Mat á fullvissustigi auðkenna

Rafræn skilríki undir Íslandsrót á farsímum

Útgáfa 1.0 - 18. júní 2015

Inngangur

Í þessu skjali er mat sérfræðinga ráðgjafarfyrirtækisins Admon ehf. á fullvissustigi rafrænna skilríkja sem gefin eru út af Auðkenni fyrir farsíma. Skilríkin eru metin sem almenn auðkenni til afnota fyrir einstaklinga í samfélaginu gagnvart þjónustuveitum.

Skjalið er sett fram sem viðauki við skýrslu Admon *Mat á fullvissustigi auðkenna: Sannvottun á auðkennum fyrir rafræna þjónustu*[1] þar sem lagt var mat á mismunandi útfærslur á rafrænni auðkenningu og sannvottun með hliðsjón af svokölluðu QAA matskerfi sem kennt er við STORK verkefnið.

Þetta mat á rafrænum skilríkjum í farsíma er gert með hliðsjón af alþjóðlega staðlinum ISO/IEC 29115:2013 *Entity authentication assurance framework*. Í matinu er vísað til stýringa í staðlinum með kaflanúmerum og númerum stýringa (sjá kafla 10 í ISO/IEC 29115:2013).

Efnistök skjalsins miða við lesendur sem eru sérfræðingar í rafrænum auðkennum og í útfærslu á útgáfu þeirra og notkun í rafrænni þjónustu yfir fjartengingar. Niðurstöður matsins ættu einnig að höfða til stjórnenda og annarra sem þurfa að taka ákvörðun um útfærslu á öryggi í rafrænni þjónustu.

Mat á fullvissustigum rafrænna auðkenna í þessu skjali er byggt á opinberum upplýsingum, meðal annars á vefsetrum útgefenda og annarra hagsmunaaðila. Farið var yfir lýsingar þeirra á ferlum við skráningu áskrifenda og afhendingu auðkennanna og á útfærslu á rafrænni sannvottun á notendum sem krefjendum réttinda til innskráningar. Einnig er byggt á fyrirliggjandi upplýsingum um kröfur til útgáfu og útgefenda, meðal annars í opinberum vottunarstefnuskjölum. Að auki er í sumum tilvikum byggt á sértækri þekkingu skýrsluhöfunda á fyrirkomulagi við skráningu og notkun rafrænu auðkennanna.

Niðurstöður matsins afmarkast því að miklu leyti af þeim gögnum sem eru aðgengileg og eru ekki réttari en þær upplýsingar sem byggt er á. Ef lesendur hafa athugasemdir eða ábendingar um rangfærslur er mikilvægt að þeir komi þeim á framfæri við Admon í tölvupóstfangi info@admon.is.

Rafræn skilríki undir Íslandsrót á farsímum

Rafræn skilríki á farsímum eru gefin út af Auðkenni undir Íslandsrót og byggja því á dreifilyklaskipulagi Íslandsrótar (e. public key infrastructure – PKI). Uppruni traustsins er Íslandsrót sem er sjálfundirrituð rót í eigu ríkisins. Fjármála- og efnahagsráðuneytið fyrir hönd ríkisins

[1] *Mat á fullvissustigi auðkenna: Sannvottun á auðkennum fyrir rafræna þjónustu*. Admon ehf., útgáfa 2.0 frá 27. júní 2013.

rekur vottunarstöð Íslandsrótar[2] og tryggir trúverðugleika rótarinnar. Útgáfa Íslandsrótar er samkvæmt Vottunarstefnu Íslandsrótar[3]. Auðkenni sem útgefandi rafrænna skilríkja til fullgildra rafrænna undirskrifta er undir eftirliti Neytendastofu.

Íslandsrót undirritaði útgáfuskilríki Auðkennis „Fullgilt auðkenni“ 6. júní 2008. Auðkenni gefur út endaskilríki til einstaklinga sem eru undirrituð af „Fullgilt auðkenni“ og þar með undir trausti á Íslandsrót[4]. Í dag eru endaskilríkin bæði fyrir auðkenningu og undirskriftir og eru gefin út á örgjörvum snjallkorta, meðal annars á debetkortum allra banka og sparisjóða, og fyrir SIM-farsímakort.

