

Morgunblaðið, 30.05.2024, síðu 43.
grein stærð: 388.87 sm2
grein hæð: 15.05 sm

Traust í stafrænni þróun

Í lok apríl samþykkti Evrópusambandið nýja reglugerð á sviði rafrænna auðkenninga og traustþjónustu, svokallaða eIDAS-2-reglugerð nr. 2024/1183. Reglugerðin breytir gildandi reglugerð frá árinu 2014, þ.e. eIDAS-1, sem kvað á um lagalegan ramma fyrir rafræna auðkenningu og traustþjónustur, t.d. rafrænar undirskriftir.



Unnur Kristín Sveinbjarnardóttir

Hin nýja reglugerð útvíkkar og styrkir fyrri löggjöf til muna. Hún kynnir til leiks hið evrópska stafræna auðkenningarveski sem veitir öllum ESB-íbúum öruggt, samhæft og notendastýrt stafrænt auðkenni. Veskið gerir íbúum kleift að geyma persónuupplýsingar sínar, s.s. opinber gögn, læknisvottorð, fjárhagsupplýsingar o.fl., í þeim tilgangi að þeir sjálfir hafi stjórn á þeim og geti deilt þeim eftir því sem við á með öruggum hætti. Umrætt veski er skyldubundið, þarf að byggjast á samræmdum tækniforskriftum, uppfylla ákveðnar öryggiskröfur og lúta eftirliti.

Reglugerðin þróar og styrkir lagalega umgjörð í þeim tilgangi að tryggja öryggi og traust stafrænna samskipta og viðskipta. Þannig er sambandið í raun að tryggja stafræna þróun innri markaðarins og réttindi borgara þess.

En eIDAS-reglugerðin fjallar einnig um traustþjónustur og kröfur til þeirra. En hvað er traustþjónusta? Þetta orð er fólki alla jafna ekki tamt en í okkar daglega lífi þekkjum við hvað best traustþjónustu á borð við rafrænar undirskriftir sem gera okkur kleift að undirrita ýmis lögformleg skjöl í gegnum tækin okkar, svo sem bílalán, kaupsamninga o.fl. Við auðkennum okkur áður en við skrifum rafrænt undir og þannig á mótaðili að geta treyst að það séu sannanlega við sem erum að skrifa undir lánið.

Þegar rætt er um traustþjónustur þarf að hafa í huga að þær flokkast í mismunandi flokka, fullgildar og ófullgildar.

Fullgildar traustþjónustur þurfa að uppfylla mun ítarlegri kröfur og undirgangast heildstætt mat á hlítingu á tveggja ára fresti hjá vottuðum aðila og eftirlitsstjórnvaldi. Fullgilding á traustþjónustu hlýst eingöngu eftir slíkt ferli og eru traustþjónusturnar skráðar á traustlista Evrópusambandsins.

Ófullgildar traustþjónustur ganga ekki í gegnum framangreint ferli þótt vissulega eigi þær að uppfylla ákveðnar kröfur. Ekki eru framkvæmdar úttektir á hlítingu við kröfur og aðilum er óheimilt að markaðssetja sig sem fullgildar traustþjónustur.

Aðilar sem vilja auka stafræna þjónustu og sjálfvirknivæðingu, svo sem við gerð umsókna, gagnaskila, samninga o.fl., ættu ávallt að kynna sér þessar kröfur út frá því hvaða gögn og þjónustu er um að ræða. Þannig er ekki nægjanlegt að horfa einungis til rafrænnar undirskriftar sem slíkrar þar sem þær geta verið byggðar upp á mismunandi vegu, á mismunandi fullvissustigi, með eða án samnýtingar annarrar traustþjónustu líkt og tímastimpla, sem og verið ófullgildar eða fullgildar.

Það er auðvelt að týnast í tæknilega flókinni umræðu þegar kemur að þessum málum en í raun er regluverkið að auðvelda aðilum með því að tryggja ákveðið öryggi og fullvissustig fullgildrar traustþjónustu. Regluverkið felur í raun m.a. í sér að notkun fullgildra rafrænna undirskrifta hafi sama lagagildi og eiginhandaráritun og auðkenningu á háu fullvissustigi megi líkja við að auðkenning á einstaklingi fari fram í persónu.

Í ört vaxandi stafrænu landslagi, þar sem netógnum og svikum fer fjölgandi, verður ekki undan því vikist að tryggja með sem bestum hætti öryggi og traust í stafrænni þjónustu. Nýting aðila, sér í lagi opinberra aðila, á traustþjónustum verður því að ná lengra en eingöngu til rafrænnar auðkenningar og undirskrifta sem slíkra. Horfa þarf til öryggis slíkra lausna sem og samnýtingar á öðrum tegundum traustþjónustu í allri virðiskeðju þjónustunnar.

> Það er afar mikilvægt að allir aðilar sem eru á stafrænni vegferð meti með ítarlegum hætti hvaða kröfur eru gerðar til þeirra þjónustu og upplýsinga sem þau veita og meðhöndla.

Hér á landi eru aðilar á markaði sem veita fullgilda traustþjónustu sem ýmist hefur verið veitt fullgilding af Fjarskiptastofu eða stjórnvaldi í öðrum ríkjum á EES-svæðinu. Þá er einnig í boði nokkurt magn af ófullgildum traustþjónustum sem ekki hafa hlotið fullgildingu á grundvelli yfirferðar á heildstæðu mati á hlítni við þær tækni- og öryggiskröfur sem gilda um þær. Slíkar þjónustur geta vel verið hentugur kostur en það þarf ávallt að hafa í huga hvert markmið þjónustunnar er, hvaða upplýsingar verið er að meðhöndla sem og hvert lögmætið og fullvissutigið þarf að vera.

Það kemur ekki á óvart að í nýrri netöryggislöggjöf Evrópusambandsins (NIS-2), sem verið er að innleiða um alla Evrópu, eru mikilvægir innviðir sérstaklega hvattir til að nýta sér einungis fullgildar traustþjónustur við veitingu þjónustu sinnar. Hér er vert að geta að gildissvið netöryggislöggjafarinnar er nokkuð víðtækt og nær m.a. til opinberra stofnana.

Traust almennings á stafrænni þjónustu er forsenda framþróunar á hinu stafræna sviði. Að fólk vilji nýta sér slíka þjónustu, hún uppfylli lögmætar kröfur og að fólk geti treyst því að oft viðkvæmar upplýsingar þess séu verndaðar. Það er því afar mikilvægt að allir aðilar sem eru á stafrænni vegferð meti með ítarlegum hætti hvaða kröfur eru gerðar til þeirra þjónustu og upplýsinga sem þau veita og meðhöndla. Val á viðeigandi traustþjónustu verður að mæta þeim kröfum og byggjast á réttu öryggis- og fullvissustigi. Það er því afar mikilvægt að óska skýrra upplýsinga frá mögulegum traustþjónustuveitendum um hvort eða hvernig umrædd þjónusta kemur til móts við umræddar kröfur.

Ísland státar af því að vera hvað lengst komið í veitingu opinberrar þjónustu með stafrænum hætti. Það fylgir því ákveðin ábyrgð í því að tryggja öryggi þjónustunnar og efla traust almennings á henni.

Höfundur er sviðsstjóri stafræns öryggis hjá Fjarskiptastofu.