ÚRSKURÐUR
ÁFRÝJUNARNEFNDAR NEYTENDAMÁLA

MÁL NR. 5/2016

Kæra Friðjóns Guðjohnsen á ákvörðun Neytendastofu nr. 35/2016.

1. Þann 20. október 2016 er tekið fyrir mál áfrýjunarnefndar neytendamála nr. 5/2016: Kæra Friðjóns Guðjohnsen á ákvörðun Neytendastofu nr. 35/2016 frá 13. júlí 2016. Í málinu úrskurða Halldóra Þorsteinsdóttir, Áslaug Árnadóttir og Egill Heiðar Gíslason.

2. Með kæru, dags. 11. ágúst 2016, hefur kærandi kært til áfrýjunarnefndar neytendamála ákvörðun Neytendastofu nr. 35/2016 frá 13. júlí 2016 um að ekki sé ástæða til aðgerða vegna ábendingar kæranda um ætlaða öryggisgalla í rafrænum skilríkjalausnum Auðkennis ehf. Kærandi krefst þess að „nefndin úrskurði að Neytendastofu beri að láta fara fram endurskoðun á búnaði og kerfum Auðkennis og eftir atvikum endurskoði hvort lausnin uppfyllir þau skilyrði að geta talist fullgild í skilningi laganna.“ Þá krefst hann úrskurðar nefndarinnar um hvort „áskriftarskilmálar Auðkennis, sér í lagi grein 6.5, séu eðlilegir og sanngjarnir í garð neytenda og hlutist til um að þeim verði breytt sé niðurstaðan sú að þeir séu ósanngjarnir eða óeðlilegir.“ Loks krefst kærandi þess að Neytendastofu verði gert að upplýsa um nánar tilgreind atriði varðandi vottun lausna Auðkennis ehf.

3. Mál þetta varðar lög nr. 28/2001 um rafrænar undirskriftir. Samkvæmt 6. mgr. 18. gr. laganna verður ákvörðunum sem Neytendastofa tekur á grundvelli laganna skotið til áfrýjunarnefndar neytendamála, sbr. 2. mgr. 4. gr. laga um Neytendastofu nr. 62/2005.

MÁLAVEXTIR

4. Með bréfi kæranda, dags. 15. september 2014, var Neytendastofu bent á ætlaðan öryggisgalla á rafrænum skilríkjalausnum Auðkennis ehf. sem kærandi kvaðst hafa uppgötvað eftir athugun á öryggi þeirra. Í bréfinu kemur fram að svokallað PIN númer notenda sé ekki varið með fullnægjandi hætti þegar lausn Auðkennis ehf., sem beri heitið „Rafræn skilríki í farsíma“, sé notuð í snjallsíma. Væri öðrum hugbúnaði komið fyrir í símanum gæti sá hugbúnaður miðlað umræddu PIN-númeri til annars kerfis. Gæti „meinfýsinn árásaraðili“ nýtt sér þetta til að villa á sér heimildir sem rétthafi auðkennisins. Fylgdi bréfinu fylgiskjal þar sem prófun kæranda var lýst. Samkvæmt skilgreiningu 2. mgr. 8. gr. laga nr. 28/2001 um rafrænar undirskriftir eigi „öruggur undirskriftabúnaður“ að tryggja leynd undirskriftagagna undirritanda og sé ljóst að lausn Auðkennis ehf. uppfylli ekki þennan áskilnað, enda sé vernd PIN-númers notanda ábótavant. Af þessum sökum sé ekki unnt að líta á undirskriftir með þessari lausn sem „fullgildar rafrænar undirskriftir“ í skilningi sömu laga.

5. Í bréfinu kemur fram að kærandi telji prófanir sínar gefa sterkar vísbendingar um að gera þurfi frekari „árásarmiðaðar öryggisprófanir“ á öllum skilríkjalausnum Auðkennis ehf. af aðilum með sérþekkingu á þessu sviði. Eigi rafrænar undirskriftir að hafa sömu þýðingu og undirskriftir á pappír þurfi kröfur til „öruggs undirskriftarbúnaðar“ í skilningi laganna að vera túlkaðar nógu þröngt til að ekki sé auðvelt að framkalla slíkar undirskriftir án samþykkis réttmæts undirritanda. Kærandi hafi áhyggjur af því að á markaðnum sé lausn eins og „Rafræn skilríki í farsíma“ sem gefi fyrirheit um öryggi en sé haldin alvarlegum öryggisgalla. Gera verði kröfu um að öll rafræn skilríki fyrir farsíma sem gefin hafi verið út verði afturkölluð tafarlaust. Þá verði að stöðva frekari útgáfu slíkra skilríkja þangað til tekið hafi verið á umræddum öryggisgalla. Meðfylgjandi bréfi kæranda var fylgiskjal þar sem umræddum öryggisgalla var lýst. Þar kemur fram hvernig unnt sé að koma fyrir njósnahugbúnaði á snjallsíma annars manns, skila símanum aftur til hans, nota njósnahugbúnaðinn til að komast að PIN númeri hans, koma aftur höndum yfir símann og geta þá notað rafræna undirskrift eigandans.

6. Með bréfi Neytendastofu til kæranda, dags. 30. október 2014, kemur fram að um fullgild rafræn skilríki, útgáfu þeirra og eftirlit gildi ákvæði laga nr. 28/2001, sbr. og reglugerð nr. 780/2011. Framangreind lög og reglur séu innleiðing á tilskipun Evrópusambandsins nr. 93/1999 um rafrænar undirskriftir. Í reglunum sé að finna ítarleg ákvæði um vernd og öryggiskröfur sem gerðar séu til fullgildra rafrænna undirskrifta. Auðkenni ehf. sé eini aðilinn hér á landi sem hafi tilkynnt um starfsemi sína og gefi út fullgild rafræn skilríki í skilningi laga nr. 28/2001. Í samræmi við ákvæði laganna hafi Neytendastofa yfirfarið öll gögn sem Auðkenni ehf. sé skylt að leggja fram, sbr. 22. gr. reglugerðar nr. 780/2011. Einnig fái Neytendastofa upplýsingar frá hinum eftirlitsskylda aðila þegar og ef breytingar verði á atriðum sem skylt sé að upplýsa stofnunina um vegna eftirlits hennar. Neytendastofu sé einnig heimilt að krefjast þess að endurskoðun fari fram á kerfi, búnaði og starfsskipulagi vottunaraðila sem gefi út fullgild vottorð telji hún að rökstuddur grunur sé fyrir hendi um að framangreind atriði fullnægi ekki kröfum laga, reglugerða, tilvísana til staðla og annarra samþykktra kröfuskjala um innihald fullgildra vottorða og öruggan undirskriftarbúnað.

7. Í bréfi Neytendastofu segir að í framhaldi af ábendingu kæranda hafi stofnunin sent erindi hans til umsagnar Auðkennis ehf. 15. september 2014 og veitt frest til andsvara í samræmi við 13. gr. stjórnsýslulaga nr. 37/1993. Svar hafi borist frá Auðkenni ehf. 24. sama mánaðar. Neytendastofa hafi yfirfarið erindi kæranda og svör Auðkennis ehf. og komist að þeirri niðurstöðu að sú áhætta varðandi öryggi sem kærandi hafi bent á tengist að öllu leyti áhættuþáttum sem séu á ábyrgð einstaklinga og því utan þeirrar kerfisáhættu sem lög nr. 28/2001, reglugerð nr. 780/2011, stöðlum og öðrum kröfuskjölum sé ætlað að vernda og falli undir opinbert eftirlit Neytendastofu. Ekki sé ástæða til að fara fram á endurskoðun á kerfi eða búnaði Auðkennis ehf., enda ekkert sem bendi til þess að áhættuþættirnir sem kærandi hafi bent á að séu fræðilega fyrir hendi geti tengst starfsemi félagsins, kerfi eða búnaði, sem að öðru leyti uppfylli skilyrði laga, reglugerða og staðla sem um starfsemina gildi.

8. Í bréfinu er einnig vísað til þess að 23. október 2014 hafi borist beiðni frá kæranda um að honum verði afhent „öll þau gögn sem Neytendastofa hafi um málið, þar með niðurstöðu þess, sé málinu lokið af hálfu Neytendastofu“. Samkvæmt 4. mgr. 20. gr. laga nr. 28/2001, sbr. og „lög nr. 50/1996“, séu gögn sem varði starfsemi vottunaraðila og útgáfu fullgildra rafrænna skilríkja bundin trúnaði af hálfu eftirlitsaðila, þ.e. Neytendastofu. Þó geti stofnunin látið í té skjalið „Kröfur til öruggs undirskriftarbúnaðar“, þar sem þeim kröfum, sem gerðar séu til öruggs undirskriftarbúnaðar hjá Auðkenni ehf., sé lýst. Að öðru leyti sé ekki ástæða til frekari aðgerða og sé málinu því lokið af hálfu stofnunarinnar. Í bréfinu var ennfremur vísað til ákvæða gildandi laga og reglugerða um kröfur til starfsemi vottunaraðila.

9. Af hálfu kæranda var fyrrgreindri ákvörðun skotið til áfrýjunarnefndarinnar með kæru, dags. 2. mars 2015. Í úrskurði hennar 11. júní 2015 í máli 5/2015 var m.a. vísað til þess að nefndin hefði í framkvæmt viðurkennt að neytendur sem leituðu til Neytendastofu vegna ætlaðra brota á lögum á málefnasviði hennar, og vörðuðu viðskipti sem þeir hefðu tekið þátt í, kynnu að teljast aðilar að málum sem stofnunin tæki til meðferðar í tilefni af kvörtun þeirra. Rakið var að kærandi hefði verið notandi rafrænna skilríkja Auðkennis ehf. og yrði ekki annað ráðið en að hann væri viðskiptavinur félagsins. Erindi kæranda til Neytendastofu lyti að því hvort sú þjónusta sem Auðkenni ehf. veitti honum væri eins trygg og áskilið væri samkvæmt lögum nr. 28/2001, sem Neytendastofa hefði eftirlit með. Meðal annars með vísan til þessa var fallist á það með kæranda að Neytendastofu hefði borið að líta á hann sem aðila þess stjórnsýslumáls sem stofnunin hóf gagnvart Auðkenni ehf. greint sinn. Þar sem kærandi hefði ekki notið réttinda stjórnsýslulaga nr. 37/1993 við úrlausn málsins, m.a. varðandi aðgang að gögnum samkvæmt 1. mgr. 15. gr. laganna, hefði hann ekki átt þess kost að gæta hagsmuna sinna eins og hann hefði átt rétt á og yrði því að fella hina kærðu ákvörðun úr gildi.

10. Með bréfi kæranda til Neytendastofu, dags. 14. júlí 2015, var þess óskað að stofnunin tæki mál hans upp að nýju. Mun Neytendastofa í kjölfarið hafa óskað eftir skýringum og athugasemdum Auðkennis ehf. og á tímabilinu 21. júlí til 18. desember 2015 átti stofnunin í margs konar samskiptum við aðila máls sem ekki er ástæða til að rekja frekar.

MÁLAVEXTIR

11. Í niðurstöðukafla hinnar kærðu ákvörðunar er rakið að um fullgild rafræn skilríki, útgáfu þeirra og eftirlit gildi ákvæði laga nr. 28/2001 um rafrænar undirskriftir, sbr. og reglugerð nr. 780/2011. Umrædd lög og reglur séu innleiðing á tilskipun Evrópusambandsins nr. 93/1999 um rafrænar undirskriftir. Í reglunum sé að finna ítarleg ákvæði um vernd og öryggiskröfur sem gerðar séu til fullgildra rafrænna undirskrifta sem ætíð skuli teljast fullnægjandi ef í lögum eða öðrum stjórnvaldsfyrirmælum séu gerð skilyrði um undirskrift af hálfu einstaklinga. Samkvæmt 6. tölulið 3. gr. laga nr. 28/2001 sé „undirskriftarbúnaður“ hugbúnaður eða vélbúnaður sem notaður sé til að mynda rafræna undirskrift með hjálp undirskriftargagna. Samkvæmt 5. tölulið 3. gr. laganna séu „undirskriftargögn“ einstök gögn, svo sem kótar eða einkalykill dulritunar,

sem undirritandi noti til að mynda rafræna undirskrift. Samkvæmt 7. tölulið 3. gr. sé sá undirskriftarbúnaður öruggur sem fullnægi skilyrðum sem kveðið sé á um í 8. og 9. gr. laganna.

