fara yfir sérstök viðmið sem tilgreind eru í viðauka tæknistaðlanna. Ástæða er því til að vekja athygli á þessari undanþágu sérstaklega.

IV. kafli (22. – 27. gr.) Trúnaður og heilleiki vegna persónumiðaðra öryggisskírteina (e. personalised security credentials)

Í fjórða kafla tæknistaðlanna er fjallað um það hvernig greiðsluþjónustuveitendum ber að tryggja heilleika og trúnað vegna þeirra persónumiðuðu öryggisskírteina sem eru notuð. Á meðal þess sem nefnt er í kaflanum er að tryggja skuli að skilríkin séu hulin þegar þau birtast á skjá og ekki lesanleg í heild sinni (22. gr.), en einnig er þar að finna ákvæði um það hvernig milda skuli áhættuna af óheimilaðri notkun þeirra áður en þau hafa borist notandanum. Þá er einnig að finna sérstök ákvæði um endurnýjun skilríkja (26. gr.) og eyðingu eða afturköllun þeirra (27. gr.).

V. kafli (28. – 36. gr.) Almennir og öruggir opnir staðlar varðandi samskipti milli banka og þriðju aðila (AISP og PISP)

Fimmti kafli tæknistaðlanna fjallar um upplýsingamiðlun milli banka og þriðju aðila sem notendur hafa veitt heimild til að kveikja greiðslu (PISP) eða afla upplýsinga um sig (AISP). Í stuttu máli fjallar kaflinn um auðkenningu þriðju aðilanna gagnvart bankanum sem afhendir gögnin, rekstur sérhæfðra forritaskila (e. dedicated interface), þ.e. API, til að koma upplýsingum milli aðila, og að lokum um upplýsingar sem bönkum er heimilt að veita aðilum, þ.m.t. hve oft á dag þeir eiga að hafa aðgang að þeim.

Að því er varðar auðkenningu þriðju aðila gagnvart bönkum skipta tvö atriði miklu máli: annars vegar skráning þeirra í miðlæga skrá EBA yfir greiðsluþjónustuveitendur og hins vegar notkun vottorða sem gefin eru út með vísan til svonefndrar eIDAS reglugerðar (sbr. 34. gr. tæknistaðlanna, en nánar er fjallað um eIDAS reglugerðina síðar í þessari grein).

Í 30. gr. tæknistaðlanna, sem er almenns eðlis, segir að bankar eigi að hafa til staðar viðmót sem uppfyllir skilyrði ákvæðisins þannig að þriðju aðilar geti fengið afhentar upplýsingar frá bankanum. Ástæða er til að vekja athygli á að þetta er hægt að framkvæma á marga vegu og fjallar 31. gr. tæknistaðlanna um það. Í 32. gr. eru nánari lýsingar á því hvaða skilyrði sérhæfðu forritaskilin þurfa að uppfylla, þ. á m. að þjónusta sem veitt er í gegnum þau eigi að vera svipuð að gæðum og ef verið væri að vinna í gegnum greiðslureikning á netinu.

Í 33. gr. tæknistaðlanna er að finna ákvæði sem vakið hefur nokkuð umtal en það fjallar um til hvaða viðbragðsaðgerða (e. contingency measures) greiðsluþjónustuveitendur eiga að grípa ef forritaskilin eða greiðslukerfi virka ekki sem skyldi. Í ákveðnum tilfellum munu eftirlitsstjórnvöld, svo sem Fjármálaeftirlitið, geta veitt bönkum undanþágu frá því að setja upp viðbragðskerfi, að uppfylltum þeim skilyrðum sem koma fram í ákvæðinu.

Í 35. gr. tæknistaðlanna er fjallað um öryggi í samskiptum allra aðila sem koma að greiðslum. Slík samskipti eiga að vera dulkóðuð og allar samskiptalotur að vera eins og stuttar og hægt er. Þá er í 36. gr. fjallað stuttlega um þær upplýsingar sem bankar eiga að veita þjónustuveitendum vegna greiðsluvirkjunar (PISP) annars vegar og þjónustuveitendum vegna reikningsupplýsinga (AISP) hins vegar. Í ákvæðinu kemur m.a. fram að bankar eigi að tryggja aðgengi þriðju aðila að upplýsingum eins oft og viðskiptavinur þeirra óskar eftir, en að lágmarki fjórum sinnum á sólarhring.

Eru tæknistaðlarnir nógu skýrir? Hvernig verður leyst úr álitamálum vegna þeirra? Nýtt álit EBA og nýjar viðmiðunarreglur

Í ljósi þess hve aðdragandinn að gerð tæknistaðlanna var langur og umfangsmikill mætti ætla að skýru ljósi hefði nú þegar verið varpað á öll 37 ákvæði þeirra. Enn er þó verkefnum ólokið þar. Breytingum fylgir enda alltaf ákveðin óvissa, sem svo leitar jafnvægis með tímanum í gegnum túlkanir og þær venjur sem stuðst verður við.

