



1710-01/05/DA-rev
WP 112
04/09/12

Udtalelse 3/2005

om gennemførelsen af Rådets forordning (EF) nr. 2252/2004 af 13. december 2004 om standarder for sikkerhedselementer og biometriske indikatorer i pas og rejsedokumenter, som medlemsstaterne udsteder

(Den Europæiske Unions Tidende L 385 af 29.12.2004, s. 1-6)

Vedtaget den 30. september 2005

Artikel 29-Gruppen er nedsat ved artikel 29 i direktiv 95/46/EF. Den er et uafhængigt EU-rådgivningsorgan vedrørende databeskyttelse og beskyttelse af privatlivets fred. Dens opgave er beskrevet i artikel 30 i direktiv 95/46/EF og artikel 15 i direktiv 2002/58/EF.

Sekretariatet varetages af Direktorat C (Civilret, grundlæggende rettigheder og EU-borgerskab) i Europa-Kommissionen, Generaldirektoratet for Retfærdighed, Frihed og Sikkerhed, B-1049 Bruxelles, Belgien, kontor LX-46 01/43.

Websted: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

Indhold

1.	Indledning.....	3
1.1.	Problemstilling	3
1.2.	Sagsforløb og baggrunden for Rådets forordning (EF) nr. 2252/2004	4
1.3.	Gruppens tidligere udtalelse.....	5
1.4.	Resolution vedtaget af Den Internationale Konference for Databeskyttelseskommissærer.....	6
2.	Indførelse af biometriske identifikatorer i pas, andre rejsedokumenter og id-kort.....	7
2.1.	Generelle overvejelser.....	7
2.2.	Etiske risici ved brugen af biometriske identifikatorer i pas, andre rejsedokumenter og id-kort	7
2.3.	Lovgivningsmæssige aspekter af indførelsen af biometri.....	8
a)	Forbehold over for en centraliseret europæisk eller national database for biometri...	8
b)	Adgang til biometriske identifikatorer begrænset til de kompetente myndigheder	9
2.4.	Tekniske aspekter	9
a)	Indførelse af et digitalt ansigtsbillede	10
b)	Indførelse af yderligere biometriske identifikatorer, specielt med hensyn til fingeraftryk.....	11
3.	Konklusioner	11

Udtalelse 3/2005
om gennemførelsen af Rådets forordning (EF) nr. 2252/2004 af
13. december 2004 om standarder for sikkerhedselementer og biometriske
indikatorer i pas og rejsedokumenter, som medlemsstaterne udsteder
(Den Europæiske Unions Tidende L 385 af 29.12.2004, s. 1-6)

GRUPPEN VEDRØRENDE BESKYTTELSE AF FYSISKE PERSONER I FORBINDELSE MED BEHANDLING AF PERSONOPLYSNINGER,

som er nedsat ved Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995¹,

som henviser til artikel 29, artikel 30, stk. 1, litra c), og artikel 30, stk. 3, i ovennævnte direktiv,

som henviser til sin forretningsorden, særlig artikel 12 og 14,

HAR VEDTAGET FØLGENDE UDTALELSE:

1. Indledning

1.1. Problemstilling

I sit "**Arbejdsdokument om biometri**"² understregede Artikel 29-Gruppen, at "de seneste års store fremskridt inden for biometrisk teknologi og den bredere anvendelse heraf kræver en grundig undersøgelse af databeskyttelsen. En omfattende og ukontrolleret udnyttelse af biometri skaber bekymring med hensyn til beskyttelsen af fysiske personers grundlæggende rettigheder og frihedsrettigheder. Der er her tale om en særlig form for data, idet de vedrører en fysisk persons adfærdsmæssige og fysiologiske karakteristika og gør det muligt at foretage en entydig identifikation af vedkommende".

