Handelshögskolan
VID GÖTEBORGS UNIVERSITET
Institutionen för informatik
2003-12-30

Biometrisk teknologi i praktiken

Organisationers intresse för och ställningstagande till biometrisk teknologi

Abstrakt

Biometri är en snabbväxande och utbredd teknologi som bygger på igenkänning av individers karakteristiska fysiologiska egenskaper för att verifiera och identifiera individernas identitet. Användning av biometri gör det mjöligt att bekräfta individens identitet med hjälp av en noggrann autentiseringsteknik. Biometriska teknologier används inom olika organisationer över hela världen och i olika applikationer. I den här uppsatsen redogörs för vad biometri är, hur biometriska system fungerar samt vilka olika typer av biometriska teknologier och applikationsområden som finns. Syftet och målet med uppsatsen är att undersöka och kartlägga organisationers inställning till biometri, att presentera en djupare teoretisk bakgrund och praktiska erfarenheter av säkerhet vid användningen av biometriska metoder. Teoriavsnittet baseras på litteraturstudier, veteskapliga artiklar och rapporter. Metoden bygger på en kvantitativstudie som genomfördes med hjälp av en enkätundersökning till olika organisationer, samt analys av insamlade data. Slutsatsen av studien visar att organisationers intresse för biometri idag är svagt, men det finns ett visst intresse för att använda tekniken. Användning av rätt teknik till rätt användare i rätt verksamhet kan leda till ökad säkerhet och enorma besparningar.

Nyckelord: biometriska system, template, enrollment, verifikation, identifikation.

Författare: Sarbast Såran
Handledare: Maria Bergenstjerna
Examensarbete II, 10 poäng

Abstract

Biometrics is a rapidly emerging technology which uses physiological or behavioural characteristics to verify identity. By using biometrics it is possible to confirm or establish individual's identity based on strong authentication. Biometrics is applied in different sectors. Implementing the right biometric technologies can improve data security and lead organisations to significant cost savings. In this thesis, I give a brief overview of the field of biometrics technology, how a biometric system works, and I give examples of applications. The purpose of this report clarifies the position of organisations as regards biometric technologies and provides information about security in a context to increase the general public's knowledge about biometric system. The theoretical study is based on both literature study and available technical documentation. I focused on studying relevant and scientific literature and technical papers with qualified academic recognition. A quantitative study has been accomplished with analyses of different companies and organisations. My conclusion is that there is a weak interest and consideration today; however there is some interest from organisations to use and implement biometric technology. Biometrics is not yet widespread in organisations and companies. Implementing the right technology to the right user in the right activity can increase the security and save money.

Förord

Jag vill tacka min handledare Maria Bergenstjerna för hennes goda råd och för den tid hon avsatt för den här uppsatsen. Samtidig vill jag också tacka de företag sam har ställt upp i min undersökning.

Göteborg, december, 2003
Sarbast Såran

Innehållsförteckning

1. Inledning

Denna uppsats är skriven inom kursen IA730B: Examensarbete II hösten 2003, inom ämnet Informatik vid Göteborgs universitet. Mitt intresse för biometri väcktes under 1999, när jag läste vid universitet i Växjö. Sedan dess har jag följt utvecklingen och läst vetenskapliga artiklar om biometri. Jag valde att skriva om biometri dels för att jag tycker att ämnet är mycket intressant och har stor betydelse för informationssäkerhet, dels för att jag märkt att det inte finns någon vid universitetet gjort undersökningar och skrivit om ämnet tidigare.

Vi kommer normalt en eller flera gånger om dagen i kontakt med system för att komma åt och logga in på bankkonto, datorer, mm. Vem är du? Är du den som du påstår dig vara? är två fundamentala frågor som förekommer ofta i säkerhetssammanhang. Att logga in och identifiera dig med datorsystem sker ofta antingen med hjälp av någonting du vet t.ex. lösenord eller någonting du har som bankkort, passeringskort mm.

Biometri använder en eller flera attribut av kroppens delar i stället för lösenord karaktäriska särdrag är unika för varje individ. Biometri betraktas som en av de tillförlitligaste teknikerna för att sätta stop för identitets- och kontokortsbedrägerier. Det säkraste sättet att identifiera och autenticera användare är s.k. biometriska tekniker, vilka emellertid än så länge för allmänheten är alltför anonyma. I dag finns några betydande sådana metoder, nämligen fingeravtryck, handgeometri, röstmönster, retinaavläsning, signaturdynamik och anisktavläsning *(Nanavati S, 2002).*

Biometrisk registrering (enrollment), är det första steget i varje typ av biometriska system. Systemet fångar upp urval eller prov på biometriska karaktärsdrag hos användare. Varje användare måste presentera ett prov av det särskilda biometriska särdraget för senare verifiering av användarens identitet. Systemet skapar ett mönster (template) som lagras i något biometriskt lagringsmedium t ex, på ett smartkort eller i en databas. Verifikation är en process, där biometriska system jämför individens unika karaktärsdrag med redan lagrade data. Biometrisk teknik mäter och analyserar individens karaktärsdrag. Biometriska system består vanligtvis av en avläsare och mjukvara, som konverterar den skannade informationen till digitalform, som sedan lagras i en databas för senare matchning eller jämförelse *(Woodward J, 2003).*

Forskning och utveckling pågår kontinuerlig kring den biometriska teknologin. System som baseras på biometri används för områdena IT-säkerhet, passersystem och inbyggda system. Biometriska system kommer att ersätter lösenord, PIN- koder och nycklar vid identifiering, verifiering, inloggning på datornätverk, och inpasseringssystem i byggnader. Biometri kan användas på många olika sätt inom myndigheter och företag.

1.1 Bakgrund

Informatik definieras som en designorienterad disciplin inom informationsteknologi. Den handlar om användning och utveckling av informationsteknik[1]. Informatik kan bidra till användandet och utvecklandet av själva informationstekniken *(Dahlbom, B. 1995)*. Den revolutionerande Informationsteknologin[2] ändrar vårt sätt att leva och se på tillvaron. Informationsteknologin spelar en viktig roll i vardagslivet såväl socialt för varje individ som i samhället som helhet. För att kunna förstå hur tekniken formar samhället, måste vi ändra vårt tillvägagångssätt att tänka och se på informationsteknologin och hur informationsteknologin kan används för kontroll av individer eller stödja verksamheten i en organisation *(Dahlbom, B. 1997).*

Synen på IT säkerhet har under senare år genomgått en rad förändringar och nytänkande. En av de senaste teknologierna inom IT-säkerhet är biometriska metoder eller biometri. Biometri och biometrisk säkerhet är ett nytt och spännande område, där det pågår ständig forskning och utveckling. Biometri kommer allt närmare oss och smyger sig in samhället. Biometri är vetenskaplig användning av digital teknik, för att identifiera individer, baserad på fysiska och biologiska unika karaktärsdrag.

Inom biometri finns det en hel rad applikationsområden som är anpassade till olika organisationer. En del myndigheter skolor och företag använder sig av biometriska metoder för att förhindra identitetsstöld och lösenordshackning. *Precise Biometrics AB* är ett av de ledande företagen inom biometri. De har tecknat avtal om leverans av fingeravtrycksläsare till Stockholms stads skolor. Eleverna i skolan använder en fingeravtrycksbaserad lösning för inloggning i datorsystemen istället för användarnamn och lösenord. Kriminalvårdsstyrelsen arbetar med att höja IT-säkerheten. Företag har visat intresse att testa ett antal fingeravtrycks- och smartkortläsare. Företag vill byta ut eller komplettera dagens inloggningsrutiner, som bygger på lösenord, med biometrisk fingeravtrycksidentifiering och smartkort *(Precise Biometrics AB, 2003, Newsletter, No.3)*

Flygplatser är ett annat viktigt område där biometri används, inte bara i USA och Europa utan också i Sverige, som redan har börjat använda och testa metoden. På flygplatser där säkerhetskraven är skärpta, kan kontroller av passagerare med hjälp av biometriska metoder bli aktuella, speciellt vid incheckning. I Sverige har SAS börjat kundtesta med biometri- lösning på två flygplatser. Företagets utvärdering av biometrianvändning omfattar förenklad incheckning och ombordstigning av passagerare. SAS-resenärer på Umeå flygplats får gå igenom vändkorset vid utgången till planet sedan de frigjort spärren med hjälp av sitt fingeravtryck. En annan teknik som också ska testas senare på skandinaviska flygplatser är avläsning av ögat. Testet, som ska genomförs med smarta SAS-kort ska vara klart våren 2004. På kortet lagras resenärens fingeravtryck eller bild av iris [3].

---

[1]Informationsteknik: är samlingsnamnet för den nya revolutionen inom dataområdet där hanteringen och behandlingen av informationen har hamnat i centrum.

[2] Informationsteknologi är läran om informationsteknik Oftast sägs eller skrivs informationsteknologi när det är informationsteknik som avses. Jämför med engelskans *Information Technology.*

[3] SAS kundtestar biometri- lösning. 2003-09-10. http://www.compare.nu/news/index.asp?id=424

1.2 Mål och syfte

Syftet med examensarbetet är att undersöka organisationers inställning till biometri och att arbetet ska kunna väcka ett stort intresse och öka kunskap inom biometri hos läsaren.
Mitt eget mål med detta examensarbete är att skaffa mig en djupare teoretisk kunskap och praktisk erfarenhet om teorier kring säkerhet och biometriska metoder. Genom att genomföra en empirisk undersökning inom olika organisationer vill jag komma ett steg närmare verkligheten och betydelsen av säkerhet i organisationer. IT-säkerhet är en viktig fråga i organisationer, som i hög grad måste anpassa sig efter ny teknologi, genom att använda nya metoder för att säkerställa sina resurser.

1.3 Problemformulering

Behovet av och kraven på säkerhet ökar i takt med att utvecklingen i samhället går mer och mer datorisering. Informationssäkerhet är ett område som omfattar logiska såväl som fysisk access till datoriserade system. På senare tid har antalet datorrelaterade brott ökat markant. Biometriska system kan användas till många applikationer hos olika organisationer.
Effektiv hantering av ett växande antal kontokreditsbedrägerier i dagens IT-samhälle, är ett ständigt återkommande problem, inte bara för individen, utan även för företagen och myndigheterna.
Det ökade intresset för biometriska säkerhetslösningar i USA och i Europa hos såväl myndigheter som företag har gett upphov till ökade investeringar i biometrisk marknad. Enligt (**I**nternational **B**iometric **G**roup)[4] förväntas den globala biometrimarknaden växa från 399$ miljoner år 2000 till 1,9 billion dollar till och med år 2005. I Sverige har vissa företag börjat satsa och testa biometri, medan andra avvaktar och ser hur utvecklingen blir. Därför är det intressant att forska och kartlägga följande frågor:

- **Hur stort är intresset för biometrisk teknologi bland svenska organisationer?**
- **Vad kan biometrisk teknologi bidra med?**

[4] International Biometric Group, http://www.biometricgroup.com/press_releases/pr_2001_market_report.html

1.4 Avgränsningar

Biometri är ett ganska brett område. Därför begränsa mig till att studera själva tekniken hur det fungerar, olika teknologier och olika användningsområden för biometri. Jag kommer inte att behandla matematiska eller algoritmiska frågor, som är en väsentlig del av biometriska teknologin. Inte heller kommer jag att beröra följande områden:

- Biometrisk standard.
- Sårbarhetsanalys och test av biometri.
- Frågor kring den personliga integriteten vid användning av biometriska system.
- Allmänhetens och användarnas acceptans av biometrisk teknologi.

1.5 Disposition

Rapportens struktur består av följande:

- **Kapitel 1**, *Introduktion*. Kapitlet inleds med en kort beskrivning av biometrisk teknologi. Bakgrund, sammanfattning av problemområdet, mål, syfte och problemformulering samt avgränsning av ämnet.

- **Kapitel 2**, *Metod*, handlar om arbetsprocessen i rapporten, en översikt av datasamlingen och en allmän beskrivning av den vetenskapliga undersökningen.

- **Kapitel 3**, *Teori*. Redovisar vad som skrivits i litteratur, vetenskapliga tidsskrifter och andra tekniska rapporter kring biometri och om olika biometriska metoder och användningsområden.

- **Kapitel 4**, *Empiriska resultat och analys*. Presenterar resultatet av enkätundersökningen i tabeller och diagram, med analys för varje fråga.

- **Kapitel 5,** *Slutsatser och diskussion*, ger svar på frågställningar och diskussioner om biometriska teknologier.

- **Kapitel 6,** *Referenser,* innehåller referenser till litteratur, artiklar och webbadresser.

- **Kapitel 7,** *Appendix*, innehåller enkätundersökningens frågor och resultatsammanställning.

1.6 Begreppslista

Nedan följer några termer som förekommer i uppsatsen. Vissa specialuttryck saknar direkt motsvarighet på svenska. Då används den engelska termen. Så är det med ”template”, som närmast skulle kunna översättas med ”digital identitet”.

Autentisering - Autentisering är en verifiering av användarens identitet, vilket har till syfte att kontrollera huruvida en användare är behörig att få åtkomst eller tillgång till information.

Biometri– Teknisk analys av biologiska data, exempelvis ett fingeravtryck för att fastställa en persons identitet.

Biometrisk autentisering – processen att fastställa en individs identitet med hjälp av biometri, 1-till-1 matchning.

Biometriskt system– hårdvara och mjukvara används för att bekräfta biometrisk identifikation eller verifikation.

Enrol– (Br), **enroll** (Am) – registrera.

Enrolment– (Br), **enrollment** (Am) – biometrisk registrering.

FAR (False Acceptance Rate) – sannolikheten att biometriska system misslyckas med att avvisa en obehörig.

FRR (False Rejection Rate) – sannolikheten att biometriska system avvisar en behörig användare som alltså nekas åtkomst.

Identifikation – en persons identitet bestäms genom jämförelser med många templates och bilder i en databas.

Matcha – jämföra eller verifiera biometriskt prov mot tidigare lagrade template.

Minutiae– Allmän term för karaktäristiska egenheter såsom åsar, dalar, öar och delningar i ett fingermönster

PIN-kod (**P**ersonal **I**dentity **N**umber) – personlig sifferkod ofta bestående av fyra siffror.

Smartkort – ett kort i kontokortsformat som innehåller mikroelektronik med minne. Kan lagra stora datamängder som med hjälp av en inbyggd mikroprocessor kan kommunicera och utföra transaktioner.

Template– matematisk representation av verkliga biometriska värden eller andra biometriska uppgifter**,** t. ex lagrad information om ett fingeravtryck. (”Digital identitet”)

Token – fysisk apparat som innehåller specificerad information för användare.

