**Biometriska säkerhetssystem – en studie av aspekterna säkerhet, integritet och användaracceptans**

**(HS-IKI-EA-04-609)**

**Johan Gustafsson (b00johgu@student.his.se)**
*Institutionen för kommunikation och information*
*Högskolan i Skövde, Box 408*
*S-54128 Skövde, SWEDEN*

Examensarbete i datavetenskap 10 poäng under vårterminen 2004.
Handledare: Lennart Börjesson

**Biometriska säkerhetssystem – en studie av aspekterna säkerhet, integritet och användaracceptans**

Examensrapport inlämnad av Johan Gustafsson till Högskolan i Skövde, för Kandidatexamen (B.Sc.) vid Institutionen för kommunikation och information.

2004-06-06

Härmed intygas att allt material i denna rapport, vilket inte är mitt eget, har blivit tydligt identifierat och att inget material är inkluderat som tidigare använts för erhållande av annan examen.

Signerat: _____

**Biometriska säkerhetssystem – en studie av aspekterna säkerhet, integritet och användaracceptans**

**Johan Gustafsson (b00johgu@student.his.se)**

# Sammanfattning

Det här arbetets syfte är att undersöka huruvida det är lämpligt för ett företag eller en organisation att införa ett säkerhetssystem baserat på biometri. Studien begränsades till att undersöka aspekterna säkerhet, integritet och användaracceptans eftersom dessa aspekter ansågs vara de som var viktigast och att de kunde undersökas på ett generellt plan. En ytterligare begränsning som gjorts är att för integritetsaspekten har endast svenska lagar studerats. Arbetet har genomförts i form av en litteraturstudie.

För säkerhetsaspekten har en översikt gjorts över biometriska systems säkerhetsfördelar och säkerhetsnackdelar i jämförelse med traditionella säkerhetsmetoder. Integritetsaspektens resultat är att den svenska personuppgiftslagen gäller vid behandlandet av biometriska egenskaper då dessa kan betraktas som personuppgifter. För användaracceptansaspekten så har olika undersökningar bearbetats med resultatet att det är viktigt att ett företag eller en organisation som vill införa ett biometriskt system tar hänsyn till vilken biometrisk metod som väljs och att ett förtroende skapas för tekniken.

**Nyckelord:** Biometri, Autentisering, Identifiering, Säkerhet, Integritet, Användaracceptans

# Innehållsförteckning

**1. Introduktion ..... 1**

**2. Bakgrund ..... 2**

2.1 Identifiering och autentisering ..... 2

2.2 Lösenord ..... 2

2.3 Biometri ..... 3

2.3.1 Biometriska tekniker ..... 4

2.3.2 Falska matchningar och falska avvisningar ..... 6

2.3.3 Multimodala biometriska system ..... 6

2.3.4 Säkerhet ..... 7

2.3.5 Integritet och användaracceptans ..... 7

2.3.6 Standarder ..... 7

**3. Problembeskrivning ..... 8**

3.1 Problemprecisering ..... 9

3.2 Avgränsning ..... 9

3.3 Förväntat resultat ..... 9

**4. Metod ..... 10**

4.1 Möjliga metoder ..... 10

4.1.1 Litteraturstudie ..... 10

4.1.2 Intervjustudie ..... 11

4.1.3 Enkätundersökning ..... 12

4.2 Val av metod ..... 12

**5. Genomförande ..... 13**

5.1 Planering av litteraturstudie ..... 13

5.2.1 Säkerhetsaspekten ..... 13

5.1.2 Integritetsaspekten ..... 13

5.1.3 Användaracceptansaspekten ..... 13

5.2. Genomförande av litteraturstudien ..... 13

5.2.1 Redovisning och värdering av insamlat material ..... 14

5.3 Redovisning av litteraturstudien ..... 15

5.3.1 Säkerhetsaspekten ..... 16

5.3.1.8 Svaga punkter i biometriska system ..... 18

5.3.2 Integritetsaspekten ..... 18

5.3.3 Användaracceptansaspekten ..... 20

**6. Analys ..... 24**
6.1 Säkerhetsaspekten ..... 24
6.1.1 Lösenord är lätta att lista ut ..... 24
6.1.2 Lösenord blir nerskrivna ..... 24
6.1.3 Lösenord lånas ut och andras lösenord används utan deras medgivande ..... 25
6.1.4 Samma lösenord på flera olika system ..... 25
6.1.5 Unika föremål kan tappas bort, bli stulna eller bli förfalskade ..... 25
6.1.6 Säkerhetsproblem med biometri ..... 26
6.1.7 Analys av resultatet för säkerhetsaspekten ..... 26
6.2 Integritetsaspekten ..... 26
6.2.1 Syfte och typ av personuppgifter ..... 27
6.2.2 Behandling av biometriska uppgifter inkräktar inte alltid på integriteten ..... 27
6.2.3 Analys av resultatet för integritetsaspekten ..... 27
6.3 Användaracceptansaspekten ..... 27
6.3.1 Medvetenhet om biometri ..... 27
6.3.2 Acceptans av olika biometriska metoder ..... 28
6.3.3 Tilltro till biometri ..... 29
6.3.4 Misstro mot biometri ..... 30
6.3.5 Analys av resultatet för användaracceptansaspekten ..... 30
**7. Slutsats ..... 31**
7.1 Säkerhetsaspekten ..... 31
7.2 Integritetsaspekten ..... 32
7.3 Användaracceptansaspekten ..... 32
7.4 Förslag till fortsatt arbete ..... 32
**8. Diskussion ..... 33**
**Referenser ..... 34**

# 1. Introduktion

Dagens samhälle kräver att vi som individer identifierar oss och autentiserar oss mer eller mindre dagligen, ofta flera gånger. Detta inkluderar alldagliga aktiviteter som att ta ut pengar från en bankomat, handla med olika rabattkort, logga in på arbetsstationer och stämpla in på jobbet.

Vanligen görs detta med en, eller flera i kombination, av följande metoder (Pfleeger, 2003):

- En unik kännedom om något,
- Innehav av ett unikt föremål eller
- Unika egenskaper hos individen.

Exempel på unik kännedom om något är traditionella lösenord och PIN-koder. För innehav av ett unikt föremål kan körkort, passerkort och pass nämnas som exempel. Och identifiering eller autentisering genom unika egenskaper hos individen är det som brukar kallas för biometri.

Metoder som använder biometriska egenskaper kan i sin tur delas in i två separata grupper. En grupp för de metoder som mäter en distinkt fysisk egenskap och en annan grupp för de metoder som mäter ett för individen unikt beteende (Rejman-Greene, 2001).

De traditionella identifieringsmetoderna är dock enligt Luis-García et al. (2003) osäkra till sin natur - Kort kan tappas och stjälas och det är lätt att glömma bort lösenord och de sistnämnda är dessutom möjliga att gissa sig till. Trots detta är den vanligaste identifierings- och autentiseringsmekanismen en kombination av ett inloggningsnamn och ett lösenord (Sasse, Brostoff & Weirich, 2001), där inloggningsnamnet är det som identifierar användaren och lösenordet är det som autentiserar användaren av just det inloggningsnamnet.

Som en eventuell ersättare, alternativt komplement, till de traditionella autentiserings- och identifieringsmetoderna har den biometriska tekniken utvecklats. Och vissa av de traditionella metodernas problem kan kanske lösas med hjälp av sådan teknik men biometritekniken har också sina egna svagheter (Bolle, Connell, & Ratha, 2002).

Det här arbetet syftar till att undersöka huruvida det för ett företag eller en organisation är lämpligt att införa ett säkerhetssystem baserat på biometri. Undersökningen begränsar sig till att studera aspekterna säkerhet, integritet och användaracceptans och har skett i form av en litteraturstudie. För säkerhetsaspekten kommer en översikt presenteras över vilka säkerhets-fördelar och säkerhetsnackdelar som biometriska system har och hur sådana system står sig mot traditionella säkerhetssystem. Integritetsaspekten ska studeras utifrån svenska lagar och regler för skydd av den personliga integriteten vid behandlandet av biometriska egenskaper. För användaracceptansaspekten kommer tidigare genomförda undersökningar presenteras, analyseras och jämföras.

Rapporten börjar med ett bakgrunds kapitel och en beskrivning av problemet följt av val av metod. Därpå beskrivs studiens genomförande och de resultat den ger. Efter detta analyseras resultaten för de olika aspekterna var för sig varpå en slutsats presenteras. Slutligen följer ett kortare diskussions kapitel där arbetet i sig diskuteras.

# 2. Bakgrund

I det här kapitlet kommer en del begrepp som är viktiga inom området att tas upp och vissa bakgrunds fakta om lösenord och biometri kommer att presenteras. Först klargörs skillnaden mellan identifiering och autentisering. Där på tas vissa fördelar och nackdelar med lösenord upp och efter det ges en bakgrund till biometritekniken.

## 2.1 Identifiering och autentisering

Identifiering är när ett säkerhetssystem ska avgöra vem en specifik individ är, det är alltså en 1:n (en-till-många) situation där personen i frågas identitet ska fastställas bland flera olika möjliga identiteter (Gifford, McCartney & Seal, 1999). När det handlar om autentisering enligt Gifford et al (1999), eller verifiering som det också kallas, är det istället en 1:1 (en-till-en) situation. Systemet ska alltså vid autentisering avgöra om den aktuella personen är den som han eller hon utger sig för att vara. Identifiering är mycket mer krävande än autentisering (Luis-García, Alberola-Lopez, Aghzout & Ruiz-Alzola, 2003).

De flesta säkerhetssystem använder sig av ett tvåstegssystem som kombinerar identifiering med autentisering (Sasse et al. 2001). Till exempel för att passera genom en dörr dras ett passerkort med en magnetremsa genom en kortläsare för att identifiera personen som vill passera. Där efter slår personen i fråga in en PIN-kod för att autentisera/verifiera sin identitet.

## 2.2 Lösenord

I den här rapporten kommer alla metoder som baseras på unik kunskap om något att benämnas som lösenord. Systemet med att använda sig av lösenord har fördelarna att det inte behöver någon särskild hårdvara och kan användas ifrån terminaler av vilken typ som helst så länge de är kopplade till målsystemet (Spafford, 1992). Dessutom är lösenordsystemet enkelt att förstå rent konceptuellt för både för användare och designare av system (Furnell, Dowland, Illingworth, & Reynolds, 2000).

Att lösenord kan vara ett dåligt skydd visades redan 1979 av Morris och Thompson då en dator kunde lista ut 86% av de 3289 lösenord som hade samlats in. Samma sak har gjorts om senare av Klein (1990) och Spafford (1992). Resultaten från Kleins undersökning är vid en första anblick lite mindre oroande än de som Morris (1979) kom fram till då bara 21% av de 15000 lösenord som insamlats kunde gissas på en vecka. Dock motsvarar det runt 3000 lösenord. Dessutom kunde 2,7% gissas redan under de första 15 minuterna vilket motsvarar 368 lösenord. Det intressanta är att dessa 368 lösenord bestod av användarens inloggningsnamn eller användarens eget namn. Spafford (1992) visade i sin undersökning att så många som vart femte lösenord kunde hittats relativt snabbt genom att alla ord i en ordbok provades med hjälp av en dator. I en något nyare undersökning där 1200 brittiska kontorsarbetare från 30 olika företag deltog framgår det att så många som 47,5% av de tillfrågade använde sig av sitt eget, en familjemedlems eller sitt husdjurs namn som lösenord, eller någon av dessas födelsedag (CentralNic, 2001). Trots detta ansåg endast 15% av de till frågade i en undersökning gjord av Furnell, et al. (2000) att deras lösenord var lätta att gissa sig till. Klein (1990) påpekar att det räcker med att ett användarkontos lösenord avslöjats för att en hacker ska kunna få fotfäste i ett system. Inget system är alltså säkrare än det svagaste lösenordet det har (Prabhakar, Pankanti & Jain, 2003).

En lösning på detta är att se till att systemet inte tillåter lösenord som är lätta att lista ut och att alla användare har lösenord av den hårdare typen (Klein, 1990). Det vill säga lösenord som består av minst 8 tecken och som inte är ett ord som finns i någon ordbok och har minst ett skiljetecken och där gemener och versaler är blandade (Klein, 1990). Problemet är att den

typen av lösenord är svårare att komma ihåg och detta leder i sin tur till att användarna istället skriver ner lösenorden på en mer eller mindre tillgänglig plats (Prabhakar et al. 2003).

I undersökningen som gjordes av Furnell, et al. (2000) visade det sig att så många som 40% av de tillfrågade använde samma lösenord på flera olika system. Om en inkräktare lyckats knäcka lösenordet för en användare på ett system är det därför ganska troligt att inkräktaren kan använda samma lösenord för den användaren på ett annat system (Furnell et al. 2000).

Problem som anses typiska för lösenord är att användare skriver ner dom, låter andra använda deras lösenord, glömmer av dom och väljer lösenord som är lätta att lista ut (Furnell et al. 2000). Autentiseringen är den svagaste länken i ett systems säkerhetsutformning men biometri kan i termer av rå styrka stärka den länken (Ratha, Connell & Bolle, 2003). Dessutom skriver Ratha, et al. (2003) att biometriska autentiseringsmetoder är att föredra framför användandet av lösenordssystemet eftersom de åtminstone erbjuder samma säkerhet men en bättre bekvämlighet för användaren.

## 2.3 Biometri

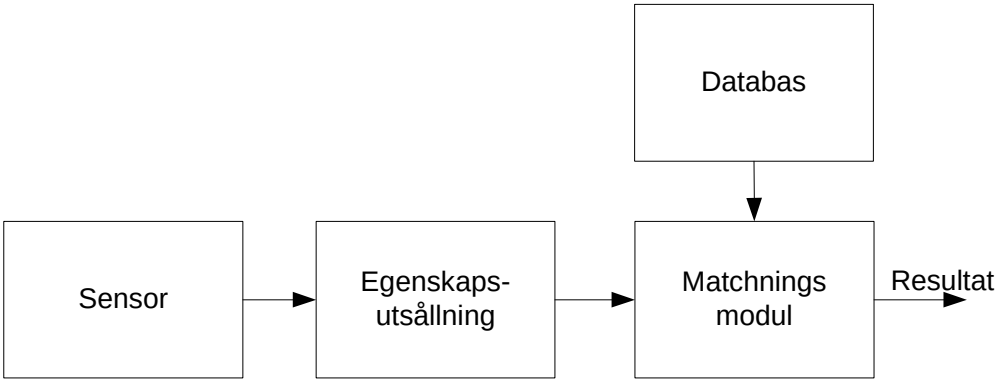
Tekniken för datoriserad biometrisk autentisering och identifiering har funnits ända sedan 70-talet men har inte varit praktiskt användbar tills för några år sedan på grund av att de biometriska systemen nu mera är nere på en rimlig prisnivå och tekniken är pålitligare, träffsäkrare och hållbarare (Matyas & Stapleton, 2000). Andra anledningar till att biometriska system tidigare inte haft så stor kommersiell framgång beror enligt Gifford et al(1999) på att det saknats social acceptans och att de tidigare systemen varit användarovänliga.

Den kanske mest kända biometriska tekniken är troligen fingeravtrycksavläsning och tekniken används redan i ett flertal tillämpningar. En annan teknik som också är populär är ansikts-igenkänning eftersom den anses vara den mest användarvänliga, men än så länge har tekniken inte lyckats uppnå någon hög träffsäkerhetsgrad. Men den teknik som för tillfället verkar var den mest träffsäkra är regnbågshinneigenkänning (Luis-García et al. 2003).