Siden disse grundlæggende bemærkninger om biometri blev fremsat, er der sket store fremskridt inden for lovgivningen. Det Europæiske Råd bekræftede på sit møde i Thessaloniki den 19. og 20. juni 2003, at der er brug for en sammenhængende strategi i EU med hensyn til biometrisk identifikation eller biometriske data i forbindelse med tredjelandsstatsborgeres rejsedokumenter, EU-borgeres pas og informationssystemerne (VIS og SIS II). I efteråret 2003 fremlagde Europa-Kommissionen et udkast til Rådets forordning om ændring af forordning 1683/95 og 1030/2002 om ensartet udformning af henholdsvis visa og opholdstilladelser til tredjelandsstatsborgere.

¹ EFT L 281 af 23.11.1995, s. 13, kan findes på:
http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm.

² MARKT/10595/03/DA – WP 80, vedtaget den 1. august 2003.

1.2. Sagsforløb og baggrunden for Rådets forordning (EF) nr. 2252/2004

Den 18. februar 2004 fremlagde Europa-Kommissionen et udkast til forordning om standarder for sikkerhedselementer og biometriske identifikatorer i EU-borgernes pas³. Formålet med forslaget var at gøre passene sikrere ved at indføre et juridisk bindende instrument om standarder for harmoniserede sikkerhedselementer og samtidig etablere en pålidelig sammenhæng mellem den ægte indehaver og dokumentet ved at indføre biometriske identifikatorer. Desuden ville det gøre det muligt for EU-medlemsstaterne at overholde kravene i det amerikanske visumfritagelsesprogram i overensstemmelse med internationale standarder. I dette udkast foreslog Europa-Kommissionen, at pas og andre rejsedokumenter obligatorisk skulle omfatte et lagringsmedium med et ansigtsbillede. Medlemsstaterne fik mulighed for at indsætte fingeraftryk i passene i henhold til national lovgivning. Desuden foreslog Europa-Kommissionen, at den biometriske identifikator skulle lagres på et lagringsmedium med tilstrækkelig kapacitet. Det kunne være en kontaktløs chip, men kunne også være et andet lagringsmedium med den nødvendige kapacitet; detaljerne skulle fastlægges af de tekniske eksperter i det ansvarlige udvalg. Udkastet til forordning gav også mulighed for at lagre fingeraftryk i en national database med henblik på et fremtidigt europæisk register over udstedte dokumenter.

I sommeren 2004 var forslaget blevet drøftet i Visumgruppen. Den 6. oktober 2004 drøftede SCIFA (Det Strategiske Udvalg for Indvandring, Grænser og Asyl) endelig forslaget og sendte det til Europa-Parlamentet. Ifølge det endelige forslag skulle den første biometriske identifikator obligatorisk være et digitalt ansigtsbillede, mens fingeraftryk skulle være en valgfri anden biometrisk identifikator.

Som følge af mødet i RIA-Rådet (Retlige og Indre Anliggender) den 25.-26. oktober 2004 blev forslaget ændret, så begge biometriske identifikatorer blev obligatoriske⁴.

Europa-Parlamentets ikke-bindende lovgivningsmæssige beslutning af 2. december 2004 om Kommissionens forslag til Rådets forordning om standarder for sikkerhedselementer og biometriske identifikatorer i EU-borgernes pas⁵ blev vedtaget med 471 stemmer for og 118 stemmer imod, mens 6 afholdt sig fra at stemme. Parlamentet støttede indførelsen af pas, som indeholder et ansigtsbillede, fordi denne biometriske identifikator vil gøre det vanskeligere at forfalske pas. Det fremførte, at de biometriske data vil sikre, at en person, som foreviser et pas, faktisk er den person, som passet oprindeligt blev udstedt til. Det fastslog, at indførelsen af biometriske identifikatorer ikke må skade rettighederne i forbindelse med privatlivets fred og databeskyttelse, og afviste derfor obligatorisk medtagelse af fingeraftryk og oprettelsen af en central database over EU-pas og -rejsedokumenter. I den lovgivningsmæssige beslutning af 2. december 2004 fastslås det, at biometriske identifikatorer i pas kun bør bruges til kontrol af dokumentets ægthed samt pasindehaverens identitet, og at de skal lagres på "et lagringsmedium med et højt sikkerhedsniveau og tilstrækkelig kapacitet, som skal kunne sikre de lagrede datas integritet, ægthed og fortrolighed". Det anføres også, at det kun er de myndigheder i medlemsstaterne, der er kompetente med hensyn til læsning, lagring, ændring

³ Dokument KOM(2004) 116 endelig, nævnt i EUT C 98 af 23. april 2004, s. 39.