Verifikation – en användares påstådda identitet bekräftas.

2. Metod

I det här kapitlet redogör jag för metoden eller arbetsprocessen, sedan följer kvantitativ och kvalitativ metodbeskrivning samt datasamling (primära och sekundära data). För att kunna precisera problemformuleringen, avslutas kapitlet med en kritisk analys av datainsamlingen.

2.1 Kvalitativ och kvantitativ metod

Kvalitativa metoder avser studier av subjektiva fenomen samt vid tolkning innebörden av symboler. I kvalitativa metodfrågor kan djupintervju, deltagande observation förekomma. Ofta kan tolkningar av fenomen exemplifieras i kvalitativa metoder *(Wallén 1996)*. Den kvalitativa metoden studerar enligt *Backman (1998),* hur människan uppfattar och tolkar den omgivande verkligheten. Det handlar alltså inte om observation och mätning av verkligheten. Det kvalitativa synsättet bygger på hur individen tolkar och formar sin verklighet. Skillnaden mellan den traditionella kvantitativa metoden och den kvalitativa är att den senare metoden inte uppfattas objektiv utan subjektiv.

Den kvantitativa metodens främsta syfte är att kartlägga och beskriva ett fenomen systematisk. Forskaren i denna typ av metod ska ha ett neutralt förhållningssätt till informationskällan. I kvantitativa metoder använder forskaren ofta information, som kan mätas i siffror och tal. Ofta används någon form av statistisk bearbetning, beräkning eller metod för att analysera det kvantifierade datamaterialet. Studier som baseras på kvantitativa metoder är oftast systematiska och strukturerade, exempelvis enkätundersökningar, tillskillnad från den kvalitativa metoden som innehåller ostrukturerade observationer till exempel djupintervjuer. Kvantitativ metod ger ett bredare perspektiv och en bättre förförståelse för det man undersöker och beskriver, samt förklarar det som är genomsnittligt och representativt (*Holme & Solvang, 1997).*

2.2 Metod val

I denna del av uppsatsen presenteras de metoder som anses vara praktiska och användbara. Därför är det viktigt att beskriva vilka metoder som ska användas och som bäst lämpar med tanke på aktuell problemformulering.

Eftersom uppsatsen baseras på empiriska studier måste metoder väljas, som på bästa sätt stödjer detta tillvägagångssätt. Den kvantitativa metoden är mest lämpad för min uppsats. Den empiriska undersökningen baseras på kvantitativ datainsamling i form av enkätundersökning. Undersökningens mål är att kartlägga organisationers inställning till och intresse för biometrisk teknologi. Enkätundersökning ger en bättre och mer generell bild av organisationernas inställning och intresse än djupintervjuer. Det går att använda djupintervjuer, men för min studie passar enkätundersökningen bättre än djupintervjuer. Kartläggning och analys kräver att man samlar in en stor mängd information från en bred och representativ grupp. Med utgångspunkt från den insamlade informationen ger man sedan en generell bild av undersökningsområdet och verkligheten.

2.3 Datainsamling

Data delas ofta in i primärdata och sekundärdata. Primärdata samlas in genom till exempel enkäter, intervjuer och observationer. Sekundärdata är data som redan finns dokumenterade av någon annan, exempelvis i form olika källor. Källorna[5] kan klassificeras enligt följande:

- *Pappersbaserande källor omfattar litteratur, forskningsrapporter, konferensdokumentation, marknadsrapporter, organisationers interna rapporter, vetenskapliga artiklar, tidningar och tidsskrifter.*
- *Elektroniska källor finns på olika lagringsmedia såsom CD-ROM:s, DVD:s osv. och on-line (på Internet). såsom uppslagsböcker, databaser, webb-tv, videos, e-böcker osv. Sändningar i radio eller TV tillhör också denna grupp.*

Fördelen med sekundärdata är att insamlingsarbetet inte är lika tids- och resurskrävande som vid insamling av primärdata. Det kan vara en nackdel, att någon annan har sammanställt informationen, kanske med helt andra utgångspunkter för analys och tolkning. En annan nackdel med att använda sig av sekundärdata är, att viss information kan vara inaktuell. Detta gäller särskilt när det handlar om ny teknologi såsom biometri och biometriska teknologier som är ett område i ständig utveckling.

De sekundära källor som jag har använt mig av är litteratur, interna organisationers rapporter, vetenskapliga artiklar och olika tidningsartiklar. Det finns en hel del information på Internet som handlar om biometri, men endast ett fåtal böcker till hands på biblioteken. Jag har valt att göra en enkätundersökning för att få en bredare och djupare förståelse i undersökningen. Syftet med enkäten är att undersöka säkerhetspersonals uppfattning och inställning kring biometriska teknologier.

2.3.1 Reliabilitet, validitet och relevans

I forskningssammanhang används ofta begreppen reliabilitet och validitet. Validitet anger om en forskare undersöker det han/hon har tänkt undersöka, dvs. om en mätning mäter vad den ska mäta. Reliabilitet framställer hur väl undersökningens resultat stämmer överens med verkligheten. För ett gott resultat är det viktigt att forskaren väljer rätt person att fråga. Information som samlas in är relevant om resultatet skulle bli det samma vid en förnyad studie *(Halvorsen, 1992)*.

För att uppnå hög reliabilitet och validitet har jag valt ut personer, representativa för sin kategori, till att ingå i en webbaserad enkätundersökning. Avsikten med det är att öka sannolikheten för att enkäten verkligen mäter vad som avses, med andra ord att stärka validiteten.

[5] Thames Valley University, http://www.tvu.ac.uk/dissguide/hm1u2/hm1u2fra.htm

2.3.2 Webb-baserad enkät

En undersökning inom en stor begränsad grupp av människor kan göras med hjälp av intervjuer med, eller enkätundersökning till, en utvald grupp individer, som förmodas vara representativ för den population man vill undersöka. Med en enkätundersökning kan man samla in information om ett stort eller ett begränsat antal variabler. Frågorna i en enkät inleds oftast med vad, när, hur eller var *(Patel/Davidsson, 1994).*

En enkät är ett standardiserat frågeformulär baserat på kvantitativ teknik. Med hjälp av frågeformulär kan man få en sorts kvantitativa svar. Det finns två sätt att formulera sig kring enkät frågor. Det ena är öppna frågor, dvs. frågor utan givna svarsalternativ, där det är fritt fram för respondenten att formulera sig. Den andra är slutna frågor, där respondenten kan välja mellan ett eller flera givna svarsalternativ. Vid användning av den senare typen av frågor i en undersökning är det mycket enkelt att ta fram och sammanställa statistik, rita tabeller, diagram och dra slutsatser *(Holme & Solvang, 1997).*

Undersökningen är en typ av kvantitativ forskning, som syftar till att samla in data från ett urval av en publik. Undersökningen kan administreras via e-post och telefon till en målgrupp eller en potentiell grupp. En undersökning genomförs i fyra steg: identifiera målgruppen, skriva undersökningen, sköta enkätundersökningen och analysera datainsamlingen *(Mie-Yun Lee, 2002).*

Enkätundersökningen genomfördes under tiden 13 augusti – 5 oktober, 2003. Enkäterna skickades till säkerhetsansvariga i de utvalda företagen och organisationerna via en länk i e-post. Det var viktigt att enkäten skulle vara så enkel som möjligt att besvara, vilket är en förutsättning för att få en hög svarsfrekvens. Det finns alltid fördelar och nackdelar med den valda metoden. Jag kommer att redovisa dem i ”kapital 2.3.5 i kritisk analys av datainsamlingen”, där jag tar upp problem med att använda en enkätundersökning. I nästa avsnitt kommer en mer detaljerad redovisning av den webbaserade undersökningen och genomförandet.

2.3.3 Genomförande

Litteraturstudiens syfte är att ge kunskap om vilka begrepp som finns inom området och vad de har för betydelse. I teoriavsnittet presenteras en teoretisk genomgång och presentation av biometriska system, olika typer av biometriska tekniker och olika användningsområden, som tas till utgångspunkt för frågorna i enkätundersökning. Det finns inte tidigare undersökningar inom området. Det är i varje fall näst intill omöjligt att få tag på publicerade undersökningar att jämföra med och dra slutsatser från. Därför är det extra intressant att kartlägga de tillfrågade organisationernas inställning till användning av biometri och synen på biometriska teknologier.

I uppsatsen utförs en webbaserad enkätundersökning om biometri. I vissa studier kan en enkätundersökning via webben vara en lämplig datainsamlingsmetod för ett examensarbete. En förutsättning är man har tillgång till e-postadresser till respondenterna.

Enkäten består av 11 frågor där respondenten fritt kan välja och skriva in ett svar på frågan. Frågorna är hämtade från en webbsida[6]. Komplettering har gjorts med ytterligare frågor. I undersökningen används en webbaserad enkät, eftersom det blev mycket lättare och gick snabbare att nå ut till respondenterna på det sättet.

Efter att utformningen av enkäten var avslutad och respondenterna valts ut, så skickades enkäten till respondenterna via en länk i e-post. Respondenterna kunde sedan de fyllt i undersökningsformuläret trycka på ”skicka”, så skickades respondentens svar till en i förväg angiven e-postadress. När enkäten var genomarbetad och sammanställd skickades den ut till samtliga slumpvis utvalda 119 företagen via e-post. Frågorna handlade om organisationers förhållande till användningen av biometri. Ett kort inledande text medföljde enkäten (se bilaga). I brevet stod att svaren skulle hållas anonyma. Första omgången av enkäten skickades ut den 13: e augusti till de säkerhetsansvariga. En svarspåminnelse skickades ut efter cirka en vecka via e-post till dem som inte svarat och en andra påminnelse skickades ut efter drygt två veckor.

För att kunna fastställa de säkerhetsansvarigas uppfattningar av den nya teknologin, används till största delen olika frågor med svarsalternativ, i syfte att kunna mäta och åskådliggöra deras inställningar till frågor kring biometri.

De följande stegen förklarar hur webbundersökningen har gått till:

- Målet med enkätundersökningen klargörs under syftet i kapital 1.
- Identifiering av målgrupp som enkäten ska skickas till gjordes via Eniro´s webbkatalog (gula sidorna), där jag sökte med olika sökord beroende på vilken bransch eller vilket företagen det gällde. Först sökte jag på ordet ”säkerhet” i hela landet. Då fick jag upp 179 företag som sysslar ”med säkerhet - system, utrustning, konsulter”. Därefter gick jag in på deras hemsidor och sökte länkar till de säkerhetsansvariga på respektive företag. Jag sökte också på ordet ”vård”. Då kom 19 företag upp ”sjukhus, sjukhem”. Inom stora industrier och företag är det praktiskt taget omöjligt att hitta en länk till den säkerhetsansvarige, men vissa har en direkt länk. För att kunna täcka de flesta branscher har jag sökt på olika ord såsom utbildning, industri, vård mm. De flesta branscher har telefonnummer angivet. Vissa saknar hemsida och e-post. Det var enkelt att hitta en e-postlänk till säkerhetsansvariga personer inom vissa företag som hade en hemsida.
- Formulera frågorna till målgruppen, som är de säkerhetsansvariga i företagen i olika organisation. Testa webbfrågeformulären, så att frågorna kommer fram och hamnar rätt i min e-post adress.

[6]Inroad Consulting Inc, http://www.acap.net/survey.html

2.3.4 Kritisk analys av datainsamlingen

Det finns en uppsjö av information på Internet. Det viktig att kartlägga och granska informationskällorna kritiskt, vem har skrivit, i vilket syfte, vilken kvalitet är det på informationen. Datainsamling är en tidskrävande process framför allt inom ett ämne, om vilket det inte skrivits mycket. Det är enklare att använda sekundärdata primärdata eftersom datainsamlingen då blir mindre arbetskrävande.

Webb-baserad undersökning har sina för och nackdelar. En av de viktigaste fördelarna är, att man får hög representation. Nästan alla i en organisation har en e-post adress. Dessutom är kostnaden för att genomföra undersökningen ganska låg. Nackdelen med en sådan undersökning är att det opersonliga förhållandet till läsaren kan leda till att många slarvar med att svara, vilket leder till låg svarsfrekvens. Det kan finnas risk för att läsaren kan missuppfatta eller misstolka enkätfrågorna. Det går inte att rätt till frågorna i efterhand. Det är svårt att organisera och följa upp svar i en webbaserad undersökning. Några iakttagelser kring en webbaserad undersökning:

- Respondenterna som svarar på frågorna kan ha olika datorkunskapsnivå. Brist på den typen av kunskap kan leda till felaktigheter eller avviskelser.
- Webbaserad undersökning uppfattas inte som seriös av vissa medverkande. Därför avstå en del från att svara.
- Det kan finnas personer som ifrågasätter datasäkerhet, där den personliga integriteten också kan ingå.

Många avstod från att svara på frågorna. Ett särkilt var att många ville svara men svarade ändå inte. Det kan bero på någon eller några av ovannämnda punkter. Andra kritiska moment jag missade i den här undersökningen var att organisera en lista över deltagarna som medverkade i undersökningen. Detta ledde till svårigheter att kontrollera deltagarnas medverkan. Därför var jag tvungen att skicka frågorna upprepade gånger till en grupp företag.
Fördelen med att använda en enkät är att resultatet blir överskådligt och kan ge exakta svar. Problem som kan uppstå är att det är lätt för respondenterna att undvika att svara på vissa frågor och det kan även bli ett stort bortfall av svar. Detta gör att resultatet, trots upplägget, kan bli svårtolkat.

3. Teori

Detta kapitel handlar först och främst om teoretisk information kring ämnet biometriska system. Därefter kommer ett närmare klargörande av hur biometriska system fungerar, samt en introduktion av olika typer av biometriska teknologier. Vidare kommer jag att presentera användningsområden som är mer eller mindre väsentliga i samband med biometriska system. Slutligen diskuteras vad företag bör tänka på vid val av biometriska teknologier.

3.1 Från kunskapsbaserad till biometriska metoder

De flesta system som vi använder idag är baserad på kunskap, innehav eller ägande. Lösenord och passeringskort är exempel på kunskapsbaserad och respektive innehavsbaserad metod för inloggning och tillträdet till olika dataresurser och byggnader.

