Öryggi rafrænna skilríkja fyrir farsíma

Ályktun

2. júlí 2015

Inngangur

Þetta skjal er ályktun sérfræðinga hjá ráðgjafafyrirtækjunum Admon og Syndis á öryggi rafrænna skilríkja sem gefin eru út fyrir farsíma af fyrirtækinu Auðkenni.

Ályktunin er gerð að beiðni fjármála- og efnahagsráðuneytisins til að svara eftirfarandi spurningu:

> *Hefur áhætta sem fyrirtækið NowSecure tilkynnti um þann 16. júní 2015, sem varðar veikleika í lyklaborðsforriti í Samsung Galaxy farsímum, áhrif á öryggi rafrænna skilríkja sem gefin eru út fyrir farsíma af fyrirtækinu Auðkenni?*

Ályktunin byggir á opinberum upplýsingum og þekkingu sérfræðinga Admon og Syndis á útfærslu rafrænna skilríkja og notkun þeirra, á kröfum um rafrænar auðkenningar og fullgildar undirskriftir og á öryggi farsíma með hliðsjón af þekktum veikleikum í notkun þeirra.

Admon og Syndis hafa ekki unnið sérstaka greiningu á tilgreindum veikleikum í Samsung Galaxy farsímum. Ályktunin byggir á mati sérfræðinga Admon og Syndis á öryggi með hliðsjón af eðli veikleikans sem fyrirtækið NowSecure hefur gert greiningu á og opinberað. Ályktunin er takmörkuð við útfærslu Auðkennis á rafrænum skilríkjum sem gefin eru út undir Íslandsrót fyrir farsíma.

Ályktun

Öryggisáhætta í Samsung Galaxy snjalltækjum sem fyrirtækið NowSecure tilkynnti um þann 16. júní 2015 er marktæk. En það þarf þekkingu og einbeittan brotavilja til að nýta veikleikann.

Illvilja aðili sem nær að nýta sér veikleika í Swift lyklaborðsforriti Samsung Galaxy snjalltækja getur náð stjórn á keyrslu forritakóta sem kerfisnotandi (*system user*) með mikil réttindi á tækinu án þess að handhafi tækisins verði var við það. Þá er mögulegt að koma fyrir spillihugbúnaði og ná stjórn á tækinu.

Hinn illvilja aðili þarf ekki að hafa snjalltækið í höndunum. Honum nægir að vera í nálægð við tækið til að brjótast inn á þráðlausu fjarskiptin og ná þannig stjórn á gagnastraumi frá tækinu til að brjótast inn á tækið, gera breytingar eða koma fyrir spillihugbúnaði. Hann getur hins vegar ekki nýtt sér þennan tiltekna veikleika nema þegar gerð er uppfærsla á Swift lyklaborðsforritinu sem gerist við endurræsingu og með handahófskenndu millibili.

Rafræn skilríki Auðkennis fyrir farsíma eru fullgild skilríki gefin út undir Íslandsrót. Þau eru útfærð í öruggum undirskriftarbúnaði sem uppfyllir kröfur laga nr. 28/2001 um rafrænar undirskriftir hvað varðar myndun, varðveislu og notkun einkalykilsins til að framkvæma fullgildar rafrænar undirskriftir. Einkalykill skilríkjanna er varðveittur í örgjörva SIM-farsímakortsins. Til að beita skilríkjunum fyrir auðkenningu eða til undirskrifta þarf notandinn að hafa farsíma með skilríkjunum á SIM-farsímakortinu og þekkja notkunaraðgangsorð sem er PIN-númer.

Kröfur í lögum um öruggan undirskriftarbúnað ná ekki til öryggis í snjallsímanum sjálfum. Kröfurnar eru afmarkaðar við búnað sem er frá Auðkenni í SIM-farsímakortinu og traust samskipti hans við næsta umhverfi. Sem dæmi þá eru samskipti frá lyklaborði yfir í viðmótið sem tekur á móti PIN-númerinu utan afmörkunar. Hins vegar er gerð krafa um að tenging viðmótsins við öruggan búnað í örgjörva SIM-farsímakortsins sé gerð traust með viðeigandi tæknilegum aðferðum og útfærslu. Veikleikar í búnaði notenda sem gera mögulegt með einbeittum brotavilja að komast á milli lyklaborðsins og viðmótsins til að stela PIN-númeri, t.d. með lyklaborðsrita, eða til að falsa samskipti við SIM-farsímakortið, varða því ekki kröfur í IV. kafla laga nr. 28/2001.

