Veebilehitsejas Chrome läheb ID-kaardiga allkirjastamine (korraks) katki

9. aprill 2015 - 22:25 Autor: Anto Veldre

RIA analüütik Anto Veldre kirjutab sellest, mida toob kaasa Google Chrome'i brauseriuuendus.

Järgmisel nädalal üllitab Google uue versiooni Chrome'i brauserist versiooninumbriga 42. Uuendus toob Eestis kaasa vajaduse uuendada digiallkirjastamiseks kasutatavat tarkvara (kuuekohaline kasutajahulk) ning teha muudatusi allkirjastamist pakkuvates veebiteenustes (kümneid, sadu teenuseid).

Chrome'i versioon 42 muudab viisi, kuidas ID-kaart brauseriga suhtleb – tegemist on padutehnilise standardiga, mille nime teadsid seni vaid programmeerijad. Kui tänaseni toimus brauseri ja ID-kaardi omavaheline suhtlus NPAPI (Netscape Plugin Application Programming Interface http://en.wikipedia.org/wiki/NPAPI) tehnoloogias, siis alates Chrome'i versioonist 42 alustab Google loobumist sellest pisut aegunud standardist. Säilitamaks Chrome'i puhul ID-kaardiga allkirjastamise funktsionaalsust, tuleb üle minna uuele tehnoloogiale "Native Messages API". Seda tuleb teha umbes 4-kuulise akna jooksul, mis Google meile jätab.

NPAPI –> Native Messages API

Sellel sügavalt tehnoloogilisel muudatusel on mõju ja nõudeid nii kasutajale kui ka teenusepakkujale. Mõlemad pooled peavad edukaks üleminekuks astuma teatud samme. Õnneks pole üleminek järsk, vaid toimub etapiviisiliselt. NPAPI tugi lõpetatakse lõplikult alles Chrome'i augustikuises versioonis (44?) ning siis juba sellisel moel, et seda polegi võimalik tagasi sisse lülitada.

NB! Ühtlasi muutub alates Chrome'i versioonist 42 algoritm, mille alusel hinnata veebisaitide turvasertifikaate. Edaspidi märgitakse punasega ebaturvaliseks need veebisaidid, mis pruugivad aegunud SHA-1 tehnoloogiat (Krüptograafiliste algoritmide kasutusvaldkondade ja elutsükli uuring, lk 21). Kuivõrd tegu on eraldi teemaga, siis tuleb neis küsimusis pöörduda veebiteenuse pakkuja poole.

NPAPI kadu – mis muutub kasutaja jaoks?

1. Kuniks kasutaja saab oma arvutis pruukida alternatiivseid sirvikuid (nagu Mozilla Firefox ja IE), võib Chrome'i uuendamisega kaasnevast lihtsalt mööda vaadata ja kasutada neid teisi brausereid.
2. Pärast seda kui Google on kättesaadavaks teinud Chrome'i versiooni 42 ning kasutaja ongi selle juba alla laadinud, tuleb astuda ka teine samm – uuendada ID-kaardi tarkvara viimasele versioonile (https://installer.id.ee) ka siis, kui seda on äsja tehtud. Tarkvara uuendamise käigus tuuakse Google'i poest kohale edaspidi vältimatu laiendus (*extension*) nimega "Token signing" (kasutajalt RIA). Paigalduse käigus sobitatakse Chrome'i häälestused üleminekuaegseteks. Pärast NPAPI hülgamist ja veebisaitide uuendamist augustiks 2015 tagab allkirjastamise Chrome'i laiendus "Token Signing" iseseisvalt ning Chrome'i häälestusi ei ole enam vaja modifitseerida.
3. Veebiteenuste pakkujad asendavad oma veebilehtedel vana lahenduse uuega, misjärel hakkab veebis digiallkirjastamine taas igas kontekstis tööle. Üleminekuperioodi vältel saab allkirjastamine toimuda nii uues kui vanas tehnoloogias. Eeldusel, et arvutis on tarkvara uuendatud, toimub valik automaatselt.
4. Alati on võimalik, et Murphy külastab just Sinu arvutit. Siis tuleb abi küsida oma IT-osakonnalt, ID-kaardi abiliinilt 1777 … või ajutiselt pruukida teist brauserit.

NPAPI kadu – mis muutub teenusepakkuja jaoks?

