LIIKENNE- JA VIESTINTÄMINISTERIÖN JULKAISUJA 80/2005
Viestintä

# Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja

Liikenne- ja viestintäministeriö
Helsinki, 2005

LIIKENNE- JA VIESTINTÄMINISTERIÖ

**KUVAILULEHTI**

Julkaisun päivämäärä
15.11.2005

| Tekijät (toimielimestä: toimielimen nimi, puheenjohtaja, sihteeri) | Julkaisun laji |
|---|---|
| VTT Elektroniikka, Oulu | Selvitys |
| Heikki Ailisto, Pasi Ahonen, Mikko Lindholm | Toimeksiantaja<br>Liikenne- ja viestintäministeriö |
| | Toimielimen asettamispäivämäärä |

Julkaisun nimi

Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja


Tiivistelmä

Suomen tietoturvastrategian yhtenä keskeisimmistä tavoitteista on rakentaa kansalaisten ja yritysten luottamusta tietoyhteiskuntaan. Biometria on tietoturvan ja luottamuksen alueella voimakkaassa kehitysvaiheessa oleva ilmiö. Palveluntarjoajat ja muut toimijat, jotka biometriaa hyödyntävät, tarvitsevat selkeätä ja helposti omaksuttavaa tietoa siitä, mitä tietoturvaan liittyviä seikkoja niiden tulisi ottaa huomioon biometriaa hyödyntävissä palveluissaan ja järjestelmissään. Tässä selvityksessä pyrittiin arvioimaan biometrisen tunnistamisen käyttöön liittyviä tietoturvakysymyksiä, keskeisimpiä riskejä ja ongelmia. Tietoturvakysymysten selvittämisellä ja analysoinnilla pyritään edistämään suomalaisten yritysten liiketoimintamahdollisuuksia ja biometrista tunnistamista hyödyntävää palvelukehitystä.

Keskeiset biometrisen järjestelmän teknisiä perusratkaisuja koskevat johtopäätökset voidaan tiivistää seuraavasti. Pelkkään biometriaan, esimerkiksi sormenjälkeen, perustuva tunnistaminen on suositeltavaa vain kohteissa ja palveluissa, joissa on kysymys hyvin pienestä taloudellisesta tai muusta arvosta, koska nykyisiä biometrisia tunnistusjärjestelmiä pystytään huijaamaan. Biometrian ja älykortin ja/tai salasanan yhdistelmä on ainoa suositeltava biometrisen tunnistamisen ratkaisu, jos kysymys on vähäistä suuremmista taloudellisista tai muista arvoista. Biometrisen tiedon säilyttäminen hajautetusti käyttäjien hallitsemalla välineellä, esimerkiksi älykorteilla, on useimmiten suositeltavaa verrattuna paikallisiin tai keskitettyihin tietokantoihin. Biometrinen tieto on salattava mahdollisimman varhaisessa vaiheessa käsittelyä, mieluiten laitteistopohjaisesti jo anturilla. Lisäksi on suositeltavaa, että tieto säilytetään eipalautettavassa muodossa (mallineena) eikä raakatietona.

Yleiset biometrian käyttöä koskevat periaatteet: lähtökohtana yksityisyyden suojan kunnioittaminen, suhteellisuus: etujen ja haittojen välinen hyväksyttävä suhde, biometriikan käyttö vain käyttäjän suostumuksella, biometrista tietoa koskevat henkilötietolain vaatimukset, yksityisyyden suojan kannalta herkkiä biometrisiä menetelmiä, joissa tunnistetiedosta voidaan tehdä päätelmiä henkilön sairauksista tai perimästä (erityisesti DNA) tulee välttää. Biometrisen tiedon suojaaminen ja/tai salaaminen.



Avainsanat (asiasanat)

Biometria, sähköinen tunnistaminen, biometrinen tunnistaminen, tietoturva, yksityisyyden suoja

Muut tiedot

Yhteyshenkilö/LVM Juha Perttula

| Sarjan nimi ja numero | ISSN | ISBN |
|---|---|---|
| Liikenne- ja viestintäministeriön julkaisuja 80/2005 | 1457-7488 (painotuote)<br>1795-4045 (verkkojulkaisu) | 952-201-458-3 (painotuote)<br>952-201-459-1 (verkkojulkaisu) |

| Kokonaissivumäärä | Kieli | Hinta | Luottamuksellisuus |
|---|---|---|---|
| 68 | suomi | 12 € | julkinen |

| Jakaja | Kustantaja |
|---|---|
| Edita Publishing Oy | Liikenne- ja viestintäministeriö |

KOMMUNIKATIONSMINISTERIET

**PRESENTATIONSBLAD**

Utgivningsdatum
15.11.2005

| Författare (uppgifter om organet: organets namn, ordförande, sekreterare) | Typ av publikation |
|---|---|
| VTT Elektroniikka, Oulu | Rapport |
| Heikki Ailisto, Pasi Ahonen, Mikko Lindholm | Uppdragsgivare<br>Kommunikationsministeriet |
| | Datum för tillsättandet av organet |

Publikation

Biometrisk identifierings informationssäkerhet och integritetsskydd


Referat

Ett av de centrala mål i Finlands dataskyddsstrategi är att skapa förtroende hos medborgare och företag för informationssamhället. Biometri är en viktig teknik för dataskydd och förtroende och den befinner sig i ett kraftigt utvecklingsskede. Tjänsteproducenter och andra grupper som utnyttjar biometrin behöver information som är tydlig och lätt att tillägna sig i sammanhang med frågor som måste iakttas i biometriska tjänster och system. I denna utredning uppskattades frågor i dataskydd, centrala risker och problem som berör användningen av biometrisk identifiering. Med hjälp av utredning och analys av dataskyddsfrågor strävas det efter att befrämja både möjligheter till affärsverksamhet för finska företag och utvecklingen av de tjänster som utnyttjar biometrisk identifiering.

De centrala slutledningarna som gäller tekniska grundlösningar i biometriska system kan sammanfattas på följande sätt: Identifiering med hjälp av bara biometrin, t. ex. fingeravtryck, är rekommenderad endast för de tjänster som är avsedda för att öka bekvämlighet för användarna eller som berör små ekonomiska värde. En kombination av biometrin och smartkort och/eller lösenord är den enda lösningen när det är fråga om större ekonomiska eller andra värde. Oftast är det bättre att lagra biometriskt data på ett decentraliserat sätt i användares eget datamedel än i lokala eller centraliserade databaser. Under databehandlingen i biometriskt system måste man dölja eller kryptera biometriskt data så tidigt som möjligt, gärna redan i biometrisk sensor.

De allmänna principerna rörande användningen av biometri: proportionalitet: en acceptabel proportion av fördelar och nackdelar, användares samtycke, kraven av Personuppgiftslag rörande biometriskt data, man måste undvika de biometriska metoder (speciellt DNA) som har direkt relevans för integritetsskydd och skyddande och/eller kryptering av data.



Nyckelord

biometri, elektronisk indentifiering, informationssäkerhet, integritetsskydd

Övriga uppgifter

Kontaktperson vid ministeriet är Juha Perttula

| Seriens namn och nummer | ISSN | ISBN |
|---|---|---|
| Kommunikationsministeriets publikationer 80/2005 | 1457-7488 (trycksak)<br>1795-4045 (nätpublikation) | 952-201-458-3 (trycksak)<br>952-201-459-1 (nätpublikation) |

| Sidoantal | Språk | Pris | Sekretessgrad |
|---|---|---|---|
| 68 | finska | 12 € | offentlig |

| Distribution | Förlag |
|---|---|
| Edita Publishing Ab | Kommunikationsministeriet |

MINISTRY OF TRANSPORT AND COMMUNICATIONS FINLAND

**DESCRIPTION**

Date of publication
15 November 2005

| Authors (from body; name, chairman and secretary of the body) | Type of publication |
|---|---|
| VTT Elektroniikka, Oulu | Report |
| Heikki Ailisto, Pasi Ahonen, Mikko Lindholm | Assigned by<br>Ministry of Transport and Communications |
| | Date when body appointed |

Name of the publication

Biometrics, data protection and privacy protection


Abstract

Building trust of citizens and companies is one of the key elements of the Finnish national ICT strategy. Biometrics is an important field from this point of view, especially since it is under going a tremendous development. In this situation, service providers and other enterprises need guidelines for the deployment of biometrics in a way which respects privacy and data protection. The purpose of this report is to identify, analyze and give guidelines for situations regarding data protection and privacy in biometric based applications.

The key conclusions regarding the basic technological structures of biometric based systems are as follows: solutions based solely on biometrics are recommended only for applications where the monetary or other risk involved is minimal. This is motivated by the threat of spoofing and the eventual consequences of identity theft. Combination of biometrics and smart card or some other token AND/OR password is recommended for all other identification applications. In most cases distributed storage of biometric data in users' tokens is preferable over local or centralized databases. The data should be encrypted as early as possible, preferably within the sensor hardware. Templates with non-reversible information content are better than storing raw biometric data.

General principles: basic guideline is respect to citizens right to privacy, proportionality: reasonable proportion between benefits and threats / disadvantages, user consent, the requirements and limitations set by Finnish Personal Data Act, sensitive methods, which contain information about user's genetic heredity or health condition, such as DNA should be avoided and protection of biometric data - either by encryption or other means of strong protection.



Keywords

biometrics, identification, verification, data protection, privacy protection

Miscellaneous

Contact person at the Ministry Mr Juha Perttula

| Serial name and number | ISSN | ISBN |
|---|---|---|
| Publications of the Ministry of Transport and Communications 80/2005 | 1457-7488 (printed version)<br>1795-4045 (electronic version) | 952-201-458-3 (printed version)<br>952-201-459-1 (electronic version) |

| Pages, total | Language | Price | Confidence status |
|---|---|---|---|
| 68 | Finnish | €12 | Public |

| Distributed by | Published by |
|---|---|
| Edita Publishing Ltd | Ministry of Transport and Communications |

# Esipuhe

Tämän selvityksen taustalla on Suomen hallituksen periaatepäätös kansallisesta tietoturvastrategiasta. Tietoturvastrategian yhtenä keskeisimmistä tavoitteista on rakentaa kansalaisten ja yritysten luottamusta tietoyhteiskuntaan. Selvitys liittyy Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja -hankkeeseen, joka on osa kansallisen tietoturvastrategian toimeenpanoa. Hanketta vetää Liikenne- ja viestintäministeriö (LVM). Hankkeen keskeisenä tavoitteena on lisätä luottamusta biometrian käyttöön myös kaupallisissa sovelluksissa ja palveluissa. Luottamus on välttämätön edellytys myös biometrisen tunnistamisen yleistymisen kannalta ja tietoturvasta huolehtiminen on keskeinen tekijä näitä menetelmiä koskevan luottamuksen rakentamisessa. Palveluntarjoajat ja muut toimijat, jotka biometriaa hyödyntävät tarvitsevat selkeätä ja helposti omaksuttavaa tietoa siitä, mitä tietoturvaan liittyviä seikkoja niiden tulisi ottaa huomioon biometriaa hyödyntävissä palveluissaan ja järjestelmissään.

Tietoturvakysymysten selvittämisellä ja analysoinnilla pyritään edistämään suomalaisten yritysten liiketoimintamahdollisuuksia ja biometrista tunnistamista hyödyntävää palvelukehitystä. Hankkeen toteuttamisella pyritään omalta osaltaan vaikuttamaan myös siihen, että biometrisessa tunnistamisessa otetaan Suomessa huomioon perustuslain turvaamat tietoturvaan ja yksityisyyden suojaan liittyvät oikeudet ja varmistetaan biometriaan liittyvien tietoturvariskien riittävä hallinta.

Selvitys toteutettiin huhtikuun ja elokuun 2005 välisenä aikana. Selvityksen tekijät ovat erikoistutkija, FL Pasi Ahonen, tutkimusprofessori, TkT Heikki Ailisto ja tutkija, TkL Mikko Lindholm VTT Elektroniikasta Oulusta. Heikki Ailiston ja Mikko Lindholmin asiantuntemus on biometrian alalta ja Pasi Ahosen tietoturvan alalta. Selvitystyön vastuuhenkilö VTT Elektroniikassa oli Heikki Ailisto. Raporttia kommentoi sen kirjoittamisen eri vaiheissa LVM:n koollekutsuma biometrisen tunnistamisen tietoturvallisuus ja yksityisyydensuoja -työryhmä, johon kuuluvat Kaarlo Karvonen (Finnair Oyj), Lauri Karppinen (Tietosuojavaltuutetun toimisto), Tuomas Kivinen (Nordea Pankki Suomi Oyj), Tommi Rakshit (sisäasiainministeriö), Ari Saapunki (Aldata Solution Finland Oy), Helvi Salminen (Setec Oy) sekä hankkeen alkuvaiheessa Tuire Saaripuu (Väestörekisterikeskus) ja myöhemmässä vaiheessa Päivi Pösö (Väestörekisterikeskus). Työryhmän puheenjohtajana toimii neuvotteleva virkamies Juha Perttula (liikenne- ja viestintäministeriö).

Liikenne- ja viestintäministeriö haluaa kiittää selvityksen tekijöitä poikkeuksellisen korkeatasoisesta työstä ja työryhmän jäseniä tärkeästä panoksesta hankkeen toteuttamiseen.

*Helsingissä 10 päivänä marraskuuta 2005*

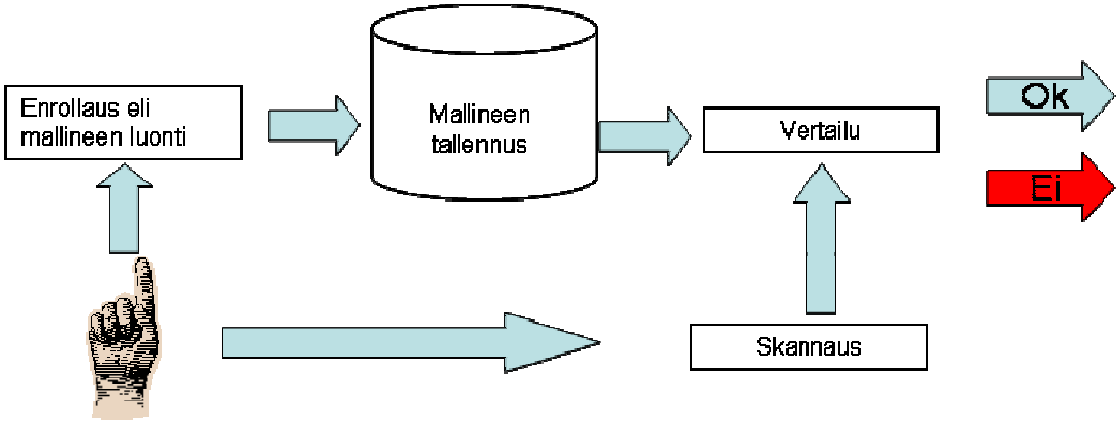
*Juha Perttula*

## SISÄLLYSLUETTELO

# 1 Johdanto

## *1.1 Tausta*

Biometrisella tunnistuksella tarkoitetaan henkilön automaattista tunnistamista jonkin fysiologisen ominaisuuden, kuten sormenjäljen tai käyttäytymispiirteen, kuten kävelytyylin, avulla. Tieteellisen biometrisen tunnistamisen taustalla ovat 1800-luvulla kehittyneet rikostutkinnan menetelmät: antropometria ja sormenjälkien luokittelu. Varsinaisesti nykymuotoinen biometria syntyi 1960-luvulla. Biometrisen tunnistamisen menetelmät, anturit ja ohjelmistot kehittyivät voimakkaasti 1990-luvulla ja jonkin aikaa on ollut kaupallisesti saatavilla kohtuuhintaisia ja toimivia laitteita ja järjestelmiä biometrista tunnistusta varten. Kuva 1 on esitetty biometrisen tunnistusjärjestelmän toimintaperiaate.




**Kuva 1** Biometrisen tunnistusjärjestelmän toimintaperiaate

Tällä hetkellä päähuomio kiinnittyy biometristen tekniikoiden viranomaissovelluksiin. Syynä tähän on New Yorkin terrori-iskujen seurauksena voimakkaasti kasvanut huomio turvallisuusasioihin, kuten esimerkiksi maahantulotarkastuksiin. Yhdysvallat ja Euroopan Unioni ovat asettaneet tavoitteeksi biometrisen elementin sisällyttämisen matkustusasiakirjoihin, kuten passeihin ja viisumeihin. Yhdysvallat vaatii vuoden 2005 lokakuun[1] jälkeen myönnettyihin passeihin ICAO:n suosituksen mukaisen biometrisen tunnisteen (digitaalinen kasvokuva), joka on luettavissa kosketuksettomasti passin mikrosirulta. EU on päättänyt vaatia työntekijöiltä, jotka tulevat maista, joilla ei ole viisumivapaussopimusta EU:n kanssa, viisumia, jossa on biometrinen tunniste. Malesiassa henkilökorteissa on jo pitempään ollut sormenjälkitunniste. Nigeriassa, jossa on 60 miljoonaa asukasta, on toteutettu aikuisväestön rekisteröinti vaaliluetteloita ja väestörekisteröintiä varten tallentamalla henkilötietojen lisäksi myös digitoitu sormenjälki. Britannia aikoo ottaa biometristä tunnistetietoa sisältävän henkilökortin käyttöön vuonna 2008. Esimerkit osoittavat biometrisen tunnistamisen etenevän nopeasti viranomaissovelluksissa.

Kaupallisissa ja yksityisissä sovelluksissa tapahtunut biometrisen tunnistamisen yleistyminen on toistaiseksi jäänyt osittain viranomaissovellusten varjoon, vaikka siinäkin kentässä on tapahtunut merkittävää kehitystä. Esimerkkejä kaupallisista asiakaspalveluun liittyvistä sovelluksista ovat

[1] EU on pyytänyt lykkäystä takarajalle teknisten ongelmien vuoksi. Määräaikaa on lykätty.

- allekirjoituksen automaattinen tunnistus, Nationwide Building Society, UK 2002
- myyntipisteissä (Point of sale, POS) oleva käyttäjän tunnistus sormenjäljellä, useita kokeiluja, mm. Englanti ja TeleTrustT, Saksa 2004
- pankkiautomaattisovellukset, joissa iiristunnistus, USA, Englanti
- kuntosalin ja tanssipaikan asiakkaiden tunnistus, Suomi, 2004 ja Englanti 2004
- kasinot, yökerhot, ei-toivottujen henkilöiden poisto, kokeiluja USA ja UK

Esimerkkejä yrityksen työntekijöiden käyttämistä sovelluksista

- kulunvalvonnan ja työaikaseurannan varmistus esimerkiksi sormenjäljellä, useita sovelluksia, mm. Deltabit, Suomi, 2004
- tietoverkon työasemaan sisään kirjoittautuvan henkilöllisyyden varmistus
- lentohenkilökunnan henkilöllisyyden tarkastus, useita kokeiluja esimerkiksi Finnair, Suomi 2004-2005

## *1.2 Markkinoiden kehitys*

Biometrisen tunnistuksen markkinat ovat kasvaneet voimakkaasti ja saman kehityssuunnan uskotaan jatkuvan. International Biometrics Group (IBG) arvioi biometria-alan liikevaihdon kasvavan vuoden 2003 719 miljoonasta dollarista yli kuusinkertaiseksi viidessä vuodessa, mikä vastaa noin 45% vuosittaista kumulatiivista kasvua. Taulukossa 1 on IBG:n arvio alan liikevaihdosta vuodelta 2004.

Taulukko 1. Biometria-alan liikevaihto

| Biometria-alan liikevaihto 2003 - 2008 (miljoonaa US dollaria) | | | | | |
|---|---|---|---|---|---|
| 2003 | 2004 | 2005 | 2006 | 2007 | 2008 |
| 719 | 1201 | 1347 | 2684 | 3682 | 4639 |

Teknologioista sormenjälki on edelleen hallitseva. Taulukossa 2 on esitetty IBG:n arvio eri teknologioiden markkinaosuuksista vuonna 2004

Taulukko 2. Eri biometristen teknologioiden osuudet

| Teknologioiden osuudet 2004 (poislukien rikostutkinta) | | | | | | |
|---|---|---|---|---|---|---|
| Sormenjälki | Kasvotunnistus | Kämmen | Iiris | Ääni | Muu | Middleware |
| 48% | 12% | 11% | 9% | 6% | 2% | 12% |

Teknologiat, sovellukset ja asiakassektorit voidaan karkeasti luokitella Taulukon 3 tapaan (lähde IBG). Taulukko tulee käsittää esimerkinomaiseksi, ja eräät siinä esitetyt arviot, esimerkiksi iiristunnistuksen liittäminen toisaalta sähköiseen etätunnistukseen ja toisaalta lainvalvontaan tuntuu vielä nykytekniikalla kyseenalaiselta.