Rafrænt skilríki á farsíma er í raun bæði rafrænt vottorð undirritað af „Fullgilt auðkenni“ sem varðveitt er miðlægum áreiðanlegum kerfum Auðkennis og einkalykill sem myndaður er samhliða undirritun vottorðsins. Einkalykillinn er notaður til að beita skilríkjunum við sannvottun og undirskriftir. Hann er myndaður og vistaður í öruggum dulritunarbúnaði í örgjörva SIM-farsímakortsins.

SIM-farsímakortin innihalda tvo einkalykla. Annar einkalykillinn er ætlaður fyrir rafrænar undirskriftir og uppfyllir kröfur laga nr. 28/2001 um rafrænar undirskriftir[5] en hinn einkalykillinn er ætlað fyrir auðkenningar. Gerð vottorða og myndun beggja einkalykla fer fram á sama hátt og þeir uppfylla því sömu kröfur að öllu leyti, nema hvað auðkenningarlykillinn er ekki ætlaður til undirskrifta.

Endaskilríkin eru gefin út í samræmi við kröfur í Vottunarstefnu Auðkennis[6]. Framkvæmd vottunar við útgáfu skilríkjanna er lýst í yfirlýsingu Auðkennis[7].

Rafræna sannvottunin byggir á nokkrum þáttum í dreifilyklaskipulaginu, meðal annars staðfestingu á umráðum krefjandans yfir einkalyklinum sem byggir á dulritun. Rafrænu skilríkin eru því margþætt; þau eru vottorð, þau eru undirskriftarbúnaður, þau eru dulritunarbúnaður og þau eru örugg hirsla fyrir einkalykil sem er leynilykill notaður sem dulmálslykill bæði í sannvottun og við myndun rafrænnar undirskriftar.

Rafræn skilríki undir Íslandsrót á farsímum hafa fullvissustig LoA4.

[2] Sjá www.islandsrot.is og www.skilriki.is.
[3] *Vottunarstefna Íslandsrótar*. Fjármálaráðuneytið, útgáfa 1.0, 19. maí 2008. Kennimark viðfangs {joint-iso-itu-t(2) country(16) is(352) fyrirtæki-samtök-og-stofnanir(1) fjarmalaraduneyti(1) dreifilyklaskipulag-cp(1) íslandsrót(1)}. Sjá http://cp.islandsrot.is/Vottunarstefna Íslandsrótar 01-00-00.pdf.
[4] Milliskilríkið „Fullgilt auðkenni“ er í eigu Auðkennis ehf. „Fullgilt auðkenni“ undirritar þau skilríki sem gefin eru út undir Íslandsrót í dag og votta einstaklinga. Sjá nánar á www.audkenni.is/rafraenskilriki/.
[5] Lög nr. 28/2001 um rafrænar undirskriftir með síðari breytingum, samþykkt 7. maí 2001.
[6] *Vottunarstefna Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni*. Auðkenni, útgáfa 1.1, 27. nóvem ber 2013. Kennimark viðfangs {joint-iso-itu-t(2) country(16) is(352) fyrirtæki-samtök-og-stofnanir(1) audkenni(2) pki(1) public-pki(1) cp-fa(1) version(2)}.
[7] *Yfirlýsing Auðkennis um framkvæmd vottunar fyrir fullgild rafræn skilríki gefin út undir Fullligldu auðkenni*. Auðkenni, útgáfa 2.0, 4. janúar 2012. Kennimark viðfangs {joint-iso-itu-t(2) country(16) is(352) companies-organizations-and-institutes(1) audkenni(2) pki(1) public-pki(1) cps-fa(5) version(1)}.