⁴ Rådskokument 15139/2004.

⁵ Europa-Parlamentets lovgivningsmæssige beslutning om Kommissionens forslag til Rådets forordning om standarder for sikkerhedselementer og biometriske identifikatorer i EU-borgernes pas (KOM(2004)0116 – C5-0101/2004 – 2004/0039(CNS)),
http://www.europarl.eu.int/omk/sipade3?SAME_LEVEL=1&LEVEL=2&NAV=X&DETAIL=&PUBREF=-//EP//TEXT+TA+P6-TA-2004-0073+0+DOC+XML+V0//DA.

og sletning af biometriske data, der må få adgang til dem. Desuden fremsatte Parlamentet et ændringsforslag til udkastet til forordning med følgende ordlyd: "Der oprettes ingen central database over EU-pas og -rejsedokumenter indeholdende biometriske og andre data for alle indehavere af EU-pas". I betænkningen fra Udvalget om Borgernes Rettigheder og Retlige og Indre Anliggender af 25. oktober 2004 hedder det: "Oprettelse af en central database vil krænke formåls- og forholdsmæssighedsprincippet. Det vil desuden øge faren for misbrug og for, at dataene anvendes til andre formål end de tilsigtede. Endelig vil det også øge faren for, at biometriske identifikatorer anvendes som "adgangsnøgler" til diverse databaser og derved forbinder datasæt."

Den 13. december 2004 vedtog Rådet forordning (EF) nr. 2252/2004 om standarder for sikkerhedselementer og biometriske identifikatorer i pas og rejsedokumenter, som medlemsstaterne udsteder⁶, på grundlag af det udkast, der blev vedtaget på RIA-Rådets møde den 25.-26. oktober 2004. Ifølge Rådets forordning er det digitale ansigtsbillede den første obligatoriske biometriske identifikator, mens fingeraftryk er den anden, ligeledes obligatoriske biometriske identifikator. Rådet tog ikke hensyn til de forslag og anmodninger om ændringer, som Parlamentet havde fremsat. Forordningen trådte i kraft den 18. januar 2005 i overensstemmelse med forordningens artikel 6. I samme artikel 6 hedder det, at medlemsstaterne anvender forordningen:

"a) for så vidt angår ansigtsbilledet: senest 18 måneder

b) for så vidt angår fingeraftryk: senest 36 måneder

efter vedtagelsen af de foranstaltninger, der er omhandlet i artikel 2."

Den 28. februar 2005 vedtog Europa-Kommissionen en "beslutning om fastsættelse af de tekniske specifikationer for standarderne for sikkerhedselementer og biometriske identifikatorer i pas og rejsedokumenter, som medlemsstaterne udsteder"⁷, der henviser til artikel 2 i Rådets forordning (EF) nr. 2252/2004.

1.3. Gruppens tidligere udtalelse

Formanden for Artikel 29-Gruppen sendte den 18. august 2004 et brev til formanden for Europa-Parlamentet, formanden for LIBE-Udvalget, generalsekretæren for Rådet for Den Europæiske Union, formanden for Europa-Kommissionen, generaldirektøren for Generaldirektoratet for Erhvervspolitik og generaldirektøren for Generaldirektoratet for Retlige og Indre Anliggender. Han pegede på følgende konkrete forslag⁸:

"1. Gruppen er stærkt imod lagring af biometriske data og andre data for alle indehavere af EU-pas i en central database for europæiske pas og rejsedokumenter.