12. Þá er rakið að samkvæmt ummælum í greinargerð með frumvarpi til laga nr. 28/2001 teljist undirskriftarbúnaður búnaður sem sé notaður við gerð rafrænu undirskriftarinnar. Búnaðurinn noti undirskriftargögnin til að búa til undirskriftina. Búnaðurinn geti bæði verið vélbúnaður og hugbúnaður. Sem dæmi um vélbúnað megi t.d. nefna snjallkort og sem dæmi um hugbúnað megi nefna hluta tölvupóstforrits. Samkvæmt 8. gr. laganna skuli öruggur undirskriftarbúnaður 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.“ Samkvæmt ummælum í greinargerð með frumvarpi til laga nr. 28/2001 byggi ákvæðið á III. viðauka tilskipunarinnar sem geri tilteknar kröfur til undirskriftarbúnaðar til að tryggja ákveðið öryggisstig. Búnaður sem uppfylli þessar kröfur geti verið notaður til að mynda fullgildar rafrænar undirskriftir.

13. Samkvæmt 9. gr. laganna skuli kröfum til undirskriftabúnaðar samkvæmt 8. gr. laganna talist fullnægt þegar: „a. þar til bær aðili hefur staðfest að hann uppfylli kröfur 8. gr.; ráðherra geti í reglugerð kveðið á um þá aðila sem veitt geta slíka staðfestingu, eða b. þar til bær aðili á Evrópska efnahagssvæðinu eða í aðildarríki stofnsamnings Fríverslunarsamtaka Evrópu hefur viðurkennt hann. Líta skal svo á að undirskriftarbúnaður teljist öruggur skv. 8. gr. ef hann er í samræmi við staðla sem framkvæmdastjórn Evrópusambandsins hefur sett um slíkan búnað og birtir hafa verið í Stjórnartíðindum Evrópubandalagsins.“ Í ummælum í greinargerð með frumvarpi til laga nr. 28/2001 segi að í 9. gr. sé gerð grein fyrir því hvernig undirskriftarbúnaður fái viðurkenningu sem öruggur, þ.e. að hann uppfylli ákvæði 8. gr. frumvarpsins. Ákvæðið byggi á 4. mgr. 3. gr. tilskipunar 1999/93/EB. Í almennum athugasemdum með frumvarpinu segi jafnframt að líta skuli svo á að undirskriftabúnaður sé öruggur sé hann í samræmi við staðla sem framkvæmdastjórn Evrópusambandsins hafi sett og birtir hafi verið í stjórnartíðindum ESB.

14. Samkvæmt 20. gr. reglugerðar nr. 780/2011 um rafrænar undirskriftir teljist undirskriftarbúnaður fyrirfram ávallt öruggur samkvæmt ákvæðum greinarinnar sé hann í samræmi við staðla og önnur kröfuskjöl sem framkvæmdastjórn Evrópusambandsins hafi ályktað um og gefið út tilvísanir til og birtar séu í Stjórnartíðindum Evrópusambandsins. Samkvæmt 1. mgr. 21. gr. reglugerðarinnar teljist kröfum til undirskriftarbúnaðar samkvæmt 19. og 20. gr. reglugerðarinnar fullnægt þegar hann hafi 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. Á grundvelli 3. mgr. 21. gr. reglugerðarinnar kanni Neytendastofa upplýsingar um og staðfestingar á að úttekt og vottun undirskriftarbúnaðar uppfylli grunnkröfur, staðla og önnur

samþykkt kröfuskjöl í samræmi við ákvæði reglugerðarinnar og hafi verið gerð af þar til bærum aðila sem uppfyllir skilyrði þessarar greinar. Neytendastofa geti óskað eftir gögnum og upplýsingum sem hún telji nauðsynlegar til þess að leggja mat á hæfni, hæfi og sjálfstæði aðila sem annast frumúttektir og reglulegar úttektir samkvæmt ákvæðum reglugerðarinnar.

15. Í ákvörðuninni segir síðan að Auðkenni ehf. sé eini aðilinn hér á landi sem tilkynnt hafi um starfsemi sína og gefi út fullgild rafræn skilríki í skilningi laga nr. 28/2001. Í samræmi við ákvæði laganna hafi Neytendastofa yfirfarið öll gögn sem félaginu sem eftirlitsskyldum aðila sé skylt að leggja fram, sbr. 22. gr. reglugerðar nr. 780/2011. Jafnframt fái Neytendastofa upplýsingar þegar og ef breytingar verði á atriðum sem skylt sé að upplýsa stofnunina um vegna eftirlits hennar. Neytendastofu sé jafnframt heimilt að krefjast þess að endurskoðun fari fram á kerfi, búnaði og starfsskipulagi vottunaraðila telji hún að rökstuddur grunur sé fyrir hendi að framangreind atriði fullnægi ekki kröfum laga, reglugerða, tilvísana til staðla og annarra samþykktra kröfuskjala um innihald fullgildra vottorða og öruggan undirskriftarbúnað.

16. Neytendastofa telji að við nánari skoðun beri gögn málsins með sér að kærandi sé ekki handhafi rafrænna skilríkja sem útgefin séu af Auðkenni ehf. Í bréfi kæranda, dags. 25. janúar 2016, komi fram að kærandi hafi afturkallað rafræn skilríki sín hjá Auðkenni ehf. rúmum hálftíma eftir að hafa komið upphaflegu erindi sínu á framfæri við Neytendastofu. Þetta sé jafnframt staðfest í bréfi Auðkennis ehf., dags. 14. desember 2015. Að þessu virtu sé að mati Neytendastofu vandséð hvernig kærandi hafi beina, verulega, sérstaka eða lögvarða hagsmuni af úrlausn málsins, sjá sbr. m.a. úrskurð áfrýjunarnefndar neytendamála 6. september 2007 (6/2007). Neytendastofa bendi á að eftirlit Neytendastofu með lögum nr. 28/2001 sé tæknilega flókið og afar sérhæft allsherjarréttarlegt eftirlit. Ekki verði séð að kærandi njóti sérstakari eða beinni hagsmuna en aðrir viðskiptavinir Auðkennis ehf. eða aðrir notendur rafrænna skilríkja almennt. Með vísan til ofangreinds telji Neytendastofa að kærandi hafi ekki nægilegra hagsmuna að gæta af úrlausn málsins. Þegar af þeirri ástæðu telji Neytendastofa ekki ástæðu til aðgerða af hálfu stofnunarinnar.

17. Auk ofangreinds bendi Neytendastofa á að stofnunin hafi virkt eftirlit með Auðkenni ehf. og hafi í samræmi við 3. mgr. 21. gr. reglugerðar nr. 780/2011 yfirfarið og kannað vottorð frá aðilum á Evrópska efnahagssvæðinu sem uppfylli skilyrði b. liðar 9. gr. laga nr. 28/2001 um að undirskriftarbúnaður Auðkennis ehf. og burðarlag fyrir farsíma uppfylli sannanlega þær öryggiskröfur sem mælt sé fyrir um í tilskipun 1999/93/EB, sbr. lög nr. 28/2001 og reglugerð nr. 780/2011. Undirskriftarbúnaðurinn hafi staðist kröfur gagnvart hæsta öryggisstigi, þ.e. öryggisstigi EAL 5+. Í matsskýrslu Admon ráðgjafar um mat á fullvissustigi auðkenna 2.0., dags. 27. júní 2013, komi jafnframt fram að undirskriftarbúnaður Auðkennis ehf. nái fullvissustigi QAA.

18. Í hinni kærðu ákvörðun er næst rakið að í matsskýrslu Admon ráðgjafar fyrir rafræn skilríki undir Íslandsrót á farsímum, útgáfu 1.0, dags. 18. júní 2015, komi einnig fram að búnaðurinn fyrir rafræn skilríki í farsíma uppfylli kröfur fyrir matsþrep EAL 4+ í svonefndri Common

Criteria, sem samþykkt sé af Evrópuþinginu sem fullnægjandi fyrir öruggan undirskriftarbúnað fyrir fullgildar undirskriftir samkvæmt lögum nr. 28/2001 um rafrænar undirskriftir, sbr. ákvæði tilskipunar 1999/93/EB. Að mati Neytendastofu sé því ljóst að skilyrði laga nr. 28/2001 og reglugerðar 780/2011 teljist uppfyllt og undirskriftarbúnaður Auðkennis ehf. teljist öruggur undirskriftarbúnaður. Að því er varði ábendingar kæranda um skilgreiningu hugtaksins öruggur undirskriftarbúnaður og undirskriftargögn skuli bent á að Auðkenni ehf. notist við svonefnt dreifilyklaskipulag eða PKI kerfi til dulritunar (e. public key infrastructure). Í slíku kerfi sé það einungis einkalykill í kerfinu sjálfu sem teljist til undirritunargagns í skilningi laganna. PIN númer teljist ekki hluti undirskriftarbúnaðar þar sem hann sé ekki forsenda rafrænnar undirskriftar innan dreifilyklakerfis.

19. Í fyrrgreindri matsskýrslu Admon ráðgjafar komi einnig fram að PIN númer til auðkenningar sem viðkomandi noti til að beita einkalykli sínum fari ekki yfir samskiptatengingar við þjónustuveitu heldur einungis frá lyklaborði farsíma til örgjörva. Auk þess séu öll samskipti yfir internetið við sannvottun á rafrænum skilríkjum dulrituð. Bent sé á að það sé fræðilega mögulegt að illvilja aðili geti komist á milli lyklaborðs farsíma og örgjörva, en slík áhætta sé þekkt og nái í hverju tilviki aðeins til eins farsíma. Skaðinn sem sé fræðilega mögulegur nái því ekki til örugga undirskriftarbúnaðarins sjálfs. Undir öllum kringumstæðum verði einstaklingar að vernda þau einstaklingsbundnu gögn og tæki sem þeir eigi og noti við framkvæmd undirritunar og sýna eðlilega aðgæslu við meðferð og notkun þeirra.

20. Að lokum er í ákvörðuninni vísað til þess að í erindi kæranda sé bent á þann möguleika að með aðgæsluleysi og einbeittum brotavilja sé fræðilega unnt við ákveðnar og sérhæfðar kringumstæður að misnota fullgild rafræn skilríki. Ábendingar kæranda lúti að öryggisatriðum sem varði notkun neytandans sjálfs á þeim tækjum þar sem rafræn skilríki séu varðveitt. Neytendastofa telji ljóst að slíkir möguleikar séu hverfandi miðað við fjölda útgefinna skilríkja og séu engin slík tilvik þekkt, hvorki hér á landi né annars staðar á EES-svæðinu, þar sem sambærilegar reglur gildi um fullgildar rafrænar undirskriftir. Þess beri að gæta að mikil þjóðhagsleg hagkvæmni sé tengd því að stuðla að auknum framgangi fullgildra rafrænna skilríkja til auðkenningar og undirskrifta jafnt í viðskiptalífi sem og gagnvart stjórnvöldum. Framangreint mikilvægi þessarar tækni til undirritunar, svo og lög og reglur sem settar hafi verið um fullgildar rafrænar undirskriftir, byggi einmitt á þeirri forsendu. Jafnvel þótt kærandi hefði lögvarða hagsmuni í máli þessu telji Neytendastofa að athugasemdir hans gefi ekki tilefni til frekari aðgerða af hálfu Neytendastofu á grundvelli laga nr. 28/2001 eða reglugerðar 780/2011 vegna erindis um að hugsanlega uppfylli undirskriftarbúnaður Auðkennis ehf. ekki kröfur gildandi laga, reglna og annarra kröfuskjala, um öryggi undirskriftarbúnaðarins. Neytendastofa telji að framangreindur búnaður uppfylli gildandi kröfur og því sé ekki ástæða til frekari aðgerða í málinu.

