

Biometri och personlig integritet

- biometriska säkerhetsfunktioners påverkan på individens personliga integritet samt hur detta beaktas

Karin Jansson
Veronica Wahrman

Magisteruppsats 20 poäng¹
Institutionen för Data- och Systemvetenskap
Stockholms Universitet

Handledare: Yngve Monfelt

¹ Uppsatsen motsvarar 20 poäng för vardera författare.

Sammanfattning

Biometriska säkerhetsfunktioner för autentisering blir allt vanligare för rutinmässiga tillämpningar i vardagen, som i skolor, banker samt på arbetsplatser. Där kan de t.ex. användas för inloggning på datorer samt för att få fysisk åtkomst till lokaler. Istället för lösenord kan t.ex. fingeravtryck användas för att autentisera en individ. Detta ökar säkerheten eftersom en biologisk egenskap, som fingeravtryck, inte lätt kan stjälas, tappas bort eller lånas ut. Då syftet med biometriska säkerhetsfunktioner för autentisering är att kontrollera en individs uppgivna identitet, uppkommer dock kritiska aspekter ur ett integritetsperspektiv. Samtidigt som de biometriska säkerhetsfunktionerna ska skydda oss från personligt intrång på ett bättre sätt än tidigare finns dock risker att de kränker den personliga integriteten.

Målet med denna studie är att utreda om, och i så fall hur, den personliga integriteten kan kränkas vid användning av biometriska säkerhetsfunktioner för autentisering och vilka krav som därför bör ställas i samband med dessa. Utöver detta avses även att ta reda på om, och i så fall hur, företag i praktiken beaktar den personliga integriteten när de utvecklar eller i sin verksamhet använder biometriska säkerhetsfunktioner för autentisering.

För att uppnå dessa mål har vi med hjälp av sekundärdata tagit fram en definition av begreppet personlig integritet för att på så sätt reda ut om, och hur, den kan påverkas av de risker som biometriska säkerhetsfunktioner kan föra med sig. Vidare har krav som beaktar den personliga integriteten presenterats och i anslutning till detta även hur kraven kan skydda den personliga integriteten. Vi fann att de biometriska säkerhetsfunktionerna kränker alla de variabler som ingår i definitionen av personlig integritet samt att det därför finns flera krav man bör beakta. Svaren på det frågeformulär som skickades ut till företagen tyder på att man beaktar den personliga integriteten men kanske på ett något ensidigt sätt.

Våra förhoppningar med studien samt dess resultat är att öka medvetenheten hos både företagen och de tänkta användarna kring problemområdet. Om de tänkta användarna blir uppmärksamma och får exempel på hur de biometriska säkerhetsfunktionerna kan kränka deras personliga integritet, tror vi att det kan leda till att biometribranschen kommer att arbeta mer med detta. Studiens resultat kan även göra biometribranschen mer uppmärksam på problematiken och därigenom få den mer fokuserad på vilka aspekter av den personliga integriteten som man bör beakta. Att vår undersökning ger en antydning om att några företag ser på den personliga integriteten ur ett något ensidigt perspektiv, gör att man kan önska mer av företagen inom detta område. Kanske kan detta få allmänheten i form av de framtida användarna att bli mer medvetna om dagens situation och kräva mer av biometribranschen i framtiden.

Nyckelord: biometri, personlig integritet, autentisering, fingeravtryck

Biometrics and privacy

- biometric systems effect on the individual's privacy and how this is taken into consideration

Abstract

Biometric authentication systems are being more frequently used in ordinary life, such as in schools, banks and at places of work. At these places the biometric authentication system can be used for login in on a computer or getting physical access to premises. Instead of using a password, a fingerprint can be used to authenticate an individual. This increases the security since a biological characteristic can not easily be stolen, lost or lend out. The purpose of the biometric authentication systems is to check an individual's identity. This will raise critical aspects concerning the individual's privacy. So, at the same time as biometric authentication systems will protect us from invasion of privacy in a more secure manner than before, they also can violate an individual's privacy.

The aim of this thesis is to examine if, and how, the individual's privacy can be violated when using biometric authentication systems, and which measures one should take into consideration to protect privacy. Further, the purpose of the thesis is to examine if, and how, companies in practise handle the individual's privacy when developing or using biometric authentication systems.

To achieve the purposes of the thesis we have, by analyzing literature, created a definition of privacy in order to examine if, and how, biometric authentication systems will affect it. Further, we have presented measures one should take into consideration when developing and using biometrics systems, and how those measures can protect the individual's privacy. The results showed that biometric authentication systems violate all of the variables that are included in the definition of privacy, and, because of this, there are several measures one should take into consideration. The answers of the questionnaire that was sent to companies indicate that they take the individual's privacy into consideration, although maybe in a one-sided way.

Our expectation with the thesis and its results, is to increase the companies' and the prospective users' awareness within this domain. If the prospective users can be aware of how biometric authentication systems can violate their privacy, we think it can force the biometric industry to work more with this aspect. The results of the thesis can also make the biometric industry more aware of the problem with biometrics and privacy, and therefore make them to take privacy into consideration in several ways. The fact that our study indicates that some companies handle privacy maybe a bit one-sided, makes one require a little bit more. Maybe this can make the prospective users more aware of the situation of today and therefore demand more of the biometric industry in the future.

Keywords: biometrics, privacy, authentication, fingerprints

Innehållsförteckning

1 INLEDNING	1
1.1 BAKGRUND	1
1.2 PROBLEMBESKRIVNING	3
1.3 FRÅGESTÄLLNINGAR	3
1.4 MÅL	3
1.5 SYFTE OCH MÅLGRUPP	3
1.6 AVGRÄNSNING	4
1.7 METOD	4
1.7.1 BAKGRUNDSARBETE	5
1.7.2 TEORI	5
1.7.3 EMPIRISK UNDERSÖKNING	5
1.8 TIDIGARE ARBETEN INOM OMRÅDET	6
1.9 DEFINITIONER	6
1.10 DISPOSITION	6
2 METOD	8
2.1 UPPSATSENS STRUKTUR OCH UPPLÄGG	8
2.2 VAL AV METOD	8
2.2.1 VAL AV METOD FÖR TEORIDELEN	8
2.2.2 VAL AV METOD FÖR EMPIRIDELEN	9
2.3 ALTERNATIVA METODER	10
2.4 URVAL AV UNDERSÖKNINGSENHETER	10
2.5 VALIDITET OCH RELIABILITET	10
2.5.1 VALIDITET OCH RELIABILITET FÖR TEORIDELEN	11
2.5.2 VALIDITET OCH RELIABILITET FÖR EMPIRIDELEN	11
2.6 KÄLLKRITIK	11
3 BIOMETRI	13
3.1 BESKRIVNING AV EN BIOMETRISK SÄKERHETS FUNKTION FÖR AUTENTICERING	13
3.1.1 ENROLLERING	13
3.1.2 AUTENTICERING	14
3.2 OLIKA BIOMETRISKA EGENSKAPER	15
3.3 FINGERAVTRYCK	17
3.3.1 FINGERAVTRYCKETS FORM	18
3.3.2 DESIGN AV EN FINGERAVTRYCKSBASERAD BIOMETRISK SÄKERHETS FUNKTION	18
4 PERSONLIG INTEGRITET	22
4.1 DEFINITION AV PERSONLIG INTEGRITET	22
4.1.2 SAMMANFATTANDE DEFINITION AV PERSONLIG INTEGRITET	23
4.2 KRÄNKNING AV DEN PERSONLIGA INTEGRITETEN	24
4.2.1 HOT MOT DEN PERSONLIGA INTEGRITETEN	25
4.3 LAGSTIFTNING SOM REGLERAR DEN PERSONLIGA INTEGRITETEN	26
4.3.1 EG-DIREKTIVET, 95/46/EG, OM PERSONUPPGIFTER	26
4.3.2 PERSONUPPGIFTLAGEN, PUL	27
5 BIOMETRINS RISKER FÖR DEN PERSONLIGA INTEGRITETEN	28
5.1 BIOMETRISK UPPGIFT SOM PERSONUPPGIFT	28

5.2 KRÄNKNING AV DEN PERSONLIGA INTEGRITETEN I SAMBAND MED BIOMETRISKA SÄKERHETSFUNCTIONER.....	29
5.2.1 HEMLIG IGENKÄNNING OCH BRIST PÅ ANONYMITET	29
5.2.2 SEKUNDÄR ANVÄNDNING AV BIOMETRISKA UPPGIFTER	30
5.2.3 EXPONERING AV BIOMETRISKA UPPGIFTER GENOM SYSTEMATTACKER.....	32
5.2.4 AVSLÖJANDE AV KÄNSLIG INFORMATION	33
5.2.5 SYSTEMFEL.....	34
5.2.6 LAGRING.....	35
6 SKYDDSÅTGÄRDER FÖR ATT BEAKTA DEN PERSONLIGA INTEGRITETEN I SAMBAND MED BIOMETRI	37
6.1 DEFINIERA SYFTE OCH VARAKTIGHET.....	37
6.2 BEGRÄNSAD BEHANDLING	38
6.3 ÖPPENHET	38
6.3.1 INFORMATION TILL INDIVIDEN OCH SAMTYCKE FRÅN DENSAMMA	39
6.4 VIDTA TEKNISKA SÄKERHETSÅTGÄRDER.....	40
6.4.1 DIGITAL PROFIL	40
6.4.2 DECENTRALISERAD LAGRING	41
6.4.3 KRYPTERING.....	41
6.5 ANVÄNDARKONTROLL	42
6.6 BEAKTA LAGSTIFTNING OCH RIKTLINJER.....	43
6.7 UPPDELNING AV KRAVEN FÖR UTVECKLING RESPEKTIVE ANVÄNDNING	44
6.8. SAMMANFATTNING TEORIDELEN.....	46
7. EMPIRISK UNDERSÖKNING.....	47
7.1 GENOMFÖRANDE.....	47
7.1.1 UNDERSÖKNINGENS RESPONDENTER.....	47
7.1.2 FRÅGEFORMULÄRET	48
7.2 RESULTAT	50
7.2.1 RESULTAT UTVECKLING.....	51
7.2.2 RESULTAT ANVÄNDNING	52
7.3. ANALYS	53
8. SLUTSATS OCH DISKUSSION.....	56
8.1 TEORI	56
8.1.1 SLUTSATS FÖR TEORIDELEN.....	56
8.1.2 DISKUSSION KRING TEORIDELEN	57
8.2 EMPIRI.....	60
8.2.2 SLUTSATS FÖR EMPIRIDELEN	60
8.2.1 DISKUSSION KRING EMPIRIDELEN.....	61
8.3 FÖRSLAG TILL VIDARE FORSKNING.....	65
REFERENSER.....	66
BÖCKER.....	66
INTERNET.....	66
BILAGOR	71
BILAGA 1: DEFINITIONER.....	71
BILAGA 2: FRÅGEFORMULÄR	75
BILAGA 3: E-POSTSVAR FRÅN CHARLOTTE ROSENGREN-EDGREN, SAS.....	83

Figurförteckning

Figur 1: Modell över en biometrisk säkerhetsfunktion för autentisering.	13
Figur 2: Exempel på applikationer där man använder fingeravtrycksigenkänning.....	18
Figur 3: Förgrening av fingeravtryckets åsar och upphörande av fingeravtryckets åsar...	19
Figur 4: Svårigheten med att matcha fingeravtryck.	21
Figur 5: Översikt över teorin.	46

1 Inledning

1.1 Bakgrund

I samhällen som blir mer beroende av IT-system, och där värdefull information hanteras inom och mellan dessa IT-system, leder detta till att kraven på säkerhet ökar. Det blir allt viktigare att kunna säkerställa vem som är vem, vem som ska få tillgång till vilken information, och vem som har gjort vad. Därigenom räcker det inte längre med att endast använda sig av traditionella metoder, framförallt lösenord, för att säkerställa en identitet. [Nilsson 97] Ett lösenord är inte unikt, i och med att det inte är direkt bundet till en individ. Detta kan leda till att lösenordet utnyttjas av en annan individ. En lösning på detta problem, som blir allt vanligare, är att använda biometri för **autenticering**² av individer. Detta innebär att en individs fysiska eller beteendemässiga egenskaper används och mäts för **verifiering*** och/eller **identifiering*** av denne. Fingeravtryck och röst är exempel på fysiska egenskaper medan signatur är ett exempel på en beteendemässig egenskap [DI 1]. Till skillnad från t.ex. lösenord kan de biologiska egenskaperna inte lätt stjälas, tappas bort eller lånas ut, vilket ökar säkerheten.

Syftet med en biometrisk säkerhetsfunktion är således att erbjuda autenticering, vilket är en process som möjliggör verifiering och/eller identifiering av en individ. Verifiering innebär att fastställa om en individ verkligen är den som den utger sig för att vara genom att individen först påstår en identitet genom att presentera sin biometriska egenskap. Den biometriska uppgiften jämförs sedan mot en redan lagrad biometrisk uppgift från samma individ. Här sker således en **en-mot-en-jämförelse***. Denna typ av jämförelser görs t.ex. när en individ vill få åtkomst till sitt bankkonto, då det krävs en kontroll som ser till att endast den behöriga individen får åtkomst till bankkontot. Här behövs ingen genomsökning eller **matching*** i någon databas över flera lagrade biometriska uppgifter, utan endast en kontroll över validiteten i den presenterade biometriska uppgiften görs. [Tomko 98] Här lagras således individens biometriska uppgift på t.ex. ett **smart kort*** som endast individen själv har tillgång till och som endast innehåller just dennes biometriska uppgift. Vidare kan verifieringsprincipen också användas för att t.ex. avgöra om en individ är behörig att öppna en dörr [Fingerprint Cards 00]. När identifiering krävs måste däremot en **en-mot-många-jämförelse*** göras för att urskilja en individ från andra individer, och på så sätt få reda på vem individen är. Det innebär således att en individs biometriska uppgift jämförs med flera andra individers biometriska uppgifter som finns lagrade i en databas. Denna typ av jämförelser görs t.ex. i applikationer inom hälsovården, och i registreringsystem över t.ex. röstning och körkort. En en-mot-många-jämförelse är också en metod som används av polisen för att identifiera brottslingar. [Tomko 98] Ett annat tillämpningsområde är närvarokontroll [Fingerprint Cards 00]. En identifieringskontroll med hjälp av biometri vid en flygplats för att förhindra att terrorister går ombord på flygplanen kräver också en en-mot-många-jämförelse [Prabhakar et al 03].

² Ord som i uppsatsen markeras med **fet** stil och med * förklaras i en definitionslista som finns i Bilaga 1.

Efter attackerna mot USA den 11 september 2001 uttrycks behov av att förstärka säkerheten runt om i världen för att minska förekomsten för liknande händelser [Gilså 03]. En åtgärd USA planerar för att höja säkerheten är att alla länder som har avtal med dem om visum-fria inresor ska införa biometri i sina pass under hösten år 2005 [Norlin 04]. USA:s krav gör att man inom Europeiska Unionen, EU, diskuterar huruvida passen för EU-medborgarna ska innehålla **biometriska uppgifter*** [Bjurman 03]. Vidare har händelsen den 11 september 2001 inneburit att den personliga integriteten får stå tillbaka till förmån för kontroll. Detta har även medfört en förändrad attityd hos individer och inom rättsväsendet som bl.a. inneburit att polis och andra myndigheter har fått ökade befogenheter att söka efter personliga uppgifter. [Ström 03] I t.ex. USA ställer man krav på enklare kartläggning och registrering av personliga uppgifter, vilket är något som man efterliknar i många europeiska länder. Regeländringar som påverkar den personliga integriteten, som tidigare skulle ha lett till långdragna diskussioner, har genomförts snabbt utan sedvanliga diskussioner. [Bjurman 03] Detta kan leda till kompromisser gällande den personliga integriteten i och med att säkerhetskraven verkar dominera över kraven för att skydda den personliga integriteten.

En aspekt som ofta påpekas i samband med biometri är just den personliga integriteten. I och med de höga krav som nu ställs på säkerheten vid autentisering, och som de **biometriska egenskaperna*** anses uppfylla, har skyddet av den personliga integriteten fått stå tillbaka. [ARBDOK 03] "Risken för att en utbredd och okontrollerad användning av biometri föranleder oro beträffande skyddet av individens grundläggande fri- och rättigheter", skriver Arbetsgruppen för dataskydd i ett arbetsdokument om biometri [03].

Den personliga integriteten kommer upp redan i själva begreppet biometri eftersom det handlar om individens beteendemässiga och fysiska egenskaper och därmed möjliggör en unik identifiering av honom/henne. Vidare måste de biometriska uppgifterna lagras någonstans, t.ex. i en databas. Man kan då inte utesluta risken för att databasen kan utnyttjas av tredje part för jämförelser eller i forskning för andra ändamål än vad som var avsikten från början. Med tanke på att biometri blir vanligare och även börjar användas för rutinmässiga tillämpningar, som i t.ex. skolor³ och bibliotek⁴, finns också risk att allmänheten blir mindre uppmärksam på hur behandling av dessa uppgifter kan påverka dem. [ARBDOK 03]

Den snabba utvecklingen och den allt bredare tillämpningen av biometriska egenskaper har således gett upphov till kritik och rädsla för att de **biometriska säkerhetsfunktionerna*** inte förmår att skydda den personliga integriteten. Samtidigt som det hävdas att de biometriska säkerhetsfunktionerna skyddar oss från personligt intrång på ett bättre sätt än tidigare, påstås det från annat håll att de i sig ger upphov till personligt intrång [Crompton 02a]. Peter Moon, IT-jurist, har sagt följande: "Det finns mycket pengar i biometri och industrin har för bråttom med att

³ I Kvarnbyskolan i Tensta, Stockholm, använder eleverna sitt fingeravtryck för att logga in på datorerna.

⁴ I skolbibliotek i Australien och Storbritannien använder man tumavtryck istället för lånekort.

släppa sina produkter. När man misslyckas för att tekniken inte är färdig kommer integriteten i kläm”. [DI 1]

1.2 Problembeskrivning

I och med att autentisering är en metod för att kontrollera en individs uppgivna identitet uppkommer kritiska aspekter ur ett integritetsperspektiv. Risker för att en **bedräglig aktör*** t.ex. stjälar en behörig individs identitet och utför handlingar i dennes namn är en risk för den personliga integriteten. Om identiteten är förknippad med biometriska uppgifter blir aspekterna för den personliga integriteten problematiska. Enbart själva upplevelsen av ett intrång i den personliga integriteten blir obehagligare och svårare att värja sig emot om t.ex. ens fingeravtryck exponeras än om ens lösenord gör det. Biometriska egenskaper är personliga, omöjliga att ersätta, och avslöjar mer information om en individ än enbart individens identitet. I och med detta och att de existerar under en individs hela livscykel uppstår flera sårbara punkter som kan utsätta individens personliga integritet för fara. Hur de biometriska uppgifterna lagras och hur övrig verksamhet kring de biometriska säkerhetsfunktionerna för autentisering hanteras, kommer således att ha inverkan på den personliga integriteten.

1.3 Frågeställningar

Utifrån ovan presenterade bakgrund och problembeskrivning har vi formulerat följande frågeställningar:

1. Kräns biometriska säkerhetsfunktioner för autentisering den personliga integriteten, och i så fall hur?
2. Vilka krav bör ställas i samband med utveckling och användning av biometriska säkerhetsfunktioner för autentisering, för att skydda den personliga integriteten?
3. Beaktar man i praktiken vid utveckling och användning av biometriska säkerhetsfunktioner för autentisering den personliga integriteten, och i så fall hur?

1.4 Mål

Målet är att utifrån en definition av begreppet personlig integritet utreda om, och i så fall hur, den personliga integriteten kränks i samband med biometriska säkerhetsfunktioner för autentisering. Vi har även som mål att ta fram krav som därför bör ställas i samband med dessa för att skydda den personliga integriteten. Utöver detta avser vi även att via ett frågeformulär undersöka om, och hur, företag som utvecklar eller använder biometriska säkerhetsfunktioner för autentisering beaktar den personliga integriteten.

1.5 Syfte och målgrupp

Målgruppen för den här studien är företag som utvecklar, samt företag som i sin verksamhet använder, biometriska säkerhetsfunktioner för autentisering. Utvecklare bör vara medvetna om hur den personliga integriteten kan kränkas i samband med biometri samt hur den kan skyddas genom de krav man bör ställa på biomet-

riska säkerhetsfunktioner för autentisering. Detta för att de ska kunna utveckla biometriska säkerhetsfunktioner för autentisering som värnar om den personliga integriteten. Företag som nyttjar biometriska säkerhetsfunktioner för autentisering i sin verksamhet bör också vara medvetna om detta, så att användarna inte får sin personliga integritet kränkt.

Syftet med studien är även att göra, både nutida och framtida, användare av biometriska säkerhetsfunktioner, uppmärksamma på hur deras integritet kan kränkas i samband med biometri. Detta för att vidare göra dem medvetna om hur deras personliga integritet kan skyddas genom de krav man bör ställa på biometriska säkerhetsfunktioner för autentisering.

En fördel när man läser vår uppsats är att man har grundläggande kunskaper inom ämnet data- och systemvetenskap. Vi anser dock att uppsatsen är skriven på en så allmän och grundläggande nivå att även allmänt intresserade läsare kan förstå uppsatsens innehåll.

1.6 Avgränsning

Uppsatsen tar endast upp de vanligaste biometriska egenskaperna som kan användas för autentisering. Vidare berörs dessa enbart kortfattat och istället koncentrerar vi oss på fingeravtryck i studien, då fingeravtryck är den vanligaste förekommande egenskapen som används vid autentisering.

En annan avgränsning har att göra med geografisk inriktning. Den empiriska undersökningen, som avser att besvara den tredje frågeställningen, är främst inriktad på förhållandena i Sverige. I och med att det än så länge finns få företag som utvecklar och använder biometriska säkerhetsfunktioner för autentisering i Sverige har vi därför blivit tvungna att även vända oss utomlands. Vi har då tagit kontakt med företag i länder som vi via olika källor fått kännedom om. Ett krav har dock varit att företagen finns i länder inom EU. Detta pga. att vi i uppsatsen endast berör lagstiftning inom Sverige och EU. För litteraturstudien, som avser att besvara de två första frågeställningarna, har vi däremot inte gjort några särskilda avgränsningar vad gäller geografisk inriktning då vi anser att riskerna för den personliga integriteten som biometriska säkerhetsfunktioner för autentisering för med sig, inte skiljer sig åt mellan länder.

Ytterligare en avgränsning som vi gör i uppsatsen gäller litteraturens detaljeringsgrad. Vi har valt att undvika tekniska detaljbeskrivningar och istället hålla uppsatsen på ett allmän och övergripande nivå. Detta beror på att vi inte har någon tidigare erfarenhet eller någon tidigare kunskap inom det valda studieområdet.

1.7 Metod

Nedan beskrivs kortfattat hur vi gått tillväga när vi bedrivit arbetet med uppsatsen. Utförligare metodbeskrivning görs i kapitel två.

1.7.1 Bakgrundsarbete

Bakgrundsarbetet med studien påbörjades hösten 2003 genom breda litteraturstudier och efterforskning via Internet om information inom biometriområdet. Även kontakt med personal inom biometribranschen togs. Genom dessa kontakter fick vi reda på att kombinationen biometri och personlig integritet är ett aktuellt område som för närvarande diskuteras. Med detta som utgångspunkt fortsatte vi att göra litteraturstudier inom nämnda områden. Det som då utkristalliserade sig var att den personliga integriteten i samband med biometri är ett omtvistat ämne som det finns olika uppfattningar om. Med tanke på att nyttjandet av biometri för autentisering dessutom är ett relativt nytt fenomen är problematiken kring den personliga integriteten i samband med detta inte ordentligt utredd. Detta fick oss att anta problemet med personlig integritet i samband med användning av biometri som vår studiefokus.

1.7.2 Teori

Den teoretiska delen av uppsatsen bedrivs som en kvalitativ litteraturstudie och avser att besvara de två första frågeställningarna som är satta för uppsatsen. Teorin som består av kapitlen tre till sex, tar upp hur en allmän biometrisk säkerhetsfunktion är uppbyggd, vad personlig integritet innebär, vilka risker de biometriska säkerhetsfunktionerna för autentisering för med sig, samt vilka krav man bör ställa vid utveckling och användning av biometriska säkerhetsfunktioner för autentisering. Diskussion och slutsats görs sedan i kapitel åtta.

De fakta som vår teori grundar sig på har hämtats från böcker och från Internet. Den teoretiska studien presenterar och resonerar kring om, och hur, den personliga integriteten kränks vid nyttjandet av biometriska säkerhetsfunktioner för autentisering samt hur den personliga integriteten kan skyddas vid beaktande av krav som man bör ställa i samband med biometriska säkerhetsfunktioner för autentisering. Målet är att utreda, och därmed skapa en förståelse för, de frågeställningar vi valt att undersöka.

1.7.3 Empirisk undersökning

Utöver den teoretiska studien utförs även en empirisk studie som avser att besvara den tredje frågeställningen som är satt för uppsatsen. Den empiriska delen av uppsatsen utgörs av en kvalitativ undersökning i form av ett frågeformulär med öppna och slutna frågor som företag som utvecklar och använder biometriska säkerhetsfunktioner för autentisering förväntas besvara via e-post. Syftet med den kvalitativa aspekten av undersökningen är att vi vill skapa en helhetsbild och inte påverka eller styra respondenterna i deras svar. Vi vill få en förståelse för den praktiska verkligheten, dvs. om, och hur, företag som utvecklar respektive använder biometriska säkerhetsfunktioner för autentisering beaktar den personliga integriteten.

Den empiriska delen av uppsatsen består av kapitel sju där genomförandet av undersökningen beskrivs, samt där resultaten av undersökningen presenteras och analyseras. Diskussion och slutsats av den empiriska undersökningen görs sedan i kapitel åtta.

1.8 Tidigare arbeten inom området

Det har skrivits en del om de risker, vad gäller den personliga integriteten, som biometriska säkerhetsfunktioner för autentisering medför. I rapporter och i artiklar på Internet samt i tidningar nämns ofta den personliga integriteten i samband med biometri, men djupare kartläggning och utredning kring varför och hur den personliga integriteten faktiskt kränks, verkar inte ha gjorts. Det som framkommit inom litteraturstudien är t.ex. ett arbetsdokument om biometri framtaget av Arbetsgruppen för dataskydd [03] vars syfte är "att bidra till en effektiv och enhetligt tillämpning av de nationella bestämmelserna om dataskydd som antagits i överensstämmelse med direktiv 95/46/EG om biometriska system" [ARBDOK 03]. Detta dokument visar på ett initiativ till att beakta de lagar som finns för personuppgifter vid användning av biometriska säkerhetsfunktioner.

Det finns även flera rapporter som behandlar just biometri och personlig integritet, t.ex. "Consumer Biometric Applications: A Discussion Paper" av Ann Cavoukian [99], "Biometrics and privacy - the end of the world as we know it or the white knight of privacy?" av Crompton, Malcolm [02], och "Biometric Recognition: Security and Privacy Concerns" av Prabhakar et al [03]. Även det utarbetade tillägget till **Common Criteria***, "Common Criteria: Common Methodology for Information Technology Security Evaluation: Biometric Evaluation Methodology Supplement" av Common Criteria Biometric Evaluation Methodology Working Group [02], som är en metod för att utvärdera biometriska produkter, kan också till viss del betraktas som ett arbete inom området biometri och personlig integritet.