Enligt Matyas och Stapleton (2000) är ett biometrisk system ett automatiserat system som samlar, distribuerar, lagrar och bearbetar biometrisk data eller biometrisk information. Ett biometriskt system kan generaliseras till fyra olika moduler (Jain, Ross & Prabhakar, 2004):

1. Sensor – Denna del läser av den egenskap som ska mätas.
2. Egenskapsutsållning – Identifierar de unika egenskaperna på det som lästs in.
3. Matchning – Matchar de utsållade egenskaperna med de lagrade profilerna.
4. Databas – Den del där registrerade användares biometriska profiler lagras.

Figur 2.1 visar en modell över hur de olika modulerna relaterar till varandra i ett sådant generellt biometriskt system.




*Figur 2.1. En generell skiss över ett biometriskt system som visar de olika delarna i systemets inbördes relation (efter Ratha et al.2003, s. 2106).*

Ett biometriskt system är i grund och botten ett mönsterigenkänningssystem som känner igen en person utifrån specifika fysiska egenskaper eller utifrån ett specifikt beteende (Prabhakar et al. 2003). Rent teoretiskt går det att använda vilken som helst av de fysiska egenskaperna hos en individ för identifikation (Luis-García et al. 2003). Men hur lämpad en specifik egenskap är avgörs av följande variabler (Prabhakar et al. 2003):

- *Universalitet* – Alla måste ha den.
- *Särpräglighet* – Det måste finnas en distinkt skillnad för egenskapen mellan vilka två personer som helst.
- *Permanenthet* – Den måste vara oföränderligt i så stor grad som möjligt över tiden.
- *Insamlingsbarhet* – Egenskapen måste vara kvantifierbar.

Detta betyder att en idealisk biometrisk egenskap ska vara något som alla har, men som ingen har likadana av, som aldrig förändras och som går att läsa av i mätbara enheter.
Biometrisk identifikation utnyttjar det faktum att vissa beteenden eller fysiska attribut på ett pålitligt sätt skiljer en person från en annan (Matyas & Stapleton, 2000).
Jain, et al. (2004) skriver att det finns fler saker som måste tas hänsyn till i ett biometriskt system för att avgöra hur praktisk användbar en viss metod är:

- *Prestanda* – Vilken träffsäkerhet och hastighet som uppnås, vilka resurser som behövs för att uppnå den önskade hastigheten och träffsäkerheten och de yttre faktorer som påverkar så som till exempel arbetsmiljön.
- *Godtagbarhet* – I vilken grad användandet av den specifika biometriska egenskapen accepteras av de som ska använda systemet.
- *Överlistbarhet* – Som visar på hur lätt eller svårt det är att överlista ett system som använder sig av den biometriska egenskapen.

Av detta följer att ett biometriskt system bör vara så snabbt, resurskrävande och träffsäkert som specificerats, vara accepterat av dem som ska använda det och ofarligt för användarna, och vara tillräckligt skyddat mot bedrägerier och liknande (Jain et al. 2004).

### 2.3.1 Biometriska tekniker

Det finns ett flertal olika biometriska metoder och tekniker i dagsläget vilka befinner sig i olika stadier av utveckling. Det här kapitlet kommer att ge en kortare översikt över några av dessa. Värt att notera är att olika metoder och tekniker har olika möjligheter till användbarhet, dessa möjligheter förändras i takt med att de utvecklas och kommer inte att beskrivas närmare här.

- *Hand- och fingergeometri* - Metoden går ut på att handens geometriska attribut så som handflatans storlek och form och längden och bredden på fingrarna avläses (Jain

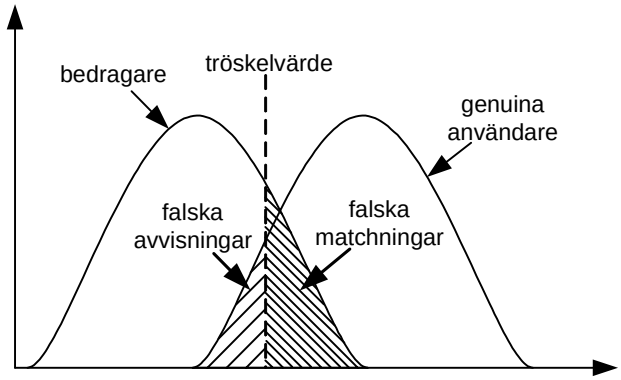
et al. 2004). Dessa attribut är efter en viss ålder i stort sett oföränderliga (Luis-García et al. 2003).

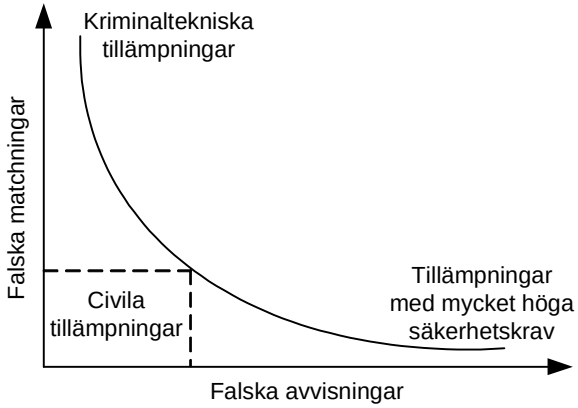
- *Ansiktsigenkänning* - Ansikten kan läsas av på flera olika sätt bland annat genom stillbilder och videoupptagningar (Luis-García et al. 2003).
- *Regnbågshinneigenkänning* - Regnbågshinnans vävnad formar ett för varje individ unikt mönster, inte ens enäggstvillingar har likadana regnbågshinnor (Jain et al. 2004). Metoden går ut på att denna vävnad avläses.
- *Röstigenkänning* - Är en blandning av att mäta både en fysik egenskap och ett beteende eftersom röstens egenskaper beror på hur individen är uppbyggd biologiskt och på hur orden uttalas (Jain et al. 2004). Det finns två olika kategorier av röstigenkänningssystem, text-beroende och text-oberoende.
- *Fingeravtrycksavläsning* - Den kanske mest välkända metoden för biometrisk igenkänning. Det mönster som huden formar på fingertopparna är unikt för alla individer (Jain et al. 2004).
- *Handavtrycksavläsning* - Fungerar på samma sätt som fingeravtrycksavläsning men i stället används hela handen. Dessutom så går det enligt Jain, et al. (2004) att kombinera handavtrycksavläsningstekniken med handgeometriavläsningstekniken.
- *DNA-analys* - Används mest inom kriminalteknik (Jain et al. 2004). Metodens styrka ligger i att det räcker med några få vävnadsceller från vilken kroppsdel som helst för att kunna identifiera någon (Rudin, Inman, Stolovitzky, Rigoutsos, 1999). Ett problem med metoden är att insamlad DNA kan analyseras för andra ända mål som till exempel för att få fram tecken på ärftliga sjukdomar (Jain et al. 2004).
- *Öronavläsning* - Den här tekniken jämför olika individers öronform och även hur brosket i öronsnäckan är strukturerat (Jain et al. 2004).
- *Infraröda* - termogram av ansiktet eller händerna Den värme som utstrålas från en människa bildar ett mönster som kan avläsas med hjälp av en kamera som kan ta bilder av infrarött ljus (Jain et al. 2004).
- *Gångstilsanalys* - Genom att analysera det sätt på vilken en person går är det i viss mån möjligt att fastställa personens identitet (Jain et al. 2004).
- *Tangentbordshanteringsanalys* - Det sätt på vilket en individ skriver på ett tangentbord är en mer eller mindre personlig egenskap som skulle kunna användas för att avgöra vem som sitter och skriver på ett visst tangentbord (Jain et al. 2004). Det som mäts är bland annat tiden mellan tangentnertryckningar (Rejman-Greene, 2002).
- *Doft-/luktanalys* - Allting utsöndrar en viss doft eller lukt vilkens kemiska sammansättning skulle kunna användas för att göra skillnad mellan de olika objekten vilket även gäller den mänskliga kroppen (Jain et al. 2004).
- *Avläsning av näthinnan* - En individs identitet kan fastställas genom att det lager av blodkärl som finns på ögats näthinna läses av med infrarött ljus (Luis-García et al. 2003).
- *Signatur* - Det finns två olika generella sätt att analysera en signatur, den ena görs efter att signaturen har blivit skriven och den andra görs under det att signaturen skrivs (Kim, 1995).

- *Mushanteringsanalys* - Läser av på vilket sätt musen hanteras av användaren för att på så sätt verifiera användarens identitet (Furnell, et al. 2000).

### 2.3.2 Falska matchningar och falska avvisningar

Ett biometriskt system ska jämföra inkommande data från en sensor med sedan tidigare lagrad data, till exempel i en databas, och avgöra om den matchar med en viss identitet. Problemet är att den data som läses in av sensorn innehåller störningar som varierar från gång till gång (Jain et al. 2004), till exempel från omgivningen eller som i fallet med fingeravtrycks-avläsning så kan fingret tryckas olika hårt mot sensorn. Därför måste ett biometriskt system även kunna matcha sådan data med en identitet. Detta görs genom att matchningar som är närliggande accepteras som fullgoda matchningar, problemet är att avgöra hur stor skillnaden får vara (Kim, 1995). Om en generös skillnad tillåts kommer personer att accepteras av systemet som en identitet de inte är, falska matchningar (Kim, 1995). Och om en mycket snäv skillnad efterlevs kommer personer som egentligen borde ha accepteras som de identiteter de faktisk har att avvisas av systemet, falska avvisningar (Kim, 1995). Därför är det mycket viktigt vilket tröskelvärde som sätts för hur exakt matchningen måste vara beroende på hur strikt säkerhet som eftersträvas (Kim, 1995). Figur 2.2 visar hur tröskelvärdet påverkar andelen falska matchningar och falska avvisningar. Med en så kallad ROC (Receiver Operating Characteristics) kurva synliggörs hur på vilket att olika tröskelvärden passar olika bra eller dåligt beroende på tillämpningsområde för det biometriska systemet (se figur 2.3).




*Figur 2.2 (till vänster). Hur tröskelvärdet för matchningar påverkar andelen falska avvisningar och falska matchningar (efter Jain et al. 2004, s.7).*
*Figur 2.3 (til höger). En ROC kurva över hur tröskelvärdet visar vilka tillämpningar som systemet lämpar sig för med avseende på det plottade tröskelvärdet. Olika punkter på linjen anger olika tröskelvärden. Några olika exempel på tillämpningar har satts ut. (efter Jain et al. 2004, s.7).*

### 2.3.3 Multimodala biometriska system

För vissa system tycks det vara så att ingen enskild biometrisk identifierings- eller autentiseringsmetod kan tillhandahålla en tillräckligt hög träffsäkerhet och tillförlitlighet, därför har metoden med multimodala biometriska system kommit att framstå som ett alternativ (Luis-Gracía et al. 2003). Ett multimodalt biometriskt system, eller multibiometriskt system som det också heter, kan definieras som ett system som använder sig av mer än en biometrisk metod för att identifiera eller autentisera en person (Luis-Gracía et al. 2003).

I ett biometriskt system som används för autentisering kan en högre träffsäkerhet uppnås med hjälp av användandet av flera olika biometriska metoder men någon större skillnad i hastighet kan inte uppnås (Hong & Jain, 1999). I ett system som används för identifiering, där ett stort antal matchningar alltid måste göras, kan ett multibiometriskt system implementeras på ett sådant sätt att en metod som är väldig särskiljande mellan olika individer kan kombineras med

en metod som är mer beräknings effektiv men inte lika särskiljande för att uppnå högre hastighet och ändå få en god träffsäkerhet (Hong & Jain, 1999). För att ett multibiometriskt system ska kunna fatta ett beslut måste det vilket de olika mätningarna kommer fram till kombineras på något sätt, detta kan göras både tidigt eller sent i processen (Jain et al. 2004).

### 2.3.4 Säkerhet

Kim (1995) visar på två möjliga svaga punkter i ett biometriskt system, den ena är när den avlästa biometriska informationen skickas till andra delar i systemet kan signalerna avlyssnas och den andra är att det kan vara möjligt att komma åt användarprofiler som lagrats i systemets databas. Om detta skulle ske så skulle det vara möjligt för en bedragare att amvända den informationen till att uppträda som den personen informationen avser (Kim, 1995). Hade detta hänt med ett vanligt lösenord hade det varit en enkel sak att ändra lösenordet till ett nytt men det är inte lika enkelt att byta ut någons biometriska egenskaper (Kim, 1995). Vidare är det också eventuellt möjligt att lura ett biometriskt säkerhetssystem med hjälp av imitationer av biometriska egenskaper (Prabhakar et al. 2003).

En möjlig säkerhetsfördel med biometriska metoder för identifiering eller autentisering är att de anses stå emot så kallade ”brute force” attacker bättre än vad lösenord gör (Ratha et al. 2003). Men däremot kan det vara så att biometriska system är mer känsliga för så kallade ”replay attacker” än vad system som använder sig av lösenord är (Ratha et al. 2003).

### 2.3.5 Integritet och användaracceptans

Redan som det är idag lagras mycket information om kunder av olika företag vilket har inneburit att det finns ett ökat motstånd till att mer blir lagrat (Bolle et al. 2002). Dessutom finns det en allmän misstänksamhet gentemot central lagring av data rörande individer (Bolle et al. 2002). Det finns en risk att den biometriska data som lagras kanske används till mer än vad den ursprungligen var avsedd för (Prabhakar et al. 2003). Så som att till exempel dra slutsatser om enskilda individers hälsa, vanor och annat som kan leda till någon form av diskriminering. Och det är också så att ett biometriskt system kan komma att avslöja identiteten på människor som, till exempel för sin personliga säkerhets skull, vill kunna hålla sig anonyma (Prabhakar et al. 2003). Identifiering skulle också kunna ske i det dolda utan att personen som identifieras är medveten om det vilket minskar den privata sfären (Prabhakar et al. 2003).

För att undersöka hur användare ställer sig till att använda sig av biometriska metoder som ett alternativt sätt att autentisera sig med har Furnell, et al. (2000) genomfört en undersökning. Dom svarande visade sig vara någorlunda positivt inställda till att använda sig av den biometriska tekniken. De tekniker som fick ett mest positivt mottagande i den undersökningen var röstigenkänning och fingeravtrycksavläsning. Dock hade troligen ingen av de tillfrågade använt sig av några biometriska system i praktiken.

### 2.3.6 Standarder

Inom andra industrier finns det standarder och så även inom biometri industrin. The BioAPI Consortium (www.bioapi.org) är initierat av flera olika intressenter i biometri industrin och har utvecklat ett standard API för mjukvarutvecklingen (Luis-García et al, 2003).
Enligt Rejman-Greene (2002) har finans sektorn antagit ANSI X9.84 (www.x9.org ANSI) standarden och en standard för utbytet av biometriska data finns också tillgänglig CBEFF (Common Biometric Exchange File Format) ( www.itl.nist.gov/div895/isis/cbeff).

# 3. Problembeskrivning

Lösenord används i stor utsträckning i många av dagens system för autentisering (Furnell et al. 2000). Dessvärre omgärdas den autentiseringsmetoden av ett flertal problem så som att användare skriver ner lösenorden, låter andra använda deras lösenord, glömmer av dom och väljer lösenord som är lätta att lista ut (Furnell et al. 2000). En nyare autentiseringsmetod som utvecklats är biometritekniken och den skulle eventuellt kunna lösa de problem som finns med lösenordsautentisering. Till exempel så är det svårt att låna ut en biometrisk egenskap till någon annan, och det är även svårt att glömma bort den. Men även biometritekniken har sina brister och problem.

Är det då för ett företag eller en organisation i dagens läge lämpligt att införa ett system baserat på biometriska metoder? Det finns flera olika aspekter som kan beaktas för att besvara den frågan. Några sådana aspekter som identifierats är kostnad, säkerhet, träffsäkerhet och prestanda (Kim, 1995). Ytterligare aspekter är integritet (29-gruppen, 2003) och användaracceptans (Deane, Barrelle, Henderson & Mahar, 1995).