RÖKSTUÐNINGUR KÆRENDA OG ATHUGASEMDIR NEYTENDASTOFU

21. Kærandi fer fram á að nefndin úrskurði að Neytendastofu skuli láta fara fram endurskoðun á búnaði og kerfum Auðkennis ehf. og eftir atvikum endurskoði hvort lausnin uppfylli þau skilyrði að geta talist fullgild í skilningi laganna. Enn fremur er farið fram á að nefndin úrskurði að Neytendastofa skuli meta hvort áskriftarskilmálar Auðkennis ehf., sér í lagi grein 6.5, séu eðlilegir og sanngjarnir í garð neytenda og hlutist til um að þeim verði breytt sé niðurstaðan sú að þeir séu ósanngjarnir eða óeðlilegir. Að lokum er einnig farið fram á að nefndin úrskurði að Neytendastofu beri að upplýsa um nánar tilgreind atriði varðandi vottun fullgildra lausna Auðkennis.

22. Vegna tilvísunar Neytendastofu til þess að stofnunin fari með virkt eftirlit með framkvæmd laga nr. 28/2001 um rafrænar undirskriftir bendir kærandi á að ekki komi fram í hinni kærðu ákvörðun hvaða búnaður hafi verið vottaður, hvort eingöngu hafi verið um SIM kortið sem vélbúnað að ræða eða hvort þar hafi einnig verið um að ræða þann hugbúnað sem finnska fyrirtækið Valimo hafi látið Auðkenni ehf. í té og keyri á SIM kortunum. Auðkenni ehf. hafi sjálft lýst því yfir að bandaríska fyrirtækið ViaForensics hafi vottað hugbúnaðinn sem keyri á SIM kortinu. Ljóst sé að sá aðili uppfylli ekki skilyrði laganna sem þar til bær aðili. Í kærunni er að öðru leyti vísað til efasemda kærenda um vottun lausnar Auðkennis ehf. sem fram kom í bréfi hans til Neytendastofu, dags. 26. janúar 2016.

23. Neytendastofa hafi þrátt fyrir ítrekaðar fyrirspurnir hvorki viljað upplýsa neitt frekar um það hvaða vottunaraðila um sé að ræða né til hvaða búnaðar vottunin hafi náð. Sé því engan veginn hægt að átta sig á því hvort sú vottun sem Neytendastofa vísi til nái til allrar lausnarinnar eða aðeins afmarkaðra hluta hennar. Augljóslega verði öryggi lausnar aldrei meira en öryggi veikasta hluta hennar. Þannig geti lausn sem noti t.d. vottuð SIM kort sem vélbúnað ekki talist vottuð í heild sinni ef hugbúnaður sem hluti af slíkri lausn hafi enga vottun. Varðandi leynd gagna beri stofnunin fyrir sig að gögnin séu bundin trúnaði og varði efnahagslega mikilvæga hagsmuni ríkisins, en kærandi geri í þessu samhengi athugasemd við túlkun Neytendastofu á 9. gr. og 3. tölulið 10. gr. upplýsingalaga nr. 140/2012.

24. Í kærunni kemur næst fram að í a. lið 1. mgr. 9. gr. laga nr. 28/2001 um rafrænar undirskriftir sé tiltekið að ráðherra geti í reglugerð kveðið á um þá aðila sem veitt geti þá vottun sem um ræði. Þetta hafi ekki verið gert í þeirri reglugerð nr. 780/2011 sem sett hafi verið um málaflokkinn og sé því hægt að álykta að annar þar til bær aðili á Evrópska efnahagssvæðinu hafi vottað búnaðinn í samræmi við b. lið sömu greinar. Þar sem lögin geri ráð fyrir að reglugerðir eigi að upplýsa um slíka aðila sé vandséð að nafn slíks aðila eigi að vera bundið jafnmiklum leyndarhjúp og Neytendastofa gerir ráð fyrir. Því sé óskiljanlegt hvers vegna Neytendastofa vilji ekki upplýsa um það hver sá aðili sé.

25. Það sé full ástæða til þess að lágmarks upplýsingar um vottun búnaðarins liggi fyrir almenningi. Þrátt fyrir að Neytendastofa segist hafa virkt eftirlit með rafrænum skilríkjalausnum sé

stofnunin vanbúin til að sinna slíku eftirliti. Þannig hafi stofnunin upplýst í bréfi til kæranda, dags 31. maí 2016, að hún hafi engar prófanir eða úttektir gert eða látið gera að eigin frumkvæði á öryggi lausna Auðkennis ehf. Þessi málaflokkur hafi einnig setið á hakanum hjá stofnuninni vegna niðurskurðar hjá henni. Vísa megi til ummæla í ársskýrslu Neytendastofu fyrir árið 2014 þar sem fram komi að forstjóri stofnunarinnar stýri starfsemi öryggissviðs vegna niðurskurðar, en það svið sinni meðal annars málum tengdum rafrænum undirskriftum. Ekki sé heldur að sjá að stofnunin hafi á að skipa sérmenntuðum starfsmönnum á þessu sviði, enda virðist stofnunin ítrekað hafa reitt sig á tækniþekkingu hins eftirlitsskylda aðila eða aðila tengdra honum. Sem dæmi megi nefna að ekki verði séð að stofnunin hafi sjálf sannreynt þennan öryggisveikleika sem kærandi bendi á. Hins vegar hafi Auðkenni ehf. sannreynt þennan öryggisveikleika eins og fram komi í bréfi þess til Neytendastofu, dags. 24. september 2014.

26. Neytendastofa vísi til álits einkafyrirtækisins Admon ráðgjöf ehf. um rafræn skilríki. Út frá þessu áliti komist Neytendastofa svo að þeirri niðurstöðu að skilyrði laga nr. 28/2001 og reglugerðar 780/2011 séu uppfyllt og að undirskriftarbúnaður Auðkennis ehf. teljist öruggur undirskriftarbúnaður. Fyrirtækið Admon ráðgjöf ehf. sé nátengt uppbyggingu dreifilyklaskipulagsins sem rafræn skilríkjalausn Auðkennis ehf. byggi á. Admon ehf. sé m.a. höfundur skilgreininga og kröfuskjala í tengslum við slíkt dreifilyklaskipulag, auk þess sem fyrirtækið hafi ritstýrt öllum sameiginlegum skjölum samstarfsverkefnisins. Fyrirtækið hafi að eigin sögn einnig verið í samstarfi við ýmsa lausnaraðila og birgja sem sérhæfi sig í lausnum fyrir rafræn skilríki. Líklegt verði að telja að Auðkenni ehf. sé meðal þessara lausnaraðila þar sem það sé eini slíki aðilinn starfandi hér á landi.

27. Þar sem fullyrðing Neytendastofu um að búnaðurinn uppfylli skilyrði laganna sé sett fram í beinu framhaldi af vísun til álits Admon ráðgjafar ehf. sé ekki annað hægt en að álykta að Neytendastofa byggi þessa niðurstöðu sína á þessu áliti. Hér sé því verið að byggja á áliti aðila sem hafi verið í samstarfi við lausnaraðila á sviði rafrænna skilríkja og tekið þátt í uppbyggingu slíkra kerfa. Neytendastofa virðist þannig aftur reiða sig á tæknilegt álit lausnaraðila og aðila þeim tengdum. Ekki verði séð að stofnunin hafi við þessa niðurstöðu sinnt rannsóknarskyldu sinni sem stjórnvald á fullnægjandi hátt. Þá hafi Neytendastofa hafnað að telja gögn um vottun undirskriftarbúnaðarins til gagna í málinu, líkt og kærandi hafi farið fram á með bréfi, dags. 29. júní 2016. Þessi fullyrðing Neytendastofu um samræmi undirskriftarbúnaðarins við lög geti því ekki talist byggð á slíkum gögnum.

28. Varðandi undirskriftargögn, einkalykil og PIN númer bendi kærandi á að í hinni kærðu ákvörðun taki Neytendastofa fram að Auðkenni ehf. notist við svonefnt dreifilyklaskipulag eða PKI kerfi til dulritunar (e. public key infrastructure). Telji stofnunin að í slíku kerfi teljist einungis einkalykill í kerfinu sjálfu til undirskriftargagns í skilningi laga nr. 28/2001. Sé því ekki annað að sjá en að Neytendastofa hafni því að líta á PIN númer sem notandi noti til að framkalla undirskrift sem undirskriftargagn í skilningi laganna. Þetta sjónarmið, þ.e. hvað teljist til undirskriftargagna í skilningi laganna, sé ekki rökstutt frekar í ákvörðuninni.

29. Kærandi hafi mótmælt slíkri túlkun og rökstyðji ítarlega hvers vegna líta skuli á PIN númer sem undirskriftargögn í skilningi laganna í bréfi sínu til Neytendastofu, dags. 25. janúar 2016. Rétt sé að benda á að sé fallist á þá túlkun Neytendastofu komi til álita hvort lausnin uppfylli skilyrði c. liðar 1. mgr. 8. greinar laganna. Þar segi að öruggur undirskriftarbúnaður skuli tryggja að undirskriftargögnin séu varin með fullnægjandi hætti gegn notkun annarra en undirritanda. Verði ekki litið á PIN númer sem undirskriftargögn heldur aðeins sem einhvers konar öryggisráðstöfun af hendi hönnuðar lausnar Auðkennis ehf. sé ljóst að þessi öryggisráðstöfun tryggi ekki að einkalykillinn sé varinn með fullnægjandi hætti gegn notkun annarra en undirritanda. Þetta sé ljóst af lýsingu kæranda á öryggisveikleika lausnarinnar. Óprúttinn aðili geti með aðgangi að síma fórnarlambsins framkallað undirskriftir í hans nafni með því að nota einkalykil rafrænna skilríkja undirritandans.

30. Í kærunni kemur næst fram að í hinni kærðu ákvörðun sé að finna afar einkennilega fullyrðingu þess efnis að PIN númer teljist „ekki ekki“ hluti undirskriftarbúnaðar þar sem það sé ekki forsenda rafrænnar undirskriftar innan dreifilyklakerfisins. Kærandi bendi á að augljóslega sé undirskriftarbúnaður nauðsynlegur til þess að framkalla rafrænar undirskriftir. Fullyrðingin standist því ekki, enda ekki í samræmi eða samhengi við nálægar setningar. Hér gæti meiningin verið það álit Neytendastofu að PIN númer teljist ekki til hluta undirskriftargagna og sé það túlkun kæranda sem hér sé byggt á. Líklega hafi Neytendastofa átt við að PIN númer teljist ekki hluti undirskriftargagnanna þar sem það sé ekki forsenda rafrænnar undirskriftar innan dreifilyklakerfisins. Hafi þetta verið afstaða Neytendastofu sé rétt að benda á að einkalykillinn sé geymdur dulkóðaður á SIM kortinu. Með því að beita PIN númerinu sé einkalykillinn afruglaður þannig að hægt sé að nýta hann til að framkalla rafræna undirskrift. Notandi undirskriftarbúnaðarins verði aldrei var við einkalykilinn og hafi ekki aðgang að honum. Hins vegar slái notandinn inn PIN númerið og sé það því kóði sem gagnvart notandanum sé notaður til að framkalla rafrænu undirskriftina. Gagnvart notandanum sé þá PIN númerið (þ.e. innsláttur á því) einmitt orðin forsenda fyrir því að hægt sé að framkalla rafræna undirskrift. Ekki sé mögulegt fyrir notanda að framkalla undirskrift án þess að hafa PIN númerið.

