VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Tapani Karvonen

SIRUKORTIN KÄYTTÖMAHDOLLI-SUUDET NYT JA TULEVAISUUDESSA

Tekniikka ja liikenne
2012

VAASAN AMMATTIKORKEAKOULU

Tietotekniikan koulutusohjelma

TIIVISTELMÄ

Tekijä	Tapani Karvonen
Opinnäytetyön nimi	Sirukortin käyttömahdollisuudet nyt ja tulevaisuudessa
Vuosi	2012
Kieli	suomi
Sivumäärä	43 + 1 liite
Ohjaaja	Martti Mustonen

Opinnäytetyön tarkoituksena on tutkia sirukorttiteknologiaa, sen käyttötarkoituksia sekä tulevaisuudennäkymiä. Kyseessä on suurimmaksi osaksi kvalitatiivinen tutkimus, joka pohjautuu teoreettiseen tietoon.

Tutkimuksessa pyritään käymään läpi sirukortin historiaa Suomessa sekä erilaisia sirukorttityyppejä. Tutkimuksessa käydään myös läpi erilaisia sirukortin salausmenetelmiä ja sirukortin monipuolisia käyttömahdollisuuksia.

Sirukortin käyttömahdollisuudet yritysmaailmassa ja oppilaitoksissa ovat monipuolisia. Sirukorttia voidaan käyttää kulunvalvonnassa, kirjastokorttina, opiskelijakorttina sekä monissa muissa tehtävissä. Yhdellä kortilla voidaan korvata useita kortteja.

Varsinkin oppilaitosten turvallisuuden tarve on lisääntynyt viime aikojen kouluammuskelujen takia ja turvallisuusmääritysten tarve on lisääntynyt entisestään. Sirukortti pystyy vastaamaan turvallisuuden asettamiin haasteisiin. Varsinkin biometrinen tunnistautuminen yhdistettynä sirukortin käyttöön on hyvin turvallinen.

Sirukortin mahdollisuudet ovat suuret ja biometrinen tunnistautuminen liitettynä siihen on varmasti tulevaisuudessa kehittyvä ala. Haasteena on kuitenkin identiteetin suojaaminen. Siihenkin on varauduttu, mutta uuden teknologian edessä ollaan monesti varuillaan. Tulevaisuuden kehitystyö kuitenkin avaa ja tuo sirukortin käytön yhdessä biometrisen tunnistautumisen kanssa entistä tutummaksi ja turvallisemmaksi.

Avainsanat sirukortti, tietoturva, biometrinen tunnistautuminen

VAASAN AMMATTIKORKEAKOULU

UNIVERSITY OF APPLIED SCIENCES

Tietotekniikan koulutusohjelma

ABSTRACT

Author	Tapani Karvonen
Title	Usability of Smart Card Now and in Future
Year	2012
Language	Finnish
Pages	43 + 1 Appendix
Name of Supervisor	Martti Mustonen

The aim of this research is to investigate smart card technology, its usability and future possibilities. This research is mostly qualitative, which is based on theoretical knowledge. However, to support the theory, an experiment is done.

The aim is to investigate the history of smart card in Finland and get to know the types of smart cards. The research will also present different methods of smart card encryptions and versatile possibilities to use smart card technology.

The use of smart card technology in enterprises and educational institutes is versatile. Smart card can be used as a method of access control, library card, student card, and in many other tasks. With smart card technology one card can replace many.

Especially in educational institutes, the need of security has increased due to recent school shootings. Smart card technology is able to respond to the increased security challenges and needs. In particular, the use of smart card with biometric authentication is a combination that gives high degree of security.

Smart card technology has great possibilities and with biometric authentication combined with it, it is definitely the future developing field. The challenge of this combination is, however, identity protection. The developers of this technology have taken this into consideration and it is a secure method. However, with new technology everybody is always first on guard. I believe that future development will make the use of smart card with biometric authentication even more familiar and safer.

Keywords Smart card, data security, biometric authentication

LYHENNELUETTELO

AD	Microsoft Active Directory
	Microsoft Active Directory käyttäjätietokanta ja hakemistopalvelu
CPU	Central Processing Unit
	Keskusyksikkö
EEPROM	Electrical Erasable Programmable Read-only Memory
	Sähköisesti tyhjennettävä haihtumaton puolijohdemuisti
ID	Identity Card
	Henkilöllisyyskortti
OTP	One Time Password
	Kertakäyttöinen salasana
PKI	Public Key Infrastructure
	Julkisten Avainten Infrastruktuuri
RAM	Random Access Memory
	Työmuisti
ROM	Read-Only Memory
	Lukumuisti

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

1 JOHDANTO 8

1.1 Gemalto Oy 8
1.2 Raportin rakenne 10

2 SIRUKORTTI 11

2.1 Sirukortin materiaalit 12
2.2 Erilaiset sirukorttityypit 14
2.2.1 Kontaktikortti 15
2.2.2 Etäluettava kortti 15
2.2.3 Muistikortti 15
2.2.4 Yhdistelmäkortti 16

3 SIRUKORTIN TEKNIIKKA 17

3.1 Sirun prosessori 18
3.2 Sirun muistijärjestelmät 18
3.3 Sirun käyttöjärjestelmä 18

4 TIETOTURVA JA SIRUKORTTI 20

4.1 Kertakäyttöinen salasana 20
4.2 Julkisen avaimen infrastruktuuri PKI 21
4.3 Biometrinen salaus 21
4.4 Erilaiset sirukorttilaitteet ja – välineet 22

5 SIRUKORTTI KÄYTÄNNÖSSÄ 25

5.1 Sirukortti henkilöllisyyden tunnistamisessa 25
5.2 Sirukortti yritysmaailmassa 26

5.3 Sirukortin käyttö oppilaitoksissa 26
5.4 Sirukortin käyttö terveydenhuollossa 27
5.5 Sirukorttiympäristön suunnittelu 27
5.6 Sirukorttijärjestelmän käyttöönotto 30

6 SIRUKORTIN MAHDOLLISUUDET OPPILAITOKSISSA 32

7 SIRUKORTIN TULEVAISUUDENNÄKYMÄT 37

8 YHTEENVETO 39

LÄHTEET 41

LIITTEET 44

TAULUKKOLUETTELO

Taulukko 1. Sirukortin historia s.9

Taulukko 2. Sirukorttiympäristön suunnittelukysymyksiä. s.28

KUVIOLUETTELO

Kuvio 1. ISO 7810 –standardin mukainen henkilökortti. Paksuus: 0,76 mm ± 0,08 mm; kulman säde 3,18 mm ± 0,30 mm. s.11

Kuvio 2. Pienempi sirukortti –malli. s.12

Kuvio 3. Kortin komponentit. s.13

Kuvio 4. Sirukorttityypit. s.14

Kuvio 5. Sirukortin kontaktikohdat. s.17

Kuvio 6. Sirukortin markkinasegmentit. s.25

Kuvio 7. Sirukorttiympäristö. s.30

1 JOHDANTO

1.1 Gemalto Oy

Gemalto Oy on Vantaalla toimiva yritys, joka markkinoi ja valmistaa pääasiassa digitaalisia tietoturvaratkaisuja ja -tuotteita. Yhtiön asiakkaina ovat eri maiden viranomaistahot, pankit ja myös erilaiset yritykset, joille toimitetaan siru- tai SIM-korttiratkaisuja. Vantaalla työskentelee yli 400 työntekijää, joista yli puolet työskentelee tuotannon töissä ja noin 150 henkilöä työskentelee markkinoinnin ja myynnin tehtävissä, tuotekehityksen tehtävissä sekä erilaisissa hallinnollisissa tehtävissä. (Gemalto Oy 2006-2010a; Gemalto Oy 2006-2010b.)

Gemalto on erikoistunut korkean turvatason siru- ja ID-tuotteiden kehitykseen ja tuottamiseen. Näihin tuotteisiin kuuluvat muun muassa passit, maksukortit, henkilökortit, asiakaskortit ja SIM-kortit. Gemaltonin on tarkoitus tarjota asiakkaille turvallisia tapoja pitää yhteyttä ja suojata henkilötietoja sekä muita tietoja nykyajan digitalisoituvassa maailmassa. (Gemalto Oy 2006-2010a; Gemalto Oy 2006-2010b.)

Tytär- ja osakkuusyhtiöitä on Gemaltolla yhteensä neljä. Gemalto Norge AS on Norjassa toimiva tytäryhtiö, joka on keskittynyt Norjan biometrisien passien ja ajokorttien tekoon. Tanskassa toimii tytäryhtiö nimeltä Gemalto Danmark A/S. Yhtiö hoitaa Tanskan biometriset passit, henkilökortit, EMV-kortit ja maksukortit Tanskan markkinoille. AB Svenska Pass on osakkuusyhtiö, joka hoitaa Ruotsin biometriset passit. Ruotsissa toimiva Gemalto AB markkinoi ja myy kortteja sekä niihin kuuluvia ohjelmistoja, laitteita ja palveluita. (Gemalto Oy 2006-2010c.)

Toiminta yrityksessä on alkanut jo vuonna 1885, kun perustettiin Suomen Pankin setelipaino. Ensimmäisiä tuotteita olivat mm. setelit ja postimerkit. Lähes sata vuotta valmistettiin näitä perinteisiä turvapainotuotteita. 1980-luvulla oli yrityksen aika muuttua ja näin alettiin valmistaa ensimmäisiä maksukortteja. 1990-luvulla Setec Oy:stä kasvoi kansainvälinen konserni, joka myöhemmin 2000-luvulla oli yhdistynyt osaksi Gemalto-konsernia. Taulukosta 1 nähdään yrityksen kasvu ja kehittyminen. (Gemalto Oy 2006-2010d.)

Taulukko 1. Sirukortin historia. (Gemalto Oy 2006-2010d.)

”1885	Suomen Pankin setelipaino perustettiin: seteleitä, postimerkkejä ja muita turvapainotuotteita
1983	Maksukortteja
1988	Älykorttiteknologia, polttolaseroitu polykarbonaattikortti
1991	Setec Oy
1994	SIM-kortti
1996	PKI-älykortti
1998	Maailtaman ensimmäinen valtiollinen kortti eID-kortti
1999	Maailman ensimmäinen PKI SIM-kortti
2000	Maailman ensimmäinen EMV PKI -monisovelluskortti
2003	Maailman ensimmäinen biometrinen passidovellus
2005	Gemplus S.A osti Setecin
2006	Gemplus ja Axalto yhdistyivät ja syntyi Gemalto, maailman johtava digitaaliseen turvallisuuteen keskittynyt yhtiö
2008	Gemalto Oy” (Gemalto Oy 2006-2010d.)

Sirukortti ei ole aivan uusi keksintö, koska se keksittiin jo vuonna 1967 Saksassa. Vasta parikymmentä vuotta myöhemmin sirukortti tuli kuitenkin laajempaan käyttöön. Tällöin ranskalaiset ottivat sen käyttöön maksupuhelimissa. 1990-luvulla tulleiden SIM-korttien myötä sirukorttien määrä alkoi kasvaa räjähdysmäisesti. (Lerssi-Lahdenvesi 2006, 4.)