Att installera, driva och underhålla ett säkerhetssystem kostar, oavsett vilken metod för autentisering eller identifiering som systemet använder sig av. Frågan är om ett säkerhetssystem baserat på biometriska metoder skulle vara mer kostnadseffektivt. För att utvärdera detta skulle antagligen en specifik kostnadsanalys behöva utföras för just det företag eller den organisation som undersöker möjligheterna med ett biometriskt säkerhetssystem.

Bolle, et al. (2002) skriver att biometritekniken förvisso kan lösa en del säkerhetsproblem som andra autentiserings- eller identifieringsmetoder har men att i gengäld har biometri som autentiserings- eller identifieringsmetod egna säkerhetssvagheter. Vilka säkerhetsproblem löser den biometriska tekniken och vilka säkerhets problem finns med tekniken? Eftersom det är just säkerhet som är syftet med ett biometriskt system är det en viktig aspekt vid en diskussion om ett sådant systems nytta.

Vidare så introducerar användandet av biometriska egenskaper som autentiserings- eller identifieringsmetod en del oro för den personliga integriteten. Det finns till exempel ett allmänt motstånd mot allt för mycket central lagring av personlig information (Bolle et al. 2002) och även en oro för att den informationen ska användas till mer än vad som var avsett från början (Prabhakar et al. 2003). En organisation eller ett företag som planerar att använda sig av biometri för autentisering eller identifiering av individer bör ta i beaktande de lagar och regler som finns vid behandling av persondata. Frågan är vilka lagar som gäller för biometriska system. Samma lagar gäller för alla svenska företag och organisationer.

Om de som ska komma att använda systemet inte accepterar det så finns risken att säkerheten minskar i stället för att den ökar (Deane et al. 1995). Eller de anställda upplever det som om att de blir övervakade vilket kan leda till att arbetet som utförs på företaget eller organisationen blir mindre effektivt (Deane et al. 1995). Om ett företag eller en organisation försöker införa biometri för att autentisera eller identifiera sina kunder riskerar företaget eller organisationen att förlora kunder om kunderna anser att det är oacceptabelt att använda sig av ett sådant system. Därför är användaracceptansen av avgörande vikt.

Rent generellt är ett biometriskt autentiserings- eller identifieringssystem ett mönster-matchningssystem som ska avgöra om det inkommande mönstret matchar ett sedan tidigare känt mönster (Prabhakar et al. 2003). Nu är det så att den indata som systemet får aldrig kan matcha perfekt på grund av att en ny inläsning av samma biometriska egenskap inte blir exakt

(Jain et al. 2004). Så istället måste ett tröskelvärde användas för att avgöra hur nära två mönster måste matcha med varandra för att det ska räknas som en fullgod matchning (Kim, 1995). Problemet är att avgöra hur generöst respektive strikt värde som ska användas då ett för lågt krav på matchningslikhet ökar risken att obehöriga accepteras och ett för hårt krav leder till att behöriga avvisas från systemet (Kim, 1995). Detta betyder att det går att anpassa kraven på biometrisystemets träffsäkerhet efter företagets eller organisationens behov. Denna aspekt kommer inte att undersökas djupare i den här rapporten då det kan tänkas vara lämpligare att göra en fallstudie på ett specifikt företag eller organisation.

Det samma gäller för prestanda aspekten. Behovet av prestanda i avläsningen av biometriska egenskaper och utvärdering av den data som lästs in är olika på olika företag och organisationer. Då olika biometriska metoder och tekniker ger olika prestanda är det svårt att generalisera prestanda behovet.

Det här arbetet är tänkt att inrikta sig på en undersökning om biometriteknikens lämplighet för företag och organisationer i allmänhet. Det vill säga att behoven för specifika företags- eller organisations typer inte kommer att undersökas närmare.

## 3.1 Problemprecisering

Är det i dagens läge lämpligt för ett företag eller en organisation att införskaffa ett säkerhetssystem baserat på biometri med avseende på aspekterna säkerhet, integritet och användaracceptans?

## 3.2 Avgränsning

Rapporten avgränsar sig till att granska aspekterna kring säkerhet, användaracceptans och integritet eftersom dessa anses vara de viktigaste aspekterna som går att undersöka på en generell nivå. För integritetsaspekten är det endast svenska lagar som kommer att tas i beaktande.

## 3.3 Förväntat resultat

En översikt över vilka säkerhetsproblem som biometritekniken förväntas kunna lösa och vilka säkerhetsproblem tekniken anses kunna föra med sig. Rapporten avser också att ge en överblick av vilka svenska lagar som gäller för integritetsskydd vid behandlandet av biometriska egenskaper. Dessutom kommer en jämförelse och analys göras av några tidigare genomförda undersökningar angående nivån av användaracceptans för biometriska säkerhets-system.

# 4. Metod

Det finns ett flertal olika tekniker för att besvara en frågeställning och ingen av dessa kan sägas vara mer rätt eller fel utan vilken metod som bör användas avgörs av vad som verkar kunna ge det bästa svaret i förhållande till de resurser som finns tillgängliga (Patel & Davidson, 1994). I det här kapitlet kommer ett antal metoder att beskrivas kortfattat och på vilket sätt dessa skulle kunna användas för att bemöta problemet. Dessutom kommer en eller flera av dessa metoder att väljas ut med motivering för varför den eller dessa skulle vara mest lämpade att använda i genomförandet av det här arbetet. Det som är viktigt vid val av metod är att metoden eller metoderna ska ge en god validitet och reliabilitet (Patel & Davidson, 1994). Med reliabilitet menas i vilken grad som det mätinstrument man använt sig av är pålitligt i avseendet att det som mätts verkligen har de uppmätta värdena och med validitet menas att det som undersöks verkligen är det som kommer att ge ett relevant resultat (Patel & Davidson, 1994).

## 4.1 Möjliga metoder

De metoder som skulle kunna vara lämpliga att använda sig av vid genomförandet av detta arbete är litteraturstudie, intervjustudie och enkätundersökning. Nedan följer en beskrivning av var och en av dessa. Andra metoder så som implementation, fallstudie eller experiment utesluts som möjliga eftersom de antingen inte skulle ge ett resultat som relaterar till problemställningen eller så saknas de nödvändiga resurserna.

### 4.1.1 Litteraturstudie

En litteraturstudie är en systematisk analys av den för problemområdet tillgängliga litteraturen med syftet att granska problemet (Berndtsson, Hansson, Olsson & Lundell, 2002). För det här arbetet skulle en litteraturstudie kunna ge mycket information om hur problematiken runt säkerhet ser ut. Detta eftersom det finns mycket litteratur som behandlar ämnet datasäkerhet i allmänhet vilket även är tillämpbart på biometritekniken och dessutom finns det publikationer som specifikt avhandlar säkerhet för biometriska system. Vidare skulle en analys av befintlig litteratur kunna ge uppgifter om vad tidigare undersökningar rörande användaracceptans har kommit fram till för resultat. Dessa resultat kan sedan analyseras och jämföras med varandra. Dessutom skulle en litteraturstudie kunna analysera vilka lagar och regler som finns rörande skydd av den personliga integriteten.

En nackdel med en litteraturstudie är att det är svårt att veta när en tillräckligt stor mängd material har granskats och om någon viktig källa saknas vilket är av betydelse för arbetets validitet (Berndtsson et al. 2002). Därför är det viktigt att planera insamlandet av den litteratur som ska komma att användas i ett arbete och för att på så sätt nå målet att få fram det material som är av relevans för problemlösningen (Bell, 2000). För att uppnå detta bör vissa parametrar för litteratursökandet formuleras som till exempel vilken typ av publikationer som skall tas i beaktande, hur gamla eller nya dessa ska vara, hur materialet tas fram och var det eftersöks (Bell, 2000). Det finns också en risk att studiens resultat vinklas av att materialet inte väljs ut på ett objektivt sätt (Patel & Davidson, 1994).

Det finns ett flertal olika typer av publikationer. Dawson (2000) har listat några som kan vara aktuella för det här arbetet:

- Böcker – Är en bra utgångspunk i en litteraturstudie efter som de kan ge en grundförståelse för problemområdet. Böcker innehåller dock sällan särskilt nytt material.
- Journaler – Innehåller artiklar, oftast med referenser, och behandlar det senaste inom området.

- Proceedings från konferenser – Samlar de artiklar som presenterats på en konferens. Kvalitén på dessa artiklar kan variera kraftigt men innehåller oftast det absolut senaste tänkandet inom just det området.

Att kritiskt utvärdera det insamlade materialet är av största vikt och några saker som bör tas i beaktande är enligt Dawson (2000) bland annat:

- Vilken typ av publikation är det?
- Kan materialet tillföra något?
- Är författaren en auktoritet inom området?
- Hur relaterar materialet till annan litteratur inom området?
- Vilka referenser använder sig författaren eller författarna av?

En litteraturstudie ska inte vara en uppräkning av de texter som har lästs och behöver inte presentera materialet med en paragraf eller ett kapitel för varje källa (Dawson, 2000). I stället är det oftast så att materialet används och tas upp allteftersom olika del problem tas upp (Dawson, 2000).

### 4.1.2 Intervjustudie

Genom att genomföra en intervjustudie skulle det vara möjligt att göra en kvalitativ analys av materialet och på så sätt få en fördjupare kunskap (Patel & Davidson, 1994). Något som kanske skulle kunna vara lämpligt i fråga om integritet och användaracceptans eftersom det kan vara en bra metod för att få insikter om hur dessa aspekter betraktas på ett djupare plan. Utifrån ett sådant insamlat material skulle då eventuellt en slutsats kunna dras huruvida biometriska system är lämpliga att implementera i en organisation eller i ett företag ur ett användarperspektiv. Även när det gäller säkerhet skulle en intervjustudie möjligen kunna ge upplysningar med avseende på uppfattningar kring säkerhet och biometriska system. Dessa uppfattningar skulle kunna inhämtas från både ett användarperspektiv och ett expertperspektiv.

Befring (1994) beskriver intervjuer som en både krävande men flexibel studiemetod. Vidare skriver också Befring (1994) att en intervju tar formen av ett samtal där olika problemställningar och teman tas upp. Det finns olika typer av intervjuer, var och en med sina styrkor och svagheter (Berndtsson et al. 2002). Det finns öppna intervjuer där få eller inga frågor är förutbestämda vilket ger den fördelen att de frågor som är viktiga för den intervjuade får möjlighet att komma fram, men en sådan intervjuform är svår att behärska (Berndtsson et al. 2002). Istället så finns det mer kontrollerade former av intervjuer där frågorna är definierade på förhand vilket har den fördelen att intervjuerna får en högre grad av repeterbarhet (Berndtsson et al. 2002). Själva intervjun kan ske vart som helst men vanligast är att personen som ska intervjuas uppsöks i deras bostad, på deras arbetsplats eller i skolan vilket brukar kallas för fältintervjuer eller uppsökande intervjuer (Befring, 1994). Den som ska intervjuas kan också kallas till den institution där forskningen är baserad och då benämns dessa intervjuer som kliniska intervjuer (Befring, 1994). Det är också möjligt att genomföra en intervju utan någon form av direktkontakt till exempel genom telefonsamtal (Befring, 1994).

Befring (1994) lägger vikt vid att själva frågorna vid en intervju utformas på ett korrekt sätt. Med vilket bland annat menas att frågorna inte bör vara ledande på något sätt. Dessutom är det också viktigt att personen som blir intervjuad vet på vilket sätt som svaren kommer att användas och i vilken grad han eller hon som uppgiftslämnare är anonym. Befring (1994) vill dock hävda att intervjustudier ofta blir resurskrävande.

### 4.1.3 Enkätundersökning

En enkätundersökning kan ske genom att ett formulär med frågor med fasta svarsalternativ skickas ut till en undersökningsgrupp eller genom en så kallad ”enkät under ledning” vilket innebär att undersökaren närvarar när formuläret besvaras och har då möjligheten att förtydliga om något är oklart (Patel & Davidson, 1994). När enkäterna skickas på post till individerna som ska delta i undersökningen kallas det för en postenkät (Befring, 1994). En enkätstudie skulle kunna ses som ett specialfall av en intervjustudie där intervjuformen har mycket strikta krav på sin struktur och uppbyggnad både med avseende på frågeformuleringar och vilka svarsalternativ som tillhandahålls (Befring, 1994).

En undersökning av den här typen skulle kunna användas för att mäta hur väl olika typer av biometriska system accepteras på ett kvantitativt sätt. Och så skulle det eventuellt vara möjligt att generalisera olika uppfattningar runt säkerhet och integritet. Nackdelar med enkätundersökningar är att det är svårt att få ett högt deltagande i undersökningen och att undersökaren inte har någon kontroll över hur frågorna bemöts eller vilket intryck de ger (Berndtsson et al. 2002). Enkäter som forskningsmetodik är bäst lämpade vid insamlandet av data från en stor grupp och validiteten för en enkätundersökning är mycket beroende av själva frågeformulärets utformning.

## 4.2 Val av metod

Den metod som valts är litteraturstudie. En litteraturstudie av de texter som publicerats rörande säkerhetsaspekten vid användandet av ett biometriskt säkerhetssystem är lämplig eftersom andra metoder för undersökandet av denna aspekt kräver resurser som ligger utanför det här arbetets ramar. Till exempel resurser så som tillgång till teknik och laborations-möjligheter. Dessutom finns det material publicerat inom ämnet som förhoppningsvis håller god kvalité och går att använda för att arbeta med just den delen av problemet.

En litteraturstudie är också lämplig för att ge en översikt över de svenska lagar som finns gällande lagrandet av biometrisk data. Tanken är att de lagar som finns ska studeras och presenteras i korthet. Vidare så är även en litteraturstudie tillämpbart på aspekten användaracceptans eftersom författaren inte ser någon anledning till att göra om de studier som redan gjorts på området, åtminstone inte för att fullfölja det här arbetets syfte. I stället ska redan gjorda undersökningar av användaracceptans rörande biometriska metoder eftersökas.

Tidsbegränsningar förhindrar att de andra metoder som är lämpliga för det här arbetet används som komplement till en litteraturstudie. Och ingen av de andra två metoderna, intervjustudie och enkätundersökning, skulle kunna användas enskilt för att svara på rapportens samtliga del frågor. En intervjustudie eller enkätundersökning skulle exempelvis inte ge den typ av resultat som önskas på problematiken runt biometriska systems säkerhet då det inte är enskilda individers uppfattningar som efterfrågas. Däremot skulle dessa metoder vara intressanta vid en fördjupad studie av problemområdet eller för att använda som jämförelse av tidigare publicerade resultat.

# 5. Genomförande

I detta kapitel kommer litteraturstudiens upplägg och genomförande att beskrivas. Det material som samlats in kommer att bli presenterat och slutligen kommer undersökningens resultat att redovisas.

## 5.1 Planering av litteraturstudie

Litteraturstudien kommer att delas upp i tre olika studier för varje aspekt som avses att studeras. Alltså en del för säkerhetsaspekten, en för integritetsaspekten och slutligen en för användaracceptansaspekten.

### 5.2.1 Säkerhetsaspekten

När det gäller säkerhetsaspekten kommer litteratur att studeras och sammanställas som påvisar säkerhetsproblem med biometritekniken. Mot detta kommer även litteratur att studeras som påvisar vilka säkerhetsproblem med traditionella autentiserings- och identifierings-metoder som biometritekniken anses kunna lösa. Den litteratur som i första han kommer att användas är artiklar publicerade i olika tidskrifter och journaler.