31. Í hinni kærðu ákvörðun sé byggt á því að einstaklingar verði að vernda þau einstaklingsbundnu gögn og tæki sem þeir eigi og noti við framkvæmd undirritunar og sýna eðlilega aðgæslu við alla meðferð og notkun. Hér sé um að ræða mjög opna og matskennda fullyrðingu. Hvorki Neytendastofa né Auðkenni ehf. hafi gefið út hvað sé „eðlileg aðgæsla“. Sú misnotkun sem kærandi hafi lýst að óprúttnir aðilar geti framkvæmt byggi á því að fá lánaðan síma hjá notanda eða komast á annan hátt í símtæki notandans. Tilvitnun stofnunarinnar til „eðlilegrar aðgæslu“ veki upp margar spurningar. Spyrja megi hvort aðili sem láni síma eða skilji hann við sig um stundarsakir teljist hafa brugðist við með eðlilegri aðgæslu eða hvort aðili sem noti þráðlaust net í eigu annarra hafi sýnt af sér eðlilega aðgæslu. Sama megi spyrja um aðila sem hafi frestað því að uppfæra símtæki sitt með hugbúnaðarbreytingum framleiðanda. Hvorki Auðkenni ehf. né Neytendastofa hafa gefið út neinar leiðbeiningar um hvað teljist til eðlilegrar aðgæslu. Á hinn bóginn komi fram í áskriftarskilmálum Auðkennis ehf. vegna rafrænna skilríkja sú

skuldbinding í grein 6.5 að „áskrifandi ber ábyrgð á öllum aðgerðum sem framkvæmdar eru með rafrænum skilríkjum”. Ekki verði betur séð en áskrifandi sé þannig ábyrgur fyrir misnotkun sem hann gæti orðið fyrir af völdum óprúttins aðila.

32. Með þessu sé verið að koma mjög stóru ábyrgðarhlutverki á herðar áskrifendum sem engan veginn sé hægt að telja eðlilegt eða sanngjarnt. Hafa beri í huga að þessi áskriftarsamningur sé gerður með miklum aðstöðumun milli aðila. Annars vegar sé um að ræða fyrirtæki sem hafi sérhæft sig í öryggi og rafrænum skilríkjum og sé eitt um að bjóða meint fullgild rafræn skilríki á íslenskum markaði. Hins vegar sé um að ræða áskrifendur, þ.e. almenning, sem ekki sé hægt að ganga út frá að séu sérfræðingar í öryggismálum farsíma. Þrýstingur sé frá stjórnvöldum um að almenningur fái sér slík rafræn skilríki, sbr. ákvörðun ríkisstjórnarinnar í svokallaðri höfuðstólsleiðréttingu, auk hugmynda skattayfirvalda um að gera slík skilríki að skyldu. Þrátt fyrir það séu þessir áskrifendur gerðir ábyrgir fyrir öllum aðgerðum sem framkvæmdar séu með rafrænum skilríkjum.

33. Hér þurfi einnig að líta til þess að verði áskrifandi fyrir misnotkun áþekkri þeirri sem kærandi lýsi sé engan veginn víst að hann geri sér grein fyrir því hvernig slíkri misnotkun hafi verið beitt. Aðeins standi eftir rafræn undirskrift eða önnur aðgerð sem telja megi víst að hafi verið gerð með rafrænum skilríkjum áskrifandans. Neiti áskrifandinn að hafa framkvæmt þessa aðgerð sé ekki annað að sjá af áskriftarskilmálunum en að hann beri engu að síður ábyrgð á henni. Töluvert vanti upp á að áskrifendum sé gerð grein fyrir þessari skyldu sinni af hálfu Auðkennis ehf., auk þess sem slík leiðbeiningaskylda kunni að hvíla á Neytendastofu. Augljóst sé að talsverður kostnaður fylgi því að tryggja öryggi lausnarinnar með viðeigandi hætti, bæði í peningum, tíma og breyttri notkun á farsímanum. Þannig verði hægt að auka öryggið umtalsvert, t.d. með því að nota ekki sama farsíma fyrir rafræn skilríki og fyrir aðra notkun, uppfæra síma reglulega, nota ekki þráðlaus net og lána ekki síma ásamt mörgum fleirum aðgerðum. Þótt Auðkenni ehf. sé sérfróður aðili á sviði öryggismála leiðbeini fyrirtækið áskrifendum sínum ekki í þessum efnum, heldur varpi allri ábyrgðinni á hendur áskrifanda.

34. Til þess að sinna þeirri skyldu að vernda einkalykil sinn þurfi áskrifandi að vera mjög vel upplýstur um öryggismál farsíma og ábyrga öryggishegðun. Og jafnvel þótt viðkomandi fari eftir öllum góðum venjum í öryggismálum sé hreint ekki hægt að útiloka að hann verði fyrir misnotkun og að gerð verði aðgerð með rafrænum skilríkjum hans sem hann ekki stóð að sjálfur. Engu að síður beri hann samkvæmt áskriftarskilmálunum ábyrgð á þannig aðgerðum. Það ákvæði í áskriftarsamningi Auðkennis ehf., um að áskrifandi beri ábyrgð á öllum aðgerðum sem framkvæmdar séu með rafrænum skilríkjum, sé því augljóslega ósanngjarnt. Áskrifandi ætti einungis að bera ábyrgð á þeim aðgerðum sem óumdeilt sé að hann hafi sjálfur gert með rafrænu skilríkjunum. Þetta sé sérstaklega mikilvægt í ljósi þess að sýnt hafi verið fram á að vel sé mögulegt að slíkar aðgerðir séu gerðar af öðrum aðilum en áskrifanda.

35. Þrátt fyrir að Neytendastofa hafi í ákvörðun sinni samþykkt ósk kæranda um að telja áskriftarskilmála Auðkennis ehf. til gagna í málinu sé ekki að sjá í ákvörðuninni nein merki um

að stofnunin hafi lagt mat á hvort þessir skilmálar séu sanngjarnir og eðlilegir. Að öðru leyti komi í fram í hinni kærðu ákvörðun að möguleikar á misnotkun líkt og þeirri sem kærandi lýsi séu hverfandi. Sé það rökstutt með því að mikill fjöldi skilríkja hafi verið gefinn út og að engin þekkt tilvik liggi fyrir um slíka misnotkun, hvorki hérlendis né annars staðar á EES svæðinu þar sem sambærilegar reglur gildi. Neytendastofa hafi ekki lagt mat á misnotkunina enda segi stofnunin hana einungis fræðilega þótt henni hafi verið afhent leiðbeiningar um hvernig hægt sé að hagnýta hana. Hvergi í gögnum málsins komi fram að stofnunin hafi sjálf sannreynt að þessi misnotkun sé möguleg. Renni þetta stoðum undir það álit kæranda að stofnunin hafi í máli þessu vanrækt rannsóknarskyldu sína sem stjórnvald, sbr. 10. gr. stjórnsýslulaga nr. 37/1993.

36. Þótt sambærilegar reglur gildi annars staðar á EES svæðinu komi ekki fram í hinni kærðu ákvörðun hvar finna megi slíkar fullgildar rafrænar skilríkjalausnir í notkun á svæðinu. Þar sé ekki heldur að finna útlistun á hvar sambærilegar fullgildar rafrænar skilríkjalausnir fyrir farsíma sé að finna. Ljóst sé þó að sú lausn sem Auðkenni ehf. bjóði upp á sé eingöngu í boði hér á Íslandi og sé ekki í notkun annars staðar á EES svæðinu. Neytendastofa virðist ekki hafa kynnt sér þetta mál til hlítar og bendi kærandi aftur á rannsóknarreglu stjórnsýslulaga í þessu samhengi.

37. Varðandi ábendingar Neytendastofu um þjóðhagslega hagkvæmni tengda framgangi fullgildra rafrænna skilríkja horfi stofnunin framhjá þeirri staðreynd að notagildi slíkra skilríkja sé háð því að hafið sé yfir vafa að misnotkun þeirra sé möguleg. Í raun megi segja að rafræn skilríki og rafrænar undirskriftir nýtist til þess að leysa úr ágreiningi sem kunni að koma upp um hver undirriti hvað. Ef auðvelt sé að sýna fram á hvernig slíkar undirskriftir sé hægt að kalla fram án samþykkis undirritanda sé notagildi þeirra lítið sem ekkert við slíkan ágreining. Aðili sem með réttu eða röngu haldi því fram að hann hafi ekki framkallað tiltekna rafræna undirskrift geti alltaf bent á þann möguleika að annar aðili hafi komist í síma hans og framkallað undirskrift án hans vitneskju eða samþykkis. Rafrænni undirskrift sé ætlað að sýna fram á að undirritandi hafi samþykkt tiltekið rafrænt skjal. Með lögum nr. 28/2001 sé fullgildum rafrænum undirskriftum færð sama staða og undirritunum með öðrum leiðum, t.d. á pappír, að því gefnu að þær uppfylli skilyrði laganna.

38. Sá meginmunur sé þó þarna á að sönnunarbyrði sé í reynd snúið við þegar komi að rafrænum undirskriftum. Ef upp komi ágreiningur um hver hafi undirritað skjal með penna á pappír sé alltaf hægt að skoða skjalið sjálft. Slíkar undirskriftir séu ekki ófalsanlegar, en tæknin á bak við undirskrift á pappír sé ekki flókin. Margra alda hefð sé fyrir slíkum undirskriftum og dómstólar hafi tekið afstöðu til álitaefna hvað þær snerti. Sá sem haldið er fram að hafi skrifað undir skjal sem hann hafi ekki gert sé í ágætis aðstöðu til að hrekja slíkt. Rafræn undirskrift sé hins vegar bara mynstur af núllum og einum. Hægt sé að sýna fram á að til þess að gera þessa undirskrift þurfi tiltekinn einkalykil (sem er annað mynstur af núllum og einum). Í lausn Auðkennis ehf. sé þessi einkalykill geymdur, dulkóðaður með PIN númeri á SIM korti símans.

39. Þetta sé hreint ekki það sama og að fullyrða að undirritandi hafi sjálfur að yfirlögðu ráði framkallað umrædda undirskrift. Til þess að svo sé þurfi öll lausnin að vera örugg, og vottuð sem slík, en ekki bara einstakir hlutar hennar. Ef þetta öryggi sé ekki til staðar sé fullkomlega órökrétt af undirritanda að taka á sig þá skuldbindingu að vera bundinn af undirritunum gerðum með rafrænum skilríkjum. Aðstaða aðila sem vilji hrekja slíka rafræna undirskrift, sem sé ekki frá honum komin, sé mjög slæm og þurfi viðkomandi að hafa á hreinu allar tæknilegar forsendur sem áhrif hafi á möguleikann á undirskriftinni. Nokkur atriði geti skipt máli í því samhengi, t.a.m. hvort einkalykillinn á kortinu sé áreiðanlega bara til á SIM kortinu, hvort með einhverjum leiðum sé hægt að láta einkalykilinn „leka“ af SIM kortinu, hvort með einhverjum leiðum sé hægt að láta PIN númerið „leka“ á leiðinni frá innslætti til SIM kortsins, hvort skjalið sem undirritandi taldi sig vera að undirrita sé örugglega það sem var raunverulega undirritað, hvort undirritaða skjalið sé „virkt“ og breyti framsetningu sinni síðar (án þess þó að hash-gildi skjalsins breytist), hvort öruggt sé að enginn annar geti komist að PIN númeri undirritandans og notað skilríkin án hans samþykkis og hvort einhver hafi sett þunnt SIM kort (0.17 mm) á milli símans og SIM kortsins til að gera MITM árás á samskiptin á milli símans og SIM kortsins.