1. Teenusepakkuja all mõtleme siinkohal kõigi sääraste veebisaitide omanikke, kus (vastavuses digitaalallkirja seadusega) pakutakse dokumendi või andmete allkirjastamist. See puudutab nii riigiasutuste portaale kui ka eraõiguslikke (nt pangad) ja ühiskondlikke portaale.
2. Teenusepakkujatel on vajalik ajavahemikus aprillist augustini 2015 viia oma veebisait vastavusse Native Messaging API tehnoloogiaga. Seni pruugitav Javascripti vahekiht tuleb asendada **hwcrypto.js vahekihiga**. Kui veebiserveris seda uuendust mitte teha, siis alates (umbes) augustist pole Chrome sel konkreetsel saidil enam allkirjastamiseks kasutatav. Chrome'i turuosa (ligi 40%) teades võib see osutuda probleemiks.
3. Muudatus võib veebisaidi omanikule tähendada mõningat, kuigi mitte väga suurt kulu. Kes kasutavad vana idCard.js vahekihti, nende jaoks on muudatus lihtne. Kes aga on valmis pusinud omaenda lahenduse, neile võib muudatus osutuda keerulisemaks.

Mis juhtub, kui ma lihtkasutajana seda uudist ignoreerin?

1. Kui oma arvutis leiduva Chrome'i versiooni pärast üldse mitte muretseda, siis varem või hiljem saabub olukord, kus arvutis on Chrome juba värskendunud, aga ID-kaardi tarkvara veel mitte, ühtlasi puudub allkirjastamiseks edaspidi vajalik Chrome'i laiendus (*extension*). Kui mitte reageerida, siis lühemaks või pikemaks ajaks muutub Chrome allkirjastamise jaoks kasutamatuks. Kuivõrd ID-kaardi tarkvara uueneb ka automaatselt, peaks see olukord nädalaga iseeneseslikult mööduma.
2. RIA ja SK teevad hetkel pingsalt tööd, et publitseerida võimalikult selged juhendid selle kohta, kuidas ning mis järjekorras peab kasutaja mainitud tarkvaru uuendama. Juhendid muutuvad kättesaadavaks mõni tund pärast Chrome 42 tegelikku avalikustamist (ligikaudu 15. aprillil).

Mis juhtub, kui ma teenusepakkujana muutust ignoreerin?

1. Alates Chrome'i versiooni 42 avalikustamisest hakkab järsult tõusma pöördumiste arv, sest inimesed ei saa enam veebiteenuses

allkirja anda… seega tuleks planeerida võimekus pöördumistele vastamiseks (Helpdesk vms). Kui ma oma veebisaidis hwcrypto.js tuge ei realiseeri, siis alates umbes augustist 2015 ei saa Chrome'iga minu portaalis digiallkirjastamise teenust enam kasutada.

Olen itimees. Rääkige mulle, mis TEGELIKULT sünnib?!

1. Külasta neid linke ja vii end uue olukorraga kurssi:

- eestikeelsed õppematerjalid RIA kodulehel,
- ingliskeelne Wiki (https://github.com/open-eid/hwcrypto.js/wiki),
- abivahend kasutaja installatsiooni testimiseks (https://open-eid.github.io/hwcrypto.js/sign.html) – kuid tulemusi tõlgendama ja kasutajale selgitama peab kindlasti IT-inimene.

2. Kontrolli üle oma firma või asutuse tööjaamalahendused. Juhul, kui mingi teadaolev piirang/sõltuvus sunnib Sind kas Chrome'i või ID-kaardi tarkvara **MITTE UUENDAMA** ning kui tööprotseduur näeb ette massilist Chrome'iga allkirjastamist, siis varu aega ja tegele lahendustega. Mida varem asud neid otsima, seda parem, sest septembriks 2015 on valikud juba ahtad.

3. Arvesta, et firma või asutuse võrgus on kasutajaõiguste piirangud ning kasutajad ei saa arvutisse ise programme installeerida. Korralda uuenduste paigaldamine nii, et see ei segaks normaalset töörütmi.

Miks küll Chrome nii teeb?

1. Tehnika progress on vältimatu, selle ignoreerimine tähendaks reaalsusega võitlemist. Võimalik, et mingi aja jooksul lähevad Native Messaging API suunas ka teised internetibrauserid.

Suured tarkvaratootjad ei arvesta muudatusi tehes Eesti ID-kaardi ökosüsteemiga, mis tähendab, et peame oma muudatustega hakkama saama meile eraldatud ajavahemikus (seekord umbes 4 kuud).

Artikkel on pärit Riigi Infosüsteemi Ameti blogist.

- Uudised

- Turvalisus
- Tarkvara