### 5.1.2 Integritetsaspekten

För integritetsaspekten kommer de lagar som berör området biometri att tas fram och presenteras i den mån de kan bli funna. I första hand kommer information från förvaltnings-myndigheten Datainspektionen att användas. Dessutom kan även material från EU-kommissionen komma att beaktas.

### 5.1.3 Användaracceptansaspekten

För att analysera användaracceptansaspekten kommer tidigare genomförda undersökningars resultat att jämföras och utvärderas. För detta ändamål kommer sådana resultat att inhämtas från rapporter och artiklar som publicerats i olika journaler och tidskrifter att användas. Även statistik från andra källor kan komma att vara av intresse.

## 5.2. Genomförande av litteraturstudien

Vid genomförandet av litteraturstudien eftersöktes texter som behandlade ämnet via ett flertal databaser, där ibland Wiley InterScience, ScienceDirect, Kluwer Online, Springer Emerald, LINK och Academic Search Elite. Även böcker som kunde vara av intresse eftersöktes i högskolans bibliotek, då framförallt böcker om datasäkerhet. Dessutom användes olika söktjänster på Internet som till exempel www.google.se. Vid sökandet efter material användes till samtliga delstudier sökord med relevans till biometri på både svenska och engelska. Några av dessa sökord var: Biometri, biometric, security, recognition, automatisk igenkänning, integritet, privacy, user acceptability, questionary, enkät och survey.

För säkerhetsaspekten så identifierades först olika problem med traditionella identifierings- och autentiseringsmetoder för att veta vad som biometriska säkerhetsmetoder skulle jämföras mot. Där på insamlades material om vilka säkerhetsfördelar och säkerhetsproblem som biometriska system skulle kunna föra med sig. Nästan allt material inhämtades från olika artiklar publicerade i diverse journaler.

Litteraturen för integritetsaspekten plockades fram med hjälp av information från Datainspektionen. Vilket ledde till att material även inhämtades från EU instansen 29-gruppen. Materialet studerades och de mest intressanta resultaten av studien presenteras nedan i rapporten.

Vid studien av användaracceptansaspekten eftersöktes i första hand artiklar publicerade i journaler men eftersom endast två artiklar hittades så användes även andra sök resurser så som olika söktjänster på Internet. För att försöka få en så hög kvalité som möjligt på materialet användes bara sådana uppgifter som kunde hämtas direkt från ursprungskällan och där syftet med de genomförda undersökningarna framgick någorlunda tydligt. De mest intressanta resultaten från de studier som hittats presenteras senare i rapporten.

### 5.2.1 Redovisning och värdering av insamlat material

Materialet för säkerhetsaspekten har i huvudsak inhämtats från artiklar publicerade i journaler som tillämpar peer-review vilket borde borga för en viss kvalité. Vidare så är de flesta författarna ofta förekommande namn inom området och är flitigt refererade. Ett undantag är boken författad av Pfleeger (2003) vilken har använts som källa till allmänna uppgifter om datasäkerhet. Att just den boken valdes grundar sig på att innehållet verkade vara av god kvalité och att den senaste upplagan är relativt ny. Flera av artiklarna är publicerade i syfte att presentera författarens eller författarnas forskningsresultat vilket leder till att de kan vara vinklade på ett sätt som är fördelaktigt för dessa resultat. Detta har tagits i beaktande och därför har i huvudsak endast sådant som kunnat styrkas av flera källor tagits med i studien eller sådant som bedömts vara någorlunda objektivt. Förhoppningsvis är dessa bedömningar riktiga. Då det fanns ett stort utbud av artiklar inom området biometri så kunde inte allt det hittade materialet behandlas av tidsskäl, därför gavs nyare artiklar förtur om det fanns flera som berörde samma sak.

För integritetsaspekten är det den svenska personuppgiftslagen (PuL, SFS 1998:204) och det arbetsdokument om biometri som tagits fram av 29-gruppen (2003) som varit utgångspunkten. Detta eftersom PuL är den svenska tillämpningen av EU direktivet 95/46/EG och det är 29-gruppen som har till uppgift att se till att direktivet tillämpas enhetligt i alla EU:s medlemsländer och ge råd till EU-kommissionen om förslag till ändringar av direktivet. 29-gruppen ska vara en oberoende rådgivande instans i EU och är inrättad av EU-parlamentet och EU-rådet efter artikel 29 i direktiv 95/46/EG och är en arbetsgrupp för skydd av enskilda med avseende på behandlingen av personuppgifter. Arbetsgruppen består av representanter från EU-medlemmarnas respektive datainspektioner. Syftet med det arbetsdokument om biometri som gruppen har antagit är att bidra till en enhetlig tillämpning av direktiv 95/46/EG i de olika medlemsländerna när det gäller behandlingen av biometriska uppgifter. Dokumentet är intressant eftersom det ger en fingervisning om hur PuL ska tillämpas i Sverige och hur en eventuell framtida lagstiftning kan komma att se ut. Dock är dokumentet inte en lag som måste följas utan endast rådgivande.

Litteraturen som hittades för användaracceptansaspekten hade olika styrkor och nackdelar. Artikeln av Deane, et al. (1995) är i det här avseendet något gammal och undersökningsgruppen var inte särskilt stor. Dess styrka är att det är tydligt hur resultaten tagits fram och i vilket syfte. Dessutom har även undersökningens resultat analyserats. Undersökningen som artikeln beskriver utfördes på Australian National University. Syftet var att undersöka om hypotesen att användare var mer beredda att acceptera biometriska tekniker som bygger på beteende än på fysiska egenskaper var korrekt och även att se om hypotesen att användare var mer benägna att acceptera biometriska tekniker när användarna ansåg att känsligheten i det som skulle skyddas steg. Enligt artikeln så motbevisas den första hypotesen men den andra hypotesen får ett visst stöd.

Den artikel som skrevs av Furnell, et al. (2000) beskriver en undersökning som omfattar en något större undersökningsgrupp. Dock är den inte särskilt stor, endast 175 individer. Undersökningens syfte var att undersöka användares inställning till användandet av olika biometriska metoder vid identifiering eller autentisering både vid en initial inloggning till ett system och vid kontinuerlig övervakning vid användandet av systemet. Undersökningen är utförd i Storbritannien vid universitetet i Plymouth i samarbete med Orange Personal Communication Services Ltd. Artikelns styrka är att tillvägagångssättet vid framtagandet av resultatet redovisas noggrant och en analys av det samma görs. En eventuell svaghet med undersökningen är att 80% av de svarande var män och att de flesta var under 35 år fyllda. I den undersökning som beskrivs i artikeln ställdes också frågor om användandet av lösenord vilket är intressant för att studera säkerhetsaspekten i den här rapporten eftersom svaren visar på olika problem med lösenord som biometritekniken eventuellt skulle kunna lösa.

En rapport av den svenska Post- och telestyrelsen (PTS, 2004) som bland annat avhandlar olika identifierings- och autentiseringstekniker så tas även biometri upp. Det intressanta med den här rapporten är att undersökningarna har genomförts på svenskar och är tyvärr den enda som hittats som har gjort det. Dessvärre är resultaten inte särskilt tydliga och allt som går att utläsa i rapporten om just biometri är några få rader.

Sen har även en rapport om resultatet av en undersökning utförd i Kanada hittats. Undersökningen är genomförd på uppdrag av den kanadensiska myndigheten Citizenship and Immigration Canada (CIC, 2003). Det som är intressant med den här rapporten är att den omfattar ett stort antal individer och resultaten är relativt nya. En nackdel med rapporten är att den i första hand berör användandet av biometri ur ett regeringsperspektiv. Alltså hur dom kanadensiska medborgarna ställer sig till att regeringsmakten i Kanada använder sig av biometri för att säkra olika dokument så som till exempel identitetshandlingar. Rapporten är av intresse för det här arbetet då den speglar en allmän inställning till biometri.

Ytterligare en rapport har hittats med resultat från en undersökning genomför i USA (SEARCH, 2002). Undersökningen har gjorts på uppdrag av SEARCH som är en ideell organisation. Som enligt organisationen självt bland annat har som syfte att förbättra rättsväsendet och kvaliteten på rättvisa genom att förbättra hanterandet av information, effektivisera användandet av den samma och att förbättra identifikationsteknologin. Organisationen är instiftad av de amerikanska delstaterna och styrs av en av varje delstat utvald representant. Syftet med den undersökning som genomförts är att mäta allmänhetens inställning till användandet av biometriska identifikations tekniker av statsmakten och i den privata sektorn. En stor grupp har deltagit i undersökningen och den är relativt nygjord. Det som är mest intressant i den här rapporten är vilka olika inställningar som blivit funna till användandet av biometritekniken i den privata sektorn för specifika tillämpningar eftersom inga andra sådana undersökningar hittats. Dessutom är det den enda rapporten där det har undersökts hur många som har erfarenhet av att använda en biometrisk metod och vilken inställning dessa har till de olika metoderna.

## 5.3 Redovisning av litteraturstudien

Nedan följer en redovisning av de resultat som framkommit vid litteraturstudien. Den här delen av kapitlet är uppdelat i tre olika underkapitel. Ett underkapitel för varje aspekt som undersökts i studien.

### 5.3.1 Säkerhetsaspekten
Här tas det material upp som blivit funnet vid studien av säkerhetsaspekten.

#### 5.3.1.1 ”Brute force” attacker
Ett säkerhetsproblem med traditionella lösenord är att många användare väljer enkla lösenord som är lätta att lista ut med hjälp av en så kallad ”brute force” attack vilket visats av bland andra Morris (1979), Klein (1990) och Spafford (1992). Detta är ett problem som biometriska system eventuellt skulle kunna lösa. En “brute force” attack går ut på att samtliga möjliga alternativ testas och är mycket effektiv mot lösenord, dessutom är en sådan attack alltid garanterad att lyckas (Pfleeger, 2003). Den här typen av attack fungerar även på biometriska system vilket visats av Ratha, et al. (2003) men som de också visade så står biometriska system emot en sådan attack betydligt bättre än traditionella autentiseringssystem. Detta eftersom mängden av olika alternativ som behöver prövas för att säkert hitta det rätta är väldigt stor när en biometrisk egenskap används. För även om en ”brute force” attack är garanterad att lyckas kan den ändå vara opraktisk att genomföra då det kan krävas mycket stora resurser och mycket tid för att knäcka ett system beroende på hur många alternativ som måste testas (Pfleeger, 2003).

#### 5.3.1.2 Utlåning av lösenord
Furnell, et al. (2000) påvisar att det inte är helt ovanligt att en användare av ett system lånar ut sitt lösenord till andra användare av samma system. I den undersökning som Furnell, el al. (2000) genomfört var det 29% av de tillfrågade som hade för vana att göra så. Dessutom var det 21% av de som svarade på undersökningen och använde datorer i sitt arbete som hade använt någon annans lösenord utan deras medgivande. Detta försvagar säkerheten i ett system då det blir svårt att veta vem som egentligen var inloggad och risken för att lösenord kommer på avvägar ökar. Kopplingen mellan ett lösenord och en specifik person är mer abstrakt än kopplingen mellan en person och dess biometriska egenskap. Med ett biometriskt säkerhetssystem blir det betydligt svårare att låna ut sitt biometriska ”lösenord” utan att fysiskt befinna sig på platsen ifråga (Jain et al. 2004). Dock hindrar detta inte att någon till exempel loggar in på ett system eller öppnar en dörr åt någon annan och sen lämnar denna någon ensam. För att komma runt det problemet skulle en kontinuerlig kontroll behövas av de biometriska egenskaper personen har som använder systemet (Furnell et al. 2000).

#### 5.3.1.3 Lösenord skrivs ner
Enligt Furnell, et al. (2000) finns det användare skriver ner sina lösenord och förvarar dom på platser som inte alltid är så lämpliga eftersom de tycker att det är svårt att komma ihåg alla lösenord. Om istället en biometrisk metod användes för att autentisera användarna skulle den minnesbördan vara avhjälpt. Men i gengäld så är det omöjligt att förhindra att biometrisk data kan insamlas från vem som helst av vem som helst, till exempel genom röstinspelningar, fotografier, filmer, fingeravtryck och celler från kroppen (Matyas & Stapleton, 2000).

#### 5.3.1.4 Imitationer
Eftersom biometrisk data kan insamlas utan att en person är medveten om det skulle det eventuellt vara möjligt att använda dessa data till att konstruera en kopia av den biometriska egenskapen (Bolle et al. 2002). Till exempel så kan fingeravtryck från en person läsas av för ändamålet att skapa en imitation av den personens finger, eller så kan foton eller filmer användas för att skapa en ansiktsmask eller så kan signaturer förfalskas. Prabhakar, et al. (2003) påpekar att när det gäller fingeravtryck så finns det en hel del krav för att en sådan imitation ska vara möjlig att tillverka. För det första måste ett fingeravtryck av tillräckligt god kvalité hittas vilket inte alltid är lätt då många fingeravtryck inte är fullständiga, ligger på olämpliga ytor eller är suddiga på grund av att fingret rört sig över ytan. Sen måste en

tredimensionell modell skapas från det avlästa avtrycket vilket kräver speciell teknik eftersom det inte duger med en tvådimensionell bild för att lura de allra flesta fingeravtrycks-avläsningssensorer. Allt detta kräver enligt Prabhakar, et al. (2003) en omfattande expertis och tillgång till laboratorieutrustning. Men det är möjligt att genomföra. Därför har ett antal olika metoder för att avslöja sådana imitationer föreslagits, bland annat genom att mäta motståndskraften i huden, genom att mäta blodets syrehalt med hjälp av infrarött ljus, genom elektrokardiogram, puls, kroppstemperatur och svettningsmönster (Derakhshani, Schuckers, Hornak & O'Gorman, 2003). Dessvärre kan eventuellt även dessa tester bli överlistade om en tillräckligt sofistikerad imitation tillverkas som kan efterhärma dessa egenskaper (Prabhakar et al. 2003).

#### 5.3.1.5 Samma ”lösenord” på flera olika system

Ett problem som identifierats med traditionella lösenord är att många användare tenderar att använda samma lösenord till mer än ett system, enligt den undersökning som utfördes av Furnell, et al. (2000) var det 40% av de tillfrågade som använde samma lösenord på flera olika system. Ett biometriskt säkerhetssystem skulle kunna lida av samma problem enligt Kim (1995) eftersom samma biometriska egenskap kan komma att användas för identifiering eller autentisering på flera olika system. Om en sådan biometrisk egenskap stjäls antingen genom att den blir stulen direkt från innehavaren eller genom att den stjäls från ett system som har den lagrad skulle det kunna vara möjligt att använda den egenskapen för att olovligen ta sig in i flera olika system. Dessutom är problemet allvarligare eftersom om ett vanligt lösenord blir stulet är det oftast inte svårt att ändra lösenordet till ett nytt, det är däremot inte lika lätt att återkalla en biometrisk egenskap (Kim, 1995). Olika tekniska lösningar har föreslagits för att lösa det här problemet bland annat av Bolle, et al. (2002). Den lösningen går ut på att vid inregistreringen förvrängs den biometriska profilen på ett sätt som är unikt för det systemet och för den individen. Samma förvrängning appliceras sedan vid autentiseringen och på så sätt skulle en biometrisk profil stulen från ett system inte gå att använda på ett annat och dessutom skulle det vara möjligt att registrera en person på nytt men med en annan förvrängning för att på så sätt byta ut den stulna profilen. Bolle, et al. (2002) anser också att det kan vara lämpligt att göra så att förvrängningen inte går att invertera, alltså göra om baklänges för att få fram originalet igen.

