TDDC03 Informationssäkerhet, projekt
Vt 2005

Biometri i svenska pass

Boris Asadanin
Klara Lundgren

Handledare: Kristin Anderson

Sammanfattning

Den 1:a oktober 2005 inför Sverige ett nytt pass. Passet ska ha ett kontaktlöst chip av typen RFID och innehålla biometriskt underlag i form av ett digitalt ansiktsfoto. Informationen kommer inte att vara krypterad men kommer ändå att skyddas med passiv autentisering med PKI för att säkra att informationen inte har ändrats sedan utfärdandet. Passet anses på detta sätt bli säkrare eftersom informationen sparad på chipet ska vara svårare att förfalska och bandet mellan person och pass blir starkare.

Det finns dock både fördelar och nackdelar med det nya passet. Säkerheten blir bättre, men integritets-förespråkarna får betala ett högre pris. Om människor dessutom fås att lita på att passet är säkrare än vad det är, så kan följden bli att identitetsstölderna blir allvarligare. Vi ser samtidigt diskussioner om att i framtiden införa nya biometrier eller till och med skapa en central databas med människors information och biometriska underlag.

1. Inledning

Den svenska regeringen antog nyligen en proposition som innebär att biometri ska införas i svenska pass den 1:a oktober 2005. Vad var det egentligen som ledde fram till detta beslut? Sedan attackerna mot USA den 11:e september 2001, har landet vidtagit många åtgärder för att höja känslan av säkerhet mot hotet utifrån. En av de åtgärderna innebär att de vid gränskontrollerna tar både fingeravtryck och ansiktsbild av samtliga inresande i landet. I dagens informationssamhälle är det naturliga steget att genom ytterligare datorisering effektivisera processen. För visumfria resor in i landet har USA därmed ställt krav på att biometri ska finnas i passen. Även om USA har varit drivande i frågan verkar viljan att vidta åtgärder för att höja säkerheten i pass finnas även i stora delar av övriga världen, inklusive Sverige. Syftet med denna rapport är att utreda vad beslutsfattare har sagt om den praktiska implementeringen samt att identifiera de problem som uppkommer.

1.1. Problemformulering

Följande frågeställningar har identifierats som intressanta för denna rapport:

- Vilka beslut har tagits rörande införsel av biometri i svenska pass och vilka internationella påtryckningar har lett fram till dessa?
- Hur ska biometri i pass implementeras?
- Vad kan vi se för säkerhetsproblem, för- och nackdelar?

1.2. Avgränsningar

Vi har valt att koncentrera oss på de diskussioner och bestämmelser som rör Sveriges införsel av de nya passen. Detta innebär dock inte att det enbart är svenska rapporter som är relevanta, då Sverige även är styrt av internationella krav och specifikationer. Exempelvis är rekommendationerna från FN-organet International Civil Aviation Organisation (ICAO) av stor vikt eftersom Sverige har valt att följa dessa. Då det gäller olika biometrier och lagringsmedier så ligger fokus enbart på dem som har diskuterats i beslut. När det gäller biometri så innebär detta alltså att främst ansiktsjämförelse behandlas, men även fingeravtryck och iris kan komma att kort benämnas.

1.3. Klargöranden

I detta stycke görs vissa klargöranden för att läsaren bättre ska kunna följa med och förstå följande text. Nedan förklaras några begrepp.

1.3.1. Verifiering och identifiering

Läsaren behöver kunna skilja på identifiering och verifiering. Vid en identifiering är uppgiften att ta reda på vem någon är. Vid verifiering gäller det istället att verifiera påstådd identitet. Identifiering ställer alltså frågan: Vem är du? Verifiering ställer istället frågan: Är du den du utger dig för att vara?

Detta spelar stor roll eftersom metoderna för att verifiera och identifiera skiljer sig. Vid en verifiering matchas till exempel ett ansikte med en ansiktsbild. Det görs en så kallad en mot en-jämförelse. För identifiering görs istället en en till många-jämförelse eftersom ett ansikte ska jämföras med många ansikts-bilder. Detta kräver en databas med många ansikts-bilder. Ett praktiskt exempel på detta är kriminal-enhetens arbete med att identifiera brottslingar på en brottsplats.