Erilaisten sirukorttien käyttö maailmalla on kasvanut koko ajan ja uskon, että näin on myös tulevaisuudessa. Sirukortin uusia mahdollisuuksia myös opiskelijayhteisössä hyödynnetään jo eri puolilla maailmaa. Banco Santander ja useat yliopistot yhteistyössä ovat tutkineet ja hyödyntäneet sirukortin erilaisia käyttömahdollisuuksia. (Banco Santander 2011.)

Uusimman teknologian avulla sirukortista otetaan kaikki hyöty irti ja personoidaan se yliopistojen tarpeeseen. Korttia on suunniteltu yli 200 yliopistossa ja 11 eri maassa, joten projekti on varsin kattava. Tämän sirukortin avulla opiskelija voi liikkua yliopiston tiloissa, lainata kirjoja sekä saada alennuksia useissa kaupoissa.

Perinteinen opiskelijakortti ei pysty samaan kuin sirukortti. Sirukortin avulla pystytään varmentamaan käyttäjä paremmin ja varmistamaan, että tietoja käyttää oikea henkilö. Sirukortin käyttömahdollisuudet ovat laajempia kuin perinteisen opiskelijakortin, koska siihen voidaan liittää pankkiominaisuuksia ja muita hyötyjä. (Banco Santander 2011.)

Sirukortin hyödyt myös erilaisissa organisaatioissa puhuvat puolestaan. Tietoturva on entistä tärkeämpää ja salattuja tietoja,, esimerkiksi yritysten työntekijöistä on entistä enemmän sähköisessä muodossa. Sirukortin avulla voidaan tällaiset henkilökohtaiset tiedot suojata paremmin. Organisaation on mahdollista käyttää sirukorttia tietojen turvaamisessa useissa eri kohteissa, kuten kiinteistöjen kulunvalvonnassa, verkon käyttäjähallinnassa, tietojen salaamisessa, sähköisissä allekirjoituksissa, kulkukorteissa, etäkäyttöyhteyksissä, pre-boot tunnustautumisissa sekä biometrisissä tunnistautumisissa. (Gemalto Oy 2006-2010e.)

Tämä opinnäytetyön tarkoitus on tutkia sirukortin kehitystä ja teknologiaa. Lisäksi tarkoituksena on selvittää, mihin tarkoituksiin sirukortteja jo käytetään ja mihin sirukorttia voisi tulevaisuudessa hyödyntää. Sirukortin suurin hyöty on siinä, että se pystyy varmentamaan käyttäjänsä, jolloin myös erilaiset tietoturvariskit pienentyvät. Tietoturva onkin suurin sirukortin puolestapuhuja.

1.2 Raportin rakenne

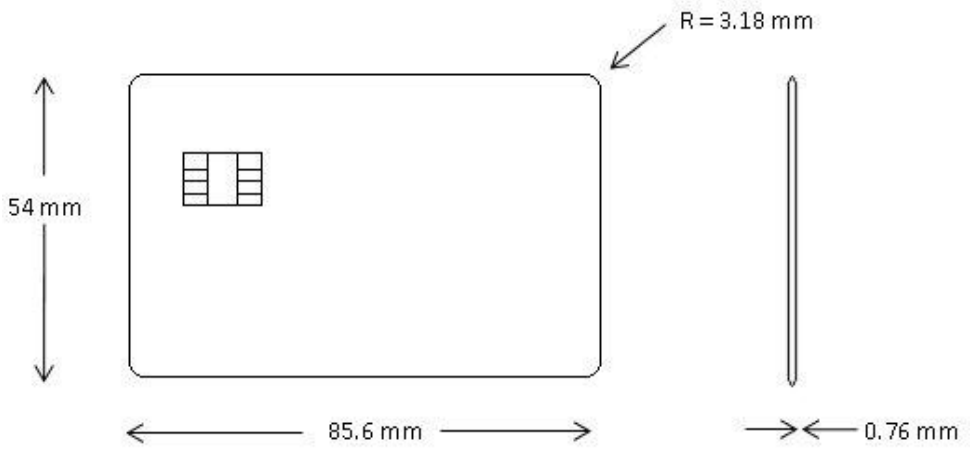
Tutkimuksen tarkoituksena on syventyä siihen, mikä sirukortti on ja sen erilaisiin käyttötarkoituksiin. Tutkimus etenee sirukortin historiasta siihen, mikä sirukortti teknisiltä ominaisuuksiltaan on ja millaisiin eri tyyppeihin ne lajitellaan. Tarkoituksena on myös selvittää uuden teknologian luomia mahdollisuuksia organisaatioissa lisäämässä turvallisuutta.

Tutkimuksessa on kvalitatiivinen ote, koska tarkoituksena on saada kokonaisvaltainen kuva sirukorttien käyttötarkoituksista ja tulevaisuuden mahdollisuuksista. Tarkoituksena on osoittaa sirukortin käyttökelpoisuus turvallisena vaihtoehtona erilaisissa ympäristöissä. (Hirsjärvi, Remes & Sajavaara 2007, 160.)

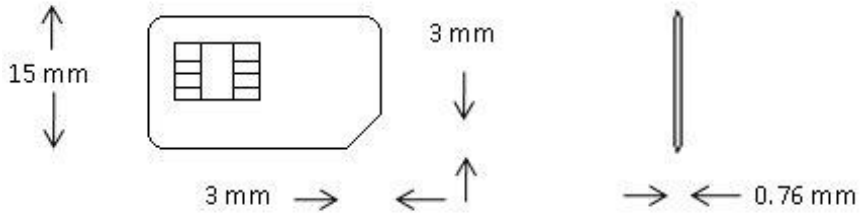
2 SIRUKORTTI

Sirukortti on yleensä muovinen kortti, jonka sisälle on upotettu piiri. Helpointa tällainen kortti on tunnistaa päällä olevasta kultaisesta neliöstä. Sirukortti on leveydeltään 85,6 mm ja korkeudeltaan 54 mm, mikä on ISO 7810 standardin mukainen. Tämä standardi on otettu käyttöön vuonna 1985 ja se on koskenut ID-kortteja eli henkilökortteja. Vaikkakaan tuo standardi ei suoranaisesti koske sirukorttia, on sitä käytetty myös siihen ja monesti useat sirukortit ovatkin juuri tuon standardin mukaisia. (Wolfgang & Wolfgang 2003, 28.)

Kortti voi kuitenkin olla myös huomattavasti pienempi. Tärkein osa kortissa on juuri tuo siru, johon tarpeellinen tieto on säilötty. Uusi teknologia ja laitteiden pienentyminen toi aikoinaan tarpeen myös pienemmälle mallille, kuten lähes kaikki kännykän omistajat tietävät. Nykyään kehitys tuntuu olevan sellainen, että kaikki pyritään saamaan kompaktimpaan kokoon. Alla olevassa kuviossa 1 näkyy ISO 7810 standardin mukainen kortti, eli ihan perinteisen pankkikortin kokoinen kortti ja kuviossa 2 näkyy pienempi sirukortti –malli. (Wolfgang et al. 2003, 28.)



Kuvio 1. ISO 7810 –standardin mukainen henkilökortti. Paksuus: 0,76 mm ± 0,08 mm; kulman säde 3,18 mm ± 0,30 mm. (Wolfgang et al. 2003, 29.)



Kuvio 2. Pienempi sirukortti –malli (Wolfgang et al. 2003, 30.)

Jos sirukortti on niin sanottu kontaktikortti, on siru näkyvissä kortissa. Kortti voi kuitenkin toimia erilaisissa lukulaitteissa eri tavalla ja tämän takia on olemassa myös kortteja, jotka toimivat ilman kontaktia kortinlukijan ja kortin välillä. Tällaisissa korteissa siru on asennettu kortin sisään, josta kortinlukija voi langattomasti lukea kortin tiedot. (Smart Card Alliance 1997-2011 a.)

2.1 Sirukortin materiaalit

Sirukortit rakennetaan enimmäkseen kerroksittain erilaisista materiaaleista, jotta kortista saadaan mahdollisimman kestävä ja toimiva. Nykyään kortit tehdään yleensä PVC:stä, polyesteristä tai polykarbonaatista. Kortin eri kerrokset tehdään ensimmäisenä ja sen jälkeen ne laminoidaan. Tämän jälkeen kortti leikataan standardin mukaisesti. Viimeisenä osana korttiin lisätään itse siru, joka säilöö tarvittavan infomaation. Kaiken kaikkiaan kortin rakentamisessa voi olla jopa 30 eri vaihetta riippuen siitä, mikä kaikkea korttiin halutaan sisällyttää. (CardLogix Corporation 2010a.)

Wolfgang ja Wolfgangin kirjassa Smart Card Handbook sirukortin rakenne on kuvattu hyvin selkeästi. Kortin eri komponentit voivat koostua kortin rungosta, etiketistä, magneettinauhasta, allekirjoitusnauhasta, kuvasta, sirusta ja erilaisista turvallisuusominaisuuksista. Kuviosta 3 nähdään kortin eri komponentit. (Wolfgang & Wolfgang 2010, 40.)

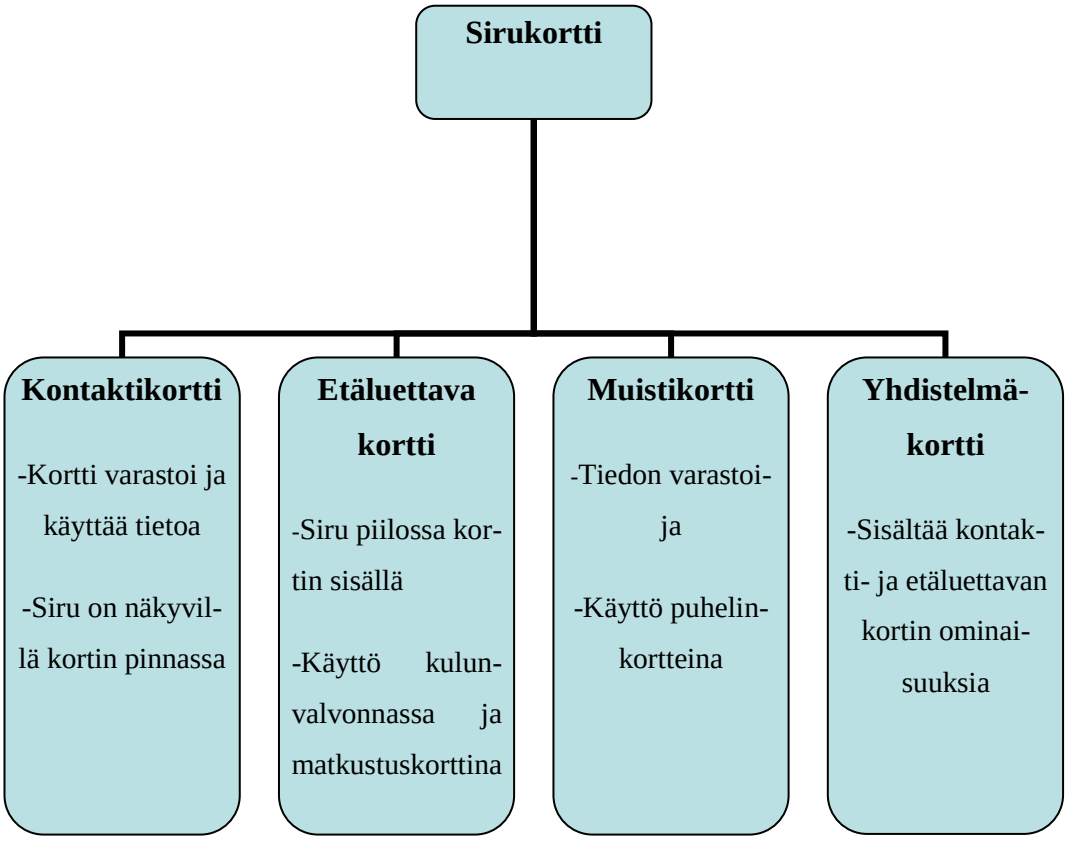
Kuvio 3. Kortin komponentit. (Wolfgang et al. 2010, 40.)