#### 5.3.1.6 Förlust av unika föremål

Ett problem med traditionella autentiserings- och identifieringsmetoder som baseras på innehav av ett unikt föremål som tillexempel ett pass eller magnetkort är att dessa kan tappas bort (Luis-García et al. 2003) Detta är inte bara ett problem för användaren om det skulle inträffa utan det är även en försvagande länk i ett säkerhetssystem eftersom då ett sådant föremål förlorats måste ett nytt tilldelas användaren och i den processen kan det finnas luckor. Till exempel så har det hänt att personer lyckats skaffa sig falska identitetshandlingar. Biometriska egenskaper kan inte tappas bort på samma sätt (Jain et al. 2004). Eftersom biometriska egenskaper baserar sig antingen på någon form av unikt beteende eller någon unik karaktäristik hos en kroppsdel.

#### 5.3.1.7 ”Replay” attacker

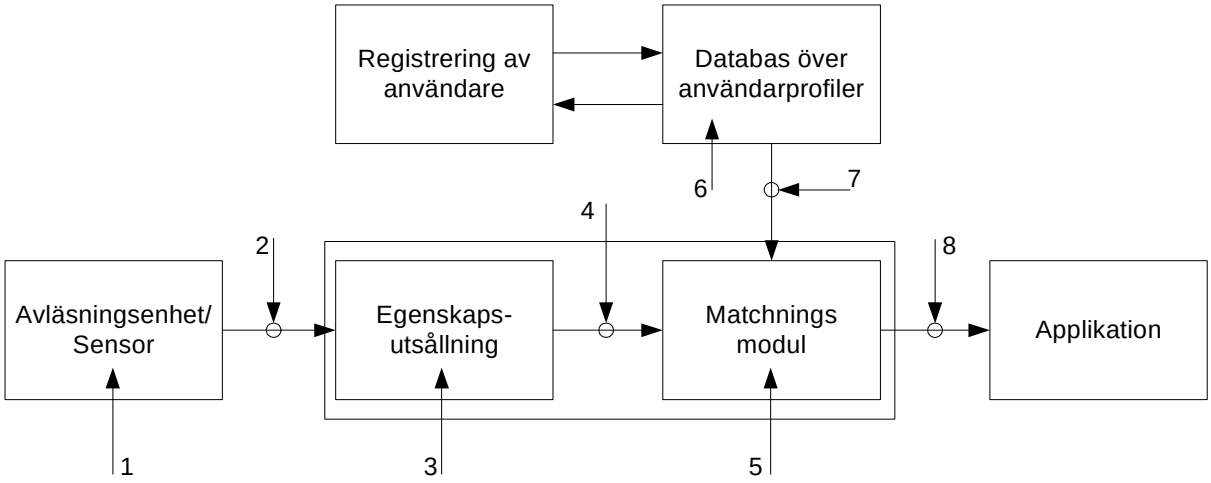
Autentiseringssystem som använder sig av lösenord är inte hotade av så kallade ”replay” attacker (Bolle et al. 2002). Däremot är biometriska system känsliga för sådana attacker (Ratha et al. 2003). ”Replay” attacker fungerar på så sätt att en signal som skickas mellan två system eller delar i ett system snappas upp var på det kan manipuleras och skickas igen när uppsnapparen så vill (Pfleeger, 2003). Att till exexempel. kryptera signalerna är enligt Ratha, et al. (2003) inte en bra lösning eftersom krypteringen accepterar en gammal inläsning lika väl som en ny.

#### 5.3.1.8 Svaga punkter i biometriska system

Ratha, et al. (2003) har identifierat 9st olika hot och möjliga attacker mot ett biometriskt system (se figur 5.1):

1. Att visa upp en artificiell biometrisk egenskap för systemets avläsningsenhet, kan genomföras som antingen en ”replay”-attack eller med hjälp av en imitation.
2. En attack riktad mot kopplingen mellan avläsningsenheten och resten av systemet kan vara en typ av ”replay”-attack eller en elektronisk imitering av en biometrisk egenskap.
3. En attack med hjälp av en trojansk häst kan göra det möjligt att få egenskaps-utsållningsmodulen att genera den profil som önskas från vilken som helst indata.
4. En attack på kopplingen mellan egenskapsutsållningsmodulen och matchningsmodulen är möjlig, särskilt om de båda modulerna befinner sig på geografiskt olika platser.
5. En trojansk häst placerad i matchningsmodulen kan användas för att manipulera matchningsresultaten.
6. Manipulation av de användarprofiler som finns lagrade i databasen över användar-profiler skulle kunna leda till att en bedragare blir accepterad av systemet eller åtminstone till att en legitim användare nekas tillträde.
7. Om en attack riktades mot kopplingen mellan databasen och matchningsmodulen skulle det vara möjligt att förändra användarprofilerna som kommer från databasen innan de når matchningsmodulen.
8. Genom att ta kontroll över kopplingen mellan det biometriska systemet och den applikation det är avsett att skydda kan det biometriska systemets resultat åsidosättas.

Ratha, et al. (2003) skriver också att det finns ett nionde hot mot biometriska system och det infinner sig i registreringsfasen och består i att en individ som inte är avsedd att ha tillgång till systemet lyckas genom bedrägeri bli en registrerad användare. Eller att någon lyckas registrera sig mer än en gång.




*Figur 5.1. Svaga punkter i ett generellt biometriskt system (efter Ratha et al.2003, s. 2106).*

### 5.3.2 Integritetsaspekten

Här presenteras resultaten från studien av integritetsaspekten.

#### 5.3.2.1 Personuppgifter och PuL

En personuppgift är all sådan information som på ett direkt eller indirekt sätt kan kopplas till en fysisk levande person enligt den svenska personuppgiftslagen (PuL, SFS 1998:204). PuL är till för att skydda personer mot att deras integritet kränks vid hel- eller halvautomatisk behandling av personuppgifter. Även viss manuell behandling innefattas av lagen ifall uppgifterna är en del av eller är tänkta att bli en del av någon form av register. Som

behandling räknas insamling, registrering, lagring, bearbetning, sammanställning eller samkörning. Lagen har införts i enlighet med direktiv 95/46/EG utfärdat av EU-kommissionen. Det är alltså så att varje land som är medlem i EU ska implementera direktivet i nationell lag och i Sverige är det PuL som följer direktivet.

#### 5.3.2.2 Biometri är personuppgifter i de flesta fall

Enligt det arbetsdokument om biometri som utformats av 29-gruppen (2003) är biometriska egenskaper att betrakta som personuppgifter i de flesta fall och bör då behandlas enligt direktiv 95/46/EG för att hanteringen ska kunna anses vara laglig. Arbetsgruppen anser dock att om biometriska uppgifter lagras på ett sådant sätt att varken den registreringsansvarige eller någon annan person kan identifiera den som har blivit registrerad så är uppgifterna inte att betrakta som en personuppgift. Dessutom gäller inte direktivet för skydd av person-uppgifter om uppgifterna behandlas av en fysisk person där behandlingen är en del av en verksamhet av helt privat natur eller har ett samband med denna persons hushåll. Många biometriska produkter avsedda för hushållsändamål kommer att falla inom den sistnämnda gruppen (29-gruppen, 2003).

#### 5.3.2.3 Behandling av personuppgifter

En personuppgift får endast behandlas om personen i fråga har givit sitt uttryckliga medgivande men det finns undantag. Enligt PuL är sådana undantag när behandling är nödvändig för att ett avtal med den registrerade personen ska kunna fullgöras, när den som ansvarar för personuppgifterna måste fullfölja en rättslig skyldighet, när en myndighet behöver uppgifterna i samband med sitt utövande, vid utförandet av en arbetsuppgift som är av allmänt intresse och efter en intresseavvägning. En intresseavvägning innebär att den personuppgiftsansvariges intresse av att behandla uppgifterna vägs emot den registrerade personens intresse av skydd för sin personliga integritet.

Dessutom så gäller att den som ska bli registrerad blir ordentligt informerad om vad uppgifterna ska användas till och vem som är den registeransvarige för att behandlingen av uppgifterna ska vara laglig. Det är också förbjudet att använda de insamlade person-uppgifterna till ändamål som inte är förenliga med det ursprungliga syftet. Det är alltså till exempel inte lagligt att använda biometriska uppgifter som lagrats i syfte att avgöra någons identitet för att till exempel övervaka personens arbetseffektivitet eller för att försöka ställa en diagnos över personens mentala hälsa (29-gruppen, 2003).

#### 5.3.2.4 Proportionalitet

Enligt 29-gruppen (2003) bör proportionaliteten tas i beaktande vid hanterandet av biometriska data. Detta eftersom det inte är tillåtet att lagra mer än vad som behövs för att uppnå syftet med registreringen och vid inläsningen av biometriska egenskaper kan mer information än vad som är nödvändigt bli lagrad. Därför anser 29-gruppen (2003) att lagringen bör utformas så att ett minimalt antal uppgifter behöver lagras och att all överflödig information förstörs i enlighet med direktiv 95/46/EG som säger att inga personuppgifter får lagras längre tid än vad som är nödvändigt. Vidare anser också 29-gruppen (2003) att då lagring av biometriska uppgifter ska ske i någon form av central databas bör rimligheten i detta prövas, alltså om känsligheten i de uppgifter som lagras står i proportion till syftet med att lagra dom.

Dessutom anser 29-gruppen (2003) att biometriska uppgifter endast får användas om antalet uppgifter som behandlas inte är orimligt stort och att uppgifterna är relevanta och lämpliga. Som exempel på detta ges den franska datainspektionens beslut att inte tillåta att ett system infördes för att låta skolbarn i frankrike identifiera sig med sina fingeravtryck för att få

tillträde till skolmatsalen men att de däremot tillät att ett system baserat på handgeometri användes. I Sverige har den svenska datainspektionen i frågan att använda fingeravtryck vid instämpling på en arbetsplats beslutat att den typen av behandling av biometriska personuppgifter inte är förenligt med PuL (Datainspektionen, 2004). Detta eftersom de ansåg att behandlingen av fingeravtryck medför integritetsrisker som är svåra att överblicka i dagsläget och att sådan kontroll kan ske på ett minde integritetskränkande sätt.

#### 5.3.2.5 Känsliga personuppgifter

Det är inte heller tillåtet att behandla personuppgifter som anses vara känsliga. Sådana uppgifter är etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa och sexualliv. När det gäller biometriska data är det framför allt uppgifter om etniskt ursprung och personens hälsa som riskerar att bli behandlade vilket alltså är förbjudet (29-gruppen, 2003).

#### 5.3.2.6 Vad 29-gruppen anser

29-gruppen (2003) ställer sig positivt till användandet av biometriska system där den biometriska profilen inte lagas i en databas eller terminal utan istället endast innehas av den som informationen avser, alltså till exempel på ett smartkort eller liknande. Detta eftersom de anser att det medför mindre risker för individens fri- och rättigheter. Vid lagring i centrala databaser bör därför särskild hänsyn tas till riskerna för felaktig behandling av de biometriska uppgifterna och den registeransvarige är skyldig att följa de säkerhetsföreskrifter som finns i direktiv 95/46/EG. Vidare anser de också att det är möjligt att användandet av biometriska personuppgifter eventuellt skulle kunna leda till ett ökat skydd för den personliga integriteten om biometriska uppgifter skulle kunna ersätta andra personuppgifter.

### 5.3.3 Användaracceptansaspekten

Det finns ett flertal olika undersökningar som genomförts angående nivån av användares acceptans för införandet och användandet av biometriska system och olika biometriska metoder. Nedan presenteras resultatet av den genomförda studien inom det här området. Olika undersökningar presenteras var för sig efter varandra följande.

#### 5.3.3.1 Deane et al. (1995)

Den äldsta artikel av intresse som hittats som avhandlar en sådan undersökning är den skriven av Deane, et al. (1995). Artikeln beskriver en undersökning utförd på 76 individer anställda inom banksektorn eller vid universitet i Australien. De har fått svara på ett formulär med frågor om vilken inställning de har till sju olika typer av biometriska metoder för identifiering eller autentisering. Svarsalternativen låg på en skala mellan 1 och 5. Där 1 betydde att den metoden ansågs vara fullständigt oacceptabel och 5 betydde att metoden i fråga var fullständigt acceptabel. Svaren sammanställdes och ett medelvärde togs fram, se tabell 5.1. Enligt Deane et al. (1995) pekar deras resultat på att biometriska metoder som baseras på fysiska egenskaper är mer accepterat än vad biometriska metoder baserat på individuella beteenden är accepterat.

*Tabell 5.1. Visar medelvärdena för svaren på undersökningen som genomfördes av Deane et al. (1995). (Tabellen hämtad från Deane et al. 1995, s. 227)*

| Metod | Medelvärde |
|---|---|
| *Baserade på beteende* | |
| Signatur | 2,78 |
| Röstigenkänning | 3,02 |
| Tangentbordshanteringsanalys | 2,40 |
| Mushanteringsanalys | 2,47 |
| **kombinerat** | **2,66** |
| *Baserade på fysiska egenskaper* | |
| Fingeravtryck | 3,87 |
| Handgeometri | 3,48 |
| Hornhinneavläsning | 2,66 |
| **kombinerat** | **3,34** |

Vid en närmare undersökning av resultatet visade det sig att 49% ansåg att hornhinneavläsning var oacceptabelt, 56% angav att mushanteringsanalys var oacceptabelt, 59% tyckte att tangentbordshanteringsanalys var oacceptabelt och 42% uppgav att signaturavläsning inte var acceptabelt (Deane et al. 1995). Med oacceptabelt menas här att metoden hade fått en 1:a eller 2:a av den tillfrågade.

Deane, et al. (1995) hade också en hypotes om att acceptansen för biometriska identifieringsmetoder skulle vara relaterad till det uppfattade behovet av säkerhet baserat på hur känslig informationen ansågs vara. I de flesta fall kunde ingen sådan relation påvisas mellan en viss metods acceptans och hur känslig informationen ansågs vara (Deane et al. 1995). Dock fanns vissa undantag. Metoderna tangentbordshanteringsanalys och avläsning av fingeravtryck fick en tydligt ökande acceptans i och med att det uppfattade skyddsbehovet steg (Deane et al. 1995)

#### 5.3.3.2 Furnell et al (2000)

Furnell, et al. (2000) har genomfört en undersökning med 175 svarande från olika organisationer i Storbritannien. Syftet med undersökningen är att försöka få en överblick av acceptansen för olika biometriska metoder och hur användare ställer sig till att bli fortlöpande övervakade för att göra autentiseringen till en process som pågår under hela tiden som systemet i fråga används. De flesta som deltog i undersökningen var män (80%) och så många som 74% av deltagarna var under 35 år fyllda. Dessutom var 103 av de 175 svarande verksamma inom någon form av tekniskt verksamhetsområde. Vidare så efterfrågades de svarandes datorvana, med resultatet att 98% hade använt datorer i mer än ett år, 84% använde en dator i hemmet och 88% använde sig av datorer i sitt arbete.

På formuläret som besvarades fanns det fem olika svarsalternativ för acceptansen av varje metod som varierade mellan ”totalt accepterbar” och ”totalt oacceptabel”. De två positiva svaren summerades för sig och de två negativa svaren summerades för sig var på summan av de positiva svaren subtraherades med summan från de negativa svaren. Resultatet av undersökningen kan ses i tabell 5.2.

Det undersöktes även i vilken grad användarna var beredda att bli kontinuerligt övervakade och vilka metoder de skulle acceptera vid ett sådant förfarande. Det var 43% som ansåg att det skulle vara acceptabelt och 29% svarade att de var osäkra.