1.3.2. Biometriska metoder

Det är stor skillnad mellan att lagra biometrisk data och att använda sig av biometriska metoder för att identifiera eller verifiera en identitet. Som vi senare kommer att gå igenom så är det för närvarande olagligt i Sverige att lagra biometrisk data. Däremot är det fullt lagligt att använda sig av biometri för att fastställa en identitet. För att få bättre förståelse för detta förklaras här kortfattat hur biometri fungerar. Ansiktsprop-ortioner tas som biometriskt exempel.

För att skapa ett foto lämpligt för biometriskt underlag tas några foton på personen i fråga och en dator får räkna ut avstånden mellan olika punkter i ansiktet som t.ex. näsa, ögon och öron. Avstånden utgör personens biometriska data för ansiktet och är alltså rådata. I svenska pass får inte denna typ av data lagras. Däremot får bilden lagras i passet och vid en

passkontroll kan ett nytaget foto av resenären jämföras med det lagrade fotot. Biometriskt görs detta genom att ta fram biometrisk data från bilderna och jämföra.

I texten nedan kommer begreppen ”biometriskt underlag” och ”biometrisk data” att användas, där underlaget är i form av bilder som biometrisk data kan tas fram ur.

2. Bakgrund

Det första som bör utredas är vad som ledde fram till att säkerheten i pass ansågs behöva höjas genom införsel av biometri. I följande kapitel presenteras huvudaktörerna och de beslut, rekommendationer och kommentarer som de har bidragit med.

2.1. Vad startade allt?

Enligt en proposition från den svenska regeringen om ökad säkerhet i pass [1] har säkerhetsfrågor när det gäller pass och andra resehandlingar blivit alltmer aktuella under senare år. Propositionen talar vidare om att förfalskningar och missbruk av pass och andra resehandlingar utgör ett allvarligt problem, både internationellt och nationellt. Därför pågår ett intensivt internationellt arbete för att komma till rätta med dessa problem.

USA visade sig vara mest drivande i denna fråga när de i maj 2002 beslutade om nya bestämmelser med krav för dem som vill resa in i landet utan visum. De nya kraven innebär att fr.o.m. den 26:e oktober 2004 ska passen ha ett kontaktlöst chip med ”biometrisk säkring”. Denna biometriska säkring ska följa rekommendationer från FN-organet International Civil Aviation Organisation (ICAO). [2] Den 22:a maj 2003 antog ICAO en rekommendation att införa biometri i resehandlingar. Ansiktsjämförelse ska användas som minimistandard, medan avläsning av fingeravtryck eller iris rekommenderas som frivilligt komplement. [1]

Även om USA är mest drivande i frågan så verkar alltså övriga länder inom FN tycka att det finns ett behov av att höja säkerheten i passen genom att införa biometri. Sverige vill också vara med i den nya utvecklingen och i oktober 2003 fick Rikspolisstyrelsen (RPS) i uppdrag av regeringen att förbereda bl.a. så att biometriskt underlag ska kunna lagras i pass. [1]

2.2. Vad har beslutats?

För Europa och Sverige beslutades det definitivt om biometri i pass först den 13:e december 2004 då Europeiska rådet antog en förordning om pass och resedokument. Denna innebär i korthet att inom 18 månader från att de tekniska specifikationerna antagits ska ansiktsbilden lagras elektroniskt i dokument och inom 36 månader ska även innehavarens fingeravtryck lagras. Detta gäller pass med giltighetstid på mer än 12 månader och uppgifterna ska bara finnas i själva dokumenten. [1]

Eftersom införsel av biometri i pass innebär automatiserad behandling av personuppgifter och eventuell lagring av dessa uppgifter kan det vara värt att nämna att Datainspektionen följer utvecklingen. Exempelvis har de i ett yttrande [3] angående lagrådsremiss ”Ökad säkerhet i pass” [4] påpekat att det saknas en analys av hur principerna i personuppgiftslagen och dataskyddsdirektivet beaktas. Särskilt nämns kraven på säkerhet och information till den registrerade.