Kortin valmistukselle on asetettu minimivaatimuksia, jotka on määritelty ISO-standardeissa 7810, 7813 ja 7816. Nämä määräykset koskevat muun muassa kortin kestävyyttä, lämmön vastustuskykyä, sähköstaattisia purkauksia ja ultravioletisäteilyä. Erilaisten standardien avulla korteista pyritään tekemään mahdollisimman kestäviä ja laadukkaita. Nämä standardit asettavat kuitenkin vaatimuksia materiaaleille, joista kortti rakennetaan. (Wolfgang et al. 2010, 39.)

Kortin tärkein osa on kuitenkin ennen kaikkea siru itsessään. Siru sisältää kaiken tarvittavan tiedon ja sirukortissa olevien kontaktikohtien avulla sirukortti kommunikoi kortinlukijan kanssa. Etäluettava kortti rakennetaan samoista materiaaleista kuin kontaktikortti. Poikkeuksena kuitenkin on se, että siru ei tule kortin päälle, vaan se rakennetaan kortin sisäpuolelle. Etäluettavassa kortissa on myös antenni ja pieni radiovastaanotin ja –lähetin. (Lerssi-Lahdenvesi 2006, 6; Wolfgang et al. 2003, 21.)

2.2 Erilaiset sirukorttityypit

Sirukortit luokitellaan eri ryhmiin sen mukaan, kuinka ne käsittelevät tietoa sekä sirutyypin ja sirun ominaisuuksien mukaan. Sirukortti voi olla joko kontaktikortti, jolloin tullakseen luetuksi se tarvitsee kontaktin kortinlukijaan, tai kortti voi olla langaton, jolloin kortin ei tarvitse olla kiinteässä kontaktissa kortinlukijaan. Näiden kategorioiden alla kortit jaotellaan kontaktikortteihin, etäluettaviin kortteihin, muistikortteihin sekä yhdistelmäkortteihin. Kuviossa 4 näkyy erilaisten sirukorttityyppien jaottelu ryhmiin. (CardLogix Corporation 2010a; Lerssi-Lahdenvesi 2006, 5.)



Kuvio 4. Sirukorttityypit. (Lerssi-Lahdenvesi 2006, 5-7.)

2.2.1 Kontaktikortti

Kontaktikortti on mikroprosessorilla varustettu älykortti, joka sisältää käyttöjärjestelmän, prosessorin, muistin sekä syöttö- ja lähetysjärjestelmän. Korttia käytetään asettamalla kortti sille tarkoitettuun kortinlukijaan ja antamalla PIN-koodi. Nykyään myös biometrinen tunnistautuminen kontaktikortin käytössä on yleistynyt. Tämä kortti on turvallisempi vaihtoehto magneettijuovakortille, koska tätä ei voi kopioida ja ilman PIN-koodia se on hyödytön. Kontaktikortti on perinteisen luottokortin näköinen, jossa siru on näkyvissä. Sirun avulla kortti ottaa yhteyden kortinlukijaan. (Lerssi-Lahdenvesi 2006, 6.)

2.2.2 Etäluettava kortti

Etäluettava kortti näyttää lähes samalta kuin kontaktikortti, mutta tällaisessa kortissa siru on kortin sisällä eikä näkyvillä, kuten kontaktikortissa. Etäluettavassa kortissa kortti koostuu sirusta, antennista ja pienestä radiovastaanottimesta ja –lähettimestä. Kortti toimii radiotaajuudella, joten kortin sisään asennetut osat vaikuttavat merkittävästi kortin toimintaan. (Lerssi-Lahdenvesi 2006, 6.)

Etäluettavalla kortilla on useita etuja ja suurin niistä onkin varmasti kortin käytettävyyden nopeus. Etäluettavaa korttia käytetään monesti erilaisina matkustuskortteina sekä kulkukortteina. Tulevaisuudessa etäluettavien korttien käyttö saattaakin lisääntyä, koska ne nopeuttaisivat huomattavasti myös kaupoissa maksuprosessia. (Lerssi-Lahdenvesi 2006, 7; CardLogix Corporation 2010a.)

2.2.3 Muistikortti

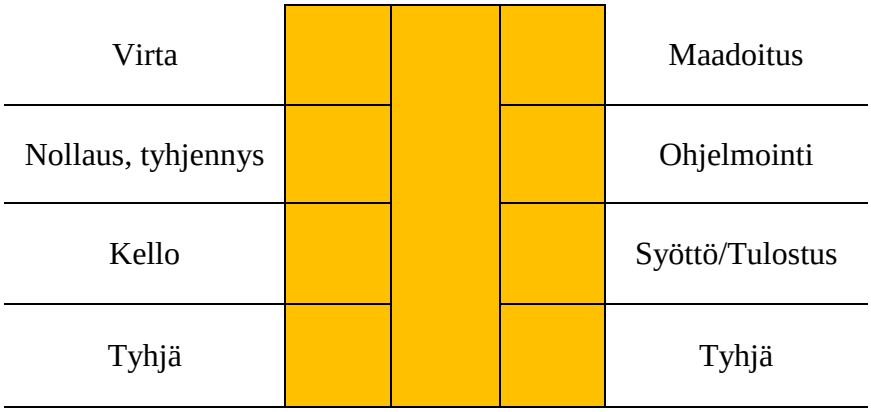
Muistikortti on kortti, joka ei pysty prosessoimaan siihen tallennettua tietoa, vaan se toimii varastona tiedolle. Jokaiselle muistikortille voi lukea ja kirjoittaa tietoa riippumatta siitä, millainen muistikortti on. Erilaiset muistikortit toimivat eri tavalla. Jotkut kortit ovat sellaisia, että ne vain säilövät tietoa eikä niissä ole oikeuksia tiedon prosessoimiseen. (CardLogix Corporation 2010a.)

2.2.4 Yhdistelmäkortti

Yhdistelmäkortilla on nimensä mukaisesti useampia metodeja kommunikoida erilaisten kortinlukijoiden kanssa. Tällaisissa korteissa on siru sekä kortin sisällä että sen päällä. Yhdistelmäkortin kanssa on siis mahdollista saada parhaat puolet eri korttien toiminnoista tai käyttää korttia laajemmin eri asioissa. (Lerssi-Lahdenvesi 2006, 7.)

3 SIRUKORTIN TEKNIIKKA

Sirukorttia voisi verrata pieneen tietokoneeseen, sillä se sisältää samat komponentit. Sirukorttiin on upotettu siru, joka tekee mahdolliseksi sen, että muisti voi säilyttää tietoa ja mikroprosessori voi käyttää tuota tietoa. Sirukortin tärkeimmät ominaisuudet ovat tietenkin sirussa itsessään. Sirukortin päällä on kultainen moduuli, jossa on sirukortin kontaktikohdat, ne kohdat joiden avulla kortinlukija pystyy lukemaan kortin tietoa. Alla olevassa kuviossa 5 on kuvattu sirukortin kontaktikohdat. (Lerssi-Lahdenvesi 2006, 8-9.)



Kuvio 5. Sirukortin kontaktikohdat (Lerssi-Lahdenvesi 2006, 9.)

Moduulin kahdeksalla kontaktikohdalla on omat käyttötarkoituksensa. Kontakteissa on kaksi tyhjää kohtaa, jota ovat varattu mahdollisia tulevia käyttötarkoituksia varten. Kontaktit tuottavat kortille virran, maadoituksen, nollauksen/ tyhjennyksen, ohjelmoinnin, kellosignaalin sekä syöttö-/tulostusportin. (Lerssi-Lahdenvesi 2006, 9.)

Kontaktimoduulin alla sijaitsee sirun tekniikka. Sirussa on yleensä muistijärjestelmä, prosessori (CPU) sekä syöttö- ja lähetysportit (I/O). Kortissa oleva muistijärjestelmä sisältää kolmenlaista muistia, lukumuistin (ROM), työmuistin (RAM) sekä ohjelmamuistin (EEPROM). Joissakin sirukorteissa voi myös olla rinnak-

kaisprosessori, joka suorittaa monimutkaisia laskutoimituksia, jotka liittyvät salaustoimiin. (Lerssi-Lahdenvesi 2006, 8-9.)

3.1 Sirun prosessori

Sirun mikroprosessori eli CPU on yleensä 8- tai 16-bittinen mikroprosessori, joka käyttää siruun tallennettua tietoa. Yleisimmin käytetään Motorolan tai Intelin prosessoreja. Gemalton .NET -sirukortissa, jonka käyttöönottoa Windows-käyttöjärjestelmä tukee, on 32-bittinen mikroprosessori. Korteissa saattaa olla myös rinnakkaisprosessori, joka tukee salaustoimien vaatimia laskutoimituksia. Sirun prosessorin avulla kortilla on suhde kortinlukijaan syöttö-/tulostusportin kautta ja tätä kautta se lähettää tietoa kortinlukijaan. (Gemalto Oy 2008-2011: 3; Lerssi-Lahdenvesi 2006, 10.)

3.2 Sirun muistijärjestelmät

Sirukorteissa käytetään useita eri muistityyppejä. ROM-muisti (Read Only Memory) eli lukumuisti on pysyvä muisti, johon ei voi tehdä muutoksia. Tähän osaan muistia ajetaan tietoa vain kortin valmistusvaiheessa ja tämän jälkeen se on ainoastaan luettavissa. ROM-muistissa sijaitsee kortin käyttöjärjestelmä ja joitain ohjelmia. ROM-muistin tiedot säilyvät, vaikka virta katkeaisikin. (Gemalto Oy 2008-2011, 3.)

RAM-muisti on sirukortin työmuisti. Tähän osaan muistia voidaan kirjoittaa ja lukea tietoa. Tieto ei kuitenkaan säily, mikäli virta katkaistaan. Kortissa on lisäksi EEPROM-muistia, joka on ohjelmamuisti. Tämä on pysyvä tiedon säilytyspaikka. Kuten ROM-muistissa, myös tässä muistissa tieto säilyy, vaikka virta katkeaisikin. (Gemalto Oy 2008-2011, 3.)

3.3 Sirun käyttöjärjestelmä

Sirukortissa on myös käyttöjärjestelmä, joka hallinnoi kortin tietoja. Sirussa voi olla joko kiinteä tiedostojärjestelmä tai dynaaminen sovellusjärjestelmä. Kiinteä tiedostojärjestelmä on yleinen henkilökorteissa ja tällaisessa järjestelmässä oikeudet kortin tiedostoihin annetaan alkuvaiheessa eikä niitä pysty muuttamaan. Dy-

naamisessa sovellusjärjestelmässä oikeuksia ja tiedostoja on mahdollista päivittää. (Lerssi-Lahdenvesi 2006, 10-11.)