*Tabell 5.2. Resultatet från undersökningen genomförd av Furnell et al. (2000). (Tabellen hämtad från Furnell et al. (2000), s. 535).*

| Metod | Initial inloggning | Fortlöpande övervakning |
|---|---|---|
| Tangentbordshanteringsanalys | 29,80% | 25,50% |
| Ansiktsigenkänning | 49,10% | 3,20% |
| Mushanteringsanalys | 21,30% | 21,80% |
| Röstigenkänning | 53,40% | -0,60% |
| Signatur | 40,10% | -35,90% |
| Avläsning av regnbågshinnan | 47,20% | -16,80% |
| Handgeometri | 44,40% | -19,90% |
| Fingeravtryck | 48,80% | -16,00% |

#### 5.3.3.3 PTS (2004)

I en rapport från Post och telestyrelsen (PTS, 2004), som avhandlar hur marknaden ser ut och vilka hinder som finns för en ökad användning av elektronisk identifiering och elektroniska signaturer, har svenska konsumenter tillfrågats om deras inställning till biometri. Deltagarna i undersökningen var positivt inställda till att använda biometriska tekniker för att identifiera sig i framtiden enligt PTS (2004). Anledningen till detta uppgavs vara att det skulle förenkla för dom som användare eftersom de skulle slippa att komma ihåg en mängd olika koder och att de skulle spara tid. Men det uttrycktes också del oro för användandet av biometriska metoder. Bland annat så kunde ovilja uttryckas mot att använda en viss typ av personlig egenskap för biometrisk avläsning som till exempel ögonen. Även oro uttrycktes för vad som skulle hända om den egenskap som mättes gick förlorad, till exempel om en tumme som användes vid identifiering förlorades.

#### 5.3.3.4 CIC (2003)

I Kanada har Citizenship and Immigration Canada (CIC, 2003) genomfört en undersökning där 1200 slumpmässigt utvalda kanadensare deltog. Undersökningen syftade till att undersöka kanadensiska medborgares inställning till biometri och bland annat vilka argument som fanns för och emot. Utgångspunkten för undersökningen tycks vara frågor som rör medborgarskap och identitetshandlingar. Undersökningens resultat uppges ha en felmarginal på +/-2,8% 19 gånger av 20.

I undersökningen (CIC, 2003) svarade 85% att de tyckte att biometriska tekniker skulle vara ett mycket effektivt eller åtminstone någorlunda effektivt sätt att skydda dokument så som till exempel identitetshandlingar. Vidare så var det 68% av deltagarna som var för att den kanadensiska federala regeringen använde biometriska tekniker för att minska olagligt användande av identitetshandlingar.

För att undersöka medvetenheten bland de tillfrågade om biometri ställdes frågan: Vad, om något, betyder termen biometri för dig? 83% svarade då att den termen betydde antingen ingenting eller väldigt lite. Bara några få procent av de svarande relaterade till olika biometriska metoder eller att det hade med fysiska egenskaper att göra. Men efter att ha läst en definition av begreppet biometri var det 56% som kunde erinra sig att de hade hört talas om det tidigare. De källor som uppgavs vara de vanligaste för information om biometri var från TV (61%) och dagstidningar (41%). Undersökningen visade också att det var vanligare att en person kände till biometri ju högre utbildning som personen i fråga hade.

Många av de svarande ställde sig bakom argument emot användandet av biometri dock aldrig någon majoritet. Till exempel ansåg 48% att biometri skulle begränsa den personliga integriteten eftersom regeringen lättare skulle kunna spåra individer. Och 45% ansåg att det fanns en allt för stor potential för att regeringen skulle missbruka informationen. Vidare så ansåg 46% att tekniken inte skulle fungera eftersom kriminella personer ändå skulle kunna komma runt den på något sätt (CIC, 2003).

#### 5.3.3.5 SEARCH (2002)

En undersökning utförd i USA av SEARCH (2002) omfattade 1046 slumpmässigt utvalda individer som intervjuats per telefon och syftade till att mäta den amerikanska allmänhetens inställning till biometriska teknologier. Både med utgångspunkt för samhälleliga tillämpningar som kontrolleras av landets regering och i kommersiella tillämpningar där företag använder sig av tekniken.

Medvetenheten om existensen av olika biometriska tekniker låg på 49% hos de tillfrågade. Av dom tillfrågade var det 5% som någon gång hade använt sig av biometriska egenskaper för att identifiera sig med hjälp av ett biometriskt system. Av dessa hade 82% använt sig av fingeravtrycksavläsning, 46% av signaturanalys, 27% av röstigenkänning, 22% av ansiktsigenkänning, 20% av någon form av ögonavläsning, 19% av handgeometri, 7% av tangentbordshanteringsanalys och 2% hade inte använt någon av de uppräknade metoderna eller så visste de inte vilken det var de hade använt (SEARCH, 2002). Av de som hade använt någon form av biometrisk teknik var de flesta bekväma med att använda sig av tekniken. Alla utom tangentbordshanteringsanalys fick mer än två tredjedelars stöd utifrån bekvämlighets-faktorn. Tangentbordshanteringsanalys fick ett väldigt svagt stöd då ingen av de tillfrågade kände sig varken väldigt eller någorlunda bekväma med att använda sig av den tekniken. Värt att notera är att den del av populationen som hade erfarenheter från användandet av biometriska metoder var liten vilket försämrar resultatens tillförlitlighet.

När det gäller inställningen till användandet av biometriska tekniker av den amerikanska regeringen så finns ett utbrett stöd för detta (SEARCH, 2002). Till exempel ansåg 95% att det var acceptabelt att alla som vill komma in i regeringsanläggningar med höga säkerhetskrav blir jämförda med en databas med biometriska egenskaper och 87% tyckte att det var acceptabelt att säkerhetsvakter skulle kunna övervaka skolor genom att läsa av biometriska egenskaper hos dem som ville komma in på skolområdet. När det gäller röstning vid val tyckte 41% att det var mycket acceptabelt att de som skulle rösta blev jämförda med en databas över biometriska egenskaper hos individer som av olika anledningar inte hade rätt att rösta.

Inom den privata sektorn tyckte 91% att det var acceptabelt att personer som skulle köpa vapen blev jämförda med en databas över dömda förbrytare. Och 85% ansåg att det var acceptabelt att kreditkortsföretag skulle kunna erbjuda sina kunder att använda biometri som ett sätt att identifiera sig vid transaktioner av stora summor. I undersökningen (SEARCH, 2002) går det också att läsa att 49% tycker att det skulle vara mycket acceptabelt om det krävdes att en biometrisk egenskap tillhandahölls vid uttag på en bankomat, att arbetsgivare skulle kunna jämföra någons biometriska egenskaper mot ett brottsregister vid anställning ansåg 46% vara mycket acceptabelt, att administratörer av ett datorsystem skulle kunna använda en persons biometriska egenskaper för att ge access till känslig data ansågs också vara mycket acceptabelt av 46% och att kasinon skulle kunna använda sig av ansiktsigenkänningsteknik för att kunna identifiera personer som inte har tillåtelse att spela i kasinot ansåg 24% vara mycket acceptabelt.

# 6. Analys

I det här kapitlet kommer resultaten från litteraturstudien att analyseras närmare. Aspekterna säkerhet, integritet och användaracceptans tas upp var för sig i olika underkapitel. Dessutom kommer det för varje aspekt att göras en analys av kvalitén på resultatet från studien.

## 6.1 Säkerhetsaspekten

De problem med de traditionella identifierings- och autentiseringsmetoderna, att antingen använda sig av en unik kunskap om något eller innehav av ett unikt föremål, som kunde identifieras var att:

- Lösenord är ofta lätta att lista ut och känsliga mot ”brute force” attacker.
- Lösenord blir nerskrivna vilket gör att de kan hittas av andra.
- Användare lånar ut sitt lösenord och använder andras lösenord utan deras medgivande.
- Samma lösenord används på flera olika system.
- Unika föremål kan tappas bort eller bli stulna.
- Unika föremål kan bli förfalskade.

Frågan är om biometritekniken löser dessa problem eller inte. Nedan tas dessa problem upp var för sig i ett försöka att avgöra det med hjälp av en analys av litteraturstudiens resultat. Dessutom kommer de säkerhetsproblem med biometri som identifierats i studien att analyseras utifrån studiens resultat.

### 6.1.1 Lösenord är lätta att lista ut

Enligt de av studien framkomna resultaten är det även möjligt att använda sig av ”brute force” attacker mot system som använder sig av biometriska metoder för identifiering eller autentisering men att ett sådant system är mycket mer motståndskraftigt mot en sådan attack (Ratha et al. 2003). Detta grundar sig på att det skulle finnas så många olika varianter att prova sig igenom. Men eftersom tekniken ständigt utvecklas och datorernas beräkningskraft ständigt ökar kanske mängden alternativ som måste prövas med tiden inte är så svårt att hantera. Dessutom kan det eventuellt vara möjligt att mer sofistikerade metoder för att utföra en attack utvecklas, till exempel genom att skapa en algoritm som börjar med att pröva de alternativ som har störst sannolikhet att lyckas. Samma skyddsmekanismer som för lösenord skulle eventuellt kunna användas. Och det är inte troligt att sådan datorkraft kommer att finnas tillgänglig inom överskådlig framtid så vida inte de biometriska profilerna som skapas använder ett väldigt litet antal bitar. Så på den här punkten är nog biometriska system att se som säkrare än system baserade på lösenord. Dessutom har biometriska system den fördelen att alla användares identitet har samma skyddsnivå eftersom alla biometriska ”lösenord” är lika svaga eller starka vilket ger den fördelen att systemets säkerhet som helhet möjligen kan bli lättare att bedöma.

### 6.1.2 Lösenord blir nerskrivna

Att användare skriver ner sina lösenord beror troligen på att de är för många eller för svåra för att de ska vara lätta att komma ihåg. Vid biometrisk autentisering eller identifiering behöver användaren bara komma ihåg vilken kroppsdel eller annan egenskap som ska användas vilket borde vara mycket enklare. Dock kan det bli problem om någon till exempel använder flera olika biometriska system som alla använder sig av fingeravtrycksavläsning att komma ihåg vilket finger som ska användas vart. Men det borde vara ett betydligt mindre problem än att komma ihåg olika lösenord. Så även på den här punkten tycks biometri kunna vara en lösning som ger högre säkerhet. Men flera biometriska egenskaper går inte att dölja och kan insamlas utan den utsattes vetskap vilket kan leda till andra eller liknande problem, till exempel att imitationer kan tillverkas.

### 6.1.3 Lösenord lånas ut och andras lösenord används utan deras medgivande

Ett annat problem med lösenord är att användare lånar ut dom till varandra och använder andras lösenord utan deras medgivande. Med ett biometriskt säkerhetssystem blir det svårt att låna ut sitt biometriska ”lösenord” och ännu svårare för någon att använda någon annans biometriska egenskap utan deras medgivande. Det är dock fortfarande möjligt att en användare autentiserar eller identifierar sig med sin biometriska egenskap men låter någon annan använda systemet sedan, för att lösa det problemet skulle någon form av kontinuerlig övervakning krävas (Furnell et al. 2000). Vilket enligt den undersökning som Furnell, et al. (2000) genomfört har ett visst stöd men det finns en stor tveksamhet. Vilket skulle kunna bero på att användarna är rädda att ett sådant system till exempel dessutom dolt skulle kunna användas för att övervaka hur effektivt dom arbetar enligt Deane, et al. (1995). Och det skulle kunna medföra risker för skyddet av den personliga integriteten och det är förbjudet att använda de uppgifter som behandlas till annat än det angivna syftet (29-gruppen, 2003). Därför skulle ett sådant system med kontinuerlig övervakning eventuellt kunna bli svårt att införa så det problemet kan nog inte biometriska system anses lösa om kontinuerlig övervakning får ett stort stöd hos användarna. Däremot måste det till betydligt större ansträngningar för att identifiera sig som någon annan med hjälp av biometriska egenskaper än med hjälp av lösenord utan denna någons medgivande.

### 6.1.4 Samma lösenord på flera olika system

Problemet med att användare använder samma lösenord på flera olika system beror troligen på att det blir färre lösenord att komma ihåg då. Med ett biometriskt säkerhetssystem försvinner problemet med att minnas men problemet med att samma sak används för identifiering eller autentisering på flera olika system kvarstår (Kim, 1995). Om lagringen av de biometriska profilerna sker på olika sätt på olika system skulle den här risken minska eftersom de olika systemen då troligen inte skulle vara kompatibla med varandra, alltså att det är olika detaljer hos den biometriska egenskapen som lagras i de olika systemen. Men då flera system kan vara tillverkade av samma företag skulle det till exempel kunna vara så att alla system från det företaget är kompatibla med varandra. Den lösning som presenterats av Bolle, et al. (2002) skulle kunna fungera för att garantera att de olika biometriska profilerna ser olika ut på alla system. Men den lösningen skulle inte fungera som skydd mot imitationer av biometriska egenskaper. Dessutom skulle den lösningen inte vara lämplig för system som använder sig av identifiering genom biometriska egenskaper eftersom det skulle krävas att samtliga användare blir omregistrerade även ifall det bara är en användares biometriska profil som blivit stulen på något sätt.

### 6.1.5 Unika föremål kan tappas bort, bli stulna eller bli förfalskade

Att kort och andra liknande föremål som används för att autentisering eller identifiering kan bli borttappade eller stulna är ett gammalt problem. Detta försvagar säkerheten på system som använder sig av den metoden eftersom en osäkerhet uppstår om det är personen som är den rättmätige innehavren som använder sig av föremålet eller om det är någon som har stulit det. Och om dessa saker kan tappas bort måste nya sådana föremål kunna bli utfärdade om personen som förlorat sitt föremål inte ska bli utesluten från att använda sig av just det systemet vilket skapar luckor i säkerheten. Med ett biometriskt system har användaren alltid med sig den biometriska egenskapen och det går inte att förlägga den. Däremot finns risken kvar att någon lyckas bli en legitim användare av ett system genom någon form av bedrägeri. Men riskerna denna person då tar är större eftersom en sådan individ som avslöjas kan bli lättare att spåra då en biometrisk egenskap efterlämnats.

Ett problem som dock kan uppstå är att en biometrisk egenskap faktiskt kan förloras genom till exempel en olycka. Om ett system använder sig av fingeravtrycksavläsning och en

användare förlorar sina händer kommer den användaren att vara utestängd från det systemet. I studien hittades inga förslag på lösningar till det här problemet. Men en möjlighet är att ett reserv system skulle kunna finnas för dessa specialfall men då blir hela systemet inte säkrare än vad det reserv systemet skulle vara. Biometriska egenskaper är i de flesta fall ingen hemlighet och kan därför stjälas från en person utan att denne är medveten om detta (Matyas & Stapleton, 2000). Detta kräver att en imitation görs vilken kan vara svårt att genomföra utan teknisk expertis och rätt utrustning men det är dock fullt genomförbart (Phrabhakar et al. 2003). Enda lösningen som blivit funnen i studien är olika metoder för att testa om den biometrisk egenskapen som avläses är artificiell eller äkta men för att en sådan metod ska vara verkligt effektiv måste den testa egenskapen mot något som en imitation aldrig skulle kunna efterhärma. Om något sådant finns framgår inte av studien men det finns olika förslag i alla fall. Så biometriska egenskaper är antagligen inte säkrare än användandet av unika föremål.

### 6.1.6 Säkerhetsproblem med biometri

Ett säkerhetsproblem som säkerhetssystem som använder sig av lösenord inte lider av är så kallade ”replay” attacker (Bolle et al. 2002). Vilket dock biometriska säkerhetssystem gör enligt Ratha, et al. (2003) som också har föreslagit olika lösningar. Huruvida dessa lösningar är tillräckliga eller ens bra är svårt att bedöma utan att genomföra någon form av utvärdering. Men helt klart är att det är till biometriteknikens nackdel jämfört med lösenordsbaserade system sett ur ett säkerhetsperspektiv.