Sverige följde Europeiska rådets linje när regeringen den 10 mars 2005 beslutade om en proposition som innebär att svenska pass ska förses med biometriskt underlag. Det biometriska underlaget är en ansiktsbild i digitalt format. Samma uppgifter som finns på passets personsida lagras också. [1] Datainspektionens invändningar bemöts speciellt genom att propositionen påpekar att ansiktsbilden enbart lagras i passet, som den registrerade själv har hand om. Biometriska data och ansiktsbilder som används för kontroll ska genast förstöras efter kontrollen. Dessutom får inte ansiktsbilder och biometriska data användas vid sökning efter uppgifter. [1] Lagen träder i kraft den 1:a oktober 2005. Observera dock att dessa lagar gäller endast i Sverige. I andra länder är det fullt möjligt att den biometriska datan eller underlaget sparas. Ett exempel är USA där detta sedan ett tag görs. Pass som har utfärdats före detta datum kommer fortsätta att gälla som vanligt till ordinarie förfallodatum.

Utöver ansiktsbild kommer även bild av fingeravtryck att lagras i passen i framtiden. EU ställer krav på att medlemsländerna ska ha infört fingeravtryck i sina pass före 31:a december 2007. Datum för införandet i svenska pass är ännu inte bestämt. [5]

3. Implementering

För att kunna föra en diskussion om säkerhetsaspekterna av biometri i pass behövs en grundlig genomgång om vad införseln egentligen innebär. I detta kapitel presenteras den avsedda strukturen för både själva passen och organisationen runtomkring.

3.1. Pass

Då de nya passen är en internationell fråga har väldigt många människor också fått lägga fram sina önskemål och krav i frågan. De drivande ländernas grundtanke för de nya passen är att göra resehandlingarna svårare att förfalska och därmed förebygga terrorism eller annan kriminell verksamhet. FN-organet ICAO har sammanställt en teknisk rapport [6] där önskemål och krav för maskinellt avläsbara pass sammanställs. Ett av de viktigaste kraven är att passen ska kunna lagra biometriskt underlag. Detta görs elektroniskt och därför kommer de nya passen att behöva förses med ett chip. Andra önskemål rör

exempelvis kontaktlös avläsning av chip och sänkt giltighetstid för passen. Enligt svenska polisens hemsida [7] så ska det nya passet följa ICAOs rekommendationer.

Nedan skiljer vi på strukturen i passet och det chip som ska placeras i det. Dessa ges en utförlig beskrivning separat.

3.1.1. Struktur

Passen kommer att vara nästan likadana och innehålla samma information som tidigare så när som på ett chip som beskrivs närmare i nästa avsnitt. ICAO har gett olika förslag på var i passet chipet ska placeras. [6] De tre viktigaste förslagen är i persondatasidan, i mitten av passet eller mellan det sista pappret och omslaget. Ur säkerhetssynvinkel har alla förslagen olika för- och nackdelar. T.ex. har lagring av chipet i datasidan fördelen att all information ligger samlat och att materialet i datasidan är lämpligt för integrering av ett chip. Nackdelen blir att en förfalskare bara behöver manipulera en sida, till skillnad från om chip och persondata separeras. Vilken implementering som är vald för de svenska passen vet vi inte i skrivande stund. För att indikera att passet innehåller ett datachip ska de svenska passen ha en av ICAO rekommenderad symbol [6] på framsidan. Bilder på symbolen och placeringen av den finns i bilaga 1.

En skillnad mellan de gamla och nya passen är att ansiktsbilden behöver vara densamma som den som lagras i chipet. Detta medför att bilden kommer att vara digital och att den måste tas hos polisen, eftersom de av säkerhetsskäl är de enda som kan skriva till chipet. Resten av uppgifterna är desamma. De maskinläsbara raderna i underkanten av passets personsida kommer också att vara kvar.

