

Tekniikka edennyt korttirintamalla

Sähköinen henkilökortti on huipputurvallinen

Sähköinen henkilökortti on kuvallinen kortti, jossa on mikrosiru. Siruun ei ole tallennettu kortin haltijan henkilötunnuksia, kotiosoitetta tai syntymäaikaa. Siruun on kuitenkin tallennettu käyttäjän sähköinen asiointitunnus SATU, eli e-tunnus. Sähköinen henkilökortti on erittäin turvallinen. Se on varmentettu varmenteen varmenteella.

Teksti Merja Kihl
Kuva Hannu Mäntylä



Sähköistä henkilökorttia ei voi kopioida, eikä sille tallennettuja haltijan yksityisiä avaimia voida siirtää kortilta. Yksityisistä avaimista ei ole kopioita missään. Edes kortinhaltija itse ei tiedä yksityisiä avaimiaan, selvittää Väestörekisterikeskuksen yksikönjohtaja Tapio Aaltonen sähköisen henkilökortin turvallisuutta.

Sähköinen henkilökortti on henkilökortti, mikä toimii niin sanottuna yleisenä verkkoavaimena sähköisissä asiointipalveluissa.

Kun kansalainen hakee ensimmäisen kerran sähköistä henkilökorttia, poliisin lupahallinnon virkailija luo väestötietojärjestelmään sähköisen asiointitunnuksen, SATUn. SATU on sisällöltään juokseva sarjanumero. Se ei kerro haltijastaan mitään tietoja – toisin kuin henkilötunnus. SATU loppuu tarkistusmerkkiin, mikä lasketaan samoin kuin henkilötunnuksen tarkistusmerkki. Vaikka SATU on elinikäinen, sähköinen henkilö-

kortti on voimassa vain kolme vuotta kerrallaan.

Tiedostopohjaisten avainten turvallisuudessa puutteita

Yritykset ja yksityishenkilöt ovat pitkään käyttäneet tiedostopohjaisia avaimia ja/tai varmenteita, esimerkiksi PGP-sovellusta.

Tiedostopohjaisten varmenteiden tietoturva on älykorttipohjaiseen tekniikkaan verrattuna huomattavasti heikompi, sillä tiedostopohjaisia varmenteita voidaan kopioida rajattomasti. Niitä voidaan myös 'pommittaa' murto-ohjelmilla, koska salasana-arvausyrityksiä ei voida rajoittaa.

Yksityiset avaimet voivat myös levitä huomaamatta, esimerkiksi käyttäjän kotihakemistosta palvelimelle. Silloin ei tiedetä kopioiden määrää”, Väestörekisterikeskuksen yksikönjohtaja Tapio Aaltonen va-

roittaa. Hän ehdottaa riskin vähentämistä muun muassa lisäämällä varmennehakemistoja ja sulkulistoja.

Sähköinen henkilökortti erittäin luotettava

Sähköisellä henkilökortilla olevat

roittaa. Hän ehdottaa riskin vähentämistä muun muassa lisäämällä varmennehakemistoja ja sulkulistoja.

Sähköinen henkilökortti erittäin luotettava

Sähköisellä henkilökortilla olevat

Sähköisen henkilökortin avulla sähköinen allekirjoitus

Asiapaperi voidaan allekirjoittaa sähköisesti eli tietokonetta käyttäen.

Allekirjoituksen luotettavuuteen vaikuttaa muun muassa käytetyn allekirjoitusavaimen pituus sekä allekirjoitusalgoritmi.

Avaimen pituus on 1024 bittiä.

Monenlaisia käyttömahdollisuuksia

- Sähköisen henkilökortin avulla henkilö voidaan tunnistaa sähköisesti.
- Kortti kelpaa virallisena matkustusasiakirjana 15 Euroopan maan alueella (niin kutsuttu minipassi).
- Kortin haltija voi allekirjoittaa asiapapereita sähköisesti Internetissä.
- Kortin varmenne mahdollistaa viestien ja asiakirjojen salauksen.
- Esimerkiksi posti, maistraatit ja Väestörekisterikeskus voivat ottaa vastaan muutto- ja osoitteenmuutosilmoituksia sähköisellä henkilökortilla.
- Myös työvoimatoimistoissa, LEL-Työeläkekassoissa, TaELTyöeläkekassoissa, TEL-eläkevakuutusyhtiöissä, Tilastokeskuksessa, Tullissa, Yrittäjien Fenniassa, Tekesissä sekä Tampereen, Lappeenrannan ja Vantaan kaupunkien virastoissa voi asioida sähköisen henkilökortin avulla.
- Lisää palveluita tulee koko ajan, muun muassa Kolumbuksen sähköpostiin.