2. Formålet med at indføre biometriske identifikatorer i pas og rejsedokumenter som omhandlet i forordningen skal være eksplicit, relevant, proportionalt og klart.

⁶ EUT L 385 af 29.12.2004, s. 1-6.

⁷ C(2005)409 (ikke offentliggjort i EUT).

⁸ Brev fra formanden for Artikel 29-Gruppen til formanden for Europa-Parlamentet, formanden for LIBE-Udvalget, generalsekretæren for Rådet for Den Europæiske Union, formanden for Europa-Kommissionen, generaldirektøren for Generaldirektoratet for Erhvervspolitik og generaldirektøren for Generaldirektoratet for Retlige og Indre Anliggender, dateret den 18. august 2004 (ikke offentliggjort).

3. Medlemsstaterne bør på en teknisk forsvarlig måde sikre, at passene omfatter et lagringsmedium med tilstrækkelig kapacitet og kapacitet til at sikre dataenes integritet, ægthed og fortrolighed.
4. Forordningen bør fastsætte, hvem der kan få adgang til lagringsmediet og til hvilke formål (læsning, lagring, ændring eller sletning af data).
5. Medlemsstaterne skal oprette et register over de kompetente myndigheder."

Formanden påpegede, at sikkerhedselementerne i pas og rejsedokumenter skal være gyldige og garanterede i hele dokumentets gyldighedsperiode. De udstedende enheder er ansvarlige for sikkerhedsstandarderne og den nødvendige infrastruktur. Borgerne må ikke pålægges ansvaret for eventuelle mangler på dette område, som opstår under redigeringen og udstedelsen af dokumentet eller i løbet af gyldighedsperioden.

Endelig henledte han opmærksomheden på udtalelsen om biometri (WP 80), som blev vedtaget af gruppen den 1. august 2003⁹, og udtalelsen om biometriske identifikatorer i visa og opholdstilladelser (WP 96), som blev vedtaget den 11. august 2004¹⁰.

I det brev af 30. november 2004 til formanden for LIBE-Udvalget og formanden for Rådet for Den Europæiske Union udtalte formanden for Artikel 29-Gruppen sig imod indførelsen af en yderligere obligatorisk biometrisk identifikator. Formanden understregede, at indførelsen af en yderligere biometrisk identifikator gør det endnu mere nødvendigt at oprette et sikkert system, som garanterer, at den grundlæggende ret til privatlivets fred ikke bringes i fare.

I den forbindelse må der også tages hensyn til den nylige udtalelse fra Artikel 29-Gruppen (WP 110) af 23. juni 2005 om forslaget til Europa-Parlamentets og Rådets forordning om visuminformationssystemet (VIS) og udveksling af oplysninger mellem medlemsstaterne om visa til kortvarigt ophold (KOM(2004) 835 endelig)¹¹. I udtalelsen fastslås Artikel 29-gruppens holdning til biometri endnu en gang, og gruppen anmoder om, at der indføres passende garantier for behandlingen af biometriske oplysninger i VIS.

1.4. Resolution vedtaget af Den Internationale Konference for Databeskyttelseskommissærer

Den 16. september 2005 vedtog den 27. Internationale Konference for Databeskyttelseskommissærer i Montreux en **resolution om brug af biometri i pas, identitetskort og rejsedokumenter**¹². I denne resolution påpeger Den Internationale Konference, at udbredt brug af biometri vil få vidtgående konsekvenser for det globale samfund og derfor bør være genstand for en åben debat på verdensplan. Den Internationale Konference kræver:

1. at der på et tidligt tidspunkt indføres effektive garantier for at begrænse de risici, som ligger i selve biometriens natur

⁹ MARKT/10595/03/DA – WP 80, vedtaget den 1. august 2003.

¹⁰ MARKT/11224/04/EN – WP 96, vedtaget den 11. august 2004.

¹¹ 1022/05/EN.