Rafræn skilríki undir Íslandsrót farsímum			
Stýringar	**Gæðastig**	**Fullvissustig fasa**	**Fullvissustig auðkenna**
Sönnun á kennslum	LoA4	LoA4	LoA4
Myndun skírteina	LoA4	LoA4	
Útgáfa skírteina	LoA4		
Virkjun skírteina	LoA4		
Afturköllun skírteina	LoA4		
Endurnýjun skírteina	LoA4		
Skráavarsla	LoA4		
Sannvottun eininda	LoA4	LoA4	

Forsendur matsins eru í köflunum hér á eftir.

Innritun (*Enrolment phase*)

Rafræn skilríki eru afhent á skráningarstöðvum eftir ítarlega sannvottun á áskrifandanum í eigin persónu. Einungis skráningarfulltrúar sem hafa fengið sérstaka þjálfun annast afhendingu rafrænna skilríkja. Skráningarstöðvar eru í flestum útibúum banka og sparisjóða á Íslandi og hjá Auðkenni.

Þeir ferlar sem notaðir eru uppfylla kröfur í lögum nr. 28/2001 um rafrænar undirskriftir. Við sannvottun í eigin persónu er tekið afrit af opinberum persónuskilríkjum með mynd og skráð raðnúmer þeirra og kenni áskrifandans staðfest með uppflettingu í gögnum frá þjóðskrá. Skráningarfulltrúi staðfestir skráningu með aðgerðum og rafrænni undirskrift í sérstöku skráningarstöðvarkerfi.

Þessir ferlar uppfylla einnig kröfur um aðgerðir gegn peningaþvætti og fjármögnun hryðjuverka sbr. lög nr. 64/2006[8] og leiðbeinandi tilmæli Fjármálaeftirlitsins nr. 5/2014[9].

Ef vottorðshafinn (sá sem er vottaður í skilríkinu) er með fullgild rafræn skilríki til auðkenningar og undirskrifta, sem hann hefur virkjað áður, getur hann sótt um og virkjað rafræn skilríki á farsíma yfir Internetið á þjónustuvef Auðkennis. Sú þjónusta notar rafrænu skilríkin fyrir auðkenningu af fullvissustigi LoA4 og fyrir fullgilda rafræna undirskrift á nauðsynlegum gögnum. Sú þjónusta uppfyllir þannig öll skilyrði og kröfur fyrir afhendingu og virkjun fullgildra rafrænna skilríkja.

Sönnun á kennslum er því í samræmi við skjalfesta og viðurkennda ferla fyrir auðkenningu sem styðja mestu fullvissu (LoA4; sjá stýringu #1 í kafla 10.1.2 í ISO/IEC 29115:2013).

Viðveru áskrifandans er krafist við afhendingu og virkjun skilríkjanna, eða skilríkin eru virkjuð yfir Internetið með sömu fullvissu á auðkennum og staðfestingu með rafrænni undirskrift með skilríkjum af hæsta öryggisstigi (LoA4), sem styður mestu fullvissu við afhendingu og virkjun (LoA4; sjá stýringu #2 í kafla 10.1.2 í ISO/IEC 29115:2013).

[8] Lög nr. 64/2006 um aðgerðir gegn peningaþvætti og fjármögnun hryðjuverka með síðari breytingum, samþykkt 14. júní 2006.
[9] Leiðbeinandi tilmæli nr. 5/2014 um aðgerðir gegn peningaþvætti og fjármögnun hryðjuverka.

Upplýsingar um kennsl einstaklingsins byggja á opinberum gögnum og eru sannprófuð byggt á opinberum gögnum. Staðhæfingar um auðkenni hans eru margföld, skila ótvíræðri auðkenningu og innihalda sértæk gögn. Staðhæfingarnar eru staðfestar með raunlægum opinberum persónuskilríkjum með mynd auk þess að vera undirrituð rafrænt af skráningarfulltrúa. Áreiðanleiki upplýsinga styður því mestu fullvissu (LoA4; sjá stýringu #6 í kafla 10.1.2 í ISO/IEC 29115:2013).

Fullvissustig við innritun fyrir rafræn skilríki undir Íslandsrót á farsímum er því LoA4.