Taulukko 3. Teknologiat, sovellukset ja asiakassektorit

| Teknologia | Sovellus | Sektori |
|---|---|---|
| Sormenjälki | Kansalaisten ja maahantulijoiden tunnistus | Viranomais |
| Kasvot | Valvonta ja epäiltyjen haravointi | Matkustus |

| | | |
|---|---|---|
| Kämmen | Työasemat ja verkot | Rahoitus |
| Iris | Sähköinen kauppa ja etätunnistus (puhelin) | Lainvalvonta |
| Ääni | Pääsyn ja läsnäolon valvonta | E-ja M-kauppa |
| Allekirjoitus | Väärennösten tunnistus | Rahoitus, kauppa |
| Multimodaalinen | Korkea turvallisuus / huijauksen esto | - |

## *1.3 Selvityksen tavoite*

Tämän selvityksen taustalla on Suomen hallituksen periaatepäätös kansallisesta tietoturvastrategiasta. Tietoturvastrategian yhtenä keskeisimmistä tavoitteista on rakentaa kansalaisten ja yritysten luottamusta tietoyhteiskuntaan. Selvitys liittyy Biometrisen tunnistamisen tietoturvallisuus ja yksityisyyden suoja -hankkeeseen, joka on osa kansallisen tietoturvastrategian toimeenpanoa. Hanketta vetää Liikenne- ja viestintäministeriö (LVM). Hankkeen keskeisenä tavoitteena on lisätä luottamusta biometrian käyttöön myös kaupallisissa sovelluksissa ja palveluissa. Luottamus on välttämätön edellytys myös biometrisen tunnistamisen yleistymisen kannalta ja tietoturvasta huolehtiminen on keskeinen tekijä näitä menetelmiä koskevan luottamuksen rakentamisessa. Palveluntarjoajat ja muut toimijat, jotka biometriaa hyödyntävät tarvitsevat selkeätä ja helposti omaksuttavaa tietoa siitä, mitä tietoturvaan liittyviä seikkoja niiden tulisi ottaa huomioon biometriaa hyödyntävissä palveluissaan ja järjestelmissään.

Luottamuksen edistämiseksi hankkeessa pyritään arvioimaan biometrisen tunnistamisen käyttöön liittyviä tietoturvakysymyksiä, keskeisimpiä riskejä ja ongelmia. Tietoturvakysymysten selvittämisellä ja analysoinnilla pyritään edistämään suomalaisten yritysten liiketoimintamahdollisuuksia ja biometrista tunnistamista hyödyntävää palvelukehitystä.

Hankkeen toteuttamisella pyritään omalta osaltaan vaikuttamaan myös siihen, että biometrisessa tunnistamisessa otetaan Suomessa huomioon perustuslain turvaamat tietoturvaan ja yksityisyyden suojaan liittyvät oikeudet ja varmistetaan biometriaan liittyvien tietoturvariskien riittävä hallinta. Suomessa biometrisen tiedon luonteeseen henkilötietona, esim. tavallisena tai arkaluonteisena, ei ole vielä otettu virallista kantaa[2] ja siitä ei ole säädetty nimenomaisesti lainsäädännössä. Onkin syytä lähteä ajatuksesta, että (biometriselle) tiedolle tarvittava tiedon turvataso määräytyy tiedon luonteen mukaan.

Myös kansalaiset kokevat biometrisen tiedon yksityisyyden suojan kannalta haastavammaksi kuin tavallisen henkilötiedon ja siksi nähdään, että tietoturvasta huolehtiminen on keino varmistaa yksityisyyden suojan toteutuminen. Alan toimijoiden, kuten yritysten, kannalta tietoturvasta ja yksityisyydestä huolehtiminen on heidän etujensa mukaista, koska se luo luottamusta palveluihin. Kääntäen: yksityisyyden suojan mahdolliset ongelmat voivat viedä luottamuksen palveluihin varsinkin alkuvaiheessa pahastikin.

[2] Ranskassa asiaan on suhtauduttu tiukemmin ja sikäläinen tietosuojaviranomainen on suhteellisuusperiaatteeseen vedoten pitänyt biometriaa muihin tunnistusmenetelmiin verrattuna yksityisyyttä loukkaavampana.

## *1.4 Biometrian tunnetut uhkakuvat*

Biometriseen tunnistukseen liitetään julkisessa keskustelussa eräitä uhkakuvia, jotka otetaan huomioon tässä selvityksessä. Selvitys ei kuitenkaan rajoitu pelkästään niihin. Julkisessa keskustelussa esitetyistä uhkakuvista tunnetuimmat ovat yhteiskunnan valvonnan ja seurannan kohtuuton lisääntyminen (Big Brother -ilmiö), identiteettivarkaudet sekä biometrian huijaaminen (Taulukko 4**)**

Taulukko 4. Biometriaan liitetyt uhkakuvat

| Uhkakuva | Selite tai esimerkki |
|---|---|
| Vallan keskittyminen | "Tieto on valtaa", esim. Viranomaiset tai yritystahot saavat kohtuuttomasti valtaa keräytyvän tiedon ja yhdistelyn kautta |
| Kerätyn tiedon käyttö muuhun tarkoitukseen | Esimerkiksi bio-passikuvatietojen käyttö katu- tai liikennevalvonnassa |
| Biometrisen tiedon vuotaminen | Vrt. Luottokorttinumeroiden vuotaminen internettiin, =>uhka esim. Sormenjälkitietojen kohdalla laittomien kopioiden valmistus ja rikollinen käyttö |
| Biometrisen tiedon luvaton myynti | Sama kuin yllä |
| Ihmisen arvon ja yksityisyyden kunnioituksen rapautuminen | Kuluttaja voi antaa biometrisen tunnisteen vähäistä taloudellista etua, esimerkiksi pientä alennusta tai lahjaa, vastaan harkitsematta seurauksia |
| Identiteettivarkaus | Varkaus voi tapahtua enrollauksessa, ts. henkilö A esiintyy henkilönä B ja "syrjäyttää" hänen identiteettinsä TAI henkilö A kopioi henkilön B tunnisteen, esimerkiksi sormenjäljen, väärentää sen ja käyttää sitä |
| Identiteettihuijaus | Kuten yllä, mutta henkilö B osallistuu huijaukseen |
| Syrjäytyminen | Henkilöt, jotka eivät voi, osaa tai halua käyttää biometrisia tunnisteita esimerkiksi fyysisen vamman, oppimiskyvyn puutteiden, uskonnollisen tai muun vakaumuksen takia ovat vaarassa jäädä joidenkin palvelujen, etujen tai alennusten ulkopuolelle |
| Liiallinen luottamus | Biometrista tunnistusta käyttävä yritys, viranomainen tai niiden työntekijät tai suuri yleisö luottaa sokeasti biometriseen tunnistukseen, ts. sen oletetaan olevan 100% varma. |
| "Biometrian spam" | Biometrista tunnistusta tarjotaan käytettäväksi hyvin monissa kohteissa, joissa tunnistamistarve ei ole perusteltavissa olevassa suhteessa käytettyyn menettelyyn. Voi johtaa kasvaneeseen identiteettivarkauden riskiin, koska monet henkilöt ja tahot pääsevät käsiksi biometriseen tietoon. |

### 1.4.1 Identiteettivarkaus -uhkakuva

Taulukossa (Taulukko 4) esitetyistä uhkakuvista **identiteettivarkaus koetaan yleensä vaarallisimmaksi** ja muutamat muut kuten biometrisen tiedon vuotaminen ja biometrisen tiedon luvaton myynti liittyvät siihen. Identiteettivarkautta, sen seurauksia ja torjumista tarkastellaan seuraavassa tarkemmin.

Taulukko 5. Identiteettivarkaus, seuraukset ja torjunta

| Järjestelmän luonne | Seuraus uhrin kannalta | Torjuntakeinot ja niiden luotettavuus |
|---|---|---|
| Pelkkä biometrinen tunniste | Käytetty biometria menettää käyttökelpoisuutensa järjestelmässä. | 1) Biometrisen tunnisteen "mitätöinti" pysyvästi. Luotettava, mutta ei tyydyttävä keino.<br>2) Aitouden (liveness) varmistus anturissa. Ei koskaan täysin luotettava, asiantuntijan huijattavissa. Olemassa olevan laitekannan ongelma.[3] |
| Biometrinen tunniste ja kortti tms. tunniste. | Uhka, jos kortti varastetaan yhtä aikaa biometrian kanssa. | Kortin mitätöinti. Luotettavuus kortin turvatason mukaan, yleensä hyvä. |
| Biometrinen tunniste ja PIN tai tunnussana | Uhka, jos PIN myös luvattoman käyttäjän tiedossa. | PINin vaihto. |
| Biometrinen tunniste ja keskusrekisteri | Käytetty biometria menettää käyttökelpoisuutensa järjestelmässä. | 1) Biometrisen tunnisteen "mitätöinti" pysyvästi. Luotettava mutta ei tyydyttävä keino.<br>2) Aitouden (liveness) varmistus anturissa. Ei täysin luotettava, asiantuntijan huijattavissa. |
| Useita biometrisia tunnisteita ja keskusrekisteri (esim. sormenjälki ja kasvokuva kuten passissa voi tulevaisuudessa olla). | Haittavaikutus ei niin suuri kuin yllä. | Ihmisen tekemä tunnistus varmistaa (käytännössä kasvot). |

Tarkastelu (ks. Taulukko 5) osoittaa, että pelkkää biometriaa käyttävä järjestelmä on hyvin haavoittuva identiteettivarkauksien suhteen. Varsinkin, jos useat toisistaan riippumattomat järjestelmät, esimerkiksi bussit, kahvilat, kaupat ja kirjastot käyttävät samaa biometriaa, sen menettäminen identiteettivarkaalle olisi yksilön kannalta todella haitallista: joko hän mitätöi biometrisen tunnisteensa kaikissa näissä järjestelmissä ja sulkee siten itsensä (osittain) niiden ulkopuolelle tai hän ottaa riskin, että identiteetin varastanut taho voi milloin tahansa tunnistautua häneksi. Selvästikin pelkkään biometriaan perustuva tunnistaminen on sopiva vain tarkoituksiin, joissa sekä yksilön että palvelun tarjoajan kannalta väärinkäyttöön liittyvä riski on pieni. Tällaisia sovelluksia voi ajatella olevan mukavuutta lisäävät sovellukset, kuten laitteiden

[3] Aitouden varmistus ja huijauskeinot käyvät kilpajuoksua, jota voi verrata virusten ja virustorjuntaohjelmien vastaavaan. Koska aitouden (aliveness) tunnistus on paljolti laitteistopohjaista, ei päivitys ole läheskään niin helppoa kuin virustorjunnan kohdalla. Vanha laitekanta on altista uusille huijauskeinoille.

personointi: auton istuimen säädöt, kodin viihde-elektroniikan tai kuntoilulaitteiden esiasetukset jne.

Yksilön ja palvelun tarjoajien kannalta turvallisempi vaihtoehto on se, että biometrinen tunnistaminen liittyy aina älykortin, avaimen tai muun vastaavan fyysisen tunnisteen tai salasanan käyttöön. Tällöin identiteettivarkaus yksin ei aiheuta luvattoman käytön vaaraa, jos kortti tai salasana ei joudu varkaan haltuun. Vaikka näin tapahtuisi, ongelma voidaan ratkaista kortti tai salasana vaihtamalla. Toisaalta järjestelmä on turvallisempi kuin pelkkä kortti tai salasana, koska niiden varastaminen yksin ei aiheuta uhkaa ilman biometrista tunnistetta.

Suurin turvallisuustaso saavutetaan luonnollisesti yhdistämällä biometria, kortti ja salasana [4]. (What you are, what you have and what you know).

[4] Tällöin voidaan jopa ajatella, että turvataso on liian hyvä, sillä häikäilemätön rikollinen voi kaapata henkilön kortteineen saadakseen haltuunsa suojatun kohteen, esimerkiksi pankkitilin tai auton.

# 2 Biometristen sovellusten luokittelu ja käyttöesimerkit

## 2.1 Luokittelu käyttötavan mukaan

Biometrisen henkilöntunnistamisen sovellukset voidaan luokitella karkeasti kahteen pääryhmään: verifiointiin (*verification, one-to-one*) ja identifiointiin (*identification, one-to-many*). Tätä jakoa voidaan tarkentaa esimerkiksi seuraavasti (LVM:n tarjouspyyntö):

Taulukko 6. Sovellusten luokittelu.

| | Tyyppi | Esimerkki |
|---|---|---|
| 2.1 | Pääsynvalvonta (1:1). | Yrityksen sisäinen kulunvalvontajärjestelmä |
| 2.2 | Tunnistaminen verkkopalvelussa (1:1). | Verkkokaupan asiakkaiden tunnistamismenetelmä |
| 2.3 | Henkilökohtainen sovellus (1:1). | Yhden käyttäjän oma biometrisen tunnistamisen hyödyntäminen |
| 2.4 | Pienen käyttäjäpiirin sovellus (1:few). | Perheen sisäinen tunnistamisjärjestelmä esim. sormenjälki ulko-ovella avaimen korvikkeena |
| 2.5 | Tietojärjestelmän pääsynvalvonta (1:1). | Esim. yrityksen tietojärjestelmän salasanojen korvaaminen |
| 2.6 | Aktiivinen identifiointi (1:many). | Kauppakeskuksen ovella tunnistaminen esim. sormenjäljen perusteella |
| 2.7 | Passiivinen identifiointi (1:many). | Kasvotunnistukseen perustuva tietylle alueelle saapuvien tai tietyllä alueella liikkuvien henkilöiden tunnistaminen |
| 2.8 | Passiivinen watch list -identifiointi (1:many). | Tiettyjen, aiemmin jollakin epätoivottavalla tavalla toimineiden asiakkaiden etsiminen asiakkaiden joukosta |

Kullekin ryhmälle asetettavat tietosuoja- ja yksityisyyden suojavaatimukset poikkeavat toisistaan.

## 2.2 Luokittelu tiedon tallennustavan mukaan

Biometrisen tiedon tallentamistapa ja -paikka vaikuttavat sovelluksen käyttäjien sovellusta kohtaan tuntemaan luottamukseen. Tähän vaikuttaa talletettavan biometrisen tiedon

- tallennuspaikka (käyttäjän, yrityksen tai viranomaisen hallussa; paikallisesti tai keskitetysti),
- tiedon suojaus (esimerkiksi missä tiedot talletettava palvelin fyysisesti sijaitsee),
- tiedon salaus.

Seuraavassa kutakin näistä kolmesta näkökohdasta tarkastellaan erikseen käyttäjien luottamuksen sekä riski- ja uhkatekijöiden kannalta. Taulukoissa alla on tarkasteltu tallennuspaikan ja suojauksen merkitystä.

Taulukko 7. Tallennuspaikan merkitys

| Tallennuspaikka | Edut (käyttäjän luottamuksen kannalta) | Riskit ja uhat |
|---|---|---|
| Käyttäjällä (älykortti, biopassi) | Tieto on käyttäjän hallinnassa ja hallussa. Ei tietokantoja. | Kortin tai passin hukkaaminen tai varkaus.<br>Luvaton etäluku, jos kontaktiton siru. |
| Viittaus kortilta tietokantaan | Tietokanta vain yhdessä paikassa, suojaus ammattimaista. | Tietokannan joutuminen vääriin käsiin, tietoliikenteen vaarantuminen |
| Yrityksessä paikallisesti (kassapääte, paikallinen palvelin) | Nopea vasteaika.<br>Ymmärrettävyys. | Tiedon luvaton kopiointi.<br>Tietovaraston, esimerkiksi palvelimen varkaus.<br>Päivitykset, poistot asiakassuhteen päättyessä.<br>Varmuuskopioinnin toteutus. |
| Yrityksessä keskitetyssä tietokannassa | Sijoituspaikan fyysinen turvallisuus, asianmukainen ja ammattitaitoinen hallinnointi. | Suureen henkilötietorekisteriin liittyvät riskit, esimerkiksi massiivinen tietovuoto tai -varkaus.<br>Rekistereiden (luvaton) yhdistäminen yrityksen etujen vuoksi.<br>Tarve tiedonsiirtoon verkon yli käyttöpaikoille. |
| Viranomaisen hallussa oleva tietokanta, jossa vertailu suoritetaan | Luotettu viranomainen pitää yllä biometrista rekisteriä | Suureen henkilötietorekisteriin liittyvät riskit, esimerkiksi massiivinen tietovuoto tai -varkaus.<br>Verkko, tietoliikenne |

Taulukko 8. Suojauksen merkitys

| Suojaus | Edut (käyttäjän luottamuksen kannalta) | Riskit ja haitat |
|---|---|---|
| Fyysinen pääsynvalvonta (kortin, päätelaitteen, palvelimen) | Yksinkertainen ja ymmärrettävä. | Ei koskaan aukoton.<br>Henkilökunta.<br>Kallis.<br>Korttien kadottaminen yleistä. |
| Tietotekninen (salasana, vaihtuva koodi tms.) | Asiantuntematon ei pääse käsiksi luvattomasti.<br>Edullinen | Salasanojen normaalit riskit. |

Biometrisen tiedon salauksen (enkryptauksen) problematiikkaa on esitetty alla (

Taulukko **9**) Salaukseen liittyy eräitä ongelmia, joita ei esimerkiksi ole 'luonteeltaan digitaalisessa' tiedossa, kuten tekstissä. Koska esimerkiksi sormenjälkeä ei eri kuvauskerroilla saada tallennettua koskaan täysin samalla tavalla (johtuen mm. sormen

asennosta, paikasta ja paineesta anturilla, ihon elastisuudesta, anturin kohinasta) ei sormenjäljestä muodostettua mallinekaan useimmiten ole täysin sama. Näin ollen mallineiden tai niiden salattujen (enkryptattujen) versioiden suora vertailu ei ole mielekästä. Tästä seuraa, että tyypillisesti sormenjäljen tai muun biometrisen tunnisteen vertailu edellyttää salauksen purkamista. Näin ollen, ja kun vertailu suoritetaan tyypillisesti työasemassa, on käyttäjän kortilla salattuna oleva malline kuitenkin avattava tunnistuksen suorittajan järjestelmän sisällä. Lisäksi on syytä huomata, että yleensä biometrinen ominaisuus, kuten sormenjälki, mitataan ja digitoidaan tunnistuksen suorittajan laitteistolla. On siis aina olemassa vaara, että sinne jää tahattomasti tai tahallisesti kopio käyttäjän biometrisista tiedoista.

Taulukko 9. Salauksen merkitys

| Salaus | Edut (käyttäjän luottamuksen kannalta) | Riskit ja haitat |
|---|---|---|
| Biometrisen tiedon salaus anturilla, vertailu salatulla tiedolla. | Biometrinen tieto salataan mahdollisimman aikaisin | Esim. sormenjäljen salausalgoritmit vasta kehittymässä. |
| Mallineen salaus | Toteutettavissa jo nyt | Biometrista tietoa joudutaan käsittelemään ennen salausta. |

## *2.3 Luokittelu laskennan mukaan (kortilla, paikallisesti vai verkon yli)*

Ennen tunnistusta biometrista tietoa on esikäsiteltävä mm. kohinan poistamiseksi. Biometrinen tieto on kohdistettava esimerkiksi paikallistamalla kasvokuvasta silmät ja suu tai sormenjäljestä hallitsevat piirteet. Tämän jälkeen tieto normalisoidaan esimerkiksi valaistuksen tai sormenjäljen kontrastin suhteen. Vasta sitten voidaan luoda malline ja suorittaa tunnistuksen edellyttämä vertailu tallennettuun mallineeseen. Kaikki nämä toimenpiteet vaativat tietokonelaskentaa.

Laite, jossa biometrisen tiedon käsittelyn vaatima laskenta suoritetaan vaikuttaa tietoturvaan kohdistuviin uhkiin. Tässä suhteessa voidaan erottaa seuraavat kolme perusratkaisua ja niiden yhdistelmiä.

- Laskenta kortilla: kaikki laskenta tapahtuu käyttäjän hallitsemalla laitteella, esimerkiksi älykortilla. Jopa anturi voi olla tässä. Tällöin tieto ei lähde koko prosessin aikana käyttäjän hallinnasta eikä sen sieppaus tai luvaton kopiointi ole mahdollista. Tämän ratkaisun käytännön ongelmana on, että älykorttien laskentateho ei vielä riitä vaadittuun laskentaan ja niihin on hankala integroida anturia. USB-tikulla tämä on jo mahdollista. Periaatteellisempi ongelma liittyy keinoihin, joilla toinen osapuoli voi varmistua tunnistuksen aitoudesta.
- Laskenta paikallisesti: malline, anturi ja laskenta kaikki paikallisesti. Etuna on, että tiedon sieppausta (tele) tietoliikenneyhteyden aikana ei voi tapahtua. Edellyttää luottamusta järjestelmän ylläpitäjään ja tämän osalta huolellista suojautumista esimerkiksi murtoja, tietomurtoja ja sisäpiirissä tapahtuvia luvattomia kopiointeja vastaan.