40. Þetta séu bara örfá þekkt atriði sem nefna megi og engan veginn tæmandi listi. Við þennan lista bætist síðan allir þeir öryggisveikleikar sem kunni að finnast í farsímanum sem notaður sé. Sum af þessum atriðum geti lausnin á SIM kortinu hugsanlega tryggt, en önnur velti á hlutum sem ómögulegt sé fyrir lausnina á SIM kortinu að tryggja. Sá sem verði fyrir slíkri fölsun þurfi að komast að því hvað hafi raunverulega gerst og sýna fram á hvernig fölsunin á samþykki gæti hafa átt sér stað. Til þess þurfi hann að hafa allar tæknilegar upplýsingar sem geti skipt máli. Það megi segja að þetta jafngildi því í besta falli að sönnunarbyrðinni sé snúið við, en í versta falli sé ómögulegt fyrir viðkomandi að hrekja slíka fölsun. Í ljósi þess að sönnunarbyrði sé í reynd snúið við þegar komi að rafrænum undirskriftum verði að gera skýrar kröfur um að lausnir sem myndi slíkar rafrænar undirskriftir séu öruggar. Þetta hafi verið gert með lögum nr. 28/2001, sem samin hafi verið af sérfræðingum. Lausnir sem telja eigi fullgildar í skilningi laganna þurfi að uppfylla þessi skilyrði. Það geri rafræn skilríkjalausn Auðkennis ehf. fyrir farsíma ekki.

41. Með bréfi, dags. 23. ágúst 2016, barst áfrýjunarnefnd neytendamála greinargerð Neytendastofu vegna kærunnar. Þar kemur fram að það sé ekki hlutverk áfrýjunarnefndar neytendamála að endurskoða aðra þætti í starfsemi Neytendastofu en þá sem lúti beinlínis að ákveðnu fyrirliggjandi máli sem kært hafi verið til nefndarinnar á grundvelli stjórnsýslukæru. Kröfur kæranda varði starfsemi Neytendastofu með almennum hætti og ekki með beinum hætti hina kærðu ákvörðun. Með vísan til þessa hafni Neytendastofa kröfum kæranda. Að því er varði virkni eftirlits Neytendastofu bendi stofnunin á að allar skilríkjalausnir Auðkennis ehf. hafi fengið staðfestingar þar til bærra erlendra aðila og að kröfum til öruggs undirskriftarbúnaðar teljist fullnægt, sbr. 8. og 9. gr. laga nr. 28/2001. Hafi Auðkenni ehf. upplýst stofnunina um efni umræddra staðfestinga, sbr. ákvæði IV. og V. kafla reglugerðar um rafrænar undirskriftir nr. 780/2011, en efni þeirra lúti að öryggi undirskriftarbúnaðar félagsins samkvæmt fyrrgreindum

ákvæðum laga nr. 28/2001. Upphaflegt umkvörtunarefni kæranda hafi lotið að öryggi neytenda við notkun á PIN númeri en slíkt númer teljist ekki til undirskriftarbúnaðar í skilningi laganna. Efni staðfestinganna lúti því að öðrum öryggisþáttum en upphaflegt umkvörtunarefni kæranda hafi lotið að en ekki að öryggi undirskriftarbúnaðar í skilningi laga nr. 28/2001. Meðal annars þess vegna hafi slík gögn ekki verið talin til gagna fyrirliggjandi máls. Þá hafi Neytendastofa ekki látið framkvæma prófanir eða úttektir á starfsemi Auðkennis ehf. að eigin frumkvæði eins og henni sé heimilt samkvæmt ákvæðum reglugerðar nr. 780/2011, enda hafi ekkert komið fram sem gefið gæti tilefni til slíkrar endurskoðunar.

42. Neytendastofa hafni því að mat stofnunarinnar byggi eingöngu á álitum Admon ráðgjafar. Staðfesting á öryggi viðkomandi undirskriftarbúnaðar byggi á viðvarandi eftirliti stofnunarinnar með öllum skilríkjalausnum Auðkennis ehf. og gögnum frá þar til bærum erlendum aðilum á Evrópska efnahagssvæðinu um að kröfum til öruggs undirskriftarbúnaðar teljist fullnægt, sbr. 8. og 9. gr. laga nr. 28/2001. Varðandi það hvort PIN númer teljist til undirskriftargagna ítreki stofnunin að það sé einungis einkalykill í kerfinu sjálfu sem teljist undirskriftargagn í skilningi laga nr. 28/2001. PIN númer teljist ekki hluti undirskriftarbúnaðar þar sem hann sé ekki forsenda rafrænnar undirskriftar innan dreifilyklakerfis. Í þessu samhengi bendi Neytendastofa á að í 5. tölulið 3. gr. laga nr. 28/2001 segi að undirskriftargögn séu einstök gögn, svo sem kótar eða einkalykill dulritunar, sem undirritandi noti til að mynda rafræna undirskrift. Í ummælum í greinargerð í frumvarpi því sem varð að lögum nr. 28/2001 segi um hugtakið undirskriftargögn að átt sé við þau gögn sem notuð séu til að mynda rafræna undirskrift. Í dreifilyklakerfi nefnist þessi gögn einkalykill. Í 4. tölulið 2. gr. tilskipunar Evrópuþingsins og ráðsins 1999/93/EB sem innleidd hafi verið í íslenskan rétt með lögum nr. 28/2001 séu undirskriftargögn kölluð „signature-creation data“. Í 4. tölulið 2. gr. tilskipunarinnar segi svo: „signature-creation data means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature“.

43. Í 6. tölulið 3. gr. laga nr. 28/2001 komi fram að undirskriftarbúnaður sé hugbúnaður eða vélbúnaður sem notaður sé til að mynda rafræna undirskrift með hjálp undirskriftargagna. Í ummælum í greinargerð frumvarps þess sem varð að lögum nr. 28/2001 segi um hugtakið að það sé búnaður sem notaður sé við gerð rafrænu undirskriftarinnar. Búnaðurinn noti undirskriftargögnin til að búa til undirskriftina. Búnaðurinn geti bæði verið vélbúnaður og hugbúnaður. Sem dæmi um vélbúnað megi t.d. nefna snjallkort og sem dæmi um hugbúnað megi nefna hluta tölvupóstsforrits. Í 5. tölulið 2. gr. tilskipunar Evrópuþingsins og ráðsins 1999/93/EB sé undirskriftarbúnaður kallaður „signature creaton device“. Í 5. tölulið 2. gr. segir „signature-creation device means configured software or hardware used to implement the signature-creation data“.

44. Þá er í greinargerðinni rakið að í 15. gr. aðfararorða tilskipunarinnar segi eftirfarandi um öruggan undirskriftarbúnað: „Annex III covers requirements for secure signature-creation devices to ensure the functionality of advances electronic signatures; it does not cover the entire

system environment in which such devices operate; the functioning of the internal market requires the Commission and the Member States to act swiftly to enable the bodies charged with the conformity assessment of secure signature devices with Annex III to be designated; in order to meet market need conformity assessment must be timely and efficient.“

45. Öruggur undirskriftarbúnaður sé notaður í ýmsu mismunandi burðarlagi. Hann geti til dæmis verið hluti af debetkorti, persónuskilríkjum eða SIM korti. PIN númer sé aðgangsstýring að undirskriftarbúnaði. PIN númer sé viðbótaröryggislausn við þá skilríkjalausn sem Auðkenni ehf. bjóði upp á og sé ekki nauðsynleg forsenda undirskriftar með dreifilyklakerfi. Það sé eingöngu einkalykillinn sem teljist til undirskriftargagna, þ.e. sá hluti sem sé tæknilega notaður til þess að útbúa undirskriftina. PIN númer séu hvorki hluti undirritunargagna né hluti undirskriftarbúnaðar í skilningi laganna eða tilskipunarinnar. Þá segi í lið 5.8 í greinargerð með frumvarpi því er varð að lögum nr. 28/2001 að undirskriftarbúnaður teljist eingöngu öruggur ef hann hafi verið viðurkenndur af tilnefndum aðilum innan aðildarríkjanna. Líta skuli svo á að undirskriftarbúnaður sé öruggur ef hann sé í samræmi við staðla sem framkvæmdastjórn Evrópusambandsins hafi sett og birtir hafi verið í Stjórnartíðindum EB. Í 6. lið 2. gr. tilskipunar 1999/93/EB segi eftirfarandi um öruggan undirskriftarbúnað: „secure-signature-creation device means a signature-creation device which meets the requirements laid down in Annex III“.

46. Líkt og fram komi í hinni kærðu ákvörðun hafi Neytendastofa í samræmi við 3. mgr. 21. gr. reglugerðar nr. 780/2011 yfirfarið og kannað vottorð frá erlendum aðilum á Evrópska efnahagssvæðinu sem uppfylli skilyrði b. liðar 9. gr. laga nr. 28/2001 um að undirskriftarbúnaður Auðkennis ehf. og burðarlag fyrir farsíma uppfylli sannanlega öryggiskröfur sem mælt sé fyrir um í tilskipun 1999/93/EB, sbr. lög nr. 28/2001 og reglugerð nr. 780/2011. Undirskriftarbúnaðurinn hafi staðist kröfur gagnvart hæsta öryggisstigi, þ.e. öryggisstigi EAL 5+. Umkvörtunarefni kæranda lúti að öryggi PIN númers í meðförum notenda símtækis. Umkvörtunarefnið lúti þannig ekki að öryggi þess undirskriftarbúnaðar sem Auðkenni ehf. noti í skilningi laga nr. 28/2001. Mati kæranda sé því hafnað með öllu af Neytendastofu.

47. Varðandi athugasemdir kæranda sem lúti að því að skilmálar Auðkennis ehf. séu ósanngjarnir þar sem neytandi sé látinn bera ábyrgð á öllum aðferðum sem framkvæmdar séu með rafrænum skilríkjum telji Neytendastofa að þær lúti að því hver sé æskileg ábyrgð áskrifenda rafrænna skilríkja. Upphafleg kvörtun kæranda hafi ekki lotið að þessu, auk þess sem kærandi hafi í engu rökstutt á hvaða lagagrundvelli Neytendastofa eigi að hafa eftirlit með sanngirni skilmála Auðkennis ehf. að því er varði notkun á PIN númeri. Engu að síður bendi Neytendastofa á að í a. lið 1. mgr. 15. gr. laga nr. 28/2001, sbr. 18. gr. reglugerðar nr. 780/2011, komi fram að áður en vottunaraðili geri samning um útgáfu fullgilds vottorðs skuli hann upplýsa undirritanda skriflega og með varanlegum hætti um skilmála og takmarkanir á notkun vottorðsins. Þetta geri Auðkenni ehf. áður en samningar séu gerðir við áskrifendur skilríkja. Neytendastofa bendi einnig á að samkvæmt lið 6.6 í skilmálum Auðkennis ehf. skuli áskrifandi skila inn skilríkjum

sem hann telji að hafi með einhverjum hætti verið misnotuð eða öryggi einkalykils eða PIN númeri stefnt í hættu á gildistíma skilríkjanna.

48. Neytendastofa hafnar því að stofnunin hafi brotið gegn 10. gr. stjórnsýslulaga með því að rannsaka málið ekki á fullnægjandi hátt. Auðkenni ehf. hafi uppfyllt öll skilyrði laga nr. 28/2001 og reglugerðar nr. 780/2011 til útgáfu fullgildra vottorða og að virtum athugasemdum félagsins og skoðunar sérfræðinga Neytendastofu hafi stofnunin talið að athugasemdir kæranda gæfu ekki tilefni til svo ítarlegrar rannsóknar sem kærandi hefði talið að fara ætti fram.