3.1.1 Kunskapsbaserad metod

En allmänt känd typ av kunskapsbaserad metod är lösenord som endast behörig användare känner till. Lösenord är den mest generella metoden vid autentisering med datorsystem. Det vanligaste sättet att autenticera är att varje användare har ett eget lösenord, som måste användas tillsammans med användaridentiteten för att man ska få tillgång till ett datorsystem. För att kunna uppnå en effektive säkerhetsmekanism måste lösenorden ägas personligen och därutöver bör verkligen hållas hemligt. Att grunda ett lösenord som är enkelt att komma ihåg men svårt att gissa är en väsentlig utmaning. *Lee Henry (1997)* hävdar att ett extremt viktigt problem kring lösenordssäkerhet är att samma lösenord ofta används till många olika system. Även ett starkt lösenord kan utsättas för attack. *RSA Security Inc (2001*) poängterar att lösenord är den svagaste metoden för autentisering. Historiskt har det påvisats att det är enkelt att gissa, lätt att glömma och stjäla ett lösenord. Ett annat problem är användarnamn och lösenord inte skyddar helt säkert, särskilt inte över Internet. Vidare anser *RSA Security Inc* att det inte räcker att enbart använda lösenord. Någonting som användaren vet är inte en adekvat säkerhetslösning. Ett exempel är att en typisk webbserver som grundar sig på http autentiseringssystem. Det används till många webbplatser, där användarnamn eller lösenord inte krypteras.

3.1.2 Innehavsbaserad metod

Användaren måste ha en fysisk sak, för att kunna autenticera sig i systemet. Token är den mest sprida metoden för att identifiera sig och få åtkomst till olika applikationer i ett datorsystem. Exempel på denna typ av metod är bankkort, passeringskort osv. Användaren har ofta med sig korten och det krävs under alla omständigheter fysisk närvaro. Token är kostnadseffektiv när den kombineras med kunskapsbaserad metod alltså lösenord. Användning av token kräver en omfattande organisation och administration. Token kan också tappas bort eller lånas ut så som lösenord *(Enrique J. Vargas, u.å).*

Smartkort kan ersätta den konventionella identifierings metoden med lösenord och verifiering av användaren via PIN nummer. Samma problematik, angående lösenord, gäller också vid användning av t ex av bankomatkort. Kortet utgör en personlig metod för autentisering, d.v.s.

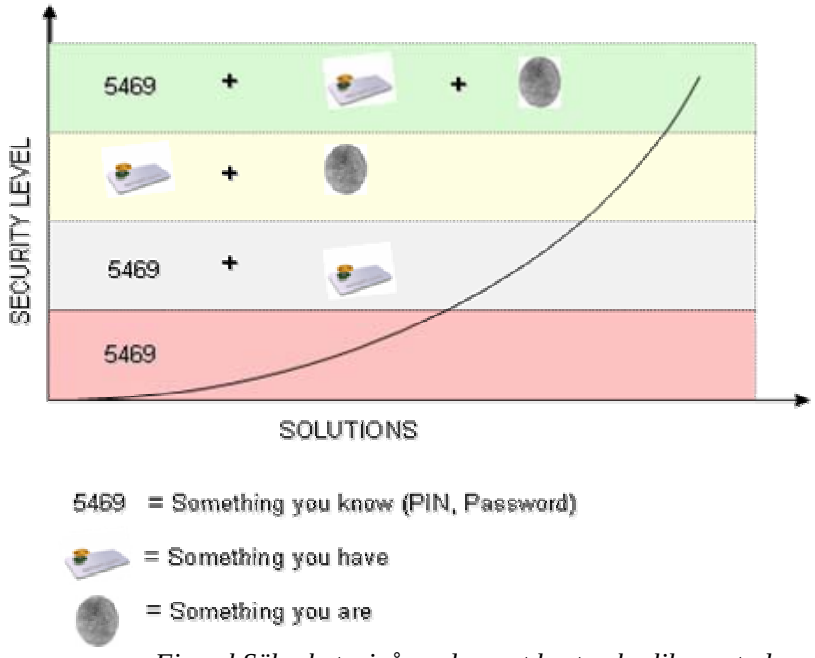
man använder kortet både för att bekräfta identitet och behörighet. Risken med kortet är när det tappas bort eller blir stulet. En annan central risk är att vem som helst kan komma åt koden på något sätt och sedan använda kortet. Obehöriga kan på det sättet använda och upprepa samma process. Det är också viktigt att kortet måste vara svårt att kopiera eller förfalska anser *S. Lee Henry, (1997).*

Den här typen av autentisering är betydligt starkare än den första kunskapsbaserade metoden, som enbart baseras på lösenord. Här ställs krav på att användaren ska presentera två identifikationsformer för inloggning eller tillträde till ett datorsystem, exempelvis måste användaren veta sin PIN kod och ha sitt kort t ex smartkort. Denna kombination visar att användaren vet och har någonting *(RSA Security Inc, 2001)*.

3.1.3 Biometrisk metod

Till skillnad från tidigare metoder, utgår man här från de fysiska egenskaperna hos en användare. För denna metod används unika mänskliga karakteristiska egenskaperna både för bekräftelse av identitet och av behörighet vid autentisering.

Fördelen med att använda en biometrisk metod är att den, till skillnad från traditionella metoder som lösenord, passerkort och koder, är mycket svår att förfalska eller kopiera. Biometrin medför mycket hög säkerhet om den kombineras med andra metoder t ex smartkort. Genom att kombinera någonting du vet med någonting du har och med någonting du är, kan betydligt högre säkerhet ernås. De tre metoderna enligt *Smart cards Alliance (2002)* kan kombineras med smart kort enligt figuren nedan:



Figur l Säkerhetsnivå med smart kort och olika metoder
Källa: Smart cards Alliance (2002)

Biometriska teknologier används med smart kort för identitetssystem applikationer särskilt för identifiering av människor. Då smartkortet skall användas för autentisering, lagras personlig information eller fingeravtrycket direkt på smartkortet i stället för på en databas eller på en server. Metoden baserade på ”vem du är” i stället för ”någonting du vet” som PIN- kod *(Smart cards and Biometrics 2002).*

3.2 Autentisering

Autentisering är en grundläggande aktivitet vid interaktion mellan människa och dator i datorsystem. En definition av. *Woodward J. D (2003):*

“Authentication may be defined as “providing the right person with the right privileges, the right access at the right time.”

Autentisering av användare är en väsentlig del av informationssäkerhetssystem. Med autentisering av användare menas att användaren får en identitet och ett lösenord, en metod som har använts i över ett decennium. För att kunna ge behörig tillgång till systemet måste användaren säkerställa sin identitet alltså traditionellt genom ett lösenord och en PIN (personligt identifikationsnummer). Denna metod hittills dominerat i nästan alla datorsystem.

En stark autentiseringsteknik ger emellertid högre grad av säkerhet, dvs. garanti för att en person är det hon uppger sig för att vara vid rätt tidpunkt. Biometri ger en helt ny på användareautentisering. Lösenord betraktas som den svagaste länken i ett säkerhetssystem och i ett nätverk. Organisationer kanske vill införa biometriska system i stället för lösenord. *Woodward J D, 2003* menar att pålitlig identifikation gör finansiella och andra verksamheter säkrare och effektivare genom att deltagare tar bättre ansvar för sina handlande. Enligt *(Woodward J. D. 2003)* och *(Nalini K, Jonathan H, Ruud M u.å),* finns det tre generella accepterade metoder för upprättande av användareautentisering:

Metod	Exempel	egenskaper
1. Någonting du vet	Lösenord Pin	Många lösenord är enkelt att gissa lätt att glömma
2. Någonting du har	Token (kontokort, passerkort) Nycklar	Kan lånas ut Kan gå förlorad eller tappas bort
3. Någonting du är	Fingeravtryck Iris Röst	Det kan inte att lånas ut Går inte att tappas bort Svårt att förfalska

Tabell. 1 Existerande autentiseringstekniker

Autentisering ska inte förväxlas med identifiering. Identifiering är att kontrollera att en person som uppger en viss identitet (namn, personnummer, användarnamn) verkligen är den personen. Autentisering är att kontrollera att identitetshandlingarna är äkta och att de inte är förfalskade, ogiltiga, återkallade eller spärrade.

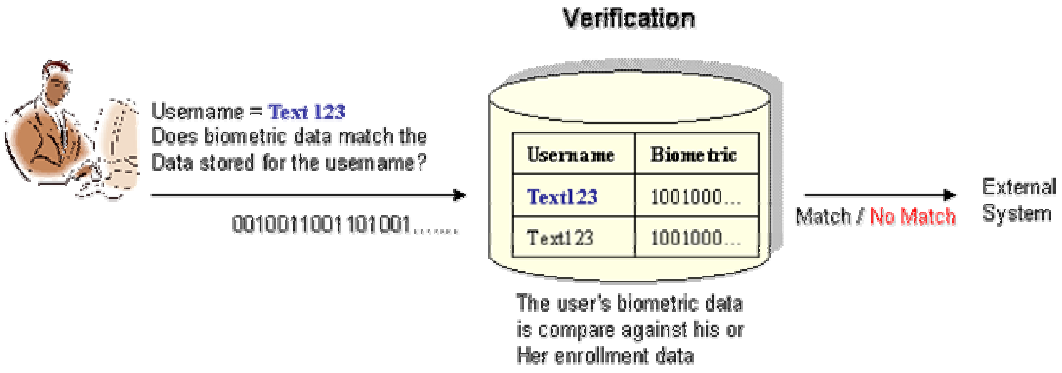
3.3 Biometri

Termen biometri används generellt för att beskriva, vetenskap, teknik och teknologier som har med mätning och analys av fysiologiska egenskaper och karakteristiska beteenden hos människan, framför allt för igenkänning eller autentisering. Enligt Nationalencyklopedin definieras ordet biometri som ”studiet av levande organismer med hjälp av matematisk-statistisk behandling av mätvärden”. Begreppet har följaktligen ett biologiskt underlag och bygger på att varje individ är unik. Medan Woodward J *(2003*), definierar biometri som automatisk igenkänning av kroppens unika kännetecken som fingeravtryck, iris, ögonbotten eller röst. Exempel på vanliga fysiska biometriska drag är fingeravtryck, handgeometri och ansiktsform. Exempel på beteendekaraktärsdrag är röst, eller signatur. Biometri är den teknik som används för att analysera unika mänskliga drag. Unika mänskliga drag lagras digitalt och används sedan för att identifiera individer på ett tillförlitligt sätt. Biometriska produkter och lösningar ersätter på så sätt PIN- koder, lösenord och nycklar. Med hjälp av biometriska säkerhetslösningar kan säkerhetsnivån höjas väsentligt, eftersom det är betydligt svårare att stjäla eller kopiera personliga data än koder, nycklar och lösenord.

3.3.1 Identifikation och verifikation

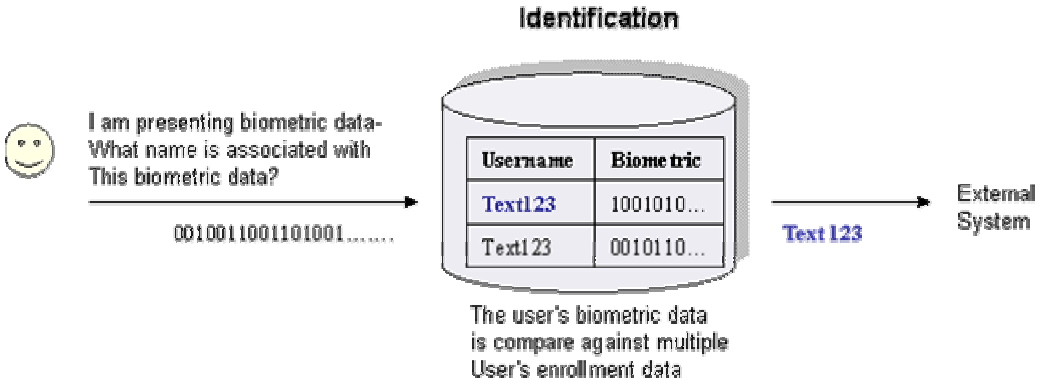
En organisation kan använda biometriska teknologier för två olika ändamål, identifiering och verifiering. Verifiering är när systemet försöker svara på ”är denna X”. När biometri används för att verifiera individens identitet, kräver systemet först input från användaren. Användaren kan hävda sin identitet genom lösenord, token eller användarenamn. I biometriska fall kräver systemet också biometriska prov från användaren *(Woodward J, med flera, 2001)*.

Med verifiering gör systemet en 1:1- sökning i en databas efter data/template som matchar eller stämmer överens med användarens tidigare registrerade data Genom verifiering bekräftas en användares påstådda identitet. Användaren lägger sitt finger på en



Figur 2 Verifikation
Källa: Nanavati S, 2002

fingeravtrycksläsare och hävder att han eller hon ”är X”. Systemet verifierar sedan detta påstående genom en enda biometrisk jämförelse mot tidigare registrerade data. Antingen påträffas en matchning mellan två eller inte. Verifikationssystem kan omfatta tusentals eller miljontals sammansatt biometriska datatyper *(Nanavati S, 2002).*



Figur 3 Identifikation
Källa: Nanavati S, 2002

Identifikation skiljer sig betydlig från verifikation. Identifikationssystem svarar på frågan ”vem är X” och systemet försöker att identifiera individen bland ett urval av personer. Genom identifiering bestäms användarens identitet genom att användaren lägger sitt finger på en fingeravtrycksläsare. Systemet bestämmer därpå identiteten, ”X”, genom ett antal biometriska jämförelser mot en databas eller på ett smartkort, detta kallas 1:M sökning.