3.1.2. Chip

Chipet är den mest intressanta delen av den nya typen av pass och resehandlingar. Det är här som det nya passet väsentligt kommer att skilja sig från dagens pass. Framförallt har det handlat om vad som behövs för att kunna lagra biometriskt underlag i passet. Andra frågor har rört vilken information som ska lagras på chipet och vilka säkerhetsmetoder som ska användas för att skydda informationen.

Chipet är av typen RFID som står för Radio Frequency IDentificaion. Precis som namnet antyder bygger tekniken på radiovågor. Dessa har fördelen att kunna färdas genom kläder, väskor och dylikt och svarar då mot ländernas krav på att chipet ska vara kontaktlöst. En fördel med ett kontaktlöst chip är att det snabbt kan läsas av och är oberoende av den omgivande miljön. Som det står i ICAOs tekniska rapport om kontaktlösa chip [8], består ett sådant här system dels av själva chipet och dels av en avläsare.

Det kontaktlösa chipet är passivt, vilket innebär att det inte har någon egen kraftkälla. Detta är lämpligt eftersom ett batteri normalt inte har tillräckligt lång livslängd. Kraftförsörjningen kommer istället från avläsaren via den antenn som är fastsatt på chipet. Chipet använder avläsarsignalens energi för att skicka ett svar. All kommunikation sker via denna antenn. Samma rapport [8] specificerar att det kontaktlösa chipet ska stämma överens med ISO-standard ISO/IEC 14443, som är en standard för RFID-chip. Räckvidden på dessa chip är 0-10 cm. En annan standard med räckvidd upp till 1 m utreddes också, men förkastades framför allt eftersom lagringskapaciteten för tillfället inte är tillräckligt stor.

För att garantera global interoperabilitet rekommenderar ICAO att biometrin som används ska lagras i form av en bild. [6] Olika länder använder olika algoritmer för att ta fram biometriska data från biometriska underlag och om underlaget är sparat som en bild kan biometriska jämförelser göras oberoende av vilken algoritm som används. Därtill kommer att det i vissa länder, som t.ex. Sverige, är olagligt att lagra biometrisk data. [9] Vidare rekommenderas att ansiktsbilden bör vara jpg-komprimerad och i storleksintervallet 15-20 kB (kilobytes). Med beräkning av ett minimum på 15 kB för en ansiktsbild och ungefär 5 kB för lagring av textdata samt information som signeringsnycklar, rekommenderas slutligen att chipet bör ha en minimal lagringskapacitet på 32 kB. [6] Enligt uppgifter från Thomas Wahlberg på RPS [9] så kommer chipet i de svenska passen ha en lagringskapacitet på just 32 kB, vilket följer rekommendationerna från ICAO.

Informationen som ska lagras kommer inte att vara krypterad. Däremot kommer den att skyddas med hjälp av Basic Access Control, vilket innebär att de maskinläsbara raderna måste läsas för att kunna komma åt informationen på chipet. Från de maskinläsbara raderna erhålls nycklar som är individuella för chipet. Avläsaren använder dessa nycklar för att bevisa sin behörighet till chipet i ett challenge-response protokoll. [10] Denna funktion är valfri enligt ICAOs rekommendationer, men eftersom den effektivt förhindrar att vem som helst okontrollerat kan läsa av en persons pass på avstånd, har den implementerats i svenska pass. Hur svårt det är att med hjälp av kända maskinläsbara rader avläsa ett chip är för oss i skrivande stund okänt. Om Basic Access Control används säger ICAO dessutom att kryptering av kommunikationskanalen mellan avläsaren och chipet är obligatorisk, detta för att förhindra avlyssning när avläsaren väl har autentiserats. Sessionsnycklarna för krypteringen är desamma som tas fram i samband med autentiseringen och är 2 nycklars 3DES nycklar. Kommunikationen skyddas sedan med Secure Messaging som förklaras närmare i ICAOs rapport om PKI. [10]