- Laskenta edellyttää biometrisen tiedon lähettämistä tietoliikenneverkon yli paikkaan, jossa laskenta (ja tietokanta) sijaitsevat. Etuna voidaan pitää sitä, että keskitetyssä laskennassa ja tietokannassa suojaus ja salaus voidaan hoitaa ammattimaisesti. Uhkana tiedon sieppaus tietoliikenteen aikana. Edellyttää siirrettävän tiedon salausta.

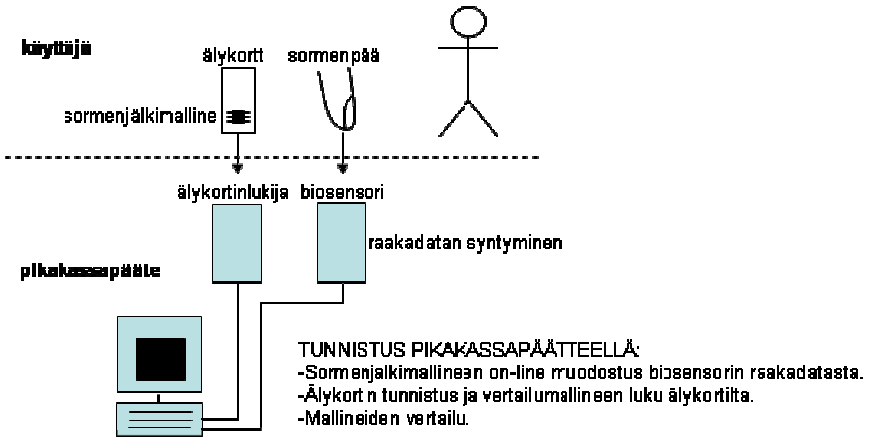
## *2.4 Käyttöesimerkit*

Esimerkkitapausten avulla tarkastellaan tietoturvan ja yksityisyyden suojan vaatimuksia biometrian kaupallisissa sovelluksissa. Tapaukset edustavat erityyppisiä sovelluksia, jotka eroavat myös tiedontallennuksen ja hallinnan kannalta. Esimerkkitapaukset (Kuva 2 - Kuva 5) voivat sisältää myös kyseenalaisia ratkaisuja ongelmien esiin tuomiseksi.

Esimerkkitapaus 1 *Maksutapahtuma - Biometrinen tunniste kortilla*

Kauppaketju A tarjoaa asiakkaille maksukortin, johon voi liittää biometrisen tunnisteen, jolla maksu varmennetaan kassalla. Asiakkaan saama etu on, että hän voi käyttää pikakassajonoja, jotka ovat nopeampia kuin tavalliset käteistä ja pankkikorttia käyttävät jonot. Korttihakemuksessa asia kuvataan asiakkaalle ja hän ilmoittaa suostumuksensa allekirjoituksella.

Teknisesti biotunniste on sormenjälkimalline (template), jonka hash on talletettu älykortille. Korttia personoitaessa asiakas todistaa henkilöllisyytensä. Tunnistustilanteessa asiakas asettaa sormen kassalla olevalle sensorille, joka lukee sormenjäljen, muodostaa mallineen ja edelleen siitä hashin, lukee vertailumallineen hashin asiakkaan älykortilta (lähiluettava, n. 5 cm), vertaa hasheja ja antaa hyväksynnän, jos vertailulaskennan tulos antaa riittävän suuren arvon. Mallineet poistetaan tämän jälkeen kassapäätteen muistista..

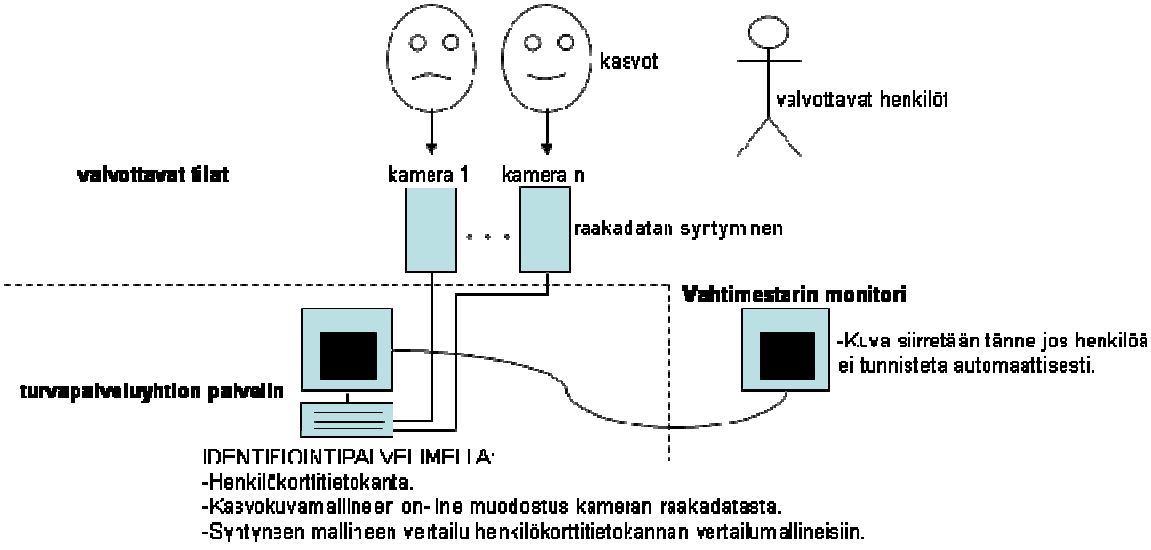



Kuva 2 Maksutapahtuma - Biometrinen tunniste kortilla

Esimerkkitapaus 2 *Aluevalvonta - Biometrinen tunniste paikallisesti keskitettynä*

Yritys B päättää yritysvakoiluepäilyjen ja varkauksien takia tilata turvapalveluyhtiöltä S tunnistavan kameravalvontajärjestelmän. Yrityksen työntekijöitä pyydetään toimitusjohtajan allekirjoittamalla kirjeellä antamaan suostumus kirjallisesti siihen, että henkilökorttitietokannassa olevia kasvokuvia saa käyttää myös biometriseen tunnistukseen. Yrityksen tiloihin, mm. käytäviin, laboratorioihin ja varastotiloihin asennetaan tunnistavat kamerajärjestelmät. Liiketunnistimilla varustetut kamerat suuntautuvat ja zoomaavat automaattisesti alueella liikkuvia henkilöitä kohti, ottavat heistä kasvokuvan ja vertaavat kuvaa tietokantaan talletettuihin kuviin.Jos henkilöä ei tunnisteta, kuva ohjataan valvovan vahtimestarin monitorille ja jos hänkään ei tunnista henkilöä, hän lähettää työparin tarkistamaan tilanteen ja mahdollisesti ottamaan tunkeilijan kiinni tai ohjaamaan vierailijan sallitulle alueelle.

Kasvokuvat talletetaan turvapalveluyhtiön palvelimelle, joka sijaitsee vahtimestarikopin takahuoneessa, Huom. suunnitellaan uutta versiota, jossa palvelin vartiointiliikkeen S tiloissa Vantaalla tai mahdollisesti Tallinnassa. Videokuva lähetetään valvontakameroilta raakatietona palvelimelle, jossa vertailu kasvotietokantaan suoritetaan reaaliajassa.



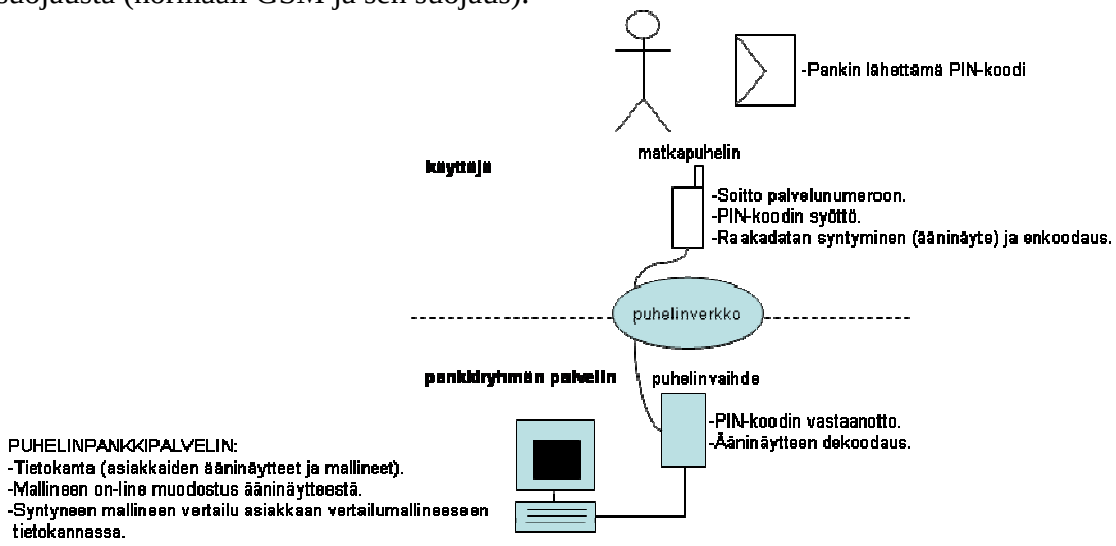

Kuva 3 Aluevalvonta

Esimerkkitapaus 3 *Puhelinpankki - Biometrinen tunniste keskitetysti*

Pankkiryhmä C tarjoaa puhelinpankkia käyttäville asiakkaille tunnuslukujen sijasta äänitunnistetta varmenteeksi. Asiakkaalle kerrotaan mahdollisuudesta kirjeellä. Jos hän haluaa uuden palvelun, hän allekirjoittaa vastauskirjeen ja soittaa annettuun numeroon. Hän antaa kirjeessä tulleen PIN-koodin ja antaa sitten ääninäytteen. Puhelinpankkia käyttäessään asiakas soittaa palvelunumeroon, jossa hän tunnistautuu syöttämällä oman tunnusnumeronsa ja antamalla sitten kyselyyn

vastaavam (promptatun) ääninäytteen, esimerkiksi "luettele vuoden kolme ensimmäistä kuukautta". Kyselyyn vastaava näyte vähentää toisto (replay-) hyökkäyksen mahdollisuutta.

Ääninäytteet ja mallineet on talletettu pankin palvelimelle, joka on vartioidussa tietokonehuoneessa. Mallineet on salattu (enkryptattu). Laskenta tapahtuu myös suojatussa tilassa olevalla palvelimella. Ääninäytteet lähetetään piirikytkentäisen puhelinverkon yli ilman erillistä suojausta (normaali GSM ja sen suojaus).

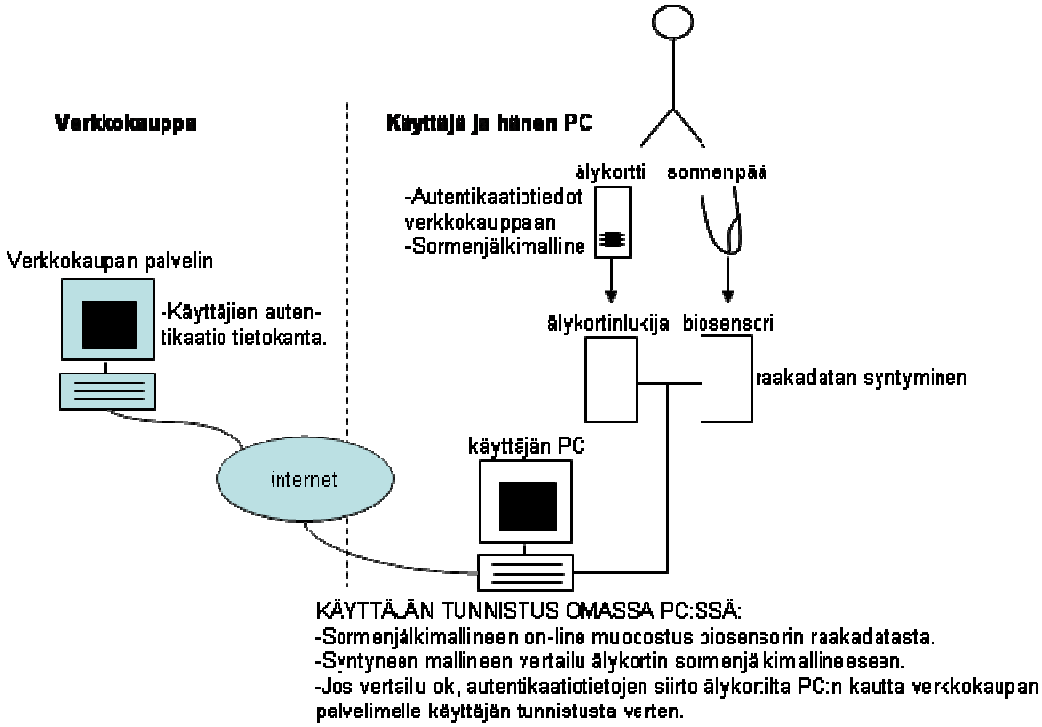



Kuva 4 Puhelinpankki - tunniste keskitetysti

Esimerkkitapaus 4 *Verkkokauppa - Biometrinen tunniste paikallisesti*

Verkkokauppa D tarjoaa asiakkaille biotunnisteen käyttöä elektronisen tunnistekortin (eID) paikallisena varmennuksena. Asiakkaalle kerrotaan mahdollisuudesta kun hän hankkii eID kortin. Kortille talletetaan asiakkaan sormenjälki ja hän hankkii kortin kanssa yhteensopivan PC-sormenjälki- ja kortinlukijan. Tilatessaan tuotteita verkkokaupasta asiakas ensin "avaa" eID-kortin sormenjäljellään ja sitten käyttää sen sisältämiä tunnuksia autentikointiin.

Sormenjälki malline on tallennettu eID-kortille, joka on asiakkaan hallussa. Malline on salattu. Laskenta tapahtuu asiakkaan PC:llä.




Kuva 5 Verkkokauppa - tunniste paikallisesti

Taulukko **10** sisältää yhteenvedon ylläkuvatuista neljästä esimerkkitapauksesta.

Taulukko 10. Yhteenveto esimerkkitapausten ominaisuuksista

| | Esimerkki 1 | Esimerkki 2 | Esimerkki 3 | Esimerkki 4 |
|---|---|---|---|---|
| Menetelmä | Sormenjälki | Kasvojentunnistus | Äänen tunnistus | Sormenjälki |
| Enrollaus (mallin luonti) | Kassapäätteellä, tunnistus ajokortista tms. | Vahtimestaritilan takahuone, tunnistus henkilökortista | Etänä, PIN koodi varmenne kirjeestä | eID kortin myöntäjän tilassa |
| Mallineen tallennus | Asiakkaan älykortilla | Vartiointiliikkeen palvelin | Pankin palvelimella | Asiakkaan älykortilla |
| Mallineen salaus | Kyllä | Ei | Kyllä | Kyllä |
| Keskusrekisteri tms. | Ei | Kyllä | Kyllä | Ei |
| Laskenta (vertailu) | Kassapäätteellä | Serverillä | Serverillä (etä) | Asiakkaan PC |
| Anturi | Kassapäätteellä | Kamera | Puhelimen mikrofoni | Kortin ja sormenjäljen lukulaite |
| Tunnistustilanteen valvonta | Kyllä (kassahenkilö) | Vahtimestari videokuvasta | Ei | ei (itse) |
| Tietoliikenne | Ei | Kyllä, toistaiseksi firman sisällä, siirto Vantaalle tai Tallinnaan vartiointiliike S:n tiloihin mahdollinen | Kyllä, ei erillistä suojausta tai salausta. | Ei |

| | | | | |
|---|---|---|---|---|
| Suostumus ja kannuste | Vapaaehtoinen, palvelun nopeus | "Puolivapaaehtoinen", halu säilyttää työ, ulkopuolisilta ja vierailijoilta ei kysytä | Vapaaehtoinen, palvelun nopeus. | Vapaaehtoinen, varmuus, luottamus. |

## *2.5 Esimerkkeihin liittyvät uhkakuvat*

Tässä kappaleessa tarkastellaan kullekin kappaleessa 2.4 esitetylle esimerkille ominaisimpia uhkakuvia ja niiden oletettuja todennäköisyyksiä, ilman eri biometristen teknologioiden vertailua yksittäisissä esimerkkitapauksissa toisiinsa. Luvussa 4.3 Teknologioita analysoidaan suhteessa toisiinsa yleisen periaatteen, **yksityisyyden suojan** näkökulmasta.

Esimerkkitapaukseen 1, *Maksutapahtuma - Biometrinen tunniste kortilla,* liittyy kaksi uhkakuvatyyppiä, joista ensimmäinen kohdistuu korttiin ja toinen kaupan järjestelmään. Korttia voidaan käyttää väärin joko varastamalla alkuperäinen ja muuttamalla sen tietoja tai tuottamalla vääriä "uusia" kortteja. Tällaiset väärinkäytökset edellyttävät kortin suojauksen tuntemista ja murtamista, mitä pidetään hyvin vaikeana. Erityisesti biometriaan liittyvä uhka koskee aidon kortin käyttämistä väärennetyn biometrian (esimerkiksi gelatiinisormenjäljen) kanssa. Tämä on analogista pankkikortin ja tunnusluvun varastamiselle. Vastatoimena on kortin mitätöinti ja uuden hankinta. Kaupan järjestelmien kautta tuleva uhka ei liity suoranaisesti biometriaan vaan henkilökuntaan ja järjestelmän turvallisuuteen.

Esimerkkitapaukseen 2 *Aluevalvonta - Biometrinen tunniste paikallisesti keskitettynä,* liittyviä vaikutuksia ja uhkia ovat luvallisten kasvokuvatietokantojen yleistyminen (jota saatettaisiin pitää yksityisyyden kannalta ongelmallisena), sekä näiden tietokantojen luvaton myyminen tai vuotaminen.

Esimerkkitapauksessa 3 *Puhelinpankki - Biometrinen tunniste keskitetysti,* uhat ovat samantapaiset kuin esimerkkitapauksessa 2, nyt vain biometrinen tunniste on kasvokuvan sijasta ääni. Erityisenä uhkatekijänä on postissa lähetettävien PIN-tunnisteiden joutuminen vääriin käsiin.

Esimerkkitapauksen 4 *Verkkokauppa - Biometrinen tunniste paikallisesti,* uhat liittyvät kortin varastamiseen tai väärennettyjen korttien valmistukseen, kuten esimerkkitapauksessa 1. Lisäuhkana on koti-PC:n luvaton käyttö tai sinne mahdollisesti jääneen biometrisen tiedon varastaminen.

Kaikkiin esimerkkitapauksiin liittyy väärällä henkilöllisyydellä tehtävän rekisteröitymisen vaara.

Taulukko 11. Esimerkkitapausten uhkakuvat ja uhan todennäköisyys ( 1 / vaikeus)

| Esimerkkitapaus 1 *Maksutapahtuma - Biometrinen tunniste kortilla* | |
|---|---|
| Kortin varastaminen ja murtaminen (hakkerointi) | Pieni - vrt. muut älykortit |
| Troijalainen tai muu keino tiedon varastamiseen kassapäätteellä | Melko pieni / kohtalainen, riippuu kassapäätejärjestelmän avoimuudesta |

| | |
|---|---|
| Esimerkkitapaus 2 *Aluevalvonta - Biometrinen tunniste paikallisesti keskitettynä* | |
| Kasvokuvien tallennus tietokantaan | Suuri (100%) Voidaan kokea ongelmaksi |
| Tietokannan joutuminen luvattomiin käsiin | Pieni / melko pieni |
| Tietoliikenteen sieppaus | Pieni |
| Esimerkkitapaus 3 *Puhelinpankki - Biometrinen tunniste keskitetysti* | |
| Tunnukset (PIN) sisältävän kirjeen varastaminen | Melko pieni / kohtalainen |
| Tietoliikenteen sieppaus | Melko pieni (GSM aika hyvin suojattu) |
| Tietokannan joutuminen luvattomiin käsiin | Pieni |
| Esimerkkitapaus 4 *Verkkokauppa - Biometrinen tunniste paikallisesti* | |
| Kortin varastaminen ja murtaminen (hakkerointi) | Pieni - vrt. muut älykortit |
| Troijalainen tiedon varastamiseen koti-PC:ltä | Melko pieni / kohtalainen, |
| Kaikki | |
| Rekisteröityminen (enrollaus) väärällä henkilöllisyydellä | Pieni / melko pieni, riippuen tunnistamismenettelystä |

# 3. Järjestelmätason vaatimukset biometriselle tunnistusjärjestelmälle

Biometriselle tunnistusjärjestelmälle asetettavat vaatimukset riippuvat käyttötilanteesta ja ympäristöstä, jossa tunnistus suoritetaan. Tässä luvussa kuvataan yleiset järjestelmätason vaatimukset kaupallisille sovelluksille. Perusteeksi otetaan kaupallisten sovellusten yleiset tietoturva- ja yksityisyydensuoja vaatimukset, jotka pohjaavat mm. perustuslain 10 §:ään ja muuhun lainsäädäntöön. Näkökulma on järjestelmätasolla ja tarkoituksena on johtaa yleisistä periaatteista lähtien käytännölliset vaatimukset.