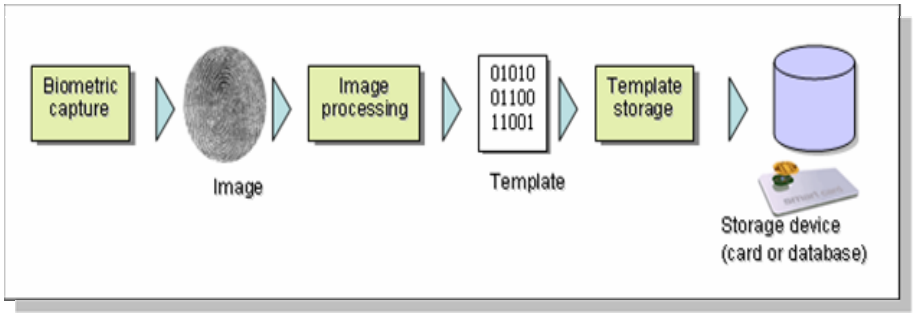
Det är ovanligt att möta ett specifikt problem i en organisation. För vissa användningsområden lämpar sig verifikation bäst och i andra fall identifikation. Nätverk och persondatorssäkerhet kräver ofta verifikationssystem, medan tillträde till byggnader och andra platser kan bli effektivast med antingen verifikations- eller identifikationssystem. För stora system med flera användare är verifiering effektivare då en sökprocedur inte genomförs (*Nanavati S, 2002).*

3.3.2 Biometriska huvudelement

Enligt *(Woodward J, med flera, 2001),* består alla biometriska system av följande tre huvudelement:

- Enrollment, eller biometrisk registrering som figur 4 visar, innebär att biometriska prov samlas från en person via en sensor (t ex för fingeravtryck), mikrofon (för röstverifiering) eller kamera (för ansiktsigenkänning). Därefter genereras template från det prov som har tagits genom extrahering *(Smart cards and Biometrics 2002).*

Normalt tar den biometriska hårdvaruenheten tre prover och sedan registreras genomsnittsdata med utgångspunkt från dessa. Det biometriska systemet använder algoritmer för att extrahera karakteristiska egenskaper från personers biometriska data och upprätta en biometrisk ”profil” *(Woodward J, med flera, 2001).*



Figur 4 Enrollment process
Källa: Smart cards and Biometrics (2002)

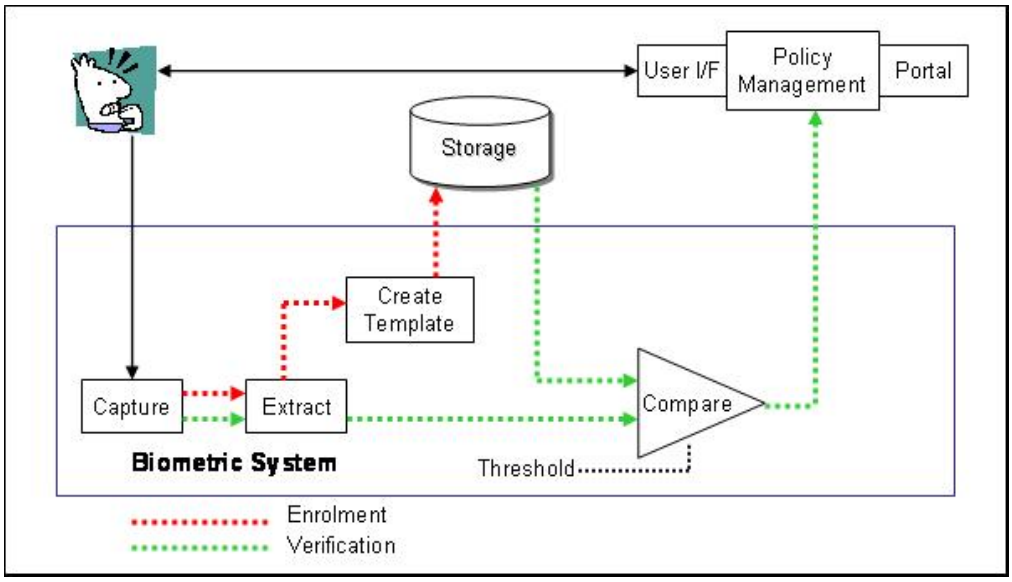
- Template, är den biometriska profilen omvandlad till digital form, som lagras på en lagringsmedia, och inte det biometriska attributet eller själva bilden t ex, av ett fingeravtryck. Formatet på template är ofta är litet och kräver inte stort lagringsutrymme. Därför går det att lagra template på ett magnetkort eller på ett smartkort. *(Woodward J, med flera, 2001)*

- Matchning, är den process som jämför två templates. Jämförelse mellan en levande template under registreringen med en eller flera redan lagrade templates t ex i en databas.

En förenklad bild av ett biometriskt system med informationsflöde kan beskrivas såhär: *Biometric Evaluation Methodology Supplement (2002)*:

Enrollment

- Capturing: (1) en sensor/avläsare läser av en kroppsdel eller ett beteende hos en användare;
- Extraction: (2) informationen behandlas och registreras digitalt i form av en biometrisk template.
- Storing: (3) template lagras i en stor databas, på en portabel enhet eller på ett smartkort.



Figur.2 Förenklad biometriskt system
Källa: Biometric Evaluation Methodology (2002)

Verifikation

- Capturing: (4) sensor/avläsare läser av en kroppsdel eller ett beteende hos en levande användare;
- Levande skanning av den valda biometrin;
- Extraction: (5) Biometrin omvandlas till en biometrisk template;
- Comparison: (6) Den skannade biometrin jämförs med lagrad template;
- (Non-)Matching: (7) Beslut om matchning för att kunna gå vidare.

3.4 Hur fungerar ett biometriskt system?

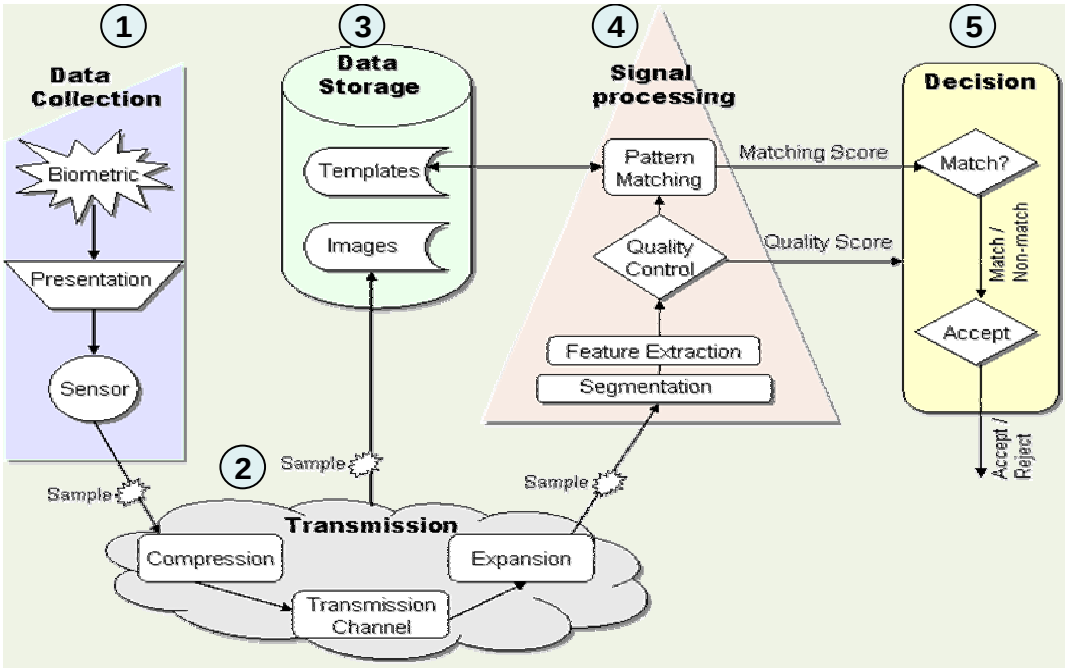
Alla säkerhetssystem kräver att användaren måste godkännas innan han/hon ska använda systemet. I biometriska system består autentiseringsinformationen av kroppens unika karaktäriska drag, som konverteras till digital kod och sedan lagras på en databas. För att kunna komma åt systemen skannas användarens kroppssärdrag och jämföras med tidigare data som finns lagrade i databasen. På samma sätt som vid användning av lösenordsystem, måste användaren ange rätt kod för att få tillträde till datorsystemet. Skillnaden är lösenordet ersätts med ett skannat kroppssärdrag.

Ett av de viktigaste skälen till att använda biometriska system, är förmåga att noggrant och med stor pålitlighet identifiera användaren. Biometrisk teknologi minskar gapet mellan mänsklig precision och maskinigenkänning. Ett grundläggande skäl för att använda biometri är individen identifieras tillförlitligt, noggrant, snabbt, bekvämt och inte minst till en låg kostnad menar *Woodward J (2003).*

Biometriska system kan utformas med olika komplexitet, utvecklingsmöjligheter och prestanda, men huvudbeståndsdelarna är de samma. Ett biometriskt identifikationssystem består av mjukvara, hårdvara och algoritmteknologi. Enligt *National Biometric Test Center* kan ett biometriskt system delas in i fem subsystem: datainsamling, överföring, datalagring, signalbehandling och beslut, se figur 3.

Datainsamling
Första steget i biometriska system är att kartlägga och registrera en individs karakteristiska fysiska egenskaper med hjälp av sensorer eller biometrisk avläsare. En avläsare kan exempelvis vara en kamera eller en mikrofon. För att kunna registrera individen i systemet måste han eller hon presentera sig för systemet levande. Sedan skapas en profil av individens karakteristiska fysiska egenskaper.

Överföring
En del biometriska system behandlar och lagrar data på olika ställen. Andra system använder en avläsare från vilken data skickas till en annan maskin för behandling och/eller lagring. Det kan också överföras till databasen för att lagras för senare användning. För ett sådant system krävs dataöverföring. Beroende på datamängd och kompression kan det vara nödvändigt med fördröjd överföring, lagring och användning. Figur 3 visar att kompression och överföring sker innan signalbehandling och profillagring. I sådana fall måste överföring ske och lagrade komprimerade data expanderas innan vidare användning. Vid komprimering och expandering kan signalkvaliteten gå förlorad under återställning *(National Biometric Test Center)*.



Figur.3 Ett generellt biometriskt system
Källa: A. J. Mansfield, J. L. Wayman 2002,

Datalagring
Det finns olika lagringsmöjligheter. Valet beror på systemets ändamål. De fysiologiska eller beteendemässiga kännetecknen till en profil kan lagras på en databas, vilken sedan används som referens vid jämförelse, när man försöker logga in vid senare tillfällen. Här lagras data som rådata, exempelvis ett mönster av ett fingeravtryck. Enligt *Woodward J (2003)*

Biometriska data kan lagras på följande ställen:

- Lokalt på avläsningsenheten.
- Centralt på en databas.
- På smarta kort. Denna lagringsmetod möjliggör för personen att bära med sig sin biometriska profil.

En säkerhetslösning avser Precise Biometrics fingeravtrycksläsare, som genom smartkort och fingeravtrycksidentifiering ökar säkerheten, när det gäller transaktioner över nätverk och inom myndigheter. Precise Biometrics ledande teknik för fingeravtrycksidentifiering och smartkort, kan användas som en dellösning för accesskontroll och autentisering.
(Precise Biometrics AB, 2003, Newsletter, No.1)

Signalbehandling
Signalbehandling kan ibland räknas till profilbehandling eller referensdata. Den består av en klass algoritmer som används för att modifiera störning i data eller för att skärpa till referensprofilerna. Signalbehandling består av provsegmentering, isolering och extrahering av relevanta karakteristiskt drag från data, som kapar biometriska template[7].
Datareferenserna lagras i databasen i form av template. Genom signalbehandling kan olika karaktäristiska template jämföras med varandra i databasen och sedan skickas en mått till beslutsystemet, som i sin tur avgör matchning eller den närmaste träffen *(Woodward J, 2003)*.

Beslut
Sista steget i biometriska system är när applikationen tar hänsyn till signalbehandlingens resultat som anger grad av kvalitet och matchning och fastställer ett ja- eller nej-beslut, se figur 3. Matchning eller avvisningsbeslut är baserat eller beror på systemets policy *(Woodward J 2003)*.

[7] I ett template lagras den data som används som mall vid jämförelser.

3.5 Biometriska typer

I boken *Intelligent Biometric techniques in Fingerprint and face*, klargör författarna karakteristiska och fysiska egenskaper hos individer, som kan användas för att identifiera personer, så länge de uppfyller följande krav *(L. C. Jain 1999)*:

- Universality, allmängiltighet, innebär att alla individer måste ha det specifika karaktärsdraget.
- Uniqueness, unikhet, som indikerar att två individer inte får ha samma karaktärsdrag och att varje individs karaktärsdrag måste vara unikt.
- Permanence, permanens eller beständighet, innebär att karaktärsdraget inte får förändras med tiden.
- Collectability, innebär att karaktärsdraget ska kunna mätas kvantitetsmässigt.

Detta kapitel grundas på boken *"Biometrics: identify verification in a Networked World"* av *Nanavati S, 2002).* De ledande biometiska teknologierna använder fingeravtryck, ansikte, iris, röst, handgeometri, näthinna och signaturer. *Nanavati S, 2002* menar att var och en av de teknologier, som baserar sig på igenkänning av olika personkarakteristika, har sina styrkor och svagheter. De kan också vara mer eller mindre lämpliga i olika sammanhang.

3.5.1 Fingerskanning

Fingerskannings teknik utnyttjar särskiljande fingerssärdrag (feature) för att identifiera eller verifiera individer. Fingerskanningsteknik betraktas som den mest generella metoden av de biometriska teknologierna. Den har utvecklat sig på bred front och används för fysiska och logiska access applikationer. Det finns en rad underleverantörer som konkurrerar i detta marknadssegment och erbjuder olika hårdvarauenheter, mjukvara och standardlösningar. Fingerskannings styrka är:

- En utvecklad teknik som har visat prestanda för hög nivå av tillförlitlighet och noggrannhet.
- Det kan användas inom ett brett område.
- Enkelt att använda och hantera hårdvaruenheterna.
- Registreringsmöjlighet för multipla fingers som ökar systemets tillförlitlighet.

Svagheter med Fingerskannig är bland annat:

- De flesta hårdvaruenheter lämpa sig inte för en liten del av en användare.
- Prestanda kan försämras med tiden.
- Förknippa med juridiska användningsområden.

3.5.2 Ansiktsskanning

Ansiktsskanningsteknik använder karakteristiska kännetecken i individens ansikte för att verifiera eller identifiera individer. Ansiktsskanningsteknik spelar för närvarande en betydelsefull roll när det gäller användning av biometri vid 1: N identifikation. Ansiktsteknik används i samband med Id-kortsystem och i olika typer av kameraövervakningssystem.

Ansiktsskanningsteknik kan också användas för 1:1 verifikation både när det gäller fysisk och logisk accessäkerhet.
Styrkan med ansiktsskannig är bland annat följande:

- Det går att göra sökningar på statistiska bilder eller foto som finns på körkortet.
- Den enda biometrin kan fungera utan användarnas samverkan.

Utifrån ett foto kan en mätning göras så, att man inte längre behöver personens närvaro när man läser av ansiktsformen.

Svagheter är bland annat:

- det kan vara en potential risk för missbruk av den personliga integriteten.
- Ändringar i fysiologiska kännetecknen kan minska matchningsprecision och noggrannhet.

Det finns andra faktorer som kan påverka systemets noggrannhet. Användarens ansikte måste hålla rätt vinkel mot kameran varje gång. Avstånd, belysningen och bakgrund får inte heller variera. Systemet blir ineffektivt när användaren registrerar sig på ett ställe och verifierar sig på något annat ställe. Ansiktsskanningar håller sig inte så relativt stabila över tiden i jämförelse med fingeravtryck. Flera system som baseras på ansiktsskanning passar perfekt för att identifiera förbjudna personer, t ex på casinon och flygplatser.