Passiv autentisering är obligatorisk enligt ICAOs rekommendationer. [10] Översiktligt går det till så att en digital signatur på chipet verifieras genom att använda den publika nyckel som tillhör den som signerat dokumentet. Denna persons certifikat för denna nyckel är lagrat hos avläsaren och försäkrar att informationen kommer från den rätta källan och inte

har förvanskats sedan utfärdandet. Denna metod förhindrar däremot inte exakta kopior eller utbyte av chip. [10]

3.2. Organisation

Organisationen kring de nya passen kommer att behöva uppdateras och i vissa fall förändras. Rutinerna vid anskaffning av pass förändras främst genom att passfotot tas direkt på passexpeditionen. Detta innebär att det vid varje mottagningskassa på passexpeditionen ska finnas en fotostation med digital fotoutrustning samt mjukvara för att verifiera fotokvalitet och ta fram biometrisk data. Även utrustning för att fånga namnteckningar digitalt hör till fotostationen. Vid fotografering tas ett flertal digitala foton varefter kvaliteten säkerställs samt att biometriska data tas fram ur ansiktsbilden för att verifiera att fotografiet är användbart som biometriskt underlag. Ett digitalt foto används sedan för att lasergravera den synliga ansiktsbilden i passet och lagras dessutom i komprimerad form på chipet. Den sökande bekräftar sin ansökan genom att skriva sin namnteckning på en digital skrivplatta. Normalt kan passet hämtas ut på passmyndigheten inom fem dagar och vid uthämtning kontrolleras ytterligare en gång om det biometriska underlaget är användbart. [1] Priset på det nya passet kommer att höjas från 270 kronor till 400 kronor inklusive foto. [7]

Efter införandet av passen kommer det att läggas större vikt vid chipet än den övriga informationen i passet. Chipet kommer att behöva avläsas och informationen visas upp på en skärm. Enligt Rikspolisstyrelsen kommer olika länder själva att få bestämma vilken metod för verifiering som ska användas. Den kommer enligt ICAO [6] förmodligen att gå till på något av följande två sätt:

1. Den resande jämförs med ansiktsbilden från chipet.
2. Kontrollpersonalen tar ett kort på den resande och jämför det med ansiktsbilden från chipet.

Det senare av sätten är mer fördelaktigt då jämförelsen kan ske med biometriska metoder. Metoden går ut på att jämföra avstånd mellan olika punkter i ansiktet, t.ex. avståndet mellan ögonen eller mellan ögon och näsa. Detta skulle naturligtvis vara fullt lagligt då ingen biometrisk data behöver sparas.

Passet kommer att ha en giltighetstid på fem år. Den främsta anledningen till att begränsa passets giltighetstid är att förkorta den period under vilket ett stulet eller förkommet pass kan komma att missbrukas. Eftersom passen också innehåller biometriskt underlag kan tio år vara för mycket med tanke på hur en persons utseende förändras. Med införsel av ett chip med lagrad biometrisk information följer en annan mycket viktig anledning till den förkortade giltighetstiden och det är den snabba utvecklingen inom både teknik- och biometriområdet. För att säkerheten ska kunna bevaras behöver tekniken förmodligen uppdateras så ofta som vart femte år.

Den nya typen av pass kommer att införas den 1:a oktober 2005. Gamla pass behöver inte bytas ut men kommer inte heller att kunna förnyas. Under övergångstiden då resenärer kan inneha den nuvarande typen av pass kommer verifieringen förmodligen att gå till som vanligt. Resor till USA kommer att kräva visum för resenärer med den nuvarande typen av pass.

4. Diskussion

Nedan gäller samma uppdelning av organisation och pass som under rubriken ”Implementering”. Här fokuseras på riskanalys och bedömning av systemet. Det kan vara på sin plats att nämna att det har varit svårt att få tag på information kring säkerheten hos de nya passen. Det är stor sannolikhet att en riskanalys gjorts, men den har för oss inte blivit känd. Därför kommer många frågor att ställas utan att kunna besvaras. Vi eftersträvar dock att läsaren ska bli introducerad i vilka frågeställningar som kan vara intressanta för att kritiskt och med egna ögon kunna bedöma systemet.