I och med att ovan nämnda arbeten tar upp aspekter som berör vårt studieområde, har dessa varit av intresse för vår studie. Vi använder därför dem som källor i vår studie.

1.9 Definitioner

Ord som uppträder i uppsatsen och som behöver förklaras markeras med **fet** stil och med * första gången det förekommer. Förklaring av ordet ges i en definitionslista som finns i Bilaga 1.

1.10 Disposition

Kapitel 2 presenterar uppsatsens struktur, den metod som valts för uppsatsen, samt alternativa metoder som skulle kunna användas för att uppnå studiens mål. Även urval av undersökningsenheter, validitet och reliabilitet samt källkritik, tas upp och diskuteras i kapitel två.

Kapitel 3 beskriver vad biometri är och hur en biometrisk säkerhetsfunktion för autentisering är uppbyggd. Vidare ges i kapitlet en presentation över olika biometriska egenskaper som kan utnyttjas i en biometrisk säkerhetsfunktion, samt en närmare beskrivning av fingeravtryck och hur en fingeravtrycksbaserad biometrisk säkerhetsfunktion är utformad.

Kapitel 4 redogör för begreppet personlig integritet samt för de lagar som berör den personliga integriteten i Sverige och inom EU.

Kapitel 5 ger en presentation över de risker som biometriska säkerhetsfunktioner för autentisering för med sig. I samband med detta ges resonemang kring hur dessa risker kränker den personliga integriteten.

Kapitel 6 redogör för de krav som man vid utveckling och användning av biometriska säkerhetsfunktioner för autentisering bör beakta för att på så sätt värna om den personliga integriteten. Även hur dessa krav skyddar den personliga integriteten presenteras.

Kapitel 7 redogör för hur uppsatsens empiriska studie genomförts. Även studiens resultat presenteras och analyseras i kapitel sju.

Kapitel 8 utgörs av slutsats och diskussion av både den teoretiska och av den empiriska studien. Här ges även förslag till vidare forskning inom området biometri och personlig integritet.

Bilaga 1 - Definitioner.

Bilaga 2 - Frågeformulär.

Bilaga 3 - E-postsvar från Charlotte Rosengren-Edgren, SAS.

2 Metod

I det här kapitlet presenteras hur uppsatsen är strukturerad, vilken metod som valts för uppsatsens teoretiska och empiriska del samt vilka alternativa metoder som kunde ha valts. Utöver detta presenteras urvalet av undersökningsenheter och där- efter tas det upp hur validitet och reliabilitet hanteras i uppsatsen samt källkritik.

2.1 Uppsatsens struktur och upplägg

Uppsatsen består av en teoretisk del och en empirisk del. Den teoretiska delen utgörs av kapitel tre till sex, med slutsats och diskussion i kapitel åtta, och avser att svara på de två första frågeställningarna som är satta för studien. Kapitel tre och fyra, som tar upp biometri respektive personlig integritet, fungerar som utgångspunkt och underlag för kapitel fem och sex. Kapitel fem avser att utreda frågeställning ett, dvs. om, och i så fall hur, biometriska säkerhetsfunktioner för autentisering kränker den personliga integriteten. Frågeställningen besvaras sedan i kapitel åtta. Frågeställning två, dvs. vilka krav som bör ställas i samband med biometriska säkerhetsfunktioner, utreds i kapitel sex och besvaras sedan i kapitel åtta. Den empiriska delen utgörs av kapitel sju, med slutsats och diskussion i kapitel åtta, och avser att besvara frågeställning tre, dvs. hur man i praktiken vid utveckling och användning av biometriska säkerhetsfunktioner beaktar den personliga integriteten.

2.2 Val av metod

Metod är ett redskap som används för att uppnå de målsättningar man har med t.ex. en undersökning. Metodvalet bör göras utifrån de frågeställningar man har och med tanke på vilken kunskap man vill komma fram till. Kvalitativa och kvantitativa metoder är två angreppssätt som man kan använda. De kvalitativa metoderna har primärt ett förstående syfte, vilket innebär att de ska ge en bättre förståelse för de faktorer man undersöker. Kvalitativa metoder har även en ringa grad av formalisering. Kvantitativa metoder är i sin tur mer formaliserade och strukturerade till sin natur och präglas av en större kontroll från forskarens sida. Utöver det så avgör de kvantitativa metoderna vilka svar som är tänkbara när man utför en undersökning. [Holme et al 97]

I denna uppsats används kvalitativa metoder både i den teoretiska delen samt vid den empiriska undersökningen. Detta i och med att uppsatsens mål primärt är att skapa en djupare förståelse för det ämne som tas upp. I den teoretiska delen försöker vi förstå, och själva tolka hur biometriska säkerhetsfunktioner för autentisering påverkar den personliga integriteten. I den empiriska delen försöker vi förstå om, och hur, man vid utveckling och användning av biometriska säkerhetsfunktioner för autentisering beaktar den personliga integriteten.

2.2.1 Val av metod för teoridelen

Den teoretiska delens mål försöker vi uppnå genom en kvalitativ litteraturstudie där vi avser att studera och presentera sekundärdata i form av skriven litteratur samt rapporter och artiklar från Internet. Vid informationsinsamling skiljer man i huvudsak mellan primärdataundersökningar och sekundärdataundersökningar

[Dahmström 00]. Studiens teoretiska del bedrivs som en sekundärdataundersökning. Den bygger på att man i arbetet använder sig av redan insamlad information som finns i form av t.ex. publikationer och böcker [Dahmström 00]. Utöver detta gör vi även egna tolkningar och bildar egna uppfattningar utifrån sekundärdata när det gäller att utreda om, och hur, den personliga integriteten kränks. Detta beror dels på att den personliga integriteten är något subjektiv, men också på att vi inte funnit någon litteratur som lite djupare beskriver på vilka sätt den personliga integriteten kan kränkas i samband med biometriska säkerhetsfunktioner.

Då vi inte har någon kunskap kring det valda studieområdet sedan tidigare, bedrivs den teoretiska studien som en iterativ process. Detta innebär att vi under arbetets gång gått tillbaka i studien för att modifiera och komplettera det som tidigare gjorts.

2.2.2 Val av metod för empiridelen

För den empiriska undersökningen utformas ett frågeformulär med öppna och slutna frågor. De frågor som har fasta svarsalternativ följs dock av följdfrågor där respondenten, beroende av sitt svar, kan utveckla sina svar kring frågans innehåll. De öppna frågorna innebär således att varje respondent får svara fritt, vilket ger respondenten en möjlighet att svara med egna ord och utan allt för stor påverkan från vår sida. Vi vill med de öppna frågorna undvika att respondenterna svarar på ett sätt som de tror att vi förväntar oss. Detta är också anledningen till varför frågorna i frågeformuläret inte är direkt baserade på teorin där vi presenterar vilka krav som man bör beakta vid utveckling och användning av biometriska säkerhetsfunktioner. Vi tror att detta skulle vara ledande och ge svar som vi är ute efter men som kanske inte stämmer överens med verkligheten. Nackdelen med att använda sig av öppna frågor är att respondenterna kan tröttna och tycka att det är besvärligt att besvara frågor av denna karaktär. Denna risk har vi försökt minimera genom att ha få frågor.

Frågeformuläret skickas till respondenterna per e-post. Detta sätt valdes då det geografiska avståndet till vissa respondenter är stora. Trots att några av respondenterna finns på närmare håll och därigenom skulle ha kunnat intervjuas, valde vi att skicka frågeformuläret per e-post även till dem. Orsaken till detta är att ge alla respondenter samma utgångspunkt. Skulle vi intervjua några av respondenterna skulle det kunna leda till t.ex. skevhet då dessa respondenter därigenom skulle kunna ställa frågor till oss och vi därmed medvetet eller omedvetet skulle kunna ha påverkat dem. Ytterligare en fördel med att använda e-post är att respondenterna ges möjlighet att ge genomtänkta svar. Respondenterna får god tid på sig att svara och behöver inte känna sig stressade av en intervjuare. Nackdelar med att använda e-post är att man inte får den närhet till respondenten som är viktigt vid kvalitativa metoder. På så sätt hamnar vi långt ifrån den verklighet vi vill undersöka. Dessutom har intervjuer via e-post en tendens att inte bli lika uttömmande som vid en intervju öga-mot-öga.

I och med att den empiriska delen består av material som samlas in för första gången, dvs. primärdata, är den empiriska delen av studien en primärdataundersökning.

2.3 Alternativa metoder

Den empiriska undersökningen kan även angripas med enbart ett kvantitativt angreppssätt. Då skulle man t.ex. ha kunnat utforma en enkät med fördefinierade svarsalternativ som man skickar till respondenterna. Det man då undersöker är generaliseringar av den företeelse man vill undersöka [Holme et al 97]. Vi ansåg dock att risken med detta tillvägagångssätt är att respondenterna skulle kunna försköna verkligheten om de i frågeformuläret inte behöver uttrycka sina egna åsikter. Ett annat alternativ att utföra den empiriska undersökningen på är att man gör personliga intervjuer med respondenterna öga-mot-öga. Detta förfaringssätt förkastades dock då de geografiska avstånden i vissa fall är stora.

2.4 Urval av undersökningsenheter

Respondenterna i den empiriska undersökningen består av personer som representerar företag som i sin verksamhet utvecklar eller använder biometriska säkerhetsfunktioner för autentisering. Personerna har valts på basen av att de har en inblick i själva området biometri och personlig integritet. Detta val gjordes genom att vi via e-post bad om att få skicka frågeformuläret till den person som ansvarar för utvecklingen respektive användningen av de biometriska säkerhetsfunktionerna på företaget.

I och med att det i Sverige finns få företag som utvecklar och använder biometriska säkerhetsfunktioner för autentisering, har vi inte gjort något traditionellt urval. Urvalet är istället baserat på att vi tagit kontakt med de företag som vi via olika källor, t.ex. andra biometriföretag som Precise Biometrics, fått kännedom om. Ett krav har dock varit att företagen finns inom EU. De företag som är med i undersökningen är de som svarar ja på vår förfrågan att delta i den.

2.5 Validitet och reliabilitet

Reliabilitet (pålitlighet) bestäms av hur man utför mätningar och hur noggrann man är vid bearbetningen av den insamlade informationen. Reliabiliteten är hög om lika och oberoende mätningar av ett och samma fenomen ger samma eller ungefär samma resultat. Validiteten (giltigheten) är beroende av vad det är man mäter och om detta är utklarat i frågeställningen som man utgår ifrån. Hög validitet har man om man i hög utsträckning mäter den teoretiska egenskap man söker efter, dvs. om man mäter det man avser att mäta. [Holme et al 97]

Reliabilitet har inte samma centrala plats i kvalitativa undersökningar som de har i kvantitativa undersökningar. Detta beror på att kvalitativa undersökningars syfte är att skapa en bättre förståelse för vissa faktorer, vilket gör att den statistiska representativiteten inte har lika stor betydelse. Trots detta bör man även i kvalitativa undersökningar ta hänsyn till reliabiliteten. [Holme et al 97]

Problemet med validitet är inte lika stor i kvalitativa undersökningar. Detta då man vid kvalitativa undersökningar har en större närhet till det eller den som undersöks. Den kvalitativa metodiken gör det även möjligt för enheten att själv styra över sin medverkan. [Holme et al 97]

2.5.1 Validitet och reliabilitet för teoridelen

Reliabiliteten för den teoretiska delen av uppsatsen bestäms bl.a. av hur pålitlig den insamlade informationen är samt hur den tolkas. I och med att vi till stor del använder oss av digitala källor kan det leda till att reliabiliteten blir lidande. Vi har dock försökt använda oss av så trovärdiga digitala källor som möjligt. Med trovärdiga digitala källor menar vi officiella digitala källor och digitala källor med källangivelser. Dessutom har vi använt oss av många olika källor som beskriver samma fenomen på liknande sätt. Som nämnts har reliabilitet även med tolkning att göra. I och med att den teoretiska delen av uppsatsen är av kvalitativ karaktär och bygger på egna tolkningar är dock reliabiliteten av underordnad betydelse. Stor fokus ligger på den personliga integriteten och hur den påverkas i samband med biometri. Den personliga integriteten är något subjektivt och man bör vara medveten om att våra egna värderingar och tolkningar utgör en del av uppsatsen.

I och med den subjektivitet som ligger i tolkningen av personlig integritet kan man också anta att validiteten blir lidande. Vi har dock försökt kompensera detta med att ha en tydlig frågeställning och en distinkt definition av begreppet personlig integritet som vi i studien utgår ifrån. På så sätt har det blivit lättare att verkligen undersöka det vi avser att undersöka. Validiteten för den teoretiska delen av uppsatsen har även att göra med huruvida målet stämmer överens med uppsatsens innehåll. För att uppnå detta har vi under arbetets gång kontinuerligt gått tillbaka till kapitel ett där målet för studien anges. På så sätt kan vi undvika att vi under arbetets gång hamnar på sidospår och börjar undersöka något som inte stämmer överens med det vi avser att undersöka.

2.5.2 Validitet och reliabilitet för empiridelen

Även den empiriska undersökningen är av kvalitativ karaktär vilket gör att reliabiliteten blir av underordnad betydelse. Detta eftersom det även här handlar om egna uppfattningar och föreställningar, men i detta fall respondenternas. Vi är ute efter respondenternas uppfattningar och vi vill undvika att vi påverkar dem eller leder in dem på ett specifikt spår. Reliabiliteten borde dock bli hög då respondenterna får god tid på sig att svara, får svara relativt fritt och kan uttrycka svaren men egna ord.

Validiteten handlar om huruvida vi får giltiga svar från respondenterna. Eftersom vi inte baserar frågorna på teorin utan ställer fristående öppna frågor, hoppas vi att vi undviker att styra respondenterna. På så sätt försöker vi öka chanserna till att respondenterna inte svarar så som de tror att vi vill att de ska svara. Eftersom vi inte är ute efter att mäta resultaten är det också lättare att ställa relevanta frågor som verkligen undersöker det vi avser att undersöka, vilket torde öka validiteten.

2.6 Källkritik

Vi har till stor del baserat studien på digitala källor då böcker som behandlar biometri har varit svårt att få tag på. Dessutom är det oftast lättare att få tag på aktuell information om man använder sig av digitala källor. Man ska dock alltid vara kritisk till digitala källor och deras vetenskapliga dignitet. De digitala källor som vi använt oss av har vi dock upplevt som officiella, t.ex. Common Criteria, rapport

från EU och Datainspektionen. Dessutom har vi försökt undvika sådana digitala källor som inte har några källangivelser.

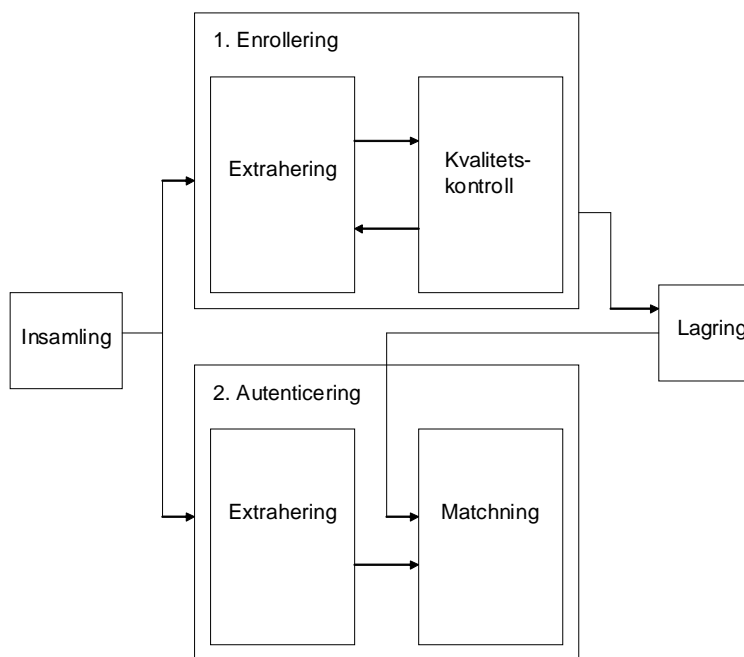
I och med att vi inte har några erfarenheter kring området biometri kan vissa fel-tolkningar av källorna ha gjorts.

3 Biometri

I det här kapitlet kommer vi att ge en introduktion till ämnet biometri. Kapitlet inleds med en översiktlig beskrivning av en allmän biometrisk säkerhetsfunktion för autentisering. Därefter ges en presentation över olika biometriska egenskaper som kan användas i en biometrisk säkerhetsfunktion. Kapitlet avslutas med en närmare beskrivning av fingeravtryck och hur en fingeravtrycksbaserad biometrisk säkerhetsfunktion är utformad.

3.1 Beskrivning av en biometrisk säkerhetsfunktion för autentisering

En biometrisk säkerhetsfunktion för autentisering består av teknisk utrustning och/eller datorprogram. Vidare konstrueras en biometrisk säkerhetsfunktion för två faser, **enrollering*** och autentisering. Vid enrollering insamlas en individs fysiska eller beteendemässiga egenskaper för att registrera och lagra dessa som **referens***. Vid autentisering insamlas individens fysiska eller beteendemässiga egenskaper för att jämföras med referensen som lagrades under enrolleringen. Om den tillförda egenskapen matchar referensen så är individen autentiserad. Figur 1 visar en modell över en biometrisk säkerhetsfunktion för autentisering.



Figur 1: Modell över en biometrisk säkerhetsfunktion för autentisering.
Källa: Egenmodifierad ur [Jain et al 97a]

3.1.1 Enrollering

För enrollering samlas de biometriska egenskaperna in med hjälp av en biometrisk avläsare. Vid enrolleringen registreras individer och detta sker således för varje ny individ som använder säkerhetsfunktionen. De insamlade uppgifterna behandlas sedan genom att de utsätts för **extrahering***. Det innebär att det fångas upp unika och karaktäristiska drag som sedan lagras som referens i form av en **digital pro-**

fil*. [Maltoni et al 03] Det är således inte individens ursprungliga biometriska egenskap som lagras utan en strukturerad förminskning av en biometrisk avbildning i form av ett numeriskt resultat som beräknas utifrån de unika egenskaperna, dvs. den digitala profilen. Behandling och lagring av de biometriska uppgifterna kan dock även ske i form av bilder som utgörs av rådata. [ARBODOK 03] Inför lagringen kan även **kryptering*** och **digital signering*** av referensen göras [CC 1].

Lagring av de biometriska uppgifterna kan ske på olika sätt beroende på säkerhetsfunktionens tillämpning och storleken på de biometriska uppgifterna som samlas in. Biometriska uppgifter kan antingen lagras lokalt inom den biometriska säkerhetsfunktionen, i en separat central databas utanför säkerhetsfunktionen, eller på ett smart kort som individen själv har kontroll över. För verifiering är det inte nödvändigt att lagra de biometriska uppgifterna från enrollerade individer i en databas utan det räcker med att de lagras decentraliserat på t.ex. ett smart kort eftersom det här endast krävs en en-mot-en-jämförelse. För identifiering krävs dock att de biometriska uppgifterna lagras i en central databas i och med att säkerhetsfunktionen måste matcha den inkommande biometriska uppgiften mot samtliga biometriska uppgifter som finns lagrade, dvs. en en-mot-många-jämförelse. [CC 1]

Vanligtvis utförs också en kvalitetskontroll under enrolleringsfasen. Detta för att försäkra att den biometriska uppgiften har tillräckligt hög kvalitet för att kunna användas som referens som de inkommande biometriska uppgifterna sedan ska matchas mot. Om det vid kvalitetskontrollen kommer fram att kvaliteten är låg måste extraheringen göras om tills en tillräckligt unik och pålitlig referens av de biometriska uppgifterna kan skapas. [CC 1]

3.1.2 Autenticering

För autenticering samlas de biometriska egenskaperna in med hjälp av en biometrisk avläsare för att verifiera och/eller identifiera en individ. Därefter behandlas de biometriska uppgifterna genom att de utsätts för extrahering för att sedan skapa ett exemplar av uppgifterna i form av en digital profil. [Maltoni et al 03] Som nämnades tidigare kan dock behandlingen av biometriska uppgifter även ske i form av bilder som utgörs av rådata [ARBODOK 03]. Den inkommande biometriska uppgiften jämförs därefter med den lagrade biometriska uppgiften som skapades under enrolleringsfasen för att bland dessa försöka hitta en matchande uppgift [Maltoni et al 03]. Ett matchningsförsök resulterar i en summa som, i de flesta fall, jämförs mot ett **gränsvärde***. Om summan överstiger gränsvärdet lyckas matchningen. Om summan är mindre än gränsvärdet misslyckas matchningen. [BioPrivacy 1] Summan som fås vid matchningsförsöket talar om hur väl den inkommande biometriska uppgiften stämmer överens med den lagrade referensen. Detta värde måste vara minst lika högt som gränsvärdet för att matchningen ska accepteras.

I en biometrisk säkerhetsfunktion kan det uppstå två typer av fel vid matchningen. Den första typen är falsk acceptans, False Acceptance Rate – **FAR***, och innebär att biometriska uppgifter från två olika individer misstas att komma från samma

individ. Det kan t.ex. resultera i att en obehörig individ, t.ex. en bedräglig aktör, får behörighet trots att han eller hon inte är behörig. Den andra typen av fel är falskt avslag, False Rejection Rate – **FRR***, vilket innebär att säkerhetsfunktionen misstar två biometriska uppgifter från samma individ att komma från två olika individer. Det kan t.ex. medföra att säkerhetsfunktionen inte släpper igenom en individ som är behörig. [Prabhakar et al 03] Att dessa fel uppstår kan bero på allt från smuts eller att de kroppsdelar som används är skadade till verkligt bedrägeri [Hochman 02]. Då de biometriska egenskaperna som samlas in varierar i kvalitet kan det ge upphov till att säkerhetsfunktionen inte lyckas matcha två biometriska uppgifter trots att de kommer från samma individ [BioPrivacy 1].

FAR och FRR är funktioner av den biometriska säkerhetsfunktionens gränsvärde. Om gränsvärdet är högt för att göra säkerhetsfunktionen mer tolerant mot t.ex. variationer i kvaliteten och smuts på de kroppsliga egenskaperna, ökar FAR. Om gränsvärdet är lågt för att göra säkerhetsfunktionen mer säker, ökar FRR. [Prabhakar et al 03]

En matchning kan ske mot en enstaka lagrad uppgift eller mot en lista bestående av flera lagrade uppgifter beroende på om syftet är verifiering eller identifiering. Matchning mot en enstaka lagrad biometrisk uppgift är vad som sker vid verifiering medan matchning mot flera lagrade biometriska uppgifter är vad som krävs vid identifiering. [CC 1]

3.2 Olika biometriska egenskaper

Man kan i en biometrisk säkerhetsfunktion använda vilken fysisk eller beteendemässig egenskap som helst, så länge den uppfyller följande krav [Maltoni et al 03]:

- Universiell – att varje individ har den karaktäristiska egenskapen.
- Unik – att egenskapen är utmärkande för varje individ, det får inte finnas två individer med samma identifierbara egenskap.
- Permanent – att egenskapen inte förändras med tiden.
- Mätbarhet – att egenskapen är kvantifierbar och kan mätas.

För olika tillämpningar finns det biometriska egenskaper som är mer eller mindre lämpliga. Varje biometrisk egenskap har styrkor och svagheter och vilken egenskap som passar bäst beror på säkerhetsfunktionens tillämpning, praktiska användning och den biometriska egenskapens kavaliteter. [Maltoni et al 03]

Följande biometriska egenskaper är de vanligaste [Maltoni et al 03]:

- **Ansikte** – Ansiktsgigenkänning är en av de mest accepterade biometriska metoderna. Detta då ansiktet är en av de vanligaste egenskaperna för igenkänning som människor använder i sina dagliga interaktioner. Vidare anses metoden inte vara påträngande. Det är dock en stor utmaning att utveckla tekniker för ansiktsgigenkänning som klarar av åldringseffekter, an-

siktsuttryck och hur ansiktet är placerat i förhållandet till den kamera som ska avläsa ansiktet.

- **DNA** – DNA (DeoxyriboNucleic Acid) är den unika koden för en individs egenart. Egenskapen innehåller dock flera begränsningar för att kunna användas för biometrisk igenkänning. En av dessa är att det är enkelt att stjäla en del av DNA från en individ och sedan utnyttja den för olovliga syften.
- **Gång** – Det sätt som en individ går på är en beteendemässig egenskap som kan användas som en biometrisk egenskap. Gångstilen är tillräckligt karaktäristisk för att man ska kunna använda den för identifiering i applikationer som har låga krav på säkerhet. Ett problem är dock att gångstilen förändras över tid, t.ex. vid viktförändring.
- **Hand- och fingergeometri** – Vissa kännetecken som är relaterade till den mänskliga handen, t.ex. fingerlängd, är relativt oföränderliga och karaktäristiska för att skilja individer åt. De är dock inte tillräckligt utmärkande vilket gör att säkerhetsfunktioner baserade på handgeometri oftast används för verifiering och inte för identifiering. Detta eftersom man vid identifiering skulle vara tvungen att urskilja egenskapen från övriga i en databas.
- **Iris** – Teknologin som utnyttjar iris som biometrisk egenskap anses vara exakt och snabb. Den är säker eftersom det inte finns två människor som har identiska iris, vilket även gäller för tvillingar. Irisskanning innebär att endast en ljusstråle och en videokamera behövs för att läsa av sammansättningen av ögats mönster [Halvarsson et al 00]. Detta innebär att det inte krävs någon nära kontakt mellan individen och avläsaren vilket ökar användaracceptansen [Hochman 02].
- **Lukt** – Varje individ avsondrar en lukt som i sin kemiska sammansättning är karaktäristisk för individen och som därför kan användas för att urskilja individer från varandra. En biometrisk säkerhetsfunktion som använder lukt för igenkänning består av kemiska sensorer som känner av en individs specifika lukt. Ett problem är dock att man är osäker på om en individs lukt kan kännas igen när denna använder deodorant.
- **Retina** – Retinan är ögats näthinna och är unik för varje individ och även för varje öga. Det påstås att retinaskanning är den mest säkra biometriska igenkänningsmetoden då det inte är lätt att ändra eller återskapa retinan. Retinaskanning innebär att en svag laserstråle riktas rakt in i ögat vilket dock gör metoden impopulär [Halvarsson et al 00].
- **Röst** – Röstigenkänning är en icke påträngande biometrisk metod som är accepterad hos allmänheten. En röst är dock inte tillräckligt unik för att man ska kunna urskilja denna från övriga röster i en större databas. En rösts signal för igenkänning är beroende av kvaliteten hos bl.a. mikrofonen som ska fånga in rösts signalen och kommunikationskanalen. Rösten i sig kan även påverkas av individens hälsa.
- **Signatur** – Sättet en individ skriver sitt namn på är karaktäristiskt för varje individ. Trots att signering kräver kontakt med ett skrivinstrument, och därmed kräver en viss ansträngning är metoden ändå accepterad på många håll. Signatur är en beteendemässig biometrisk egenskap som kan förändras över tiden och influeras av individens fysiska och känslomässiga tillstånd.