Vidare har Ratha, et al. (2003) identifierat 9st möjliga svagheter och risker för ett generellt biometrisystem. Det som verkar vara en svag länk är de olika modulernas kommunikation i systemet. För att denna svaghet ska försvinna måste modulerna kunna kommunicera med varandra på ett säkert sätt. Det är alltså samma problem som återfinns i nästan all data-kommunikation och är så vitt det går att bedöma utifrån studien inte ett specifikt problem för just biometriska säkerhetssystem. Dessutom är det tydligt att de olika modulerna måste skyddas från direkta intrång. Alla dessa svagheter bör tas i beaktande vid införandet av ett biometriskt säkerhetssystem.

### 6.1.7 Analys av resultatet för säkerhetsaspekten

Utifrån studiens resultat så tycks biometritekniken inte erbjuda en större säkerhet i allmänhet gentemot de traditionella metoderna för autentisering eller identifiering. Detta eftersom tekniken har kvar en del av dom gamla problemen även om dom tar sig nya former och de problem som tekniken kan lösa vägs upp gentemot de nya problem som tekniken för med sig. Förvisso kan det vara så att de nya problemen kan lösas eller åtminstone är lättare att hantera men det ligger utanför den bedömning som kan dras utifrån den här studien.

En litteraturstudies validitet är starkt beroende av vilka källor som tagits med i studien. Eftersom just den här studien har syftat till att ge en översikt till vilka säkerhetsproblem och säkerhetsfördelar biometritekniken har så bör inte resultatet ses som någon annat än just en översikt från det perspektiv som de använda källorna ger. Och det är långt ifrån alla vinklar som har beaktats i studien då det finns ett stort utbud av litteratur. Men studiens resultat pekar mot att biometritekniken kan vara en lösning för vissa problem men inte för alla och att den för med sig sina egna nya säkerhetsproblem.

## 6.2 Integritetsaspekten

Enligt den studie som genomförts är biometriska egenskaper att ses som personuppgifter i många fall och därför gäller PuL vid behandlingen av dem. Studiens resultat visar också på att ett biometriskt system som använder sig av en decentraliserad lagring av de biometriska

uppgifterna anses vara de som bäst tar hänsyn till den personliga integriteten (29-gruppen, 2003). Vilket innebär att ett sådant system har större chanser att bli accepterat ur en juridisk synvinkel. Eftersom system som använder centraliserad behandling av uppgifterna utsätts för en hårdare granskning och kan få svårare att bli godkända vid en intresseavvägning.

### 6.2.1 Syfte och typ av personuppgifter

Ett företag eller en organisation som vill använda sig av biometriska system bör kunna påvisa att fördelarna överväger riskerna för den personliga integriteten. Vidare så framgår också att det företag eller den organisation som vill införa ett biometriskt system bör se upp med vilka uppgifter om användarna som kommer att behandlas av systemet. Vilket beror på att det finns en risk att personuppgifter som anses vara extra känsliga och därför inte får behandlas enligt PuL läses in och behandlas av ett biometriskt system utan att det är den ursprungliga avsikten. Ett exempel på detta skulle kunna vara ett biometriskt system som använder sig av ansikts-igenkänningsmetoden och som då även eventuellt skulle kunna användas till att särskilja personers olika etniska ursprung.

### 6.2.2 Behandling av biometriska uppgifter inkräktar inte alltid på integriteten

All behandling av biometriska egenskaper är dock inte personuppgifter (29-gruppen, 2003). Dessa är egenskaper som lagras på ett sådant sätt att det inte går att identifiera personen de kommer från på något sätt. Ur en säkerhets synvinkel är det kanske tveksamt om sådana uppgifter är intressanta för ett företag eller en organisation. Dessutom behöver inte införandet av biometriska uppgifter i ett säkerhetssystem innebära en försämring av den personliga integriteten. Detta eftersom dessa uppgifter kanske kan ersätta andra personuppgifter vilket till och med skulle kunna leda till att inskränkningarna på den personliga integriteten minskas.

### 6.2.3 Analys av resultatet för integritetsaspekten

För integritetsaspekten hittades endast den svenska lagen om personuppgifter (PuL) och därför togs även det arbetsdokument som antagits av 29-gruppen (2003) i beaktande då det gav riktlinjer för hur PuL bör tillämpas på biometriska uppgifter. Viktigt att påpeka är att arbetsdokumentet inte är lag utan endast rådgivande. Det är möjligt att det finns fler lagar som berör biometritekniken som inte har blivit funna vid de efterforskningar som gjorts. Men helt klart är dock att ett företag eller en organisation som funderar på att införa ett biometriskt säkerhetssystem bör ta i beaktande om uppgifterna som systemet behandlar berörs av PuL.

## 6.3 Användaracceptansaspekten

För användaracceptansaspekten har analysen av studiens resultat delats in i fyra olika delar. En del för medvetenhet om biometri eftersom både Deane, et al. (1995) och Furnell, et al. (2000) antyder att ökad kunskap hos användarna skulle ge en större acceptans av den biometriska tekniken och för att klargöra vilken medvetenhet som finns då detta antagligen påverkar resultatet av en undersökning om användaracceptans. En del för acceptansen av olika specifika biometriska metoder eftersom det är intressant att veta om olika metoder har olika acceptansnivå hos användarna. En annan del för att analysera den allmänna tilltron till biometritekniken och ytterligare en del för att göra det samma med den allmänna misstron till biometritekniken. Slutligen analyseras resultatet för studien av användaracceptansaspekten.

### 6.3.1 Medvetenhet om biometri

I studien som genomförts framgår det att medvetenheten om biometri inte är särskilt stor. Till exempel var det bara några få procent som utan hjälp visste vad biometri var i den kanadensiska undersökningen (CIC, 2003). Och efter att ha läst en beskrivning av biometri var det bara lite mer än hälften (56%) som hade hört talas om det tidigare. I den amerikanska undersökningen kände endas 49% till begreppet biometri (SEARCH, 2002).

Vidare var det endast 5% i den undersökningen som hade någon egen erfarenhet från att använda sig av biometriska system (SEARCH, 2002). Övriga undersökningar som studerats har inte tagit upp den frågan. Men med tanke på att det bara var några få procent i undersökningen gjord av CIC (2003) som visste vad biometri var utan att få hjälp är det inte troligt att det var fler än de procenten som hade någon egen erfarenhet av biometri. I undersökningen genomförd av Furnell, et al. (2000) så ställs inte frågan men enligt författarna själva är det inte troligt att det är någon av de svarande som har använt ett biometriskt system.

Enligt CIC (2003) var det från TV och dagstidningar som de flesta hade fått den kunskap de hade om biometri. Och enligt samma undersökning ökade medvetenheten om biometri i grupper med högre utbildning.

Att kunskapen är begränsad kan påverka acceptansen av biometritekniken. Troligtvis åt det negativa hållet då det inte är ovanligt att människor i allmänhet är mindre positivt inställda till sådant som de inte känner till så bra. Det som är nytt och främmande tas av många emot med skepsis. Gissningsvis skulle en ökad medvetenhet hos användarna ha en positiv påverkan av acceptansen för tekniken. Men det kan också innebära motsatsen då eventuella nackdelar med tekniken kommer till kännedom. Åtminstone skulle det ge en bättre utgångspunkt för diskussioner om biometritekniken.

### 6.3.2 Acceptans av olika biometriska metoder

Olika biometriska metoder för identifiering eller autentisering har enligt studien olika stor grad av acceptans hos användare. Dock skiljer sig acceptansnivån åt i de olika undersökningar som har studerats.

Vid en jämförelse av resultaten från undersökningarna som genomförts av Deane, et al. (1995) och Furnell, et al.(2000) visar acceptansnivåerna från den tidigare undersökningen över lag högre siffror (se tabell 6.1). I undersökningen som genomförts av Deane, et al (1995) har acceptansen av hornhinneavläsning undersökts och i undersökningen av Furnell, et al (2000) har acceptansnivån för regnbågshinneavläsning undersökts. Men eftersom det är ögat som är det som avläses i båda fallen och med liknande teknik har dessa två tekniker i avseendet användaracceptans blivit direkt jämförda med varandra. Dessutom så har resultaten från undersökningen gjord av Deane, et al. (1995) blivit normaliserade för jämförelsens skull.

*Tabell 6.1. En sammanställning av acceptansnivåerna som uppmätts i undersökningarna genomförda av Deane, et al (1995) och Furnell, et al (2000). *I Deane, et al (1995) så är det acceptansen av hornhinneavläsning som undersökts och i Furnell, et al. (2000) så är det acceptansen av regnbågshinneavläsning som undersökts.*

| Metod | Deane, et al. (1995) | Furnell, et al. (2000) |
|---|---|---|
| Tangentbordshanteringsanalys | 48,00% | 29,80% |
| Mushanteringsanalys | 49,40% | 21,30% |
| Röstigenkänning | 60,40% | 53,40% |
| Signatur | 55,60% | 40,10% |
| Avläsning av ögat* | 53,20% | 47,20% |
| Handgeometri | 69,60% | 44,40% |
| Fingeravtryck | 77,40% | 48,80% |

Den metod som fått starkast stöd i Deane, et al. (1995) undersökningen är avläsning av fingeravtryck. Den tekniken har även i Furnell, et al. (2000) fått ett relativt starkt stöd. Men i den undersökningen är det röstigenkänning som ligger i topp. Det kan vara så att metoden att

använda sig av fingeravtryck är mer accepterad därför att tekniken är känd sedan tidigare eftersom den används av polisen vid brottsutredningar.

I båda undersökningarna har metoderna tangentbordshanteringsanalys och mushanteringsanalys fått de lägsta nivåerna för användaracceptans. En anledning till att det skulle kunna vara att det finns en oro för att det som skrivs på tangentbordet eller det som görs med musen ska registreras och användas till andra saker än autentisering eller identifiering. Till exempel för att mäta hur effektivt någon arbetar eller för att kunna se vad någon skriver.

Men när det kommer till att bli kontinuerligt övervakad är det endast de två metoderna som ens får positiva acceptansnivåer i undersökningen genomförd av Furnell, et al. (2000), förutom ansiktsigenkänningsmetoden som dock endast får 3,2%. Även för tangentbordshanteringsanalys och mushanteringsanalys är siffrorna låga, 25,5% respektive 21,8%. Trots detta var det ett relativt högt antal (46%) som ansåg att det var acceptabelt att autentiseringen eller identifieringen skulle kunna ske fortlöpande.

I både undersökningen av Deane, et al. (1995) och undersökningen av Furnell, et al. (2000) så är det inte troligt att någon av de tillfrågade har använt något biometriskt system i praktiken. Därför är undersökningen genomförd av SEARCH (2002) intressant eftersom i den har de som svarat att de har erfarenhet av en eller flera biometriska metoder fått uppge hur bekväma de kände sig med att använda just den eller de metoderna. Det visade sig att nästan alla de metoder som undersökningen tog upp ansågs vara bekväma eller åtminstone någorlunda bekväma att använda sig utav av minst en tredjedel av de tillfrågade personerna. Dock var det ingen som ansåg att de kände sig ens någorlunda bekväma med att använda sig av tangentbordshanteringsanalys. Här ska påpekas att det för det första bara var ett litet antal personer som hade erfarenhet av biometriska system (5%) i den här undersökningen (SEARCH, 2002) och att det bara var 7% av dessa som hade använt just tangentbordshanteringsanalys. Därför går det nog inte dra så stora slutsatser av just det resultatet förutom att de flesta av de som använt en biometrisk metod var bekväma med att använda sig av just den metoden. Detta skulle kunna tyda på att erfarenheter av biometriska metoder ökar acceptansen för dom samma.

### 6.3.3 Tilltro till biometri

Den allmänna acceptansen till biometri kan mätas i vilken tilltro som tekniken har hos människor i allmänhet. I undersökningen gjord av PTS (2004) uttrycks en positiv inställning till biometri och de tillfrågade framhåller framförallt bekvämligheten som den största fördelen med tekniken. Och enligt undersökningen CIC (2003) ansåg 85% att biometri skulle vara en effektiv metod för att skydda viktiga handlingar och dokument. Vilket visar på en i grund positiv inställning till biometritekniken som en säkerhetsmetod.

Acceptansnivån för användandet av biometriska identifierings- eller autentiseringsmetoder varierar för olika typer av tillämpningar. Enligt den amerikanska undersökningen SEARCH (2002) anser 91% att det var acceptabelt att de som ville köpa vapen skulle få sina biometriska egenskaper jämförda mot en databas över dömda brottslingar. Det samma gäller för personer som vill komma in på skolområden ansåg 87%. Däremot var det bara 41% som tyckte att det var acceptabelt att biometriska metoder användes för att undvika att personer utan rösträtt kunde delta i olika allmänna val. Och endast 24% tyckte att det var en bra idé att kasinon skulle övervaka sina besökare med hjälp av ansiktsigenkänningstekniker. Vilket kan bero på flera orsaker som till exempel att många eventuellt ställer sig negativa till just den tekniken eller att de inte vill bli identifierade på kasinon i allmänhet. Mest intressant var dock

att endast knappt hälften (46%) av de tillfrågade hade åsikten att det var mycket acceptabelt att biometriska metoder användes för skydd av känsliga uppgifter i ett datorsystem (SEARCH, 2002). Detta pekar nämligen på en brist på förtroende för biometritekniken som skydd i datorsammanhang. Men i allmänhet tycks det vara så att det finns en grundtilltro till tekniken som ett sätt att öka säkerheten. Dock är det nog viktigt att den metod som väljs för ett specifikt ändamål anses stå i proportion till just det syftet.

### 6.3.4 Misstro mot biometri

I undersökningarna togs även en del misstro mot biometriska system upp. Detta är intressant därför att det visar på det eventuella motstånd som införandet av ett biometriskt system skulle kunna stöta på. Det motstånd som kunde utläsas från PTS (2004) undersökningen var en oro för att använda vissa biometriska metoder och vad som skulle hända om egenskapen som användes för identifiering eller autentisering gick förlorad. Enligt CIC (2003) undersökningen ansåg 48% av de som deltog i undersökningen att införandet av biometriska tekniker skulle få ett negativt inflytande på deras personliga integritet. Detta eftersom de ansåg att det skulle vara lättare att blir spårad då. Och 45% trodde att risken var mycket stor att biometriska uppgifter skulle komma att missbrukas. Slutligen var det enligt samma undersökning 46% som inte trodde att biometritekniken skulle fungera.

Dessa siffror tyder på att det finns många som tvivlar på biometriteknikens effektivitet och att det är många som ser risker med tekniken med avseende på den egna integriteten. Därför är det antagligen viktigt att om ett biometriskt säkerhetssystem ska införas måste ett förtroende skapas dels för att tekniken fungerar och dels för att den information som används inte utnyttjas i några andra sammanhang.

### 6.3.5 Analys av resultatet för användaracceptansaspekten

Resultatet från studien visar på en låg medvetenhet om biometritekniken hos användare och en blandad tilltro och misstro till den samma. Det verkar finnas en tro på tekniken som ett sätt att öka säkerheten hos en del personer men det är ändå ganska många som inte litar på den. Eftersom medvetenheten var låg hos användarna kanske en del av svaret till misstron finns där. Men det är i alla fall säkert att ett företag eller en organisation som vill införa ett biometriskt säkerhetssystem bör informera de tänkta användarna ordentligt om både hur tekniken fungerar och syftet med den.

När det gäller acceptansen av specifika biometriska metoder finns vissa variationer mellan resultaten men i stort är de likvärdiga. Men den biometriska metod som fått det starkaste stödet hos användarna tycks vara fingeravtrycksavläsning och tangentbordshanteringsanalys tycks vara den metod som har det svagaste stödet. Det är också så att det enligt studien så verkar det vara så att stödet för en viss biometrisk metod är beroende av i vilken situation metoden tillämpas. Dock är undersökningen av Deane, et al. (1995) och undersökningen av Furnell, et al. (2000) båda ganska gamla. Då i synnerhet den förstnämnda undersökningen. Detta gör att det blir svårare att veta om resultaten från de undersökningarna fortfarande är aktuella i dagsläget vilket försvagar studiens resultat.