Það er á ábyrgð notandans sem áskrifanda skilríkjanna (þess einstaklings sem vottaður er með skilríkjunum) að vernda einkalykil sinn og halda leynd um PIN-númerið sem þarf til að beita einkalyklinum. Áskrifandinn ber einnig ábyrgð á öllum aðgerðum sem framkvæmdar eru með rafrænum skilríkjum (einkalyklinum) og PIN-númerinu. Honum ber að biðja um afturköllun skilríkja um leið og hann telur að öryggi þeirra sé ógnað á einhvern hátt. Slík afturköllun gerir skilríkin ógild og ónothæf til auðkenninga eða undirskriftar.

Það er jafnframt á ábyrgð notandans að halda farsíma sínum ásættanlega öruggum. Ef illvilja aðili nær stjórn á tækinu, annað hvort með því að stela sjálfu tækinu af notandanum eða SIM-farsímakortinu úr tækinu eftir að hann hefur stolið PIN-númerinu eða með því að brjótast inn á tækið, þá gæti hann villt á sér heimildir, fengið innskráningu inn á kerfi byggt á réttindum notandans og undirritað rafræn gögn í nafni hans.

En það eru aðrir veikleikar þekktir í farsímum og það eru til einfaldari leiðir til að brjótast inn á farsíma, sérstaklega ef illvilja aðila nægir að hafa réttindi notanda til að valda skaða. Þá er einnig hægt að beita mun einfaldari aðferðum til að stela PIN-númeri úr farsímum, ef það er einbeittur vilji til þess. Ein vel þekkt leið er að setja upp löglegt forrit (app) sem ritar allan áslátt lyklaborðsins og miðlar því til ytri aðila[1]. Slíkur hugbúnaður er í boði, meðal annars fyrir foreldra til að fylgjast með notkun barna sinna á farsímum.

Þessi umræddi veikleiki í Samsung Galaxy snjallsímum eykur því ekki mögulegan skaða af innbrotum þó honum fylgi ný árásarleið.

Það er mikilvægt að hafa í huga að það er ekki til fullkomið öryggi og það er ekki hægt að útiloka að illvilja aðili með einbeittan brotavilja, nægja þekkingu, nægan tíma og með öflug verkfæri geti brotið hverjar þær varnir sem útfærðar eru í tæknibúnaði. Það eru þekktir veikleikar í borðtölvum, fartölvum, spjaldtölvum, snjallsímum, farsímum og öðrum nettengdum búnaði sem nota má til að koma fyrir spillihugbúnaði í þeim tilgangi að ná stjórn

[1] Dæmi um hugbúnað sem ætlaður er til vöktunar á snjallsímum er iKeyMonitor Mobile Keylogger sem vaktar alla notkun símans í rauntíma og sendir gögn upp á vefsíðu. Með hugbúnaðinum er einnig hægt að fylgjast með skjánum og taka yfir stjórn á símanum í fjartengingu (sjá www.spy-mobile-phone.com).

á búnaðinum og til að komast yfir leyndarmál eins og aðgangsorð, greiðslukortanúmer og PIN-númer þegar þau eru slegin inn. Slíkir veikleikar geta haft áhrif á nánast öll samskipti sem eiga sér stað í tölvuvæddu umhverfi og ógna öryggi almennt. Veikleikar þessara tækja eru mismunandi og erfitt er að fullyrða hvaða tegund búnaðar er viðkvæmari en annar.

Að okkar mati eru gerðar viðeigandi ráðstafanir með tæknilegum aðferðum og útfærslu til að koma í veg fyrir að illvilja aðili geti brotið varnir öruggs búnaðar fyrir rafræn skilríki Auðkennis í SIM-farsímakorti og geti þannig falsað samskipti við skilríkjabúnaðinn í örgjörvanum, lesið einkalykilinn eða á annan hátt beitt einkalyklinum.