49. Með bréfi áfrýjunarnefndar neytendamála, dags. 16. ágúst 2016, var kæranda boðið að koma að athugasemdum sínum við greinargerð Neytendastofu. Svar barst með bréfi, dags. 11. september 2016. Þar kemur fram að kærandi hafi bent Neytendastofu á ákveðinn öryggisgalla í rafrænni skilríkjalausn Auðkennis ehf. sem geri þriðja aðila mögulegt að framkalla fullgildar rafrænar undirskriftir án vitneskju og vilja eiganda skilríkjanna. Þetta geti þessi þriðji aðili gert ef hann fái aðgang að síma eigenda skilríkjanna, jafnvel þótt eigandi skilríkjanna fari að öllum eðlilegum og sanngjörnum öryggiskröfum sem hægt sé að gera til hans. Í allri meðferð málsins hafi Neytendastofa reynt að halda því fram að öryggi lausnarinnar uppfylli skilyrði laganna og hafi í því sambandi notið liðsinnis Auðkennis ehf. og tengdra aðila varðandi tæknileg atriði. Þetta sé afar sérkennilegt því lögum samkvæmt beri Neytendastofu að hafa eftirlit með umræddu fyrirtæki. Ekkert í gögnum málsins bendi til þess að Neytendastofa hafi sjálf sannreynt öryggisgallann eða metið hvaða afleiðingar hann hefur fyrir traust á rafrænum skilríkjum. Rétt sé að ítreka að samkvæmt lögum hafi fullgildar rafrænar undirskriftir afar sterka lagalega stöðu og aðili sem lendi í slíkri misnotkun sé því í afar slæmri stöðu til að hrekja hverskyns fölsun. Þegar við bætist að áskriftarskilmálar Auðkennis ehf. virðist varpa allri ábyrgð á herðar neytandans sé ómögulegt annað en að komast að þeirri niðurstöðu að um óeðlilega og ósanngjarna skilmála sé að ræða.

50. Í bréfi kæranda er rakið að Neytendastofa telji kröfur kæranda varða starfsemi Neytendastofu með almennum hætti og þannig ekki með beinum hætti hina kærðu ákvörðun. Kærandi hafni þessari túlkun Neytendastofa á kröfum sínum. Kröfur kæranda snúi að því hvaða ákvörðun Neytendastofa tók í þessu máli sérstaklega og því fái kærandi ekki séð á hvern hátt sé hægt að túlka þær sem kröfur varðandi almenna starfssemi Neytendastofu. Að mati kæranda hafi Neytendastofa hafið stjórnsýslumál með meðferð sinni á erindi kæranda. Málinu hefði getað lokið á þann hátt að Neytendastofa tæki ákvörðun sem uppfyllti kröfur kæranda í stað þess að aðhafast ekkert í málinu líkt og Neytendastofa hafi kosið. Það að stjórnsýslumál hafi hafist megi einnig lesa út úr meðferð umboðsmanns Alþingis á málinu, sbr. bréf hans til kæranda, dags. 26. febrúar 2015, og fyrri meðferð áfrýjunarnefndar neytendamála. Varðandi rökstuðning Neytendastofu um þá afstöðu stofnunarinnar að undanskilja frá gögnum málsins staðfestingar þar til bærra aðila um að lausnir Auðkennis ehf. uppfylli skilyrði laganna, telji kærandi afar nauðsynlegt að þessar staðfestingar, eða hlutar þeirra, verði gerðar opinberar því ætlaður öryggisgalli sé í miklu ósamræmi við meint innihald slíkra staðfestinga. Þegar hægt sé að sýna

fram á misnotkun bendi það sterklega til þess að taka verði slíkum staðfestingum með fyrirvara. Neytendastofa kjósi hins vegar að upplýsa ekki um lágmarks atriði varðandi þessar staðfestingar.

51. Öryggisgallinn sem kærandi bendi á gefi fullt tilefni til þess að upplýst sé hvaða þar til bær aðili hafi gefið út staðfestingu á því að búnaður Auðkennis ehf. uppfylli skilyrði laganna. Hér skipti líka máli að Auðkenni ehf. sjálft hafi á opinberum vettvangi upplýst um það að bandaríska netöryggisfyrirtækið NowSecure, áður viaForensics, hafi vottað öryggi lausnar fyrirtækisins. Hafi þetta verið sá aðili sem Neytendastofu hafi verið tilkynnt um sé ekki að sjá að viðkomandi uppfylli þau skilyrði sem gerð séu í lögum um slíkan aðila. Neytendastofa hafi hins vegar ekki viljað staðfesta hvort þetta sé aðilinn sem hafi vottað hugbúnaðinn á SIM kortinu eða hvaða annar aðili hafi gert slíkt. Kærandi hafi því farið fram á að það yrði upplýst hvaða aðili hafi gefið út slíkar staðfestingar, hvenær staðfestingarnar hafi verið gefnar út, hvenær þær bárust Neytendastofu og til hvaða búnaðar þær nái. Þessar upplýsingar séu grundvöllur þess að lausnum Auðkennis ehf. sé færð ákveðin lagaleg staða sem geti framkallað fullgildar rafrænar undirskriftir. Þessar upplýsingar feli ekki í sér atvinnuleyndarmál eða upplýsingar sem leynt eigi að fara, enda hafi Auðkenni ehf. áður gefið upp opinberlega hver votti öryggismál tiltekinna lausna þess. Rétt sé að geta þess að úrskurðarnefnd um upplýsingamál sé nú með kæru vegna neitunar Neytendastofu á að láta þessar upplýsingar af hendi í annað sinn.

52. Neytendastofa hafi neitað því að hún byggi niðurstöðu sína eingöngu á álitum Admon Ráðgjafar. Stofnunin haldi því fram að staðfesting á öryggi undirskriftarbúnaðarins sé byggð á „viðvarandi eftirliti stofnunarinnar með öllum skilríkjalausnum Auðkennis og gögnum frá þar til erlendum bærum aðilum á Evrópska efnahagssvæðinu um að kröfum til öruggs undirskriftarbúnaðar teljist fullnægt, sbr. 8. og 9. gr. laga nr. 28/2001“. Kærandi bendi á að þau gögn sem Neytendastofa hafi talið til gagna málsins innihaldi engar slíkar staðfestingar og stofnunin hafi harðlega neitað að gefa nokkrar frekari upplýsingar um slíkar staðfestingar. Einu tæknilegu skjölin sem fram komi í gögnum málsins séu áðurnefnd álit Admon ráðgjafar sem kærandi telji of tengda Auðkenni ehf. til að hægt sé að taka sem hlutlausum aðila.

53. Hafi ákvörðun Neytendastofu byggt á slíkum staðfestingum beri Neytendastofu að upplýsa um það hvaða tilteknu staðfestingar sé um að ræða og til hvaða búnaðar þær nái. Kærandi hafi ekki séð þessar staðfestingar og geti því ekki fullyrt um hvort þau skjöl innihaldi einhverjar þær upplýsingar sem leynt eigi að fara. Sé sú raunin geti Neytendastofa að skaðlausu fyrir Auðkenni ehf. upplýst um það hver hafi gefið slíkar staðfestingar út, hvenær þær hafi verið gefnar út, hvenær þær hafi borist Neytendastofu og til hvaða búnaðar þær ná. Slík upptalning geti með engu móti flokkast sem atvinnuleyndarmál.

54. Neytendastofa rökstyðji þá skoðun Auðkennis ehf. og stofnunarinnar að PIN númer teljist ekki til undirskriftargagna í skilningi laganna. Kærandi gerir þrjár athugasemdir við þetta. Í fyrsta lagi sé óumdeilt að í lausn Auðkennis ehf. slái notendur inn PIN númer sitt til þess að framkalla rafrænar undirskriftir. Í 3. gr. laga nr. 28/2001 segi að undirskriftargögn séu einstök gögn, svo

sem kótar eða einkalykill dulritunar, sem undirritandi noti til að mynda rafræna undirskrift. Í lausn Auðkennis ehf. sé einnig notaður einkalykill en hann sé algerlega óaðgengilegur notanda. Notandi hafi ekki á nokkurn hátt beinan aðgang að þessum einkalykli, heldur sé hann geymdur dulkóðaður á SIM korti notandans. Til þess að nota einkalykilinn, t.d. til að framkalla rafræna undirskrift, slái notandinn inn PIN númer sitt í símann. Þetta númer sé sent til SIM kortsins þar sem það sé notað til þess að afdulkóða einkalykilinn og í framhaldinu gerð rafræn undirskrift. Með þessu sé ljóst að PIN númer gefi aðgang að notkun einkalykilsins. Það sé því slíkur „kóti“ sem talað sé um í lögunum. Öryggisgallinn sem kærandi bendi á nýti sér einmitt það að í venjulegum farsíma sé innslegið PIN númer ekki verndað á nokkurn hátt.

55. Aðferðafræði Neytendastofu við að leggja mat á þennan öryggisgalla sé meingölluð. Í stað þess að meta öryggisgallann í samhengi við lausnina sem hann finnist í sé eingöngu leitað til Auðkennis ehf. og aðila því tengdu varðandi tæknileg úrlausnarefni. Öryggisgalli á borð við þann sem kærandi bendi á hverfi ekki við það að benda á lagarök eða vísa í lög, greinargerðir eða tilskipanir. Þetta virðist stafa af því að Neytendastofa hafi aðeins nálgast málið frá lögfræðilegum sjónarhóli en ekki tæknilegum, enda virðist aðeins lögfræðingar hafa komið að málinu hjá stofnuninni. Neytendastofa hafi samkvæmt lögum úrræði til að láta fara fram endurskoðun á búnaði og kerfum Auðkennis ehf., líkt og kærandi geri kröfu um. Fullt tilefni sé til slíks að mati kæranda. Eftir standi að aðili sem vilji misnota lausn Auðkennis ehf. geti það með einföldum hætti eins og kærandi hafi bent á. Þeir sem verði fyrir slíkri misnotkun hafi litla sem enga möguleika á að hrekja kröfur gerðar með rafrænni undirskrift án samþykkis.

56. Í öðru lagi haldi Neytendastofa fram að hún hafi kannað vottorð um að undirskriftarbúnaður Auðkennis ehf. og burðarlag farsíma uppfylli skilyrði sem mælt sé fyrir um í tilskipun 1999/93/EB. Ekki komi nákvæmlega fram hvað Neytendastofa telji að felist í orðunum „undirskriftarbúnaður Auðkennis“ en kærandi geti sér til um að vísað sé til SIM korts og þess hugbúnaðar sem þar keyri. Þetta þurfi Neytendastofa að skýra betur. Enn fremur sé óljóst af hverju Neytendastofa hafi aflað sér staðfestinga tengdu „burðarlagi farsíma“ og raunar sé óljóst hvað nákvæmlega felist í því hugtaki. Kærandi geti sér til um að hér sé um að ræða samskiptaleið sem samskipti hugbúnaðar á SIM korti til tölvuþjóna Auðkennis ehf. fari um. Þetta þurfi Neytendastofa einnig að útskýra betur.

57. Loks sé ekki ljóst hvort frumkvæði að öflun staðfestinga á öryggi þessa „burðarlags farsíma“ hafi komið frá Neytendastofu eða frá Auðkenni ehf. og hvernig þörfin á slíkri staðfestingu hafi verið metin. Þetta þurfi Neytendastofa enn fremur að skýra betur. Ómögulegt sé fyrir notanda að nota sér burðarlag farsíma og SIM kort ein og sér til þess að framkalla rafrænar undirskriftir. Augljóslega þurfi einnig farsíma til þess. Neytendastofa og Auðkenni ehf. hafi ekki gefið upp neinar kröfur til slíkra farsíma og ekki gefið ítarlegar öryggisleiðbeiningar sem gætu minnkað möguleika á misnotkun. Hafi verið sérstök ástæða til að huga sérstaklega að öryggi í „burðarlagi farsíma“ og afla staðfestinga þar um, sé ljóst að einnig sé full ástæða til þess að staðfesta öryggi í samskiptaleiðum notanda til örugga undirskriftarbúnaðarins (SIM korts). Neytendastofa þurfi

að útskýra af hverju öryggi í þessari leið falli að mati stofnunarinnar ekki undir eftirlitssvið hennar þegar slíkt hafi augljóslega alvarlegar afleiðingar fyrir öryggi lausnarinnar í heild sinni, líkt og eigi við um „burðarlag farsíma“.