## *3.1 Lainsäädännöstä johtuvat vaatimukset*

Biometristen ominaisuuksien pysyvyys ja peruuttamattomuus aiheuttavat vaatimuksia sääntelylle. Nykyisessä laissa biotunnistusta ei ole kuitenkaan vielä nimenomaisesti säännelty, ja se voi aiheuttaa ongelmia yritysten yrittäessä itse tulkita nykyistä lainsäädäntöä. Aluksi käsitellään yleisiä tietoturva- ja yksityisyydensuoja vaatimuksia, jotka pohjaavat mm. perustuslain (731/1999) 10 §:ään ja muuhun lainsäädäntöön ja koskevat myös kaupallisia sovelluksia. Huom.: Biometrisen tunnistamisen yksityisyydensuojan sääntelyyn liittyviä asioita on yksityiskohtaisemmin käsitelty esimerkiksi LVM:n viestintämarkkinaosaston raportissa http://www.mintc.fi/www/sivut/dokumentit/julkaisu/julkaisusarja/2003/a442003.pdf.

Taulukko 12. Lainsäädännöstä johtuvat vaatimukset kaupalliselle järjestelmälle.

| Referenssi (§) | Laki/asetus | Vaatimusalue |
|---|---|---|
| (523/1999) Henkilötietolaki | Sääntelee henkilötietojen keräämistä, tallettamista ja käyttämistä sekä henkilörekisterien ylläpitämistä.<br>Henkilön biometrinen ominaisuus on henkilötietolain mukainen henkilötieto.<br>Henkilöiden tunnistamisessa käytettävä vertailurekisteri on henkilötietolain mukainen henkilörekisteri.<br>Tietoturvallisuus ja tietojen säilytys:<br>8 § Käsittelyn edellytykset ja luovuttaminen<br>32 § Tietojen suojaaminen.<br>33 § Vaitiolovelvollisuus.<br>34 § Henkilörekisterin hävittäminen.<br>35 § Henkilötietojen siirto arkistoon.<br>36 § Ilmoitusvelvollisuus. Rekisterinpitäjän on ilmoitettava mm. henkilötietojen automaattisesta käsittelystä tietosuojavaltuutetulle lähettämällä tälle rekisteriseloste.<br>Lisäksi rekisterinpitäjän on ilmoitettava tietosuojavaltuutetulle mm. automatisoidun päätöksentekojärjestelmän käyttöönotosta. | Tietoturvallisuus ja tietosuoja |
| (759/2004) Laki yksityisyyden suojasta | Henkilötietojen käsittelyn edellytykset:<br>3 § Tarpeellisuusvaatimus.<br>4 § Työntekijän henkilötietojen keräämisen yleiset | Yksityisyydensuoja työelämässä |

| | | |
|---|---|---|
| työelämässä | edellytykset ja työnantajan tiedonantovelvollisuus.<br>16 § Kameravalvonnan edellytykset.<br>Kameravalvontaa ei saa käyttää **tietyn** työntekijän tai tiettyjen työntekijöiden tarkkailuun työpaikalla. Työnantaja voi kuitenkin kohdentaa kameravalvonnan tiettyyn työpisteeseen, jossa työntekijöitä työskentelee, jos tarkkailu on välttämätöntä laissa määritellyin edellytyksin.<br>17 § Avoimuus kameravalvontaa toteutettaessa. Mm.:<br>-työntekijän yksityisyyteen ei puututa enempää kuin on välttämätöntä toimenpiteiden tarkoituksen saavuttamiseksi;<br>-valvonnalla saatujen henkilöitä koskevien tallenteiden käyttö ja niiden muu käsittely suunnitellaan ja toteutetaan ottaen huomioon, mitä henkilötietolaissa säädetään;<br>-tallenteita käytetään vain niihin tarkoituksiin, joita varten tarkkailua on suoritettu;<br>-työntekijöille tiedotetaan 21 §:ssä tarkoitetun yhteistoiminta- tai kuulemismenettelyn jälkeen kameravalvonnan alkamisesta, toteuttamisesta ja siitä, miten ja missä tilanteissa mahdollisia tallenteita käytetään;<br>-kameravalvonnasta ja sen toteuttamistavasta ilmoitetaan näkyvällä tavalla niissä tiloissa, joihin kamerat on sijoitettu.<br>-tallenteet on hävitettävä heti, kun ne eivät enää ole tarpeen kameravalvonnan tarkoituksen toteuttamiseksi ja viimeistään vuoden kuluttua tallentamisen päättymisestä. Tallenteen saa kuitenkin säilyttää tämän määräajan jälkeen, jos tallenteen säilyttämiseen on erityinen syy. | |

## *3.2 Yleiset vaatimukset järjestelmätasolla*

Taulukko 13. Yleiset vaatimukset järjestelmän *saatavuudelle*.

| Vaatimusalue | Kohde (laitteisto, ohjelmisto) | Tavoitetila |
|---|---|---|
| Biometrisen tunnistusjärjestelmän vasteajat | Käyttäjän laite | Tunnistussovelluksen käynnistys < 3 s. Tunnistuksen vasteaika < 2 s. |
| | Yrityksen laitteet | Yrityksen laitteet, jossa mallineen vertailu tapahtuu, tulisi normaalitilanteessa olla aina toimintavalmiina uuteen tunnistukseen. Vastaus kyselyyn < 0,5 s. Palvelinkapasiteetti riippuu käyttäjien määrästä ja valitusta tunnistusmenetelmästä. |

| | | |
|---|---|---|
| | Tietoliikenneyhteys | Yrityksen laitteiden tulisi normaalitilanteessa olla aina verkkoyhteydessä. Käyttäjän laite verkkoyhteydessä muutamassa sekunnissa (alustariippuvainen). |
| Biometrisen tunnistusjärjestelmän sitkeys (robustness) | Käyttäjän laite, yrityksen laitteet | Samat vaatimukset kuin perinteistenkin tunnistusjärjestelmien (kuten käyttäjätunnus/salasana) käytännön sitkeydelle. Sitkeys testattava jossain tuotekehityksen vaiheessa, usein valmistajan vastuulla. |
| Biometrisen tunnistusjärjestelmän vaihdettavuus, modulaarisuus | Käyttäjän laite, yrityksen laitteet | Järjestelmän tulee olla sellainen, että vaikeiden ongelmien ilmaantuessa se voidaan korvata uudella, vastaavia toimintoja suorittavalla järjestelmällä. |

Saatavuus tulee varmistaa myös muilla kuin yllä olevin keinoin ja menetelmin. Järjestelmää kohtaavia uusia uhkia ja käyttötilanteita tulee arvioida tietyin väliajoin, ja asettaa uusia vaatimuksia saatavuudelle tilanteen mukaan.

Taulukko 14. Yleiset vaatimukset järjestelmän *käytettävyydelle*.

| Vaatimusalue | Kohde (laitteisto, ohjelmisto) | Tavoitetila |
|---|---|---|
| Käyttöönoton helppokäyttöisyys | Käyttäjän laitteen biotunnistusjärjestelmän asennus, alustus ja asetusten määrittely | Lisälaite: tehtävissä ilman ohjekirjaa päätelaitteen ohjatessa käyttöönottotapahtumaa.<br>Integroitu järj.: kuten lisälaite, mutta ei vaadi asennusta. |
| | Yrityksen biotunnistusjärjestelmä-laitteiden asennus, alustus ja asetusten määrittely | Samalla vaikeustasolla kuin muutkin tunnistusmenetelmät. Mallineen luonti kaikille käyttäjille voi viedä aikaa, mutta se täytyy suunnitella käyttäjiä hyvin informoiden, mm. käyttötilanteista. |
| | Biotunnistusjärjestelmän liittäminen osaksi yrityksen muita tunnistus- ja henkilöhallintajärjestelmiä. | Vaikeusasteeltaan tulisi olla samaa luokkaa kuin muut tunnistusjärjestelmät, mutta järjestelmävaatimukset voivat olla vaativampia. |
| | Käyttäjän rekisteröityminen järjestelmään. | Rekisteröitymisen yhteydessä käyttäjästä luetaan ja tallennetaan vertailutiedot (malline) tietovarastoon, joka voi olla keskitetty tai hajautettu. Rekisteröitymisen tulee olla sujuva ja erittäin luotettava prosessi. |
| Tunnistuksen käytettävyys kokonaisuutena | Koko järjestelmä | Loppukäyttäjän kannalta vähintään yhtä helppokäyttöinen ja käytettävä kuin käyttäjätunnus/salasana parin käyttö. |

| | | |
|---|---|---|
| Biotunnistuksen toimintavarmuus | Käyttäjän laite | Laitteen anturin on toimittava häiriöttömästi ja luotettavasti vaikeissakin olosuhteissa (lika, kuluminen, sää). Tunnistuksen hyväksytty onnistumisprosentti riippuu sovelluskohteesta. Mitä useammin tunnistusta käytetään, sitä nopeampi ja luotettavampi sen on oltava. Liityntä muuhun käyttäjän laitteeseen ei saa aiheuttaa toimintahäiriöitä. |
| | Yrityksen laitteet | Samat käyttövarmuuden suorituskykyarvot kuin muissakin tunnistusmenetelmissä. |
| | Tietoliikenneyhteys | Esim. teleoperaattorin liityntä määriteltävä vaadittuun palvelunlaatu (QoS) luokkaan. |
| Järjestelmän käytöstä poistettavuuden vaatimukset | Malline-tietokannat ja raakadata. | Vain määritelty ryhmä ihmisiä pystyy poistamaan nämä tietokannat ja toimimaan lain säätämällä tavalla. |

Taulukko 15. Yleiset vaatimukset järjestelmän *eheydelle, luottamuksellisuudelle ja muille perinteisille tietoturvaominaisuuksille.*

| Vaatimusalue | Kohde (laitteisto, ohjelmisto) | Tavoitetila |
|---|---|---|
| Järjestelmäohjelmiston eheys | Ohjelmisto | Ohjelmiston osat tulisi olla integrointivaiheessa esim. digitaalisesti allekirjoitettuja. Järjestelmän eheys tulisi voida tarkistaa myös tuotantovaiheessa. |
| Järjestelmäkomponenttien autenttisuus | Laitteisto | Laitteiston osien tulisi olla toisensa autentikoivia, jolloin moduulin vaihtuminen havaitaan ja tavanmukainen pääsy järjestelmään estetään. |
| Pääsynvalvonta järjestelmään | Ohjelmistoon perustuva | Käyttäjäryhmät ja tunnistuskoodit käytössä. Sovellusalueriippuvainen. |
| Järjestelmärajapintojen tietoturva | Ohjelmisto | Tietoturvatestatut rajapinnat. |
| Tietosuoja: Mallineen ja raakadatan salaus mm. datansiirron ja säilytyksen aikana | Laitteisto tai ohjelmisto | Mallineita säilytetään ja siirretään vain salattuna. Jos raakadataa on välttämätöntä säilyttää, on se salattava ja pääsy asiattomilta suojattava erittäin hyvin. Kriittisissä järjestelmissä raakadatan käsittely on suotavaa järjestää siten, että se vaatii kahden |

| | | |
|---|---|---|
| | | henkilön osallistumisen (ns. dual control-periaate). |
| Tietosuoja: Identiteetin luottamuksellisuus | Laitteisto tai ohjelmisto | Identiteetin muodostavia henkilötietoja säilytetään vain salattuna. |
| Hyökkäyksiltä suojautuminen | Kaikki (lähinnä palvelin) | Erilaisia hyökkäyksiä vastaan on suojauduttava tehokkaasti ennakoiden tulevia tilanteita. Haittaohjelmat, palvelunesto, jne. |
| Järjestelmän toiminta virhetilanteessa | Kaikki | Järjestelmässä oltava esim. itsetarkkailulogiikka ja vain muutama, hyvin määritelty virhetila, josta palautumisen toimenpiteet ovat yksinkertaisia. |
| Järjestelmän auditointi | Kaikki | Järjestelmä tulisi olla pätevän ulkopuolisen tahon auditoima tai sertifioima. |

## *3.3 Käyttöesimerkkiratkaisujen vaatimukset*

Tarkemmin järjestelmätason vaatimuksia määriteltäessä huomioidaan aiemmin tehty luokittelu eli tarkastellaan kohdassa ”2.4 Käyttöesimerkit” kuvattujen neljän esimerkkitapauksen tietoturvavaatimuksia.

Taulukko 16. Esimerkkitapauksen 1 ”Maksutapahtuma - Biometrinen tunniste kortilla” tietoturvavaatimuksia.

| Vaatimusalue | Vaatimus | Huomioitavaa |
|---|---|---|
| Muistinsuojaus | Kortti sisältää turvallisen muistialueen, jossa mm. malline säilytetään. | Toimikortissa myös eriytetyt sovellukset mahdollisia. |
| Muistinsuojaus | Kortti tunnistaa lukijan lailliseksi ja lukija kortin. | Pääsynvalvonnan perustoiminne. |
| Muistinsuojaus | Kortin sisältämä malline tulisi olla salattu. | Esim. uusiin, tuntemattomiin uhkia voidaan varautua osin etukäteen kaikki kriittinen tieto salaamalla. |
| Mallineen käyttö | Käyttäjäryhmät ja tunnistuskoodit käytössä. | Kassapäätteen pääsynvalvontajärjestelmän riittävyys varmistettava. |
| Mallineen käyttö | Kortin oltava suojattu fyysiseltä kajoamiselta. Esim. kortti rikkoutuu peruuttamattomasti jos sen purkaa osiin. | Toimikortin valmistus on hyvä tilata luotetulta toimittajalta. |
| Mallineen käyttö | Vertailun suorittava laite (esim. kassapääte) ei saa tallettaa kuin hetkellisesti mallineen. Häiriön sattuessa malline ei saa joutua järjestelmän ulkopuolelle millään keinoin. | Standardoituja, koeteltuja ratkaisuja ja laitteita tiedon hävittämiseen tulee käyttää. |
| Erikoistilanteet | Kortin häviämisestä tulee selviytyä tietoturvallisesti siten, että hävinnyt kortti | Myös muita erikoistilanteita on pyrittävä tunnistamaan ja |

| | | |
|---|---|---|
| | voidaan helposti ja nopeasti poistaa käytöstä ja antaa asiakkaalle uusi kortti tilalle. | varautumaan etukäteen. |
| Yhteen-sopivuus | Toimikorttien standardeja hyödynnettävä modulaarisuuden ja yhteensopivuuden varmistamiseksi. | Esim. CBEFF (Common Biometric Exchange File Format) (NIST ja NSA) toimikorteille tulevaisuudessa. |
| Uhkakuvien torjunta | Varmistettava, että sormenjälkeä jäljittelevien menetelmien käyttö ei onnistu. | Esim. sormeen kiinnitettävät lisäkkeet pitäisi havaita. Muut uhkakuvat selvitettävä. |

Taulukko 17. Esimerkkitapauksen 2 ”Aluevalvonta - Biometrinen tunniste paikallisesti keskitettynä” tietoturvavaatimuksia.

| Vaatimusalue | Vaatimus | Huomioitavaa |
|---|---|---|
| Muistinsuojaus | Pääsy paikallisen palvelimen tietokantaan (jossa mallineet säilytetään) täytyy olla erityisen hyvin kontrolloitu lukituin ovin ja pääsynvalvonnan avulla. | Myös kovalevyn salaus olisi mahdollista toteuttaa. |
| Mallineiden hallinta | Henkilöiden lisäys (mallin luonti esim. valokuvista) ja poisto palvelimelta täytyy olla erityisen hyvin kontrolloitu pääsynvalvonnan avulla. | Esim. vain tietyt henkilöt voivat lisätä ja poistaa henkilöitä tietokannasta. |
| Tiedonsiirron turvallisuus | Kameran lähettämän pysäytyskuvan tiedonsiirron turvaaminen. | Laitteiden tunnistus tiedonsiirtoyhteyttä muodostettaessa, tiedon salaus ja eheys. |
| Tiedonsiirron turvallisuus | Jos järjestelmää laajennetaan tai operointia ulkoistetaan, on erittäin tärkeää huolehtia kaiken tiedonsiirron salauksesta ja autenttisuudesta. Mitään dataa ei saa lähettää suojaamattomana julkisissa verkoissa. | Ratkaisuina mm. VPN, sekä yhteistyökumppanin tietoturvallisuusmenettelyjen varmistaminen. Lisäksi huomioonotettava henkilötietolain vaatimukset sille, minne henkilötietoja on soveliasta siirtää: yksityisyyden suojan pitää olla taattu kohdeympäristössä. |
| Erikoistilanteet | Palvelin täytyy olla suojattu haittaohjelmilta troijalaisten ja keyloggereiden varalta. | Järjestelmä voidaan esimerkiksi eristää kokonaan Internet verkosta ja kieltää käyttäjiltä omien ohjelmien asennus. |
| Uhkakuvien torjunta | Kameraa ei saa pystyä huomaamatta vaihtamaan toiseen laitteeseen ilman erityispääsyoikeuksia järjestelmään. | Laitteiden tunnistus järjestelmän käynnistyksen yhteydessä. |

Taulukko 18. Esimerkkitapauksen 3 ”Puhelinpankki - Biometrinen tunniste keskitetysti” tietoturvavaatimuksia.

| Vaatimusalue | Vaatimus | Huomioitavaa |
|---|---|---|
| Muistin suojaus | Mallineet on suojattava salattuna pankin palvelimella. | Mallineet eivät saa joutua tarpeettomasti levitellyiksi edes |

| | | |
|---|---|---|
| | | pankin sisällä. |
| Mallineen käyttö | Mallineiden laskennassa ja vertailussa käytettävän palvelimen täytyy olla sitkeydeltään ja saatavuudeltaan varmistettu eri keinoin. | Sallitut rajapinnat oltava rajoitetut ja testatut poikkeustilanteiden varalta. Mm. rajapinta puhelinverkkoon on kriittinen ja siksi testattava erityisen hyvin. |
| Mallineiden hallinta | Mallineiden luonti on tapahduttava eristetyssä palvelimessa. | Käytettävä palvelin pitää olla eristetty julkisista verkoista mm. mahdollisten haittaohjelmien takia. |
| Tiedonsiirron turvallisuus | Selvitettävä, mitä uhkakuvia puhelinverkkoyhteyden tietoturvan puutteet voivat aiheuttaa. | Mm. Man-in-the-middle skenaarioiden selvittäminen. |
| Uhkakuvien torjunta | Järjestelmä suunniteltava siten, että käyttäjälle ei voi koitua uhkakuvia oman äänensä käytöstä esim. julkisissa tilaisuuksissa. | Onko hyökkääjän mahdollista nauhoittaa soittajan ääntä riittävän monipuolisesti? Mitä uhkakuvia hyökkääjän käyttämät mallinnusohjelmistot voivat aiheuttaa? |

Taulukko 19. Esimerkkitapauksen 4 ”Verkkokauppa - Biometrinen tunniste paikallisesti” tietoturvavaatimuksia.

| Vaatimusalue | Vaatimus | Huomioitavaa |
|---|---|---|
| Muistinsuojaus | Kortti sisältää turvallisen muistialueen, jossa mm. malline säilytetään. | Toimikortissa myös eriytetyt sovellukset mahdollisia. |
| Muistinsuojaus | Kortti tunnistaa lukijan lailliseksi ja lukija kortin. | Pääsynvalvonnan perustoiminne. |
| Muistinsuojaus | Kortin sisältämä malline tulisi olla salattu. | Esim. uusiin, tuntemattomiin uhkia voidaan varautua osin etukäteen kaikki kriittinen tieto salaamalla. |
| Mallineen käyttö | Tunnistuskoodit käytössä. | Kortinlukijan pääsynvalvontajärjestelmän riittävyys varmistettava. |
| Mallineen käyttö | Kortin oltava suojattu fyysiseltä kajoamiselta. Esim. kortti rikkoutuu peruuttamattomasti jos sen purkaa osiin. | Kortin valmistus on hyvä tilata luotetulta toimittajalta. |
| Mallineen käyttö | Vertailun suorittava käyttäjän laite (esim. PC) ei saa tallettaa kuin hetkellisesti mallineen. Häiriön sattuessa malline ei saa joutua järjestelmän ulkopuolelle. | Tieto on hävitettävä laitteen eri muisteista. |
| Erikoistilanteet | Kortin häviämisestä tulee selviytyä tietoturvallisesti siten, että hävinnyt kortti voidaan helposti ja nopeasti poistaa käytöstä ja antaa asiakkaalle uusi kortti tilalle. | Myös muita erikoistilanteita on pyrittävä tunnistamaan ja varautumaan etukäteen. |
| Uhkakuvien torjunta | Varmistettava, että sormenjälkeä jäljittelevien menetelmien käyttö ei onnistu helposti. | Muut uhkakuvat selvitettävä. |

# 4 Biometriset tunnistusmenetelmät ja niiden turvallisuustasot

## 4.1 Yleiset ominaisuudet

Biometristen tunnistusmenetelmien yleisiä ominaisuuksia voidaan kuvailla lukuisilla eri tavoilla, mutta ehkä kaikkein suosituin tapa on eritellä niitä professori Anil Jainin taulukko-muodossa esittämillä perusominaisuuksilla (**Taulukko 20**). Perusominaisuuksien tasoa (”Korkea”, ”Keskitaso”, ”Matala”) on päivitetty Maltonin uudemmilla arvioilla. Tasot eivät ole tarkkoja arvoja vaan asiantuntija-arvioita, jotka muuttuvat teknologioiden kehittyessä.