Ef illvilja aðili nær að brjótast inn í snjalltæki og ná réttindum kerfisnotanda er ekki hægt að útiloka að hann geti náð algjörri stjórn á tækinu og þar með á beitingu rafrænna skilríkja sem eru í öruggum búnaði á SIM-farsímakorti, jafnvel án þess að notandi tækisins verði var við það. Skaði af slíkri árás, ef hún tekst, er þá væntanlega afmarkaður við einn einstakling og mögulega misnotkun á rafrænum skilríkjum þess einstaklings. Slík árás ógnar ekki trausti á rafrænum skilríkjum Auðkennis fyrir farsíma í heild sinni né því skipulagi sem gerir notkun rafrænna skilríkja undir Íslandsrót mögulega.

Umræddur veikleiki í Samsung Galaxy snjallsímum eykur því að okkar mati ekki þá hættu sem nú þegar er þekkt í farsímum og varðar öryggi í notkun rafrænna skilríkja. Veikleikinn hefur sem slíkur ekki áhrif á öryggi rafrænu skilríkjanna sem gefin eru út undir Íslandsrót fyrir farsíma af fyrirtækinu Auðkenni. Fyrst og fremst hefur þessi tiltekni veikleiki alvarleg áhrif á notendur Samsung Galaxy síma.

Eins og fyrr segir þá eru notendur farsíma og snjalltækja ábyrgir fyrir öryggi þeirra. Þeir bera ábyrgð á leynd um PIN-númerin og verndun tækisins sem búnaðar með rafrænum skilríkjum á SIM-farsímakorti. Það er því mikilvægt að notendur séu almennt vakandi fyrir öryggisveikleikum í tækjum sínum, uppfæri hugbúnað reglulega til að koma upp lagfæringum og bótum á þekktum veikleikum og gæti þess að nota nettengdan búnað ekki á óöruggum netum. Notendur þurfa einnig að þekkja áhættu sem varðar notkun rafrænna skilríkja og hafa möguleika á því að fylgjast með notkun sinni á þeim til að geta brugðist við öryggisatvikum.

Til að styðja notendur í því að tryggja öryggi sem best við notkun rafrænna skilríkja ætti að þrýsta stöðugt á lausnaraðila að bæta og lagfæra þekkta veikleika, miðla upplýsingum um veikleika í öllum búnaði til notenda og auka vitund þeirra um ábyrgð sína. Þeir lausnaraðilar sem gefa út rafræn skilríki þurfa að veita betri upplýsingar til notenda um notkun á rafrænu skilríkjunum fyrir auðkenningu og undirritanir svo einstaklingar geti sjálfir sinnt eftirliti með notkun á sínum eigin skilríkjum.

Hér á eftir eru forsendur ályktunarinnar og nánari skýringar á þáttum sem liggja til grundvallar.

Forsendur og skýringar

Veikleiki í lyklaborðskóta Samsung Galaxy farsíma

Öryggisfyrirtækið NowSecure hefur tilkynnt um marktæka öryggisáhættu í Samsung Galaxy snjalltækjum vegna veikleika í lyklaborðsforriti (Swift) sem er hluti af for-uppsetningu

tækjanna[2]. Samkvæmt greiningu NowSecure er veikleikinn í Swift lyklaborðsforritinu sem Samsung hefur byggt á SwiftKey lyklaborðsforriti frá breska fyrirtækinu SwiftKey og útfært með tólum frá þeim (kallað Swift SDK). Swift lyklaborðsforritið er með gangverk fyrir uppsetningu á nýjum tungumálum eða uppfærslu á þeim sem þegar eru uppsett.

Veikleikinn er talinn mjög alvarlegur, meðal annars vegna þess að Swift lyklaborðið keyrir sem kerfisnotandi með réttindi sem eru nánast rótarréttindi. Swift lyklaborðsforritið er þó frábrugðið SwiftKey smáforritinu (app) sem hægt er að hlaða í snjalltækin frá Google play smáforritavefsetrinu, þó það hafi að hluta til sama veikleika.