Aiemmin käyttöjärjestelmät ovat olleet valmistajakohtaisia, mutta nykyään pyritään käyttämään sellaisia sovelluksia ja järjestelmiä, että valmistajalla ei ole merkitystä. Tällöin päästään eroon ongelmasta, että kortinlukija ja kortti eivät toimi yhdessä. (Lerssi-Lahdenvesi 2006, 11.)

4 TIETOTURVA JA SIRUKORTTI

Tietoturvallisuuden klassinen määritelmä koostuu kolmesta osa-alueesta: luottamuksellisuudesta, käytettävyydestä ja eheydestä. Luottamuksellisuus tarkoittaa sitä, että tietojärjestelmä tulee olla vain niiden henkilöiden käytössä, jotka ovat siihen oikeutettuja. Käytettävyydellä tarkoitetaan tiedon saatavuutta oikeassa muodossa ja oikeaan aikaan. Eheydellä taas tarkoitetaan sitä, että tietojärjestelmän tiedot ovat paikkansa pitäviä eikä joukossa ole virheellisiä tietoja. (Hakala, Vainio & Vuorinen 2006, 4.)

Tietojärjestelmän laajennettu käsite sisältää klassisen määritelmän lisäksi kiistämättömyyden ja pääsynvalvonnan. Kiistämättömyydellä pyritään varmistamaan, kuka tietojärjestelmää käyttää tai tallentaa sinne tietoja. Tällä tavalla pyritään varmistamaan, ettei tietojen luvatonta käyttöä tapahdu. Pääsynvalvonta taas tarkoittaa niitä menetelmiä, joilla rajataan käyttöoikeuksia. Näillä kaikilla eri osa-alueilla pyritään varmistamaan nimenomaan se, että tieto on oikeiden ihmisten käytettävissä ja samalla estämään tietojen luvaton käyttö. (Hakala ym. 2006, 5.)

Sirukortti pystyy vastaamaan tietoturvan erilaisiin haasteisiin ja se on turvallinen vaihtoehto, esimerkiksi yrityksille tietoverkkojensa suojaamiseen, koska se antaa monipuolisen suojauksen ja näin varmistaa, että käyttäjänä on oikea henkilö. Sirukortin avulla tietoturva pystytään takaamaan useiden erilaisten salausratkaisujen avulla. Salausratkaisuina toimivat niin kertakäyttöiseen salasanaan perustuvat ratkaisut eli OTP (One Time Password), PKI –pohjainen tunnistautuminen (Public Key Infrastructure), kortinlukijat että uusimpana biometrinen tunnistus. (Gemalto Oy 2006-2010e.)

4.1 Kertakäyttöinen salasana

Kertakäyttöinen salasana (OTP) takaa, että vanhoja tai kopioituja salasanoja ei pystytä käyttämään tunnustautumisessa toistamiseen. OTP:n avulla on mahdollista kirjautua tietojärjestelmään tai palvelimeen uniikilla salasanalla, jota voidaan käyttää vain kerran, kuten salauksen nimikin jo kertoo. Tällä tavalla estetään, että samaa käyttäjätunnus- ja salasanakombinaatiota ei voida käyttää toistamiseen.

OTP on niin sanottu vahva tunnistautumismenetelmä, joka takaa paremman turvan, esimerkiksi nettipankkiin tunnistauduttaessa. Vahva tunnistautuminen tarkoittaa nimenomaan sitä, että tunnistus perustuu vaihtuvaan salasanaan. (Gemalto Oy 2006-2012a.)

4.2 Julkisen avaimen infrastruktuuri PKI

Julkisen avaimen infrastruktuuri (PKI) on järjestelmä, jolla hallinnoidaan julkisia avaimia ja varmenteita. Julkisen avaimen salakirjoitusmetodiin tarvitaan kaksi avainta, jotka muodostavat avainparin. Ensimmäistä julkista avainta käytetään viestin salaukseen, tällöin viesti salataan henkilön yksityisellä avaimella. Toinen avain muodostetaan julkisesta avaimesta, jolloin viesti salataan vastaanottajan julkisella avaimella. (Viestintävirasto 2009.)

Tämän salausmenetelmän tärkein asia on luottamus. Kaksi keskenään tuntematonta henkilöä tarvitsevat kolmannen osapuolen, joka varmentaa osapuolten henkilöllisyyden. Varmentaja antaa varmenteen, jossa hän on tarkistanut sen, että salauksessa käytetty julkinen avain todella kuuluu oikealle vastaanottajalle. (Viestintävirasto 2009.)

4.3 Biometrinen salaus

Biometrinen salaus perustuu ihmisen fyysiseen ominaisuuteen kuten sormenjälkeen tai ääneen. Muihin salausmenetelmiin verrattuna biometrinen tunnistautuminen antaa todella hyvän suojan, koska se on vaikea varastaa tai kopioida, jolloin myös salauksen luotettavuus lisääntyy. Biometrisen tunnistautumisen lisäksi salauksessa voidaan käyttää myös muita salausmenetelmiä tuomaan lisäturvaa, kuten sirukortti ja salasana. (Gemalto Oy 2006-2012b.)

Sirukortin on tarkoitus olla hyvin suojattu metodi, joten kun lisänä käytetään biometristä tunnistautumista, saadaan suojaukselle entisestään lisävarmuutta. Biometrinen tunniste on mahdollista tallentaa suoraan sirukorttiin, jolloin sitä ei tallenneta mihinkään ulkoiseen tietokantaan, vaan se on jatkuvasti käyttäjänsä hallussa. Tällöin, esimerkiksi sormenjälkitunnistimen ja sirukortin varmennus toimii sau-

mattomasti, kun tunnistin vertaa jälkeä jo kortissa olevaan tietoon. (Gemalto Oy 2006-2012b.)

Biometrinen salaus on nousemassa uusimpana muiden salausratkaisujen rinnalle. Biometrinen salaus on ehdottoman yksilöllinen, koska jokaisella on erilainen sormenjälki. Tämä lisää entisestään varmuutta ja turvallisuutta. Nykypäivänä biometriseen tunnistukseen käytettäviä älykortteja on lähinnä erittäin korkeaa turvallisuutta vaativissa yrityksissä ja organisaatioissa. Varsinkin terrorismi on lisännyt turvallisuuden tarvetta ja biometrinen tunniste on ollut vastaus tuohon turvallisuuden tarpeeseen. (Hentilä 2002.)

Sirukortteja valmistava Miotec Oy on panostanut älykortteihin ja he uskovat biometrisen tunnistamisen kasvuun. Heidän tuotteissaan sormenjälkitunniste on sirukortin sisällä, eikä tietokoneella. Kynnys biometrisen tunnisteen käyttöön olisikin varmasti korkea, jos se tarkoittaisi sitä, että sormenjäljet kerättäisiin yhteiseen tietokantaan. (Hentilä 2002.)

4.4 Erilaiset sirukorttilaitteet ja – välineet

Smartjac on yksi johtavista sirukorttien ja sirukorttivälineiden jakelijoista Pohjois-Euroopassa ja Yhdysvalloissa. Smartjac tekee yhteistyötä Gemalton kanssa ja heidän kauttaan on mahdollista saada sirukorttiratkaisuja, esimerkiksi yrityksen kulunvalvontaan. Smartjac tarjoaa markkinoille Gemalton erilaisia laitteita ja kortteja, joilla voidaan rajata käyttöoikeuksia ja kulkuja, esimerkiksi yrityksissä. Smartjac tarjoaa markkinoille Gemalton .NET-sirukorttiratkaisuja sekä muita erilaisia sirukorttiratkaisuja yritysten käyttöön. (Smartjac 2012.)

Gemlaton .NET-sirukortti on edelläkävijä, koska se toimii Windows käyttöjärjestelmässä siten, että laitteen voi vain liittää koneeseen ja se toimii. Windows Vista käyttöjärjestelmässä Gemalton .NET-sirukorttiratkaisut ovat tuettuja, mutta vanhemmissa käyttöjärjestelmissä toiminnot saa helposti käyttöön lataamalla Windows Päivityksen kautta Microsoft's Base Smart Card Cryptographic Service Provider (CSP) paketin. (Smartjac 2012.)

Gemalton .NET-ratkaisujen etu on sirukorttiteknologian käyttöönotossa, koska toimivuus Windows ympäristössä vähentää kustannuksia ja käyttöönottovaikeuksia. Tämä sirukorttiratkaisu on hyvä tapa todentaa verkon käyttäjä tietokoneella. .NET-sirukortti on mahdollista yhdistää myös kulunvalvontaan, jolloin sirukortti voi toimia laajemmassa mittakaavassa yritysten ja oppilaitosten käytössä. (Smartjac 2012.)

Sirukortin käyttöä varten tarvitaan toki kortinlukijoitakin, jotka voivat olla ominaisuuksiltaan erilaisia. Sirukortinlukija voi olla kontaktilukija, joka siis toimii siten, että kortti asetetaan kortinlukijan sisään. Tällainen sirukortti on varmastikin kaikkein yleisin ja monelle tuttu kaupoista. Tällaisen lukijan etu on turvallisuus, koska tarvitaan kiinteä kontakti kortinlukijan ja kortin välillä, mutta etuna on myös sen nopeus. (CardLogix Corporation 2010b.)

Langattomasti toimiva sirukortinlukija toimii siten, että kortin ei tarvitse olla kiinteässä kontaktissa lukijaan. Tällainen lukija toimii radiotaajuudella ja kommunikoi kortin kanssa, kun se tulee riittävän lähelle kortinlukijaa. Tällaisia kortinlukijoita käytetään usein nimenomaan kulunvalvonnassa ja joukkoliikenteen tarkoituksissa. Tällainen kortinlukija on kätevä, koska välitöntä yhteyttä kortin ja lukijan välillä ei tarvita. (CardLogix Corporation 2010b.)

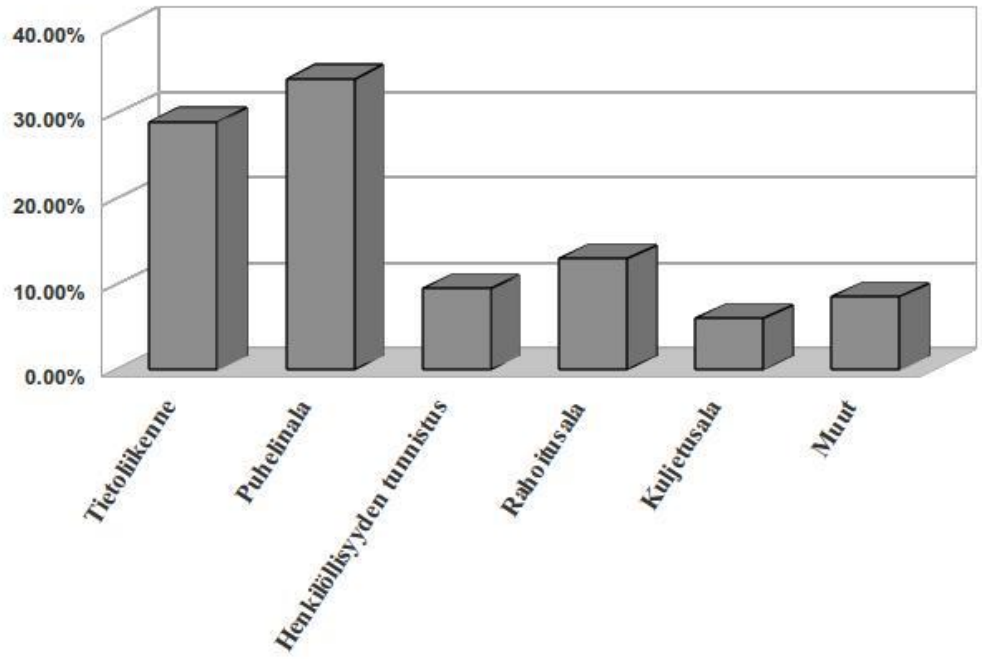
Erilaiset lukijat eritellään yleensä sillä perusteella, miten ne ovat liitännässä tietokoneeseen. Tällaisia liitäntöjä ovat muun muassa RS232 sarjaportti, USB-portit, levykepaikat ja näppäimistöjen erilaiset lukijat. Lisäksi joissakin korinlukijoissa voi olla useampia ominaisuuksia samassa laitteessa. (CardLogix Corporation 2010b.)