Taulukko 20. Seitsemän perusominaisuutta neljälle kuvatulle menetelmälle.

| Piirre | Yleisyys | Erottelevuus | Pysyvyys | Keräiltävyys | Toimivuus | Hyväksyttävyys | Kierrettävyys |
|---|---|---|---|---|---|---|---|
| Sormi | Keskitaso | Korkea | Korkea | Keskitaso | Korkea | Keskitaso | Keskitaso |
| Kasvo | Korkea | Matala | Keskitaso | Korkea | Matala | Korkea | Korkea |
| Iiris | Korkea | Korkea | Korkea | Keskitaso | Korkea | Matala | Matala |
| Ääni | Keskitaso | Matala | Matala | Keskitaso | Matala | Korkea | Korkea |

Taulukossa esiintyvät termit merkitsevät:

| | |
|---|---|
| Yleisyys | Jokaisella on oltava tämä biometrinen piirre |
| Erottelevuus | Jokaisella on oltava yksilöllinen biometrinen piirre |
| Pysyvyys | Piirre ei saa ajan myötä muuttua |
| Keräiltävyys | Piirre voidaan mitata helposti (tarkasteltuna järjestelmän kannalta). |
| Toimivuus | Tunnistustarkkuus, tarvittavat resurssit, toimintakyky ja ympäristö |
| Hyväksyttävyys | Miten käyttäjät suhtautuvat tämän piirteen käyttöön tunnistuksessa |
| Kierrettävyys | Mahdollisuus huijata (tai joissain tapauksissa ohittaa) |

Taulukko 21 arvioidaan eri biometristen piirteiden hyvyyttä vastata seitsemään perusominaisuuteen. ”Korkea” tarkoittaa, että piirre on kyseisen perusominaisuuden suhteen korkealla tasolla, ”Keskitaso” ilmaisee melko korkeaa tasoa ja ”Matala” tarkoittaa, että kyseinen piirre ei ole suhteessa muihin piirteisiin korkeatasoinen biometria. Esimerkiksi sormenjäljen ”Pysyvyys” on korkea, kasvoissa se on keskitasoa, sillä kasvot muuttuvat iän myötä (tosin profiili säilyy aikuisiässä suhteellisen hyvin) mutta äänen pysyvyys on matala, sillä ääni voi vaihdella jopa päivittäin.

**Kuitenkin kohdassa ”Kierrettävyys” arvosana ”Matala” on paras tulos, ”Korkea” huonoin**. Esimerkiksi tuntemattoman ihmisen ääntä on helppo nauhoittaa salaa ja nauhoitusta voidaan käyttää alkeellisessa puhujantunnistusjärjestelmässä, mutta iiriksen kuvaaminen on vaikeaa ilman käyttäjän suostumusta. Lisäksi riittävän korkearesoluutioisen iiriskopion tekeminen on teknisesti hankalaa.

## 4.2 Teknologioiden lyhyt esittely

Seuraavassa on lyhyesti esitelty tärkeimmät biometriset teknologiat. Niiden yksityiskohtaisempi kuvaus on liitteessä 1.

***Sormenjälki***

Sormenjälkitunnistus toteutetaan sormenjälkilukijalla ja tunnistusohjelmistolla. Lukija voidaan toteuttaa mm. CCD-pohjaisella optisella anturilla, piistä valmistetulla kapasitiivisella anturilla, lämpötila-anturilla tai ultraääniteknologialla. Tunnistusohjelmien algoritmit toimivat eri valmistajilla eri tavoin. Yleensä ne etsivät lukijan tuottamasta kuvasta tyypillisiä sormenjälkeen liittyviä piirteitä ja niiden keskinäistä sijaintia. Nämä tiedot tallennetaan jokaisen käyttäjän omaan mallineeseen. Tunnistusvaiheessa mallineita verrataan keskenään. Jos kahdella mallineella on jonkin turvallisuusrajan määräämällä tavalla riittävästi yhteisiä piirteitä, mallineet katsotaan kuuluvan samalle henkilölle.

Sormenjälkilaitteet kuvaavat yleensä sormenjäljen tarkasti, mutta sormenjälki voi muuttua piirteiden kulumisen tai vammautumisen vuoksi. Sormenjälkilukijaa käytettäessä sormi ”elää” aina jonkin verran. Lukijan likaisuus ja/tai vaurioituminen vaikuttavat myös kuvan laatuun.

***Kasvo***

Kasvontunnistus on varsinkin v. 2001 New Yorkissa tapahtuneen terrori-iskun jälkeen saanut suurta huomiota osakseen. Kasvontunnistuksessa ihmisen kasvoista erotellaan eri algoritmien vaatimalla tavalla erityyppisiä piirteitä. Varhaisemmissa järjestelmissä piirteitä olivat esimerkiksi silmien, nenän, leuan ja suun väliset geometriset suhteet. Uudemmissa ohjelmistoissa kasvoista lasketaan monimutkaisempia piirteitä (esim. Eigen-piirteitä). Tunnistus tapahtuu vertaamalla henkilön kuvasta laskettuja piirteitä muistissa oleviin piirteisiin.

Kasvojentunnistuksen suurena haasteena on saada riittävän hyvä kuva valvontatyyppisissä sovelluksissa, esimerkiksi lentokentillä, jolloin henkilö ei välttämättä tiedä, että häntä tunnistetaan. Muita käytännön tunnistamiseen liittyviä haasteita ovat mm. kasvokuvan kulma ja valaistus, silmälasit, hiukset ja miesten parta/viikset.

***Iiris***

Silmän iiriksessä oleva kuviointi on monimutkainen ja jokaisella ihmisellä yksilöllinen. Iiristunnistusjärjestelmä ottaa silmästä kuvan kameralla ja laskee iiriksen kuvioinnista mallineen. Mallinetta verrataan muistissa oleviin mallineisiin. Iiristunnistusjärjestelmiä pidetään yleisesti tarkkoina ja luotettavina. Niiden ongelmana on mm. suhteellisen korkea hinta.

***Ääni***

Puhujantunnistus perustuu siihen, että ihmisillä on suhteellisen yksilöllinen puheääni. Kun puhuja on antanut puhenäytteen puhujantunnistusohjelmalle, puheesta erotellaan kullekin algoritmille tyypillisiä piirteitä. Näitä piirteitä vertailemalla voidaan tunnistaa ihmiset toisistaan melko suurella varmuudella. Luotettavuudessa

puhujantunnistusjärjestelmien katsotaan sijoittuvan sormenjälki- ja iiristunnistusjärjestelmien alapuolelle.

Puhujantunnistuksesta poiketen ”puheentunnistus” löytää puheesta eri sanat. Tällaista järjestelmää voidaan käyttää esimerkiksi puhekomentojen antoon.

## *4.3 Teknologioiden analyysi yksityisyyden suojan kannalta*

Seuraavassa analyysissä tarkastellaan eri teknologioiden vahvuuksia ja heikkouksia yksityisyyden suojan kannalta International Biometric Groupin (IBG) tutkimuksen pohjalta. Teknologioita analysoidaan suhteessa toisiinsa yleisen periaatteen, yksityisyyden suojan näkökulmasta. Luvun 2.5 taulukossa 11 tarkastellaan neljää esimerkkitapausta spesifisten uhkien kannalta, eikä eri biometrisia teknologioita ole vertailtu yksittäisissä esimerkkitapauksissa toisiinsa.

Eri teknologioiden yhteydessä esitellään lyhyesti myös luvussa 4.1 kuvatut arviot eri menetelmistä seitsemän perusominaisuuden osalta. Nämä arviot sopivat melko hyvin yhteen verrattuna IBG:n arvioimiin riskeihin. Jos jonkun teknologian kohdalla eri riskiarviot poikkeavat toisistaan, se käsitellään erikseen kunkin teknologian riskejä esittelevän luvun lopussa.

Eri teknologioiden vaikutukset yksityisyyden suojaan poikkeavat toisistaan. Tämä johtuu siitä, että eri biometrisilla piirteillä on erilaiset vaikutukset yksityisyyteen. Esimerkiksi DNA ei muutu ihmisen elinaikana, kasvot on suhteellisen pysyvä tunnistuspiirre, mutta kävelytyyli muuttuu jatkuvasti vaikkapa kenkien vaihtamisen tai vammautumisen takia.

Teknologioita tarkastellaan seuraavien neljän piirteen kautta:

**Verifiointi/Identifiointi**

Verifioinnissa tarkastetaan vain, onko henkilö se, joka hän väittää olevansa. Jos esimerkiksi älykortti väittää VTT:lle illalla tulevan henkilön olevani Turo Tutkija, kulunvalvontaa hoitava sormenjälkilaitteisto vertaa henkilön antamaa sormenjälkeä älykortissa olevaan sormenjälkeen. Vertailua ei tehdä mihinkään muuhun henkilöön.

Identifioinnissa tutkitaan, kuka henkilö on. Esimerkiksi poliisi suorittaa rutiininomaisesti hakuja, jossa tuntematonta sormenjälkeä verrataan suureen joukkoon rekisterissä olevia sormenjälkiä. Rekisteristä etsitään esimerkiksi 5 todennäköisintä henkilöä joista ihmisen tekemä lopullinen tarkastus valitsee oikean tuloksen.

Analyysissä niitä teknologioita, jotka kykenevät laajamittaiseen identifiointiin pidetään yksityisyyden suojan kannalta ongelmallisina. Ne teknologiat, jotka kykenevät vain verifiointiin ovat yksityisyyden suojan kannalta ongelmattomia.

**Julkinen/Salainen (Overt / Covert)**

Ne teknologiat, jotka voivat toimia siten, että käyttäjä ei ole huomannut tai hyväksynyt biometrista tunnistusta, ovat yksityisyyden suojan kannalta ongelmallisia. Vastaavasti ne teknologiat, jotka voivat toimia vain käyttäjän myötävaikutuksella ovat ongelmattomia.

**Käyttäytymiseen perustuva piirre/Fysiologiaan perustuva piirre**

Käyttäytymiseen perustuvia piirteitä ovat esimerkiksi kävelytyyli ja nimikirjoituksen kirjoitustapa. Vahvoja fysiologisia piirteitä ovat esimerkiksi sormenjälki ja silmän iiris.

Näin niitä teknologioita, jotka pohjautuvat muuttumattomiin fysiologisiin piirteisiin, pidetään yksityisyyden suojan kannalta ongelmallisina. Muuttuviin, käyttäytymiseen liittyviin piirteisiin perustuvat teknologiat ovat puolestaan ongelmattomia.

**Tietokannat**

Tässä tarkastellaan sellaisia tietokantoja, joita on olemassa jo nyt tai joita todennäköisesti tehdään tulevaisuudessa ja joilla voidaan tehdä tietokantahaku. Tällaisia tietokantoja on luonnollisesti niillä teknologioilla, jotka soveltuvat identifiointi-tyyppiseen tunnistukseen.

Ne teknologiat, joilta tällaiset tietokannat puuttuvat, ovat siis yksityisyyden suojan kannalta ongelmattomia. Sen sijaan esimerkiksi sormenjälkeen perustuva tunnistus on yksityisyyden suojan kannalta ongelmallinen, sillä sormenjälkijärjestelmissä on tyypillisesti laajat tietokannat, jotka joku voi mahdollisesti varastaa. Kaupallisten palveluiden kannalta tämä mm. merkitsee sitä, että biometristen tietokantojen suojaamiseen on kiinnitettävä erityistä huomiota. Tässä esimerkiksi viranomaisvalvonnalla on merkittävä rooli.

**Teknologioiden luokitus**

Teknologiat luokitellaan neljän edellä kuvatun piirteen osalta kolmeen tasoon: ”Matala”, ”Keskitaso” ja ”Korkea”.

”Matala” tarkoittaa, että teknologiassa on yksityisyyden suojalle vähäinen riski. Teknologian toimintatapa on sellainen, että se sisältää yksityisyyden suojaan liittyviä kysymyksiä vähän tai ei lainkaan.

”Keskitaso” tarkoittaa, että teknologia sisältää potentiaalisia riskejä. Sen käyttö voi johtaa yksityisyyden suojan rikkomuksiin, mutta väärinkäyttöä ei luultavasti esiinny laajassa mitassa.

”Korkea” tarkoittaa, että riski kohtuullinen. Sitä siis voidaan käyttää jopa laajassa mittakaavassa yksityisyyden suojan rikkomuksissa.

## *4.4 Teknologioiden riskit yksityisyyden suojan kannalta*

Tässä luvussa arvioidaan eri teknologioiden riskejä yksityisyyden suojan kannalta. Taulukossa 21 on aluksi koottu luvussa 4.3 kuvatut piirteet ja selitetty ne lyhyesti. Piirteiden avulla voidaan saada yleiskuva eri teknologioiden vaikutuksista yksityisyyden suojaan.

Taulukko 21. Piirteet, joiden avulla arvioidaan teknologioiden riskiä yksityisyyden suojalle.

| | |
|---|---|
| Verifiointi/Identifiointi | **Verifiointi** on **pieni riski** yksityisyyden suojan kannalta, sillä vertailu tehdään vain yhteen mallineeseen<br>**Identifiointi** on **suuri riski** yksityisyyden suojan kannalta, sillä vertailu tehdään suureen joukkoon mallineita |
| Julkinen/Salainen | Jos teknologia vaatii käyttäjän myötävaikutusta (**Julkinen, Overt**), sillä on **pieni riski** yksityisyyden suojan kannalta,<br>Jos teknologia ei vaadi käyttäjän myötävaikutusta, (**Salainen, Covert**), sillä on **suuri riski** yksityisyyden suojan kannalta |
| Käyttäytymiseen/Fysiologiaan | **Käyttäytymiseen** perustuva piirre on muuttuva ja sillä on **pieni riski** yksityisyyden suojan kannalta,<br>**Fysiologiaan** perustuva piirre on pysyvä ja sillä on **suuri riski** yksityisyyden suojan kannalta |
| Tietokannat | Jos teknologialla **ei ole** suuria tietokantoja, sillä on **pieni riski** yksityisyyden suojan kannalta,<br>Jos teknologialla **on** suuria tietokantoja, sillä on **suuri riski** yksityisyyden suojan kannalta |

Taulukkoon (Taulukko 22) on koottu luvussa 4.3 kuvattujen piirteiden luokittelutasot. Luokittelutasot ovat ”sumeita”, sillä tarkkoja kvantitatiivisia arvioita eri teknologioiden vaikutuksista yksityisyyden suojaan on vaikea tehdä. Eri teknologioille annetut luokittelutasot ovat lähinnä asiantuntija-arvioita. Tarkkaa ”mitta-asteikkoa” on siis vaikea antaa. Luokittelutasojen avulla saadaan kuitenkin yleiskuva eri teknologioiden tämänhetkisestä statuksesta yksityisyyden suojan kannalta.

Taulukko 22. Piirteiden riskitasot yksityisyyden suojan kannalta.

| | |
|---|---|
| Matala | Teknologiassa on yksityisyyden suojan kannalta matala riski (ko. piirteen osalta) |
| Keskitaso | Teknologiassa voi olla rajoitettu riski yksityisyyden suojalle nyt tai tulevaisuudessa (ko. piirteen osalta) |
| Korkea | Teknologiassa on kohtuullinen riski ja sitä voidaan käyttää laajasti yksityisyyden suojaa vastaan (ko. piirteen osalta) |

Taulukko 23 on kuvattu neljän tärkeimmän biometriateknologian riskianalyysit yllä esitettyjen piirteiden avulla. Taulukon kohta ”Yleinen Riski” on kokonaisarvio kyseisen teknologian riskistä yksityisyyden suojalle. Taulukon arviot ovat hyvin yleisellä tasolla. On myös huomattava, että jotkin arviot voivat tulevaisuudessa muuttua. Esimerkiksi tällä hetkellä iiristunnistuksen katsotaan olevan suhteellisen harmiton

yksityisyyden suojalle tietokanta-piirteen valossa. Nykyisin ei tällaisia tietokantoja olekaan laajasti käytössä, mutta lähitulevaisuudessa, jos ja kun iiristunnistuksen käyttö lisääntyy, tilanne voi muuttua.

Taulukko 23. Neljän tärkeimmän biometriateknologian riskit yksityisyyden suojalle.

| **PIIRTEET/TEKNOLOGIAT** | **Sormenjälki** | **Kasvo** | **Iiris** | **Ääni** |
|---|---|---|---|---|
| **Verifiointi/Identifiointi** | Korkea | Korkea | Korkea | Matala |
| **Julkinen/Salainen** | Keskitaso | Korkea | Matala | Korkea |
| **Käyttäytymiseen/Fysiologiaan** | Korkea | Keskitaso | Korkea | Matala |
| **Tietokannat** | Korkea | Korkea | Matala | Matala |
| **Yleinen Riski** | Korkea | Korkea | Keskitaso | Keskitaso |

Seuraavaksi kutakin teknologiaa tarkastellaan yksityiskohtaisemmin.

### 4.4.1 Sormenjälki

Tällä hetkellä sormenjälkeen perustuva henkilön automaattinen tunnistus on yleisin teknologia. Sen valta-asema kulunvalvonnassa ja henkilökohtaisessa käytössä säilyy lähitulevaisuudessa ja rikostutkinnassa sen käyttö lisääntyy, kun entistä useampi maa hankkii pitkälle kehittyneitä AFIS-tyyppisiä (Automated Fingerprint Identification Systems) laitteistoja.

Sormenjäljen käytössä tunnistamisessa on yksityisyyden suojan kannalta hyvänä piirteenä on se, että käyttäjä voi halutessaan antaa eri järjestelmille eri sormen. Näin sormenjäljen käyttö esimerkiksi eri tietokantoja yhdistelevissä hauissa vaikeutuu oleellisesti. Myös sitä pidetään hyvänä, että erilaisia sormenjälkilaitteistoja on lukemattomia määriä kaupallisesti saatavana. Koska eri valmistajat käyttävät erilaisia algoritmeja, myös käytössä olevat sormenjälkimallineet poikkeavat toisistaan. Näin eri laitteistojen pohjalta luodut biometriset tietokannat eivät ole sormenjäljen osalta yhteismitallisia.

Yksityisyyden suojan kannalta ongelmallista on puolestaan se, että julkinen sektori kerää yhä lisääntyvässä määrin tietokantoja, jossa ei säilytetä sormenjäljen mallinetta vaan sormenjäljen kuvaa. Tästä hyvänä esimerkkinä on USA:ssa käyttöön otettu laaja ulkomaalaisten sormenjälkien rekisteröinti. On myös selvää, että jos on suorittanut rikoksen ja saanut rikosrekisterin, tieto sormenjäljistä säilyy halusipa teon suorittaja sitä tai ei. Sormenjälki on myös hyvä biometrinen piirre identifiointia varten.