- **Tangentdynamik** – Man utgår från att varje individ trycker på tangentbordet på ett karaktäristiskt sätt. Tangentdynamik är en beteendemässig biometrisk egenskap och förväntas inte vara unik för varje individ men erbjuder ändå tillräcklig information för att kunna användas för verifiering.
- **Värmestrålning från kroppen** – Värmemönstret som en kropp alstrar är utmärkande för varje individ och kan fångas upp av en infraröd kamera utan att vara påträngande för individen.
- **Öra** – Örats form och struktur är utmärkande för varje individ och igenkänningen av örat baseras på en matchning av avståndet mellan framträdande punkter på örat.

Fingeravtrycksavläsning är den äldsta och mest välkända biometriska metoden [Hochman 02]. I och med att fingeravtryck är den mest utbredda och använda biometriska egenskapen i dagsläget [Halvarsson et al 00] presenteras den närmare nedan. Detta är också anledningen till att uppsatsen till största del fokuserar på fingeravtryck.

3.3 Fingeravtryck

Att fingeravtryck är den biometriska egenskap som rönt störst intresse beror på att den uppfyller alla de krav som en biometrisk egenskap måste uppfylla för att kunna användas i en biometrisk säkerhetsfunktion (se avsnitt 3.2). Varje individ har ett fingeravtryck och varje fingeravtryck är unikt och permanent, även om det temporärt kan förändras något på grund av t.ex. skärsår och väderförhållanden. [Maltoni et al 03] Endast iris och retina har liknande egenskaper, men säkerhetsfunktioner baserade på dessa två egenskaper är ofta dyra samtidigt som de kräver mycket utrymme och kan upplevas som obekväma att använda [Fingerprint Cards 00]. Fingeravtrycksavläsare är däremot relativt små och billiga, och när man kombinerar fingeravtrycksigenkänning med bl.a. kryptering anses säkerhetsfunktioner baserade på fingeravtryck dessutom vara svåra att överlista [Maltoni et al 03].

Eftersom fingeravtryck under lång tid har använts inom ordningsmakten och polisväsendet förknippas egenskapen ofta med brottslighet och kriminalitet. Detta är emellertid något som håller på att förändras och idag har teknik för fingeravtrycksigenkänning blivit allt populärare och vanligare även för rutinmässiga applikationer i vardagen. Framförallt beror detta antagligen på att behovet att bekämpa identitetsbedrägeri i vårt elektroniska samhälle ökar. Faktum är att fingeravtrycksbaserade säkerhetsfunktioner blivit så populära att de nästan blivit synonyma med biometriska säkerhetsfunktioner. [Maltoni et al 03] Exempel på användningsområden för applikationer med fingeravtrycksigenkänning är dator- och nätverksinloggning, kontroll av kunder innan de betalar med kreditkort, fysisk åtkomstkontroll, samt kontroll av immigranter vid flygplatser. Figur 2 visar dessa exempel.



Figur 2: Exempel på applikationer där man använder fingeravtrycksigenkänning.

Källa: Ur [Prabhakar et al 03]

3.3.1 Fingeravtryckets form

Ett fingeravtryck är ett stämpelliknande avtryck av fingertoppens papillarlinjemönster. Papillarlinjerna utgörs av åsar i huden på fingrarnas böjsida. Åsarna bildar mönster som är unika för varje individ. [NE 91a] I formationen av ett fingeravtryck förekommer så många variationer att det är omöjligt för två fingeravtryck att vara identiska [Maltoni et al 03].

De biologiska principerna för ett fingeravtryck är följande [Maltoni et al 03]:

- Fingeravtryckets papillarlinjemönster har olika kännetecken för olika fingeravtryck.
- Fingeravtryckets former är föränderliga, men förändringarna håller sig inom vissa gränser vilket möjliggör systematiska klassifikationer.
- Konturerna och detaljerna i papillarlinjemönstret i fingeravtrycket är permanenta och oföränderliga.

Ordet fingeravtryck ses ofta som en synonym till en unik särprägel, även om ett fingeravtrycks utmärkande drag inte är etablerad fakta utan en empirisk observation. Det börjar dock bli en allmän uppfattning att ett fingeravtrycks egenart vilar på vetenskapliga grunder i och med att fingeravtrycksigenkänning blivit populärt och används på många håll. [Maltoni et al 03]

3.3.2 Design av en fingeravtrycksbaserad biometrisk säkerhetsfunktion

En fingeravtrycksbaserad biometrisk säkerhetsfunktion fungerar och består av samma grundläggande komponenter som den allmänna biometriska säkerhetsfunktionen som beskrevs i avsnitt 3.1. Eftersom den här studien fokuserar på fingeravtryck följer här en närmare beskrivning av det som utmärker designen för en fingeravtrycksbaserad biometrisk säkerhetsfunktion. Vi kommer dock även här att hålla oss på en övergripande nivå och inte beskriva tekniska detaljer.

Insamling för enrolling och autentisering

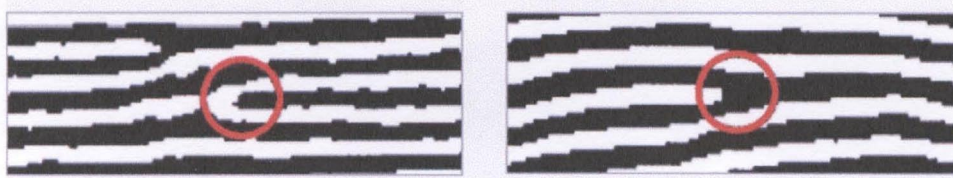
Det finns i huvudsak två metoder för att erhålla en fingeravtrycksbild: off-line och live-scan [Jain et al 97a]. Vid den första metoden, off-line-metoden, får man en bild av ett fingeravtryck genom att applicera bläck på fingertoppen och sedan trycka fingret på ett papper så att ett avtryck i bläck erhålles. Därefter digitaliseras avtrycket genom att pappret skannas med hjälp av en optisk skanner eller en högkvalitetskamera. [Maltoni et al 03] Live-scan är en metod som används för att få en bild av ett fingeravtryck genom att läsa av fingertoppen direkt utan att först generera avtrycket på ett papper [Jain et al 97a]. Detta görs med hjälp av en sensor

som kan digitalisera fingeravtrycket genom att komma i direktkontakt med det [Maltoni et al 03]. Det finns flera olika tekniker att använda för live-scan. Den mest använda tekniken är att använda sig av en optisk sensor bestående av en glaslins där fingret placeras. Under glaslinsen finns en ljuskälla och en kamera placerad. En laserstråle från ljuskällan belyser sedan glaslinsen så att kameran kan fånga in ljuset som reflekteras från linsen och skapa en bild av fingeravtrycket. [Jain et al 01b] Då optiska sensorer är för stora för att integreras i applikationer som t.ex. bärbara datorer, mobiltelefoner och digitala fickkalendrar har andra alternativa tekniker blivit allt vanligare. Exempel på en sådan teknik är solid-state. [Maltoni et al 03] En solid-state sensor har endast en liten kontaktyta för fingertoppen att vidröra. Detta gör att endast en begränsad del av fingeravtrycksmönstret läses av och därmed ger väldigt små fingeravtrycksrepresentationer jämfört med en optisk sensor. [Jain et al 01c]

För att kunna avgöra om två fingeravtryck kommer från samma finger eller olika fingrar är det nödvändigt att samla in oföränderliga kännetecken av fingeravtrycket [Jain et al 01b]. Detta för att det ska kunna skapas en representation av fingeravtrycket. En bildbaserad representation (eng. image-based representation) består av rådata, i form av pixlar, av fingeravtrycket [Jain et al 97a]. Användningsområden för säkerhetsfunktioner som använder sig av sådana representationer är dock begränsade på grund av bl.a. varierande ljusnyanser och variationer i bildkvaliteten [Jain et al 97a]. Dessutom kräver sådana typer av representationer stora lagringsutrymmen [Maltoni et al 03]. Vanligare är då att man använder sig av en minutiösbaserad representation (eng. minutiae-based representation) som lagras som punkter på en tvådimensionell yta. Till skillnad från en bildbaserad representation så baseras en minutiösbaserad representation inte på hela fingeravtrycket, utan koncentrerar sig på det mönster som de minutiösa och unika detaljerna i ett fingeravtryck bildar. [Jain et al 01b] Dessa förvärvas genom extraheringen som beskrivs närmare nedan.

Extrahering för enrollering och autenticering

En extraherande kapacitet försöker hitta och fånga in de minutiösa unika detaljerna från fingeravtrycket. De minutiösa detaljerna som man vill hitta utgörs dels av punkter där åsarna plötsligt upphör och dels av punkter där åsarna förgrenar sig och skiljer sig åt. [Maltoni et al 03] Figur 3 visar detta.



Figur 3: Förgrening av fingeravtryckets åsar (bilden till vänster) och upphörande av fingeravtryckets åsar (bilden till höger).

Källa: Ur [Jain et al 97a]

Om dessa punkter kan lokaliseras i ett fingeravtryck blir extraheringen en relativt lätt uppgift. Dessa punkter är dock inte alltid enkla att hitta och hur väl extraheringen fungerar är beroende av kvaliteten på det inkommande fingeravtrycket.

Även andra faktorer, som t.ex. abnorma formationer av fingeravtrycket, födelsemärken, och problem med anordningen som ska samla in de biometriska egenskaperna, påverkar hur enkelt strukturen på åsarna kan definieras för att de unika detaljerna ska kunna hittas. [Jain et al 97a]

Matchning för autentisering

Inför matchning får jämförelsemodulen i säkerhetsfunktionen två fingeravtryck. Det ena utgörs av det lagrade referensavtrycket och den andra av det inkommande avtrycket som ska matchas mot det lagrade referensavtrycket. Matchningsmodulen ska sedan bestämma om avtrycken stämmer överens och därmed kommer från samma finger. För att göra detta används ett gränsvärde som bestämmer om två fingeravtryck kommer från samma finger eller inte. [Jain et al 97a] Ett par fingeravtryck som genererar värden som är högre eller lika med gränsvärdet benämns som matchande par, dvs. avtrycken kommer från samma finger. Ett par av fingeravtryck som genererar värden som är lägre än gränsvärdet benämns som icke-matchande par, dvs. avtrycken kommer inte från samma finger. [Maltoni et al 03]

Säkerhetsfunktioner som använder sig av bildbaserade representationer av fingeravtryck använder ofta korrelationsbaserad matchning (eng. correlation-based matching). Här används rådatainformation direkt, och i stort sett innebär korrelationsbaserad matchning att två fingeravtrycksbilder läggs på varandra så att överensstämmelsen hos de båda bildernas pixlar för olika positioner kan beräknas. [Maltoni et al 03] Vid minutiösbaserad matchning (eng. minutiae-based matching), som baseras på extraherade minutiösbaserade representationer av fingeravtrycken, gäller det att hitta positioner i det minutiösa mönstret i det lagrade referensfingeravtrycket och det inkommande testfingeravtrycket som stämmer överens. [Jain et al 97a]

Att matcha fingeravtryck är ofta svårt i och med att det förekommer stora variationer i olika avtryck av samma finger. Det som orsakar dessa variationer är bl.a. att avtrycket inte utgörs av exakt samma område på fingret varje gång, att individen vrider fingret olika och trycker olika hårt varje gång han/hon avger avtrycket. [Maltoni et al 03] Ytterligare aspekter som kan försvåra matchningen är torrhet, sjukdomar, smuts och svett på huden som gör att representationen av fingeravtrycket inte blir av tillräckligt hög kvalitet [Jain et al 97a]. Detta gör att fingeravtryck från samma finger kan se väldigt olika ut från gång till gång samtidigt som fingeravtryck från olika fingrar ibland kan se ganska lika ut [Maltoni et al 03]. Figur 4 illustrerar detta.



Figur 4: Svårigheten med att matcha fingeravtryck.
De två övre fingeravtrycken kommer från samma finger,
men ser olika ut. De två nedre fingeravtrycken ser lika ut,
men kommer från olika fingrar.
Källa: Ur [Maltoni et al 03]

4 Personlig integritet

Kapitlet inleds med en presentation av begreppet personlig integritet. Utifrån några definitioner över begreppet ger vi en sammanfattande definition av dessa som vi kommer att utgå ifrån i uppsatsen. Därefter ges en kort introduktion till vad som kan kränka den personliga integriteten. Sist i kapitlet presenteras den lagstiftning som reglerar den personliga integriteten i EU och i Sverige.

4.1 Definition av personlig integritet

Det finns inte någon entydig definition på begreppet personlig integritet vilket gör det svårt att klargöra vad det egentligen innebär och handlar om. Det hela blir ännu mer komplicerat i och med att varje individ även har en personlig uppfattning om vad personlig integritet innefattar.

Vissa definitioner fokuserar på förhållandet mellan personlig integritet och anonymitet och individens rätt att bestämma över sig själv samt till vilken grad informationen om dem förs vidare till andra. Andra definitioner fokuserar på en individs okränkbarhet där en kränkning av den personliga integriteten utgörs av en överträdelse på en individs särprägel, värdighet och frihet. [Crompton 02b]

Personlig integritet ges olika definitioner i olika ordböcker. Bonniers svenska ordbok har följande förklaring på integritet; ”*okränkbarhet*” och ”*oberoende*”. Vidare innebär personlig något som ”*har med den enskilde individen att göra*”. [Bonniers 02] Personlig integritet innebär således okränkbarhet och oberoende som har med den enskilde individen att göra.

Nationalencyklopedins definition av personlig integritet är ”*rätt att få sin personliga egenart och inre sfär respekterad samt att inte utsättas för personligen störande ingrepp*”. Vidare säger man att personlig integritet har nära samband med människans värdighet. Begreppet personlig integritet definieras dock olika i olika sammanhang. I Regeringsformen säger man att ”*den offentliga makten skall utövas med respekt för [...] den enskilda människans frihet och värdighet*” medan man i de lagar som styr hälso- och sjukvården benämner personlig integritet som ”*respekt för självbestämmande och integritet*”. [NE 94b]

Informationstekniska Standardiseringen i Sverige (ITS) anser att personlig integritet har med insyn, användning och kvalitet hos de personliga uppgifterna att göra [ITS 94].

Att begreppet personlig integritet definieras på olika sätt kan göra att begreppet uppfattas som brett. Om en individ vågar stå upp för sina åsikter säger man att den individen har integritet. Men vad man i andra sammanhang menar med personlig integritet har mycket att göra med en individs privatliv. Privatliv kan beskrivas som en personlig sfär där man har rätt att vara för sig själv. [Ström 03]

På 1890-talet definierade Louis Brandeis, domare i USA:s högsta domstol, personlig integritet som ”*individens rätt att bli lämnad ifred*” (egen översättning).

Att bli lämnad ifred innebär att en individ ska få begrunda, ifrågasätta, växa, utvecklas, göra misstag och prova på nya sätt att uppleva intimitet utan att andra lägger sig i. Detta kräver i sin tur att individen ges viss avskildhet och anonymitet. Anonymitet är således ett sätt för individen att uppnå en viss grad av personlig integritet. Anonymitet har att göra med hur mycket uppmärksamhet som riktas mot individen, dvs. huruvida individen är oidentifierad. [Crompton 02b]

Robert Ellis Smith, chefsredaktör på Privacy Journal, definierar personlig integritet som [Laurant 03]:

”En önskan hos varje individ för fysiskt utrymme där hon kan vara fri från störningar, intrång, förlägenhet, eller ansvarsskyldighet samt individens försök att själv kontrollera när och hur information om denne avslöjas” (egen översättning).

En annan beskrivning av personlig integritet togs fram av en brittisk kommitté, The Calcutt Committee, inriktad på journalistisk etik och tillsatt med anledning av massmedias förföljelse av kändisar [Ström 03]:

”Individens rätt till skydd mot intrång i hans eller hans familjs personliga liv eller angelägenheter, med direkt fysiska medel eller publicering av information.”

I artikel 12 av den allmänna förklaringen om de mänskliga rättigheterna från 1948 skriver man [FN]:

”Ingen ska vara föremål för godtyckliga intrång i integriteten (privacy), familj, hem eller korrespondens, inte heller för angrepp på hans heder eller rykte. Alla har rätt till lagens skydd mot sådana intrång eller angrepp.”

Personlig integritet kan också innebära personlig frihet, dvs. att människan ska få behålla känslan av kontroll över sig själv och sin närmiljö samt inte fräntas sitt personliga ansvar. Det innebär att personlig integritet inte behöver ha med spridning av personuppgifter att göra utan att det enbart kan handla om att ha full kontroll att bestämma över sitt eget handlande. [Ström 03]

4.1.2 Sammanfattande definition av personlig integritet

Utifrån de ovan nämnda definitionerna på begreppet personlig integritet kommer vi att ge en sammanfattande definition av begreppet. Detta för att definitionerna inte är entydiga och för att envar har sin egen uppfattning om begreppet. När personlig integritet tas upp i uppsatsen är det följande definition vi utgår ifrån:

Med personlig integritet menar vi individens möjlighet att bli lämnad ifred och få vara anonym [Crompton 02b]. Dessutom handlar personlig integritet även om värdighet [NE 94]. Vi anser därför att personlig integritet även handlar om att inte få sin värdighet kränkt. Vidare ska individen själv få kontrollera och bestämma över sitt handlande [Ström 03] och över sina personliga uppgifter [Laurant 03]. Dessutom innebär personlig integritet att insyn, användning och kvalitet hos de personliga uppgifterna ska skyddas [ITS 94].

För att definitionen ska kunna användas i uppsatsen och för att man ska förstå vad de olika variablerna i definitionen innebär, förklaras dessa närmare nedan.

Att bli lämnad ifred handlar om att man ska få lugn och ro, inte bli störd och få vara för sig själv när man själv vill. Det handlar även om att andra inte ska lägga sig i ens angelägenheter och att man inte ska övervakas.

Anonymitet handlar om att identiteten inte ska göras tillgänglig eller avslöjas för obehöriga [ITS 94].

Med **värdighet** menas att man som människa ska känna att man har ett värde och social status. Man ska få känna att man har ett socialt anseende och att man behandlas med respekt och uppskattning.

Att **själv få kontrollera och bestämma över sitt handlande** handlar om att ingen annan ska fatta en individs beslut och att ingen annan har rätt att utan individens vetskap och samtycke övervaka dennes beteende. Detta innebär även att man ska få **kontrollera och bestämma över sina personliga uppgifter**, dvs. att ingen annan än individen själv ska få tillgång till, kunna ändra i och använda dem utan individens vetskap och samtycke.

Att **insyn, användning och kvalitet hos de personliga uppgifterna ska skyddas** har med informationssäkerhet att göra. Det innebär att hantering av information ska skyddas med avseende på tillgänglighet, kvalitet, sekretess och spårbarhet [ITS 94]. Tillgänglighet innebär att information ska vara åtkomlig och användbar för behöriga entiteter [Gollman 99]. Vidare innebär detta att behöriga entiteter ska få nyttja information i förväntad utsträckning och inom önskad tid. Kvalitet har att göra med informationens användbarhet för en given individ. Kvalitetsaspekter på information kan vara objektiv felfrihet, noggrannhet, detaljeringsgrad, validitet, tillförlitlighet och konsistens. Objektiv felfrihet innebär att inga fel inträffar i processen, från insamling till användning, som påverkar informationskvaliteten. Noggrannhet innebär hur väl de specificerade egenskaperna mäts och erhåller ett värde. Detaljeringsgrad kan uttryckas i hur många klasser som beskriver ett fenomen, i detta fall informationen. Ju fler klasser desto större detaljeringsgrad. Med validitet menas att den avsedda och specificerade kvaliteten faktiskt uppnås genom t.ex. uppdateringar. Tillförlitlighet innebär i vilken grad informationen levererar den kvalitet den avser sig leverera samt tilltro till denna grad. Konsistens innebär i vilken grad information stämmer överens med varandra i ett system. Med sekretess menas att innehållet i informationen inte får göras tillgängligt eller avslöjas för obehöriga. Spårbarhet innebär att det ska finnas funktioner som gör det möjligt att entydigt härleda utförda operationer till enskilda individer. [ITS 94]

4.2 Kränkning av den personliga integriteten

Man tar ofta den personliga integriteten för given och ägnar den ingen tanke förän den kränks och man då upplever förolämpning, maktlöshet och irritation [Ström 03].

Med kränkning av den personliga integriteten menar vi att en eller flera av variablerna av definitionen i avsnitt 4.1.2. inte är uppfyllda.

4.2.1 Hot mot den personliga integriteten

Hotet mot den personliga integriteten kan huvudsakligen komma från tre olika håll, nämligen den offentliga sektorn, företag och enskilda individer. Hoten från de tre grupperna är olika till sin karaktär. [Ström 03]

Offentliga sektorn har lagen på sin sida och kan därmed tvinga individer att lämna ifrån sig information om sig själva till t.ex. olika myndigheter. Myndigheter kan även samköra olika informationskällor för att skapa en mer fullständig bild av en individ. Det är något som kan öka risken för kränkning av den personliga integriteten. [Ström 03]

Företag är ett mindre hot, jämfört med den offentliga sektorn eftersom företag endast har tillgång till information inom sitt egna begränsade område. Det går därför inte lika lätt för företag att sammanställa olika data från olika källor för att få en helhetsbild av en individ. Då företagen även bör ta i beaktande att inte stöta sig med sina kunder kan det utgöra en återhållande faktor vid insamling av information av deras kunder. Något som dock kan öka företagen som hot mot den personliga integriteten är deras lönsamhetskrav. Detta kan leda till att företag använder informationen de har om sina kunder för andra ändamål än som var syftet från början. [Ström 03]

Då personlig information i digital form blir allt mer lättillgänglig och omfattande för allmänheten ökar risken att individer i ens omgivning tar reda på information om en. Detta kan man t.ex. göra genom att utnyttja **offentlighetsprincipen*** och offentliga register. [Ström 03]

Allt detta då obehöriga får reda på information om en individ och använder informationen för syften utan individens vetskap och samtycke riskerar att kränka den personliga integriteten. Detta i och med att individen då inte har kontroll över sina personliga uppgifter och sitt handlande och därigenom kan övervakas utan dennes vetskap och samtycke.

Ett annat hot mot den personliga integriteten, förutom de tre ovan nämnda, är hotet från informationsteknologin. Ser man på IT-system så innebär det att ju mer enhetliga de är, dvs. att samma standard används i olika sammanhang och över ett stort geografiskt område, desto mer underlättas en eventuell övervakning av individer. Genom att använda en **unik identifierare***, som t.ex. personnummer, underlättas dessutom samkörning av olika register vilket i sin tur ökar risken för övervakning av individer. [Ström 03] Att ens handlande övervakas innebär att inte enbart en själv kontrollerar och bestämmer över sitt handlande, vilket är en kränkning av den personliga integriteten.

Fördelen med enhetliga IT-system är att det blir enklare och bekvämare för företag, organisationer och personer som driver dem. Om man däremot har teknisk splittring, dvs. en uppdelning på många olika delsystem, olika standarder och oli-

ka teknikplattformar, försvåras övervakningen och gynnar därigenom individens personliga integritet. Nackdelen med teknisk splittring är dock ökade kostnader för utveckling och drift av IT-system samt ökat krångel. [Ström 03]

I Sverige är samkörning av register kringgärdat av olika legala restriktioner. Efter attackerna mot USA den 11 september 2001 är det dock ingen självklarhet att det kommer att förbli så. Detta har visat sig genom att man prioriterar säkerheten på bekostnad av den personliga integriteten. Det man tidigare ansåg som otänkbart kan i dagsläget genomföras utan att mötas av något större motstånd. [Ström 03]

4.3 Lagstiftning som reglerar den personliga integriteten

I och med de tekniska möjligheterna att samla in uppgifter om individer, t.ex. genom att använda modern elektronik och datateknik, har det blivit nödvändigt för beslutsfattare och lagstiftare att beakta innebörden av begreppet personlig integritet och hur den personliga integriteten kan skyddas [Collste 97]. Nedan presenteras den lagstiftning som reglerar den personliga integriteten i EU och Sverige.

4.3.1 EG-direktivet, 95/46/EG, om personuppgifter

EG-direktivet, 95/46/EG, om personuppgifter, upprättades för att skydda enskilda personer med avseende på behandling av personuppgifter och för att skydda det fria flödet av dessa [EG-direktiv].

Personuppgifter inom EU används allt oftare inom ekonomiska och samhällliga områden, och framstegen inom informationsteknik har gjort det lättare att behandla och utbyta denna typ av uppgifter. Vidare kommer utbytet av personuppgifter mellan företag i olika medlemsländer att öka. När det gäller enskilda individers fri- och rättigheter, och då särskilt rätten till privatliv med avseende på behandling av personuppgifter, finns skillnader i skyddsnivån mellan de olika medlemsländerna. Denna skillnad kan bero på olikheter i nationella lagar och andra författningar och kan hindra översändande av denna typ av uppgifter mellan länderna. För att dessa hinder ska kunna avskaffas måste skyddsnivån i alla medlemsländer vara likvärdig. Då detta inte kan ske genom åtgärder endast av medlemsländerna har EU vidtagit åtgärder för att åstadkomma en tillnärmning av lagstiftningen. [EG-direktiv]

Medlemsländerna i EU ska i enlighet med 95/46/EG således skydda fysiska individers grundläggande fri- och rättigheter, särskilt rätten till privatliv, i samband med behandling av personuppgifter [EG-direktiv].

Medlemsländerna kan dock i sin nationella lagstiftning ange de allmänna villkor som skall gälla för behandlingen av personuppgifter. Varje medlemsland ska således tillämpa sina nationella bestämmelser som landet för genomförandet av 95/46/EG antar för behandlingen av personuppgifter. [EG-direktiv]

I Sverige är Personuppgiftslagen, PUL, genomförandet av 95/46/EG.

4.3.2 Personuppgiftslagen, PUL

Personuppgiftslagen, PUL 1998:204, trädde i kraft den 24 oktober 1998 och bygger på 95/46/EG [DI 2]. PUL ersatte den 1 oktober 2001 fullt ut den tidigare lagen inom detta område, datalagen [Ström 03]. Alla medlemsländer i EU måste anpassa sin lagstiftning till 95/46/EG så att den nationella lagstiftningen uppfyller kraven som ställs i 95/46/EG. Det är dock upp till varje nation att bestämma hur dessa krav ska uppnås. [SOU 97]

Syftet med PUL är att skydda individer mot att deras personliga integritet kränks när personuppgifter behandlas. Med behandling menas bl.a. insamling, registrering, lagring, bearbetning, spridning och utplåning. PUL gäller alla former av personuppgifter och behandlingen får endast ske för vissa ändamål och enligt huvudregeln krävs samtycke för behandling av uppgifterna. [PUL] Lagen gäller både i näringslivet och i den offentliga sektorn, men inte för privat bruk, som t.ex. register över vänner och bekanta [Ström 03].