NowSecure hefur sýnt fram á að illvilja aðili þurfi að hafa getu til að breyta umferð sem fer frá tækinu upp í farsímanetkerfið eða í gegnum þráðlaust net sem tækið er tengt við. Að því gefnu að hann hafi stjórn á umferðinni þá getur hann nýtt sér veikleikann þegar tækið er endurræst eða þegar lyklaborðsforritið er uppfært. Það er athyglisvert að hægt er að nýta sér veikleikann án þess að handhafi snjalltækisins þurfi nokkuð að gera, og jafnvel án vitundar hans.

Illvilja aðili getur náð skrifréttindum á snjalltækið sem kerfisnotandi með því að grípa sendingar frá tækinu og svara því með sínum fölsuðu gögnum. Skrifréttindin er síðan hægt að nota til að yfirskrifa keyrslukóta með spillikóta sem gerir það sem árásaraðilinn hefur útfært.

Illvilja aðili getur þannig náð stjórn á keyrslu forritakóta sem kerfisnotandi (system user) með mikil réttindi á tækinu án þess að handhafi snjalltækisins verði var við það. Hann gæti þannig fengið aðgang að skynjurum og öðrum virkum einingum eins og GPS, myndavél og hljóðnema tækisins. Hann gæti hlerað skilaboð eða samtöl í símanum. Hann gæti stolið gögnum af tækinu og fiktað í virkni tækisins á margan hátt.

Þessi veikleiki varðar alla Samsung Galaxy snjallsíma af gerðinni S4, S5 og S6. Samsung hefur boðið farsímafyrirtækjum bót (patch) en ekki hefur verið staðfest að þau hafi gefið viðskiptavinum sínum kost á því að uppfæra snjalltækin.

Það er fátt til ráða annað en að uppfæra snjalltækin með bótinni frá Samsung. Það er ekki hægt að fjarlægja Swift lyklaborðsforritið og veikleikinn er til staðar þó það lyklaborðsforritið ekki virkjað í tækinu. Ef notendur geta ekki uppfært snjalltæki sitt þá er einu valkostirnir til að forðast veikleikann að nota annað tæki eða forðast óörugg þráðlaus net (wi-fi).

Kröfur til öruggs búnaðar fyrir rafrænar undirskriftir

Í IV. kafla í lögum nr. 28/2001 um rafrænar undirskriftir eru settar fram kröfur til öruggs undirskriftarbúnaðar. Þessi lög voru sett til að innleiða tilskipun Evrópuþingsins og ráðsins nr. 1999/93/EB um rafrænar undirskriftir, þar sem kröfur til öruggs undirskriftarbúnaðar eru tilgreindar í viðauka III. Í ákvörðun framkvæmdastjórnarinnar 2003/511/EB var gefinn út listi yfir almennt viðurkennda staðla um búnað fyrir rafrænar undirskriftir og í reglugerð nr. 780/2011 um rafrænar undirskriftir er vísað í sömu kröfuskjöl í viðauka. Á þessum lista yfir

[2] Sjá vefsetur NowSecure á slóðinni www.nowsecure.com. Tæknilega lýsingu Ryan Welton sérfræðings hjá NowSecure má finna á vefslóðinni https://www.nowsecure.com/blog/2015/06/16/remote-code-execution-as-system-user-on-samsung-phones/.

kröfuskjöl er meðal annars skjalið CWA 14169 sem tilgreinir kröfur til öruggs undirskriftarbúnaðar í samræmi við viðauka III í tilskipun nr. 1999/93/EB[3].

CWA 14169 byggir á alþjóðlega staðlinum ISO/IEC 15408, hlutum 1-3 frá 1999 sem skilgreina viðmið fyrir mat á upplýsingatæknilegu öryggi. Staðallinn er þekktur undir nafninu „Common Criteria“.

Búnaður með fullgildum rafrænum skilríkjum sem uppfyllir CWA 14169 er sagður uppfylla EAL4+ fullvissustig í mati á öryggi búnaðar. Undirskrift með slíkum skilríkjum er því fullgild undirskrift samkvæmt lögum.