3.5.3 Irisskanning

Irisskanning baseras på att utnyttja utmärkande egenskaper hos en individs iris för identifiering eller verifiering. Egenskaper runt ögat som tas med hjälp av en kamera förvandlas till digital data och är ett säker sätt att identifiera användaren. Tekniken kan användas inom högteknologiska säkerhetsområden med fysisk åtkomst till känsliga applikationer.
Styrkan med irisskanning är följande:

- Det finns potential för hög nivå av precision och noggrannhet.
- Kapabel till tillförlitlig identifikation samt verifikation.
- Håller sig relativt stabil över tiden.

Svagheter med irisskanning är följande:

- Det finns benägenhet till fel av typen (False Rejection), som innebär att användaren nekas åtkomst.
- Det kan kännas obehagligt med en ögon baserad metod.

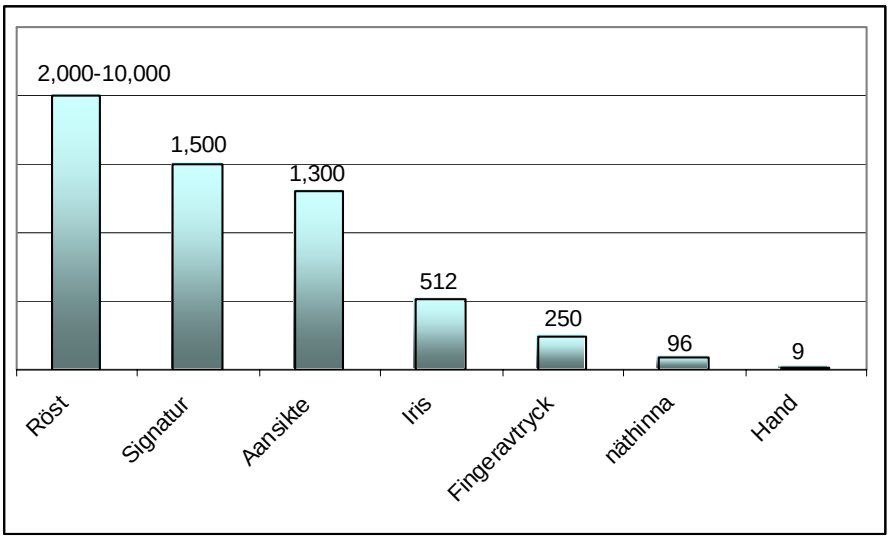
3.5.4 Röstskanning

Röstskanning bygger på utnyttjandet av karakteristiskt särdrag av rösten för identifiering och verifiering av människor. Röstskanning kombinerar element av både beteenden och fysiologisk egenskap.
Styrkan med röstskanning är följande:

- Hög acceptans i jämförelse med andra biometriska metoder.

Svagheterna med irisskanning är följande:

- Faktorer i omgivningen kan påverka ljudkvalitet, t ex störande ljud, fuktighet osv.
- Systemet ställer stora krav på storleken hos templates och är begränsat till vissa användningsområden.



Figur. 4 Biometriska template i förhållande till storlek i (byte)
Källa: Nanavati S, 2002

Röstskanningens template-storlek är betydligt större än handsskanningens, som figuren ovan visar, medan finger och iris templates sträcka sig mellan 250 bytes till 1kilobyte (1K).

3.5. 5 Handskanning

Handskanningsteknik utnyttjar särskiljande särdrag hos handen genom att analysera och mäta olika delar av handen för verifiering och identifiering av individer. Handskanning betraktas som en av de mest etablerade biometriska teknologierna och har användas i många år och i stor omfattning för verifiering där tusentals användare är involverade. Tekniken används för att kontrollera fysisk säkerhet och närvaro.
Styrkan med handskanning är följande:

- Handskannig är lätt att använda och upplevs inte så integritetskränkande.
- Tillförlitlig teknologi som kan användas i utmanade miljöer.
- Baserad på, över tiden relativt stabila, fysiologiska kännetecken.

Svagheterna med handskanning är följande:

- Handskanning har begränsad noggrannhet.
- Tekniken är begränsad till vissa användningsområden.

3.5.6 Retinaskanning (näthinna)

Retinaskanningsteknik drar nytta av särdrag i ytan i bakre delen av ögat både för identifiering och verifiering av användare. Tekniken används för kontroll av åtkomstsäkerhet ofta i högteknologiska och militära sammanhang.
Retinaskanning förväxlas ofta med irisskanning. Båda teknologierna hör till ögat. Det finns likheter när det gäller att använda referenser från ögat och deras noggrannhet. Algoritmer, hårdvara och mjukvarutillämpningar är dock mycket olika.
Styrkan med Retinaskanning är följande:
Hög noggrannhet

- Stabila fysiska karakteristiskt drag.
- Mycket svårt att lura systemet.

Svagheterna med retinaskanning är följande:

- Det är mycket svårt att använda
- Vissa användare kan känna det obehagligt att använda teknologi som baseras på ögat.

Bilden visar hur de olika teknologierna kan utnyttjas och vilken teknik som används mest. En studie från *International Biometric Group* visar marknadsandelar för olika biometriska teknologier och deras fördelning:

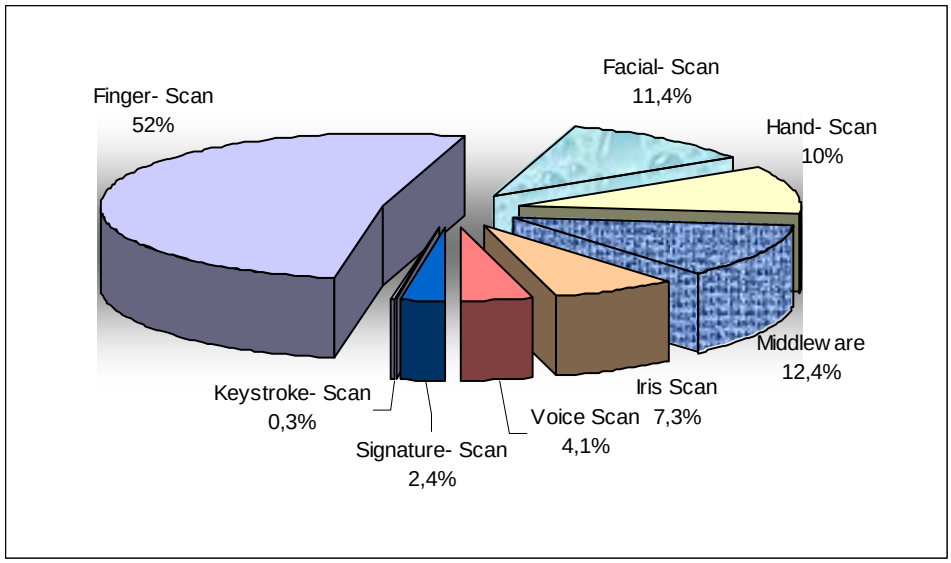


Figure.4 Biometric Market by Shared by Technology for 2003
Källa: International Biometric Group

Fingerskanning är den populäraste tekniken och har en marknadsandel på 53 %.
Ansiktsigenkänning har bara 11 % av marknadsandelen.

3.6 Biometriska applikationer

Biometriska teknologier skiljer sig fundamentalt åt på olika sätt när det gäller användningsområden, säkerhetsnivåer, användbarhet, krav, syfte och systemdesign. Biometri som används i bevakningssyfte skiljer sig betydligt från användningen i datortillämpningar och för datakommunikationssäkerhet. *Nanavati S (2002)* menar att för att kunna använda biometri effektivt bör man förstå det dynamiska behovet av den specifika tillämpningen.
Vidare delar han in biometriska tillämpningar i tre kategorier:

- Biometriska tillämpningar för **logisk access,** alltså åtkomst av data eller information.
- Tillämpningar för **fysisk access,** åtkomst av maskinell utrustning, material eller åtkomst till kontrollerade områden.
- Tillämpningar för biometrisk **identifiering** eller **verifiering.** Användarens identitet identifieras i databaser eller token.

Woodward J med flera (2001), menar att många verksamhetsområden i organisationer mer eller mindre kommer att bli involverade i biometri. Biometri används inom:

- Finansiella tjänster, som bland annat innefattar bankkort, kreditkort.
- Immigration och gränskontroll, (t ex, inresa, visum kontroll och asylansökningar).
- Sociala myndigheter, för att förhindra bedrägeri inom socialtjänsten.
- Sjukhus och läkarcentral, säkerhet kring båda personals integritet och patienternas journaler.
- Fysisk accesskontroll (t ex, till institutioner, myndigheter och bostäder).
- Tidsstämpling och tidrapportering. Systemet kan kontrollera områdesbehörigheter och kommer att ersätta den gamla stämpelklockan.
- IT- Säkerhet (t ex, PC- access, nätverkaccess, elektronisk handel och Internet användning).
- Telekommunikation (t ex tillämpningar inom mobiltelefoner, och telefonkort).
- Allmänna rättsväsendet, kriminella anstalter, fängelser, nationella identitetskort, röstkort, körkort och smarta pistoler.

Anil, J (2004), anser att traditionella kunskapsbaserade metoder som (t ex PIN och lösenord) används mest kommersiellt, medan myndighetsapplikationer använder innehavsbaserade metoder t ex ID kort, brickor och passerkort. Rättsväsendet har anlitat experter för biometrisk matchning. Biometriska system har utvecklats och ökat när det gäller civil användning.

Biometrisk teknologi används inom åtta olika sektorer. En marknadsundersökning visar följande förändringar i användning av biometriska system mellan mars 98 och december 99:

Applikation	December 1999	Mars 1998
Fysisk access	38.4%	52.8%
Rättsväsendet	19.2%	12.9%
Finans	17%	8.3%
vård	9.6%	10.8%
Immigration	5.3%	4.9%
socialhjälp	3.9%	4.1%
Datorsäkerhet	3.8%	4.1%
Telecom	2.8%	2.7%

Tabell. 2 Biometriska system och Marknadsutveckling, (Lockie M, u.å)

Applikationer inom fysisk accesskontroll dominerar fortfarande. Att marknadsandelen har sjunkit för fysisk accesskontroll från 52.8% 1998 till 38.4% 1999, beror på att andra användningsområden för biometri har ökat sina marknadsandelar. Den snabbast växande marknaden för biometri är de finansiella sektorerna, som har ökat betydligt från 8.3 % 1998 till 17 % under 1999. Den näst största tillväxten för biometri har skett inom rättsväsendet enligt tabellen ovan.

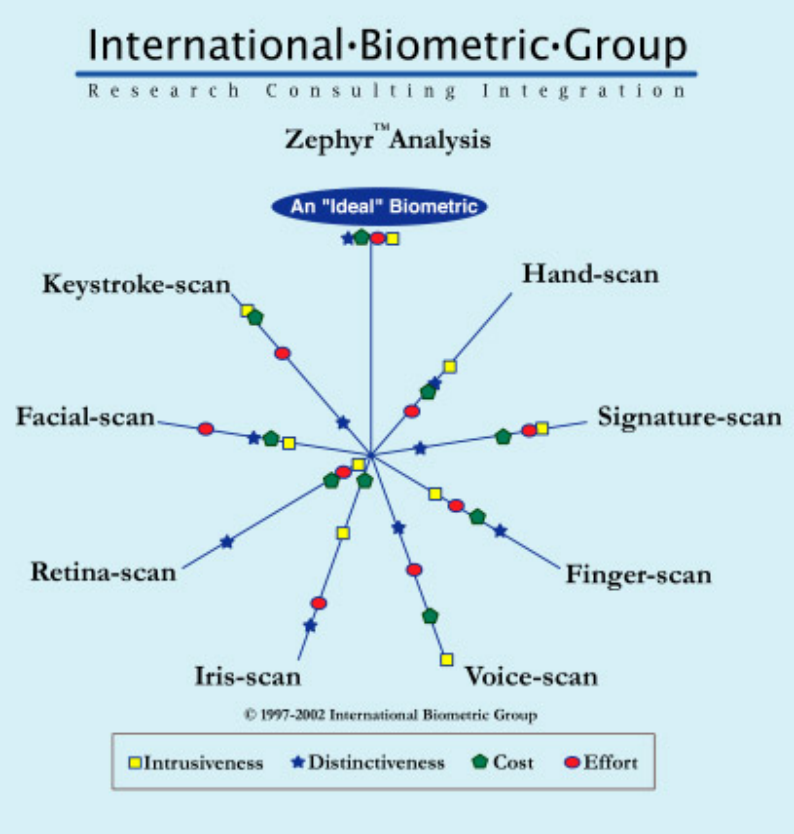
Precise Biometrics AB, levererar en säkerhetslösning med biometriska smartkort. De använder kortinnehavarens fingeravtryck som identifiering istället för eller som komplement till en PIN-kod. Systemet är i första hand tänkt för finansiella institutioner, statliga myndigheter samt inom hälso- och sjukvård.

3.7 Val av biometriska metoder

Val av biometrisk metod är ingen enkel fråga för en organisation. Det finns olika teknologier eller lösningar för olika användningsområden. Kostnad, komplexitet och användarvänlighet varierar mellan de olika biometriska metoderna. Biometriska lösningar används idag främst i passersystem och IT-säkerhetssystem för att ersätta traditionell identifieringsteknik såsom PIN-koder, lösenord och nycklar, men tekniken erbjuder även möjligheter för att utveckla helt nya tillämpningar och därigenom uppnå en högre säkerhetsnivå.

Dan Strassberg (*1998)* poängterar att man ska jämföra precision och noggrannhet mellan dessa teknologier. Vidare anser han att andra faktorer som är intressanta är att systemet ska vara lätt att använda och det ska accepteras av allmänheten. *International Biometric Group* anser att det är viktigt att tänka på vilken tillämpning som är mest noggrann, lättast att använda, enkel och billig att utveckla och billiga att introducera.

Diagrammet nedan visar en generell jämförelse mellan olika biometriska teknologier i term av ”lätt att använda”, ”kostnad”, ”noggrannhet” och ”uppfattas som inkräktande”. Symboler som visas för en ideal biometri är långt ifrån mitten av diagrammet. Trots att många försäljare har olika påståenden om biometri, så finns ingen generell bästa biometriska teknologi.
(International Biometric Group)



Zephyr diagram
Källa: International Biometric Group

Biometrisk teknologi är ett område IT- industrin inte har råd att ignorera menar *Liu S and Silverman M. (2001)* i sitt dokument. Biometri ger stora säkerhetsfördelar från IT- leverantörer till slutanvändare och från säkerhetsutvecklare till säkerhetsanvändare. Alla branscher måste utvärdera kostnads- och implementerings fördelar såsom säkerhetsmått.
Vidare anser han att olika biometriska teknologier kan lämpa sig för olika användning beroende på vilka behov användarna har och vilka de är, interaktion med andra system eller databaser, miljö förhållanden och andra specifika parametrar, såsom lätt att använda, felfrekvens, noggrannhet kostnad o.s.v. se tabell 3.