Enligt PUL är personuppgifter all slags information som direkt eller indirekt kan knytas till en individ som är i livet [PUL]. Även digitala bilder, ljud och videoupptagningar räknas som personuppgifter i de fall då individer går att identifiera. Även sk. loggfiler, t.ex. in- och utpassering från byggnader och servrar som hanterar e-post och Internettrafik, från diverse tekniska system ingår i definitionen om informationen går att koppla till individen. [Ström 03]

Det är alltid tillåtet att enligt PUL lagra och behandla personuppgifter om de som informationen avser har lämnat sitt samtycke. Samtycket kan vara muntligt eller skriftligt och ska vara "frivilligt, särskilt och informerat". Med "frivilligt" menas att individen lämnar sitt samtycke utan tvång eller press. "Särskilt" innebär bl.a. att samtycket inte kan lämnas i grupp. "Informerat" innebär att individen måste förstå vad det handlar om. Vidare måste samtycke också vara "aktivt" vilket innebär att det t.ex. inte räknas som samtycke om individen har avstått från att kryssa i en ruta som anger att hon inte samtycker. Utan samtycke är behandling av personuppgifter endast tillåten i vissa fall, som t.ex. för att en arbetsuppgift av allmänt intresse ska kunna utföras samt att en arbetsuppgift i samband med myndighetsutövning ska kunna utföras. [Ström 03]

Några av de grundläggande kraven på behandling av personuppgifter är att personuppgifter endast får behandlas om det är lagligt, att de endast får samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Personuppgifterna får inte heller behandlas för något ändamål som är oförenligt med det ursprungliga. Dessutom får inte fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen, samt inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. [PUL]

För känsliga personuppgifter gäller särskilda regler. Känsliga uppgifter är t.ex. sådana som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening och sådant som rör hälsa, sjukdom och sexualliv. [PUL]

5 Biometrins risker för den personliga integriteten

I det här kapitlet redogörs för om, och i så fall hur, den personliga integriteten påverkas i samband med biometriska säkerhetsfunktioner. Kapitlet inleds med en kort diskussion kring biometriska uppgifter som personliga uppgifter. Därefter ges en presentation över risker för den personliga integriteten i samband med biometriska säkerhetsfunktioner. Efter varje risk förs ett resonemang kring hur risken i fråga kränker den personliga integriteten utifrån definitionen av personlig integritet som ges i avsnitt 4.1.2.

5.1 Biometrisk uppgift som personuppgift

Biometriska uppgifter är personuppgifter i och med att de biometriska uppgifterna härleds från en individ och används för att bestämma en individs identitet. Beroende på teknologin kan de biometriska uppgifterna dessutom vara en utmärkande representation av en fysiologisk eller beteendemässig egenskap. [BioPrivacy 1] Det finns således en direkt koppling mellan en biometrisk uppgift och en individs identitet [CC 1].

I 95/46/EG definieras ”personuppgifter” som ”varje upplysning som avser en identifierad eller identifierbar person [...]”. En identifierbar person är ”en person som kan identifieras, direkt eller indirekt, framför allt genom hänvisning till ett identifikationsnummer eller till en eller flera faktorer som är specifika för hans fysiska, fysiologiska, mentala [...] identitet”. Vidare kan man läsa: ”För att avgöra om en person är identifierbar skall härvid beaktas alla hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den **registeransvarige*** eller av någon annan person.” [ARBDOK 03]

Arbetsgruppen för dataskydd [03] anser att det utifrån definitionen i 95/46/EG verkar som att biometriska uppgifter alltid kan anses utgöra ”upplysning som avser en [...] fysisk person”, eftersom de till sin natur lämnar information om en person. Vid biometrisk identifiering är personen vanligtvis identifierbar i och med att de biometriska uppgifterna används för att särskilja den registrerade personen från övriga personer. [ARBDOK 03]

Enligt Arbetsgruppen för dataskydd [03] kan man utifrån definitionen om personuppgifter i 95/46/EG betrakta åtgärder för biometrisk identifiering eller deras digitala översättning som personuppgifter i de flesta fall. Om de biometriska uppgifterna lagras som en digital profil så att varken den registeransvarige eller någon annan person kan använda dem på något sätt för att identifiera den registrerade, bör uppgifterna inte klassificeras som personuppgifter, enligt Arbetsgruppen för dataskydd [03].

Vidare fastslog Datainspektionen i maj 2004 i samband med en utredning om den biometriska inloggning med fingeravtryck som sker vid Kvarnbyskolan i Stockholm, att ett fingeravtryck är en personuppgift [DI 3].

Med detta som bakgrund där biometriska uppgifter i flera fall definieras som uppgifter om en individ innebär det att definitionen av personlig integritet i avsnitt 4.1.2. även är relevant för biometriska uppgifter.

5.2 Kränkning av den personliga integriteten i samband med biometriska säkerhetsfunktioner

Nedan presenteras risker som kan kränka den personliga integriteten i samband med biometriska säkerhetsfunktioner. Flera av riskerna som tas upp här går in i varandra och den ena risken omfattar ofta den andra. Vi har ändå här gjort en uppdelning över olika risker som kan kränka den personliga integriteten i samband med biometriska säkerhetsfunktioner.

5.2.1 Hemlig igenkänning och brist på anonymitet

Vissa biometriska uppgifter kan samlas in utan att individen märker det [Crompton 02a]. Biometriska egenskaper är nämligen inga hemligheter utan vissa biometriska säkerhetsfunktioner bygger på egenskaper som kan samlas in utan att individen är medveten om detta i och med att han eller hon omedvetet lämnar spår efter sig. Detta gäller t.ex. fingeravtryck eller DNA-prov. [ARBDOK 03] Genom att t.ex. använda en biometrisk algoritm på ett fingeravtryck som hittats på ett dricksglas skulle det kunna gå att avgöra om en individ finns registrerad i en databas över biometriska uppgifter och avgöra vem individen är genom att jämföra de båda profilerna. För detta krävs dock förmåga att ta prov på fingeravtrycket från glaset utan att skada avtrycket. Vidare krävs teknisk utrustning för att behandla uppgifterna från fingeravtrycket samt tillgång till tillverkarens algoritm och/eller databasen över fingeravtrycken. [ARBDOK 03] Annars kan en bedräglig aktör också försöka att använda rester av ett fingeravtryck som lämnats kvar på den biometriska säkerhetsfunktionens sensor för att försöka framställa den senast behöriga individen [CC 1].

Risken att någon erhåller en biometrisk egenskap från en individ utan att vederbörande vet om det gäller även för andra biometriska säkerhetsfunktioner, som t.ex. de säkerhetsfunktioner som bygger på analys av tangentdynamik eller ansiktsigenkänning på håll. Dessa säkerhetsfunktioner erbjuder inte bara möjligheten att samla in de biometriska egenskaperna utan att den registrerade märker det, utan de inbjuder dessutom till en generell användning i och med att de utförs på ett mindre störande sätt. [ARBDOK 03]

I vissa fall kan också den biometriska teknologins natur begränsa individers möjlighet till anonymitet. Om ett telefonnätverk t.ex. använder sig av röstigenkänning, för att tillåta eller förneka folk åtkomst till ett telefonnätverk, kanske folk inte längre kommer att ha möjlighet att använda sig av betaltelefon och samtidigt vara anonyma. [Crompton 02a]

På en del ställen där man tidigare kunnat röra sig anonymt kan man inte det längre. Vid t.ex. nöjesparken Disney World i Florida identifieras innehavare av årskort genom att de sticker in två fingrar i en handgeometriavläsare. Det är således nödvändigheten att behöva identifiera sig i en sådan situation som bidrar till att det

byggs upp en infrastruktur som ökar mängden elektroniska spår, vilket gör att individer blir identifierade i situationer där de tidigare kunnat vara anonyma. [Ström 03]

Användning av biometri kan bygga upp en ”kritisk massa” av biometriska avläsningsstationer i alla möjliga sammanhang, vilket gör att individer och samhället vänjer sig vid biometri. På lång sikt kan detta driva fram användning av biometri där det egentligen inte behövs. Detta eftersom det är lätt att följa strömmen och utnyttja existerande infrastruktur. I och med detta kan användning av biometri bli allmänt accepterat och användas i alla möjliga sammanhang, till och med i sådana sammanhang där människor tidigare med självklarhet kunnat vara anonyma. [Ström 03]

Kränkning av den personliga integriteten

Personlig integritet innebär bl.a. att individer ska ha kontroll och få bestämma över sina egna personliga uppgifter. Individer har ingen kontroll om identifierbar information om dem samlas in utan deras vetskap och samtycke vilket är vad som sker vid hemlig igenkänning.

Hemlig igenkänning och obehörig insamling av de biometriska uppgifterna kan även leda till att de som vill vara anonyma i vissa situationer kan nekas detta och därmed få sin personliga integritet kränkt. Att en individs identitet inte ska göras tillgänglig och avslöjas för obehöriga är en del av vad personlig integritet innebär utifrån definitionen i avsnitt 4.1.2.

Då man måste identifiera sig på t.ex. ett nöjesfält kan detta också kränka den personliga integriteten i och med att man då inte får vara anonym, utan måste avslöja sin identitet.

5.2.2 Sekundär användning av biometriska uppgifter

Då de biometriska egenskaperna har samlats in uppkommer risker som rör reproduktion, återskapande och kopiering av de biometriska uppgifterna. De biometriska uppgifterna kan därigenom komma till andras, både publik och privat, kännedom. [CC 1] Detta kan ske både med och utan individens vetskap. I och med att en unik identifierare kan användas i flera sammanhang och användas för andra syften än vad som var tänkta från början, finns en risk för sekundär användning av de biometriska uppgifterna [Crompton 02a]. Om dessutom brottslighet, bedrägerier och terrorism ökar i vårt samhälle kan sekundär användning eller obehörig användning av biometriska uppgifter för syften utöver de ursprungliga öka [Tomko 98].

När identifierbara uppgifter, som t.ex. fingeravtryck, används som unika identifierare finns en risk att de kan föra samman olika delar av personlig information om en individ. Om fingeravtryck används som unik identifierare kan det möjliggöra spårning av individer och en noggrann fastställning av deras identiteter. [Cavoukian 99] En konsekvens av detta är att det möjliggör för en tredje part att få tillgång till kombinerad information och kompletta personliga profiler av människor [Tomko 98]. Denna möjlighet kan ses som en metod för organisationer, regeringar

och företag att bedriva kontroll över individer och deras anonymitet [Prabhakar et al 03].

Ström [03] presenterar några meningar från företrädare för människorättsorganisationer. Beth Givens på Privacy Rights Clearinghouse⁵ i San Diego säger att en förändring i det sociala klimatet i samhället kan göra biometrin till ett verktyg för förtryck och förvandlas till en teknik för att upptäcka oliktankande och för att utöva social kontroll. Vidare säger Stephen Keating på Privacy Foundation i Denver⁶, USA, enligt tidningen Fresno Bee att en databas med fingerkreditinformation är som vilken annan databas som helst, vilket innebär att fingerkreditinformationen kan hamna på platser där kunden inte förväntar sig det. Han säger även att matchning av våra fysiska egenskaper med kommersiella rörelser i samhället kan skapa oförutsedda användningsområden för biometriska uppgifter. Samtidigt ger han ett exempel på hur en individ handlar på en McDonaldsrestaurang som flera månader senare utsätts för ett väpnat rån, vilket gör att polisen kommer och tar fingeravtryck från platsen. En risk som då kan uppstå i denna situation är att individens beställning på McDonalds resulterar i att hans eller hennes fingeravtryck hamnar tillsammans med brottslingars fingeravtryck. Stephen Keating påpekar också att det finns gott om historik som visar hur annan teknologi använts för andra syften än det var tänkt från början och med tiden blivit en tvingande teknologi. [Ström 03]

Inom biometribranschen talar man om behovet av en gemensam infrastruktur för olika biometriska tillämpningar som är byggd på en gemensam standard, vilket kan riskera sekundär användning av de biometriska uppgifterna. Enhetliga system gör det lättare att skaffa sig en helhetsbild av en individ över flera olika system över tid. Om systemen däremot är mer utspridda och tekniskt olika krävs större insatser att skaffa samma helhetsbild av individen. Oliver Tattan, VD på biometri-företaget Daon⁷, har till nyhetstjänsten ZDNet sagt [Ström 03]:

”Teknologins verkliga potential ligger i att skapa en flexibel ’biometric trust infrastructure’ som låter företag och offentlig sektor hantera säkerhetskrav som ger identifiering bortom det första införandet. I slutändan skulle en sådan infrastruktur göra det möjligt för människor att röra sig från en plats till en annan runt hela jorden, med bibehållen ’säkerhetsclearance’.”

Även Arbetsgruppen för dataskydd [03] tar upp att den standardisering som krävs för att skapa driftskompatibilitet mellan olika system där biometri ingår, skulle kunna leda till en ökad sammankoppling av olika databaser.

Kränkning av den personliga integriteten

Sekundär användning av biometriska uppgifter är ett hot mot den personliga integriteten. Detta i och med att individen då inte längre har kontroll och kan bestämma över vad som händer med dennes personliga uppgifter.

⁵ <http://www.privacyrights.org>

⁶ <http://www.privacyfoundation.org>

⁷ <http://www.daon.com>

Om en tredje part får tillgång till kombinerad information av en individ genom sammankopplade databaser kan detta leda till att individers beteende övervakas och kontrolleras både med och utan deras vetskap. Detta kan kränka den personliga integriteten eftersom ingen har rätt att utan vetskap och samtycke övervaka en individs beteende. Vidare innebär övervakning att individen inte lämnas ifred vilket är en kränkning av den personliga integriteten.

Användning av biometriska uppgifter inom oförutsedda områden kan leda till att en individs fingeravtryck hamnar tillsammans med brottslingars fingeravtryck. Detta kan kränka den personliga integriteten på så sätt att individen mister sin värdighet och därmed sitt sociala anseende.

5.2.3 Exponering av biometriska uppgifter genom systemattacker

Biometriska säkerhetsfunktioners effektivitet är beroende av datorteknologi och elektroniska anordningar. Det innebär att de flesta risker som är associerade med datorteknologi också är relevanta för biometriska säkerhetsfunktioner. Funktioner som innefattar behandling, överföring och lagring av data med hjälp av datorteknologi är måltavlor för hackning och obehörig åtkomst, obehörig användning och obehörig upptäckt. Även om det är svårt för en individ att förfalska t.ex. ett fingeravtryck så finns det de som anser att en individ kan hacka sig in i ett system, kopiera en lagrad biometrisk uppgift och återanvända den för att passera som individen som äger den biometriska uppgiften. [Crompton 02a]

En bedräglig aktör kan t.ex. modifiera sitt eget fingeravtryck eller presentera ett konstgjort falskt fingeravtryck för att försöka utgöra en utvald behörig individ eller ett utvalt fingeravtryck som är av låg kvalitet. Om den bedrägliga aktören för säkerhetsfunktionen visar upp ett fingeravtryck av dålig kvalitet kan den bedrägliga aktören eventuellt få säkerhetsfunktionen att matcha det mot en behörig individs lagrade fingeravtryck som är av låg kvalitet. [CC 1]

Dessutom kan en bedräglig aktör också använda rester av ett fingeravtryck som lämnats kvar på den biometriska säkerhetsfunktionens sensor för att försöka framställa den senaste behöriga individen som interagerade med säkerhetsfunktionen. Den bedrägliga aktören skulle också kunna utföra sk. återuppspelningsattacker. Den bedrägliga aktören fångar då upp ett fingeravtryck från en behörig individ under överföringen mellan subfunktionen för insamling och extrahering. Detta för att sedan kunna infoga en behörig individs fingeravtryck direkt till subfunktionen som utför extraheringen och därigenom gå förbi subfunktionen för insamling. Den bedrägliga aktören kan också fånga upp en behörig individs extraherade fingeravtrycksuppgifter under överföringen mellan subfunktionerna för extrahering och matchning och sedan föra in de extraherade fingeravtrycksuppgifterna direkt till subfunktionen för matchning. [CC 1]

Genom sk. **bakdörrar*** kan den bedrägliga aktören gå förbi hela den biometriska säkerhetsfunktionen utan att behöva lämna en biometrisk egenskap till säkerhetsfunktionen. Ett sätt att gå förbi säkerhetsfunktionen och undvika matchningsprocessen är att gå in och ändra på funktionens inställningar. T.ex. skulle gränsvärdet,

som avgör funktionens toleransnivå och noggrannhet vid matchning, kunna sättas till noll, vilket skulle innebära att funktionen tolererar alla matchningar oavsett om två fingeravtryck kommer från samma finger eller inte. [BioPrivacy 1] Då skulle den bedrägliga aktörens fingeravtryck kunna matchas mot en behörig individs fingeravtryck, vilket skulle innebära att den bedrägliga aktören använder den behöriga individens identitet.

Allt detta riskerar att en obehörig individ kan använda en behörig individs biometriska uppgifter för att få behörighet till t.ex. pengar eller byggnader. Då skulle en individ oärligt kunna påstå att någon utfört en transaktion eller varit på ett visst ställe trots att den egentligen inte gjort det eller varit där. Det blir dessutom svårt för den faktiska ägaren till de biometriska uppgifterna att förneka att han eller hon utfört handlingen eller varit på en viss plats vid ett visst tillfälle. Detta pga. att biometriska säkerhetsfunktioner kan ge upphov till den felaktiga föreställningen att autenticeringen av en individ alltid är riktig, vilket kan göra det mycket svårt för individen att bevisa motsatsen. Identitetsstöld av sådana slag kan också medföra att den behöriga individens fingeravtryck blir otillförlitliga för framtida applikationer. [ARBDOK 03]

Kränkning av den personliga integriteten

Att en bedräglig aktör kommer åt en individs biometriska uppgifter ger upphov till obehörig åtkomst, användning och upptäckt som kan kränka den personliga integriteten. Identitetsstöld innebär att någon annan har kontroll över en individs personliga uppgifter och kan fatta beslut i individens namn. Individen kan inte heller i en sådan situation själv välja när han eller hon vill vara anonym i och med att någon annan har kontroll över individens biometriska uppgifter. Allt detta uppfyller kriteriet för kränkning av den personliga integriteten utifrån definitionen i avsnitt 4.1.2.

Att en bedräglig aktör kommer åt och utnyttjar en individs biometriska uppgifter kan också kränka den personliga integriteten i och med att informationssäkerheten hotas. Detta i och med att den bedrägliga aktören kan påverka tillgänglighet, kvalitet och sekretess hos uppgifterna.

5.2.4 Avslöjande av känslig information

Biometriska egenskaper kan avslöja mer information om en individ än just bara individens identitet. Vissa biometriska egenskaper är känsliga. Röst kan t.ex. avslöja känslor och ansiktet kan avslöja information om en individs känslor och hälsa. Även en individs iris och retina kan avslöja information om en individs hälsotillstånd. [Crompton 02a]

Vidare kan en individs biometriska egenskaper, under vissa omständigheter, också avslöja medicinsk information som rör individens hälsotillstånd. Eftersom biometriska egenskaper är biologiska till sin natur kan de som samlar in och får tillgång till denna information därmed eventuellt få ytterligare personlig information från de biometriska egenskaperna. Även om det ännu inte är bevisat har det rapporterats att man faktiskt kan samla in hälsotillståndsuppgifter från en individs iris och fingeravtryck. En utvecklingsstörning som Downs syndrom kan t.ex. avslöjas via

uppgifter från iris och fingeravtryck. Medicinska experter har gett denna angelägenhet extra uppmärksamhet och dokumenterar möjligheterna om biometriska egenskaper skulle kunna avslöja sådan information. [CC 1] Exempelvis har Dr. Howard Chen i sitt arbete om **dermatologi*** noterat att just Downs Syndrom kan orsaka ovanliga mönster på en individs fingeravtryck. Även andra typer av sjukdomar som t.ex. leukemi och bröstcancer kan förknippas med särskilt ovanliga mönster i fingeravtrycket. [Woodward et al 03] En rädsla finns således för att det från dessa biometriska egenskaper ska gå att få ut mer information än vad som var avsikten från början. Om medicinsk information erhålles från de biometriska egenskaperna kan detta bli en grund för systematisk diskriminering av vissa särskilda segment av populationen som upplevs som riskabla och problematiska. [Prabhakar et al 03]

Ur ett mer långsiktigt perspektiv skulle en fokusering på mänskliga kännetecken kunna leda till en ökad kunskap om förhållandet mellan mänskliga kännetecken och andra vanor, beteenden eller känslor. Man skulle t.ex. kunna upptäcka att rödhåriga människor är mer troliga att köpa finansiella produkter, eller att människor med lågt röstläge är mer troliga att gå med i ett speciellt politiskt parti. Sådan information skulle säkert kunna missbrukas och användas i sammanhang som elektronisk handel och telefonförsäljning för att kartlägga och påverka kunders köpvänor. [Crompton 02a]

Kränkning av den personliga integriteten

Då känsliga uppgifter, som t.ex. medicinsk information, kan fås från de biometriska egenskaperna kan detta kränka den personliga integriteten i och med att individen inte längre har kontroll över vilken information som avslöjas till andra. Om medicinsk information avslöjas till obehöriga kan den personliga integriteten även kränkas på så sätt att individen mister sin värdighet och därigenom känner att man inte har något värde och socialt anseende.

Då en fokusering på mänskliga kännetecken kan leda till ökade kunskaper om förhållandet mellan dessa och vanor, beteenden och känslor kan den personliga integriteten kränkas i och med att individens beteende övervakas utan dennes vetskap och samtycke. Om de ökade kunskaperna används i sammanhang som t.ex. elektronisk handel och telefonförsäljning kan den personliga integriteten även kränkas i och med att individen inte blir lämnad ifred.

5.2.5 Systemfel

På grund av att den teknologi som hanterar de biometriska uppgifterna har en bristande noggrannhet och på grund av den varierande kvaliteten på de biometriska uppgifterna har teknologin en inbyggd tolerans. Detta gör att det alltid finns en risk för systemfel vid hantering av biometriska uppgifter som kan resultera i FRR eller FAR. Detta kan leda till att individer som har kännetecken och egenskaper som är annorlunda eller mindre utmärkande än genomsnittet kan löpa en större risk för att utsättas för FRR. Detta kan leda till diskriminering om individen t.ex. nekas behörighet till tjänster som han eller hon egentligen har behörighet till. Som exempel kan nämnas att hantverksarbetare ofta har fingeravtryck som är slitna eller mindre utmärkande. [Crompton 02a] Vidare skulle FRR kunna ge upphov till

att en behörig individ identifieras som en individ som inte bör tillåtas att resa med ett visst flygplan eller som en individ som inte bör tillåtas resa till ett visst land. En sådan situation behöver inte bara bli pinsam utan det skulle även kunna bli väldigt svårt för individen att bevisa att säkerhetsfunktionen har fel i och med föreställningen om att biometriska säkerhetsfunktioner alltid utför korrekta autentiseringar. [ARBDOK 03]

En annan risk är förknippad med FAR. FAR kan påverka kvaliteten på de insamlade uppgifterna i och med att obehöriga individer kan ”komma igenom” säkerhetsfunktionen. Om säkerhetsfunktionen ger åtkomst till obehöriga individer kan det leda till att insamlade uppgifter från obehöriga individer matchas mot behöriga individers lagrade uppgifter med lyckat resultat. Då kommer de insamlade obehöriga uppgifterna att tilldelas behöriga individer trots att uppgifterna inte tillhör dem. Detta kan t.ex. leda till att en individ registreras som att ha besökt en specifik plats när individen egentligen inte alls har gjort det. [Crompton 02a]

Kränkning av den personliga integriteten

Diskrimineringen som kan uppstå om en individ nekas åtkomst till tjänster på grund av t.ex. ovanliga fingeravtryck, kränker den personliga integriteten i och med att individens värdighet går förlorad. Likaså kan en individ mista sin värdighet om denne inte tillåts resa med ett visst flyg för att han eller hon identifieras som en individ som inte bör tillåtas resa med detta flyg.

Då obehöriga individer får åtkomst till den biometriska säkerhetsfunktionen och kan påverka kvaliteten på de insamlade biometriska uppgifterna hotar det den personliga integriteten i och med att kvalitetsaspekten på uppgifterna hotas. Detta hotar i sin tur informationssäkerheten vilket enligt definitionen i avsnitt 4.1.2. kränker den personliga integriteten.

Att obehöriga individer får tillgång till behöriga individers biometriska uppgifter kränker också den personliga integriteten i och med att de behöriga individerna mister kontroll över och inte kan bestämma över sina egna personliga uppgifter.

5.2.6 Lagring

Centraliserade applikationer som lagrar alla biometriska uppgifter i en central fil innebär att uppgifterna lagras på ett och samma ställe och kan komma åt direkt. Den centrala filen gör det då möjligt att utföra ytterligare kontroller som inte skulle vara möjliga om uppgifterna lagrades decentraliserat på t.ex. separata smarta kort som ägarna till de biometriska uppgifterna själva har kontroll över. [Grijpink 01] Central lagring av biometriska uppgifter kan ge upphov till användning av uppgifterna som nyckel för sammankoppling av olika databaser. Som nämndes tidigare skulle detta kunna ge upphov till detaljerad kartläggning av individens vanor i både offentlig och privat sektor. Central lagring innebär också en ökad risk för utnyttjandet av biometriska uppgifter från fysiska spår som omedvetet efterlämnas av individer, t.ex. fingeravtryck. [ARBDOK 03]

En annan aspekt i samband med lagring av biometriska uppgifter är huruvida de lagras i logiskt samband med annan personlig information som t.ex. namn och

adress så att ytterligare information utöver de biometriska uppgifterna kan erhållas. [BioPrivacy 2]

Vid lagring av de biometriska uppgifterna kan en bedräglig aktör ge upphov till flera hot. Den bedrägliga aktören kan förse sin egen biometriska uppgift på ett falskt smart kort, eller placera det i säkerhetsfunktionens databas genom att ett nytt användarkonto för en behörig individ skapas för den bedrägliga aktören eller genom att en biometrisk uppgift av en behörig individ ersätts med den bedrägliga aktörens biometriska uppgift. När det gäller lagring kan en bedräglig aktör också stjäla eller modifiera en behörig individs biometriska uppgift från lagringen. När en behörig individs biometriska uppgift överförs mellan subfunktionerna för extraheringen och lagring av de biometriska uppgifterna skulle den bedrägliga aktören kunna fånga upp denna. Den bedrägliga aktören kan också fånga upp en behörig individs biometriska uppgift under överföringen mellan subfunktionerna för lagringen av de biometriska uppgifterna och matchningen. [CC 1]

Kränkning av den personliga integriteten

Biometri i samband med identifiering innebär en risk för kränkning av den personliga integriteten då säkerhetsfunktionen måste lagra de biometriska uppgifterna centralt. Skillnaden mellan centraliserad och decentraliserad lagring är viktig ur ett perspektiv som rör den personliga integriteten eftersom central lagring innebär ökade risker för exponering till obehöriga, som t.ex. en bedräglig aktör. Exponering till obehöriga kan kränka den personliga integriteten i avseenden som rör brist på anonymitet, att inte själv få kontrollera och bestämma över sitt handlande och sina personliga uppgifter, samt att informationssäkerheten hotas.