¹² <http://www.privacyconference2005.org> (endnu ikke offentliggjort).

2. at der foretages en klar sondring mellem biometriske data, som indsamles og lagres til offentlige formål (f.eks. grænsekontrol) på grundlag af retlige forpligtelser, og biometriske data, som med de pågældendes samtykke indsamles og lagres på grundlag af en kontrakt
3. at anvendelsen af biometri i pas og identitetskort med tekniske midler begrænses til kontrolformål, hvor man sammenligner dataene i dokumentet med de data, som indehaveren fremlægger, når han foreviser dokumentet.

2. Indførelse af biometriske identifikatorer i pas, andre rejsedokumenter og id-kort

Ifølge artikel 1, stk. 2, i forordning (EF) nr. 2252/2004 skal EU-borgernes pas obligatorisk indeholde et digitalt ansigtsbillede og fingeraftryk som biometriske identifikatorer. I henhold til artikel 6 og Europa-Kommissionens beslutning C(2005) 409 af 28. februar 2005 skal medlemsstaterne have indført det digitale ansigtsbillede i deres borgeres pas senest den 28. august 2006 og fingeraftryk senest den 28. februar 2008. De første medlemsstater skal begynde at udstede såkaldte ePas med et digitalt ansigtsbillede, som er lagret på en RFID-chip, i efteråret 2005. I de medlemsstater, som udsteder id-kort, er der planer om at indføre biometriske identifikatorer i disse kort.

2.1. Generelle overvejelser

Indførelsen af biometriske identifikatorer i pas vil få vidtrækkende konsekvenser for indehaverne af passene. Det kan derfor ikke gøres uden en grundig vurdering af indvirkningerne på privatlivets fred. Indtil nu har det været nok at have en beskrivelse af visse biometriske elementer i pas eller andre rejsedokumenter, såsom et foto og oplysninger om den pågældendes køn, højde eller øjenfarve. Når forordning (EF) nr. 2252/2004 er blevet gennemført, vil borgerne skulle levere biometriske data digitalt. Disse data kan lagres i databaser, og de kan stilles til rådighed for en lang række formål, som ikke kan forudses.

2.2. Etiske risici ved brugen af biometriske identifikatorer i pas, andre rejsedokumenter og id-kort

Der er en hel del etiske risici i forbindelse med indførelsen af biometriske identifikatorer i pas, andre rejsedokumenter og id-kort. BITE-projektet¹³ (Biometric Identification Technology Ethics), som blev sat i gang i oktober 2004, finansieres af EU som led i det sjette rammeprogram. Formålene med BITE er at fremme forskningen og sætte gang i en offentlig debat om bioetik i forbindelse med biometrisk teknologi. Der vil blive iværksat en offentlig høring i juni 2006. Et andet projekt, som støttes af EU under det sjette rammeprogram, er FIDIS¹⁴ (Future of Identity in the Information Society), der gennemføres af et konsortium af europæiske universiteter og virksomheder samt andre offentlige og private institutioner. Formålet med FIDIS er at udforme kravene til den fremtidige forvaltning af identitet i det europæiske informationssamfund og at bidrage til de teknologier og infrastrukturer, som der er behov for¹⁵.

¹³ <http://www.biteproject.org/>

¹⁴ <http://www.fidis.net>

¹⁵ To andre projekter, BIOSEC og BIOSECURE, som også finansieres via det sjette rammeprogram, behandler også i et vist omfang dette spørgsmål. <http://www.biosec.org> og <http://www.biosecure.info>

Ifølge en prospektiv undersøgelse¹⁶, som var bestilt af Europa-Parlamentets LIBE-Udvalg, bør der etableres nødprocedurer, der skal udgøre væsentlige garantier i forbindelse med indførelsen af biometriske identifikatorer, da disse hverken er tilgængelige for alle eller helt nøjagtige. Disse procedurer bør indføres og anvendes for at sikre, at den menneskelige værdighed for de personer, som registreringsprocessen ikke har kunnet gennemføres for, respekteres, og for at undgå, at de gøres ansvarlige for problemer, der skyldes systemfejl¹⁷.