Sormenjälkeen perustuvan teknologian riskit on arvioitu seuraavasti:

| | |
|---|---|
| Verifiointi/Identifiointi | Korkea |
| Julkinen/Salainen | Keskitaso |
| Käyttäytymiseen/Fysiologiaan | Korkea |
| Tietokannat | Korkea |
| Yleinen Riski | Korkea |

Yllä esitettyä, neljän piirteen avulla tehtyä riskiarviota voidaan verrata luvussa 4.1 esiteltyjen seitsemän yleisen ominaisuuden avulla tehtyyn analyysiin. Seuraavassa

arvioidaan, miten näiden seitsemän ominaisuuden pohjalta tehty analyysi tukee neljän piirteen avulla tehtyä analyysiä:

| | |
|---|---|
| **Verifiointi/Identifiointi** | Ominaisuuksista ”Erottelevuus” ja ”Pysyvyys” tukevat riskiarviota voimakkaasti, ”Yleisyys” tukee osittain. |
| **Julkinen/Salainen** | Ominaisuuksista ”Keräiltävyys” tukee riskiarviota. |
| **Käyttäytyminen/Fysiologinen** | Ominaisuuksista ”Erottelevuus” ja ”Pysyvyys” tukevat riskiarviota erittäin voimakkaasti. |

Tietokanta-piirrettä ei seitsemän ominaisuuden avulla ole analysoitu. Alla on esitetty arviointi sormenjälkiteknologiasta seitsemän ominaisuuden pohjalta.

| Piirre | Yleisyys | Erottelevuus | Pysyvyys | Keräiltävyys | Toimivuus | Hyväksyttävyys | Kierrettävyys |
|---|---|---|---|---|---|---|---|
| Sormi | Keskitaso | Korkea | Korkea | Keskitaso | Korkea | Keskitaso | Keskitaso |

Seitsemän yleisen ominaisuuden pohjalta tehty analyysi tukee selvästi neljän piirteen avulla tehtyä analyysiä.

### 4.4.2 Kasvotunnistus

Kasvotunnistus on saanut valtavasti huomiota New Yorkissa v. 2001 tapahtuneen terrori-iskun jälkeen. Kasvotunnistus on tällä hetkellä käytännössä ainoa biometrinen teknologia, jolla edes periaatteessa voidaan tunnistaa tai etsiä ihmisiä esimerkiksi lentokentillä siten, että he eivät itse sitä havaitse tai myötävaikuta tunnistamiseen mitenkään. Kameravalvonnan tekniikkaa kehittämällä, esimerkiksi nopeaa ja automaattista zoomausta halutun ihmisen kasvoihin, voidaan saada korkeatasoisia kuvia kenestä tahansa julkisella paikalla liikkuvasta ihmisestä. Tunnistustarkkuus on kuitenkin vielä huono verrattuna esimerkiksi sormenjälkitekniikkaan.

Juuri se, että muutokset esimerkiksi hiuksissa, parrassa, kasvojen sijainnissa suhteessa kameraan ja valaistuksessa huonontaa oleellisesti kasvotunnistuksen toimintakykyä, on hyvä asia yksityisyyden suojan kannalta. Tämä nimittäin vaikuttaa siihen, että kasvotunnistuksen toimintakykyä voidaan parantaa vain, jos ihmiset ottavat aktiivisesti osaa tunnistustapahtumaan.

Toisaalta juuri kameravalvonnan mahdollisuudet kuvien ottoon ilman asianomaisten tietoa tai hyväksyntää on yksityisyyden kannalta ongelmallista. Tunnistustulosta voidaan myös parantaa, koska ihmisen kasvokuvia voidaan tallentaa lukemattomia määriä tietokantoihin.

Kasvotunnistukseen perustuvan teknologian riskit on arvioitu seuraavasti:

| | |
|---|---|
| Verifiointi/Identifiointi | Korkea |
| Julkinen/Salainen | Korkea |
| Käyttäytymiseen/Fysiologiaan | Keskitaso |
| Tietokannat | Korkea |
| Yleinen Riski | Korkea |

Yllä esitettyä, neljän piirteen avulla tehtyä riskiarviota voidaan verrata luvussa 4.1 esiteltyjen seitsemän yleisen ominaisuuden avulla tehtyyn analyysiin. Seuraavassa arvioidaan, miten näiden seitsemän ominaisuuden pohjalta tehty analyysi tukee neljän piirteen avulla tehtyä analyysiä:

| | |
|---|---|
| **Verifiointi/Identifiointi** | Ominaisuuksista ”Yleisyys” tukee, ”Erottelevuus” ei tue ja ”Pysyvyys” hieman heikentää tämän piirteen analyysiä. |
| **Julkinen/Salainen** | Ominaisuuksista ”Keräiltävyys” tukee riskiarviota. |
| **Käyttäytyminen/Fysiologinen** | Ominaisuuksista ”Erottelevuus” ja ”Pysyvyys” tukevat riskiarviota. |

Tietokanta-piirrettä ei seitsemän ominaisuuden avulla ole analysoitu. Alla on esitetty arviointi kasvotunnistuksesta seitsemän ominaisuuden pohjalta.

| Piirre | Yleisyys | Erottelevuus | Pysyvyys | Keräiltävyys | Toimivuus | Hyväksyttävyys | Kierrettävyys |
|---|---|---|---|---|---|---|---|
| Kasvo | Korkea | Matala | Keskitaso | Korkea | Matala | Korkea | Korkea |

Tältä pohjalta voitaisiin asettaa kasvontunnistuksen analyysissä kohta ”Verifiointi/Identifiointi” ehkä lähemmäs ”Keskitasoa” kuin ”Korkeaa”. Muilta osin ominaisuudet tukevat analyysiä.

### 4.4.3 Iiristunnistus

Iiristunnistukseen liitetään yleensä korkea turvallisuustaso ja väärien tunnistusten erittäin vähäinen määrä. Teknisessä mielessä se onkin varmin biometrinen tunnistuskeino. Toisaalta käytön vaikeus (ainakin sormenjälkitekniikkaan verrattuna), korkea hinta ja käyttäjien vieroksunta ovat estäneet sen laajenemista yleisimmäksi biometriseksi tunnistustekniikaksi.

Yksityisyyden suojan kannalta hyvänä piirteenä pidetään sitä, että iiristunnistuksen käyttö vaatii käyttäjän yhteistyötä, sillä kuvanotto silmistä vaatii jonkin verran keskittymistä. Rikostutkinnassa ei myöskään tällä hetkellä käytetä iiristunnistusta. Mikään ei tietenkään estä sitä, että tulevaisuudessa viranomaisrekistereihin kerättäisiin myös iirismalline.

Yksityisyyden suojan kannalta ongelmallista on se, että iiristunnistus soveltuu loistavasti tietokantahakuihin. Tietokantoja tosin ei ole vielä paljon olemassa. Tekniikan kehittyessä on myös mahdollista, että silmästä saadaan kuva käyttäjän huomaamatta. Kuitenkin käytännössä tähän kuluu vielä aikaa. Valmistajien määrä on tällä hetkellä niin vähäinen, että käytännössä vain muutama algoritmi, ja myös malline, on käytössä.

Iiristunnistukseen perustuvan teknologian riskit on arvioitu seuraavasti:

| | |
|---|---|
| Verifiointi/Identifiointi | Korkea |
| Julkinen/Salainen | Matala |
| Käyttäytymiseen/Fysiologiaan | Korkea |
| Tietokannat | Matala |
| Yleinen Riski | Keskitaso |

Yllä esitettyä, neljän piirteen avulla tehtyä riskiarviota voidaan verrata luvussa 4.1 esiteltyjen seitsemän yleisen ominaisuuden avulla tehtyyn analyysiin. Seuraavassa arvioidaan, miten näiden seitsemän ominaisuuden pohjalta tehty analyysi tukee neljän piirteen avulla tehtyä analyysiä:

| | |
|---|---|
| **Verifiointi/Identifiointi** | Ominaisuuksista ”Yleisyys”, ”Erottelevuus” ja ”Pysyvyys” tukevat erittäin voimakkaasti riskiarviota. |
| **Julkinen/Salainen** | Ominaisuuksista ”Keräiltävyys” osittain heikentää riskiarviota. |
| **Käyttäytyminen/Fysiologinen** | Ominaisuuksista ”Erottelevuus” ja ”Pysyvyys” tukevat erittäin voimakkaasti riskiarviota. |

Tietokanta-piirrettä ei seitsemän ominaisuuden avulla ole analysoitu. Alla on esitetty arviointi iiristunnistuksesta seitsemän ominaisuuden pohjalta.

| Piirre | Yleisyys | Erottelevuus | Pysyvyys | Keräiltävyys | Toimivuus | Hyväksyttävyys | Kierrettävyys |
|---|---|---|---|---|---|---|---|
| Iiris | Korkea | Korkea | Korkea | Keskitaso | Korkea | Matala | Matala |

Tässä ”Keräiltävyys” ei täysin tue ”Julkinen/Salainen” kohdan riskiarviota ”Matala”, mutta mielestämme arvio on silti oikea, sillä ”Julkinen/Salainen” kohdassa tarkastellaan ennemminkin sitä, miten kuvaaminen onnistuisi salassa, kun taas ”Keräiltävyys” tarkastelee iiriksen kuvaamisen teknistä toteutusmahdollisuutta. Aiemmissa kohdissa ”Keräiltävyys” on sopinut paremmin ”Julkinen/Salainen” –kohdan arviointeihin.

”Verifiointi/Identifiointi” kohta saa voimakkaan tuen, mikä on luonnollista, sillä identifiointi-mielessä ja yksityisyyden suojan kannalta iiristunnistus on biometrisista järjestelmistä potentiaalisesti kaikkein uhkaavin. Tosin rikostutkinnan ja rajaviranomaisten laajojen sormenjälkitietokantojen vuoksi sormenjälkitunnistus on käytännössä merkittävin biometrinen identifiointimenetelmä ja näin sormenjälkitunnistuksen ”Verifiointi/Identifiointi” kohdan ”Korkea” on korkein tämän kohdan arvosanoista. Tämä näkyy myös kohdassa ”Tietokannat”, jossa iiristunnistuksessa on arvosana ”Matala”, mikä pudottaa yleisen riskin ”Keskitasolle”.

### 4.4.4 Puhujantunnistus

Puhujantunnistukseen on liitetty suuria odotuksia erityisesti puhelinpohjaisissa palveluissa. Palvelun ostaja tunnistetaan hänen äänensä perusteella, jonka jälkeen palveluun saadaan oikeudet. Tämän jälkeen palvelua ohjataan puheentunnistuksella. Tällaisia järjestelmiä on jo kaupallisesti saatavilla.

Yksityisyyden turvan kannalta hyvää puhujantunnistuksessa on se, että teknologiaa on vaikea käyttää identifioinnin tarkoituksiin.

Ongelmalliseksi puhujantunnistuksen tekee se, että puhetta voidaan äänittää salaa.

Puhujantunnistukseen perustuvan teknologian riskit on arvioitu seuraavasti:

| | |
|---|---|
| Verifiointi/Identifiointi | Matala |
| Julkinen/Salainen | Korkea |

| | |
|---|---|
| Käyttäytymiseen/Fysiologiaan | Matala |
| Tietokannat | Matala |
| Yleinen Riski | Keskitaso |

Yllä esitettyä, neljän piirteen avulla tehtyä riskiarviota voidaan verrata luvussa 4.1 esiteltyjen seitsemän yleisen ominaisuuden avulla tehtyyn analyysiin. Seuraavassa arvioidaan, miten näiden seitsemän ominaisuuden pohjalta tehty analyysi tukee neljän piirteen avulla tehtyä analyysiä:

| | |
|---|---|
| **Verifiointi/Identifiointi** | Ominaisuuksista ”Yleisyys” , ”Erottelevuus” ja ”Pysyvyys” tukevat voimakkaasti riskiarviota. |
| **Julkinen/Salainen** | Ominaisuuksista ”Keräiltävyys” tukee osittain riskiarviota. |
| **Käyttäytyminen/Fysiologinen** | Ominaisuuksista ”Erottelevuus” ja ”Pysyvyys” tukevat erittäin voimakkaasti riskiarviota. |

Tietokanta-piirrettä ei seitsemän ominaisuuden avulla ole analysoitu. Alla on esitetty arviointi puhujantunnistuksesta seitsemän ominaisuuden pohjalta.

| Piirre | Yleisyys | Erottelevuus | Pysyvyys | Keräiltävyys | Toimivuus | Hyväksyttävyys | Kierrettävyys |
|---|---|---|---|---|---|---|---|
| Ääni | Keskitaso | Matala | Matala | Keskitaso | Matala | Korkea | Korkea |

”Julkinen/Salainen” kohdan arvo ”Korkea” on mielestämme oikea. Ominaisuus ”Keräiltävyys” tarkastelee puhujantunnistusta todennäköisesti teknisesti, järjestelmän näkökulmasta. On kuitenkin selvää, että ihmisen puhetta voidaan nauhoittaa salaa melko helposti.

## *4.5 Muut menetelmät*

Muita olemassa olevia tai mahdollisesti tulevaisuudessa hyödynnettäviä menetelmiä ovat mm.

- nimikirjoituksen tunnistus (signature recognition)
- käsigeometria (hand geometry)
- kasvojen lämpökuvaus (facial thermograms)
- sormen geometria (finger geometry)
- käden suonet (hand vein)
- näppäimen painalluksen dynamiikka (keystroke dynamics)
- verkkokalvon kuvaus (retinal scan)
- tuoksu (body odor)
- DNA
- korvan muoto (ear shape)
- kävelytyyli (gait)
- kämmenen jälki (palm print)
- huulten jälki (lip print)
- huulten ja kasvojen liikkeen analyysi (lip and facial movement analysis)

Yllä mainittujen muiden biometristen teknologioiden yksityiskohtaisempi kuvaus on liitteessä 1.

## *4.6 Yksityisyyden suojan turvaaminen biometrisissa teknologioissa*

International Biometrics Group (IBG) on listannut menettelytapoja, joiden tarkoituksena on varmistaa biometristen järjestelmien yksityisyyden suojaa. Samoja tai samantyyppisiä suosituksia löytyy lukuisista eri lähteistä, esimerkiksi kanadalaisen IPC:n (Information and Privacy Commissioner/Ontario) ja OECD:n julkaisuista.

Menettelytavat on jaettu neljään pääryhmään:

- soveltamisala ja järjestelmien mahdollisuudet
- tiedon suojaus
- henkilökohtainen tiedon kontrolli
- muut seikat

Nämä menettelytavat on kuvattu tarkemmin liitteessä 2.

# 5 Yhteenveto ja ohjeistus palvelujen kehittäjille

Biometrinen tieto on yksityisyyden suojan kannalta haastavampi kuin tavallinen henkilötieto, ja se koetaan myös yleisön keskuudessa herkäksi aiheeksi. Tietoturvasta huolehtiminen on siten paitsi keino varmistaa yksityisyyden suojan toteutuminen, myös keino luoda luottamusta palveluihin, joissa käytetään biometristä tunnistusta.

Tässä selvityksessä esitetyn tarkastelun perusteella voidaan antaa seuraavat käytännön suosituksit sekä esittää tiettyjä yleisiä periaatteita biometrian soveltamisesta.

**Perusratkaisut**

- *Pelkkään biometriaan, esimerkiksi sormenjälkeen, perustuva tunnistaminen on suositeltavaa vain kohteissa ja palveluissa, joissa on kysymys sekä yksilön että palveluntarjoajan kannalta hyvin pienestä taloudellisesta tai muusta arvosta.* Tämä suositus perustuu väärän biometrisen identiteetin käytön suhteelliseen helppouteen: latentteja sormenjälkiä voidaan kerätä esimerkiksi juomalasista, ja gelatiinijäljennöksen voi kohtuullisella vaivalla valmistaa kuka tahansa ja niillä kyetään huijaamaan useimpia sormenjälkilaitteita (esimerkiksi Matsumoton kokeissa gelatiinijäljitelmillä huijattiin 80% kaupallisista sormenjälkilaitteista [ks. Viitteet]). Vaikka ns. aliveness detection menetelmät kehittyvät koko ajan, myös huijausmenetelmät kehittyvät kilvan niiden kanssa. Olemassa olevan laitekannan jatkuva päivitys uusia huijauskeinoja vastaan on käytännössä mahdotonta.
- *Biometrian ja älykortin ja/tai salasanan yhdistelmä on ainoa biometrisen tunnistamisen suositeltava ratkaisu, jos kysymys on vähäistä suuremmista taloudellisista tai muista arvoista.*
- *Biometrisen tiedon säilyttäminen hajautetusti käyttäjien hallitsemalla välineellä, esimerkiksi älykorteilla, on useimmiten*[5] *suositeltavaa verrattuna paikallisiin tai keskitettyihin tietokantoihin*[6]. Hajautettu tallennus pienentää mahdollisen tietovuodon tai tietomurron haittavaikutuksia ja vähentää väärinkäytön riskiä. Teknisesti hajautetussa tallennuksessa on aina kysymys yksi-yhteen eli verifiointityyppisestä tunnistuksesta.
- *Salaamattomaan biometriseen tietoon käsiksi pääsy on tehtävä niin vaikeaksi, ettei se normaaleilla "administraattorin" ohjelmointitaidoilla onnistu.* Tällä menettelyllä vähennetään olennaisesti riskiä, että biometrista tietoa vuotaa tai varastetaan järjestelmästä. *Tieto on siis salattava mahdollisimman varhaisessa vaiheessa käsittelyä, mieluiten laitteistopohjaisesti jo anturilla.* Mitään

[5] Biometrisen tiedon säilyttäminen keskitetyssä rekisterissä voi olla tarpeen tilanteissa, joissa henkilö ei itse kykene huolehtimaan esimerkiksi älykortista (lapset, vajaavaltaiset), tai kun viranomaisella tai muulla taholla on laillinen ja perusteltu syy keskitetyn rekisterin käyttöön. Tällainen tilanne voi olla esimerkiksi tunnistava kameravalvonta tai henkilöiden tunnistus vankilassa.

[6] Tietosuoja-asiantuntijoiden piirissä on esitetty kysymys, onko keskitettyjen tietokantojen kohdalla kyseessä tietosuojadirektiivissä tarkoitettu ns. riskejä aiheuttava tietojen käsittely. Ns. 29 artiklan mukainen tietosuojatyöryhmä (tietosuojavaltuutettujen yhteistyöfoorumi) on suosittanut, että jäsenvaltiot harkitsisivat, että keskusrekisteriin perustuvat biometrisen tunnistamisen järjestelmät asetettaisiin tietosuojaviranomaisten ennalta tarkastettavaksi.

työkopioita esim. sormenjäljistä ei tule jäädä laitteiden muistiin. Raakatiedon käyttöä tulee välttää ja käyttää niiden sijasta ei-palautettavia mallineita aina kun se on mahdollista. Poikkeuksena on kasvokuvat, jotka voidaan säilyttää, jos kuvia säilytetään muutenkin. *Myös biometriset mallineet tulee salata.*

- Biometrinen tieto ja muu henkilötieto, esimerkiksi nimi, tulee tallentaa erilleen toisistaan, jos mahdollista myös fyysisesti eri paikkoihin. Tällöin esimerkiksi sormenjälki voi liittyä suoraan esimerkiksi tiettyyn numeroon, ei nimeen. Tämä mahdollistaa myös anonyymit palvelut.
- Biometrinen tieto tulisi mieluiten tallentaa asiakkaan hallitsemalle tietovälineelle, esimerkiksi älykortille. Jos tämä ei ole mahdollista, tieto tulee tallentaa ainoastaan määrättyyn paikkaan, jossa se on suojattu.
- Biometrisen tiedon päätyminen ulkopuolisiin käsiin esimerkiksi tiedonsiirron, varmuuskopioinnin tai laitteiden poistojen yhteydessä on estettävä huolellisella ohjeistuksella ja etukäteissuunnittelulla.

**Yleiset periaatteet**

1. **Lähtökohtana yksityisyyden suojan kunnioittaminen**
2. **Suhteellisuusperiaate**: etujen (tunnistautumisen turvallisuus, tehokkuus, anonyymin asioinnin mahdollisuus) ja haittojen (tietoturvan ja yksityisyyden uhat) suhde. Tunnistusmenetelmää valittaessa, esimerkiksi biometrisen ja muun menetelmän välillä, suhteellisuusperiaate on tärkeä arviointiperuste.
3. **Suostumus ja informointi**. Asiakkaan tai työntekijän tulee ymmärtää mitä biometrisen tunnistamisen käyttö merkitsee, missä tunnistetietoa säilytetään ja kenellä on siihen pääsy ja käyttöoikeus. Suostumuksen peruuttamisen tulee olla mahdollista.
4. Biometrista tietoa koskevat **henkilötietolain vaatimukset**. Näistä keskeisiä ovat rekisterin käyttö vain sille määrättyyn tarkoitukseen, kielto rekisterien luvattomasta yhdistämisestä sekä henkilön oikeus tarkistaa ja oikaista tietonsa rekisterissä.
5. **Yksityisyyden suojan kannalta herkkiä** biometrisiä menetelmiä tulee välttää aina kun se on mahdollista. Tällaisia menetelmiä ovat esimerkiksi perimään perustuvat menetelmät (DNA), jotka voivat kertoa mm. alttiudesta perinnöllisille sairauksille. Tietyissä tapauksissa biometrinen tieto voi olla henkilötietolain tarkoittamaa arkaluonteisesta tietoa (terveydentilaa koskeva tieto), jolle on säädetty erityiset käsittelyn edellytykset.
6. **Tiedon suojaaminen.** Biometrinen tieto tulee suojata asianmukaisella tavalla väärinkäytösten estämiseksi. Käytännössä tämä tarkoittaa tiedon käsittelyn huolellista suunnittelua, käsittelyn pitämistä mahdollisimman vähäisenä ja salaamista tiedonsiirron sekä tallennuksen yhteydessä. Kriittisten biometrisen järjestelmän hallinnointitehtävissä on aiheellista käyttää ns. dual control -menettelyä. Kriittisyys määräytyy järjestelmään talletetun tiedon taloudellisen tai muun arvon perusteella. Lisäksi on huolehdittava tiedon oikeellisuuden (eheyden, integriteetin) turvaamisesta.