Ytterligare en aspekt som bör tas i beaktande angående resultatet av hela studien av användar-acceptansaspekten är att olika kulturer kan ha olika inställning till att använda sina biometriska egenskaper för identifiering eller autentisering. Både i allmänhet och i avseende på olika biometriska metoder. Nästan alla de undersökningar som den här studien har använt sig av är från länder med en mer eller mindre anglosaxisk kultur, nämligen Australien, Kanada, Storbritannien och USA. Det är därför inte alls säkert att resultaten skulle vara dom samma för användare med en annan kultur.

# 7. Slutsats

Den här rapporten har beskrivit hur en litteraturstudie genomförts för att besvara frågeställningen huruvida det är lämpligt för ett företag eller en organisation att införa ett biometriskt säkerhetssystem för autentisering eller identifiering. Arbetet har avgränsats till att studera aspekterna säkerhet, integritet och användaracceptans. Resultaten från litteraturstudien har analyserats och utifrån denna analys görs följande iakttagelser angående lämpligheten för införandet av ett biometriskt säkerhetssystem. Dessa iakttagelser kan inte ge ett ja eller nej svar på rapportens frågeställning för företag eller organisationer i allmänhet. Dock kan det spekuleras runt lämpligheten för åtminstone vissa företag eller organisationer.

## 7.1 Säkerhetsaspekten

Vid studien av säkerhetsaspekten så har syftet varit att försöka ge en överblick över vilka säkerhetsproblem som den biometriska tekniken förväntas kunna lösa och vilka säkerhetsproblem som tekniken kan föra med sig. Översikten har givits i from av en jämförelse med traditionella säkerhetsmetoder. Studiens resultat kan dock inte svara på huruvida biometriska säkerhetssystem i allmänhet är bättre eller sämre ur en säkerhets synvinkel än de traditionella metoderna för autentisering eller identifiering.

Dock är det så att alla säkerhetssystem av en viss typ, vare sig det är ett baserat på traditionella metoder eller ett baserat på biometriska metoder, inte behöver vara jämngoda med varandra sett ur en säkerhets synvinkel. Med detta menas att alla system som till exempel använder sig av lösenord inte behöver vara lika bra eller dåliga säkerhetsmässigt. Det kan alltså variera. En intressant fråga är då om det skulle kunna vara så att den lägsta säkerhetsnivå som biometriska säkerhetssystem kan inneha är högre eller lägre än den lägsta säkerhetsnivå som ett traditionellt säkerhetssystem kan inneha. Med avseende på att det i ett biometriskt säkerhetssystem inte finns några så kallade svaga lösenord, så som till exempel att användare kanske använder sitt inloggningsnamn som lösenord, kan det nog sägas att biometriska säkerhetssystem har en högre lägsta nivå än lösenordsbaserade säkerhetssystem.

De huvudsakliga resultaten av studien är att biometriska system tycks vara mer motståndskraftiga mot så kallade ”brute force” attacker och att lösenord som ibland kan vara lätta att gissa försvinner ifrån systemet. Säkerhetssvagheter som biometriska system för med sig är bland annat en känslighet mot så kallade ”replay” attacker. Dessutom så har ett flertal säkerhetssvagheter för ett generellt biometriskt system blivit identifierade vilka bör tas i beaktande vid införandet av ett biometriskt säkerhetssystem. Förvisso är några av dessa svagheter inte nya för säkerhetssystem i allmänhet. Slutsatsen är att det företag eller den organisation som vill införa ett biometriskt säkerhetssystem noga måste väga säkerhetsfördelarna mot säkerhetsriskerna utifrån de krav och behov som finns för den egna verksamheten.

Exempel på företag eller organisationer som troligen skulle kunna dra mest nytta av biometritekniken ur ett säkerhetsperspektiv är sådana företag eller organisationer som har höga säkerhetskrav i sin verksamhet. I dessa företag eller organisationer skulle biometriska säkerhetssystem kunna fungera som ett extra lager av skydd. Ett exempel på sådana organisationer skulle kunna vara olika militära institutioner.

## 7.2 Integritetsaspekten

För integritetsaspekten så har en överblick över de svenska lagar för skydd av den personliga integriteten som gäller vid behandlandet av biometriska egenskaper försökt uppnås. Slutsatsen är att det vid behandlandet av biometriska egenskaper i första hand är den svenska person-uppgiftslagen (PuL) som gäller. Eftersom biometriska egenskaper kan ses som person-uppgifter enligt den tolkning som görs av 29-gruppen (2003) i deras arbetsdokument om biometri. Detta dokument är till för att ge riktlinjer vid tillämpandet av de nationella lagarna om integritetsskydd i EU. Därför är det viktigt att ett företag eller en organisation som undersöker möjligheterna med ett biometriskt säkerhetssystem tar hänsyn till bestämmelserna i PuL.

## 7.3 Användaracceptansaspekten

Aspekten användaracceptans har undersökts i studien vilket givit de resultaten att det finns en tilltro till den biometriska tekniken men den är inte särskilt stark eftersom det även finns en hel del misstro. Därför är det för ett företag eller en organisation som planerar att införa ett biometriskt system viktigt att skapa ett förtroende för tekniken och att användarna kan garanteras att den biometriska information som lagras och bearbetas inte används till något annat än det ursprungliga syftet. En anledning till misstron på tekniken kan vara den låga kunskapsnivån om tekniken som studien kunnat påvisa genom de undersökningar som bearbetats. Därför är det också troligen så att det vid införandet av ett biometriskt säkerhets-system vore en fördel att de tänkta användarna blir utbildade om biometritekniken för att göra införandet mer lyckat. Studien har också genom att jämföra olika undersökningar kommit fram till att acceptansen av olika biometriska metoder för autentisering eller identifiering varierar mellan de olika metoderna. Vilket visar på att det är viktigt att hänsyn tas till vilken metod som har störst chans att bli accepterad. Det kan också vara så att acceptansen för en viss metod är beroende av i vilket sammanhang den tillämpas enligt vissa av studiens resultat. Därför så bör ett företag eller en organisation ta hänsyn till vilken metod som av de framtida användarna anses vara den som är mest lämpad för ändamålet.

Eftersom det verkar finnas en koppling mellan det uppfattade behovet av skydd och acceptansen för biometri så är det troligen så att det i första hand är företag eller organisationer som har krav på sig att vara säkra som kan dra störst nytta av biometritekniken. Detta eftersom det då till och med skulle kunna ses som något direkt positivt om biometriska skyddstekniker infördes. Till exempel skulle det kunna vara så att en bank som inför sådan teknik som ett extra skydd får ett ökat förtroende då det kan vara så att bankens kunder känner att deras pengar är säkrare.

## 7.4 Förslag till fortsatt arbete

Vidare studier som skulle kunna göras utifrån det här arbetet är till exempel att undersöka andra aspekter så som kostnadseffektivitet, prestanda, eller träffsäkerhet. Eller så skulle studier för att undersöka ett specifikt företags eller en specifik organisations behov med avseende på någon av de i den här rapporten identifierade aspekterna kunna genomföras. Eller andra former av fördjupade studier av dessa aspekter. Vidare skulle så skulle också efterforskningar kunna genomföras för att identifiera ytterligare aspekter som bör tas hänsyn till vid införandet av ett biometriskt säkerhetssystem.

# 8. Diskussion

Det för arbetet huvudsakliga problemet har varit att identifiera och välja ut lämplig litteratur. Då i synnerhet för säkerhetsaspekten där det finns en mycket stor uppsjö att material att tillgå vilket har lett till att studien av den aspekten har blivit ganska översiktlig. Och dessutom till att det finns en överhängande risk att resultatet är vinklat på något sätt då tidsbegränsningar gjort att relativt få källor har kunnat tas i beaktande.

För integritetsaspekten så var det ursprungligen tänkt att svenska lagar för skyddet av den personliga integriteten vid behandlandet av biometriska egenskaper skulle undersökas. Då endast en lag kunde identifieras (PuL) studerades den närmare och med hjälp av det arbetsdokument om biometri som antagits av 29-gruppen (2003). Det kan vara så att studiens resultat på den här punkten är lite vagt då det inte anges i vilken mån de riktlinjer för behandlingen av biometriska egenskaper som finns i det arbetsdokumentet efterföljs i Sverige. Det kan dock sägas här för diskussionens skull att det enligt det intryck som författaren fått från den information som återfinns på Datainspektionens hemsida (www.datainspektionen.se) så verkar det som att inspektionen arbetar utifrån dessa riktlinjer. Detta kan även skönjas i det samrådsbeslut som omnämns i deras årsrapport (Datainspektionen, 2003). Därför kanske studien från början borde ha haft utgångspunkten att undersöka på vilket sätt Datainspektionen behandlar frågor om biometri. Vidare bör det kanske också nämnas att det efter studiens genomförande framkommit att ett förslag till ändring av personuppgiftslagen (SOU 2004:6, Översyn av personuppgiftslagen) har lagts fram men enligt den sammanfattning som lästs av ändringsförslaget så verkar det inte som om dessa ändringar har någon direkt inverkan på behandlandet av biometriska uppgifter.

För aspekten användaracceptans så var det svårt att bedöma de bakomliggande syftena med de undersökningar som blev funna. Och det var också svårt att hitta nyare undersökningar som behandlade acceptansen för olika metoder vilket har gjort att resultatet har blivit något svagt då det inte alls är säkert att samma inställning till metoderna fortfarande är aktuell idag. Därför hade det varit bra för studien av den här aspekten om någon form av egen undersökning hade kunnat göras, till exempel en enkätundersökning eller en intervjustudie.

För att klargöra eventuell subjektivitet från författarens sida kan det vara bra att påpeka följande. Det är rapportförfattarens åsikt att biometri är en spännande teknik under utveckling och som åtminstone borde kunna användas till att öka säkerheten vid autentisering och identifiering i form av ett komplement till de traditionella metoderna. Det vill säga om hänsyn tas till de risker som denna teknik för med sig för den personliga integriteten. Dessutom så tror rapportförfattaren att acceptansen för användandet av biometriska egenskaper vid autentisering eller identifiering avgörs till stor del hur tekniken presenteras för de som ska använda den och i vilket syfte tekniken används.

# Referenser

29-gruppen (2003) Arbetsdokument om biometri. *EU kommissionen Art.29 Data Protection Working Party*. Tillgänglig på Internet: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp80_sv.pdf [Hämtad 04.01.23].

Befring, E. (1994) *Forskningsmetodik och statistik.* Lund: Studentlitteratur.

Bell, J. (2000) *Introduktion till forskningsmetodik.* Lund: Studentlitteratur.

Berndtsson, M., Hansson, J., Olsson, B. & Lundell, B. (2002) *Planning and implementing your final year project with success! A guide for students in computer science and information systems*. London: Springer.

Bolle, R. M., Connell, J. H. & Ratha, N. K. (2002) Biometric perils and patches. *Pattern Recognition Letters, 35*, 2727-2738.

CentralNic (2001) *Password clues, the CentralNic password survey report.* Tillgänglig på Internet: http://www.centralnic.com/page.php?pid=73 [Hämtad 04.02.28].

CIC (2003) Tracking public perceptions of biometrics. *Citizenship and Immigration Canada*. Tillgänglig på Internet: www.cic.gc.ca/english/press/03/poll-biometrics-e.pdf [Hämtad 04.04.23].

Datainspektionen (2004) Datainspektionens årsredovisning 2003. *Datainspektionen*. Tillgänglig på Internet: http://www.datainspektionen.se/pdf/arsredovisningar/arsred_03.pdf [Hämtad 04.04.29].

Dawson, C. W. (2000) *The essence of computing projects: a student's guide*. Harlow: Pearson Education Limited.

Deane, F., Barrelle, K., Henderson, R. & Mahar, D. (1995) Perceived acceptability of biometric security systems. *Computers & Security, 14*, 225-231.

Derakhshani, R., Schuckers, S. A. C., Hornak, L. A. & O'Gorman, L. (2003) Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners. *Pattern Recognition, 36*, 383-396.

Furnell, S. M., Dowland, P. S., Illingworth, H. M. & Reynolds, P. L. (2000) Authentication and supervision: a survey of user attitudes. *Computers and Security, 19*, 529-539.

Gifford, M. M., McCartney, D. J. & Seal, C. H. (1999) Networked biometrics systems – requirements based on iris recognition. *BT Technology Journal, 17*, 163-169.

Hong, L., Jain, A. K. (1999) Multimodal biometrics. I: A. K. Jain, R. Bolle & S. Pankanti (red:er), *Biometrics personal identification in networked society* (s. 327-344). Boston: Kluwer Academic Publishers.

Jain, A. K., Ross, A. & Prabhakar, S. (2004) An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology, 14*, 4-20.

Kim, H-J. (1995) Biometrics, is it a viable proposition for identity authentication and access control? *Computers and Security, 14*, 205-214.

Klein, D. V. (1990) *”Foiling the cracker”: a survey of, and improvments to, password security*. Carnegie Mellon University. Tillgänglig på Internet: ftp://ftp.cert.dfn.de/pub/docs/crypt/foiling-cracker.ps.gz [Hämtad 04.02.28].

de Luis-García, R., Alberola-Lopez, C., Aghzout, O. & Ruiz-Alzola, J. (2003) Biometric identification systems. *Signal Processing, 83*, 2539-2557.

Matyas, S. M., Stapleton, J. (2000) A biometric standard for information management and security. *Computers and Security, 19*, 428-441.

Morris, R. T., Thompson, K. (1979) Password security: a case history. *Communications of the ACM, 22*, 594-597.

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

Pfleeger, C. P. (2003) *Security in Computing*. Upper Saddle River, NJ: Prentice Hall.

Prabhakar, S., Pankanti, S. & Jain, A. K. (2003) Biometric recognition: security and privacy concerns. *IEEE SECURITY & PRIVACY, 1*, 33-42.

PTS (2004) Användningen av elektronisk identifiering och signaturer - PTS-ER-2004:3. *Post- och telestyrelsen.* Tillgänglig på Internet: http://www.pts.se/Archive/Documents/SE/Anv_elektronisk_identifiering_signaturer_PTS_ER_2004-3.pdf [Hämtad 04.04.27].

Ratha, N. K., Connell, J. H. & Bolle, R. M. (2003) Biometrics break-ins and band-aids. *Pattern Recognition Letters, 24*, 2105-2113.

Rejman-Greene, M. (2001) Biometrics – real identities for a virtual world. *BT Technology Journal, 19*, 115-121.

Rejman-Greene, M. (2002) Secure authentication using biometric methods. *Information Security Technical Report , 7*, 30-40.

Rudin, N., Inman, K., Stolovitzky, G., Rigoutsos, I. (1999) DNA based identification. I: A. K. Jain, R. Bolle & S. Pankanti (red:er), *Biometrics personal identification in networked society* (s. 287-309). Boston: Kluwer Academic Publishers.

Sasse, M. A., Brostoff, S. & Weirich, D. (2001) Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*, 122-131.

SEARCH (2002) Public attitudes toward the uses of biometric identification technologies by government and the private sector. *SEARCH The National Consortium for Justice Information and Statistics*. Tillgänglig på Internet: www.search.org/policy/bio_conf/Biometricsurveyfindings.pdf [Hämtad 04.04.26].

Spafford, E. H. (1992) *Observing Reusable Password Choices. Purdue University*. Tillgänglig på Internet: ftp://ftp.cerias.purdue.edu/pub/papers/gene-spafford/spaf-OPUS-observe.pdf [Hämtad 04.02.28].