58. Í þriðja lagi sé Neytendastofa þeirrar skoðunar að PIN númer teljist „ekki ekki“ hluti undirskriftarbúnaðar þar sem hann sé ekki forsenda rafrænnar undirskriftar innan dreifilykla kerfisins. Þessi orðanotkun sé óljós, enda sé sama tvöfalda neitunin, sem fram komi í hinni kærðu ákvörðun, endurtekin í greinargerð stofnunarinnar til áfrýjunarnefndarinnar, þrátt fyrir að kærandi hafi bent á það í kæru að orðalagið væri ankannalegt. Sé þetta setning af hálfu höfundar greinargerðarinnar þarfnist hún frekari útskýringa. Kærandi spyrji hvort túlka beri hina tvöföldu neitun sem játun og hvort orðið “hann” vísi til undirskriftarbúnaðarins. Sú staðreynd að Neytendastofa endurtaki þessa setningu eftir að hafa fengið kæru kæranda í hendur hljóti að vekja upp spurningu hvort skilja eigi hana eftir orðanna hljóðan. Kærandi spyrji því hvort PIN númer teljist að mati Neytendastofu hluti undirskriftarbúnaðar og hvort undirskriftarbúnaðurinn sé þá ekki forsenda rafrænnar undirskriftar. Þetta þurfi Neytendastofa að útskýra betur.

59. Loks tjái Neytendastofa sig um þá afstöðu kæranda að skilmálar Auðkennis ehf. séu óeðlilegir og ósanngjarnir að því leyti að neytandi sé látinn bera ábyrgð á öllum aðgerðum sem framkvæmdar séu með rafrænum skilríkjum. Stofnunin telji að um vangaveltur sé að ræða um það hver sé æskileg ábyrgð áskrifenda rafrænna skilríkja. Neytendastofa haldi því fram að upphafleg kvörtun kæranda hafi ekki snúið að þessu atriði og sjái auk þess ekki á hvaða lagagrundvelli Neytendastofa eigi að hafa eftirlit með skilmálum Auðkennis ehf. Kærandi bendi á að í upphaflegu erindi kæranda hafi hann einmitt einnig vísað til almennra neytendasjónarmiða. Þessi skilningur komi fram í bréfi Neytendastofu til umboðsmanns Alþingis, dags. 23. janúar 2015, þar sem Neytendastofa hafi lagt áherslu á að erindið varðaði „almenna notkun almennings“ á rafrænum skilríkjum.

60. Neytendastofa hafi fleiri skyldur en þær sem snúi að rafrænum skilríkjum. Hér megi einnig benda á að Neytendastofa hafi eftirlitsskyldu samkvæmt lögum nr. 57/2005 um eftirlit með viðskiptaháttum og markaðssetningu, en í 2. gr. þeirra segi að þau nái til samninga, skilmála og athafna aðila. Í lögunum sé í 9. gr. tiltekið að viðskiptahættir séu villandi ef þeir séu líklegir til þess að blekkja neytendur eða séu með þeim hætti að neytendum séu veittar rangar upplýsingar í þeim tilgangi að hafa áhrif á ákvörðun þeirra um viðskipti. Einnig segi í greininni að viðskiptahættir séu villandi ef ekki sé greint frá upplýsingum sem telja megi að almennt skipti máli fyrir neytendur eða þeim sé leynt og þær séu til þess fallnar að hafa áhrif á ákvörðun neytenda um að eiga viðskipti. Við meðferð málsins hafi komið í ljós að afstaða Auðkennis ehf., og þar með einnig afstaða Neytendastofu, sé sú að neytendur beri alla ábyrgð á öryggi síma sem þeir noti við innslátt PIN númers. Verði þeir fyrir misnotkun af því tagi sem kærandi lýsi sé enn fremur allri ábyrgð á rafrænum undirskriftum, sem gerðar séu án samþykkis þeirra, varpað á þeirra herðar samkvæmt áskriftarskilmálunum. Neytendastofa eigi að hafa hagsmuni

neytenda að leiðarljósi í málinu og hlutast til um að þessum áskriftarskilmálum verði breytt eins og henni beri skylda til samkvæmt lögum nr. 57/2005.

61. Það auki á alvarleika málsins að stofnanir á vegum ríkisins, t.d. fjármálaráðuneytið og skattayfirvöld, setji þrýsting á borgarana til þess að taka upp rafræn skilríki þrátt fyrir þessa skilmála. Þannig verði áskrifendur að vera einhvers konar sérfræðingar í öryggismálum farsíma eigi þeir að taka skyldur sínar gagnvart þessum skilmálum alvarlega. Þessar stofnanir geri þetta í góðri trú því samkvæmt lögunum sé því óbeint heitið að rafræn skilríki séu örugg, einföld og þægileg. Þannig sé það ekki bara almenningur sem fái villandi upplýsingar um öryggi rafrænna skilríkja heldur einnig stofnanir ríkisins. Í ljósi framangreinds sé það afstaða kæranda að Neytendastofu hafi borið að taka áskriftarskilmála Auðkennis ehf. til skoðunar m.t.t. 9. gr. laga nr. 57/2005 eins og málið gefi fullt tilefni til.

62. Loks rekur kærandi að hann telji að Neytendastofa þurfi að gera nefndinni nánari grein fyrir ákveðnum atriðum í forsendum hinnar kærðu ákvörðunar til þess að nefndin geti tekið rökstudda afstöðu í málinu. Afla þurfi svara við því hvaða búnað sé átt við með orðunum „undirskriftarbúnaður Auðkennis“ í greinargerð Neytendastofu og hvort um sé að ræða SIM kort sem sett sé í síma, hugbúnað á þessu SIM korti eða síma auk SIM korts og hugbúnaðar sem PIN númer sé slegið inn í. Þá þurfi Neytendastofa að svara því hvað felist nákvæmlega í orðunum „burðarlag farsíma“ og hvernig staðið hafi verið að því að staðfesta að það uppfylli kröfur 8. gr. laga nr. 28/2001. Auk þess þurfi stofnunin að upplýsa hver hafi tekið ákvörðun um að þörf væri á staðfestingu á að burðarlag farsíma uppfyllti kröfur 8. gr. laganna og ef þörf hafi verið á að staðfesta að burðarlag farsíma fyllti kröfur 8. gr. laga nr. 28/2001, af hverju ekki hafi á sama hátt verið staðfest að farsími notanda, sem augljóslega sé hluti af þeim búnaði sem notandi noti til að framkalla undirskrift, uppfylli kröfur 8. gr. laga nr. 28/2001.

63. Með bréfi áfrýjunarnefndarinnar til Auðkennis ehf., dags. 20. september 2016, var félaginu boðið að koma á framfæri athugasemdum við fram komna kæru. Ekkert svar barst við bréfinu.

NIÐURSTAÐA

64. Í máli þessu leitar kærandi endurskoðunar á þeirri ákvörðun Neytendastofu að ekki sé ástæða til aðgerða vegna ábendingar hans um ætlaða öryggisgalla í rafrænum skilríkjalausnum Auðkennis ehf. Kærandi krefst þess að áfrýjunarnefndin „úrskurði að Neytendastofa skuli láta fara fram endurskoðun á búnaði og kerfum Auðkennis ehf. og eftir atvikum endurskoða hvort lausnin uppfylli þau skilyrði að geta talist fullgild í skilningi laganna“. Þá krefst hann þess að Neytendastofu verði gert skylt að meta hvort áskriftarskilmálar Auðkennis ehf., einkum grein 6.5, séu eðlilegir og sanngjarnir í garð neytenda og hlutist ella til um að þeim verði breytt. Loks krefst kærandi þess að Neytendastofu verði gert að upplýsa um nánar tilgreind atriði varðandi vottun fullgildra lausna fyrrgreinds félags. Neytendastofa krefst þess meðal annars að kröfum kæranda verði hafnað á þeim grundvelli að þær varði starfsemi Neytendastofu með almennum

hætti og ekki hina kærðu ákvörðun með beinum hætti. Auk þess telur Neytendastofa að kærandi eigi ekki aðild að málinu.

65. Kærandi hefur krafist þess að Neytendastofa grípi til tiltekinna ráðstafana og rannsóknarúrræða vegna starfsemi Auðkennis ehf., sem fram fer á grundvelli ákvæða laga nr. 28/2001. Þótt málið varði svið sem Neytendastofu er almennt falið að hafa eftirlit með, sbr. VII. kafla laga nr. 28/2001, varða kröfur kæranda fyrir áfrýjunarnefndinni viðbrögð Neytendastofu við erindi kæranda til hennar, dags. 15. september 2014. Áfrýjunarnefndin hefur þegar tekið afstöðu til aðildar kæranda að málinu fyrir Neytendastofu og heimildar hans til að kæra ákvarðanir stofnunarinnar í málinu til nefndarinnar, sbr. úrskurð áfrýjunarnefndar neytendamála 11. júní 2015 (5/2015). Verður kröfum kæranda því hvorki hafnað af þeim ástæðum einum að þær varði að einhverju marki almenna starfshætti Neytendastofu né vegna skorts á aðild hans að málinu.

66. Í erindi kæranda til Neytendastofu, dags. 15. september 2014, var stofnuninni bent á að rafræn skilríkjalausn Auðkennis ehf., „Rafræn skilríki í farsíma“, virtist ekki uppfylla það skilyrði 2. mgr. 8. gr. laga nr. 28/2001 að teljast öruggur undirskriftarbúnaður. Í erindinu er þessi afstaða kæranda reist á því að svokallað PIN númer notanda sé ekki varið með fullnægjandi hætti þegar umrædd lausn sé notuð í farsíma, enda geti einstaklingur sem komist yfir farsíma annars manns komið fyrir hugbúnaði á símanum sem miðli umræddu PIN númeri til sín. Geti viðkomandi þá notað rafræna undirskrift eiganda símans. Kærandi telji að eigi rafrænar undirskriftir að hafa sömu þýðingu og undirskriftir á pappír þurfi kröfur til öruggs undirskriftarbúnaðar í skilningi 2. mgr. 8. gr. laga nr. 28/2001 að vera túlkaðar nægjanlega þröngt til að ekki sé auðvelt að framkalla slíkar undirskriftir án samþykkis réttmæts undirritanda. Meðfylgjandi erindi kæranda var að finna nánari lýsingu á því hvernig framkvæma mætti misnotkun á undirskriftarbúnaði Auðkennis ehf.

67. Í lögum nr. 28/2001 er fjallað um rafrænar undirskriftir sem samkvæmt lögunum eru gögn „í rafrænu formi sem fylgja eða tengjast rökrænt öðrum rafrænum gögnum og eru notuð til að sannprófa frá hverjum hin síðarnefndu gögn stafa“. Telst fullgild rafræn undirskrift vera „[ú]tfærð rafræn undirskrift sem er studd fullgildu vottorði og gerð með öruggum undirskriftarbúnaði“. Með slíkri undirskrift getur svokallaður undirritandi, komið fram fyrir eigin hönd eða fyrir hönd annars einstaklings eða lögpersónu, líkt og þegar hefðbundnar undirskriftir eru notaðar. Gefur vottunaraðili út slík vottorð og veitir aðra þjónustu í tengslum við rafrænar undirskriftir. Í því skyni að framkvæma eða mynda rafræna undirskrift skal samkvæmt lögunum nota undirskriftarbúnað, sem mun vera hugbúnaður eða vélbúnaður sem notaður er til að mynda rafræna undirskrift með hjálp undirskriftargagna, sem eru nánar skilgreind í lögunum sem „einstök gögn, svo sem kótar eða einkalykill dulritunar, sem undirritandi notar til að mynda rafræna undirskrift“.