4.1. Pass

Chipet kommer egentligen att utgöra den nya delen och den stora skillnaden i de nya passen. Anledningen till att chipet är intressant är att kopplingen mellan ägare och pass kommer att bli svårare att bryta. Säkerheten kommer i och med detta att förbättras. Finns det några nackdelar med det nya systemet? Kommer det enbart att förbättra säkerheten utan att inskränka på andra områden?

I Sverige är det för närvarande olagligt att lagra biometriska data. [9] Detta anses bland annat vara en kränkning av den personliga integriteten. Det har däremot på olika håll internationellt diskuterats om biometriska data kommer att lagras i framtiden. Om ett sådant beslut skulle fattas internationellt pekar mycket mot att Sverige skulle ändra sin lagstiftning. Särskilt med tanke på Sveriges medlemskap i EU och den redan påvisade viljan att globalisera utfärdandet och kontrollen av resehandlingar. Att pass är en internationell fråga får inte glömmas. USA har varit drivande i frågan om att biometri ska användas huvudsakligen sedan terrorattackerna 2001. Men med tanke på det nya världsläget, kriget mot terrorismen med mera så blir förmodligen kritikerna till systemet med att lagra biometrisk data färre. Vår bedömning är att om en kränkning av integriteten är priset för en bättre säkerhet, så är det ett pris som många är beredda att betala.

Vilka risker finns det då med biometri i passen? Avläsningsavståndet är en diskutabel fråga. Enligt ICAO [8] rekommenderas inte avståndet för avläsning överstiga 10 cm. Detta är för att inte någon obehörig på avstånd ska kunna avläsa RFID-chipet. Eftersom informationen på chipet inte heller kommer att vara

krypterad så är det naturligtvis särskilt viktigt att obehöriga förhindras att komma åt informationen. Som nämndes tidigare kommer åtkomsten till chipet att vara skyddad av Basic Access Control där de maskinavläsbara raderna måste kunna läsas för att komma åt informationen på chipet. Vad händer om någon obehörig person redan har de maskinavläsbara raderna? Kan denne med någon avläsare skicka en extra stark signal till chipet och på så sätt få det att svara på längre avstånd än 10 cm? I ICAOs Annex I [8] nämns att detta inte är speciellt troligt eftersom energin som är tillgänglig för chipet minskar proportionellt med en 6:e-potens på avståndet mellan avläsare och chip. Men möjligheten utesluts inte och ICAO har några rekommendationer kring passens utformning som skulle avhjälpa obehörig avläsning av chipet. T.ex. föreslår ICAO att passet kan förvaras i en metallask då det inte används. Detta skulle förhindra avläsning. En annan idé handlar om att bladet näst intill chipet i passet ska vara av något metalliskt material som stör signaler till och från chipet. Vid en passkontroll kommer passägaren helt enkelt att öppna sitt pass och på så sätt vika bort det metalliska bladet. En sådan lösning skulle förstås ta bort en stor del av fördelen med kontaktlösheten hos ett RFID-chip, där framtidsvisionen är att från avstånd kunna läsa av flera pass samtidigt för att effektivisera passkontroller. Hur rimligt det är att dessa idéer blir verklighet eller hur de svenska passen kommer att se ut i detta avseende vet vi inte i skrivande stund. Skydd mot obehörig avlyssning vid en kontroll utförs, som nämndes ovan, med hjälp av den krypterade kommunikationen mellan avläsaren och chipet.

Hur svårt kan det vara att knäcka chipet och ändra informationen som finns där utan att det syns i en passkontroll? Detta är både svårt att svara på och ingår inte riktigt inom ramarna för denna rapport. För att försäkra att informationen inte är förvanskad sedan utfärdandet används passiv autentisering med hjälp av en PKI-metod som översiktligt beskrevs i ett tidigare kapitel. För djupare tekniska specifikationer hänvisas läsaren till ICAOs rapport om PKI [10]. Detta för oss direkt in på vilka risker det finns för obehöriga personer att tillverka sina egna pass. Detta skulle naturligtvis kunna bli ett mycket allvarligt problem. En central databas med information om alla pass som utfärdats skulle möjligtvis kunna förhindra detta, men det innebär också en mycket stor integritetskränkning. Mer om detta i nästa stycke.