Umsjón skírteina (*Credential management phase*)

Auðkenni ehf. sem vottunarstöð rafrænna skilríkja er fullgildur útgefandi fullgildra vottorða samkvæmt kröfum í V. kafla í lögum nr. 28/2001 um rafrænar undirskriftir og starfar undir eftirliti Neytendastofu. Rafræn skilríki undir Íslandsrót, þar með talin skilríki í farsímum, eru fullgild vottorð sem uppfylla kröfur í 7. gr. laga nr. 28/2001 um rafrænar undirskriftir.

Rafræn skilríki á farsímum eru búin til í samræmi við skjalfesta ferla sem uppfylla kröfur um fullgild skilríki. Vensl einkalykils við vottorðshafann (þann sem er vottaður) er myndað samhliða sannvottun á kennslum hans og staðfestingu á skráningu, þannig að einkalykillinn er einungis undir hans stjórn eftir að skilríkið er virkjað. Einkalykill rafrænu skilríkjanna er varðveittur í öruggum búnaði í örgjörvaflögu SIM-farsímakortsins og samsvarandi dreifilykill og vottorð er varðveitt undirritað af útgáfuskilríkinu „Fullgilt auðkenni“ í áreiðanlegum kerfum Auðkennis. Skilríkin eru því varin gegn fikti (e. tampering) til að styðja mesta fullvissustig (LoA4; sjá stýringar #2, #3 og #4 í kafla 10.2.2 í ISO/IEC 29115:2013).

Einkalykillinn er myndaður í örgjörva SIM-farsímakortsins á þann hátt að ekki er hætta á því að illvilja aðilar geti falsað skilríki á ópersónugerð kort. Virkjun allra þátta sem gerir mögulegt að mynda og beita einkalyklinum er gerð í samfelldu og rekjanlegu ferli við virkjun skilríkisins, þar sem sannvottun á kennslum vottorðshafa er órjúfanlegur lykilþáttur. Útgáfa og virkjun rafrænu skilríkjanna styður því mesta fullvissustig (LoA4; sjá stýringar #5, #8 og #11 í kafla 10.2.2 í ISO/IEC 29115:2013).

Geta til að mynda skírteini (e. credentials) til auðkenningar er alfarið og eingöngu undir stjórn vottorðshafans (þess sem er vottaður), þar sem hann einn getur beitt einkalykli sínum til auðkenningar (og undirskrifta). Einkalykillinn er eingöngu varðveittur í örgjörva SIM-farsímakortsins. Kröfur til stýringar #15 eiga því ekki við um skilríkin sjálf. Hins vegar rekur Auðkenni vottunarstöð fyrir „Fullgilt auðkenni“ í samræmi við kröfur til vottunaraðila í lögum nr. 28/2001 um rafrænar undirskriftir í áreiðanlegum kerfum með öruggum búnaði og viðhefur ferla og stýringar í samræmi við það. Trúnaðargögn og öll önnur viðkvæm gögn eru því vernduð í samræmi við mestu kröfur um öryggi sem styður mesta fullvissustig (LoA4).

Kröfum til afturköllunar og endurnýjunar skilríkja er lýst í opinberum gögnum Auðkennis og eru í samræmi við kröfur til vottunaraðila um fullgild rafræn skilríki. Ferlar og stýringar við afturköllun og endurnýjun skilríkja styðja því mesta fullvissu (LoA4; sjá stýringar #16 og #19 í kafla 10.2.2 í ISO/IEC 29115:2013).

Auðkenni uppfyllir kröfur um skráningu allra skilríkja, sögu þeirra og stöðu. Auðkenni veitir afturköllunarþjónustu bæði með afturköllunarlistum og svokölluðum OCSP-skeytum og varðveitir allar skrár í samræmi við vottunarstefnu fyrir „Fullgilt auðkenni“. Skráavarsla styður því mestu fullvissu (LoA4; sjá stýringu #21 í kafla 10.2.2 í ISO/IEC 29115:2013).

Fullvissustig við umsjón rafræna skilríkja undir Íslandsrót á farsímum er því LoA4.