Smartjac tarjoaa useita erilaisia Gemalton-kortinlukijoita sekä kontaktittomia että kontaktillisia. Yhtenä esimerkkinä varsinkin USB-kortinlukija on hyvin helppokäyttöinen ja helposti siirreltävissä. Lisäksi tarjolla on pin-koodiin perustuvia lukijoita sekä kontaktittomia lukijoita. Kortinlukijoiden valikoima on hyvin laaja. (Smartjac 2012.)

Kaiken kaikkiaan Smartjacilla on hyvin laaja valikoima Gemalton tuotteita, joiden avulla he tarjoavat yritysten käyttöön heille räätälöityjä ratkaisuja näiden tuotteiden avulla. Varsinkin .NET -sirukortin käyttöönoton helppous on tämän ratkaisun suurin puolestapuhuja. Erilaisilla välineillä on mahdollista räätälöidä juuri oikeanlaiset toiminnot yrityksen tai oppilaitoksen tarpeisiin. Lisäksi sirukortti mahdollistaa biometrisen tunnisteen käytön ja sirukortti onkin turvallisen tapa säilyttää biometrinen tunniste, kun se on aina henkilön itsensä hallussa. (Smartjac 2012.)

5 SIRUKORTTI KÄYTÄNNÖSSÄ

Sirukorttia käytetään maailmalla erilaisiin käyttötarkoituksiin. Alla olevassa kuviossa 6 näkyy, miten sirukortin käyttö on jakautunut eri markkinasegmenteille. Sirukortin monipuolisuuteen vaikuttaa hyvin paljon sirukortin erilaiset lukumahdollisuudet ja tietoturva. Sirukorttia käytetään yritysmaailmassa, pankeissa, viranomaistahoilla, terveyden alalla, henkilöllisyyden tunnistamisessa ja joukkoliikenteessä.



Kuvio 6. Sirukortin markkinasegmentit. (Mayes & Markantonakis 2008, 14.)

5.1 Sirukortti henkilöllisyyden tunnistamisessa

Henkilöllisyyden tunnistaminen on sirukortin avulla hyvin varmaa ja sen takia sen koetaankin olevan kaikkein asianmukaisin tapa tunnistamiseen, koska se täyttää hyvin erilaiset turvallisuuden vaatimukset., esimerkiksi biometrisen tunnistautumisen avulla voidaan käyttää tunnistautumista, joka vaatii niin kortin kuin henkilön oman yksillöllisen ominaisuuden. Tällöin varmistetaan henkilöllisyys, lisätään turvallisuutta ja pystytään valvomaa paremmin. Monissa yrityksissä ja viran-

omaistahoilla henkilöllisyys varmistetaan sirukortin avulla. (Smart Card Alliance 1997-2011 b.)

5.2 Sirukortti yritysmaailmassa

Erilaiset organisaatiot ympäri maailman haluavat varmistaa, kenellä on pääsy heidän verkkojärjestelmäänsä. Useat yritykset siirtyvät käyttämään salausta, joka vaatii muutakin kuin yhden salasanan. Sirukortti antaa ratkaisun tähän ongelmaan, koska se antaa mahdollisuuden vahvaan tunnistautumiseen. Sirukortin avulla voidaan valvoa niin verkkojärjestelmään pääsyä kuin fyysistä pääsyä yrityksen tiloihin. Tällöin sirukortti ratkaisee molemmat yrityksen turvallisuuden riskitekijät. Muun muassa Boeing ja Microsoft käyttävät sirukorttia tässä tarkoituksessa. (Smart Card Alliance 1997-2011 c.)

5.3 Sirukortin käyttö oppilaitoksissa

Kuten yritysmaailmassa myös oppilaitoksissa sirukorttia käytetään samantapaisissa käyttötarkoituksissa. Sirukortin avulla voidaan valvoa henkilöiden kulkua ja mahdollisesti rajoittaa sitä. Lisäksi sirukortti käytetään tunnistautumisessa, mutta myös erilaisissa maksutarkoituksissa. Eastern Illinoisin, Robert Morrisin ja Arizonan yliopisto käyttävät erilaisia sirukorttitoimintoja. (Smart Card Alliance 1997-2011 c.)

Arizonan yliopistossa on käytössä sirukortti, jolla on monia ominaisuuksia. Sirukortti oikeuttaa alennuksiin esim. kirjakaupoissa ja terveydenhoidossa, lisäksi sirukorttia käytetään henkilöllisyyden todentamisessa ja kulunvalvonnassa. Sirukortti oikeuttaa myös erilaisiin etuihin kirjastoissa. Arizonan yliopistossa on tulossa myös sirukortin oikeuttamia palveluita joukkoliikenteeseen. (The University of Arizona 2010.)

Suomessa monissa kouluissa on ollut käsitteenä ”reissuvihko”, joka on toiminut oppilaiden vanhempien ja opettajien välisenä viestinnän välineenä. Monissa Suomen kouluissa on kuitenkin jo käytössä ”sähköinen reissuvihko” viestinnän välineenä. Vuonna 2005 on helsinkiläisessä peruskoulussa kokeiltu ”sähköisen reissuvihon” viestintää sirullisen henkilökortin avulla. Korttikirjautumisella oli tässä

kokeilussa pyritty nimenomaan lisäämään oppilaiden henkilökohtaisten tietojen turvaa sekä varmentamaan sitä, että vain tietyillä henkilöillä on oikeus nähdä tietoja. (Kotilainen 8.2.2005.)

5.4 Sirukortin käyttö terveydenhuollossa

Monissa terveyslaitoksissa tiedot ovat vielä paperimuodossa. Tarve uudelle teknologialle, jonka avulla voidaan tallettaa ja jakaa potilastietoja, on kuitenkin kasvamassa. Materiaalin tallettaminen elektroniseen muotoon lisää tietojen tarkkuutta, pienennetään kustannuksia ja pystytään antamaan hyvin reaaliaikaista terveydenhoitoa. (Gemalto Oy 2006-2012c.)

Terveydenhoidossa käsitellään hyvin paljon henkilöiden luottamuksellisia tietoja ja nuo tiedot kaipaavat jatkuvaa päivitystä. Sirukortin käyttöönotossa tärkeää olisikin, että potilastiedot on suojattu, mutta kuitenkin sellaisia, että terveydenhoidon ammattilaiset pääsevät niintä helposti katsomaan ja päivittämään. Sirukorttiin voitaisiin tallentaa tietoja henkilöiden veriryhmistä, allergioista, lääkkeistä ja potilashistoriasta. Akuuteissa tapauksissa tieto olisi tällä tavalla nopeasti lääkintähenkilökunnan tiedossa. (Gemalto Oy 2006-2012c.)

Sirukortin avulla potilaille voitaisiin tarjota oikea-aikaista hoitoa. Varsinkin akuuteissa tapauksissa kortin hyöty olisi merkittävä. Kortin hyöty olisi toki selkeä myös normaalilla lääkärikäynnillä. Tultaessa vastaanotolle kortti laitettaisiin lukijaan, josta lääkäri näkisi kaikki tarvittavat tiedot tutkiessaan sinua. Terveydenhuollosta poistuessa korttiin voitaisiin ladata reseptit, joilla voitaisiin apteekista hakea tarvittavat lääkkeet. Terveydenhoidon luottamukselliset potilastiedot asettavat haasteita, mutta nykyaikaisten salausmenetelmien avulla sirukortti voisi olla vastaus niihin. (Gemalto Oy 2006-2012c.)

5.5 Sirukorttiympäristön suunnittelu

Sirukortin käyttöönotto erilaisissa ympäristöissä vaatii aina paljon suunnittelua, jotta lopputulos on toivotunlainen. Tämän takia onkin hyvä piirtää suunnitelmasta kaavio. Tästä selviää tiedonkulku ja muutkin tarpeelliset tapahtumakohdat. Kortin

käyttöönoton suunnittelussa on tärkeää myös ottaa huomioon, onko kortin tehtävä sisältää informaatiota, arvoa tai valuuttaa. (CardLogix Corporation 2010c.)

Jos kyseessä on kortti, jonka tarkoitus on sisältää informaatiota ja mahdollisesti jotain arvoa tuottavia ominaisuuksia, on kortin toiminnan suunnittelu entistä vaativampaa. Suunnittelun apuna on hyvä käyttää alla olevassa taulukossa 2 olevia kysymyksiä, jotka koskevat: perussuunnittelua, turvallisuussuunnittelua, arvo-ominaisuuksien suunnittelua sekä yleisiä asioita. (CardLogix Corporation 2010c.)

Taulukko 2. Sirukorttiympäristön suunnittelukysymyksiä. (CardLogix Corporation 2010c.)