Breytingarnar sem PSD2 hefur í för með sér varða mikla hagsmuni og því hefur EBA verið mjög virkur þátttakandi í umræðunni um það hvað breytingarnar hafa í för með sér og hvernig á að greiða úr þeim flækjum sem fyrirfinnast í regluverkinu. Nú þegar hefur EBA gefið út álit á því hvernig beri að nálgast tímabilið sem líður frá því að innleiða ber PSD2 tilskipunina og þar til tæknistaðlarnir öðlast gildi en frá því áliti var sagt í greininni *Hvenær öðlast PSD2 gildi hér á landi?*[12] Þá hefur EBA frá því í mars sl. unnið að nýju áliti þar sem leitast er við að skýra sérstaklega efnisatriði sem markaðurinn í Evrópu hefur kallað eftir að verði skýrð. Þannig er í álitinu fjallað með ítarlegum hætti, en á einföldu og skýru máli, um:

[12] *Sjá nánar hér: http://www.eba.europa.eu/-/eba-publishes-opinion-on-the-implementation-of-the-rts-on-strong-customer-authentication-and-common-and-secure-communication.*

- Nákvæmlega hvaða gögn, og hversu mikið af gögnum, þjónustuveitendur vegna greiðsluvirkjunar (PISP) og þjónustuveitendur vegna reikningsupplýsinga (AISP) eiga rétt á að fá.
- Hvernig túlka skuli regluna um að upplýsingar beri að hámarki að veita fjórum sinnum á dag.
- Hvort CVV-númer, ásamt kortanúmeri og gildistíma greiðslukorts geti talist eitthvað sem einungis notandi þekkir.
- Hver ákveður hvort beita eigi sterkri auðkenningu og hver ákveður hvort heimila eigi undanþágu frá því að beita henni, auk stuttrar umfjöllunar um þær leiðir sem eru heimilar til að uppfylla kröfur og skilyrði um framkvæmd sterkrar auðkenningar.[13]

Þessu til viðbótar hefur EBA unnið drög að viðmiðunarreglum þar sem sérstaklega verður fjallað um hvaða undanþágur verður heimilt að veita lánastofnunum frá því að hafa til staðar og ráðast í sérstakar viðbragðsaðgerðir (e. contingency measures) í tengslum við afhendingu gagna í gegnum sérhæfð forritaskil (e. dedicated interface). Í stuttu máli varða reglurnar hvaða skilyrði þurfa að vera uppfyllt til að eftirlitsaðilum sé heimilt að veita greiðsluþjónustuveitanda undanþágu frá því að skilgreina sérstaklega til hvaða viðbragða hann þurfi að grípa til ef kemur til rofs á greiðsluþjónustu við miðlun upplýsinga til þjónustuveitanda vegna reikningsupplýsinga (AISP), til þjónustuveitanda vegna greiðsluvirkjunar (PISP) eða til kortafyrirtækis í gegnum sk. API (e. application programming interface). Slík skilyrði eru öll tæmandi talin í liðum a-d í 6. mgr. 33. gr. tæknistaðlanna, en líkt og fram kemur í drögunum að viðmiðunarreglunum, er sú upptalning ekki fullnægjandi ein og sér.[14] Það hvað nákvæmlega felst í hverju skilyrði og hverri kröfu fyrir sig þarf að skýra, og verður það gert í viðmiðunarreglunum.

Að lokum verður að nefna að EBA hefur nú þegar ráðist í undirbúning þess að birta á heimasíðu sinni svör við sérfræðispurningum til viðbótar þeim sem búið er að gera sérstaklega í tengslum við gerð ofangreinds álits og viðmiðunarreglnanna. Þannig verður í náinni framtíð hægt að leita uppi svör við einstökum spurningum vegna þeirra ákvæða PSD2 tilskipunarinnar sem kunna að vera óskýr. Þau verða gerð aðgengileg á sérstakri Spurt og svarað (e. Q&A) síðu.[15] Þannig verða samræming og viðbrögð við álitaefnum ofarlega á baugi vegna PSD2 tilskipunarinnar á komandi misserum.

Kalla tæknistaðlarnir á vottun af hálfu Fjármálaeftirlitsins eða enn frekari stöðlun?