Kröfur í 8. gr. IV. kafla laga nr. 28/2001 má útleggja þannig fyrir farsímaskilríkin:

1. Búnaðurinn skal tryggja að einkalykillinn[4]
    a. sé einkvæmur og að hann verði ekki myndaður aftur (liður a) 1. mgr.),
    b. verði með hliðsjón af eðlilegum öryggiskröfum ekki brotin upp (liður b) 1. mgr.) og
    c. sé varinn með fullnægjandi hætti gegn notkun annarra en undirritanda (liður c) 1. mgr.).
2. Búnaðurinn skal einnig tryggja
    a. leynd einkalykilsins með fullnægjandi hætti (2. mgr.) og
    b. að rafræn undirskrift sé varin gegn fölsun (2. mgr.).
3. Jafnframt skal ekki vera unnt að nota öruggan undirskriftarbúnað til að breyta þeim gögnum sem undirrita á eða hindra að undirritandi geti séð gögnin fyrir undirritun (3. mgr.).

Í viðauka III í tilskipun 1999/93/EB er sagt að búnaðurinn skuli tryggja kröfurnar í lið 1 og 2 hér fyrir ofan „með viðeigandi tæknilegum aðferðum og útfærslu“. Búnaður telst því uppfylla kröfur um öruggan undirskriftarbúnað ef tæknilegar aðferðir og útfærsla eru viðeigandi og uppfylla kröfur í CWA 14169.

Útfærsla rafrænna skilríkja Auðkennis fyrir farsíma

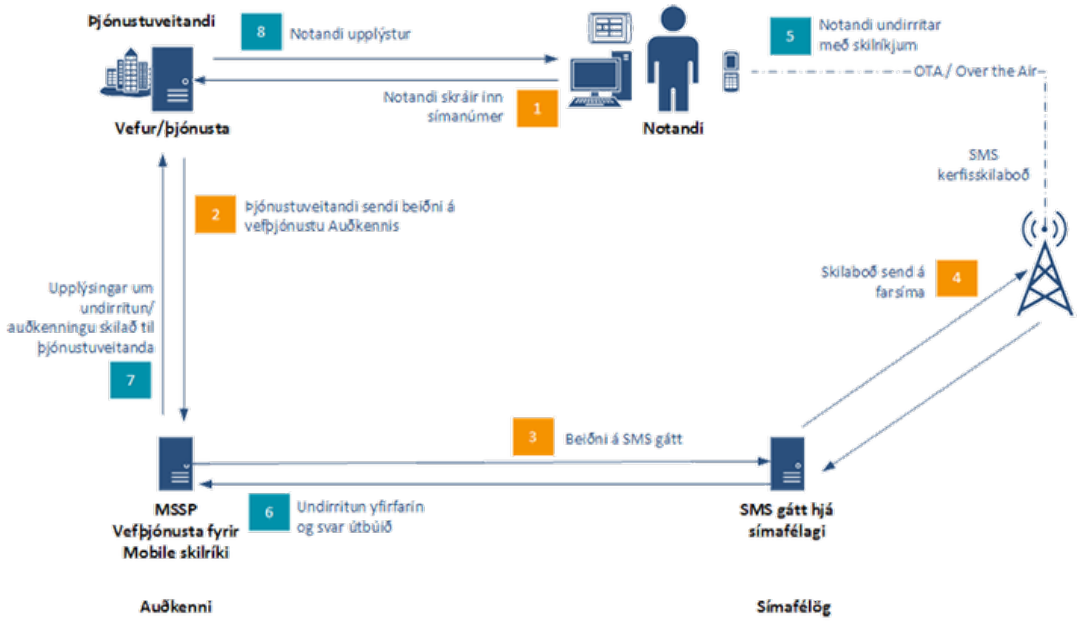
Rafræn skilríki Auðkennis fyrir farsíma eru gefin út undir Íslandsrót sem er í eigu ríkisins. Útgáfuskilríki Auðkennis er kallað „Fullgillt auðkenni“ og er undirritað af Íslandsrót sem útgefanda.

Í útfærslu Auðkennis á rafrænum skilríkjum fyrir farsíma eru skilríkin að hluta til í örgjörva SIM-farsímakorts og að hluta til í kerfum Auðkennis. Skilríki er búið til með því að mynda lyklapar (einkalykil og stærðfræðilega tengdan dreifilykil) í örgjörvanum, senda dreifilykilinn síðan yfir trausta tengingu til kerfa Auðkennis[5] sem undirrita dreifilykilinn ásamt öðrum gögnum í vottorði skilríkisins með milliskilríkinu Fullgilt auðkenni.