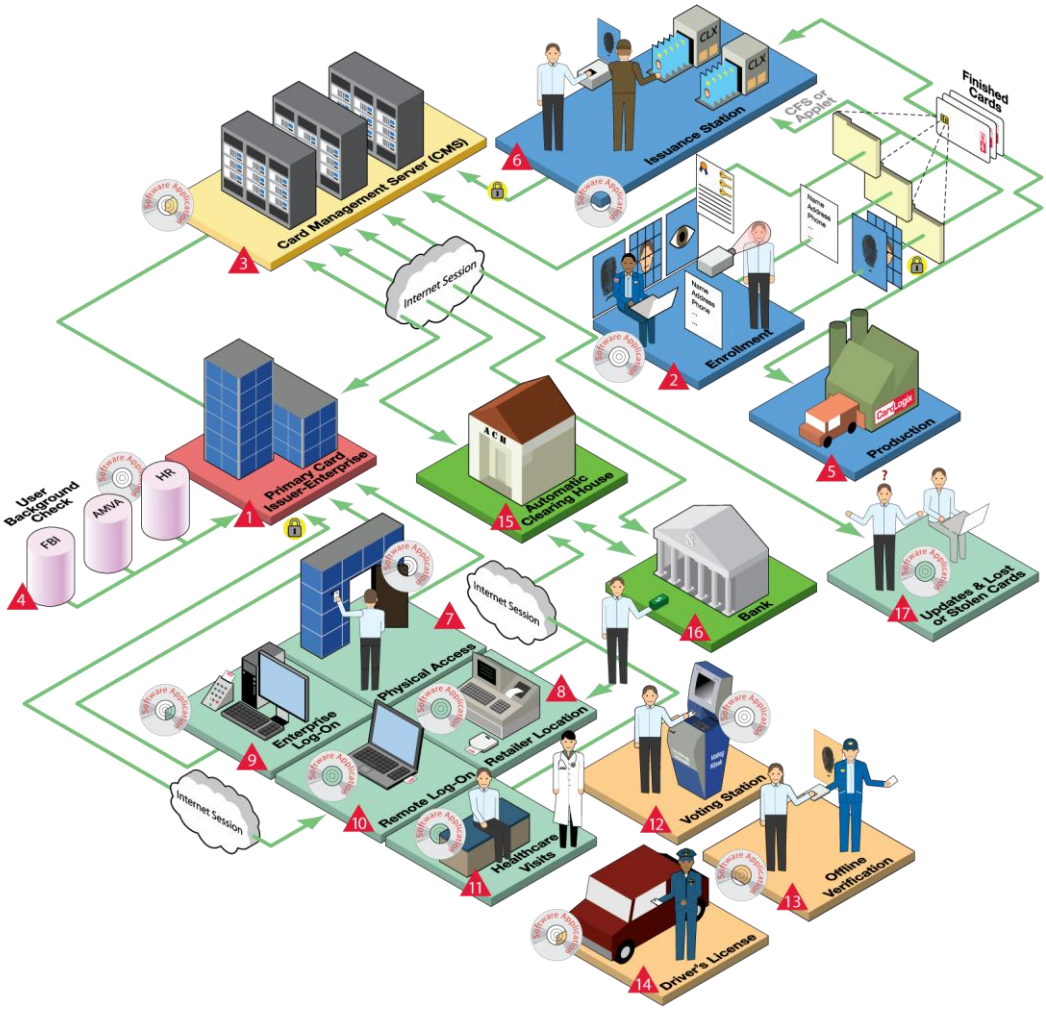
Perussuunnittelukysymyksiä:
1 . Onko olemassa selkeä kohderyhmä?
2. Onko suunniteltava yksi- vai monikäyttöinen sirukorttiympäristö?
3. Minkälaista informaatiota korttiiin ladataan?
4. Kuinka paljon muistia kukin ohjelma tarvitsee?
5. Jos kyseessä on monikäyttöinen sirukorttiympäristö, kuinka erityyppinen informaatio jaotellaan?
6. Saadanko kortin data erillisestä tietokannasta vai ladataanko se joka kerta?
Turvallisuussuunnittelu kysymyksiä:
1. Mitkä ovat turvallisuuden asettamat vaatimukset?
2. Pitääkö kaiken vai vain osan tiedosta olla turvattua?
3. Kenellä on pääsy tietoihin?
4. Kenellä on oikeus muuttaa tietoja?
5. Millä tavalla tieto suojataan?
Arvoon liittyviä kysymyksiä:
1. Onko kortin arvo kertakäyttöinen vai ladattava?

2. Kuinka kortit jaetaan?
3. Kuinka korttien arvo aktivoidaan?
4. Miten korttien käyttöä seurataan?
Yleisiä kysymyksiä:
1. Minkälaista kuvamateriaalia korttiin tarvitaan?
2. Kuka hoitaa materiaalin?
3. Mitä kaikkea tarvitaan korttia varten

Taulukossa 2 olevien kysymysten avulla päästään suunnittelussa eteenpäin ja otetaan huomioon suunnittelun eri osa-alueita. Suunnittelun lähtökohtana on tietenkin myös se, että saadaan käyttökelpoinen kaavio, jonka mukaan suunnitelmaa lähdetään toteuttamaan käytännössä.

Sirukorttiympäristön suunnitelma graafisessa muodossa voisi olla kuvion 7 näköinen, kun kyseessä on monikäyttökortti. Tällaisen ympäristön suunnittelu vaatii kuitenkin paljon suunnittelua ja etukäteistyötä, jotta se toimii varmasti myös käytännössä. Kuvio 7 voisi olla sirukortin käyttöympäristön suunnitelma suurelle yritykselle. Jokainen kohta, jossa kuviossa näkyy cd-levyn kuva on ohjelmisto, joka on yhteydessä sirukortin kanssa. Tässä kuvassa sirukortilla on siis monipuolisesti erilaisia käyttötarkoituksia, mikä tietysti vaikeuttaa suunnittelua, mutta toteutettuna on hyvä ratkaisu moneen ongelmaan. (CardLogix Corporation 2010c.)

Kuvio 7 on hyvin monipuolinen malli sirukortin käytöstä. Sirukorttia voi käyttää myös pienemmässä muodossa vastaamaan, esimerkiksi oppilaitosten tarpeisiin. Tällöin tarkoituksena olisi varmasti käyttää sirukorttia osittain samalla tavalla kuin nykyistä opiskelijakorttiakin, joten tällä kortilla saisi etuja, esimerkiksi kaupoissa, mutta sitä voitaisiin käyttää myös kulunvalvonnassa, läsnäoloseurannassa ja tietokoneiden etäkäytössä.



*Courtesy of and property of CardLogix Corporation. Permission granted for this use only.

Kuvio 7. Sirukorttiympäristö. (CardLogix Corporation 2010c. (katso liite 1.))

5.6 Sirukorttijärjestelmän käyttöönotto

Jotta sirukortti voitaisiin ottaa käyttöön oppilaitoksissa, pitää luoda pc-ympäristö joka tukee sirukortin käyttöä. Gemalton NET 2.0 Sirukortti voidaan ottaa käyttöön Windows ympäristössä, mikäli se tukee tiettyjä ominaisuuksia. Windows on varmasti yleisin käyttöjärjestelmä oppilaitoksissa ja yrityksissä, joten kortin toimivuus tällaisessa ympäristössä tukee sen käyttöönottoa.

Käytännössä sirukorttijärjestelmän käyttöönottoa varten tarvittaisiin seuraavia laitteita: serveri, Microsoft AD, MSCA asennus ja konfikurointi. Microsoft AD eli Active Directory voisi olla oppilaitoksen sisäverkossa oleva palvelin, joka varastoi opiskelijoiden ja henkilökunnan käyttäjätunnukset, henkilötiedot, oikeudet ja muuta tarvittavaa tietoa. (Tolvanen 2011.)

Active Directory (AD) on Microsoftin kehittämä sovellus, johon voidaan luoda esim. tietokanta verkon käyttäjistä. Active Direcotryn avulla voidaan luoda selkeä paikka, josta tietohallintoa ja turvallisuutta johdetaan. Tällöin pääservereillä voidaan tehdä muutoksia turvallisuusvaatimuksiin sekä ohjelmistojen päivityksiin. AD:n avulla esim. yrityksen verkkoa voidaan hallita useassa eri toimintapisteessä. AD:n toiminta perustuu siihen, että henkilön kirjautuessa verkkoon, se tarkistaa henkilön salasanan sekä sen millaiset oikeudet henkilöllä on verkkoon. Kirjautuessaan verkkoon sirukortilla, AD varmistaa käyttöoikeudet ja salasanan oikeellisuuden. (Wikipedia 2012.)

Ohjelmistoasennusten lisäksi käyttöönottoa varten tarvitaan myös muita laitteita. Olennaista on tietenkin se, että tietokoneissa on kortinlukijat, joiden avulla käyttäjä voi tunnistautua käyttöjärjestelmään. Kortinlukijoita voidaan tarvita myös oville, mikäli sillä halutaan seurata ja rajoittaa ihmisten kulkuja rakennuksissa. Kortinlukijoita tarvitaan niihin paikkoihin, joissa kortinluku on oleellista palvelun tai sisäänkirjautumisen kannalta. Tällaisia voivat siis olla lisäksi esim. ruokalat ja kirjastot. Tällöin myös näissä paikoissa henkilöllisyys ja oikeus palveluun pystytään todentamaan sirukortin avulla.

Organisaation tarpeiden perusteella yritykseen/oppilaitoikseen valitaan tarpeisiin sopivat kortit ja niihin sopivat kortinlukijat. Suomessa Gemalto ja Smartjac tarjoavat markkinoille sekä kontaktillisia että kontaktittomia vaihtoehtoja. Tällaisen järjestelmän ehdoton hyöty on sen luoma tietoturva sekä työajan tai läsnäolon seuranta. Tämä mahdollistaa myös organisaatioiden ja oppilaitosten omien verkkosivujen ja palvelinten käytön kotoa käsin.

6 SIRUKORTIN MAHDOLLISUUDET OPPILAITOKSISSA

Oppilaitoksien turvallisuuden tarve ja varsinkin tarve kulunvalvonnalle on kasvanut vuosien saatossa. Kouluammuskelut ovat osaltaan lisänneet tarvetta sille, että tarvitaan turvallisuussuunnitelmia. Sirukortti voi osaltaan luoda turvallisuutta kulunvalvonnan muodossa. Biometrisen tunnistautumisen lisääminen tähän yhtälöön takaa todella hyvän tunnistautumisen.

Sisäasiainministeriö on tehnyt julkaisun: ”Oppilaitosten turvallisuus” vuonna 2010. Tässä työryhmän raportissa kuvaillaan ohjeita ja suunnitelmia, joiden avulla voidaan varautua mahdollisiin turvallisuutta uhkaaviin tekijöihin. Suomessa olevat oppilaitokset jaetaan peruskouluun, toisen asteen koulutukseen ja korkeakouluihin sekä tietysti aikuiskoulutukseen. Jokainen näistä ryhmistä on omanlaisensa ja varsinkin opiskelijoiden ikä asettaa turvallisuudelle erilaisia tarpeita. (Sisäasiainministeriön julkaisuja 40/2009.) Tulen kuitenkin keskittymään enemmän korkeakoulutasoiseen turvallisuuden hallintaan sirukorttien avulla, koska uskon, että tällaisessa opiskeluympäristössä sirukortin käyttömahdollisuudet saadaan parhaiten käyttöön ja niiden hyödyt ovat varmasti suurimmat.

Oppilaitoksilla on useita laista tulevia velvoitteita suunnitella turvallisuusasioita. Eri lait poikkeavat toisistaan jonkun verran riippuen siitä, onko kysymys esim. pelastuslaista vai työturvallisuuslaista. Poikkeavuuksista huolimatta lakien määräämät asiat liittyvät toisiinsa ja sisältävät samoja asioita ja tavoitteena on luoda kokonaisvaltainen turvallinen opiskeluympäristö. (Sisäasiainministeriön julkaisuja 40/2009.)

Yksi tarpeellinen osa turvallisuuden huomioimisessa oppilaitoksessa on myös itse koulurakennuksen turvallisuus. Varsinkin korkeakouluissa opiskeluympäristö on hyvin avoin, jolloin opiskelijat voivat käyttää työhuoneita, -luokkia ja muita erilaisia tiloja hyvin joustavasti oman aikataulunsa mukaan. Tällainen oppimisympäristö tarjoaa opiskeluun monia hyviä puolia, mutta toisaalta sen seurauksena myös erilaiset riskit lisääntyvät. Tällaisen toiminnan varjopuolien takia kulunvalvonnan ja erilaisten turvajärjestelmien tarve on suuri. Sirukortti ja biometrinen tunnistus luovat varman tavan varmentaa, että vain oikealla henkilöllä on oikeus käyttää

tiettyjä tiloja. Varsinkin korkeakouluissa laitteet joissakin tiloissa ovat hyvin teknisiä ja kalliita, jolloin riskien minimointi on tärkeää. Sirukortin avulla voidaan varmentaa, että kukaan ulkopuolinen ei pääse tiloihin. (Sisäasiainministeriön julkaisuja 40/2009.)