Characteristic	Fingerprints	Hand	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error incidence	Dryness dirt, age	Hand injury, age	Glasses	Poor Lighting	Lighting, age, hair, glasses	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very High	Very High	High	High	High
Cost	*	*	*	*	*	*	*
User acceptance	Medium	Medium	Medium	Medium	Medium	Medium	High
Required security level	High	Medium	High	Very High	Medium	Medium	Medium
Long-term stability	High	Medium	High	High	Medium	Medium	Medium

Tabell.3 Visar en jämförelse av olika biometriska metoder.
Källa: Liu S and Silverman M (2001)

En del av biometriska metoder kan lämpa sig för flygplatsmiljö mer än andra. Fingeravtryck, iris och röstigenkänning är bland de metoder som Londons flygplats har valt för sina 1,600 anställda. Flygplatser är ett område där det krävs hög säkerhet. Fysisk access till begränsade områden måste kontrolleras noggrant. *(Daon Newsroom, 2002)*.

4. Empiriska resultat och analys

Detta kapitel innehåller analys och konstruktion av diagram med utgångspunkt från insamlade data samt en redovisning av olika utskickssteg och svarsfrekvens. Tabellen nedan redovisar de olika stegen, som e-posten skickades ut i, med svarsfrekvens. Respondenterna har fått ett e-postutskick som innehåller en länk till webbformuläret. En påminnelse har skickats ut under undersökningen. En extra påminnelse har också skickats ut, för att öka svarsfrekvensen. Enkäten skickades ut till de säkerhetsansvariga.

Steg	**Svarsfrekvens**
Första e-post	*2%*
Första påminnelse	*2% +9%*
Andra påminnelse	*2% +9%+12%*

Undersökningen omfattar institutioner, företag och myndigheter. Totalt har 31 av 119 organisationer besvarat undersökningen, vilket ger en svarsfrekvens på 26 %. Val av institutioner och organisationer har inkluderat olika branscher. I vissa företag var det svårt att få ta tag på den rätta personen. Inom industrier finns vanligtvis inga e-postlänkar eller namn att kontakta på deras hemsida. Det gjorde det mycket svårt att komma åt den säkerhetsansvarige. Tabellen nedan förklarar fördelning av svarsfrekvens. Industriföretag och banker och uppvisar låg svarsfrekvens.

Informationsteknik:	**7**	23%
Industri:	**1**	3%
Bank och finans:	**2**	6%
Utbildning:	**8**	26%
Vård och Sjukhus:	**3**	10%
Övriga: Kommuner och myndigheter:	10	32%

Tabell.4 olika typer verksamhet

Nedan följer analys och diskussion av resultatet av enkätundersökningen:

1. Hur viktigt är det för din organisation att informationen i datorsystemet ska vara åtkomlig bara för användare med tillstånd?

Organisationen måste säkerställa datorsystemet och informationen som överförs, lagras eller behandlas i datasystem. Datorer ska skyddas mot intrång och otillåten användning av obehöriga. De flesta organisationer, alltså nästan 68 % tyckte att det är viktigt att informationen i deras datorsystem ska var åtkomlig endast för användare med behörighet. 32 % ansåg att det är mycket viktigt att informationen endast är tillgänglig för behöriga användare. Ingen organisation ansåg att det inte alls är viktigt eller inte så viktigt.

2. Vilken säkerhetsnivå anser ni är nödvändig för att framställa organisationens säkerhetsbehov?

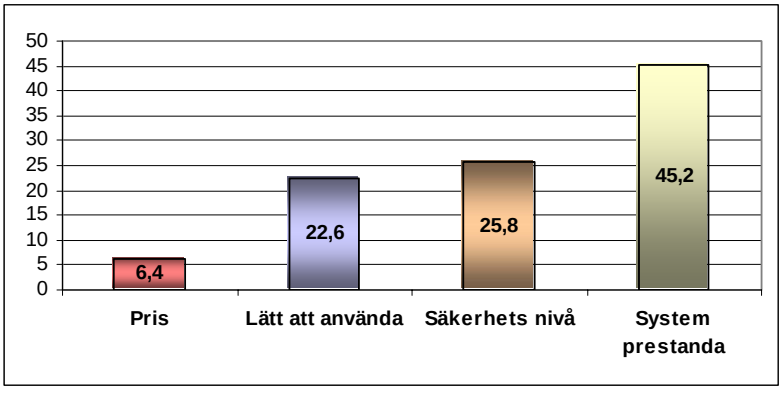
61 % tyckte att ”hög säkerhetsnivå” är nödvändig för att säkerställa en organisations säkerhetsbehov. 39% ansåg att det är krävs ”mycket hög säkerhetsnivå”. Säkerhetsnivåer utformas olika från företag till företag. Oftast sker det med utgångspunkt från organisations mål och riktlinjerna för IT-säkerheten. Säkerhetsnivåer och säkerhetsbehov beslutas av den som är ansvarig för IT-säkerheten i organisationen eller för systemet.

3. Den vanligaste metoden för autentisering är användarnamn och lösenord. Hur viktigt är det att säkerställa användarnas tilltillträde i organisationens intranät?

58 % ansåg det är viktigt. 42 % tyckte att det är mycket viktigt att säkerställa användarnas tillträde i organisations intranät. Intranät används som intern kommunikationskanal och varje organisation har är en målsättning med användningen av sitt intranät. Erfarenheterna visar att det finns olika metoder för att styra användarnas tilltillträde i organisationens intranät. Det beror på organisationens säkerhetspolicy, klassificering av information och användare samt beslut om vem som ska ha tillträdet till vad! Som regel ska det finnas riktliner för verksamheten i ett intranät. Dessa ska baseras på det specifika syftet med informationshantering inom organisationen.

4.1 Vilken är den viktigaste faktorn som påverkar ditt val vid anskaffning av specifikt autentiseringsprogram?

45 % av organisationerna ansåg att systemprestanda är den viktigaste faktorn vid anskaffning av ett specifikt autentiseringsprogram. 26 % o ansåg att säkerhetsnivån respektive 23 % lättanvändbarheten är viktiga faktorer vid anskaffning av ett autentiseringsprogram. Endast 6,4% ansåg att priset är viktigt.

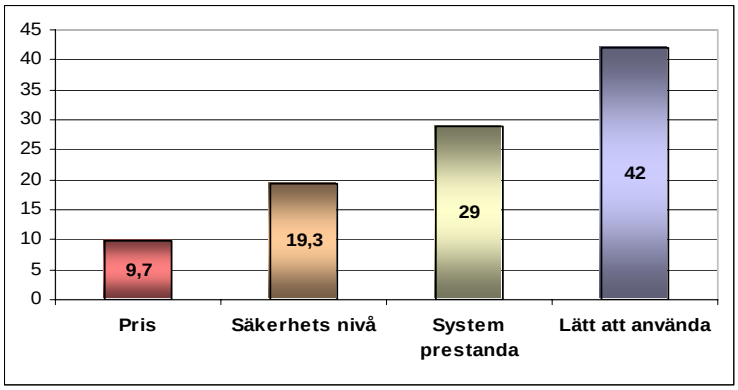


Figur 4.1 Faktorer som påverkar vid val av autentiseringsprogram

Trender inom biometri kommer att göra det nödvändigt att säkerhetsansvariga vidareutvecklar sitt systemkunnande. De ska kunna anpassa systemprestanda, säkerhetsnivå, pris och

lättanvändbarhet till biometrins krav. Valet av biometribaserat autentiseringsprogram är härvid viktigt. I kapital 3,7 beskrivs mer detaljerat de olika biometriska metoderna och hur de påverkar de nämnda faktorerna.

4.2 Vilken är den nästa viktigaste faktorn som påverkar ditt val av vid anskaffning autentiseringsprogram?

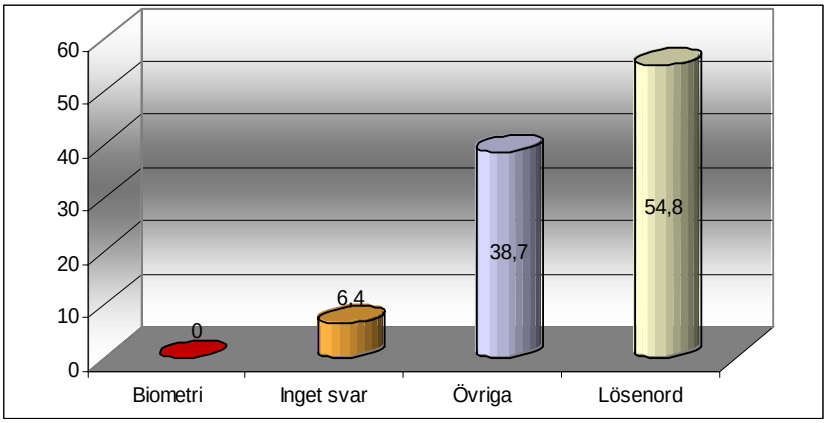


Figur 4.2 Faktorer som påverkar val av autentiseringsprogram

Näst viktigaste faktor som påverkar val av autentiseringsprogram ansåg 42 % vara att programmet ska vara lätt att använda, medan 29 % tyckte att systemprestanda är näst viktigast. 19 % satte säkerhetsnivå och10 % pris på andra plats. Se kapital 3.7

5. Vilken typ av autentisering/ säkerhetssystem använder ni för närvarande?

Lösenord är fortfarande det vanligaste sättet för användare att autentisera sig med systemet. De flesta system idag är baserade på kunskapsbaserad och innehavsbaserad metod, såsom beskrivs i kapitel 3. Lösenordsanvändning dominerar med 54,8 %. I kombination med andra token i organisationen: 38,7 %. 6,4 avstod att svara på frågan på grund av säkerhetsskäl. Identifiering som enbart bygger på en faktor, dvs. användaren identifierar sig genom att bevisa att han kan rätt lösenord, har visat sig vara en osäker metod. Av undersökningen att döma använder ingen biometri idag. Det stämmer inte riktigt med verkligheten. Två ledande företag som utvecklar biometriska teknologier har avböjt att medverka i undersökningen. Jag kommer i fråga 10 att redogöra mer detaljerat för orsaken till det. De två svenska företagen utvecklar båda programvara och hårdvara för biometri och har uppmärksammats stort internationellt. Båda företagen har flera pågående stora projekt, patentansökningar och förestående lanseringar av nya produkter.



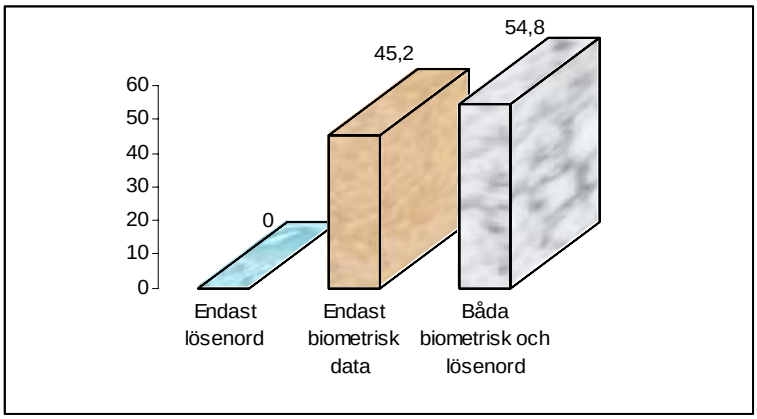
Figur 4.3 Användning av autentiseringssystem för närvarande

Trots säkerhetsadministratörers instruktioner om hur användarna ska välja svåra lösenord med olika kombinationer har tekniken med lösenord visat att den är sårbar. Det är mycket lätt att gissa sig till lösenorden med hjälp av olika krackningsprogram även om lösenord krypteras och sparas på en lösenordsfil. Att administrera lösenord kräver också ofta stora underhållsinsatser, vilket medför stora kostnader för organisationerna. Lösenord som används över Internet är inte heller helt säkra. De kan snappas upp från nätet med hjälp av snifferprogram. Författaren har själv konstaterat att så är fallet, vilket utvecklas mer i kapitel 3.1

6. Vilken typ av verksamhet bedrivs i din organisation?
Se tabell 4

7. Kommer ni att använda eller anskaffa användarebaserade system enbart med biometrisk identifikation, endast lösenord verifikation eller både och?

Alla organisationer strävar klart och tydligt efter att inte använda enbart lösenord. Figuren nedan visar att 54,8 av organisationerna ville använda både biometri och lösenord vid identifiering medan 45,2 % vill använda enbart biometrisk data. Det är inte lätt att kunna analysera hur organisationer kommer att använda biometrisk identifikation i framtiden. Det beror dels på vilken typ av verksamhet och användningsområde organisationen bedriver och dels på vilken säkerhetsnivå som krävs. En annan viktig faktor är hur pass insatt den säkerhetsansvarige är i biometri och dess tekniker och möjligheter.

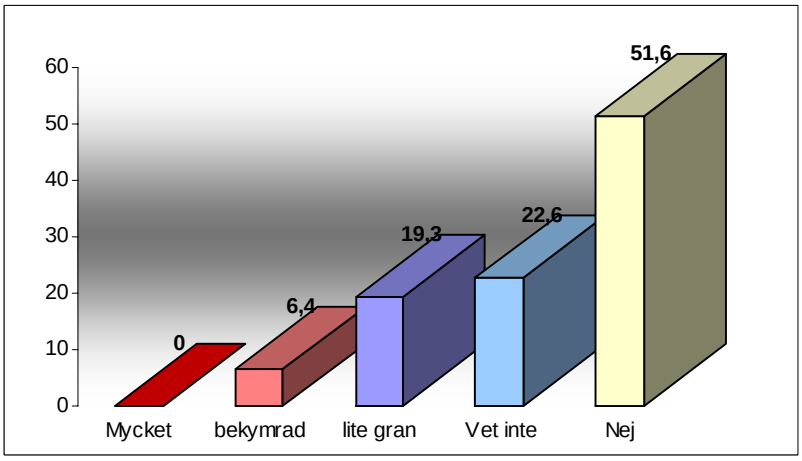


Figur 4.4 System kommer att baseras på olika autentiseringsmetoder.

I stället för biometri och lösenord går det att kombinera olika biometriska metoder. Då kallas det för multipla system. Att använda multipla system höjer säkerhetsnivån betydligt. Det går t ex att kombinera fingeravtryck med ansiktsigenkänning för verifiering och identifiering av användare. Det går även att kombinera med smartkort. Se kapitel 3.1 och 3.3

8. Är ni bekymrad över att använda biometrisk teknologi i din organisation?