68. Af gögnum málsins verður ráðið að fyrirtækið Auðkenni ehf. hafi útbúið undirskriftarbúnað í framangreindum skilningi sem virki þannig að undirritandi setji upp hugbúnað fyrirtækisins á snjallsíma í umráðum undirritandans. Hann geti þá notað svonefnt PIN númer til að undirrita

þá gerninga sem hann hyggst skrifa undir með rafrænum hætti. Munu slíkar undirritanir vera framkvæmdar þannig að undirritandi notar undirskriftina til að skrá sig inn á þar til gerð vefsvæði hjá ýmsum fjármálastofnunum, fyrirtækjum, lífeyrissjóðum og ríkisstofnunum þar sem unnt er að ráðstafa hagsmunum undirritanda gagnvart viðkomandi aðilum.

69. Í 8. gr. laga nr. 28/2001 koma fram þær kröfur sem gerðar eru til öruggs undirskriftarbúnaðar og þar með þess undirskriftarbúnaðar Auðkennis ehf. er mál þetta lýtur að. Þar kemur meðal annars fram að öruggur undirskriftarbúnaður skuli samkvæmt b. lið 1. mgr. 8. gr. tryggja að undirskriftargögnin verði „með hliðsjón af eðlilegum öryggiskröfum ekki brotin upp“ og samkvæmt c. lið sömu lagagreinar „varin með fullnægjandi hætti gegn notkun annarra en undirritanda“. Þá er kveðið á um það í 2. mgr. 8. gr. að öruggur undirskriftarbúnaður skuli tryggja leynd undirskriftargagnanna með fullnægjandi hætti og að rafræn undirskrift sé varin gegn fölsun. Í 9. gr. er fjallað um viðurkenningu undirskriftarbúnaðar samkvæmt 8. gr. laganna, en gert er ráð fyrir að þar til bærir aðilar staðfesti að kröfum laganna sé fullnægt að þessu leyti. Í 2. mgr. 9. gr. segir að líta skuli svo á að undirskriftarbúnaður teljist öruggur samkvæmt 8. gr. sé hann í samræmi við staðla sem framkvæmdastjórn Evrópusambandsins hefur sett um slíkan búnað og birtir hafi verið í Stjórnartíðindum Evrópusambandsins. Í V. kafla laganna er síðan nánar fjallað um þær kröfur sem gerðar eru til vottunaraðila sem gefa út fullgild vottorð.

70. Með lögum nr. 28/2001 var innleidd í íslensk lög tilskipun Evrópuþingsins og ráðsins 1999/93/EB frá 13. desember 1999 um ramma bandalagsins varðandi rafrænar undirskriftir. Í frumvarpi því sem varð að lögum nr. 28/2001 kemur fram að 8. gr. laganna byggi á III. viðauka umræddrar tilskipunar, sem geri tilteknar kröfur til undirskriftarbúnaðar til að tryggja ákveðið öryggisstig. Búnaður sem uppfylli þessar kröfur geti verið notaður til að mynda fullgildar rafrænar undirskriftir. Þá er tekið fram að vert sé að hafa í huga að þær kröfur sem gerðar séu samkvæmt greininni takmarkist af þeirri tækni og aðferðum sem þekktar séu hverju sinni. Í aðfararorðum framangreindrar tilskipunar segir meðal annars, í íslenskri þýðingu, að í III. viðauka hennar sé fjallað um kröfur sem séu gerðar til öruggs undirskriftarbúnaðar í því skyni að tryggja virkni þróaðra, rafrænna undirskrifta. Í fyrrnefndum viðauka sé ekki fjallað um gervallt umhverfi þess kerfis sem slíkur búnaður vinnur í.

71. Þann 16. ágúst 2011 setti efnahags- og viðskiptaráðherra reglugerð nr. 780/2011 um rafrænar undirskriftir á grundvelli laga nr. 28/2001. Í 19. gr. reglugerðarinnar eru áréttaðar þær kröfur sem fram koma í 8. gr. laganna. Þá er kveðið á um það í 20. gr. að undirskriftarbúnaður teljist fyrirfram ávallt öruggur samkvæmt ákvæðum greinarinnar ef hann er í samræmi við staðla og önnur kröfuskjöl sem framkvæmdastjórn Evrópusambandsins hefur ályktað um og gefið tilvísanir til og birtar eru í Stjórnartíðindum Evrópusambandsins. Í viðauka við reglugerðina er að finna lista yfir nöfn staðla og önnur kröfuskjöl. Þar er meðal annars að finna tilvísun til kröfuskjals um öruggan undirskriftarbúnað. Samkvæmt 21. gr. telst kröfum til undirskriftarbúnaðar samkvæmt fyrrnefndum ákvæðum reglugerðarinnar fullnægt þegar hann

hefur fengið staðfestingu frá þar til bærum aðila um að hann uppfylli kröfur 8. og 9. gr. laga nr. 28/2001.

72. Af öllu framangreindu leiðir að samkvæmt þeim lögum og reglum sem gilda um rafrænar undirskriftir getur undirskriftarbúnaður talist öruggur þótt til staðar kunni að vera einhver möguleiki á misnotkun hans. Í því sambandi vísast til þess að samkvæmt b. og c. lið 1. mgr. 8. gr. skal öruggur undirskriftarbúnaður tryggja að undirskriftargögnin verði með hliðsjón af „eðlilegum öryggiskröfum“ ekki brotin upp og séu varin „með fullnægjandi hætti“ gegn notkun annarra en undirritanda. Samkvæmt 2. mgr. skal öruggur undirskriftarbúnaður einnig tryggja leynd undirskriftargagnanna „með fullnægjandi hætti“ og að rafræn undirskrift „sé varin“ gegn fölsun. Þótt kærandi hafi bent á þann möguleika að aðrir en undirritandi kunni að verða sér út um PIN númer hans til þess að nota undirskriftarbúnað undirritandans leiðir það eitt og sér ekki til þess að undirskriftarbúnaður teljist ófullnægjandi með hliðsjón af þeim kröfum sem gerðar eru í 8. gr. laga nr. 28/2001.

73. Neytendastofu er falið að hafa eftirlit með vottunaraðilum sem gefa út fullgild vottorð og þar með að leggja tæknilegt mat á hvaða kröfur verði gerðar til öruggs undirskriftarbúnaðar á grundvelli þeirra réttarheimilda sem um hann gildir. Við þetta mat verður að hafa hliðsjón af þeirri tækni og aðferðum sem þekktar eru hverju sinni eins og bent er á í frumvarpi því sem varð að lögum nr. 28/2001. Af hinni kærðu ákvörðun og greinargerð Neytendastofu til áfrýjunarnefndarinnar verður ráðið að stofnunin telji að ekki verði gerðar svo ríkar öryggiskröfur til undirskriftarbúnaðar að komið verði í veg fyrir misnotkun hans með því að einhver verði sér úti um svokallað PIN númer undirritanda og misnoti þannig rafræna undirskrift hans. Styðst þessi afstaða meðal annars við ummæli í athugasemdum í frumvarpi því sem varð að lögum nr. 28/2001 um að þær reglur, sem innleiddar séu með 8. gr. laganna, taki ekki til gervalls umhverfis þess kerfis sem undirskriftarbúnaður vinnur í.

74. Þá er ljóst af almennum athugasemdum með frumvarpi til laga nr. 28/2001 að löggjafinn gerði ráð fyrir að öruggur undirskriftarbúnaður kynni að vera notaður á annað hvort síma eða tölvu sem tengd sé interneti, en áfrýjunarnefndin telur sig geta gengið út frá að slíkur tækjabúnaður verði ekki, við núverandi tækni, þannig úr garði gerður að komið verði með öllu í veg fyrir misnotkun annarra en eiganda viðkomandi búnaðar. Er í þessu sambandi einnig til þess að líta að forsenda þess að unnt sé að misnota þá skilríkjalausn er mál þetta lýtur að, með þeim hætti sem kærandi rekur, er að sá sem það geri afli sér PIN númers undirritandans með ólögmætum hætti. Ætlaður annmarki á umræddri lausn lýtur því að því að ekki sé til staðar neins konar vörn gegn slíkri misnotkun, en að mati áfrýjunarnefndar neytendamála er vandséð hvernig algjörlega megi verjast slíkri háttsemi með þeirri tækni sem nú er tiltæk.

75. Með vísan til þessa hefur áfrýjunarnefndin ekki forsendur til að fella úr gildi hina kærðu ákvörðun eða gera athugasemdir við mat Neytendastofu, enda verður ekki beinlínis ráðið af þeim réttarheimildum sem gilda um öruggan undirskriftarbúnað að mat stofnunarinnar sé aðfinnsluvert. Er að mati áfrýjunarnefndarinnar ekki unnt að túlka lög nr. 28/2001 þannig að

vottunaraðila beri fortakslaust að gera rafrænan undirskriftarbúnað þannig úr garði gerðan að komið sé í veg fyrir þá misnotkun sem kærandi varar við.

76. Auk framangreinds liggur fyrir af hálfu Neytendastofu að þar til bær aðili hefur staðfest að kröfum til undirskriftarbúnaðar samkvæmt 8. gr. laga nr. 28/2001 teljist fullnægt eins og stofnuninni er skylt að gera samkvæmt 3. mgr. 21. gr. reglugerðar nr. 780/2011. Verður ráðið að slíkar staðfestingar lúti í raun að öðrum þáttum í öryggi undirskriftarbúnaðarins en erindi kæranda lýtur að, enda gengið út frá að kröfur 8. gr. laga nr. 28/2001 til undirskriftarbúnaðar verji undirritanda ekki gegn slíkri misnotkun. Af þessum sökum getur áfrýjunarnefndin fallist á þá afstöðu Neytendastofu að henni hafi verið unnt að fjalla um erindi kæranda án þess að kanna sérstaklega efni umræddrar viðurkenningar og að stofnuninni hafi nægt að taka sjálf afstöðu til efnislegs inntaks 8. gr. laga nr. 28/2001 með hliðsjón af þeim atriðum sem fram koma í erindi kæranda. Var því ekki nauðsynlegt að umræddar staðfestingar yrðu gerðar að gögnum málsins í skilningi 1. mgr. 15. gr. stjórnsýslulaga eða tekin afstaða til efnis þeirra, enda var stofnunin meðvituð um að umræddar vottanir lægju fyrir og að hún hefði staðfest þær. Með vísan til alls þessa var ekki tilefni fyrir Neytendastofu til að bregðast frekar við erindi kæranda vaðandi öryggi undirskriftarbúnaðar Auðkennis ehf.

77. Við meðferð málsins fyrir áfrýjunarnefndinni hefur kærandi vísað til þess að almennir skilmálar Auðkennis ehf. brjóti gegn ákvæðum laga nr. 57/2005 um eftirlit með viðskiptaháttum og markaðssetningu. Að þessu var ekki vikið í erindi hans til Neytendastofu, dags. 15. september 2014, og er ekki að sjá í gögnum málsins að reynt hafi á umrædda skilmála í samskiptum kæranda við Auðkenni ehf. Með vísan til þessa var ekki tilefni fyrir Neytendastofu til að fjalla um þetta atriði í hinni kærðu ákvörðun.

78. Með vísan til alls framangreinds verður hins kærða ákvörðun staðfest.

ÚRSKURÐARORÐ:

Hin kærða ákvörðun er staðfest.

Halldóra Þorsteinsdóttir

Áslaug Árnadóttir

Egill Heiðar Gíslason