Et af aspekterne i diskussionen er, at statslige institutioner og andre offentlige myndigheder vil kunne indsamle og lagre en enorm mængde følsomme oplysninger om deres borgere. I den forbindelse skal det specielt påpeges, at indsamling af biometriske identifikatorer betyder indsamling af oplysninger om en persons *krop*.

Et andet aspekt er, at biometriske identifikatorer, såsom fingeraftryk, hidtil mest er blevet indsamlet i forbindelse med straffesager. Spørgsmålet er, om EU-borgerne er villige til at aflevere fingeraftryk til andre formål.

Der er også problemer af anden art: Personer, som kan have sværere ved at bevise deres identitet, såsom indvandrere, kan blive uretfærdigt ramt af et sådant system; handicappede, som ikke kan underkaste sig biometritest, kan blive stigmatiseret; og der vil måske være adgang til følsomme helbredsoplysninger. På det praktiske plan er lovgivningen om privatlivets fred forskellig fra land til land, hvilket vil få betydning for udvekslingen af oplysninger og samspillet mellem databaser.

Med hensyn til lagring af fingeraftryk må man være forsigtig, når man drøfter forskellige sammenhænge mellem visse papillære mønstre og tilsvarende sygdomme. For eksempel siges visse papillære mønstre at afhænge af moderens (og dermed fosterets) ernæring i tredje graviditetsmåned¹⁸. Der ser ud til at være en statistisk korrelation mellem leukæmi og brystkræft og visse papillære mønstre. Man kender dog ikke nogen direkte eller præcise korrelationer i disse tilfælde. Men man kan ikke se bort fra den igangværende videnskabelige diskussion.

2.3. Lovgivningsmæssige aspekter af indførelsen af biometri

a) Forbehold over for en central europæisk eller national database for biometri

I den lovgivningsmæssige beslutning af 2. december 2004 krævede Europa-Parlamentet et forbud mod en central database over EU-pas og rejsedokumenter, som indeholder biometriske og andre data om alle indehavere af EU-pas. Gruppen støtter dette krav og fastslår, at indvendingerne mod en central europæisk database over EU-pas og -rejsedokumenter er de samme som mod centrale nationale databaser over pas og -rejsedokumenter og mod centrale databaser over id-kort.

Der er risiko for, at oprettelsen af en central database, som indeholder personoplysninger og specielt biometriske data om alle (europæiske) borgere, kan stride mod det grundlæggende proportionalitetsprincip. Enhver central database vil øge risikoen for misbrug og uretmæssig

¹⁶ Biometrics at the Frontiers: Assessing the Impact on Society, februar 2005, Institutet for Teknologiske Fremtidsstudier, Det Fælles Forskningscenter, Europa-Kommissionen.

¹⁷ Progress report on the application of the principles of Convention 108 to the collection and processing of biometric data, Europarådet, 2005, s. 11.

¹⁸ FIDIS, Study on PKI and biometrics, s. 68.

anvendelse af oplysningerne. En sådan database vil også øge risikoen for omgåelse af reglerne og "function creep". Endelig vil den øge mulighederne for at bruge biometriske identifikatorer som "adgangsnøgler" til forskellige databaser og derved forbinde forskellige datasæt.

b) Adgang til biometriske identifikatorer begrænset til de kompetente myndigheder

De biometriske identifikatorer i pas, andre rejsedokumenter eller id-kort er yderst følsomme. Det må derfor sikres, at det kun er de kompetente myndigheder, der kan få adgang til de data, som lagres på chippen. Uautoriseret adgang vil være uacceptabel. I den forbindelse støtter gruppen Europa-Parlamentets krav om, at hver medlemsstat skal føre et register over de kompetente myndigheder og de ansvarlige organer, som er omhandlet i artikel 3 i forordning (EF) nr. 2252/2004. Medlemsstaterne skal sende Kommissionen dette register og om nødvendigt regelmæssige ajourføringer heraf, og Kommissionen skal føre et ajourført online-register og skal hvert år offentliggøre en kompilering af de nationale registre.