[3] CWA 14169 er samkomulag vinnuhóps CEN/ISSS um rafrænar undirskriftir (WS/E-SIGN). Ákvörðun 2003/511/EB tilgreindi CWA 14169 frá mars 2002, en vinnuhópurinn leiðrétti nokkuð af villum og sendi frá sér nýja útgáfu í mars 2004 sem almennt er miðað við. Vinnuhópurinn hefur einnig gefið út leiðbeiningar um útfærslu öruggs undirskriftarbúnaðar sem CWA 14355.

[4] Í 5. tl. 3. gr. laga nr. 28/2001 eru undirskriftargögn skilgreind sem „einstök gögn, svo sem kótar eða einkalykill dulritunar, sem undirritandi notar til að mynda rafræna undirskrift.“ Með hugtakinu er því átt við einkalykilinn. PIN-númer sem notað er til að beita skilríkinu og er þáttur í verndun gegn óheimilli beitingu þeirra getur ekki talist undirskriftargögn þar sem það er ekki notað til að mynda undirskriftina.

[5] Þegar talað er um „kerfi Auðkennis“ í þessu skjali þá er átt við vefþjónustu og önnur sérkerfi Auðkennis fyrir öryggisþjónustu (MSS: *Managed Security Services*) sem tengjast þjónustuveitu sem treystanda og SMS-gáttum fjárskiptafyrirtækja, auk vottunarkerfa Auðkennis sem m.a. undirrita vottorð útgefinna skilríkja.



Skilríki Auðkennis fyrir farsíma eru í raun tvenn skilríki. Annað er notað fyrir rafræna auðkenningu og sannvottun, til dæmis fyrir innskráningu í örugg kerfi, en hitt skilríkið er notað fyrir rafrænar undirskriftir í hugbúnaði sem er til þess gerður[6]. Útfærsla Auðkennis á báðum skilríkjum – auðkenningarskilríki og undirskriftarskilríki – uppfyllir sömu kröfur þannig að bæði búnaður og skilríkin sjálf taka mið af ströngustu kröfum fyrir fullgildar rafrænar undirskriftir, þó ekki sé tekið á kröfum til skilríkja fyrir auðkenningar í núgildandi lögum.

Myndin hér fyrir ofan sýnir flæði skilaboða þegar skilríkjum á farsíma er beitt. Myndin á við hvort sem um er að ræða auðkenningu eða undirskrift. Nánari lýsing á flæði, gögnum og samskiptaháttum er á vefsetri Auðkennis[7].

Við auðkenningu og undirskriftir eru í raun tvö sambönd í gangi. Annars vegar er notandinn í sambandi við þjónustuveitu í gegnum útstöð sína, þar sem hann þarf að auðkenna sig eða undirrita rafræn gögn. Hins vegar eru kerfi Auðkennis í samskiptum við farsíma notandans til að sannprófa auðkenningu og undirskriftir. Þar sem þau skeyti (skilaboð) sem send eru í farsímann byggja á upplýsingum frá þjónustuveitunni þá er mjög erfitt að komast inn í samskiptin til að valda skaða. Til þess þarf að brjótast á sama tíma inn í samskiptin á milli kerfa Auðkennis og farsímans og inn í samskiptin á milli útstöðvar notandans og þjónustuveitunnar eða á milli þjónustuveitunnar og kerfa Auðkennis.

Samkvæmt yfirlýsingum Auðkennis þá uppfyllir örgjörvi SIM-farsímakortsins kröfur til öruggs undirskriftarbúnaðar í CWA 14169, og þar með kröfur í IV. kafla laga nr. 28/2001 um rafrænar undirskriftir[8]. Örgjörvinn er ásættanlegur til að mynda lyklaparið, varðveita og nota einkalykilinn til auðkenningar og til að framkvæma fullgildar rafrænar undirskriftir. Leynd einkalykilsins er varin þar sem ekki er hægt að lesa hann eða birta á neinn hátt, og hann er einungis til í einu eintaki sem varðveitt er í örgjörvanum á SIM-farsímakortinu. Hirslan sem

[6] Dæmi um slíkan hugbúnað er lausn Advania sem þeir kalla Signet (http://www.advania.is).
[7] Rafræn skilríki á farsímum: http://www.audkenni.is/fyrirtaeki/thjonustuveitendu/rafraen-skilriki-farsimum/.
[8] Sjá *Vottunarstefnu Auðkennis fyrir fullgild rafræn skilríki gefin út undir Fullgildu auðkenni*, útgáfu 1.1 og *Fylgiskjal: Kröfur til öruggs undirskriftarbúnaðar*, útgáfu 2.03 (http://www.audkenni.is/um-audkenni/vottunarstodvar/).