6 Skyddsåtgärder för att beakta den personliga integriteten i samband med biometri

I det här kapitlet kommer vi att presentera krav som bör beaktas vid utveckling och användning av biometriska säkerhetsfunktioner för att skydda den personliga integriteten. De krav som presenteras i detta kapitel är krav som utarbetats av representanter för biometribranschen samt av myndighet.

Vissa av riskerna i samband med biometriska säkerhetsfunktioner är förknippade med utvecklingen av dessa medan andra risker i sin tur är förknippade med användningen av biometriska säkerhetsfunktioner. Detta innebär att vissa beaktanden bör tas av utvecklaren, medan andra beaktanden bör tas av den som ansvarar för användningen av de biometriska säkerhetsfunktionerna i en verksamhet, dvs. en registeransvarig. De flesta beaktanden gäller dock både vid utveckling och vid användning. Vi kommer till en början inte att skilja på de krav som bör ställas vid utveckling respektive användning av biometriska säkerhetsfunktioner. Istället kommer vi att dela upp kraven på olika områden där risker för den personliga integriteten kan uppkomma. Precis som med riskerna i kapitel fem går även de olika kraven in i varandra och ofta innefattar ett krav automatiskt flera andra. Efter varje krav förs ett resonemang kring hur den personliga integriteten kan skyddas utifrån definitionen av begreppet i avsnitt 4.1.2 och kravet i fråga. I slutet av kapitlet ges en sammanfattning på vad som bör beaktas vid utveckling respektive användning.

6.1 Definiera syfte och varaktighet

När personuppgifter samlas in ska de samlas in för särskilda, uttryckligt angivna och berättigade syften [ARBDOK 03]. Syftena måste vara tydliga och igenkännliga för alla inblandade [Grijpink 01]. Behandlingen av uppgifterna får inte vid senare tillfällen ske på ett sätt som är oförenligt med dessa syften. Vidare ska personuppgifterna vara adekvata och relevanta och får inte omfatta mer än vad som är nödvändigt för syftena de samlats in för. [ARBDOK 03] Undantag är om individen gett sitt samtycke eller om lagen säger annat. Den utsträckning som är nödvändig för att uppnå syftena ska vara exakt, fullständig, och hela tiden uppdaterad. [Cavoukian 99] Biometriska uppgifter som samlas in för behörighetskontroll får således inte användas i syfte att t.ex. bedöma den registrerades hälsotillstånd eller för övervakning på arbetsplatsen [ARBDOK 03].

Syftet med insamlingen och behandlingen av de biometriska uppgifterna ska klart definieras [ARBDOK 03]. Vidare bör syftet inte definieras senare än vid insamlingen av de biometriska uppgifterna eller senare än när uppgifterna börjar användas för att uppfylla syftet [Cavoukian 99]. Därefter måste det avgöras om hänsyn tas till proportionalitet och legitimitet [ARBDOK 03]. Proportionalitet innebär att det måste finnas ett rimligt förhållande till de syften för vilka de biometriska uppgifterna samlas in. Man bör inte välja att använda biometriska säkerhetsfunktioner om syftet kan uppnås på andra, mindre kränkande sätt. Med legitimitet menas att syftet ska kunna rättfärdiga biometrins karaktär. [Grijpink 01]

Skydd av den personliga integriteten

Risken för kränkning av den personliga integriteten är mindre om varaktigheten och syftet för en biometrisk säkerhetsfunktion är definierad på förhand. Då är risken mindre att användningsområdet för de insamlade uppgifterna utvidgas och därigenom blir föremål för sekundär användning av tredje part. Detta innebär att individen själv har kontroll över sina personliga uppgifter och sitt handlande vilket är en förutsättning för att uppnå personlig integritet enligt definitionen i avsnitt 4.1.2.

6.2 Begränsad behandling

Biometriska uppgifter ska endast lagras för sitt specifika användningssyfte och ska inte lagras längre än nödvändigt. De ska förstöras, tas bort eller på annat sätt göras oanvändbara när den biometriska säkerhetsfunktionen inte längre används. Specifika användaruppgifter ska förstöras, tas bort eller på annat sätt göras oanvändbar när individen inte längre förväntas interagera med säkerhetsfunktionen. [BioPrivacy 2]

Åtkomst till biometriska säkerhetsfunktioner och uppgifter bör begränsas till specifika individer under specifika förhållanden [BioPrivacy 2]. Endast de som verkligen behöver tillgång till uppgifterna ska ha det [Cavoukian 99].

Insamling och lagring av uppgifter utöver de biometriska, dvs. icke-biometriska uppgifter, bör också begränsas så mycket som möjligt. Endast de uppgifter som är nödvändiga för autentisering bör samlas in och lagras. [BioPrivacy 2]

Användningen av biometriska uppgifter ska inte automatiskt tillåtas att överskrida de fysiska områdesgränserna och de gränser som fastställts i lag. Olika områden kan t.ex. vara banker, hälsovård, utbildning, skattemyndigheter och handel. En biometrisk säkerhetsfunktion måste därför ha tydliga gränser. [Grijpink 01]

Skydd av den personliga integriteten

Genom att uppgifter från ett visst område inte automatiskt får användas inom ett annat område och att insamling, användning och lagring begränsas, minskar risken för sekundär användning. Detta innebär att den personliga integriteten skyddas på så sätt att individen själv behåller kontroll över sina personliga uppgifter och sitt eget handlande.

6.3 Öppenhet

Biometriska uppgifter ska hanteras på ett öppet sätt. Det innebär att biometriska uppgifter som samlas in från individen ska samlas in öppet och direkt. [Cavoukian 99] Säkerhetsfunktioner där individen är medveten om att biometriska uppgifter samlas in och används, och där insamlingsutrustningen tydligt syns, bör användas framför osynliga säkerhetsfunktioner. Individen bör ge sitt samtycke innan dennes biometriska uppgifter används, och det är svårare att få samtycke när slutna säkerhetsfunktioner används. Slutna biometriska säkerhetsfunktioner ska därför endast användas när det är absolut nödvändigt. [BioPrivacy 2]

Biometriska säkerhetsfunktioner där biometriska uppgifter kan samlas in utan att individen vet om det ska undvikas. Riskfyllda biometriska säkerhetsfunktioner i detta avseende är t.ex. sådana som baseras på insamling av fingeravtryck. [ARB-DOK 03]

Öppenhet har även att göra med samtycke från individen samt att synliggöra och informera syftet med den biometriska säkerhetsfunktionen till individen [BioPrivacy 2].

6.3.1 Information till individen och samtycke från densamma

Individen bör informeras om syftet med insamlingen, och den registeransvarige ska tydligt ange sin identitet [ARBDOK 03].

Vidare ska individen ha insyn i alla processer som utförs i samband med en biometrisk säkerhetsfunktion. Det innebär att individen ska ha insyn i enrolleringen, matchningen, användningen, verifieringen, identifieringen, de skydd som används för de biometriska uppgifterna och säkerhetsfunktionen, samt i de individer och entiteter som är ansvariga för säkerhetsfunktionen. Det ska t.ex. synliggöras hur biometriska uppgifter ska användas, både i och utanför den biometriska säkerhetsfunktionen. Individen bör få utförlig information om vilken typ av biometriska och icke-biometriska uppgifter som ska ges till den biometriska säkerhetsfunktionen. Vidare ska individen få information om vad en lyckad och misslyckad autentisering får för konsekvenser. Insyn bör också ges för att indikera om enrolleringen i en biometrisk säkerhetsfunktion är frivillig eller inte. Om den är frivillig bör alternativ finnas tillgängliga och individen ska göras medveten om vilka val som finns. Det bör inte ges några antydningar om att enrolleringen i en biometrisk säkerhetsfunktion är obligatorisk om den är frivillig. Innan säkerhetsfunktionen börjar användas ska det dessutom tydligt framläggas vem som är ansvarig för användningen, till vem individen ska vända sig med frågor och eventuella klagomål. De skydd som används för att säkra biometriska uppgifter bör också informeras till individen. Detta inkluderar t.ex. information om kryptering, säkra tekniska anordningar, administrativa kontroller och datasegregering. [BioPrivacy 2]

Individen måste förstå varför och hur säkerhetsfunktionen används, vilka valmöjligheter som finns, och vilka fördelar som följer av den biometriska säkerhetsfunktionen, för att kunna fatta informerade beslut kring den biometriska säkerhetsfunktionen [Cavoukian 99].

Ett sätt att informera individen är genom utbildning. Vid introduktion till en ny teknologi bör utbildning vara en förutsättning för att möjliggöra för individen att fatta egna informerade beslut angående den biometriska säkerhetsfunktionen. Dessutom kan utbildning bidra till att individen känner sig mer bekväm med den biometriska teknologin. [Cavoukian 99]

För att behandla biometriska uppgifter måste principer om tillåtelse följas. Det innebär bl.a. att individen måste ha lämnat sitt samtycke. [ARBDOK 03] Om individen känner till och samtycker till insamlingen av dennes biometriska uppgif-

ter, blir det lättare för individen att förhandla om uppgifternas användning och exponering [Cavoukian 99].

Skydd av den personliga integriteten

Genom att ha öppna biometriska säkerhetsfunktioner skyddas den personliga integriteten i och med att individen är medveten om, och därmed kan få kontroll över, insamlingen och användningen av sina biometriska uppgifter. Öppna säkerhetsfunktioner gör det också lättare att få samtycke från individen. Personlig integritet innebär att samtycke ska fås från individen innan någon annan än individen själv ska få tillgång till och kunna använda individens personliga uppgifter.

Genom att informera individen och ge denne insyn i alla processer som utförs i samband med en biometrisk säkerhetsfunktion kan detta bidra till att skydda den personliga integriteten. Detta i och med att en informerad individ som har insyn även har kontroll över och lättare kan bestämma över sina personliga uppgifter och sitt handlande. Detta uppnås även om individen förstår varför och hur säkerhetsfunktionen används, vilka valmöjligheter som finns, och vilka fördelar som följer av den biometriska säkerhetsfunktionen. Vidare kan information till individen och samtycke från individen minska riskerna för att dennes värdighet kränks. Om användningen av biometriska säkerhetsfunktioner hanteras på ett öppet sätt kan det få individen att känna att den behandlas med respekt. Om individens värdighet kränks, kränks också den personliga integriteten enligt definitionen i avsnitt 4.1.2.

6.4 Vidta tekniska säkerhetsåtgärder

Personuppgifter bör genom säkerhetsskydd skyddas mot risker som förlust, obehörig åtkomst, förstörelse, användning, modifiering eller exponering [Cavoukian 99]. Några viktiga tekniska säkerhetsåtgärder som bör vidtas för att skydda den personliga integriteten är att använda digitala profiler av biometriska uppgifter istället för rådatabilder, att lagra de biometriska uppgifterna decentraliserat och att använda sig av kryptering.

6.4.1 Digital profil

I och med att biometriska uppgifter, särskilt när det gäller originalbilder i form av rådata, ofta innehåller och kan avslöja mer information än vad som är nödvändigt för autentisering, bör den biometriska uppgiften omvandlas till en digital profil. Detta i och med att en sådan tekniskt konstrueras så att icke nödvändiga uppgifter utesluts. Då behandling av biometriska uppgifter i form av bilder dessutom ökar risken för att känslig information avslöjas är detta ännu en anledning till att digitala profiler bör användas istället. [ARBDOK 03]

Ett alternativ till rådatabilder av ett fingeravtryck är således att extrahera karakteristiska kännetecken från ett fingeravtryck, sk. minutiösa detaljer för att skapa ett minutiösbaserat exemplar av fingeravtryck, dvs. en digital profil. Från den digitala profilen kan man inte återskapa hela fingeravtrycksbilden. [Jain et al 97a]

Digitala profiler är endast värdefulla när de bearbetas genom en specifik algoritm. De kan därför inte länkas samman med en specifik biometrisk uppgift i rådata utan att behandlas genom denna algoritm. Biometriska bilder i form av rådata är generellt sätt identifierbara och kan därmed förknippas med en specifik individ. [BioPrivacy 2] Då all information i ett fingeravtryck inte är med i beräkningen för att få fram den digitala profilen, är det inte möjligt att återberäkna originalbilden av fingeravtrycket utifrån den digitala profilen. Detta eftersom man måste ta reda på vem det uträknade värdet kommer ifrån och vilken formel som användes för att beräkna värdet. [Grijpink 01]

6.4.2 Decentraliserad lagring

I och med de risker som är knutna till centraliserad lagring av biometriska uppgifter bör uppgifterna lagras decentraliserat [ARBDOK 03]. En biometrisk säkerhetsfunktion som lagrar de biometriska uppgifterna centralt är mer kapabel att missbrukas än en biometrisk säkerhetsfunktion där uppgifterna lagras hos individen [BioPrivacy 2]. Exempel på decentraliserad lagring där endast individen har tillgång till, och kontroll över sina biometriska uppgifter är lagring på ett smart kort. Det bör nog övervägas om användning av säkerhetsfunktioner som kräver central lagring verkligen är nödvändig. Om biometriska säkerhetsfunktioner som lagrar biometriska uppgifter i en central databas måste användas, som är fallet vid identifiering, bör de innan användning förhandskontrolleras. Detta i och med att de antagligen kommer att innebära särskilda risker för individens fri- och rättigheter. [ARBDOK 03]

Genom att lagra de biometriska uppgifterna utanför säkerhetsfunktionen, som t.ex. på ett smart kort, ökar således möjligheterna till att skydda den personliga integriteten. Till skillnad från lagring i en central databas bidrar inte lagring på smart kort att de biometriska uppgifterna kan länkas samman med andra personliga uppgifter som t.ex. namn och adress. Detta då det smarta kortet endast innehåller och kontrolleras av individen och enbart behöver innehålla de biometriska uppgifterna. [Cavoukian 99]

6.4.3 Kryptering

För att skydda de biometriska uppgifterna ytterligare bör de digitala profilerna behandlas matematiskt med hjälp av t.ex. kryptering eller en **hashfunktion***. Genom att skydda **krypteringsnycklarna*** och använda olika parametrar för varje biometrisk digital profil som skapas kan man undvika att en ursprunglig biometrisk uppgift rekonstrueras från en digital profil, samt att personuppgifter från olika databaser sammanställs genom att de lagrade biometriska uppgifterna jämförs. [ARBDOK 03]

Kryptering kan också lösa problemet med borttappade och stulna smarta kort som skulle kunna leda till att någon obehörig kommer åt informationen på kortet. Genom att använda biometrisk kryptering skulle t.ex. ett fingeravtryck kunna användas för att koda en nyckel som krypterar uppgifterna på kortet. Nyckeln skulle då inte behöva skyddas. Dessutom skulle enbart individen med just det fingeravtrycket som kodade nyckeln kunna komma åt uppgifterna på kortet. [Cavoukian 99] I och med detta skulle det också vara möjligt att undvika att det skapas data-

baser över biometriska digitala profiler som kan användas för andra syften än de ämnade [ARBDOK 03].

Skydd av den personliga integriteten

De tekniska säkerhetsåtgärderna kan bidra till att användarna känner att de behandlas med värdighet. De visar även på att användarnas intressen är viktiga och att de behandlas med respekt.

Utifrån den digitala profilen kan man inte återskapa hela fingeravtrycket vilket förhindrar att obehöriga får tillgång till de personliga uppgifterna. Således kommer endast individen själv att ha kontroll över och få bestämma över sina personliga uppgifter i och med att ingen annan kan komma åt dem. På så sätt skyddas även informationssäkerheten. Detta är en förutsättning för att den personliga integriteten inte ska kränkas utifrån definitionen i avsnitt 4.1.2. I och med att digitala profiler inte kan förknippas med en specifik individ kommer individen och den digitala profilen att verka orelaterade till varandra, vilket skyddar den personliga integriteten. Detta då individen ges möjlighet till anonymitet då individens identitet inte kan göras tillgänglig och avslöjas till obehöriga.

Genom att lagra de biometriska uppgifterna utanför säkerhetsfunktionen, som t.ex. på ett smart kort, kan man hindra att den personliga integriteten kränks. Detta då individen själv har kontroll över och därmed kan bestämma över sina personliga uppgifter. Vidare skyddas den personliga integriteten i och med att informations-säkerhet uppnås. Detta i och med att de personliga uppgifterna endast är tillgängliga för individen själv som därmed kan se till att ingen annan t.ex. får insyn i och ändrar i uppgifterna. Dessutom möjliggör decentraliserad lagring anonymitet då de personliga uppgifterna och identiteten inte görs tillgängliga för obehöriga.

Om man dessutom krypterar den digitala profilen skyddas ovanstående aspekter av den personliga integriteten ytterligare i och med att det blir ännu svårare för obehöriga att komma åt de personliga uppgifterna och övervaka individen.

6.5 Användarkontroll

Individer bör ha rätt att kontrollera användningen av sina biometriska uppgifter. De bör även ha en möjlighet att få information förstörd, borttagen eller på annat sätt undanröjd. Om icke-biometriska uppgifter lagras i anslutning till de biometriska uppgifterna bör användarna förses med en metod så att de kan korrigera, uppdatera och se information som lagras i anslutning till biometriska uppgifter. [BioPrivacy 2]

Biometriska säkerhetsfunktioner bör konstrueras så att individen själv äger och har kontroll över sina biometriska uppgifter [BioPrivacy 2]. Som nämndes tidigare är decentraliserad behandling i form av t.ex. smarta kort ett sätt att uppnå detta på i biometriska säkerhetsfunktioner för verifiering.

Skydd av den personliga integriteten

Genom användarkontroll skyddas den personliga integriteten på så sätt att individen själv har kontroll över och bestämmer över sina personliga uppgifter. Om t.ex. insyn i individens personliga uppgifter skyddas, skyddas även informations-säkerheten, och därmed den personliga integriteten. Användarkontroll genom att individen t.ex. kan uppdatera och korrigera sina personliga uppgifter skyddar kvaliteten av dessa, vilket även skyddar den personliga integriteten enligt definitionen i avsnitt 4.1.2.

Användarkontroll i form av t.ex. decentraliserad lagring möjliggör också för individen att bli lämnad ifred i och med att andra inte kommer åt de personliga uppgifterna och därmed kan lägga sig i individens angelägenheter och övervaka individen. Genom att själv få kontrollera över sina personliga uppgifter och över användningen av dem kan individen även känna värdighet och att denne behandlas med respekt.

6.6 Beakta lagstiftning och riktlinjer

I och med att biometriska uppgifter i flera fall kan klassas som personuppgifter bör lagstiftning som reglerar skydd på behandling av personuppgifter även beaktas vid behandling av biometriska uppgifter.

Flera av de krav som tas upp i det här kapitlet är reglerade i lagstiftning, dvs. i 95/46/EG och PUL. Det gäller t.ex. de krav som innefattar hur insamling och behandling av personuppgifter ska ske, att syftet måste definieras och att samtycke måste inhämtas innan insamling.

Genom att tillämpa skyddsbestämmelserna i t.ex. 95/46/EG på biometriska säkerhetsfunktioner kan medvetenheten hos de som utvecklar och använder biometriska säkerhetsfunktioner bli högre angående de risker som skulle kunna påverka den personliga integriteten [ARBDOK 03]. Arbetsgruppen för dataskydd [03] har tagit fram ett dokument där man tillämpar skyddsbestämmelserna i 95/46/EG på biometriska säkerhetsfunktioner för att ge enhetliga riktlinjer för företag som utvecklar och använder biometriska säkerhetsfunktioner. Dokumentet har därför fungerat som källa för denna studie. Ett krav som man vid utveckling och användning borde beakta är just att tillämpa sådana typer av dokument, men även att direkt tillämpa och följa lagstiftningen. Vidare bör biometriska säkerhetsfunktioner utvecklas så att de underlättar genomförande av tillämpningar i lagstiftning [ARBDOK 03].

Flera av de krav som tagits upp i uppsatsen är hämtade från riktlinjer och metoder som t.ex. International Biometric Group's BioPrivacy Initiative [BioPrivacy 2] tagit fram. Sådana typer av direktiv bör också beaktas vid utveckling och användning för att skapa medvetenhet och på så sätt skydda den personliga integriteten. International Biometric Group's BioPrivacy Initiative [BioPrivacy 2] använder tre utvärderingsverktyg som kan användas för detta ändamål. Det första utvärderingsverktyget, BioPrivacy Application Impact Framework, används för att utvärdera de möjliga risker som en specifik biometrisk säkerhetsfunktion för med

sig. Det andra verktyget, BioPrivacy Technology Risk Ratings, används för att bedöma och gradera en biometrisk säkerhetsfunktion inom olika områden på en skala från låg till hög risk för den personliga integriteten. BioPrivacy Best Practices är det tredje verktyget och är riktlinjer för olika försiktighetsåtgärder företag kan ta för att försäkra att de utvecklar eller använder biometriska säkerhetsfunktioner som värnar om den personliga integriteten. [BioPrivacy 2]

Skydd av den personliga integriteten

Kravet på att beakta lagstiftning och riktlinjer kan, som redan nämnts, skapa medvetenhet kring hur biometri kan påverka den personliga integriteten. Genom detta kan man se till att det utvecklas och används sådana biometriska säkerhetsfunktioner som värnar om de olika aspekterna av personlig integritet. Det innebär att man utvecklar och använder biometriska säkerhetsfunktioner som möjliggör för individen att vara anonym, att bli lämnad ifred och att få behålla sin värdighet. Vidare innebär det även att de biometriska säkerhetsfunktionerna utvecklas och användas så att individen kan kontrollera och bestämma över sina personliga uppgifter och sitt handlande, samt att insyn, användning och kvalitet hos dem skyddas.

6.7 Uppdelning av kraven för utveckling respektive användning

På grund av de risker som kan uppkomma i samband med biometriska säkerhetsfunktioner bör man iaktta åtgärder för att skydda den personliga integriteten. Det handlar om allt från tekniska skydd som byggs in i systemet, till generell lagstiftning, och till att göra individer medvetna om hur deras personliga integritet kan påverkas av de biometriska säkerhetsfunktionerna.

Följande krav bör beaktas av utvecklare:

- Begränsad behandling. Utvecklare bör t.ex. konstruera de biometriska säkerhetsfunktionerna så att de lagrade biometriska uppgifterna kan förstöras, tas bort eller på annat sätt göras oanvändbara när den biometriska säkerhetsfunktionen inte längre används. Vidare bör utvecklare helst i så stor utsträckning som möjligt konstruera sådana biometriska säkerhetsfunktioner som inte behandlar uppgifter utöver de biometriska.
- Öppenhet. Utvecklare bör framställa synliga och öppna biometriska säkerhetsfunktioner som möjliggör för individen att vara medveten om insamlingen och användningen av dennes biometriska uppgifter. Detta innebär t.ex. att insamlingsutrustningen bör göras synlig. Öppenhet innebär även att utvecklaren bör informera den registeransvarige om den biometriska säkerhetsfunktionens funktioner. Detta kan t.ex. ske via utbildning.
- Vidta tekniska säkerhetsåtgärder. När utvecklare konstruerar biometriska säkerhetsfunktioner bör de iaktta tekniska lösningar som gör att de biometriska uppgifterna behandlas som en digital profil och inte som rådata. Dessutom bör krypteringsalgoritmer läggas till den biometriska säkerhetsfunktionen. Vidare bör de biometriska säkerhetsfunktionerna konstrueras så att de möjliggör decentraliserad lagring av de biometriska uppgifterna.

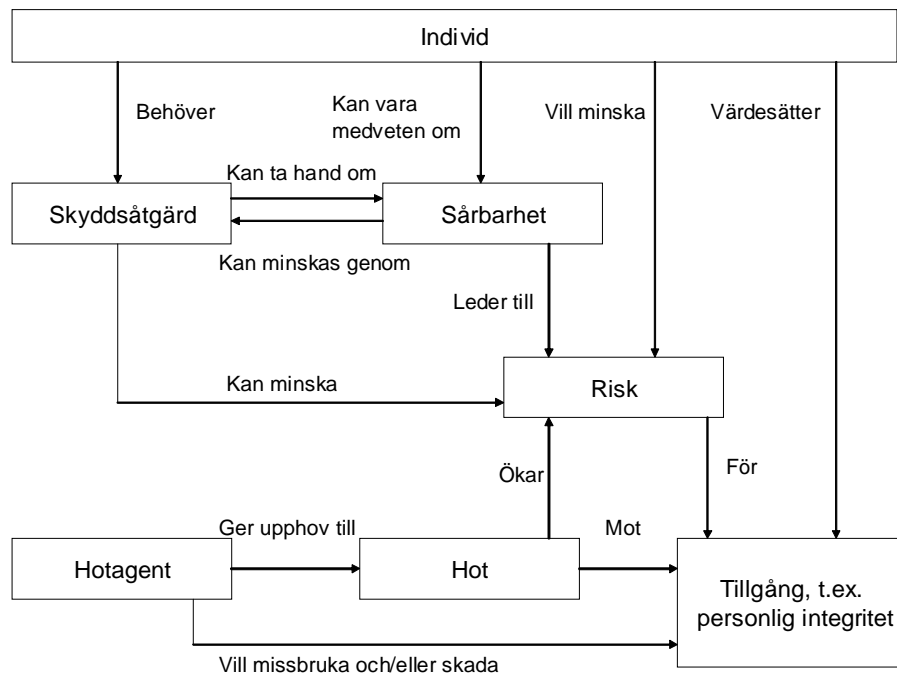
- Användarkontroll. Om icke-biometriska uppgifter lagras i anslutning till de biometriska uppgifterna bör utvecklare konstruera de biometriska säkerhetsfunktionerna så att det möjliggörs för individen att korrigera, uppdatera och se dessa uppgifter. Vidare bör de biometriska säkerhetsfunktionerna konstrueras så att individen själv äger och har kontroll över sina biometriska uppgifter, t.ex. genom decentraliserad lagring.
- Beakta lagstiftning och riktlinjer. Utvecklare bör vid utveckling av de biometriska säkerhetsfunktionerna tillämpa 95/46/EG och PUL. Vidare bör de tillämpa riktlinjer som tagits fram för att bevara den personliga integriteten i samband med biometri.