**Ohjeita biometrian käyttöönotolle**

1. Riskien hallinta. Onko järjestelmässä heikkoja lenkkejä? Yhden osan turvatason nosto ei auta, jos viereisessä osassa on aukko. Varmista koko järjestelmän ja prosessin luotettava ja turvallinen toiminta
2. Harkitse myös muita, perinteisiä tunnistusmenetelmiä: esim. vahtimestari, kortti, salasana tai varmenteet. Suhteellisuusperiaate.
3. Kerro biometrisesta järjestelmästä ja sen käyttötarkoituksesta avoimesti ja rehellisesti.
4. Ota huomioon mahdollinen epäluulo ja kulttuurinen vastenmielisyys, käsittele kysymyksiä avoimesti.
5. Kun henkilö kirjautuu biometristä tunnistusta varten on noudatettava seuraavia käytäntöjä:
   - kirjautujan (engl. enrollee) henkilöllisyys varmistetaan luotettavasti ja integriteetti eli oikeellisuus turvataan
   - henkilölle selitetään järjestelmän tarkoitus, biometrisen tiedon käyttö ja säilyttäminen
   - käytön vapaaehtoisuus tehdään selväksi
   - henkilö antaa todisteellisesti suostumuksen
   - annetaan riittävä ohjaus ja käytön opastus kirjautumisvaiheessa ja ensimmäisellä käyttökerralla
6. Toimiva varajärjestelmä on välttämätön. Esimerkiksi biometrisen kulunvalvonnan varajärjestelmä voi olla vahtimestari.
7. Biometrisia tietokantoja käsittelevien henkilöiden ja tahojen luotettavuuteen on syytä kiinnittää erityistä huomiota. Koulutuksella näille henkilöille korostetaan tehtävässä noudatettavaa huolellisuutta.
8. Aloita pienimuotoisella kokeilulla, ei kertarysäystä.

# 6 Viitteet


1. Biometrics**,** Personal Identification in Networked Society, Series: The International Series in Engineering and Computer Science, Vol. 479, Jain, Anil K.; Bolle, Ruud; Pankanti, Sharath (Eds.), 1999, 424 p., Hardcover, ISBN: 0-7923-8345-1

2. EU/Joint Research Centre: Biometrics at the frontiers, 2004. 166 p. (www.jrc.es)

3. Practical Biometrics, J. Ashbourn. Springer, 2004. 159 p.

4. Valtiovarainministeriö: http://www.vm.fi/tietoturvasanasto/sisallys.htm

5. http://www.mintc.fi/www/sivut/dokumentit/julkaisu/julkaisusarja/2003/a442003.pdf.

6. Information and Privacy Commissioner / Ontario: http://www.ipc.on.ca/

7. T. Matsumoto, H. Matsumoto, K. Yamada, S. Hoshino, "Impact of Artificial Gummy Fingers on Fingerprint Systems," Proceedings of SPIE Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.

8. OECD: http://www.oecd.org/

9. IBG BioPrivacy Initiative: http://www.bioprivacy.org/

10. Biovision - Roadmap for biometrics in Europe 2010. Roadmap issue 1.1. IST-2001-38236. Ed. Marek Rejman-Greene. 2003


**Lyhenteet ja sanasto**

| | |
|---|---|
| Aliveness | Biometrisen näytteen elävyys tai aitous, esimerkiksi sormenjäljen aitouden havainnoinnilla (aliveness detection) halutaan tieto siitä, että tunnistettava sormenjälki on aito eikä esimerkiksi gelatiinijäljennös. |
| Biometria | Henkilön automaattinen tunnistaminen, joka perustuu henkilön fysiologiseen (esim. sormenjälki, iiris) tai käyttäytymispiirteeseen (kävelytyyli). |
| Dekryptaus | Salatun tiedon avaaminen, ks. enkryptaus. |
| Dual control | Kriittinen toimenpide vaatii kahden henkilön osallistumisen. Menettely varmistaa, että kukaan ei yksin voi tehdä mitään kriittistä. Menettelytapa suojaa sekä järjestelmään talletettuja tietoja että tietojen käsittelyyn oikeutettuja henkilöitä. |
| Enkryptaus | Salaus, tiedon koodaaminen muotoon, josta sen lukeminen on käytännössä mahdotonta ilman salausavainta. |

| | |
|---|---|
| Enrollaus | Henkilön kirjaaminen tai rekisteröinti biometriseen järjestelmään. Yleensä sisältää näytteen annon, henkilön tietojen kirjaamisen ja järjestelmän opastuksen. |
| IBG | International Biometrics Group |
| Identifiointi | Tuntemattoman henkilön tunnistaminen, ts. biometrisella tunnistus-järjestelmällä ei ole etukäteistietoa tai -oletusta henkilöllisyydestä. |
| Integriteetti | Eheys, (integrity) eli oikeellisuus, tarkoittaa tiedon muuttumattomuutta tiedon luomisen, käsittelyn ja siirron aikana. |
| Malline | Malline (template) on henkilön biometrisen tunnisteen esitystapa biometrisessa järjestelmässä, yleensä alkuperäisen biometrian, kuten sormenjäljen, matemaattinen malli. |
| Multimodaalinen | Kahden tai useamman biometrian, esimerkiksi sormenjäljen ja kasvokuvan yhteinen käyttö tunnistamisen yhteydessä. |
| Sitkeys | robustness, (Järjestelmän) kestävyys vikoja, virheitä ja systeemimurtoja vastaan. --> vastustuskykyinen, vikasietoinen |
| Tietosuoja | (data protection; privacy protection) 1. Tietojen oikeudettoman saannin estäminen ja tietojen luottamuksellisuuden säilyttäminen. 2. Henkilötietojen suojaaminen oikeudettomalta tai henkilöä vahingoittavalta käytöltä. |
| Tietoturva | Ks. tietoturvallisuus. |
| Tietoturvallisuus | information security 1. Asiaintila, jossa tietojen, tietojärjestelmien ja tietoliikenteen luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhat eivät aiheuta merkittävää riskiä. 2. Keinojen ja toimenpiteiden kokonaisuus, joiden avulla pyritään varmistamaan tietoturvallisuus niin normaali- kuin poikkeusoloissa. |
| Tunnistus | Tunnistus (recognition) sisältää identifioinnin ja verifioinnin. |
| Verifiointi | Henkilöllisyyden varmistus, ts. biometrisella tunnistusjärjestelmällä on etukäteistieto tai -oletus henkilöllisyydestä. |
| Yksityisyyden suoja | privacy protection, henkilötietojen osalta ks. tietosuoja. |

# Liite 1: Biometriset teknologiat / Technologies for biometrics

The following discussion of biometrics technologies is based mainly on these articles: Tutor in the 4/6/99 issue of PC Magazine and Aidan Dysart, University of Michigan, EECS 598, Winter '98, Biometric Security Solutions OCT 25, 2002 By John Vacca and various IBG articles on biometrics.

## Fingerprint Recognition Technology

*Fingerprint recognition. This system--which consists of a hardware scanner and recognition software--records specific fingerprint characteristics, saves each user's data in a template, and then refers to the templates when the user next tries to gain access. Fingerprint systems are accurate, but they can be affected by changes in the fingerprint (burns, scars, and so on) and by dirt and other factors that distort the image.*

### Optical

Recognition systems capture fingerprints and record their characteristics. The images themselves are not stored. Three primary hardware technologies are used in finger-imaging systems. Optical technology is the oldest and most widely used. The finger is placed on a coated platen, usually built of hard plastic but proprietary to each company. In most devices, a charged coupled device (CCD) converts the image of the fingerprint, with dark ridges and light valleys, into a digital signal. The brightness is either adjusted automatically (preferable) or manually (difficult), leading to a usable image.

Optical devices have several strengths: they are the most proven over time; they can withstand, to some degree, temperature fluctuations; they are fairly inexpensive; and they can provide resolutions up to 500 dpi. Drawbacks to the technology include size - the platen must be of sufficient size to achieve a quality image - and latent prints. Latent prints are leftover prints from previous users. This can cause image degradation, as severe latent prints can cause two sets of prints to be superimposed. Hardware makers have developed several means of dealing with this problem. One method includes keeping the most recently noted latent image in memory, then erasing the image from the scan itself so only the new print remains. Also, the coating and CCD arrays can wear with age, reducing accuracy. Optical is the most implemented technology but and increasing number of vendors utilize silicon technology.

### Capacitive

Silicon technology has gained considerable acceptance since its introduction in the late 90's. Most silicon, or chip, technology is based on DC capacitance. The silicon sensor acts as one plate of a capacitor, and the finger is the other. The capacitance between platen and the finger is converted into an 8-bit grayscale digital image. With the exception of AuthenTec, whose technology employs AC capacitance and reads to the live layer of skin, all silicon fingerprint vendors use a variation of this type of capacitance.

Silicon generally produces better image quality, with less surface area, than optical. Since the chip is comprised of discreet rows and columns - between 200-300 lines in each direction on a 1cmx1.5cm wafer - it can return exceptionally detailed data. The reduced size of the chip means that costs should drop significantly, now that much of the R&D necessary to develop the technology is bearing fruit. Silicon chips are small enough to be integrated into many devices which cannot accommodate optical technology.

Silicon's durability, especially in sub-optimal conditions, has yet to be proven. Although manufacturers use coating devices to treat the silicon, and claim that the surface is 100x more durable than optical, this has to be proven. Also, with the reduction in sensor size, it is even more important to ensure that enrolment and verification are done carefully - a poor enrollment may not capture the center of the fingerprint, and subsequent verifications are subject to the same type of placement. Many major companies have recently moved into the silicon field.

**Ultrasound**

Ultrasound technology, though considered perhaps the most accurate of the fingerprint technologies, is not widely used. It transmits acoustic waves and measures the distance based on the impedance of the finger, the platen, and air. Ultrasound is capable of penetrating dirt and residue on the platen and the finger, countering a main drawback to optical technology.

Until ultrasound technology gains more widespread usage, it will be difficult to assess its long-term performance. However, preliminary usage of products from Ultra-Scan Corporation (USC) indicates that this is a technology with significant promise. It combines a strength of optical technology, large platen size and ease of use, with a strength of silicon technology, the ability to overcome sub-optimal reading conditions.

**Fraud with Fingerprints**

The following excerpt is from an article by Bruce Schneier. "Tsutomu Matsumoto, a Japanese cryptographer, recently decided to look at biometric fingerprint devices. These are security systems that attempt to identify people based on their fingerprint. For years the companies selling these devices have claimed that they are very secure, and that it is almost impossible to fool them into accepting a fake finger as genuine. Matsumoto, along with his students at the Yokohama National University, showed that they can be reliably fooled with a little ingenuity and $10 worth of household supplies."

**Typical Fingerprint Applications**

Fingerprint technology is used daily to access networks and PCs, enter restricted areas, and to authorize transactions. The technology is used primarily in PC/Network Access, Physical Security/Time and Attendance, and Civil ID. Most deployments are 1:1, though there are a number of "one-to-few" deployments in which individuals are matched against modest databases, typically of 10-100 users. Large-scale 1:N

applications, in which a user is identified from a large fingerprint database, are classified as AFIS.

## Face Recognition

*Face recognition. Recognizing the shapes and positioning of the features of a person's face is a complex task, and face recognition software has only recently begun to accomplish it. First a camera captures the image of a face, and then the software extracts pattern information it can compare with user templates.*

The face recognition process has two major parts: detection, locating a human face in an image and isolating it from other objects in the frame, and recognition, comparing the face being captured with a database of faces to find a match.

During detection, the hardware/software combination isolates the facial elements of an image and eliminates extraneous information. The software examines the image for typical facial structures (such as eyes and nose), and once it has found them, it calculates the remainder of the face. It then cuts away background details, leaving a close-up of a face inside a rectangular frame called a binary mask.

Recognition operates according to principles such as eigenfaces or eigenfeatures. (The German eigen refers in this case to the recursive mathematics used to analyze unique facial characteristics.) An eigenface-based system sees each facial image as a two-dimensional set of light and dark areas (eigenfaces) arranged in a particular pattern. The recognition algorithm stores each image as a combination of eigenfaces and then compares the eigenface characteristics of the current face with those in the database.

An eigenfeature-based system focuses on specific features such as the nose, eyes, mouth, eyebrows, and bone curvatures, and the relative distances between them. The system analyzes the currently scanned face and extracts particular eigenfeatures, then compares these with other analyses in the database. Eigenfeature systems typically work in conjunction with eigenface systems to produce the most accurate identification possible. In general, eigenfeature systems are more accurate in identifying faces despite substantial variations such as beards and glasses.

A major difficulty for face recognition systems is that a person's face changes over time. The system must take these changes into account--not only for the face being captured but all other faces in the database as well--to make the correct identification.

All face recognition products store multiple images for each user, and they depend on a set of rules to determine identity from all the relevant data. Some products use artificial intelligence neural-network technology, in which a system effectively learns from experience. In a face recognition system, this learning process allows the system to narrow the range of facial types in the database to which it compares the current face.

Face recognition systems can and do work with only frontal facial images, but some systems offer increased security by storing both front and side views. This produces a 3-D map of the face, eliminating the security problem of imposters showing photographs

of legitimate users to the camera. If the recognition system does not detect three-dimensionality, it refuses access.

### Face Recognition Applications

Facial recognition is used in large-scale citizen identification applications, surveillance applications, law enforcement applications and kiosks. It is mosly deployed in 1:N fashion, searching large databases for close matches. Facial recognition is not as good at 1:1 verification. Face recognition technology is not optimized for desktop authentication.

## Iris Recognition

*Iris recognition. The pattern of the iris (the band of tissue that surrounds the pupil of the eye) is complex, with a variety of characteristics unique in each person. An iris recognition system uses a video camera to capture the sample and software to compare the resulting data against stored templates.*

Iris scans, while relatively new, offer just as much unique character as a fingerprint or retinal scan. Also, the image can be obtained from several inches away, and is thus considered much less intrusive than a retinal scan. Once the eye is located in the image, a series of concentric circular zones are established, and the textural information (lightness and darkness of the image) along the circumference of each zone is extracted. Then a set of coefficients is extracted using neural networks, and they comprise the profile. This is then statistically compared with the template and a decision, based on a distance measurement, is issued. This process takes about 100 ms and is patented by Iriscan Inc.

### Typical Iris Recognition Applications

Iris recognition has traditionally been used in high-security employee-facing physical access implementations, although Iridian - the technology’s primary developer - is moving the technology to the desktop, and has had some success in small-scale logical access deployments. Recent deployments of iris recognition have been passenger authentication at airports in the U.S., U.K., Amsterdam, and Iceland; the technology is also used in prisons in the U.S. to identify inmates. A number of developing countries are considering iris recognition technology for national ID and other large-scale 1:N applications.

### Iris Recognition Issues

Iris recognition requires a controlled and cooperative user interaction. Many users have difficulties to interact with the system until they learn its operation. In frequent user interaction (e.g. employee physical access), the technology grows easier to use but in infrequent user interaction (e.g. national ID) there will be ease-of-use issues. With improved scanning this issue should grow less problematic.

The accuracy of iris recognition may be overstated. Because the claimed EERs are derived from ideal iris images (unlike those acquired in the field), actual results may be

worse than expected. Also, backup procedures may not be as fully developed as in a verification deployment (users accustomed to identification may not carry necessary ID, for example).

**Voice recognition**

This method captures the sound of the speaker's voice as well as the linguistic behaviors. Its primary use is in telephone-based security applications, but its accuracy can be affected by extraneous noises and effects of illness or fatigue of the voice. One obvious problem with voice recognition is fraud: The system can be fooled by a tape of someone's voice. For this reason, advanced voice systems can extend the verification process by giving the user longer and more difficult phrases to read aloud, or requesting a different phrase to be read each time. This does increase the time needed for verification, however, and thus cuts into the system's overall usability.

**Voice Recognition Applications**

Voice recognition is a good solution in applications where vocal interaction is already present. It is not a strong solution when speech is introduced as a new process. Telephony is the primary growth area for voice recognition. Telephony-based applications include, e.g., account access for financial services and customer authentication for service calls.

Voice recognition has also been implemented in physical access solutions for border crossing, although this is not the technology's ideal deployment environment.

**Voice Recognition: Strengths and Weaknesses**

Telephony-based voice recognition doesn't need an additional hardware at the user end. For this reason voice recognition can be installed as a subroutine between user and sensitive information. The ability to use existing telephones means that voice recognition vendors have hundreds of millions of authentication devices available.

Voice recognition can also use existing account access and authentication processes without confusing authentication scenarios. Automated telephone systems with speech recognition are currently ubiquitous because they can reduce the amount of employees in call centers. Voice recognition and speech recognition can function simultaneously using the same utterance. Voice recognition can function as a reliable authentication mechanism for automated telephone systems, adding security to automated telephone-based transactions in areas such as financial services and health care.

Certain voice recognition technologies are highly resistant to fraud, even more so than some fingerprint systems. While false non-matching can be a common problem, this resistance to false matching means that voice recognition can be used to protect reasonably high-value transactions.

## Signature recognition

Signature verification systems have one major thing going for them: public acceptance. People tend to accept a person's signature as proof of identity. Actually, signature recognition systems, also called dynamic signature verification systems, go far beyond simply looking at the shape of a signature: They measure both the distinguishing features of the signature and the distinguishing features of the process of signing. These features include pen pressure, speed, and the points at which the pen is lifted from the paper. These behavioral patterns are captured through a specially designed pen or tablet (or both) and compared with a template of process patterns.

The problem is that our signatures vary significantly over time and from one instance to another, so strong accuracy requires multiple samples and an extended verification process.

### Typical Signature-Scan Applications

Signature-scan is typically implemented in contract execution, formal agreements, acknowledgement of services received, access to controlled documents, etc. As the act of signing documents becomes more integrated with electronic capture processes the opportunity for biometric authentication will increase. At the moment there are few acquisition devices deployed in operational environments capable of capturing biometric data.

### Signature-Scan: Strengths and Weaknesses

Large amount of data in a signature-scan template and the difficult mimicking of the behavior of signing, signature scan is resistant to fraud. As a result of the low FAR deployers can trust that matched users are who they claim to be. Signature-scan also benefits from its ability to leverage existing processes and hardware, such as signature capture tablets and systems based on public key infrastructure (PKI), a method for data encryption. The technology is also considered less invasive than some other biometrics.

However, signature-scan has several weaknesses. The verification is based on the traits of their unique signature. If signing of the name is not made in a consistent manner there may be difficulties in enrolling and verifying with signature-scan. In enrollment subjects must provide a series of similar signatures for the system to find common characteristics between the enrollment signatures. During a successful verification enough characteristics must remain constant. People with muscular illnesses etc. might result in a higher FRR. If users are unaccustomed to signing on a tablet, their signatures may differ to their signatures on ink and paper. This increases the false rejection probability.

## Hand Geometry

*Hand geometry. With this system, the user aligns a hand according to guide marks on the hand reader hardware, and the reader captures a three-dimensional image of the fingers and knuckles and stores the data in a template. Hand geometry has been around for several years, and it was used for a security system at the 1996 Olympic games.*

Hand geometry was, until late 1990's, by far the most widely used biometric system, owing partially to its long history. In the 1960's a device called the Identimat was installed in a time-keeping system at Shearson Hammill, a Wall Street investment firm. It measured the length of the users fingers, and was the first commercial biometric product. Today, the ID3D Handkey system from Recognition Systems, Inc. is the most popular. It works as follows: The user first enters a PIN number on a keypad, and then positions their hand on a plate using a set of guidance pins which ensures that the hand will be in generally the same position for every measurement. Then a digital camera mounted above the plate, with the aid of a mirror, takes a picture of the top and side views of the hand. The dimensions of the hand, such as finger length, width and area, are extrapolated from the image and the magnification of the camera.