Työryhmä ehdottaakin tekemässään yhteenvedossa, että koulurakennuksien turvallisuutta parannetaan palovaroitinjärjestelmillä, automaattisella paloilmoituksella, sprinklerijärjestelmällä, tallentavilla kameroilla sekä kulunvalvonnalla jokaisen koulun oman riskiarvioinnin mukaisesti. Myös Vaasan ammattikorkeakoulun sivuilla on erikseen sivusto turvallisuusohjeille. Turvallisuusohjeissa on linkkejä alkusammutustoimiin, evakuointiin, henkilökunnan toimintaan rikostilanteessa sekä vaarallisen henkilön kohtaamiseen. Lisäksi sivuilla on maininta pelastussuunnitelmasta sekä siitä, että turvallisuuden vuoksi oppilaitoksissa on tallentava kameravalvonta. (Vaasan ammattikorkeakoulu 2012; Sisäasiainministeriön julkaisuja 40/2009.)

Vaasan ammattikorkeakoulun läheisyydessä sijaitsee tutkimuskeskus Technobotnia, jossa ovat koulun opetukseen ja tutkimukseen käytettävät laboratoriot. Technobotnia on usean oppilaitoksen käytössä ja siellä sijaitsevat laitteet ja varusteet ovat arvokkaita. Varsinkin tällaisessa kiinteistössä kulunvalvonnan merkitys on tärkeä ja sen puuttuminen riskitekijä. Technobotniassa on tietyt aukioloajat, jolloin liikkuminen kiinteistössä on vapaata, vasta sulkemisaikojen jälkeen kiinteistössä liikkuvalla täytyy olla avainkortti. Tällä tavoin ei kuitenkaan voida mitenkään kontrolloida, kuka tiloja käyttää aukioloaikoina tai onko joku henkilö riskitekijä. (Technobotnia 2009.)

Vaihtoehto tällaisten tilojen suojaamiseen olisi juuri sirukortti ja biometrinen tunnistus. , esimerkiksi sormenjälkitunnistus on hyvin turvallinen vaihtoehto tunnistusmenetelmänä niin oppilaitokselle kuin opiskelijalle tai työntekijälle. Sirukortti mahdollistaa sen, että sormenjälkitietoja ei tarvitse tallentaa erilliseen tietokantaan vaan ne voidaan tallentaa suoraan sirukortille. Tällöin sormenjäljen hallinta on koko ajan opiskelijalla itsellään eikä ulkoisessa tietokannassa. Tällä tavalla voidaan varmistaa myös henkilöiden yksityisyyden suoja. Ovista pääsisi siis kulke-

maan vain sirukortin ja oman sormenjälkensä avulla. Tällöin saapuessaan rakennukseen henkilö luettaa ovella olevassa lukijassa sirukorttinsa ja asettaa sitten sormensa lukijaan. Lukija vertaa sitten, että sormenjälki täsmää sirukorttiin tallennettuun sormenjälkeen. (Turvaykköset 2012.)

Biometriseen tunnisteen, kuten sormenjäljen tunnistamiseen, on erilaisissa lukulaitteissa erilaisia sensoreita. Pääperiaate on, että sormi asetetaan lukijaan ja sormesta saadaan kuva. Kuvan avulla jäljelle saadaan numeerinen vastine algoritmin avulla. Tätä verrataan sitten tietokannassa olevaan tietoon tai vaikka sirukortilla olevaan tietoon. Sirukortin etu on nimenomaan henkilön identiteetin suoja. Tieto pysyy koko ajan henkilön itsensä hallussa. (Lukkari 2004.)

Sormenjälki voidaan tunnistaa seuraavien avulla: kapasitiivinen sensori, optinen sensori, terminen sensori, painesensori, RF-sensori ja ultraäänisensori. Kukin näistä tunnistusmenetelmistä toimii eri tavalla. Lisäksi sormenjälkitunnisteen luku voi tapahtua siten, että sormi pidetään lukijalla tietyn ajan tai siten, että sormea hipaistaan lukijaan. Hipaisuun perustuvat sormenjäljen lukijat ovat virhealttiimpia kuin lukijat, joissa sormi pidetään jonkin aikaa. (Boyd 1999-2012; 360 Biometrics 2011.)

Kapasitiiviset sensorit käyttävät hyväkseen ihon johtavuutta ja muodostavat sähköisen kuvan sormenjäljestä. Sormenjäljissä on erilaisia kohoumia ja matalia kohtia. Kohoumissa johtavuus on suurempi ja matalissa kohdissa pienempi. Tällä tavoin kapasitiivinen sensori reagoi sormen muotoihin. Ympäristön valaistus ei vaikuta tällaisen sensorin toimintaan, mutta sensorit voivat olla herkkiä sähköstaattisille purkauksille. (Boyd 1999-2012; 360 Biometrics 2011.)

Optisissa sensoreissa sormi valaistaan sopivalla tavalla, josta se sitten heijastuu lukijaan. Monissa optisissa sensoreissa käytetään LED-valoa, jonka avulla kontrastit sormen kohoumien ja matalien kohtien osalta näkyvät paremmin. Optisissa sensoreissa on kuitenkin myös ongelma-alueita. Optiset sensorit reagoivat herkemmin ympäristön valoon sekä naarmuihin lukijassa tai likaan sormessa. Optisten sensoreiden ongelma on myös se, että niitä on melko helppo huijata vakuutta-

valla kuvalla sormenjäljestä. Tällaisiin ongelmiin kuitenkin kehitetään ratkaisuja koko ajan. (Boyd 1999-2012; 360 Biometrics 2011.)

Termiset sensorit reagoivat sormen lämpötilaeroihin. Kohoumat koskettavat lukijaa, mutta matalat kohdat eivät. Tällöin sormen lämpötilaerojen avulla luodaan kuva sormenjäljestä. Tämän teknologian ongelmana on kuitenkin se, että sensorit eivät tunnista alle yhden Celsius asteen eroja lämpötilassa. Lisäksi sormen on oltava lukijassa riittävän kauan, jotta tunnistus todella toimii. (Boyd 1999-2012; 360 Biometrics 2011.)

Painesensori toimii siten, että kun sormi painetaan lukjiaan, lukijassa olevat pienet kytkimet sulkeutuvat, kun sormen kohoumat koskettavat sitä. Sormenjäljen matalat kohdat eivät aiheuta samanlaista reaktiota, joten sulkeutuneiden kytkimien luoma kuvio antaa mallin sormenjäljestä. (Boyd 1999-2012; 360 Biometrics 2011.)

RF-sensorissa sormeen lähetetään alhainen radiotaajuussignaali, joka sitten vastaanotetaan lukijassa. Tämä teknologia ei lue tietoa ihon pinnalta vaan ihon sisemmästä osasta. Tällöin sormien likaisuus tai esim. pieni haava sormessa ei vaikuta tunnistautumiseen. Viimeinen biometrisen tunnisteen sensorityyppi on ultraäänisensori. Ultraäänilukijan etuna on se, että se näkee ihon alle. Tällöin tunniste on entistäkin tarkempi, koska se perustuu suurempaan määrään tietoa. Ultraääniteknologian suurimpana ongelmana on sen hitaus ja kalleus. (Boyd 1999-2012; 360 Biometrics 2011.)

Jokaisessa lukijassa yksinään on omat hyvät puolensa ja omat huonot puolensa. Suurimmat huolenaiheet biometrisessä tunnistautumisessa liittyvät oman identiteetin turvaamiseen. Aiemmin biometristen lukijoiden huijaaminen oli helpompaa. Yritykset ovat kuitenkin luoneet lukijoita, jotka hyödyntävät useampia sensoreita, jotta voidaan turvallisemmin varmentaa ja todentaa käyttäjä. (Lukkari 2004.)

Nykyaikana biometrinen tunnistautuminen on siis hyvin varmaa sen takia, että yhdistellään erilaisia tekniikoita. Biometrisen tunnisteen ja sirukortin lisäksi on

mahdollista ottaa käyttöön vielä erillinen pin-koodikin. Tällöin salaus on erittäin varma.

7 SIRUKORTIN TULEVAISUUDENNÄKYMÄT

Sirukortti on jo nyt laajalti käytössä erilaisissa yhteisöissä ja organisaatioissa. Uskon kuitenkin, että myös tulevaisuudessa sirukortin käyttö laajenee entisestään. Ihmiset ja yrityksen haluavat vaivattomampia, mutta turvallisia toimintoja entistä enemmän. Sirukortti tarjoaa nämä mahdollisuudet.

Useissa korkeamman asteen koulutuslaitoksissa ulkomailla sirukortin hyöty osana yhteisöä on jo tunnistettu ja otettu laajalti käyttöön. Monipuoliset käyttömahdollisuudet helpottavat ihmisten elämää. Jotta sirukortti voi menestyä, sen pitääkin pystyä vastaamaan monipuolisesti ihmisten tarpeisiin, jolloin, esimerkiksi erilaisten yhdistelmäkorttien käyttö varmasti kiinnostaa monia. Nykyäänhän ihmiset kantavat mukanaan useita kortteja, mikä mahdollisuus olisikaan, jos nuo tiedot voitaisiin jotenkin integroida.

Sirukortin käyttö voi myös nopeuttaa, esimerkiksi toimintaa terveydenhuollossa, jos henkilöä koskevat tiedot on tallennettu hänen mukanaan olevalle sirukortille. Tällöin diagnoosin ja henkilön perusterveydenhuollosta huolehtiminen on helpompaa hoitohenkilökunnalle. Tämäkin kuitenkin on iso askel yhteiskunnalle, mutta varsin kehityskelpoinen ja mahdollinen sirukortin hyödyntämismahdollisuus tulevaisuudessa.

Kaikissa asioissa ihmisten tietojen turvassa pysyminen tulee esille. Turvallisuus on tärkeä osa nyky-yhteiskuntaa eikä sen merkitys jatkossakaan tule varmasti vähenemään. Erilaisten salausmenetelmien tärkeys korostuu entisestään. Uskonkin, että sirukortti ja biometrinen tunnistautuminen ovat tulevaisuuden mahdollisuuksia. Biometrisen tunnistautumisen hyväksyminen vaatii kuitenkin vielä yhteiskunnan hyväksyntää ja yleisiä standardeja asioihin. Eniten ihmisiä varmasti huolettaa omien henkilökohtaisten tietojen salassa pysyminen sekä mahdollisten biometristen tunnisteiden, kuten sormenjäljen käyttö, muihin kuin sirukortin vaatimiin asioihin hyödyntäminen.

Erilaisten sirukorttien ja –laitteiden jatkuvalla kehittämisellä kuitenkin varmasti pystytään tekemään paljon näiden asioiden hyväksi. Kaiken kaikkiaan sirukorttien

tulevaisuuden näkymät ovat mielestäni lupaavat ja paljon uutta tulee varmasti tulevaisuudessa. Uskon kuitenkin, että juuri biometrinen tunnistautuminen sirukortin kanssa on vastaus moneen turvallisuuskysymykseen ja tulevaisuuden ongelmiin.

8 YHTEENVETO

Nykyaikana tietoturvan ja turvallisuuden merkitys on kasvanut oppilaitoksissa kouluammuskelujen takia. Oppilaitosten pitää kuitenkin pystyä tarjoamaan opiskelijoilleen turvallinen oppimisympäristö. Sirukortti pystyy vastaamaan näihin lisääntyviin turvallisuuden vaatimuksiin.