I tilfælde af afvisning i forbindelse med grænsekontrol eller andre former for kontrol, som foretages af de kompetente myndigheder, skal de pågældende informeres om grundene til afvisningen, om, hvordan de kan gøre deres synspunkter gældende, og om, hvilke myndigheder de kan klage til.

2.4. Tekniske aspekter

Der er forskellige tekniske risici. Risiciene vedrører indførelsen af en kontaktløs chip (RFID-chip) og indførelsen af de biometriske identifikatorer, der skal lagres på chippen.

I sin lovgivningsmæssige beslutning af 2. december 2004 krævede Europa-Parlamentet, at passet skal omfatte et lagringsmedium med et højt sikkerhedsniveau og tilstrækkelig kapacitet, som skal kunne sikre de lagrede datas integritet, ægthed og fortrolighed. Gruppen støttede dette krav¹⁹, men Det Europæiske Råd tog ikke hensyn til dette. Den RFID-chip i overensstemmelse med ISO-standard 14443, som skal anvendes ifølge forordning (EF) nr. 2252/2004, medfører betydelige risici for EU-borgernes ret til privatlivets fred. Kommissionens beslutning af 28. februar 2005²⁰ er ikke nok til at beskytte borgernes rettigheder, da kommunikationen mellem RFID-chippen og læseren kan aflyttes og oplysningerne skimmes.

Risiciene i forbindelse med indførelsen af RFID-chips i pas, andre rejsedokumenter eller id-kort samt de risici, som følger med indførelsen af biometriske identifikatorer i chippen, kræver en sikkerhedsarkitektur, som sigter mod at øge fortrolighedsniveauet for de oplysninger, der skal udveksles. Gruppen, som fuldt ud er klar over problemerne, mener derfor, at der er behov for en global Public Key Infrastruktur (PKI). Offentlige nøglecertifikater indeholder oplysninger om indehaveren. Hvert digitalt certifikat kan udelukkende spores tilbage til den person, det er udstedt til. Digitale certifikater er unikke ligesom socialsikringsnumre, kreditkortnumre og sygesikringsnumre. Men digitale certifikater kan misbruges til at nægte en certifikatindehaver adgang til tjenester. Derudover kan transaktionsrelaterede data, som udveksles med målcertifikater, filtreres ud ved hjælp af

¹⁹ Brev fra formanden for Artikel 29-Gruppen til formanden for Europa-Parlamentet, formanden for LIBE-Udvalget, generalsekretæren for Rådet for Den Europæiske Union, formanden for Europa-Kommissionen, generaldirektøren for Generaldirektoratet for Erhvervspolitik og generaldirektøren for Generaldirektoratet for Retlige og Indre Anliggender, dateret den 18. august 2004 (ikke offentliggjort).

²⁰ C(2005)409.

overvågningsredskaber og leveres elektronisk til tredjeparter eller til politiet eller andre myndigheder.

I forbindelse med disse risici skal der obligatorisk oprettes en beskyttelsesprofil (Protection Profile, PP) i overensstemmelse med Common Criteria for Information Technology Security Evaluation (Common Criteria – CC) version 2.1 (ISO-standard 15408). De udgør en generelt accepteret løsning for IT-sikkerhedsproblemer. Protection Profile beskriver et IT-sikkerhedskoncept, som skal være fuldstændigt, konsekvent og sammenhængende. Denne Protection Profile bør fremlægges af det udvalg, som er nedsat ved artikel 5 i forordning (EF) nr. 2252/2004. I overensstemmelse med de krav om ændringer, som Europa-Parlamentet fremsatte i sin lovgivningsmæssige beslutning af 2. december 2004, foreslår gruppen, at udvalget bistås af eksperter, der er udpeget af gruppen.