Sannvottun eininda (*Entity authentication phase*)

Við rafræna sannvottun, til að staðfesta að krefjandi hafi umráð og stjórn á skilríkinu, þá sendir þjónustuveitan táknstreng yfir örugga samskiptarás inn í örgjörva SIM-farsímakortsins sem er dulritaður þar með einkalyklinum. Notkun einkalykilsins er ræst með því að notandinn slær inn auðkenningar-PIN (4-6 tölustafir) fyrir skilríkið. Dulritaða strenginn er einungis hægt að dulráða með dreifilykli sem þjónustuveitan þekkir (staðfest með undirritun útgáfuskilríkisins „Fullgilt auðkenni“) og tengist krefjandanum einum. Þannig getur þjónustuveitan, sem krefjandinn biður um aðgang inn á, staðfest að einungis sá sem hefur umráð yfir einkalyklinum getur hafa dulritað táknstrenginn.

Auðkenningar-PIN sem krefjandinn notar til að beita einkalykli sínum fer ekki yfir samskiptatengingar við þjónustuveituna heldur einungis frá lyklaborði farsímans til örgjörvans. Auk þess eru öll samskipti yfir Internetið við sannvottun á rafrænum skilríkjum hjúpuð með dulritun (HTTPS). Samskipti á milli áreiðanlegra kerfa Auðkennis og appsins á farsímanum er yfir dulritaða tengingu (3DES-lykill tengdur SIM-farsímakortinu) og samskipti á milli farsímans og símafélags er einnig yfir dulritaða tengingu með öðrum dulritunarlykli (3DES).

Búnaðurinn (í örgjörvanum) sem verndar einkalykilinn og inniheldur dulmálsaðgerðir uppfyllir kröfur fyrir matsþrep EAL4+ í „Common Criteria“, sem eru samþykktar af Evrópuþinginu sem fullnægjandi fyrir öruggan undirskriftarbúnað fyrir fullgildar undirskriftir skv. lögum nr. 28/2001 um rafrænar undirskriftir (þar sem lögin uppfylla kröfur í tilmælum Evrópuþingsins og ráðsins 1999/93/EB um ramma bandalagsins varðandi rafrænar undirskriftir).

Rafræn skilríki undir Íslandsrót veita þannig öfluga vörn gegn öllum tilgreindum árásum í kafla 10.3.1 í ISO/IEC 29115:2013. Þó ber að hafa í huga að það er fræðilega mögulegt að illvilja aðili geti komist á milli lyklaborðs farsímans og örgjörvans en slík áhætta er þekkt og nær í hverju tilviki einungis til eins farsíma. Ef skaði verður þá er hann skaði eins einstaklings en hefur ekki áhrif á öryggi auðkenningarkerfisins í heild.

Sannvottun með rafrænum skilríkjum á farsímum er því fjölþátta sannvottun (e. multi-factor authentication) þar sem stýringar vernda gegn þekktum ógnum og styðja mestu fullvissu (LoA4; sjá stýringar #1 til #21 í kafla 10.3.2 í ISO/IEC 29115:2013).

Stjórnun og skipulag

Stjórnun og skipulag hjá Auðkenni styður mesta fullvissustig fyrir rafræn skilríki undir Íslandsrót á farsímum.

Auðkenni er viðurkenndur vottunaraðili fyrir útgáfu fullgildra skilríkja fyrir fullgildar undirskriftir í samræmi við kröfur í lögum nr. 28/2001. Öll þjónusta Auðkennis og undirverktaka Auðkennis er útfærð í samræmi við kröfur í lögum og samningum.

Sem vottunaraðili sem gefur út fullgild skilríki þarf Auðkenni að uppfylla kröfur um fjárhagslegan stöðugleika.

Auðkenni rekur stjórnkerfi upplýsingaöryggis í samræmi við alþjóðlega staðalinn ISO/IEC 27001. Útgáfa og notkun rafrænna skilríkja á farsímum byggir á trausti opinberrar rótar – Íslandsrótar – sem er í eigu ríkisins og rekin af fjármála- og efnahagsráðuneytinu.