Sirukortin parhaat puolet tulevat kuitenkin esille siinä, että sen käyttöä ei tarvitse rajoittaa vain kulunvalvonnan käyttötarkoituksiin. Sirukortti voi toimia myös uudenlaisena opiskelijakorttina, johon voidaan yhdistää kulkuoikeudet, kirjastokortti yms. Yhdellä kortilla pystyttäisiin siis vastaamaan useisiin tarpeisiin samanaikaisesti.

Riskinä sirukortin käytössä on tietenkin se, että se on vain tavallisen luottokortin näkoinen sirullinen kortti. Tällöin riski kortin katoamiseen ja siten myös oikeuksien siirtymiseen toiselle henkilölle on suuri. Tähänkin ongelmaan on erilaisia ratkaisuja. Sirukortti yhdistettynä vaikkapa pin-koodiin, antaa varsin vahvan suojauksen, vaikka kortti joutuisi vääriin käsiin, sen käyttöä varten tarvittaisiin koodi.

Biometrinen tunnistautuminen, joka siis perustuu johonkin henkilön yksilölliseen piirteeseen, kuten kasvoihin tai sormenjälkeen, on myös yksi suojaustapa sirukorttia käytettäessä. Tällöin esim. tiloissa kulkua varten täytyy kortinlukijaan näyttää niin sirua kuin sormenjälkeä. Biometrisen tunnistautumisen etuna on sen perustuminen ihmisen yksilölliseen ominaisuuteen. Mikäli sirukortti sattuisi katoamaan, on sen käyttäminen mahdotonta, koska esim. ovet eivät aukea ilman oikeaa sormenjälkeä.

Biometrisen tunnistautumisen merkittävin huolenaihe on ollut se, että joku pääsee käsiksi tallennettuihin tietoihin. Erillistä tietokantaa ei kuitenkaan tarvitse luoda, koska tunniste on mahdollista tallentaa sirukortille. Tällöin tunniste on koko ajan henkilöllä itsellään ja riski identiteettivarkauksiin pienenee merkittävästi. Kaiken lisäksi tunniste ei ole tallennettuna kuvana sirulle vaan matemaattisena algoritmina. Tunniste on siis suojattu todella hyvin, joten riski tunnisteiden katoamisesta tai joutumisesta vääriin käsiin on hyvin pieni. Sirukortin ja biometrisen tunnisteen

rinnalle on mahdollista ottaa vielä pin-koodikin, joten tietojen suojaaminen voidaan tehdä hyvin vakuuttavasti.

Biometrinen tunniste on mielestäni hyvin vahva tapa suojata kulkuja ja muitakin käyttöoikeuksia sirukortin kanssa. Merkittävin haaste tällaisen järjestelmän käyttöönotossa on siihen tehtävät investoinnit erilaisten kortinlukulaitteiden ja itse korttien muodossa. Uskon kuitenkin, että biometristen tunnisteiden käyttö lisääntyy ja yhteiskunnan asettamat rajat pakottavat myös oppilaitoksia siirtymään entistä varmempiin kulunvalvontoihin varsinkin korkeakouluissa, joissa oppimisympäristö on hyvin avoin ja kaikkien käytössä.

LÄHTEET

360 Biometrics 2011. FAQ - Fingerprint Scanner. Viitattu 27.4.2012. http://360biometrics.com/faq/fingerprint_scanners.php#1

Banco Santander 2011. University Card. Viitattu 1.2.2011. http://www.santander.com/csgs/Satellite?canal=CAccionistas&cid=1148977290746&empr=SANCorporativo&leng=en_GB&pagename=SANCorporativo/Page/SC_ContenedorGeneral

Boyd Karen 1999-2012. Fingerprint Reader Types. Viitattu 27.4.2012. http://www.ehow.com/list_6854736_fingerprint-reader-types.html

CardLogix Corporation 2010a. Types of Smart Card. Viitattu 23.2.2011. http://www.smartcardbasics.com/smart-card-types.html

CardLogix Corporation 2010b. Smart Card Readers & Terminals. Viitattu 9.10.2011. http://www.smartcardbasics.com/smart-card-reader.html

CardLogix Corporation 2010c. Smart Card Planning & Deployment. Viitattu 3.11.2011. http://www.smartcardbasics.com/smart-card-system-planning.html

Gemalto Oy 2006-2010a. Gemalto Oy - digitaalisen turvallisuuden ja turvapainoosaamisen asiantuntija. Viitattu 1.2.2011. http://www.gemalto.fi/index.php?id=7

Gemalto Oy 2006-2010b. Gemalto Oy - maailman johtava digitaalisen turvallisuuden kehittäjä. Viitattu 1.2.2011. http://www.gemalto.fi/index.php?id=49

Gemalto Oy 2006-2010c. Tytär- ja osakkuusyhtiöt. Viitattu 1.2.2011. http://www.gemalto.fi/index.php?id=8

Gemalto Oy 2006-2010d. Gemalto oy - turvapainon osaamista yli 120 vuotta. Viitattu 1.2.2011. http://www.gemalto.fi/index.php?id=37

Gemalto Oy 2006-2010e. Luotettavaa tunnistamista ja kulunvalvontaa. Viitattu 1.2.2011. http://www.gemalto.fi/index.php?id=43&L=0

Gemalto Oy 2008-2011. Gemalto .NET Smart Card Integration Guide. Viitattu 27.4.2012. http://www.gemalto.com/products/dotnet_card/resources/technical_doc.html?toggler=0

Gemalto Oy 2006-2012a. One Time Password. Viitattu 27.4.2012. http://www.gemalto.com/techno/otp/

Gemalto Oy 2006-2012b. Biometric Authentication. Viitattu 27.4.2102. http://www.gemalto.com/techno/biometric_authentication/

Gemalto Oy 2006-2012c. Taking care of patients' data. Viitattu 27.4.2012. http://www.gemalto.com/electronic_health_records/patient_records.html

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. 1.painos. Porvoo. WS Bookwell.

Hentilä, A. 2002. HighTech Forum: Älykorteille tulossa lisää markkinoita - sormenjälkitunniste parantaa turvallisuutta. Viitattu 24.8.2011. http://www.hightechforum.fi/index.cfm?j=238963

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2007. Tutki ja kirjoita. 13.painos. Helsinki. Tammi.

Kotilainen, S. 2005. Tietokone. Peruskouluun sähköinen reissuvihko sirukortilla. Viitattu 24.8.2011. http://www.tietokone.fi/uutiset/2005/peruskouluun_sahkoinen_reissuvihko_sirukortilla

Lerssi-Lahdenvesi, A. 2006. Sirukortti: Esitelmä digitaalisen viestintätekniikan seminaarissa 15.2.2006. Viitattu 27.4.2012. http://www2.it.lut.fi/kurssit/05-06/Ti5319200/Arja_Lerssi-Lahdenvesi.pdf

Lukkari, J. 2004. Sormenjälki haastaa avaimet ja kulkukortit. Tekniikka & Talous. Viitattu 27.4.2012. http://www.tekniikkatalous.fi/kemia/sormenjalki+haastaa+avaimet+ja+kulkukortit/a35583

Mayes, K., & Markantonakis, K. 2008. Smart Cards, Tokens, Security and Applications. New York. Springer Sciene+Business Media LLC.

Sisäasiainministeriön julkaisuja 40/2009. Oppilaitosten turvallisuus. Viitattu 27.4.2012. http://www.intermin.fi/intermin/biblio.nsf/6302A1CE9D552758C22576B0002390F2/$file/402009.pdf

Smart Card Alliance 1997-2011 a. Smart Card Primer. Viitattu 9.10.2011. http://www.smartcardalliance.org/pages/smart-cards-intro-primer

Smart Card Alliance 1997-2011 b. Identity Application Viitattu 9.10.2011. http://www.smartcardalliance.org/pages/smart-cards-applications-identity

Smart Card Alliance 1997-2011 c. Enterprise ID Applications. Viitattu 9.10.2011. http://www.smartcardalliance.org/pages/smart-cards-applications-enterprise-id

Smartjac 2012. Smartjac. Viitattu 8.5.2012. http://www.smartjac.se/

Technobotnia 2009. Viitattu 27.4.2012. http://www.technobothnia.fi/fi/

The University of Arizona 2010. CatCard Services. Viitattu 9.10.2011. http://www.catcard.arizona.edu/services

Tolvanen P. 2011. Käsitteet ojennukseen: Active Directory (AD), LDAP, SSO ja identiteetinhallinta. Viitattu 9.10.2011. http://viidestaso.wordpress.com/2011/04/29/kasitteet-ojennukseen-active-directory-ad-ldap-sso-ja-identiteetinhallinta/

Turvaykköset 2012. Biometrinen lukko aukeaa sormen painalluksella. Viitattu 27.4.2012. http://www.t1valpas.fi/biometrinentunnistusyrityksille

Vaasan ammattikorkeakoulu 2012. Turvallisuus- ja käyttäytymisohjeet. Viitattu 27.4.2012. http://www.puv.fi/fi/study/turvallisuus-ja_kayttaytymisohjeet/

Viestintävirasto 2009. Julkisen avaimen infrastruktuuri. Viitattu 27.4.2012. http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/pki.html

Wikipedia 2012. Active Directory. Viitattu 27.4.2012. http://en.wikipedia.org/wiki/Active_Directory

Wolfgang, R. & Wolfgang, E. 2003. Smart Card Handbook. 3.edition. Chichester. John Wiley & Sons Ltd.

Wolfgang, R. & Wolfgang, E. 2010. Smart Card Handbook. 4.edition. Chichester. John Wiley & Sons Ltd.

LIITTEET

LIITE 1. Lupa kuvion 7 käyttöön.

Gmail by Google

Tapani Karvonen <tapsa.karvonen@gmail.com>

re: New cardlogix.com visitor message: Permission to use pictures

1 viesti

Cathy Ross <cathy.ross@cardlogix.com> 14. toukokuuta 2012 22.55
Vastausosoite: cathy@cardlogix.com
Vast. ott.: tapsa.karvonen@gmail.com
Kopio: jeaschott <jeaschott@aol.com>

Thank you for your interest in our products. You may use the images if you caption them: "Courtesy of and property of CardLogix Corporation. Permission granted for this use only."

We would enjoy reading a copy of your thesis as well. Good luck to you.

Catherine Clemensen
CardLogix
www.cardlogix.com
+1-949-380-1312

From: tapsa.karvonen@gmail.com
Sent: Saturday, May 12, 2012 12:42 AM
To: marcom@cardlogix.com
Subject: New cardlogix.com visitor message: Permission to use pictures

Sent: Saturday, 05-12-2012, 12:33am

Name: Tapani Karvonen
Company: Student
Phone: 1234
E-mail: tapsa.karvonen@gmail.com

Message:
Hello,
I am doing my final thesis at the University of Applied Sciences in Vaasa Finland about the usability of smart card now and in the future. Can I have a permission to use the following pictures from the Internet page http://www.smartcardbasics.com/?
The first picture is about the types of smart cards found at the Internet page http://www.smartcardbasics.com/smart-card-types.html
The second picture is about system planning and the picture is found at the Internet page http://www.smartcardbasics.com/smart-card-system-planning.html
The source of the pictures will be mentioned in my work
Best Regards, Tapani Karvonen