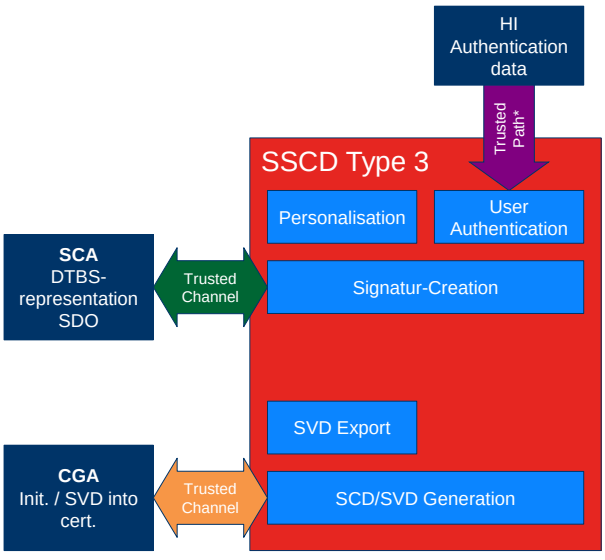
geymir einkalykilinn er varin gegn innbrotum og einungis sá sem hefur SIM-farsímakortið og veit PIN-númerið getur beitt lyklinum til auðkenningar eða undirritunar.

Sérstakur hugbúnaður frá Auðkenni er í SIM-farsímakortinu til að hægt sé að sannvotta auðkenningu og framkvæma undirskriftir. Þessi hugbúnaður uppfyllir einnig, samkvæmt yfirlýsingu Auðkennis, kröfur til öruggs undirskriftarbúnaðar og tryggir þannig að auðkenning og undirskrift séu varin gegn fölsun. Búnaðurinn styður einnig örugga útfærslu á ytri undirskriftarkerfum (SCA: *Signature Creation Application*) þannig að þau geti tryggt að ekki sé unnt að breyta þeim gögnum sem undirrita á né hindra að undirritandi sjái þau gögn sem hann er að undirrita. Samskipti kerfa Auðkennis við hugbúnað þeirra á SIM-farsímakortinu eru dulrituð með leynilyklum Auðkennis en auk þess eru samskipti fjarskiptafyrirtækisins við farsímann dulrituð á hefðbundinn hátt með leynilyklum fjarskiptafyrirtækisins.

Til viðbótar er hugbúnaður í kerfum Auðkennis sem myndar vottorð skilríkjanna (CGA: *Certification Generation Application*) og sér um samskipti á milli þjónustuveitu (treystanda skilríkjanna) og farsímans. Þessi kerfi uppfylla einnig kröfur til öruggs undirskriftarbúnaðar fyrir þá virkni sem þar er samkvæmt yfirlýsingu Auðkennis.

Kröfur til öruggs undirskriftarbúnaðar í CWA 14169 afmarkast í farsíma notandans við samskipti ytra undirritunarkerfis (SCA) við undirskriftareiningu búnaðarins (*signature creation*). Þau samskipti þurfa að vera traust, og eru það í útfærslu Auðkennis. Til skýringa er hér fyrir neðan mynd fengin úr CWA 14169:2004 (sjá mynd 3 bls. 9) sem sýnir virkniþætti öruggs undirskriftarbúnaðar af þeirri tegund sem Auðkenni hefur útfært fyrir farsíma og samskipti búnaðarins við nærumhverfi sitt.