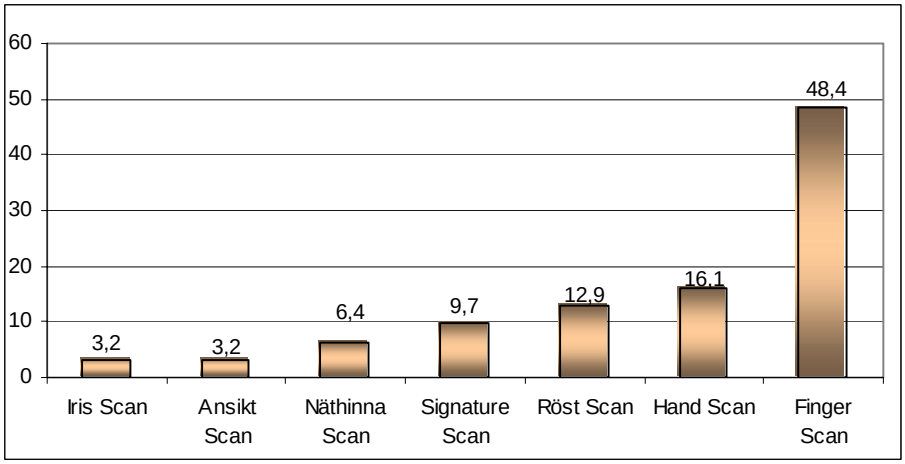
Återigen det är inte lätt att finna de faktorer som kan påverka organisations engagemang för respektive motstånd mot biometri. Vissa organisationer såsom myndigheter och statliga organisationer kan påverkas av beslut från EU. Ändå visar undersökningen att mer än hälften av organisationerna inte är tveksamma. Bara 6,4 tvekar inför att använda biometrisk teknologi. Det kan dels bero på att har tekniken inte ännu hunnit sprida sig på bred front i Sverige och dels på att inte många har tillräcklig kunskap om teknologin, bortsett från vissa ledande svenska företag, som är involverade i biometriutveckling och några andra som är på gång att testa biometriska system.



Figur 4.5 Engagemang för användning av biometrisk teknologi

9. Vilken typ av biometriska teknologier eller metoder föredrar ni?

Att välja vilken typ av biometrisk teknologi man föredrar är svårt, speciellt om man inte själv involverad i någon. Många faktorer behöver också övervägas vid anpassning av tekniken till verksamhet och användare. Det kan kännas kränkande att lämna ifrån sig ett fingeravtryck eller rikta en laserstråle mot ögat för att registrera användaren i systemet. Den personliga integriteten är mycket viktig att ta hänsyn till. Fingerskanning föredras av de flesta organisationer, 48,4 % fördrar fingerskanning. Det är enkelt att använda fingret och metoden är den äldsta av alla biometriska metoder. Iris och ansiktsigenkänning är ovanligt för allmänheten. Därför det inte konstigt att bara 3,2% respektive 6,4% föredrar iris- respektive nätthinneteknik.



Figur 4.6 Procentuell fördelning mellan olika biometriska teknologier

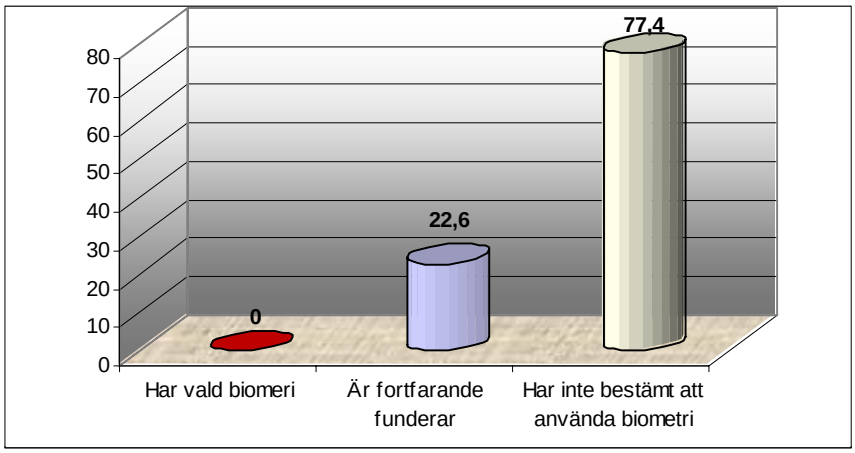
Att 48,4 % har valt fingerskanningsteknik kan också bero på, att den har hög acceptansnivå hos användare. Fördelen med fingerskanning är, att den är sprid och billig på marknaden och fingeravtryckets mönster är stabilt över en längre tid, jämfört med till exempel röst eller ansiktsform. I kapital 3.5 och 3.7 skrivs mer om för- och nackdelar med respektive teknik.

10. Var snäll och ange om ni:

Tyvärr ville de två ledande företagen Finger Print Card respektive Pricer Biometric AB, inte delta i undersökning. Orsaken är att de är involverade och utvecklar tekniken och därför inte vill lämna några yttrande i undersökningen. Dessutom betraktar de konkurrens- och marknadsläge som mycket känsligt. Pricer Biometric AB i Lund är redan involverat i många utvecklingsprojekt och har bidragit till biometriska installationer i skolor i Stockholm. Det skulle ha varit intressant om dom två företagen kunde ha bidraget med sina erfarenheter. Det skulle ha stärkt undersökningen om biometri.

I undersökningen är det 77,4 % av respondenterna som har bestämt sig för att inte använda biometri. Inget av företagen har valt biometri för identifiering. Detta undersökningsresultat är

lite missvisande, då några företag som sysslar med biometri valt att inte medverka i undersökningen.

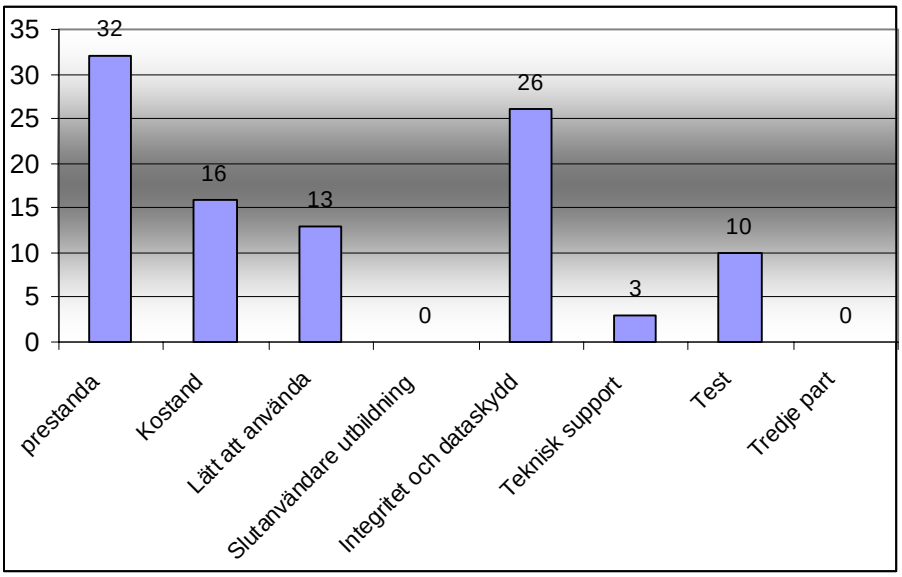


Figur 4.7 Organisationers inställning till biometri

Det är möjligt att den här undersökningen skulle ha gett ett annorlunda resultat efter ett år. Dels kommer tekniken att sprida sig och dels blir folk allt mer indragna i och medvetna om vad dessa teknologier innebär. Frågorna kan också i vissa fall ha upplevts komplicerade och besvärliga att förstå, så att utlovade 10 minuter inte räckt till för att besvara enkäten.
Michael Curry hävdar i sin rapport, att om biometri implementeras i en organisation kan man omedelbart inse effekterna i form av verkliga besparingar samt hög säkerhet för åtkomst inom många användningsområden. Vidare påpekar han att vi ska komma ihåg att 40 % av supportsamtal är lösenordsrelaterade *(Michael C, 2001).*

11. Vad anser ni att biometrisk industri ska behöva ta itu med i framtiden för att göra livet enklare?

Svaren är varierande och detta kan bero på vilken typ av verksamhets, hur många anställda och vilken säkerhetsnivå bedrivs i organisationen. Vissa företag föredrar prestanda och noggrannhet andra integritet och dataskydd. Fördelning över de faktorer som gör livet enklare är fördelas enligt tabell 4.8. Biometrisk industri är mer eller mindre involverat i de faktorerna och kommer att arbeta vetenskapligt för att utveckla metoder som gör att systemet blir enkelt att använda, skydda data/ och personligintegritet och hög prestanda till lågpris.



Figur 4.7 Olika fördelning över de faktorer som gör livet enklare.

5. Slutsats och diskussion

På senare år har intresset för biometri ökat, inte bara i USA utan även i Europa. Samtidigt pågår det omfattande utvecklingsarbete och forskning inom biometrins olika tillämpningsområden. Användning av biometri innebär att man vill förstärka både logisk säkerhet, för inloggning i arbetsstationer och nätverk och fysisk säkerhet för tillträde till byggnader som inpasseringssystem.
Biometriska system kommer att leda till stora förändringar i organisationers struktur. Vi får nya perspektiv på hur vi ska ta itu med dessa nya teknologier. Jag anser att det finns tre anledningar till att ett paradigmskifte ska inträffa. För det första har vi inte kunnat höja säkerhetsmåttet när det gäller IT-säkerhet. Vi har inte löst säkerhetsproblemen tidigare. Därför måste vi ändra vårt synsätt nu för att kunna lösa dessa problem. För det andra kräver omfattande kontokortsbedrägerier och identitetsstölder tillförlitligare och säkrare metoder. De traditionella metoderna kan inte säkerställa skyddet av informationen. För det tredje driver växande hotbilder intresset för att höja säkerhetsnivåer med hjälp av biometriska lösningar. Vi behöver nya teknologier eller verktyg som kan stödja oss för att kunna lösa säkerhetsproblemen och känna oss mer säkra. Biometri är den effektivaste metoden att motverka användandet av falska identitetshandlingar. Den syftar till att göra handlingarna säkrare och rättsligt bindande till den person som utför handlingen.

Enligt enkätundersökningen är mer än hälften intresserade av att använda både biometrisk data och lösen ord. Det är en indikation på att det finns intresse bland organisationer att använda biometrisk teknologi, även om undersökningen pekar på att bara 6,4 % bryr sig om biometri. Undersökningen har visat att nästan hälften föredrar fingeravtryck framför andra teknologier, medan bara 3% har valt irisigenkänning som metod. När organisationer ska välja vilken teknologi som kan vara lämplig för verksamheten är det viktigt att ta hänsyn först och främst till individens acceptans, dvs. om metoden accepteras av de flesta användare? Kommer denna metod att kränka den personliga integriteten? Andra faktorer som man bör ta hänsyn till och jämföra är systemets prestanda, tillförlitlighet, användbarhet och kostnad.

Behovet av biometri existerar klart och tydligt. Vi vet att enbart lösenord är en osäker metod. Det är också besvärligt för användarna att komma ihåg många olika lösenord för åtkomst av olika applikationer. Därför kan biometrisk teknologi bidra till *hög och effektiv säkerhet*. Biometrisk identitet är till skillnad från lösenord, koder och nycklar mycket svår att kopiera eller stjäla. Unika mänskliga drag kan inte glömmas eller tappas bort. För att kunna höja säkerhetsnivån ytterligare kan man kombinera olika biometriska metoder t ex en kombination av fingeravtryck med smartkort. Ett upphittat eller stulet smartkort är oanvändbart då det rätta fingeravtrycket saknas. Användning av biometriska system är mycket viktigt för varje organisation. Det skapar en säkrare och tillförlitligare koppling mellan användaren och handlingen, vilket kan bidra till högre säkerhet och effektivare system mot kontokortsbedrägerier och identitetsförfalskning.

Kostnadsreducering i form av besparning inom administrationen. Genom att använda biometriska metoder och identifiering av användare genom unika mänskliga drag, krävs endast en registrering som inte behöver uppdateras regelbundet eller bytas ut. Det reducerar de

administrativa kostnaderna väsentligt. Flera studier har visat att kostnaderna för lösenord och PIN administration betydligt högra än vid användning av biometri.

Skydd av personlig integritet. Säkerheten och skydd av personlig integritet förstärks genom möjligheten att lagra fingeravtryck på ett smartkort i stället för på en databas. Den lagrade mänskliga informationen, alltså biometriska lagrade data av den, lämnar inte kortet. På det sättet kan användarens integritet bevaras.

Säkerhet kräver ofta kompromissande mellan praktiska kostnader och övervägande av politiska och ekonomiska intressen. En riskanalys är viktig för att hjälpa organisationer att identifiera och sammanställa säkerhetsbehoven och överväga att utveckla biometriska system i stället för att förvalta befintliga system. Organisationer måste kunna identifiera målet med systemet samt kunna integrera och utveckla arbetsprocess, teknik, och användare för att kunna nå målet. Biometrisk teknik kan i princip användas i vilken verksamhet som helst i stället för lösenord. Politiska och ekonomiska beslut är två viktiga faktorer som kan engagera folk mer och få oss att förstå vad biometisk teknik innebär och hur den kommer att påverka oss. Ett bra exempel är när EU vill genomföra biometri och vill se fingeravtryck i svenska pass.
I fortsättningen vill EU därför att svenskar och andra medborgare ska bli tvungna att lämna sina fingeravtryck när de vill ha ut ett pass. Samtidigt kräver USA efter terrordåden 2001 att utländska pass ska inkludera biometrisk information. Hur kommer det att uppfattas att alla svenskar som vill ha tillgång till pass ska lämna fingeravtryck? Kan det uppfattas som ett stort intrång i den personliga integriteten? Det behövs diskussioner och seminarier på alla nivåer om hur dessa teknologier kommer att påverka oss nu och i framtiden.

Det är viktigt att biometrifrågor diskuteras i större sammanhang, ges mer publicitet och att ämnet biometri studeras på olika universitet och högskolor. Biometri är en teknologi som vi förr eller senare kommer att använda och den kommer att beröra oss alla och få många vardagliga användningsområden.