Kesäkuussa 2004 lisää mahdollisuuksia

- Kesäkuun 2004 alusta on mahdollista hankkia sähköinen henkilökortti, johon on yhdistetty sosiaaliturvakortin tiedot.
- Yhdistettyä korttia koskevan hakemuksen voi jättää poliisilaitoksen lisäksi myös Kansaneläkelaitoksen toimipisteeseen. Kortin myöntää kuitenkin aina poliisi.
- Yhdistettyä korttia voi käyttää kaikissa viranomaisten sähköisissä palveluissa mukaan lukien sosiaali- ja terveydenhuollon sähköiset palvelut.
- Uusi yhdistetty henkilökortti toimii nykyiseen tapaan myös matkustusasiakirjana, jollaisena sitä voi passin sijasta käyttää 15 Länsi-Euroopan maassa.

varmenteet perustuvat julkisen avaimen tekniikkaan (PKI) ja siihen liittyviin julkiseen ja yksityiseen avaimen.

”Sähköistä henkilökorttia ei voi kopioida eikä sille tallennettuja haltijan yksityisiä avaimia siirtää kortilta. Yksityisistä avaimista ei ole kopioita missään. Edes kortinhaltija ei itse tiedä yksityisiä avaimiaan”, Aaltonen sanoo.

Yksityisiä avaimia voi hyödyntää vain PIN-koodien syötön jälkeen, ja PIN-koodit ovat ainoastaan kortinhaltijan tiedossa. Tarvittaessa haltija voi vaihtaa niitä. Kolme väärää PIN-koodin syöttöä kuitenkin lukitsee kortin.

”Kun varmenteita käytetään esimerkiksi verkkopalvelussa, pitää sekä asiakkaan että palvelun tarjoajan voida luottaa siihen, että varmenteen haltija on todella se henkilö, jona hän esiintyy”, Aaltonen muistuttaa.

”Tästä syystä henkilökortin rekisteröijänä toimii poliisi. Sen tehtävä on todentaa luotettavasti hakijan henkilöllisyys.”

Aaltonen mukaan myös Väestörekisterikeskus (VRK) on luotettava, sillä se tarkistaa palvelinvarmenteiden osalta muun muassa kaupparekisteristä hakijan tiedot.

Henkilökortin myöntää poliisi

@ Syyskuun 2003 alusta poliisin myöntämät henkilökortit ovat aina sähköisiä henkilökortteja lukuun ottamatta alaikäisille ilman huoltajan suostumusta annettavaa henkilökorttia ja väliaikaista henkilökorttia.

@ Kortin voimassaoloaika on kolme vuotta.

@ Hakemuksen voi jättää mihin tahansa poliisin palvelupisteeseen. Korttihakemus on jätettävä poliisille henkilökohtaisesti. Mukana on oltava kaksi mieluiten mustavalkoista valokuvaa. Lisäksi oma henkilöllisyys on voitava selvittää passin, henkilökortin tai ajokortin avulla. Mikäli hakija on alle 18-vuotias, tarvitaan myös huoltajan suostumus. Poikkeuksena ovat niin sanottu alaikäisten henkilökortit.

@ Sähköinen henkilökortti maksaa 29 euroa.

@ Kortin saa kymmenen työpäivän kuluessa hakemuksen jättämisestä.

”VRK ei myönnä varmenteita väärillä tiedoilla, olemattomille henkilöille tai yrityksille, tai toisen henkilön tai yrityksen tiedoilla”, Aaltonen vakuuttaa.

Käyttö vaatii lisälaitteita

Sähköisen henkilökortin käyttö vaatii joitakin uusia laitteita, mikä aiheuttaa hieman kuluja. Käyttäjällä täytyy olla esimerkiksi kortinlukija ja sen laitteistoajuri sekä Inter-

net-käytön mahdollistava ohjelmisto, esimerkiksi SmartTrust Personal.

Myös sähköisen palvelun tarjoajalla on oltava vähintään verkkopalvelun käyttäjän tunnistamiseen soveltuva www-palvelin, jolla hoidetaan käyttäjän varmenteiden käsittely. Palvelun tarjoajan on lisäksi pystyttävä tarkistamaan sulkulista sekä käyttäjän varmenteen voimassaolo. ●