The analysis is based on the principle that there are correlations between different measurements. For instance, if your pinky finger is long, you index finger will be long. These correlations we compiled from a large sample population into a set of matrices. The feature profile for the ID3D Handkey system, which is based on these matrices, is an impressive 9 bytes. Since the profile is so small, comparison with the template (established by the PIN) is very fast (around 1.2 seconds). Enrollment is accomplished by averaging three initial measurements, and the template is modified slightly for every accepted authentication.

This system, however, is subject to an attack using a fake hand modeled after that of authorized user. If the algorithm for feature extraction is well understood by the adversaries, they could reconstruct a model hand from the template that would satisfy the measurements and thus give them access. The only other stumbling block would be obtaining the PIN.

**Hand Geometry Applications**

Hand geometry is currently among the most widely used biometric technologies, most suitable for access control and time and attendance applications. Hand scan is used reliably at thousands of places of employment, universities, apartment buildings, and airports. Hand geometry projects are commonly small-scale and involve only a few readers, but some projects have incorporated dozens of readers.

**Hand Geometry Strengths**

Ease of use - the submission of the biometric is straightforward, and with proper training can be done with few misplacements, though elderly people or those with arthritic hands may have problems. The unit also works well with dirty hands.

Fraud is difficult since casting a model of an enrolled hand and fingers would be difficult and time consuming.

Template size of 9 bytes is extremely small. This facilitates storage of a large number of templates in a standalone device, which is how many hand scan devices are designed to work. You could store 9 bytes even in magstripe cards.

As opposed to face or iris scans, which encounter some resistance, hand geometry is not problematic for the vast majority of users.

**Hand Geometry Weaknesses**

Static design - as opposed to other biometrics, which can take advantage of technological breakthroughs like silicon development or camera quality, hand scan has remained largely unchanged for years. Its size precludes it from being used in most logical access scenarios, where compact design may be a prerequisite.

Cost - hand scan readers cost approximately $1400-2000, placing them toward the high end of the physical security spectrum. Finger scan readers, whatever strengths and weaknesses they may have, can be much less expensive, in the $800-1200 range.

Injuries to hands - as with all biometrics, physiological changes can cause users to be rejected falsely. Injuries to hands are fairly common, and would make use of systems such as RSI's impossible.

Accuracy - although generally more reliable than behavioral biometrics such as voice or signature, hand geometry, in its current incarnation, cannot perform 1-to-many searches, but instead is limited to 1-to-1 verification. This limits its use in many different applications.

**Facial Thermograms**

A facial thermogram uses an infrared camera to capture the pattern of blood vessels under the facial skin and then digitize the thermal patterns. Apparently no two people, not even identical twins, have the same facial thermogram. The patterns are created by the branching of blood vessels in the face. As the blood is hotter than the tissue surrounding it, it radiates heat that can be picked up at a distance. Plastic surgery does not change a thermogram unless it involves the rerouting of the flow of blood. In addition, time does not alter a thermogram. However, it is thought that alcohol consumption can radically change a person's thermogram. These systems are still far from everyday use.

**Finger Geometry**

*Finger geometry. These devices are similar to hand geometry systems. The user places one or two fingers beneath a camera that captures the shapes and lengths of the areas of the finger and the knuckles. The system captures a three-dimensional image and matches the data against the stored templates to determine identity.*

The finger geometry technology operates on similar principles as hand geometry, but utilizes only one or two fingers. Measurements of unique finger characteristics, such as width, length, thickness and knuckle size are taken.

Finger geometry systems can perform one-to-one verification or one-to-many identification. The main advantage is that these systems are fast and designed to accommodate "a high throughput of users." According to one company, its system

confirms identity within one second. Finger geometry systems are considered very durable and able to cope well with external conditions. As an example, Disney World uses three-dimensional two-finger geometry to verify the identity of season ticket holders in the United States.

**Hand Vein**

Hand vein technology is a biometric analysis system that measures the internal structure of the human hand to positively identify an individual. It is presented here with an excerpt from the White Papers of the Baltimore Learning Center (an article by Eugene Sweeney).

"The vein map is viewable with reflected light due to the peak absorption of infrared illumination by oxy-haemoglobin in the blood, relative to the surrounding flesh, at specific frequencies. This is unrelated to thermography, which uses emission of far infrared (heat) radiation.

The size and repeatability of vein patterns means that relatively low resolution optical and imaging chip components can be used in capturing and digitizing vein images, providing significant advantages in cost, processing speed and simplicity over other biometric approaches. The security of the system is enhanced by the fact that much of the vein tree image is invisible to human sight.

The image capture hardware can be based on a simple single chip monochrome camera, with a near infrared filter. Alternatively, the IR light - which is entirely harmless - can be readily generated by infrared emitting diodes - as used in TV remote controllers, etc.

The actual comparison of images can be done using a number of different techniques, but simple bitmap comparisons of the binary images have been shown to be extremely fast and accurate using low cost computing technology. Indeed, modern smartcards are likely to have sufficient memory and processing power to handle all the storage and processing itself - thereby reducing costs and improving security."

As an example, LiveGrip™ technology by Advanced Biometrics, Inc. (ABI) uses infrared light to illuminate and analyze subcutaneous tissue and blood vessel patterns of a hand presented in a gripped position. The subcutaneous patterns that lie approximately three millimeters beneath the skin are unique in all individuals. LiveGrip™ technology stores individual hand signatures in a secure server for future identification. Future scans are matched against the stored information in order to verify identify.

**Keystroke Dynamics**

This method analyzes the way in which a user types at a computer keyboard. The input is monitored thousands of times a second, and the durations of keystrokes and the latencies between them are recorded. The set averages of these values for all pairs of keys, called digraphs, (i.e., t-h, e-s, r-e) compose the unique profile. Trigraphs and larger groups may also be analyzed, but the larger the groups, the more variable the data. The sample is compared with the template through statistical means, and the computed distance must be within a threshold to be accepted.

The goal for keyboard dynamics is continual authentication of the user while at a computer, so that if an intruder user had access to the users session while they were away, the machine would eventually be able to recognize the discrepancy. Even though typing patterns are behavioral characteristics, they are very hard to mimic. Because of network lag, all data collection must be done locally on the machine, and so authentication over remote connections would be excluded.

### Retinal Scan

*Retina recognition. Probably the single most secure of all, these biometric systems work with the retina, the layer of blood vessels located at the back of the eye. The retinal image is difficult to capture, and during enrollment the user must focus on a point while holding very still so the camera can perform the capture properly. The only thing that is actually determined is the pattern of the blood vessels, but since this pattern is unique in each person, identification can be precise.*

*The two eye-based systems, iris and retina, are generally considered to offer potentially the best security, because of the distinctiveness of the patterns and the quality of the capture devices.*

Although familiar to high security defense installations and science fiction, retinal scan products have commercially available since 1985. They rely upon the unique patterns of blood vessels on the back wall of the retina. The user positions their head against a support, and a low power infrared light is directed against the back of the retina. The image of the pattern of veins is reflected back to a camera. The image is analyzed in analogous way to the fingerprint system. The sizes of veins, location of vein bifurcations, and capillary endings form a unique set of minutiae. While it may be hard to spoof such a system by constructing an accurate model, extracting someone's eye is much easier. Both of these attacks can be avoided using a thermal test, similar to that used in a fingerprint system.

## Emerging Biometric Technologies

### Body Odor

While humans have used body odor as a basic qualitative biometric, using it as an accurate representation of identity seems a little alien and absurd. Apparently, human body odor is composed of around thirty chemical components whose level or absence form a unique profile. However, even if such a profile were a reliable source of identification, the technology would require a complex, time-consuming chemical analysis, which would hinder it's use in real-world applications.

### DNA

Genetic information, encoded in DNA, may be the ultimate source of identification. What could possibly be more unique than three billion nucleotides, each representing 2 bits of information (4 possible base pairs per location)? However, the technology necessary for quick genetic analysis is not yet available. Even so, identical twins would

pose a threat in that they possess the same genetic information. Furthermore, the collection of the biometric, most likely through blood sample, is the most intrusive system yet.

**Ear Shape**

A lesser-known physical biometric is the shape of the outer ear, lobes, and bone structure. Apparently, police are able to capture earprints of criminals left when they listen at windows and doors. The technology has been used to obtain convictions in the Netherlands.

**Gait**

Legs can be abstracted as connected pendulums, and by using computer vision to extract the magnitude and frequency of their movements gait of the users can be analyzed. While gait is not traditionally thought of as a unique trait, modest identification results have been obtained. However, this is a fairly variable behavioral characteristic, and will most likely never be reliable enough for real identification systems.

**Palm Print**

Palm print is a physical biometric that analyzes the unique patterns on the palm of a person's hand, similar to fingerprinting. Palm biometrics are predominantly used for one-to-many identification. Like fingerprinting, latent or ink palm images can be scanned into the system.

**Lip Print Identification**

Lip print identification, although seldom used, is very similar to fingerprint comparison and is a known and accepted form of scientific comparison.

**Lip and Facial Movement Analysis**

This is usually used together with speech recognition/analysis. Stand-alone lip or facial movement analysis is still an intact area.

**Nail**

Nailbed is parallel epidermal structure located directly beneath the fingernail. The identification process should generate a one-dimensional map of the nailbed resembling a barcode.

# Liite 2: Menettelytavat yksityisyyden suojaamiseksi biometrian käytössä

Seuraavassa esitellään lyhyesti International Biometrics Groupin (IBG) suosittamat menettelytavat, joilla voidaan varmistaa biometristen järjestelmien yksityisyyden suojaa. Menettelytavat voidaan jakaa neljään ryhmään ja 25 alaryhmään.

**SOVELTAMISALA JA JÄRJESTELMIEN MAHDOLLISUUDET**

1. Soveltamisala/käyttötarkoitussidonnaisuus

Biometristen järjestelmien käyttö tulisi rajoittaa siihen tehtävään, mihin se on alun perin suunniteltu. Jos käyttöaluetta laajennetaan, se tulisi selkeästi ilmoittaa järjestelmään kirjautuneille ihmisille ja heillä olisi oltava mahdollisuus poistua järjestelmän piiristä. Jos esimerkiksi biometrisen pankkikortin käyttösovellus liitettäisiin myöhemmin jonkin kauppaketjun premium-asiakkaiden etuihin, käyttötarkoitusta olisi laajennettu alkuperäisestä.

2. Yleinen ja ainutlaatuinen tunniste

Yleisenä ja ainutlaatuisena tunnisteena (universal unique identifier, UUID) voisi olla esimerkiksi yhdistelmä, jossa olisi iirismalline, muutama sormenjälkimalline ja/tai riittävän tarkka DNA-malline. Biopassi, jossa voi sormenjäljen lisäksi olla myös iirismalline on jo askel tähän suuntaan. Biometrisesta informaatiosta ei pitäisi toteuttaa tällaista tunnistetta. UUID on väärinkäytettynä vaara yksityisyyden suojalle, sillä se mahdollistaisi esimerkiksi eri tietokantojen yhdistelyn.

3. Biometrisen tiedon rajoitettu tallentaminen

Biometrista tietoa pitäisi tallentaa vain aiottua tarkoitusta varten ja vain sen ajan, kuin se on ajankohtaista. Jos esimerkiksi kauppaketju A:n tarjoaman biometrisen maksukortin käyttö loppuisi, tallennettua biometrista dataa ei saisi siirtää saman kauppaketjun joihinkin toisiin tarkoituksiin, vaan tämä tieto olisi tuhottava todisteellisesti.

4. Biometrisen järjestelmän potentiaaliset mahdollisuudet

Kun järjestelmän riskejä yksityisyyden suojalle analysoidaan, järjestelmän laajemmat toimintamahdollisuudet on myös tutkittava ja tunnettava tarkoin. Jos esimerkiksi järjestelmää A käytetään henkilöllisyyden verifiointiin, mutta sitä voitaisiin käyttää myös laajoihin tietokanta-ajoihin identifiointitarkoituksessa, tämä tulisi tietää, kun järjestelmää otetaan käyttöön.

5. Muu kuin biometrinen tieto

Muun kuin biometrisen tiedon kerääminen ja tallentaminen pitäisi minimoida. Esimerkiksi kauppaketju A:n keräämä biometrinen tieto saattaa linkittyä kauppaketjun

muuhun asiakastietoon, joka voi olla huomattavan laaja ja voisi teoriassa mahdollistaa jopa yksittäisten ostosten kontrolloinnin.

6. Alkuperäisen biometrisen tiedon tallennus

Mikäli teknisesti mahdollista, alkuperäistä biometristä tietoa (sormenjälkikuva, kasvokuva) ei tulisi tallentaa vaan olisi käytettävä vain mallineita. Mallineen teon jälkeen alkuperäinen tieto olisi tuhottava. Esimerkkinä kauppaketju A saattaisi käyttää biometrista maksukorttia kasvotunnistuksessa ja jättää kasvokuvat tietokantaan esimerkiksi vartiointiliike X:n suorittaman kameravalvonnan tarpeisiin.

**TIEDON SUOJAUS**

7. Biometrisen tiedon suojaus

Biometrista tietoa pitää suojella sen jokaisessa ”elämänvaiheessa”. Kun esimerkiksi sormenjälkitietoa otetaan, sormenjälki lähetetään (yleensä) verkon tai kaapelin välityksellä tietokoneelle, se talletetaan (ja se pitäisi myöhemmin tuhota), siitä tehdään malline joka talletetaan (ja joka myös pitäisi myöhemmin tuhota) ja mallinetta vertaillaan yhteen tai useampaan mallineeseen. Kaikissa näissä vaiheissa on varmistettava, ettei ulkopuolinen pääse tietoon käsiksi.

Suojelua varten on olemassa monia eri keinoja, kuten tiedon salaus ja suljetut paikallisverkot. Myös se mihin tieto tallennetaan fyysisesti, on tärkeää.

8. Tunnistamisen jälkeinen suojaus

Kun biometrinen tunnistaminen on tehty, siitä seuraavia päätöksiä koskeva tiedonsiirto on suojattava.

9. Rajoitettu käyttöoikeus

Biometrisen järjestelmän hoitaminen on uskottava rajoitetulle määrälle ihmisiä. Käyttöoikeuksia ei saa jakaa ”varalta” jokaiselle, joka järjestelmästä jotain tietää. Erityisen laajoissa järjestelmissä voi olla jopa tarve siihen, että järjestelmän päivityksiin/huoltoon tms. toimenpiteisiin tarvitaan useamman kuin yhden henkilön läsnäolo.

10. Biometrisen tiedon erottelu

Biometriset tietokannat pitäisi pitää erillään muista tietokannoista. Jos mahdollista, erottelun oltava fyysistä, jolloin tietokannat olisivat eri tietokoneilla.

11. Biometrisen järjestelmän toiminnan päättäminen

Jos kyseessä on järjestelmä, jota voitaisiin sen loppumisen jälkeen käyttää yksityisyyden suojaa vaarantavasti, sen toiminnan lakkauttamiseen on oltava yleisesti

hyväksytyt menettelytavat. Tähän tehtävään voitaisiin tarvita esimerkiksi viranomaistahoa. Tietovuodot ovat näissä tilanteissa suuri uhka.

**HENKILÖKOHTAISEN TIEDON KONTROLLI**

12. Mahdollisuus päästä pois biometrisen järjestelmän piiristä

Jokaisella pitää mahdollisuuksien mukaan olla oikeus kontrolloida omaa biometrista tietoaan. Jos käyttäjä haluaa, hänen biometrinen tietonsa on tuhottava. Tätä vaatimusta ei voitane toteuttaa kaikissa tilanteissa viranomaispuolella, mutta yksityisen sektorin piirissä vaatimus on itsestään selvä.

13. Omien tietojen tarkastaminen

Jokaisen on voitava korjata, päivittää ja nähdä ne tiedot, jotka on liitetty hänen biometriseen tietoonsa.

14. Salainen kirjautuminen

Jos mahdollista, henkilön olisi voitava antaa biometrinen tunnisteensa anonyymisti. Tällainen tilanne saattaa ilmetä esim. verkkopohjaisissa palveluissa. Jos biometrinen järjestelmä ei välttämättä tarvitse nimeä, osoitetta, yms., niitä ei pidä järjestelmään lisätä.

**MUUT SEIKAT**

15. Auditointi

Varsinkin suuret biometriset järjestelmät olisi alistettava ulkopuolisen ja riippumattoman auditoijan tarkastuksille ja jatkuvalle valvonnalle. Ulkopuolinen auditointi varmistaa osaltaan sen, että järjestelmän toimintaperiaatteet ovat sopimusten mukaisia.

16. Auditointi on julkista

Auditoinnin tuottaman tiedon on oltava julkista.

17. Järjestelmän tarkoituksen ilmoittaminen

Järjestelmän toimintatarkoituksen on oltava kaikille selvä, eikä mitään ”sivutoimintoja” saa jättää kertomatta.

18. Biometriseen järjestelmään kirjautumisesta on tiedettävä

Joissain tapauksissa ihminen voidaan ottaa biometriseen järjestelmään mukaan ilman, että hänen on erikseen annettava biometrista tietoa. Esimerkiksi

kasvojentunnistusjärjestelmä voisi saada kasvokuvan elektronisesta henkilökortista. Tällöin henkilölle on selvästi ilmoitettava, että hänet on kirjattu järjestelmään.

Lähtökohtaisesti, vähintäänkin yksityisen sektorin puolella, henkilöltä on saatava suostumus, ennen kuin hänet kirjataan biometriseen järjestelmään. Suostumuksen tulee olla aidosti vapaaehtoinen, eikä esimerkiksi työnantaja saa painostaa työntekijöitä käyttöön suostumiseen muutoin kuin laissa säädetyissä tarkoituksissa. Avoin kysymys on, voiko asiakasta houkutella biometrisen tunnistuksen käyttöön esimerkiksi alennuksilla.

19. Tunnistamisesta tiedotettava

Jos henkilö joutuu alueelle, missä ihmisiä saatetaan tunnistaa biometrisella järjestelmällä, tämä on tiedotettava hänelle selkeästi.

20. Biometrisen tiedon käyttö

Biometrista tietoa keräävien tahojen on selkeästi ilmaistava, mihin tietoa käytetään. Biometrista tietoa saa lähtökohtaisesti käyttää vain siihen tarkoitukseen, mihin on alun perin sovittu. Jos käyttöä laajennetaan, henkilöiltä on saatava tähän suostumus eikä heitä saa rangaista, jos he eivät tätä lupaa myönnä.

21. Biometriseen järjestelmään kirjautumisen pakollisuus/vapaaehtoisuus

Olipa biometriseen järjestelmään kirjautuminen pakollista (biopassia anottaessa) tai vapaaehtoista (kauppaketju A:n maksukortti), kirjautumisen vapaaehtoisuudesta/pakollisuudesta on selkeästi ilmoitettava.

22. Ketkä valvovat biometrista järjestelmää

Kuka vastaa järjestelmästä, keneltä kysytään tarvittaessa apua ja mikä on valitusmenettely, mikäli järjestelmästä on aiheutunut henkilölle jotain ongelmia.

23. Toimintatapa (verifiointi, identifiointi ja järjestelmään kirjautuminen) informoitava käyttäjälle

Keskeiset toimintaperiaatteet informoitava käyttäjälle: Miten biometrinen järjestelmä toimii, miten kirjaudutaan sisään, mitä verifiointi ja/tai identifiointi tarkoittavat. On myös tärkeää, että järjestelmään kirjautuneet tietävät, mitä muuta tietoa heidän tulee antaa biometrisen mallineen lisäksi, mitä tapahtuu, jos tunnistaminen onnistuu/epäonnistuu. Myös muut vastaavat, järjestelmän toimintaan liittyvät tiedot on kerrottava kirjautujalle.

24. Miten tieto turvataan

Biometrisen järjestelmän käyttäjille on kerrottava, miten järjestelmä turvaa heidän tietonsa (selkeä selostus eri tekniikoista/toimenpiteistä).

## 25. Varajärjestelmä

Jos biometriselle järjestelmälle on varajärjestelmä, kuten yleensä on tarpeen, henkilöillä on oltava oikeus tutustua ja käyttää sitä. Varajärjestelmä ei saa olla luonteeltaan henkilöitä alentava tai jopa rankaiseva. Monissa biometrisissa järjestelmissä on oltava jokin varajärjestelmä, sillä osa ihmisistä ei voi käyttää sormenjälkilaitteita tai iiris-tunnistusta. Tällöin myös niillä ihmisillä, jotka eivät jostain syystä pidä biometrisista järjestelmistä, olisi oltava oikeus käyttää varajärjestelmiä.