CGA:	Certification Generation Application
DTBS:	Data to be Signed
HI:	Human Interface
SCA:	Signature-Creation Application
SCD:	Signature-Creation Data
SDO:	Signed Data Object
SSCD:	Secure Signature-Creation Device
SVD:	Signature-Verification Data
TOE:	Target of Evaluation



* The trusted path for user authentication will be required if the HI is not provided by the TOE itself (e. g., it is provided by a SCA outside the SSCD)

Fyrirtækið NowSecure, sem tilkynnti nýlega um veikleika í Swift lyklaborði Samsung Galaxy snjalltækja, hefur tekið út og vottað útfærslu Auðkennis á SIM-farsímakortum fyrir rafræn skilríki í farsímum með bæði Android og iOS stýrikerfi[9].

Samskipti frá lyklaborði notandans í viðmót undirritunarkerfisins er utan afmörkunar á öruggum undirskriftarbúnaði. Það er því mikilvægt að hafa í huga að kröfur til öruggs undirskriftarbúnaðar taka ekki til öryggis á milli lyklaborðs og undirritunarkerfisins (SCA). Það er ávallt hætta á því að illvilja aðili sem getur fylgst með áslætti á lyklaborð útstöðvar eða farsíma geti uppgötvað PIN-númerið sem notað er til að beita skilríkjunum. Það er líka ávallt hætta á því að einhver annar sjái yfir öxlina á notandanum hvað hann slær inn þegar hann notar skilríkin sín og læri þannig PIN-númerið. Það er hins vegar lítið gagn að því að hafa náð PIN-númerinu nema hafa stjórn á skilríkjunum í farsímanum, annað hvort með því að brjótast inn á hann eða stela honum (eða SIM-farsímakortinu).

Útfærsla á kerfum Auðkennis styður lausnir ytri aðila fyrir undirskriftir á gögnum í samræmi við kröfur í 3. mgr. 8. gr. laga nr. 28/2001, þannig að tryggt sé að gögnum sem á að undirrita sé ekki breytt í örugga undirskriftarbúnaðinum og að þau gögn sem eru undirrituð eru þau sem undirritanda eru birt, ef honum eru birt gögnin. Þannig sé mögulegt að útfæra kerfi fyrir undirskriftir þar sem undirritandanum eru alltaf birt gögnin sem hann er að undirrita, eða þegar hann ákveður sjálfur að hann vilji sjá þau, án þess að öryggi undirskriftarbúnaðurinn komi í veg fyrir það.

Í dreifilyklaskipulagi Íslandsrótar er áskrifandi skilríkja ábyrgur fyrir því að vernda einkalykil sinn og halda leynd um PIN-númerið sem þarf til að beita einkalyklinum. Þessi ábyrgð kemur meðal annars fram í kafla 6.2 í vottunarstefnu Auðkennis, í 12. gr. almennra skilmála Auðkennis og í 6. gr. áskriftarsamnings einstaklings[10]. Áskrifandinn ber einnig ábyrgð á öllum aðgerðum sem framkvæmdar eru með rafrænum skilríkjum (einkalyklinum) og PIN-númerinu. Áskrifandi er jafnframt ábyrgur fyrir því að biðja um afturköllun skilríkja um leið og hann telur að öryggi þeirra hafi verið ógnað á einhvern hátt. Slík afturköllun gerir skilríkin ógild og ónothæf til auðkenninga eða undirskriftar.

Að lokum er rétt að benda á að skaði sem verður af misnotkun á skilríkjum þegar PIN-númeri og farsíma er stolið afmarkast við það tiltekna skilríki og handhafa þess. Slíkt öryggisbrot hefur ekki áhrif á öryggi dreifilyklaskipulagsins undir Íslandsrót né það öryggi sem útfært er í kerfum Auðkennis og öruggum búnaði fyrir skilríkin, sem uppfyllir allar kröfur í lögum og reglugerðum um notkun rafrænna skilríkja til fullgildra undirskrifta. Sömu kröfur eru uppfylltar fyrir rafræn skilríki Auðkennis í farsímum sem ætluð eru til auðkenningar, þó íslensk lög nái ekki yfir slík skilríki eða notkun þeirra.

Arnaldur F. Axfjörð sérfræðingur hjá Admon og
Theódór R. Gíslason sérfræðingur hjá Syndis.

[9] Sjá vefslóðina https://www.nowsecure.com/services/appsecure/certified/audkenni/.
[10] Sjá vefslóðina http://www.audkenni.is/um-audkenni/vottunarstodvar/.