4.2. Organisation

En av de viktigaste sakerna som behöver klargöras är att införandet av chip inte säkrar att en person har uppgett sitt rätta namn, medborgarskap och annan information när ett pass skapas. Men när en identitet har fastställts och skrivits till ett chip så kommer det att vara svårare för personen i fråga att använda sig av en alternativ identitet.

Vad händer om resultatet av en verifiering vid en passkontroll blir negativ? Detta är förmodligen frågan som många människor oroar sig för. Frågan är befogad eftersom människors utseende ändras i form av skägg, ärr och dylikt. Som tidigare nämnts kommer dagens pass inte att behöva bytas innan deras respektive giltighetsperiod löper ut. Dessa kommer helt enkelt att anses tillhöra en lägre säkerhetsnivå. Detta gäller även för pass där chipet fallerar. Om resultatet av en verifiering blir negativt kommer passet till en början förmodligen anses tillhöra en lägre säkerhetsnivå. Resenären kommer då att få fortsätta till en annan kontrollstation där verifieringsprocessen fungerar som dagens. Inom en snar framtid då förmodligen även fingeravtryck kommer att lagras så kan även detta komma att spela roll i en alternativ verifieringsprocess. Exakt hur verifieringsprocesserna kommer att se ut i framtiden och då eventuell biometrisk data lagras i passet är svårt att förutse. Särskilt eftersom det inte finns några klara riktlinjer för hur kontrollerna måste se ut.

En annan fråga som bland annat behandlas kort i en av ICAOs rapporter [6], är om informationen om personer som skaffat pass ska lagras centralt. Detta är inte aktuellt för tillfället men kan komma att bli det i framtiden. Det är också troligtvis en mardröm för integritetsförespråkarna. Då kommer polisen att ha information om alla som ansökt om pass, möjligtvis deras biometriska data m.m. Denna typ av register är idag förbjudna enligt lag huvudsakligen för den stora integritetskränkningen. Frågor som behöver ställas då är exempelvis vem som kommer att ha ansvaret för databasen, vem som får läsa informationen och vem som kommer att få ändra och skriva information i databasen. En central databas kan inte fungera utan att några människor får fullt förtroende, och det är en mycket kontroversiell fråga.

I inledningsavsnittet nämndes att alla länder, med USA i spetsen, vill höja känslan av säkerhet i pass. Bara känslan av att säkerheten är god bedömer vi är viktig för människor idag. Att införa ett chip i passet ger de flesta, som inte är insatta i datorer eller teknik, känslan av att passen och deras säkerhet moderniserats. Länders främsta tekniker som utvecklat produkten och garanterar dess säkerhet utgör en otrolig auktoritet som för någon tekniskt obevandrad kan vara svår att kritiskt bedöma. Känslan av säkerhet medför tillit. Det kan diskuteras hur mycket människor kommer att lita på passen och hur stor roll denna tillit kommer att spela. Kommer det att bli allvarligare fall av identitetsstölder om någon lyckas förfalska ett pass? Med tillit kan det lätt följa godtrogenhet och naivitet också. Därför kan det vara av största vikt att informera allmänheten om hur säkra passen i själva verket är. Stat och myndighet borde vara försiktiga med att skriva att passen är helt säkra mot förfalskning eftersom det inte kan garanteras. Det har säkerligen gjorts riskanalyser, som vi inte lyckats få tag på, där olika risker har identifierats, men allt sammantaget borde de nya passen vara säkrare än de gamla. Det kommer också att

ta längre tid för en förfalskning att upptäckas om inte kontrollpersonal kritiskt och noggrant granskar passen. Men som alltid så måste kontrollpersonal ändå balansera mellan kritiskt granskande och att inte vara alltför nitisk och misstänksam så att det försvårar för allmänheten att passera kontroller.