Líkt og nefnt var í inngangsorðum þessarar greinar hefur í opinberri umræðu m.a. verið fjallað um hvort tæknistaðlarnir kalli á nýja tegund eftirlits innan vébanda Fjármáleftirlitsins, þ.e. vottun með þriðju aðilum.[16] Að auki kalla ákvæði í tæknistöðlunum á umræðu um það hvort endurskoðun vegna upplýsingatækni[17] verði mikilvægara málefni en verið hefur, og þá hvaða hlutverki Fjármálaeftirlitið gegnir vegna þessa. Þá hefur jafnframt verið fjallað um það hér á landi og erlendis hvort þörf sé á frekari stöðlun í tengslum við hið breytta landslag á greiðsluþjónustumarkaði, þar sem fleiri aðilar geta fengið aðgang að gögnum og upplýsingum um greiðslureikninga en bara bankar og þar sem fleiri tegundir greiðslumiðla verða notaðar en bara plastkort.

Fagna ber ábendingunni um eftirlit Fjármálaeftirlitsins með „vottunaraðilum“ og þeirri umræðu sem hún leiðir af sér. Leggja verður þó áherslu á að í þessu samhengi skiptir skýrleiki miklu. Þótt ég hafi kynnt mér efni PSD2 tilskipunarinnar og tæknistaðlanna sem hún leiðir af sér er ég ekki fyllilega viss um stefnu þessarar umræðu. Það er einkum vegna þess að ég er ekki viss um hvað átt er við með orðinu „vottunaraðilar“ í því samhengi sem það er notað. Að óbreyttu fyrirkomulagi á eftirliti með greiðsluþjónustu hér á landi má gera ráð fyrir að Fjármálaeftirlitið hafi eftirlit með svonefndum þjónustuveitendum vegna greiðsluvirkjunar (PISP) og þjónustuveitendum vegna reikningsupplýsinga (AISP), auk þess að fjalla um starfsleyfisveitingu og/eða skráningu þeirra. Hluti af því eftirliti verður að sjá til þess að þeir fari að þeim kröfum sem til þeirra eru gerðar í þeim lögum sem munu innleiða PSD2 tilskipunina og stjórnvaldsfyrirmælum sem innleiða tæknistaðlana. Sé þetta það sem felst í umræðunni um „vottunaraðila“, þá eru málin skýr, þ.e. Fjármálaeftirlitið mun verða eins konar „vottunaraðili“ ef með því er átt við að Fjármálaeftirlitið

---

[13] Sjá nánar hér: http://www.eba.europa.eu/-/eba-publishes-opinion-on-the-implementation-of-the-rts-on-strong-customer-authentication-and-common-and-secure-communication.

[14] Sjá nánar hér: http://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-the-conditions-to-be-met-to-benefit-from-an-exemption-from-contingency-measures-under-article-33-6-of-regulation-eu-2018/389-rts-on-sca-csc-.

[15] Sjá nánar hér: http://www.eba.europa.eu/regulation-and-policy/single-rulebook/interactive-single-rulebook/-/interactive-single-rulebook/toc/5402;jsessionid=BFE95F3E3B1F0AA4BE36888B216F4BF6.

[16] Sjá nánar hér: http://www.visir.is/g/2018180439986.

[17] Sjá í þessu samhengi sérstaklega 3. gr. tæknistaðlanna, sem fjallar um þetta efni.

eigi að segja til um hvaða þjónustuveitendum vegna greiðsluvirkjunar (PISP) og þjónustuveitendum vegna reikningsupplýsinga (AISP) hér á landi verður heimilt að taka við gögnum frá bönkum. Sé hins vegar með þessu til dæmis átt við hvort Fjármálaeftirlitið muni eftir gildistöku PSD2 sinna eftirliti með útgáfu fullgildra vottorða, sbr. umfjöllun um 34. gr. tæknistaðlanna hér að framan, og þannig vera óbeint „vottunaraðili“ þá er of snemmt að fullyrða nokkuð um það fyrr en eftir innleiðingu eIDAS reglugerðarinnar hér á landi.[18] Í henni er fjallað um notkun fullgildra vottorða og slík vottorð geta til að mynda verið notuð til að bera kennsl á þriðju aðila. En þangað til innleiðingu eIDAS reglugerðarinnar er lokið má styðjast við langlíklegasta svarið út frá drögum að frumvarpi til laga til að innleiða reglugerðina, sem kynnt hefur verið í samráðsgátt Stjórnarráðsins. Það svar er nei, Fjármálaeftirlitið mun ekki vera „vottunaraðili“ eða sinna eftirliti með „vottunaraðilum“ ef með þeim er átt við traustþjónustuveitendur eða aðila sem gefa út fullgild vottorð.