Följande krav bör beaktas av den registeransvarige, dvs. vid användning:

- Definiera syfte och varaktighet. Den registeransvarige bör bl.a. se till att de biometriska uppgifterna samlas in för ett särskilt, uttryckligt och berättigat syfte, samt att behandlingen av uppgifterna inte vid senare tillfällen sker på ett sätt som är oförenligt med detta syfte.
- Begränsad behandling. Den registeransvarige bör se till att de biometriska uppgifterna inte lagras längre än nödvändigt och att de görs oanvändbara när den biometriska säkerhetsfunktionen inte längre används. Vidare bör den registeransvarige begränsa åtkomsten till de biometriska uppgifterna. Dessutom bör den registeransvarige begränsa insamling och lagring av uppgifter utöver de biometriska. Utöver detta ska användningsområdet begränsas, dvs. användningen av biometriska uppgifter ska inte tillåtas att överskrida fysiska områdesgränser och de gränser som fastställts i lag.
- Öppenhet. Den registeransvarige bör välja att använda sådana biometriska säkerhetsfunktioner där individen är medveten om att biometriska uppgifter samlas in och används, och där insamlingsutrustningen tydligt syns. Samtycke bör inhämtas från individen innan biometriska uppgifter används. Dessutom bör syftet och alla de aspekter som rör användningen av den biometriska säkerhetsfunktionen informeras till individen. Ett sätt att informera individen är genom utbildning.
- Vidta tekniska säkerhetsåtgärder. Den registeransvarige bör se till att biometriska säkerhetsfunktioner som utnyttjar digitala profiler, kryptering och decentraliserad lagring används.
- Användarkontroll. Den registeransvarige bör ge individen kontroll över sina biometriska uppgifter. Om icke-biometriska uppgifter lagras i anslutning till de biometriska uppgifterna bör den registeransvarige möjliggöra för individen att korrigera, uppdatera och se dessa uppgifter. Vidare bör den registeransvarige se till att biometriska säkerhetsfunktioner som lagrar de biometriska uppgifterna decentraliserat används.
- Beakta lagstiftning och riktlinjer. Den registeransvarige bör vid användning av de biometriska säkerhetsfunktionerna tillämpa 95/46/EG och PUL. Vidare bör den registeransvarige tillämpa riktlinjer som tagits fram för att bevara den personliga integriteten i samband med biometri.

6.8. Sammanfattning teoridelen

Innan vi går in på den empiriska undersökningen vill vi med Figur 5 ge en sammanfattande översikt över hur de olika teorikapitlen hänger ihop.



Figur 5: Översikt över teorin.
Källa: Egenmodifierad ur [CC 2]

Individen är den som använder och interagerar med den biometriska säkerhetsfunktionen. Individen värdesätter sina tillgångar, i det här fallet sin personliga integritet. Den biometriska säkerhetsfunktionen har svaga punkter som gör den sårbar vilket leder till risker för individens personliga integritet. Vidare finns hotagenter, t.ex. bedrägliga aktörer, som vill missbruka och/eller skada individens tillgångar och därmed den personliga integriteten i detta fall. Hotagenterna ger således upphov till hot mot individens personliga integritet. För att minska dessa och reducera den biometriska säkerhetsfunktionens sårbarheter som leder till risker för individens personliga integritet behövs skyddsåtgärder. Dessa skyddsåtgärder bör beaktas vid utveckling och användning av biometriska säkerhetsfunktioner för autentisering.

7. Empirisk undersökning

Detta kapitel redogör för den empiriska undersökning som genomfördes i syfte att utreda om, och hur, man vid utveckling och användning av biometriska säkerhetsfunktioner för autentisering beaktar den personliga integriteten. Kapitlet inleds med en beskrivning av genomförandet av undersökningen. Denna beskrivning inkluderar en kort presentation av de företag som tillfrågades att delta i undersökningen samt en beskrivning av det frågeformulär som skickades ut. Sist i kapitlet presenteras undersökningens resultat och en analys av dessa.

7.1 Genomförande

Den empiriska undersökningen genomfördes den 7:e och den 9:e september 2004 genom att vi per e-post skickade ett frågeformulär till fyra företag. Två av dessa utgjordes av Precise Biometrics och Vitani A/S som utvecklar biometriska säkerhetsfunktioner. De två andra utgjordes av Scandinavian Airlines System (SAS) som på test använt biometriska säkerhetsfunktioner för autentisering i sin verksamhet, och Bornholmstrafikken som i sin verksamhet utnyttjar biometriska säkerhetsfunktioner för autentisering.

Nedan ges en kort presentation av de företag som vi skickade frågeformulären till. Därefter ges en beskrivning av arbetet med frågeformuläret.

7.1.1 Undersökningens respondenter

Precise Biometrics

Precise Biometrics är ett företag som utvecklar produkter och system för autentisering baserade på fingeravtrycksigenkänning. Företaget finns i Sverige och USA och har cirka 40 anställda. [Precise Biometrics]

Användningsområden för Precise Biometrics biometriska produkter och system är inloggning till datorer och nätverk, elektronisk handel och digitala signaturer, larm, samt lås- och passersystem. Kunderna finns bland annat inom bank och finans, EU:s regeringsdepartement och inom hälsovården. [Precise Biometrics]

De teknologier som Precise Biometrics använder sig av är Precise BioMatch, Precise Match-on-Card och Precise BioCore. Precise BioMatch baseras på en metod där flera små bilder av ett fingeravtryck sparas som en digital profil. För att verifiera en individs identitet sker en insamling av en individs fingeravtryck tredimensionellt. Det innebär att fingrets mönster, åsar och djup jämförs med den lagrade digitala profilen. Precise Match-on-Card kombinerar biometri och smarta kort och används för att ersätta PIN-koden eller lösenordet genom att den digitala profilen av fingeravtrycket lagras och matchas på det smarta kortet. Precise BioCore är en teknologi som används för digitala fickkalendrar och mobiltelefoner då dessa kräver andra typer av biometriska system än vad vanliga persondatorer gör. [Precise Biometrics]

Vitani A/S

Vitani A/S är ett företag i Danmark som utvecklar säkerhetssystem som baseras på fingeravtrycksigenkänning. Teknologin som Vitani A/S utnyttjar i sina system är Bioscrypt. En fingeravtrycksavläsare som baseras på Bioscrypt karaktäriseras bl.a. av att igenkänningsprocessen sker på under en sekund, att fingeravtrycksbilden som lagras är mycket liten och vilket gör att ett smart kort kan innehålla upp till fem fingeravtrycksbilder, samt att möjlighet till kombinationer av olika avläsare och kort finns. [Vitani A/S 03]

Scandinavian Airlines System (SAS)

SAS utförde mellan november 2003 och mars 2004 ett kundtest på Umeå flygplats där man vid incheckning och ombordstigning lät ett antal resenärer bevisa sin identitet med hjälp av biometri. Första delen av perioden testade man fingeravtryck som biometrisk igenkänningsmetod och den andra perioden iris. [Rosen-gren-Edgren 04] Testet genomfördes med smarta kort i vilket resenärens fingeravtryck respektive bild av iris lagrades. Vid incheckning och ombordstigning lästes kortet av och därefter lade resenären sitt finger på, eller höll sitt öga framför, en biometrisk avläsare. Detta för att det sedan skulle göras en jämförelse mellan avläst fingeravtryck/iris och det som lagrats på det smarta kortet. [SAS 03]

Bakgrunden till att SAS testade den biometriska tekniken för att autentisera resenärerna var att myndigheter efter attackerna mot USA den 11 september 2001 förväntas skärpa säkerhetskraven för flygbolag och flygplatser. För att således höja säkerhetsnivån utan att samtidigt göra det svårare och krångligare för resenärerna tog man därför den biometriska tekniken till hjälp. [SAS 03]

Bornholmstrafikken

Bornholmstrafikken har som huvudsyfte att utföra transport av passagerare, post och gods till och från Bornholm i Danmark [Bornholmstrafikken]. Varje år åker 1,2 miljoner passagerare med rederiet Bornholmstrafikken. Bornholmstrafikken hade problem med höga administrationskostnader vad gällde biljettförsäljning och incheckning på färjan samtidigt som man även hade problem med långa köer till biljettförsäljningen och incheckningen. Lösningen på detta problem blev en kombination av fingeravtryck och smarta kort. Passageraren bokar sin biljett i förväg genom ett bokningssystem, antingen via Internet eller telefon. När passageraren sedan anländer till färjstationen avlämnar han/hon sitt smarta kort och sitt fingeravtryck på en fingeravtrycksavläsare för att på så sätt bekräfta sin bokning. [Precise Biometrics 03]

Detta förbättrade säkerheten eftersom administratörerna nu kunde veta exakt vem som gått ombord på färjan. Ingen kan gå på färjan och utge sig för att vara någon den inte är. [Precise Biometrics 03]

7.1.2 Frågeformuläret

Vi rekommenderar att man studerar frågeformulären i Bilaga 2 innan detta avsnitt läses.

När man konstruerar ett frågeformulär bör man tänka på hur det ser ut och hur det läggs upp eftersom man som forskare är beroende av respondentens välvilja att besvara frågeformuläret. Om frågeformuläret är för omfattande, om strukturen är oklar, om man använder ett obegripligt språk eller om hela frågeformuläret verkar vara slarvigt, är risken hög att respondenten väljer att inte besvara det. Det är även viktigt att inte inleda med kontroversiella frågor om t.ex. värderingar. Istället bör man inleda ett frågeformulär med faktainriktade frågor som uppvärmning. [Holme et al 97] För att öka chanserna till att respondenterna skulle besvara vårt frågeformulär valde vi att ställa få frågor. Eftersom flera frågor dessutom är av öppen karaktär, och därmed kräver en större ansträngning av respondenten än vad det skulle krävas vid frågor som har fördefinierade svarsalternativ, är det ännu viktigare att antalet frågor är få. Vidare inleds frågeformuläret med tre faktainriktade frågor som rör bakgrundsvariabler för att få en mjuk start. Därefter ställs de frågor som rör respondentens åsikter och värderingar.

När det gäller frågeformulärets utformning och innehåll gjorde vi två versioner av det, samt engelska översättningar av dessa två. Vi gjorde således en svensk och en engelsk variant av det frågeformulär som skickades till dem som utvecklar biometrisk säkerhetsfunktioner för autentisering. På samma sätt gjorde vi en svensk och en engelsk variant av det frågeformulär som skickades till dem som i sin verksamhet använder biometrisk säkerhetsfunktioner för autentisering.

Frågeformulärets frågor

Frågeformuläret till företag som utvecklar biometrisk säkerhetsfunktioner för autentisering består av sju frågor, medan frågeformuläret till de företag som använder biometrisk säkerhetsfunktioner för autentisering består av sex frågor.

De tre inledande frågorna, som rör bakgrundsvariabler, i frågeformuläret handlar om respondentens företag, respondentens position på företaget och om vi får nämna respondentens företag i samband med presentationen av vår undersökning.

Därefter kommer de frågor som rör själva undersökningen. Frågorna är inte direkt baserade på den teori som presenteras i uppsatsen utan ska mer ses som fristående frågor. Dock avser frågorna att få fram aspekter som tas upp i kapitel sex, dvs. vilka krav man vid utveckling och användning av biometrisk säkerhetsfunktioner för autentisering bör beakta.

Fråga fyra är en relativt bred fråga vars syfte är att ge utrymme för fria associationer och det finns inga på förhand definierade svar. Syftet med frågan är att försöka få en uppfattning om vad företagen associerar med beaktande av personlig integritet och vad de anser att det innebär. Genom att svara på hur de beaktar den personliga integriteten kan vi således få en antydning om hur viktig de tycker att den personliga integriteten är och hur många olika aspekter de ser den ur.

Den femte frågan har att göra med huruvida företagen har rutiner och en utarbetad policy för hur de ska beakta den personliga integriteten. Avsikten med frågan är således att få en uppfattning om hur man arbetar med den personliga integriteten, om man anser att den är så viktig att man i sin verksamhet har riktlinjer för att inte

utveckla och använda biometriska säkerhetsfunktioner för autentisering som kränker den personliga integriteten.

Syftet med fråga sex är att ta reda på om företagen upplever att de som ska använda och interagera med de biometriska säkerhetsfunktionerna för autentisering är angelägna om sin personliga integritet. Utifrån detta vill vi med frågan också ta reda på hur företagen hanterar dessa individer och deras önskemål. Man skulle kunna tolka fråga fyra och sex som någorlunda lika, men med fråga sex vill vi fokusera mer på den mänskliga faktorn och hur företagen hanterar den oro som kan uppkomma hos individer. Vi vill således ta reda på hur, och vad, man förmedlar till dem som ska använda de biometriska säkerhetsfunktionerna för autentisering för att visa hur man beaktar deras personliga integritet.

Fråga sju ställdes enbart till de företag som utvecklar biometriska säkerhetsfunktioner för autentisering. Syftet är att ta reda på om utvecklarna beaktar användarnas personliga integritet även efter själva utvecklingen och efter leveransen. Vi vill således veta om de enbart beaktar den personliga integriteten vid tillverkning eller om deras beaktande även sträcker sig till efter leverans av de biometriska säkerhetsfunktionerna för autentisering. Även denna fråga är ett sätt för oss att försöka nå den mänskliga aspekten av beaktandet av den personliga integriteten. Efter att ha besökt webbsidor på Internet tillhörande företag som utvecklar biometriska säkerhetsfunktioner för autentisering och efter att ha pratat med försäljare av desamma, har vi fått intrycket av att nästan all fokus ligger på tekniskt skydd för att beakta den personliga integriteten. Vi vill med fråga sex och sju således försöka få fram om man även beaktar den personliga integriteten på annat sätt.

Test av frågeformuläret

I och med problem med att få tag på företag som utvecklar och använder biometriska säkerhetsfunktioner för autentisering, har de som svarat ja till att vara med i vår undersökning, också fått ett frågeformulär. Vi har därför inte utfört en pilotstudie i den traditionella bemärkelsen, och har därmed inte kunnat testa våra frågeformulär på företag som liknar de som ingår i undersökningen. Istället har vi skickat frågeformuläret till studenter på Data- och Systemvetenskapliga institutionen vid Stockholms universitet för att få respons på, och åsikter kring, frågorna. De testpersoner vi skickade frågeformulären till utgjordes av tre andra studenter som vid tillfället också skrev magisteruppsats om biometri, samt två studenter som inte är involverade i biometriområdet. Av dessa studenter var det enbart de två sistnämnda, som inte är involverade i biometriområdet, som svarade och gav respons. Utifrån deras reaktioner och åsikter gjorde vi några få ändringar i frågorna vad gäller formuleringar och ordval.

7.2 Resultat

Nedan åskådliggörs de resultat som den empiriska undersökningen gav. Detta görs genom att vi först presenterar utvecklarnas resultat där vi för varje fråga redogör för vad de olika respondenterna svarade. Därefter presenteras på samma sätt resultaten från de företag som i sin verksamhet använder sig av biometriska sä-

kerhetsfunktioner. De tre första frågorna i frågeformuläret presenteras inte eftersom de inte har med själva undersökningen att göra, utan endast är bakgrundsvariabler.

7.2.1 Resultat utveckling

Fråga 4. Hur beaktar Ni användarens personliga integritet vid utveckling av biometriska system för autentisering?

Precise Biometrics

”Precise Biometrics flaggskepp är, som för många andra biometriföretag, vår algoritm för att utföra matchningen. Personlig integritet är med andra ord ett mycket starkt skäl till att tro att Match-on-Card kommer att slå igenom på bred front.”

Vitani A/S

“Different technologies are used for protecting privacy. Some gives more protection than others.”

Fråga 5.

- a) Har Ni en utarbetad policy innehållande rutiner för utvecklingen av de biometriska systemen vid autentisering, så att de vid nyttjandet inte kränker den personliga integriteten? (Ja/Nej)
- b) Om ja, vilka punkter innehåller den?
- c) Om nej, skulle en sådan underlätta arbetet med att utveckla biometriska system för autentisering som beaktar den personliga integriteten vid nyttjandet av de biometriska systemen?

Precise Biometrics

Respondenten valde att inte besvara denna fråga.

Vitani A/S

“No we do not have a prepared policy. We believe that this must be up to the end-user to decide. We inform them about the different systems and which systems might cause problems regarding privacy and which system who do not cause problems. We are selling a fingerprint reader solution where the fingerprint is stored on a Smart Card that the user himself is administering. This way the fingerprint is still in the privacy of the user. Another thing is that the fingerprint reader system that we are selling is not compatible with fingerprint systems used by the police. This way no one should be worried about abuse of their fingerprints.”

Fråga 6.

- a) Upplever Ni att tänkta användare av biometriska system för autentisering är angelägna om sin personliga integritet i samband med dessa? (Ja/Nej)
- b) Om ja, hur tillmötesgår Ni dessa personer och deras eventuella oro och önskemål som kan uppstå kring den personliga integriteten?

Precise Biometrics

”För att bäst svara på detta så ska jag kort lista hur vi hanterar biometrin:

* Då en användare enrollerar sig så skapas ett templat som läggs på det smarta kortet. Templatet kan aldrig användas för att återskapa ett fingeravtryck. Templatet finns vidare ingen annanstans än på just användarens kort. Användaren förfogar mao själv över vem han/hon ska dela med sig av informationen till.

* Vid verifiering så lägger användaren fingert på en sensor. "Live-bilden" skickas in på kortet där matchningen sker. Biometrisk data lämnar med andra ord aldrig kortet. Det rätta templatet skickas varken upp till läsaren eller till en PC. Vid positivt resultat så låser kortet upp "hemligheterna" på kortet. Bara då får man åtkomst till vad som ligger på smartkortet, tex namn, nationalitet etc om vi pratar pass.

Jag tror att ni får en god bild över PreciseBiometrics inställning till integritet om ni tittar igenom det whitepaper jag rekommenderade. Faktum är att just integritet är en mycket viktig faktor för oss eftersom Match-on-Card ger oss en unik position på marknaden. Vi upplever att intresset för biometri ökar och det är givetvis viktigare än någonsin att redan från början ta hänsyn till individen.”

Vitani A/S

“No, but we inform them anyway about the potential questions in using their fingerprint. Please look at our answer on question 5.”

Fråga 7. Vilken typ av stöd, t.ex. kundsupport och service, erbjuder Ni kunderna, efter leverans, för att de ska kunna värna den personliga integriteten vid nyttjande av biometriska system för autentisering?

Precise Biometrics

Respondenten valde att inte besvara denna fråga.

Vitani A/S

“I don't understand the question! Our customers are always welcome to contact us for customer support and service afterwards but regarding the privacy this must be handled before the systems is sold. Some systems protect more against privacy violation than others – you should be aware of this before delivery.”

7.2.2 Resultat användning

Fråga 4. Hur beaktar Ni den personliga integriteten när användarna nyttjar de biometriska systemen för autentisering?

SAS

”Det är mycket viktigt att den personliga integriteten beaktas, att man visar att det finns en seriös tanke bakom införandet av systemet i fråga.”

Fråga 5.

- a) **Har Ni en utarbetad policy innehållande rutiner för hur den personliga integriteten ska kunna skyddas vid nyttjandet av de biometriska systemen för autentisering? (Ja/Nej)**
- b) **Om ja, vilka punkter innehåller den?**
- c) **Om nej, skulle en sådan underlätta beaktandet av användarnas personliga integritet vid nyttjandet av de biometriska systemen för autentisering?**

SAS

Fråga 5a: ”Nej.”

Fråga 5c: ”Ja.”

Fråga 6.

- a) **Upplever Ni att användarna av de biometriska systemen för autentisering är angelägna om sin personliga integritet i samband med nyttjandet av dessa? (Ja/Nej)**
- b) **Om ja, hur tillmötesgår Ni de önskemål som uppkommer kring den personliga integriteten?**

SAS

Fråga 6a: ”Ja.”

Fråga 6b: Respondenten valde att inte besvara denna fråga.

Bornholmstrafikken

Bornholmstrafikken valde att inte svara på frågeformuläret.

7.3. Analys

Nedan ges en summerande analys kring de svar vi fick in genom undersökningen. Bornholmstrafikken som inte besvarade frågeformuläret tas inte upp i analysen. En djupare diskussion kring undersökningen och dess resultat ges i kapitel åtta.

Fråga fyra, där respondenterna gavs möjlighet att svara fritt angående hur de beaktar den personliga integriteten, gav kortfattade svar. Samtliga respondenter svarar genom att endast ta upp en aspekt på hur de beaktar den personliga integriteten. De två företag som utvecklar biometriska säkerhetsfunktioner, Precise Biometrics och Vitani A/S, tar upp den tekniska aspekten. Precise Biometrics tar upp en specifik algoritm som de använder för att utföra matchningen i den biometriska processen. I anslutning till detta ber de oss att titta närmare på deras officiella hemsida där de beskriver denna algoritm, Match-on-Card, vilket ger en något bredare beskrivning av hur de beaktar den personliga integriteten. I dokumentet tar man den teknologiska aspekten lite längre när det gäller den personliga integriteten. De nämner att det inte behövs någon extern databas vilket gör att individen inte behöver lämna ifrån sig sin biometriska egenskap och att utgivarna av de smarta korten slipper bekymmer med att uppdatera och underhålla databasen. Precise Biometrics tar i dokumentet också upp aspekten med stulna smarta kort och säger att den digitala profilen av fingeravtrycket, samt övriga uppgifter som finns

på kortet, inte kan erhållas från det smarta kortet. I samband med detta nämner man **PKI*** och att det smarta kortet bevarar den **privata nyckeln***. Även Vitani A/S tar endast upp den tekniska aspekten på fråga fyra. De är dock inte lika detaljerade som Precise Biometrics och går inte in på någon specifik teknologi. Istället svarar de att de använder olika teknologier som ger olika skydd för den personliga integriteten. SAS, som i sin verksamhet på prov använt biometriska säkerhetsfunktioner för autentisering, svarar också mycket kortfattat på denna fråga. De nämner dock inga tekniska aspekter utan skriver att det är väldigt viktigt att man visar att det finns en seriös tanke bakom införandet av den biometriska säkerhetsfunktionen.

På fråga fem, som ska ta reda på om företagen har någon utarbetad policy för hur de hanterar den personliga integriteten, fick vi olika respons. Precise Biometrics valde att inte besvara frågan, men Vitani A/S tar däremot upp flera aspekter. De nämner först att de inte har någon utarbetad policy då de anser att det är upp till slutanvändarna att bestämma detta. Vad de menar med detta är dock något tvetydigt. Kanske missförstod Vitani A/S frågan och trodde att vi undrade om de har någon policy för hur slutanvändarna ska beakta sin personliga integritet. Detta är dock bara spekulationer, och det är svårt att veta hur de faktiskt uppfattade frågan. Vitani A/S fortsätter svaret på frågan genom att skriva att de informerar slutanvändarna om de olika systemen och vilka av dem som kan orsaka problem för den personliga integriteten, och vilka av systemen som inte gör det. Vidare tar de upp smarta kort som individen själv har kontroll över. De säger också att deras system inte är kompatibla med sådana system som polisen använder vilket gör att ingen ska behöva vara orolig för att deras fingeravtryck kommer att utnyttjas. Vitani A/S visar således genom sitt svar på fråga fem att de är medvetna om flera aspekter av den personliga integriteten än vad som först kom fram i samband med svaret på fråga fyra. SAS svarar på frågan att de inte använder någon utarbetad policy, men att de tror att en sådan skulle underlätta för dem att beakta slutanvändarnas personliga integritet.

På fråga sex, där vi ville få fram hur företagen tillmötesgår de slutanvändare som är oroliga över sin personliga integritet, svarade Precise Biometrics genom att beskriva hur den biometriska processen går till. De tar här upp det smarta kortet och att den digitala profilen av fingeravtrycket som lagras på det smarta kortet inte kan återskapas. De svarar vidare att fingeravtrycket endast finns på det smarta kortet och ingen annanstans, vilket innebär att det enbart är individen själv som bestämmer vem som ska få ta del av informationen på kortet. Vidare beskriver Precise Biometrics verifieringsprocessen och hur den går till. De säger att individen vid verifiering lägger sitt finger på en sensor och att matchningen sker på det smarta kortet vilket innebär att biometrisk data aldrig lämnar kortet. I samband med detta får vi också reda på att det smarta kortet vid positiv matchning ger åtkomst till de uppgifter som finns på kortet, t.ex. namn och nationalitet. Precise Biometrics anser att deras inställning till den personliga integriteten kommer fram i den beskrivning av algoritmen Match-on-Card som de ger på sin hemsida på Internet. I och med att intresset för biometri ökar anser de att det är mycket viktigt att man redan från början tar hänsyn till individen. Vitani A/S svarar kortare på samma fråga, men refererar till fråga fem i samband med frågan. De säger dock

att de inte upplever att de tänkta användarna är angelägna om sin personliga integritet, men att de ändå informerar användarna om de aspekter som kan uppkomma i samband med att deras fingeravtryck används. SAS svarar ”ja” på frågan om de upplever att användarna av de biometriska systemen är angelägna om sin personliga integritet i samband med dessa. De valde dock att inte svara på följdfrågan om hur de tillmötesgår användarna och deras eventuella oro kring den personliga integriteten. Vitani A/S och SAS svarade således tvärtemot varandra på fråga 6a. Detta tror vi kan bero på att Vitani A/S utvecklar biometriska säkerhetsfunktioner och därmed inte får någon närmare kontakt med slutanvändarna. Det får antagligen SAS i större utsträckning eftersom de på test använt biometriska säkerhetsfunktioner i sin kärnverksamhet som innefattar slutanvändare.

Den sista frågan, fråga sju, ställdes enbart till de företag som utvecklar biometriska säkerhetsfunktioner för autentisering. I den frågan ville vi veta om företagen erbjuder stöd till sina kunder efter leverans av de biometriska säkerhetsfunktionerna. Precise Biometrics valde att inte besvara frågan. Vitani A/S sa att de inte förstod frågan, men de uttalade sig ändå i denna fråga. De skrev att deras kunder alltid kan kontakta dem om de behöver support och service efter leverans. Dock anser Vitani A/S att när det gäller den personliga integriteten, så måste detta hanteras innan systemet går till försäljning. De anser att man bör vara medveten om att vissa system skyddar den personliga integriteten mer än andra.

8. Slutsats och diskussion

Detta kapitel inleds med slutsats och diskussion av den teoretiska delen av uppsatsen, vilket svarar mot uppsatsens två första frågeställningar. Därefter ges en slutsats och diskussion av uppsatsens empiriska del som svarar mot uppsatsens tredje frågeställning. I slutet av kapitlet ges förslag till vad man i framtiden kan göra för forskning relaterat till uppsatsens ämne.

8.1 Teori

Nedan ges slutsats och diskussion kring studiens teoretiska del.

8.1.1 Slutsats för teoridelen

Genom att uppnå den teoretiska delens mål anser vi att vi kan besvara de två första frågeställningarna som vi satt för uppsatsen. Frågeställningarna med svar presenteras därför nedan.

Frågeställning 1: Kränker biometriska säkerhetsfunktioner för autentisering den personliga integriteten, och i så fall hur?

Svar: Utifrån den definition vi tagit fram kränker biometriska säkerhetsfunktioner en eller flera av definitionens variabler. Som framgår i kapitel fyra innebär en kränkning av den personliga integriteten att en eller flera variabler i definitionen inte uppfylls. Nyttjandet av biometriska säkerhetsfunktioner kan ge upphov till hemlig igenkänning och brist på anonymitet, sekundär användning av de biometriska uppgifterna samt avslöjande av känslig information till obehöriga. Dessutom kan systemattacker ge upphov till exponering av de biometriska uppgifterna och systemfel kan ge upphov till diskriminering samt kvalitetsbrister på de biometriska uppgifterna. Vidare kan lagringen av de biometriska uppgifterna ge upphov till ytterligare kontroller och sammankoppling av information. Detta hotar individens möjlighet till att bli lämnad ifred och att få vara anonym, individens värdighet, individens möjligheter till att själv bestämma över sitt handlande och sina personliga uppgifter, samt individens personliga uppgifters insyn, användning och kvalitet.