5. Avslutande sammanfattning

Den 1:a oktober 2005 inför Sverige det nya passet. Passet ska innehålla ett kontaktlöst chip av typen RFID och innehålla personlig information samt biometriskt underlag i form av ett digitalt ansiktsfoto. Informationen kommer inte att vara krypterad men kommer ändå att skyddas med passiv autentisering med PKI för att säkra att informationen inte har ändrats sedan utfärdandet. Passet anses på detta sätt bli säkrare eftersom informationen sparad på chipet ska vara svårare att förfalska och bandet mellan person och pass blir starkare. Observeras bör dock att passet kommer att erbjuda högre säkerhet endast då identiteten redan fastställts. Gamla pass behöver inte bytas ut innan deras respektive giltighetsperiod går ut, och de nya passens giltighetstid är sänkt till fem år.

Det finns dock både fördelar och nackdelar med det nya passet. Säkerheten blir bättre, men integritetsförespråkarna får betala ett högre pris. Känslan av att ”Storebror” observerar blir allt mer påträngande. Om människor fås att lita på att passet är säkrare än vad det är, så kan följden bli att identitetsstölderna blir allvarligare. Samtidigt förs diskussioner framförallt inom FN-organet ICAO hur reglerna för passen ska utvecklas genom att införa nya biometrier eller till och med skapa en databas med människors information och biometriska underlag. Det är en i allra högsta grad aktuell fråga som berör alla i samhället.

6. Referenser

[1] Proposition Prop. 2004/05:119 Ökad säkerhet i pass m.m., Justitiedepartementet, 10 mars 2005, http://www.regeringen.se/content/1/c6/04/05/49/010505b7.pdf, 050418

[2] Promemoria Ds 2004:8 Ökad säkerhet i pass m.m., Justitiedepartementet, 24 februari 2004, http://www.regeringen.se/content/1/c4/31/02/9f0af895.pdf, 050418

[3] Yttrande från Datainspektionen ”Utkast till lagrådsremiss Ökad säkerhet i pass m.m.”, 2005-01-12, http://www.datainspektionen.se/pdf/remissvar/biometriska_pass.pdf, 050423

[4] Lagrådsremiss Ökad säkerhet i pass m.m., Justitiedepartementet, 3 februari 2005, http://www.regeringen.se/content/1/c6/03/84/92/f6388ebe.pdf, 050418

[5] Polisens hemsida – www.polisen.se, Frågor om nya passet 050423

[6] Biometrics Deployment of Machine Readable Travel Documents, version 2.0, ICAO, 21/5 2004, http://www.icao.org/mrtd/download/documents/Biometrics%20deployment%20of%20Machine%20Readable%20Travel%20Documents%202004.pdf, 050423

[7] Polisens hemsida – www.polisen.se, Nytt pass 1 oktober, 050423

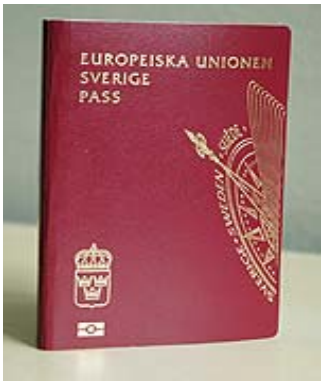
[8] Annex I, Use of Contactless Integrated Circuits in Machine Readable Travel Documents, version 4.0, ICAO, 5/5 -04, http://www.icao.int/mrtd/download/documents/Annex%20I%20-%20Contactless%20ICs.pdf, 050423

[9] RPS – Rikspolisstyrelsen, kontaktperson Thomas Wahlberg, projektledare Nya resehandlingar

[10] PKI for Machine Readable Travel Documents offering ICC Read-Only Access, version 1.1, ICAO, 1/10 2004, http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf, 050423

7. Bilagor

Figur 1. Symbol för att passet innehåller ett chip.



Figur 2. Den nya typen av pass.