Hvað snertir spurninguna um frekari stöðlun á greiðsluþjónustumarkaði, þá kann vafalítið að æra óstöðugan, og einkum ef viðkomandi er leikmaður, ef ráðist verður í frekari stöðlun til að túlka tæknistaðla. Slík verkefni eru þó þegar í vinnslu, bæði erlendis[19] og hér á landi.[20] Sú vinna er jafnframt af hinu góða, enda miðar hún að því að einfalda sum atriði sem tengjast hinum flókna markaði greiðslukerfa og greiðsluþjónustu. Þótt mörgum þyki að það felist mótsögn í því að halda því fram að hægt sé að gera flókið umhverfi auðveldara með því að bæta enn við regluverkið, og fjölga reglum sem um málaflokkinn gilda, er hinu ekki að neita að allir þeir sem koma að þessu flókna umhverfi gegna ólíkum hlutverkum og nota til þess ólíka tækni og þar með talið ólík „tungumál“. Viðskiptafræðingar, lögfræðingar, hagfræðingar, endurskoðendur og upplýsingatæknifræðingar tengjast hver sinni hliðinni og horfa á málin út frá sínum hugtökum, eða reynslu. Ef frekari stöðlun hefur í för með sér að skýra og einfalda hvernig túlka á einstök atriði eða tilgreina nákvæmlega hvað felst í ákveðnum kröfum mun slík stöðlun geta bætt regluverkið sem fyrir er. Til þess að svo verði þarf þó slík vinna að vera unnin út frá tveimur meginreglum: hún þarf a) ávallt að styðjast við þann ramma sem er til staðar og kann að vera ákveðinn með lögum og b) að minnka, og alls ekki auka, hættu á flækjum. Til að ná því fram að slík stöðlun minnki hættu á frekari flækjum, verður að gæta að því að ekki verði notast við of mikið af ólíkum eða sértækum hugtökum, og er þá sérstaklega átt við hugtök sem ekki er að finna í þeim ramma sem tilheyrir PSD2 löggjöfinni. Hins vegar er augljóst að þar sem ramma löggjafarinnar sleppir kann að vera rík þörf fyrir hugtök og orð sem ekki eru til staðar fyrir. Að sama skapi þarf að passa upp á að ekki myndist flækjur með þeim hætti að til verði of sérhæfðir staðlar á einstökum greiðslumörkuðum hvers ríkis innan EES. Slík vinna kynni að ganga í berhögg við yfirlýstan tilgang þeirra markmiða sem PSD2 tilskipunin er unnin eftir: að skapa sameiginlegan greiðslumarkað sem hluta af innri markaði EES.

Að lokum

Síðasta orðið um innleiðingu PSD2 tilskipunarinnar og fylgigerða hennar hefur ekki verið sagt og mörg skref eru enn óstigin þar til lögfesting hennar hefur átt sér stað hér á landi. Til að mynda þarf að taka tilskipunina formlega upp í EES-samninginn og er að því stefnt á þessu ári eða í upphafi þess næsta. Þangað til innleiðingu tilskipunarinnar verður að fullu lokið hér á landi skiptir miklu máli að haghafar, stjórnvöld og þátttakendur í greiðslukerfinu komi ekki bara auga á tækifærin sem felast í breyttu tækniumhverfi og lagabreytingunum, heldur að allir geri sér grein fyrir því hvaða skyldur og ábyrgð hvílir á þeim eða munu hvíla á þeim. Að sinni telur Fjármálaeftirlitið að hlutverk þess sé fyrst og fremst að miðla upplýsingum og undirbúa aðila á markaði fyrir þær breytingar sem eru í vændum. Fjármálaeftirlitið mun leitast við að upplýsa áhugasama um efni PSD2 tilskipunarinnar með því að setja inn upplýsingar á vefsíðu sína og bjóða aðilum að senda inn fyrirspurnir vegna hennar. Séu brýn álitaefni uppi um túlkun tæknistaðlanna eða efni PSD2 tilskipunarinnar er aðilum velkomið að setja sig í samband við Fjármáleftirlitið með því að senda inn fyrirspurn í gegnum vef stofnunarinnar.

---

[18] Með eIDAS reglugerðinni er átt við reglugerð (ESB) nr. 910/2014, um rafræna auðkenningu og traustþjónustu fyrir rafræn viðskipti.

[19] Slíkri stöðlun er m.a. hægt að ná fram með því að styðjast við alþjóðlega staðalinn ISO 20022, en við gerð tæknistaðlanna um sterka auðkenningu og örugga upplýsingamiðlun var m.a. tekin afstaða til þess hvort styðjast ætti við hann einan og sér í tengslum við PSD2. Þá hefur verið fjallað um slíka stöðlun á vegum Berlin Group, sjá nánar hér: https://www.berlin-group.org/psd2-access-to-bank-accounts.

[20] Sjá nánar hér: http://www.stadlar.is/thjonusta/nyjustu-frettir/stadlamal-frettabref-stadlarads/2018/05/bod-um-thatttoeku-i-taeknefnd-um-api.aspx.