Frågeställning 2: Vilka krav bör ställas i samband med utveckling och användning av biometriska säkerhetsfunktioner för autentisering, för att skydda den personliga integriteten?

Svar: Det finns flera krav som man bör ställa i samband med utveckling och användning av biometriska säkerhetsfunktioner då dessa krav på ett eller flera sätt skyddar de variabler som utgör definitionen av personlig integritet. Krav som bör beaktas är att definiera syfte och varaktighet med de biometriska säkerhetsfunktionerna, begränsa behandlingen av biometriska uppgifter, erbjuda öppenhet, vidta tekniska säkerhetsåtgärder, erbjuda användarkontroll, samt uppmärksamma lagstiftning och riktlinjer som finns för personuppgifter och biometriska säkerhetsfunktioner.

8.1.2 Diskussion kring teoridelen

Uppsatsens teoretiska del har som mål att utifrån en definition av begreppet personlig integritet utreda om, och i så fall hur, den personliga integriteten kan kränkas vid användning av biometriska säkerhetsfunktioner för autentisering. I anslutning till detta är den teoretiska delens mål även att presentera krav som bör ställas i samband med de biometriska säkerhetsfunktionerna för att skydda den personliga integriteten.

Den teoretiska delen inleds med kapitel tre där det beskrivs hur en biometrisk säkerhetsfunktion för autentisering är uppbyggd. Fokus ligger på hur en fingeravtrycksbaserad biometrisk säkerhetsfunktion är utformad. Denna beskrivning är till för att få en förståelse för området biometri vilket vi anser är nödvändigt för att förstå uppsatsens mål och syfte samt de resonemang som förs i uppsatsen.

I kapitel fyra presenteras begreppet personlig integritet. Syftet med kapitlet är att presentera olika definitioner som tas upp i litteraturen och utifrån dessa generera en tydlig och välavgränsad definition av begreppet personlig integritet. Då vi i följande kapitel bl.a. utreder hur den personliga integriteten kränks vid användning av biometriska säkerhetsfunktioner är det nödvändigt att ha en distinkt definition av begreppet att utgå ifrån. Det vi upptäckte under tiden vi arbetade med kapitlet var att begreppet personlig integritet kan tolkas på olika sätt samt att en var även har sin egen uppfattning av vad begreppet innebär. Dessutom kan begreppet ha olika innebörd beroende på omständighet och situation. Intentionen är att ge en bred men tydlig definition som inte är bunden till ett visst tillstånd. När vi tog fram definitionen var vi medvetna om att de olika variablerna av den kanske inte skulle komma att påverkas i samband med användningen av biometri. Vi fann dock i senare kapitel att så inte var fallet, utan att alla variablerna av den definition vi givit faktiskt kom att beröras i situationer där biometri används för autentisering.

Kapitel fem inleds med en kort presentation kring den biometriska uppgiften som personuppgift. Om en biometrisk uppgift verkligen bör betraktas som en personuppgift som är direkt förknippad med en individ finns det olika åsikter om. Meningsskiljaktigheter verkar framförallt uppstå då den biometriska uppgiften behandlas som en digital profil i och med att man då inte direkt kan koppla denna till en specifik individ. Så länge man inte kan komma överens om huruvida biometriska uppgifter och digitala profiler av dem, är unika eller inte, bör det också vara svårt att avgöra i vilken utsträckning användningen av biometri är ett hot mot den personliga integriteten. Samtidigt kan man också anta att oron och osäkerheten kring biometriska säkerhetsfunktioner ökar hos allmänheten när det förmedlas en splittrad och osäker bild. Eftersom man inte kan utesluta att biometriska uppgifter är personuppgifter under alla omständigheter bör man hursomhelst ta de risker som finns med användning av biometri på största allvar.

Därefter fortsätter kapitlet med en presentation av olika risker som kan kränka den personliga integriteten vid användningen av biometriska säkerhetsfunktioner för autentisering. Med utgångspunkt i de risker som de biometriska säkerhetsfunktionerna kan medföra är det huvudsakliga syftet med kapitlet att försöka ge en upp-

fattning om, och hur, varje typ av risk faktiskt kan kränka den personliga integriteten. Då vi upplever att det i källorna som vi använt oss av inte har gjorts någon uttrycklig och djupare utredning av hur den personliga integriteten kan påverkas av användningen av biometriska säkerhetsfunktioner fann vi det särskilt intressant att behandla detta. De risker som tas upp i kapitlet är de risker som tydligast framträtt på flera ställen i källorna och som vi därför ansåg vara de mest centrala. Utöver de risker som presenteras i uppsatsen finns säkerligen flera, särskilt om man väljer att undersöka detaljer i den biometriska processen och går in på djupet på dessa. Vår avsikt har dock varit att ge en översiktlig presentation, och en introduktion till problematiken kring biometri och personlig integritet.

Resultatet av kapitel fem är att de risker som presenteras på flera sätt kränker den personliga integriteten. Vi fann att varje risk, om den inträffar, faktiskt kränker flera av de variabler som ingår i vår definition av personlig integritet. Att vi fann att flera variabler i definitionen påverkas av varje typ av risk kan dock bero på att flera av de variabler som utgör definitionen hänger ihop och går in i varandra. Exempelvis innefattar variabeln om informationssäkerhet variabeln om att individen själv ska få kontrollera och bestämma över sina personliga uppgifter. Vidare, om man inte själv får bestämma över sina personliga uppgifter och sitt beteende kan man säkert känna att ens värdighet kränks. Att skilja de olika variablerna åt i beskrivningarna av riskerna har således inte varit helt problemfritt. Viktigt är också att vara medveten om att konstaterandet av hur den personliga integriteten kränks om en risk inträffar, är våra egna antaganden och därför endast bör ses som just detta. Att göra egna antaganden och dra egna slutsatser kring detta var dock nödvändigt i och med att ingen källa som vi använt oss av förklarat och utrett på vilket sätt de olika riskerna kränker den personliga integriteten. Som nämns i kapitel fem är den personliga integriteten individuell och uppfattas olika av olika individer. Det är därför viktigt att samtidigt påpeka att våra antaganden inte är några definitiva konstateranden som gäller för alla. Det vi gjort är snarare att ge exempel på hur vi tror att den personliga integriteten skulle kunna kränkas om en viss risk inträffar. Genom att utgå från definitionen och se om en eller flera av dess variabler inte uppfylls vid användning av en biometrisk säkerhetsfunktion, har vi dragit slutsatsen att den personliga integriteten kränks.

I och med att detta är en kvalitativ studie och att vi själva har tolkat situationen kan vi även mycket väl också ha styrt den. Det finns en risk att vi i uppsatsen på ett omedvetet sätt kan ha anpassat riskerna efter vår definition och försökt styra resultaten mot att riskerna ska påverka variablerna i vår definition. Det går således inte att utesluta att vi från början förväntade oss ett visst resultat och att vi försökt styra uppsatsen mot detta. Vidare bör våra tolkningar och våra upplevelser av hur den personliga integriteten kränks ses som en subjektiv bedömning som inte behöver vara definitiv och stämma för alla. Med tanke på detta skulle validiteten och reliabiliteten i resultaten därför kunna ifrågasättas. Dock är det inte det som är syftet med den kvalitativa litteraturstudie vi gjort. Meningen var inte att ta fram information som är generellt giltig och pålitlig utan att istället försöka skapa en djupare förståelse för den problematik vi valt att studera. Det anser vi också att vi gjort med den teoretiska studien i uppsatsen.

Samtidigt anser vi att vi utgått från en klar och distinkt definition av begreppet personlig integritet vilket medför att riskerna med att vi undersöker något annat än det vi avser att undersöka, minskar. Vi har genom detta således försökt klargöra vad det är vi avser att undersöka i uppsatsen. På så sätt kan man säga att vi försökt uppnå en hög validitet. Trots att den personliga integriteten är individuell bör man ändå anta att det finns en viss allmän uppfattning om vad personlig integritet faktiskt innebär. Utifrån källorna har vi således använt vad som kan anses vara vedertagna uppfattningar kring den personliga integriteten och presenterat en sammanfattande definition av dessa. Vi klargjorde även vad de olika variablerna av definitionen innebär för att tydliggöra vad det var vi ville undersöka. Vi anser således att den distinkta definitionen med tydligt angivna och förklarade variabler har underlättat att besvara den frågeställning som vi avsåg att besvara i studien.

Det största problemet som vi ser med att undersöka om den personliga integriteten kränks eller inte, är just validiteten, i och med det tvetydiga i begreppet personlig integritet. Även om vi gjort en tydlig precisering av begreppet, och presenterat vad varje variabel av definitionen innebär, kan man aldrig bortse ifrån att upplevelsen av att få sin personliga integritet kränkt är individuell. Vi tror ändå att resultaten av studien kan ha betydelse i och med att vår definition av personlig integritet består av flera variabler som tar upp flera aspekter av den personliga integriteten. Om vi endast utgår ifrån själva resultaten och att de pekar på att den personliga integriteten kränks, kan detta ha stor betydelse för individer som på ett eller annat sätt kommer att beröras av användningen av biometri. Vi upplever att problematiken kring personlig integritet och biometri är abstrakt. Det gör det svårt för allmänheten att riktigt förstå hur deras personliga integritet faktiskt kan påverkas av biometri. Om allmänheten blir uppmärksam och får exempel på hur de biometriska säkerhetsfunktionerna kan kränka deras personliga integritet, tror vi att det kan leda till att biometribranschen börjar arbeta mer med detta. Detta kan i sin tur leda till att det blir svårare för biometribranschen att släppa ofärdiga produkter där tekniken inte är tillräckligt färdig för att kunna värna om den personliga integriteten. Studiens resultat kan även göra biometribranschen mer uppmärksam på vilka aspekter av den personliga integriteten som de bör beakta.

Den teoretiska studien avslutas med kapitel sex där avsikten är att ta fram krav som bör beaktas vid utveckling och användning av biometriska säkerhetsfunktioner för att minska riskerna för att den personliga integriteten kränks vid nyttjandet av dessa. Syftet med detta kapitel är att redogöra för de krav som man vid utveckling och användning bör beakta för att minska eller helt reducera de risker som kan kränka den personliga integriteten. I samband med detta visar vi också på hur varje krav kan skydda den personliga integriteten. Precis som i kapitel fem handlar det om våra egna tolkningar och slutsatser utifrån vår definition när det gäller hur den personliga integriteten skyddas. När det gäller kraven, som var huvudsyftet i kapitel sex, försöker vi ge en sammanfattande bild av vad källorna vi använt fört fram. Framförallt tar vi upp sådana aspekter som fördes fram i mer än en källa, t.ex. aspekter som rör öppenhet, samtycke från individen och tekniska säkerhetsåtgärder som digital profil och kryptering. Vi vill understryka att det säkerligen finns fler krav man bör beakta, men att dessa antagligen ligger på en mer detaljerad nivå än vad som är avsikten med studien.

Resultatet som kapitel sex ger i form av de krav som vi presenterar, hoppas vi ska fungera som underlag och stöd för företag som utvecklar respektive i sin verksamhet använder biometriska säkerhetsfunktioner för autentisering. Framförallt hoppas vi att de presenterade kraven ska göra dem mer uppmärksamma på hur beaktandet av krav kan skydda den personliga integriteten. I och med att vi kopplar kraven till exempel på hur de kan värna om den personliga integriteten kanske intresset och drivkraften till att verkligen beakta dessa krav ökar. Dessutom kanske det blir svårare för företagen att bortse ifrån dessa krav då kraven är förenade med åskådliga exempel på vad de faktiskt gör för den personliga integriteten. Vidare förväntar vi oss att allmänheten, som är de framtida användarna av biometriska säkerhetsfunktioner, ska bli mer medvetna om vilka krav de kan ställa på biometriska säkerhetsfunktioner när de blir varse om att kraven kan skydda deras personliga integritet.

Kapitel sex har även fungerat som ett teoretiskt underlag för den empiriska undersökning som gjordes för uppsatsen. Även om den empiriska undersökningen inte direkt baseras på den teoretiska delen av uppsatsen har teorin ändå varit ett stöd. Det hade varit svårt att undersöka hur väl företag beaktar den personliga integriteten om vi inte vetat något om vilka krav de faktiskt kan beakta.

8.2 Empiri

Nedan ges diskussion och slutsats kring studiens empiriska del.

8.2.2 Slutsats för empiridelen

Det är svårt att säga till vilken grad vi uppnått den empiriska delens mål. Detta med tanke på undersökningens karaktär, att vi inte varit ute efter att ge några mätbara svar och att vi fick tag på så få företag som i vissa fall även gav kortfattade svar. Våra tolkningar av svaren spelar också roll för vilken bild av dessa företag som ges. Vi tror att det skulle behövas en större undersökning med framförallt flera respondenter, för att man på ett mer fullständigt sätt ska kunna förstå den situation vi undersökt. Vi anser ändå att vi genom frågeformulären gett företagen chans att visa att, och hur, de beaktar den personliga integriteten. Med hänsyn till undersökningens omständigheter har vi ändå kunna ge ett rimligt svar på uppsatsens tredje frågeställning. Frågeställningen med svar presenteras därför nedan.

Frågeställning 3: Beaktar man i praktiken vid utveckling och användning av biometriska säkerhetsfunktioner för autentisering den personliga integriteten, och i så fall hur?

Svar: Företagen som undersöktes i denna studie beaktar den personliga integriteten, men gör det på ett något ensidigt sätt. Stor fokus bland de företag som utvecklar biometriska säkerhetsfunktioner för autentisering ligger på teknologiska skydd. För företaget som i sin verksamhet använder biometriska säkerhetsfunktioner för autentisering, ligger fokus på att visa användarna att det finns ett seriöst syfte med införandet av en biometrisk säkerhetsfunktion. Vidare är det bland utvecklarna viktigt att individen själv ska få kontrollera och bestämma över sin per-

sonliga information och att den inte kommer till andras kännedom. Detta beaktas genom smarta kort. En utvecklare nämner, utöver smarta kort, även digital profil och kryptering. Från en annan utvecklare anses det viktigt att informera användarna om de biometriska säkerhetsfunktionerna och vad det innebär för dem att lämna en biometrisk egenskap. Samma utvecklare är också medveten om den oro som kan uppstå i samband med polisväsendet och deras fingeravtryckssystem. Man beaktar därför den personliga integriteten genom att inte sälja sådana fingeravtrycksavläsare som är kompatibla med polisens.

8.2.1 Diskussion kring empiridelen

Uppsatsens empiriska del har som mål att via ett frågeformulär undersöka om, och hur, företag som utvecklar eller använder biometriska säkerhetsfunktioner för autentisering beaktar den personliga integriteten.

För att uppnå den empiriska delens mål antog vi ett kvalitativt angreppssätt. Vi utformade ett frågeformulär med både öppna och slutna frågor. Det vi ville uppnå var att få en uppfattning av, och förståelse för, hur företag idag tar hänsyn till den personliga integriteten och på så sätt ta del av deras syn på problemområdet. I och med att vi ville undvika att styra och påverka respondenterna, och i och med de geografiska avstånden, utfördes undersökningen per e-post. Själva undersökningen var således på förhand strukturerad med fördefinierade frågor. Vår avsikt var dock att respondenterna skulle få svara fritt på frågeformuläret. Då vi inte ville styra respondenterna för mycket kunde vi heller inte kontrollera att de faktiskt svarade på frågorna såsom vi förväntade oss.

I samband med den empiriska undersökningen stötte vi på flera problem. Vi kontaktade ett flertal företag, t.ex. utvecklingsföretag inom biometribranschen, samt skolor, flygbolag och banker som använder biometriska säkerhetsfunktioner. Vi fick dock respons enbart från några få av dessa, vilket gjorde att vi fick få undersökningsenheter till undersökningen. I slutändan blev det således enbart tre företag som besvarade frågeformuläret; Precise Biometrics, Vitani A/S och SAS. Vi hade önskat att få in flera svar, framförallt från företag som i sin verksamhet använder biometriska säkerhetsfunktioner. Som det blev nu fick vi bara svar från SAS, som egentligen inte använder biometriska säkerhetsfunktioner, utan endast använt ett sådant på test under en halvårsperiod. Ett frågeformulär skickades även till Bornholmstrafikken efter att en person därifrån svarat att vi kunde ställa frågor till honom. Han valde dock att inte besvara frågeformuläret.

Det faktum att just Precise Biometrics, Vitani A/S och SAS besvarade frågeformuläret kan bero på att dessa har ett visst intresse för studieområdet. Även om det inte gjordes något direkt urval av företag från vår sida kan det, beroende på företagets intressen, ändå ha uppstått en viss snedvridning av de respondenter som ingår i undersökningen. Utvecklingsföretagen kan t.ex. ha ett intresse i studieområdet ur ett nyttoperspektiv på så sätt att de vill föra fram sin teknologi och även sig själva som företag. Även ett användarföretag vill kanske marknadsföra sig själv och föra fram att man t.ex. använder sig av ny teknologi och därmed utvecklas för att visa att man prioriterar säkerhet. Om man på detta sätt kan locka kunder kan man också öka företagets effektivitet. Att företagen utgår från ett nytto- eller

effektivitetsperspektiv kan göra att beaktandet av den personliga integriteten kommer i andra hand. Den personliga integriteten är därför kanske inte den huvudsakliga anledningen till att företagen besvarar frågeformuläret. Respondenterna och vi som forskare kan således ha olika syften, dvs. respondenterna besvarar inte frågorna av samma anledning som vi ställt dem. När respondenternas svar analyseras och tolkas bör man vara medveten om detta.

Vidare var de svar vi fick in inte så omfattande som vi hade förväntat oss. Vi hade t.ex. som svar på fråga fyra (se Bilaga 2), som vi såg som en bred fråga, förväntat oss längre utlägg från respondenterna där de förklarar hur de beaktar den personliga integriteten på flera olika sätt. Istället fick vi av de flesta respondenter korta svar som endast tog upp en aspekt av den personliga integriteten. Vi hade hoppats att frågan skulle få respondenterna att svara brett och därmed få en chans att visa sitt beaktande av den personliga integriteten ur många olika perspektiv. Tendenser till fler aspekter av den personliga integriteten kom av de flesta dock fram i efterföljande frågor. Vi skulle kunna ha försökt åtgärda detta genom att skicka ytterligare frågor till respondenterna för att försöka få in utförligare svar, och för att få en djupare förståelse för problemområdet. Vi ansåg dock att detta tillvägagångssätt skulle kunna ge en bild av respondenterna som mer hänsynstagande till den personliga integriteten än vad de faktiskt är. Vi ville dessutom undvika ledande och direkta frågor som kan härledas till de krav vi tog fram i den teoretiska delen av undersökningen. Detta tror vi skulle ha kunnat styra respondenterna till att ge sådana svar som de tror att vi vill ha. Validiteten skulle i sådana fall kunnat ha blivit tveksam.

Beträffande själva undersökningen och de svar som respondenterna gav, fick vi således inte ut så mycket som vi hade hoppats. Däremot kan även ett icke-svar säga en del. Frågeformuläret skickades ut till fyra företag. Tre besvarade formuläret. Två av tre respondenter hoppade över en eller två frågor, och en respondent sa sig inte förstå en fråga men uttalade sig ändå i frågan. Att en respondent hoppar över en fråga kan man tolka på olika sätt. Antingen var frågan dåligt formulerad vilket gjorde att respondenten inte förstod frågan, eller så förstod respondenten frågan, men valde att inte svara. Att en respondent väljer att inte svara på en fråga kan också bero på flera andra aspekter. Det kan t.ex. bero på tidsbrist, lathet eller att respondenten faktiskt inte har något svar på frågan. Det senare skulle man i vårt fall kunna tolka som att den personliga integriteten inte beaktas på det sätt som frågan försöker få fram. Men det är svårt att säga att så faktiskt är fallet. Dessutom skulle det i det här fallet kunna vara så att respondenterna upplevde flera av frågorna som lika varandra. Om så är fallet kan detta leda till att de låter bli att svara på en fråga för att de anser sig ha besvarat den i en annan. När det gäller den respondent som inte besvarade frågeformuläret är det också svårt att säga vad detta beror på. Det kan t.ex. vara så att företaget inte har så stor insyn i hur de beaktar den personliga integriteten, och inte bryr sig om den särskilt mycket, och därför valde att inte svara på frågeformuläret. Men det kan också ha andra orsaker som inte har med hur de beaktar den personliga integriteten att göra.

Av de tre respondenter som svarade verkar vissa, utifrån svaren på frågeformuläret, beakta den personliga integriteten mer än andra. Utvecklarna gav, i relation

till den som representerade företaget som använder biometriska säkerhetsfunktioner, mer uttömmande svar. Detta kan dock bero på att företaget som använder biometriska säkerhetsfunktioner endast gjort detta på test och därmed inte är lika insatt som ett utvecklingsföretag. Dessutom kan de olika svaren bero på huruvida vi frågade rätt personer. Vår avsikt var att fråga den person på varje företag som ansvarade för utvecklingen respektive användningen av de biometriska säkerhetsfunktionerna. Detta önskemål var också något som fördes fram i brevet vi skickade per e-post då vi frågade företagen om de kunde tänka sig att delta i undersökningen. Om vi fick tag på helt rätt personer i slutändan är dock svårt att veta.

Vitani A/S är den respondent som verkar beakta den personliga integriteten ur ett något bredare perspektiv än de andra. Först och främst fokuserar de på tekniska skydd som t.ex. decentraliserad lagring i form av smarta kort. Tekniska säkerhetsåtgärder är viktigt och finns med bland våra krav i uppsatsens teoretiska del. I samband med de smarta korten uttrycker Vitani A/S även att det är individen själv som administrerar över det smarta kortet. Detta utgör en del av kravet som gäller användarkontroll. Förutom detta gav de även en bild av att de tycker det är viktigt att få individen att känna sig trygg genom att informera denne om de olika biometriska säkerhetsfunktionerna. Att just informera slutanvändarna och upplysa dem om vad som kan orsaka problem med de biometriska säkerhetsfunktionerna har mycket med öppenhet att göra. Öppenhet var ett av de krav vi presenterade i den teoretiska delen, och som vi anser att man vid utveckling och användning bör beakta. Vidare nämner Vitani A/S även att deras biometriska säkerhetsfunktioner inte är kompatibla med de system som används av polisen vilket gör att användarnas fingeravtryck inte ska kunna utnyttjas av polisväsendet. Även detta tyder på att Vitani A/S ser på den personliga integriteten ur flera perspektiv då detta, utifrån vår teoretiska del, berör kravet på begränsad behandling.

Precise Biometrics fokuserar mer på det teknologiska, även om de i samband med detta får in andra aspekter. Dessutom gav Precise Biometrics, med hjälp av sin webbsida på Internet, ett mer uttömmande svar när det gäller det teknologiska skyddet för att beakta den personliga integriteten. I frågeformuläret tar de upp en särskild algoritm som de använder för matchningen. Vidare beskriver de hur de använder sig av smarta kort där en digital profil av fingeravtrycket lagras vilket gör att fingeravtrycket inte kan återskapas. De nämner här också att individen själv förfogar över vem han/hon vill dela med sig av informationen till. Här berör de således beaktandet av kravet som gäller användarkontroll. När de säger att den digitala profilen på det smarta kortet dessutom inte finns någon annanstans än just på det smarta kortet och inte lämnar det smarta kortet, kan man dra paralleller till kravet om begränsad behandling. Utöver de tekniska beaktandena nämner de vid ett tillfälle att det är viktigt att man redan från början tar hänsyn till individen. Bortsett från de tekniska beaktandena ges inte någon annan beskrivning av hur detta hänsynstagande skulle kunna gå till.

Den tredje respondenten, SAS, gav kortfattade svar vilket gör det en aning svårt att få en klar uppfattning över hur de beaktar den personliga integriteten. En aspekt som de dock tar upp är att det är viktigt att visa att det finns en seriös tanke bakom införandet av den biometriska säkerhetsfunktionen. Detta tolkar vi som

tillhörandes en del av kravet på att definiera syfte och varaktighet med den biometriska säkerhetsfunktionen. Det kravet handlar om att tydliggöra syftet för alla inblandade vilket vi anser vara ungefär samma sak som att visa att man har en seriös tanke bakom användningen av den biometriska säkerhetsfunktionen. Detta har även med kravet på öppenhet att göra, dvs. att man öppet visar och informerar syftet med den biometriska säkerhetsfunktionen.

Den helhetsbild vi får av dessa tre respondenters svar är att man vid utveckling och användning beaktar den personliga integriteten, men kanske inte ur så många perspektiv som man skulle önska. Vi hade självklart inte förväntat oss att respondenterna skulle besvara frågeformulären i detaljerad överensstämmelse med de krav vi tog upp i den teoretiska delen, men vi hade ändå hoppats att flera aspekter från den teoretiska delen skulle tas upp. Exempelvis finns en hel del som rör kravet om öppenhet att ta upp, även om två av respondenterna faktiskt berörde en del av det i sina svar. Vi hade även hoppats på att respondenterna i sina svar skulle nämna något om att man beaktar lagstiftning och riktlinjer i sin verksamhet. Vidare var det endast en av respondenterna som tog upp alla tre aspekter på de tekniska skyddsåtgärderna, dvs. digital profil, decentraliserad lagring, och kryptering.

Att fler aspekter i respondenternas svar inte fanns med kan dock bero på hur våra frågor var formulerade och hur själva undersökningen genomfördes. Dessutom är de allvarligaste hoten mot den personliga integriteten förknippade med identifiering där de biometriska uppgifterna lagras centralt i en databas. Vår empiriska undersökning är inriktad på verifiering eftersom de företag vi undersökte utvecklar respektive använder sådana biometriska säkerhetsfunktioner där de biometriska uppgifterna lagras på smarta kort. Att verifieringsfunktioner är mer kommersiellt gångbara än rena identifieringslösningar beror på att de senare kostar väldigt mycket [Fingerprint Cards 00]. Dessutom kan man anta att den personliga integriteten är en anledning till att det är just verifiering som fungerar kommersiellt och att det är det företag fokuserar på.

Det kan även vara så att företagen mycket väl beaktar den personliga integriteten på flera sätt som inte kommer fram i frågeformuläret. Så är antagligen fallet när det gäller SAS, som inte nämner någonting om tekniska skydd i form av t.ex. smarta kort, trots att det var smarta kort de utnyttjade vid testet av de biometriska säkerhetsfunktionerna. Att detta inte framkommer i svaren är dock förvånande. Flera av respondenterna nämner inte heller kryptering och digitala profiler, vilket också är något överraskande.

Trots att den här empiriska undersökningen blev något tunn, tror vi ändå att den kan ha betydelse för både biometribranschen och allmänheten som är de framtida användarna av biometriska säkerhetsfunktioner. Vi har med den här undersökningen försökt ge en antydning om hur medvetna företag är när det gäller den personliga integriteten, samt hur väl de tänkt igenom de olika aspekter som rör den personliga integriteten i samband med biometriska säkerhetsfunktioner. Att vår undersökning ger en antydning om att några av de företag som utvecklar respektive använder biometriska säkerhetsfunktioner ser på den personliga integriteten ur ett något ensidigt perspektiv, gör att man kan önska mer av dessa företag inom detta

område. Kanske kan detta få allmänheten i form av de framtida användarna att bli mer medvetna om dagens situation och kräva mer av biometribranschen i framtiden.