Avslutningsvis: Biometrisk teknologi är på frammarsch och kommer att växa snabbt beroende på det ekonomiska och politiska läget. Biometrisk teknologi kommer så småningom att ersätta de flesta system som är baserade på användarnamn och lösenord. Därför det är viktigt att företagen tar tekniken på allvar och börjar fundera över och överväga vad dessa teknologier kan bidra med och vilka konsekvenserna blir. Både myndigheter och företag inser betydelsen och fördelarna med biometri. Samtidigt måste vi komma ihåg eller inse att säkerheten inte kan nås enbart med teknik, utan samspelet mellan människor och teknik är det avgörande. Allt ska fungera tillsammans, som en del av hela säkerhetsprocessen.
Till slut vill jag poängtera att lämnar man ifrån sig ett fingeravtryck en gång, så går det inte att vare sig att byta eller radera.

5.1 Förslag till fortsatt forskning

Den tekniska utvecklingen inom biometri medför att de apparater som används för identifiering av individer kommer att vara kontroversiella. Varje individ måste lämna ifrån sig sitt fingeravtryck eller en bild av sina ögon eller iris osv. Den personliga integriteten kommer mer och mer att åsidosättas. Man tvingas att lämna ifrån sig sin unika identitet mot sin vilja.

Den personliga integriteten och privatliv vid användning av biometriska system är en viktig fråga att uppmärksammas i fortsatt forskning inom området.

6. Referenser

6.1 Litteratur

Backman, J. (1998). ”**Rapporter och uppsatser”**, Lund: Studentlitteratur.

Davide M, Dario M, Anil K, Salil Pr,(2003). ”**Handbook of Fingerprint Recognition**”. Springer Verlag Ltd.

Halvorsen, K. (1992), ”**Samhällsvetenskaplig metod**”, Lund: Studentlitteratur

Holme, I & Solvang, B. (1997). “**Forskningsmetodik, om kvalitativa och kvantitativa metoder**” Lund: Studentlitteratur.

Patel, R., Davidsson, B. (1994). ”**Forskningsmetodikens grunder: att planera, genomföra och rapportera en undersökning**” Lund: Studentlitteratur

Nanavati S., Thieme M. T, Nanavati R. (2002). “**Biometrics: Identity Verification in a Networked World”** John Wiley & Sons.

Wallén, G. (1996). “**Vetenskapsteori och forskningsmetodik**”, Lund: Studentlitteratur.

L. C. Jain, U. Halici, I. Hayashi, S. B. Lee, S. Tsutsui (1999).” **Intelligent Biometric Techniques in Fingerprint and Face Recognition**” USA. The CRC Press.

Woodward J. D, Orlans N. M, Higgins P. T, (2003).”**Biometrics: Identity Assurance in the Information Age**”. Osborne McGraw Hill,

Woodward John D., Jr, Horn C, Gatune J and Thomas A, (2003). “**Biometrics: A look at Facial Recognition**” RAND publication, Santa Monica,

6.2 www, artiklar

A. J. Mansfield, J. L. Wayman (2002).“Best Practices in Testing and Reporting Performance of Biometric Devices”. http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf

Anil, J Arun. R, Salil P. (2004)” An Introduction to Biometric Recognition”

Biometric Glossary. http://www.findbiometrics.com/Pages/glossary.html

Dahlbom, B. (1996). Göteborg Informatics ”Scandinavian Journal of Information Systems”, vol 7, nr 2. http://www.viktoria.se/~dahlbom/get/getContent.php3?style=../config/styleIEwin.css&language=swe&id=7&PHPSESSID=2aea3ec2d2641530d60bb3654f154614

Dahlbom, B. (1997). The new informatics. Scandinavian Journal of Information Systems, vol.8, No.2. http://www.viktoria.se/~dahlbom/get/getContent.php3?style=../config/styleIEwin.css&language=swe&id=7&PHPSESSID=2aea3ec2d2641530d60bb3654f154614

Dan Strassberg, (1998) Biometrics: You are your password
http://www.biometricaccess.com/company/n_050798.htm

Daon newsroom 200, http://www.daon.com/news/coverage/2002/1_12_02_lcr_bus_comm_aviat.htm

International Biometric Group’. http://www.biometricgroup.com/reports/public/market_report.html

Biometrics & Related technologies (2004)
http://www.securityatwork.org.uk/Biometrics%20Brochure%202004.pdf

Biometric Evaluation Methodology Supplement (2002)
http://www.cesg.gov.uk/site/ast/biometrics/media/BEM_10.pdf

Enrique J. Vargas u.å. “Introduction to Authentication”
http://www.jyestudio.com/labsec/docs/introauth.pdf

International Biometric Group. http://www.biometricgroup.com/reports/public/market_report.html

Inroad Consulting Inc, http://www.acap.net/survey.html

Lockie M. u.å. “Market developments and application examples of biometric systems”
http://www.igd.fhg.de/igd-a8/projects/biois/statements/lockie.pdf

Mie-Yun Lee, (2002) “Conducting Surveys and Focus Groups”
http://www.entrepreneur.com/article/0,4621,303380,00.html

Nalini K, Jonathan H, Ruud M. u.å. ”Secure User Authentication using Automated Biometrics”
http://www.assuredigit.com/tech_doc/more/ratha-sysj.pdf

N. K. Ratha, J. H. Connell, and R. M. Bolle (2001). ” Enhancing security and privacy in biometrics- based authentication systems” http://www.research.ibm.com/journal/sj/403/ratha.html

National Biometric Test Center. The Functions of Biometric Identification Devices. Biometric Publications
http://www.engr.sjsu.edu/biometrics/publications_tech.html

Precise Biometrics AB, (2003). Newsletter, No.3
http://www.precisebiometrics.com/data/content/DOCUMENTS/2003922105423185Newsletter_3_2003_final.pdf

Precise Biometrics AB, (2003). Newsletter No.1
http://www.precisebiometrics.com/data/content/DOCUMENTS/200343114743619Newsletter_Nr_1_2003.pdf

RSA Security Inc, (2001). Do You Know Who You're Doing e-business with?
http://www.rsasecurity.com/solutions/web/whitepapers/AUEB_WP_1100.pdf

SAS kundtestar biometri- lösning. (2003). http://www.compare.nu/news/index.asp?id=424

Liu S and Silverman M. (2001). A Practical Guide to Biometric Security Technology
http://ccrma-www.stanford.edu/~jhw/bioauth/general/00899930.pdf

S. Lee Henry. (1997)."Systems Administration". http://swexpert.com/C4/SE.C4.JUN.97.pdf

Smart cards Alliance (2002). Smart cards and Biometrics in.
http://www.securitymanagement.com/library/smartcard_biometrictech0802.pdf

Thames Valley University, http://www.tvu.ac.uk/dissguide/hm1u2/hm1u2fra.htm

Woodward John D., Webb K W., Newton E M, Bradley M, Rubenson D (2001). "Army Biometric Applications: Identifying and Addressing Sociocultural Concerns.
http://www.rand.org/publications/MR/MR1237/MR1237.ch2.pdf

Appendix 1

Biometrisk undersökning (2003)

Mitt namn är Sarbast Säran. Jag studerar informatik vid Göteborgs universitet. Du har blivit utvald till att medverka i en enkätundersökning med syfte att ta reda på om organisationer skulle behöva bättre system för att fastställa användareidentitet i samband med system access. Det finns intresse bland vissa organisationer för att använda biometri inom datorsäkerhetsområdet. Biometri definieras som samlingsnamn för olika tekniker som använder människokroppen som en del i en säkerhetslösning. Exempel är system baserade på ansikts-, fingeravtrycks och röstigenkänning, namnteckning, irisskanning och handgeometri mm. Många situationer i våra dagliga liv kräver autentisering, t.ex. bankbesök, inloggning i nätverk och fysiskt tillträde till datorsystem.

Att fylla i frågeformulären kan ta 10 minuter av din tid. Vi är mycket tacksamma om du vill ta dig tid att medverka.

Alla erhållna svar hålls konfidentiella.

i. Ditt namn _____
ii. Din befattning: _____
iii. Ditt företag:_____
iv. Din e-post: user@domain

1. Hur viktigt är det för din organisation att informationen i datorsystemet ska vara åtkomlig bara för användare med tillstånd?

- ☐ Mycket viktig
- ☐ Viktig
- ☐ Inte så viktigt
- ☐ Inte viktig

2. Vilken säkerhetsnivå anser ni är nödvändig för att framställa organisationens säkerhetsbehov?

- ☐ Mycket hög
- ☐ Hög
- ☐ Medel
- ☐ Ingen

3. Den mest allmänna metoden för autentisering är användarnamn och lösenord. Hur viktigt är det att säkerställa användares identitet vid tilltillträde till organisationens intranät?

- ☐ Mycket viktig
- ☐ Viktig
- ☐ Ganska viktig
- ☐ Inte viktig

4 4.1 Vilken är den viktigaste faktor som påverkar ditt val vid anskaffning av ett specifikt autentiseringsprogram?

- ☐ Lätt att använda
- ☐ Priset
- ☐ Säkerhetsnivå
- ☐ Systemetsprestanda

4 4.2 Vilken är den nästa viktigaste faktorn som påverkar ditt val av vid anskaffning autentiseringsprogram?

- ☐ Lätt att använda
- ☐ Priset
- ☐ Säkerhetsnivå
- ☐ Systemetsprestanda

5. Vilken typ av autentisering/ säkerhetssystem använder ni för närvarande?

- ☐ På grund av säkerhetsskäl avstår jag att svara på frågan
- ☐ Lösenord inloggning
- ☐ Hårdvara enhet baserad på biometri

Övriga (var snäll och specificera):

6. Vilken typ av verksamhet bedrivs i din organisation?

- ☐ IT bransch
- ☐ Industri
- ☐ Bank och finnas
- ☐ Utbildning
- ☐ Vård och sjukhus

Övriga (var snäll och specificera):

7. **Kommer ni att använda eller anskaffa användarebaserade system enbart med biometrisk identifikation, endast lösenord verifikation eller både och?**

- ☐ Enbart biometriska metoder
- ☐ Enbart lösenord
- ☐ Båda biometriska metoder och lösenord

8. **Är ni bekymrad över att använda biometrisk teknologi i din organisation?**

- ☐ Nej
- ☐ Lite gran
- ☐ Bekymrad
- ☐ Mycket bekymrad
- ☐ Vet inte

9. **Vilken typ av biometriska teknologier eller metoder föredrar ni?**

- ☐ Fingerskanning
- ☐ Irisskanning
- ☐ Anisktskanning
- ☐ Handskanning
- ☐ Näthinnaskanning
- ☐ Röstskanning

Övriga

10. **Var snäll och ange om ni:**

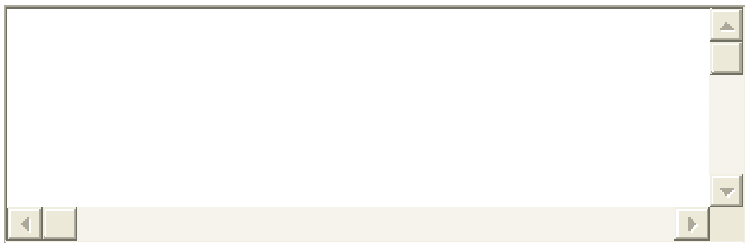
- ☐ Redan har valt biometri
- ☐ Fortfarande funderar kring specifik biometri
- ☐ Redan har bestämt att inte använda biometri

11. **Vad anser ni att biometrisk industri ska behöva ta itu med i framtiden för att göra livet enklare?**

- ☐ Noggrannhet och prestanda
- ☐ Kostand
- ☐ Lätt att använda
- ☐ Utbildning för slutanvändare

- Integritet och dataskydd
- Teknisk support
- Test
- Tredje part

Vid förslag frågor eller kommentarer kring biometrisk säkerhet var snäll skriv dem nedan:



kontakta mig via min e-post ssa275@hush.ai

Submit Reset

APPENDIX 2

Nedan följer en sammanställning av resultatet av biometrisk undersökning med säkerhetschefer och den säkerhetsansvariga på svenska storföretag.

Totalt 31 svarande, undersökningen genomfördes den 13:de augusti 2003.

---

1. Hur viktigt är det för din organisation att informationen i datorsystemet ska vara åtkomlig bara för användare med tillstånd?

Mycket viktig	32,2%
Viktig	67,7%
Inte så viktigt	
Inte viktig	

2 Vilken säkerhetsnivå anser ni att är nödvändig för att framställa organisationens säkerhetsbehov?

Mycket hög	38,7%
Hög	61,3%
Medel	
ingen	

3. Den vanligaste metoden för autentisering är användarnamn och lösenord. Hur viktigt är det att säkerställa användarnas tilltillträde i organisationens intranät?

Mycket viktig	41,9%
viktig	58,1%
Inte så viktigt	
Inte viktig	

4.1 Vilken är den viktigaste faktor som påverkar ditt val vid anskaffning av ett specifikt autentiseringsprogram?

Lätt att använda	22,6%
Priset	6,4%
Säkerhetsnivå	25,8%
Systemetsprestanda	45,2%

4.2 Vilken är den nästa viktigaste faktorn som påverkar ditt val av vid anskaffning autentiseringsprogram?

Lätt att använda	42%
Priset	9,7%
Säkerhetsnivå	19,3%
Systemetsprestanda	29%

5. Vilken typ av autentisering/ säkerhetssystem använder ni för närvarande?

På grund av säkerhetsskäl avstår jag att svara på frågan	6%
Lösenord inloggning	55%
Hårdvara enhet baserad på biometri	0%
Övriga (var snäll och specificera):	39%

6. Vilken typ av verksamhet bedrivs i din organisation?

IT bransch: **7**	23%
Industri: **1**	3%
Bank och finnas: **2**	6%
Utbildning: **8**	26%
Vård och sjukhus: **3**	10%
Övriga: Kommuner och andra myndigheter: **10**	32%

7. Kommer ni att använda eller anskaffa användarebaserade system enbart med biometrisk identifikation, endast lösenord verifikation eller både och?

Enbart biometriska metoder	46%
Enbart lösenord	0%
Båda biometriska metoder och lösenord	54%

8. Är ni bekymrad över att använda biometrisk teknologi i din organisation?

Nej	55%
Lite gran	19%
Bekymrad	10%
Mycket bekymrad	0%
Vet inte	16%

9. Vilken typ av biometriska teknologier eller metoder föredrar ni?

Fingerskanning	49%
Irisskanning	16%
Anisktskanning	13%
Handskanning	10%
Näthinnaskanning	6%
Röstskanning	3%
Övriga	3%

10. Var snäll och ange om ni:

Redan har utsedd biometri	0%
Fortfarande funderar kring specifik biometri	23%
Redan har bestämt att inte använda biometri	77%

11. Vad anser ni att biometrisk industri ska behöva ta itu med i framtiden för att göra livet enklare?

Noggrannhet och prestanda	32%
Kostand	16%
Lätt att använda	13%
Slutanvändare utbildning	
Integritet och dataskydd	26%
Teknisk support	3%
Test	10%
Tredje part	