8.3 Förslag till vidare forskning

Då användningen av biometri för autentisering är en relativt ny företeelse men som verkar få ett allt bredare och mer omfattande tillämpningsområde, finns det mycket att forska och utreda kring ämnet. Av stor betydelse är problematiken kring hur individen och samhället kommer att påverkas av en bredare tillämpning av biometri. I den här uppsatsen har vi därför försökt att föra en diskussion kring problematiken kring personlig integritet i samband med tillämpningen av biometriska säkerhetsfunktioner för autentisering. Vi har avgränsat oss till att ta reda på hur den personliga integriteten kränks, och vilka krav man bör ställa på biometriska säkerhetsfunktioner, samt om, och hur, detta beaktas i praktiken. Med utgångspunkt i detta tror vi det finns kunskap och stoff för fortsatt forskning inom detta område.

I och med att vi i vår empiriska undersökning fick få svar och i slutändan inte lyckades utföra undersökningen på ett sätt som vi hade räknat med, tror vi att det skulle behöva forskas vidare kring detta. Med utgångspunkt i vår empiriska undersökning och vårt frågeformulär tror vi att man skulle behöva förändra tillvägagångssättet för att verkligen få reda på allt det man vill ha reda på. Kanske är det nödvändigt med personliga intervjuer eller deltagande observationer för att få en ordentlig förståelse för, om, och på vilka sätt, man vid utveckling och användning av biometriska säkerhetsfunktioner beaktar den personliga integriteten. Ett sådant tillvägagångssätt tror vi skulle vara intressant att gå vidare med inom detta område. Framförallt skulle en större undersökning behöva göras där man undersöker ett större antal respondenter.

En aspekt som ligger förhållandevis nära vår studie kring hur man vid utveckling och användning beaktar den personliga integriteten, är hur väl informerade försäljare av biometriska säkerhetsfunktioner är och hur tillräckligt kunniga de är för att kunna svara på kunders frågor om den personliga integriteten. Cavoukian [99] nämner en undersökning i Kanada där syftet var att kartlägga medvetenheten och kunskapen kring lagar som rör den personliga integriteten hos försäljare samt hur väl de tillämpade och använde dessa när de bemötte kunder. Resultaten visade på att anställda i de flesta företag hade låg medvetenhet kring detta och var dåliga på att utnyttja lagar, skydd och principer som finns för att värna om den personliga integriteten. En sådan undersökning skulle man även kunna göra i Sverige för att ta reda på hur väl informerade de som ska möta kunderna här i Sverige, är. Detta skulle vara särskilt intressant med tanke på att ingen av våra respondenter ens nämner lagar och riktlinjer som finns för att underlätta beaktandet av den personliga integriteten.

Referenser

Böcker

- [Bonniers 02] Bonniers Svenska Ordbok, Albert Bonniers Förlag AB, 2002
- [Dahmström 00] Dahmström, Karin, "Från datainsamling till rapport – att göra en statistisk undersökning", Studentlitteratur AB, 2000
- [Gollman 99] Gollman, Dieter, "Computer Security", John Wiley & Sons Ltd, 1999
- [Halvarsson et al 00] Halvarsson, Andreas, Morin, Tommy, "Elektroniska signaturer – E-affärer utan elände med identifiering, signering och kryptering", Studentlitteratur AB, 2000
- [Holme et al 97] Holme, Idar Magne, Krohn Solvang, Bernt, "Forskningsmetodik - om kvalitativa och kvantitativa metoder", Studentlitteratur, 1997
- [ITS 94] ITS Rapport 6, "Terminologi för Informationssäkerhet", 1994
- [NE 91a] Nationalencyklopedin, Band 6, Bokförlaget Bra Böcker AB, 1991
- [NE 94b] Nationalencyklopedin, Band 15, Bokförlaget Bra Böcker AB, 1991
- [Ström 03] Ström, Pär, "Övervakad – elektroniska fotspår och snorkarsamhället", Liber AB, 2003
- [Woodward et al 03] Woodward Jr., John D., Orlans, Nicholas M., Higgins, Peter T., "Biometrics", McGraw-Hill/Osborne, 2003

Internet

- [ARBDOK 03] Arbetsgruppen för dataskydd, "Arbetsdokument om biometri", 2003, <http://www.europa.eu.int/comm/privacy>, hämtad 2004-01-26
- [BioPrivacy 1] BioPrivacy, "FAQ's and Definitions", http://www.bioprivacy.org/faq_main.htm, hämtad 2003-12-06

- [BioPrivacy 2] BioPrivacy, "Mission and Methodology", <http://www.bioprivacy.org/mission.htm>, hämtad 2004-03-22
- [Bornholmstrafikken] Bornholmstrafikken, <http://www.bornholmstrafikken.dk>, hämtad 2004-09-10
- [Bjurman 03] Bjurman, Torun, "Storebror större hot än någonsin", 2003, http://www.idg.se/ArticlePages/200310/17/20031017160723_CS/20031017160723_CS.dbp.asp, hämtad 2004-01-26
- [Cavoukian 99] Cavoukian, Ann, "Consumer Biometric Applications: A Discussion Paper", September 1999, <http://www.ipc.on.ca/docs/cons-bio.pdf>, hämtad 2004-04-30
- [CC 1] Common Criteria Biometric Evaluation Methodology Working Group, "Common Criteria: Common Methodology for Information Technology Security Evaluation: Biometric Evaluation Methodology Supplement", version 1.0, augusti 2002, http://www.cesg.gov.uk/site/ast/biometrics/media/BE_M_10.pdf, hämtad 2004-06-09
- [CC 2] Common Criteria, Common Criteria for Information Technology Security Evaluation, "Part 1: Introduction and general model", version 2.1, augusti 1999, <http://csrc.nist.gov/cc/Documents/CC%20v2.1/p1-v21.pdf>, hämtad 2004-06-09
- [Collste 97] Collste, Göran, "Personlig integritet, bilaga 4 i SOU 1997:39, 1997, <http://www.regeringen.se/content/1/c4/13/35/a0d1fdcc.pdf>, hämtad 2004-06-10
- [Crompton 02a] Crompton, Malcolm, "Biometrics and privacy - the end of the world as we know it or the white knight of privacy?", 2002, <http://www.biometricsinstitute.org/bi/cromptonspeech.htm>, hämtad 2004-01-26
- [Crompton 02b] Crompton, Malcolm, "Under the Gaze, Privacy Identity and New Technology", 2002, <http://www.privacy.gov.au/news/speeches/sp104notes.pdf>, hämtad 2004-06-10
- [DI 1] Datainspektionen, "Kroppen som nyckel", Magazin Direkt, nr 3/2003, <http://www.datainspektionen.se/pdf/direkt/03-3-pdf>, hämtad 2004-01-26

- <http://www.research.ibm.com/ecvg/pubs/sharat-forensic.pdf>, hämtad 2004-03-03
- [Jain et al 01c] Jain, Anil, Ross, Arun, Prabhakar, Salil, "Fingerprint Matching Using Minutiae and Texture Features", 2001, <http://biometrics.cse.msu.edu/RossMinTextureCIP01.pdf>, hämtad 2004-08-05
- [Laurant 03] Laurant, Cedric, "Privacy and human rights 2003: An international survey of privacy laws and developments", 5 september 2003, <http://www.privacyinternational.org/survey/phr2003/>, hämtad 2004-06-08
- [Maltoni et al 03] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S., "Handbook of fingerprint recognition", 2003, http://bias.csr.unibo.it/maltoni/handbook/chapter_1.pdf, hämtad 2004-02-10
- [Nilsson 97] Nilsson, Per, "Biometriska identifikations- och autentiseringsmetoder", 1997, <http://hemsidor.torget.se/users/g/godis1/cut/uppsats/Biometri.htm>, hämtad 2004-01-26
- [Norlin 04] Norlin, Arne, "USA tvingar fram nya svenska pass nästa år", Aftonbladet 2004-02-22, <http://www.aftonbladet.se/vss/resor/story/0,2789,436805,00.html>, hämtad 2004-06-08
- [Prabhakar et al 03] Prabhakar, Salil, Pankanti, Sharath, Jain, Anil K., "Biometric Recognition: Security and Privacy Concerns", mars/april 2003, <http://biometrics.cse.msu.edu/j2033.pdf>, hämtad 2004-03-28
- [Precise Biometrics] Precise Biometrics, <http://www.precisebiometrics.com>, hämtad 2004-09-10
- [Precise Biometrics 03] Precise Biometrics, 2003, <http://www.precisebiometrics.com/data/content/DOCUMENTS/2003425124915434Bornholmstrafikken.pdf>, hämtad 2004-09-10
- [PUL] Personuppgiftslagen (1998:204), 1998, <http://www.notisum.se/rnp/sls/lag/19980204.HTM>, hämtad 2004-06-08
- [Rosengren-Edgren 04] E-postsvar från Rosengren-Edgren, Charlotte, Scandinavian Airlines System, 6 september 2004, se Bilaga 3

- [SAS 03] Scandinavian Airlines System, "Scandinavian Airlines kundtestar biometri", 2003, http://www.scandinavian.net/EC/Apl/Home/Front-Door/0,3479,SO%253DD77C12686B9946_8F4E010C792FFA5E%2526MKT%253DFI,00.html, hämtad 2004-09-10
- [SOU 97] Justitiedepartement, "Integritet, offentlighet, informationsteknik", SOU 1997:39, 1997, <http://www.regeringen.se/content/1/c4/13/35/a0d1fdcc.pdf>, hämtad 2004-06-10
- [Tomko 98] Dr. Tomko, Georg, "Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy?", 15 september 1998, <http://www.dss.state.ct.us/digital/tomko.html>, hämtad 2004-03-17
- [Vitani A/S 03] Vitani A/S, 2003, <http://www.vitani.dk>, hämtad 2004-04-12

Bilagor

Bilaga 1: Definitioner

Autenticering	Metod som möjliggör verifiering och/eller identifiering för att kontrollera en uppgiven identitet.
Bakdörr	Funktion i ett system som kan utnyttjas till att gå förbi normala kontroller vid systemets användning och som därvid t.ex. kan åsidosätta säkerhetsskyddet.
Bedräglig aktör	En person som har onda avsikter och är ute efter att t.ex. skada, utnyttja, komma över eller stjäla information.
Biometrisk egenskap	Fysiologiskt eller beteendemässigt särdrag som kan mätas och användas för autenticering.
Biometrisk säkerhetsfunktion	Ett system som autentiserar en individ genom dennes fysiologiska eller beteendemässiga särdrag.
Biometrisk uppgift	Fysiologiskt eller beteendemässigt särdrag som mäts och behandlas i en biometrisk säkerhetsfunktion för autenticering.
Common Criteria	En standard för säkerhetsevaluering av IT-produkter och IT-system.
Dermatologi	Läran om huden och dess sjukdomar.
Digital profil	En strukturerad förminskning av en biometrisk egenskap i form av ett numeriskt resultat som beräknas utifrån de unika biometriska uppgifterna.
Digital signering	Omvandling av information (eller ett resulterande värde av informationen från en hash-funktion) på ett sätt som endast avsändaren kan utföra och som tillåter mottagaren att kontrollera meddelandets äkthet, innehåll och avsändarens identitet.
Enrollering	Registrering av en individ genom att biometriska egenskaper samlas in och extraheras för att upprätta en digital profil av individen.

En-mot-en-jämförelse	Ett matchningsförsök där en inkommande biometrisk egenskap endast jämförs med en lagrad referens. Sker vid verifiering.
En-mot-många-jämförelse	Flera matchningsförsök där en inkommande biometrisk egenskap jämförs med flera andra individers referenser som finns lagrade i en databas. Sker vid identifiering.
Extrahering	Process som fångar upp unika och karaktäristiska uppgifter ifrån den biometriska egenskapen.
FAR (False Acceptation Rate)	Fel som kan uppstå vid matchningen av två biometriska uppgifter i en biometrisk säkerhetsfunktion. Innebär att biometriska uppgifter från två olika individer misstas att komma från samma individ, sk. falsk acceptans.
FRR (False Rejection Rate)	Fel som kan uppstå vid matchningen av två biometriska uppgifter i en biometrisk säkerhetsfunktion. Innebär att den biometriska säkerhetsfunktionen misstar två biometriska uppgifter från samma individ att komma från två olika individer, sk. falskt avslag.
Gränsvärde	Ett värde som bestämmer hur väl två biometriska uppgifter måste stämma överens för att utgöra ett matchande par.
Hashfunktion	Matematisk funktion som avbildar värden från en mängd av godtyckligt långa datasträngar till en mängd bestående av kortare datasträngar med fast längd, sk. hashsummer. Det ska vara beräkningsmässigt mycket svårt eller tidsödande att konstruera två datasträngar som ger samma hashsummer.
Identifiering	Fastställande av en identitet genom att besvara frågan "Vem är jag?". Detta görs genom en-till-många-jämförelse där den biometriska säkerhetsfunktionen skiljer en individ från övriga individer vars biometriska uppgifter också finns lagrade.
Kryptering	Omvandling av klartext till kryptotext med hjälp av ett kryptosystem och aktuell krypto-

	nyckel i syfte att förhindra obehörig åtkomst av konfidentiell information.
Krypteringsnyckel	Varierbar information som styr en krypteringsalgoritms omvandling av klartext till kryptotext och/eller omvänt.
Matchning	Jämförelse mellan en inkommande biometrisk egenskap och en lagrad biometrisk uppgift i form av en digital profil (referens) för att avgöra om de tillhör samma individ eller inte.
Offentlighetsprincipen	Grundläggande princip för svensk rättskipning och offentlig förvaltning. Den har flera beståndsdelar varav en är ”Allmänna handlingars offentlighet”.
Personlig integritet	Med personlig integritet menas individens möjlighet att bli lämnad ifred och få vara anonym. Dessutom handlar personlig integritet även om att inte få sin värdighet kränkt. Vidare ska individen själv få kontrollera och bestämma över sitt handlande och över sina personliga uppgifter. Dessutom innebär personlig integritet att insyn, användning och kvalitet hos de personliga uppgifterna ska skyddas.
PKI	Står för Public Key Infrastructure och är en teknik för att utföra grundfunktionerna elektronisk identifiering, elektronisk signering och kryptering. PKI är en asymmetrisk krypteringsteknik där ett nyckelpar genereras, en publik och en privat nyckel.
Privat nyckel	Hemlig nyckel i ett asymmetriskt kryptosystem. Används vid elektronisk identifiering, elektronisk signering och kryptering för att omvandla klartext till kryptotext och/eller omvänt.
Referens	En lagrad biometrisk uppgift i form av en digital profil som inkommande biometriska egenskaper jämförs med. Detta för att avgöra om den inkommande biometriska egenskapen och referensen tillhör samma individ.

Registeransvarig	Den individ som i en verksamhet på ett företag är ansvarig för användningen av den biometriska säkerhetsfunktionen.
Smart kort	Kort utrustat med en eller flera integrerade kretsar inkluderande komponenter för lagring och bearbetning av data. Används t.ex. för att lagra och behandla biometriska uppgifter i autentiseringssyfte.
Unik identifierare	Fastställt nummer eller värde som är associerat med en specifik individ. Ett exempel på en unik identifierare är personnummer.
Verifiering	Fastställande av riktigheten av en uppgiven identitet. Besvarar frågan "Är jag den jag utger mig för att vara?" genom att göra en-till-en-jämförelse. Det innebär att den biometriska säkerhetsfunktionen bekräftar eller förnekar en individs identitet genom att behandla den biometriska uppgiften tillhörandes den individen.

Bilaga 2: Frågeformulär

Frågeformulär utveckling (svensk version)

FRÅGEFORMULÄR – Biometri och personlig integritet

Detta frågeformulär är en del av vår magisteruppsats som skrivs för Data- och Systemvetenskapliga institutionen, DSV, vid Stockholms Universitet. Syftet med uppsatsen är att undersöka hur den personliga integriteten beaktas vid utveckling och användning av biometriska system för autentisering. Detta frågeformulär vänder sig därför till dem som utvecklar samt använder biometriska system för autentisering. Frågeformuläret består av 7 frågor. De flesta frågor är av öppen karaktär, dvs. inga svarsalternativ ges utan Ni får svara fritt och skriva så mycket Ni anser Er behöva för att svara på frågan.

Om Ni undrar över något som rör uppsatsen eller frågeformuläret kan Ni kontakta oss per e-post.

TACK FÖR DIN MEDVERKAN!

Karin Jansson, karin-ja@fc.dsv.su.se
Veronica Wahrman, vero-wah@fc.dsv.su.se

Med personlig integritet menas individens möjlighet att bli lämnad ifred och få vara anonym. Personlig integritet handlar också om att inte få sin värdighet kränkt. Vidare ska individen själv få kontrollera och bestämma över sitt handlande och över uppgifter om sig själv. Dessutom innebär personlig integritet att insyn, användning och kvalitet hos de personliga uppgifterna som individen utlämnat om sig ska skyddas. Med kränkning av den personliga integriteten menas att en eller flera av delarna ovan inte är uppfylld.

1. Vilket företag representerar Du?
2. Vilken befattning har Du inom företaget?
3. Får vi nämna företaget i samband med presentationen av den här undersökningen? (Ja/Nej)
4. Hur beaktar Ni användarens personliga integritet vid utveckling av biometriska system för autentisering?
5.
 - a) Har Ni en utarbetad policy innehållande rutiner för utvecklingen av de biometriska systemen vid autentisering, så att de vid nyttjandet inte kränker den personliga integriteten? (Ja/Nej)
 - b) Om ja, vilka punkter innehåller den?
 - c) Om nej, skulle en sådan underlätta arbetet med att utveckla biometriska system för autentisering som beaktar den personliga integriteten vid nyttjandet av de biometriska systemen?
6.
 - a) Upplever Ni att tänkta användare av biometriska system för autentisering är angelägna om sin personliga integritet i samband med dessa? (Ja/Nej)
 - b) Om ja, hur tillmötesgår Ni dessa personer och deras eventuella oro och önskemål som kan uppstå kring den personliga integriteten?
7. Vilken typ av stöd, t.ex. kundsupport och service, erbjuder Ni kunderna, efter leverans, för att de ska kunna värna den personliga integriteten vid nyttjande av biometriska system för autentisering?

Frågeformulär utveckling (engelsk version)

QUESTIONNAIRE – Biometrics and privacy

This questionnaire is a part of our master's thesis that is written for the Computer- and System science department, DSV, at the university of Stockholm. The purpose of the thesis is to examine how privacy is handled when developing and using biometric authentication systems. This questionnaire therefore turns to those who develop and use biometric authentication systems. The questionnaire consists of 7 questions. Most of them are of open character, which means that there aren't any given answer alternatives. Instead You are supposed to answer freely and write as much as You think You need to answer the question.

If You have any questions concerning our thesis or the questionnaire You are welcome to contact us by e-mail.

THANK YOU FOR YOUR PARTICIPATION!

Karin Jansson, karin-ja@fc.dsv.su.se
Veronica Wahrman, vero-wah@fc.dsv.su.se

In this questionnaire the definition of privacy is an individual's right to be left alone and to remain anonymous. Privacy also means not offending one's dignity. Further more, an individual is supposed to be in control of and be in charge of her acting and personal information herself. Moreover, privacy means that insight, the use of, and quality of the personal information that an individual has omitted should be protected. If one part or more of the definition above isn't fulfilled, an invasion of privacy has taken place.

1. Which company do You represent?
2. What is Your position at the company that You represent?
3. May we mention Your company in the presentation of the results? (Yes/No)
4. How do You take the individual's privacy into consideration when developing biometric authentication system?
5.
 - a) Do You have a prepared policy consisting routines for the development of biometric authentication systems, so that the use of them will not cause an invasion of privacy? (Yes/No)
 - b) If yes, what parts does the policy consist of?
 - c) If no, would such a policy facilitate the development of biometric authentication systems that will not cause an invasion of privacy when using them?
6.
 - a) Do You experience that the prospective users of the biometric authentication systems are keen on their privacy? (Yes/No)
 - b) If yes, how do You comply with those people and their worries and requirements that may arise concerning their privacy?
7. What kind of support, for example customer support and service, do You offer Your customers, after delivery, so that they can protect their privacy when using the biometric authentication systems?

Frågeformulär användning (svensk version)

FRÅGEFORMULÄR – Biometri och personlig integritet

Detta frågeformulär är en del av vår magisteruppsats som skrivs för Data- och Systemvetenskapliga institutionen, DSV, vid Stockholms Universitet. Syftet med uppsatsen är att undersöka hur den personliga integriteten beaktas vid utveckling och användning av biometriska system för autentisering. Detta frågeformulär vänder sig därför till dem som utvecklar samt använder biometriska system för autentisering. Frågeformuläret består av 6 frågor. Samtliga frågor är av öppen karaktär, dvs. inga svarsalternativ ges utan Ni får svara fritt och skriva så mycket Ni anser Er behöva för att svara på frågan.

Om Ni undrar över något som rör uppsatsen eller frågeformuläret kan Ni kontakta oss per e-post.

TACK FÖR DIN MEDVERKAN!

Karin Jansson, karin-ja@fc.dsv.su.se
Veronica Wahrman, vero-wah@fc.dsv.su.se

Med personlig integritet menas individens möjlighet att bli lämnad ifred och få vara anonym. Personlig integritet handlar också om att inte få sin värdighet kränkt. Vidare ska individen själv få kontrollera och bestämma över sitt handlande och över uppgifter om sig själv. Dessutom innebär personlig integritet att insyn, användning och kvalitet hos de personliga uppgifterna som individen utlämnat om sig ska skyddas. Med kränkning av den personliga integriteten menas att en eller flera av delarna ovan inte är uppfylld.

1. Vilken organisation representerar Du?
2. Vilken befattning har Du inom organisationen?
3. Får vi nämna organisationen Du företräder i samband med presentationen av den här undersökningen? (Ja/Nej)
4. Hur beaktar Ni den personliga integriteten när användarna nyttjar de biometriska systemen för autentisering?
5.
 - a) Har Ni en utarbetad policy innehållande rutiner för hur den personliga integriteten ska kunna skyddas vid nyttjandet av de biometriska systemen för autentisering? (Ja/Nej)
 - b) Om ja, vilka punkter innehåller den?
 - c) Om nej, skulle en sådan underlätta beaktandet av användarnas personliga integritet vid nyttjandet av de biometriska systemen för autentisering?
6.
 - a) Upplever Ni att användarna av de biometriska systemen för autentisering är angelägna om sin personliga integritet i samband med nyttjandet av dessa? (Ja/Nej)
 - b) Om ja, hur tillmötesgår Ni de önskemål som uppkommer kring den personliga integriteten?

Frågeformulär användning (engelsk version)

QUESTIONNAIRE – Biometrics and privacy

This questionnaire is a part of our master's thesis that is written for the Computer- and System science department, DSV, at the university of Stockholm. The purpose of the thesis is to examine how privacy is handled when developing and using biometric authentication systems. This questionnaire therefore turns to those who develop and use biometric authentication systems. The questionnaire consists of 6 questions. Most of them are of open character, which means that there aren't any given answer alternatives. Instead You are supposed to answer freely and write as much as You think You need to answer the question.

If You have any questions concerning our thesis or the questionnaire You are welcome to contact us by e-mail.

THANK YOU FOR YOUR PARTICIPATION!

Karin Jansson, karin-ja@fc.dsv.su.se
Veronica Wahrman, vero-wah@fc.dsv.su.se

In this questionnaire the definition of privacy is an individual's right to be left alone and to remain anonymous. Privacy also means not offending one's dignity. Further more, an individual is supposed to be in control of and be in charge of her acting and personal information herself. Moreover, privacy means that insight, the use of, and quality of the personal information that an individual has omitted should be protected. If one part or more of the definition above isn't fulfilled, an invasion of privacy has taken place.

1. Which company do You represent?
2. What is Your position at the company that You represent?
3. May we mention Your company in the presentation of the results? (Yes/No)
4. How do You take the individual's privacy into consideration when using the biometric authentication system?
5.
 - a) Do You have a prepared policy of consisting routines concerning the use of biometric authentication systems, so that they will not cause an invasion of privacy? (Yes/No)
 - b) If yes, what parts does the policy consist of?
 - c) If no, would such a policy facilitate to take the individual's privacy into consideration when using the biometric authentication systems?
6.
 - a) Do You experience that the users of the biometric authentication systems are keen on their privacy? (Yes/No)
 - b) If yes, how do You comply with the requirements that may arise concerning their privacy?

Bilaga 3: E-postsvar från Charlotte Rosengren-Edgren, SAS

Måndag, September 6, 2004, em +0100
Från: Charlotte.Rosengren-Edgren@sas.se
Ärende: RE: FW: Magisteruppsats om biometri
Till: Karin Jansson
Bilagor: Attach0.html 14K

Hej igen,
lite kort om testet i Umeå,

testet pågick mellan Nov-03 och Mar-04, dvs 6 mån och vi gjorde en uppdelning så att den första delen av perioden testades fingeravtryck och den senare delen användes till Irisigenkänning. Hela testen skedde i Umeå trots att vi hade som ursprunglig tanke att låta två flygplatser vara med i testen, anledning till detta beslut var att infrastrukturen inte var redo för test på den andra flygplatsen. Registreringen av både finger och iris skedde samtidigt, dvs passagerarna gjorde bara ett besök vid registreringsstationen och bägge avtrycken sparades på "kortet" vilket innebar att det blev enkelt att byta läsarutrustning från finger till iris. Utvärdering av resultatet från testen finns här hos mig på SAS och jag delar gärna med mig av vad som kom ut av testen, hör gärna av Er om Ni vill veta mer!

Vänliga Hälsningar
Charlotte

-----Original Message-----

From: Karin Jansson [<mailto:karin-ja@fc.dsv.su.se>]
Sent: Monday, September 06, 2004 1:18 PM
To: Charlotte.Rosengren-Edgren@sas.se
Subject: Re: FW: Magisteruppsats om biometri

Hej!

Imorgon, tisdag, kommer vi att via mail skicka frågeformuläret till dig angående hur ni beaktar den personliga integriteten vid nyttjande av biometriska system. Frågeformuläret består av 6 st frågor. Du svarar på frågorna genom att besvara mailet och sedan skicka tillbaka det till oss. Precis som ett vanligt mail.

Vi undrar också om du skulle kunna säga några ord om testet ni utfört? När påbörjades testet? Och när avslutades det? Eller håller det på än? Vi har läst att ni vid Umeå flygplats testat fingeravtryck och vid annan flygplats iris. Stämmer det, eller har ni vid respektive flygplats testat både fingeravtryck och iris? Du kan svara på dessa frågor genom att besvara detta mail. Hoppas detta inte är till besvär för dig.

Med vänliga hälsningar

Karin Jansson, karin-ja@fc.dsv.su.se
Veronica Wahrman, vero-wah@fc.dsv.su.se