a) Indførelse af et digitalt ansigtsbillede

Ifølge Europa-Kommissionens beslutning af 28. februar 2005 er medlemsstaterne forpligtet til at indføre et digitalt ansigtsbillede i deres borgeres pas inden den 28. august 2006. I henhold til artikel 1 og punkt 5.2 i bilaget til beslutningen skal medlemsstaterne beskytte adgangen til dataene på chippen ved hjælp af et sikkerhedselement kaldet basal adgangskontrol (Basic Access Control, BAC). BAC anbefales af Den Internationale Luftfartsorganisation (ICAO), men er ikke obligatorisk²¹. Formålet med BAC-ordningen er at forhindre skimming og aflytning. Den skal sikre, at det kun er muligt at få adgang til oplysningerne og specielt til de biometriske data, når der, før dataene læses fra chippen, er opbygget en "Document Basic Access Key" ud fra passets maskinlæsbare felt (Machine Readable Zone, MRZ) gennem en optisk kontakt mellem passet og læseren. "Document Basic Access Key" beregnes ud fra pasnummeret, fødselsdatoen og udløbsdatoen. Når denne "Document Basic Access Key" er opbygget, kan læseren læse de data, som er lagret på RFID-chippen. Af sikkerhedshensyn sker transmissionen af data på en krypteret måde. Dette kræver en certificeret sikkerhedschip med en krypteret co-processor²².

BAC udgør dog ikke et tilstrækkeligt sikkerhedselement. Den er baseret på passets maskinlæsbare felt. Men dataene i det maskinlæsbare felt behandles ikke strengt fortroligt. Hvis en EU-borger for eksempel ønsker at købe en billet til en særlig begivenhed, såsom "2006 FIFA World Cup Germany" eller "UEFA Euro 2008" i Østrig og Schweiz, er han nødt til at oplyse navn, fødselsdato, pasnummer eller id-kortnummer samt dokumentets udstedelsesdato via en internetformular. Denne procedure for køb af billetter er allerede blevet anvendt i forbindelse med "UEFA Euro 2004" i Portugal. Den vil desuden blive anvendt i forbindelse med andre arrangementer, såsom koncerter eller andre store sportsbegivenheder, herunder de olympiske lege og verdensmesterskaberne i atletik. Da private virksomheder i nogle medlemsstater kopierer passene eller id-kortene som garanti for udestående fordringer, er de elementer, der indgår i "Document Basic Access Key", ikke fortrolige, og man kan frygte, at algoritmen for BAC på et tidspunkt vil være tilgængelig på internettet.

²¹ ICAO Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, offentliggjort den 1. oktober 2004, s. 16.

²² Med henblik på sikker transmission har den såkaldte Essen-gruppe udviklet en særlig software kaldet Golden Reader Tool. Essen-gruppen består af offentlige myndigheder, IT-sikkerhedsvirksomheder og virksomheder, der fremstiller rejsedokumenter, fra Tyskland, Nederlandene og Det Forenede Kongerige.

b) Indførelse af yderligere biometriske identifikatorer, specielt med hensyn til fingeraftryk

Forholdene i forbindelse med optagelsen af fingeraftryk skal sikre en fuldstændig pålidelighed. Mens ICAO betragter et digitalt ansigtsbillede som ikke-følsomt – fordi passet stadig indeholder et foto af indehaveren – erkender organisationen, at indførelsen af fingeraftryk og andre yderligere biometriske identifikatorer i passet er yderst følsom. ICAO anbefaler derfor en særlig sikkerhedsordning kaldet udvidet adgangskontrol (Extended Access Control)²³. Ordningen for udvidet adgangskontrol fungerer på samme måde som BAC-ordningen, der er beskrevet ovenfor. Men i forbindelse med udvidet adgangskontrol bruges der et "Document Extended Access Key"-sæt i stedet for "Document Basic Access Keys". Det er op til den gennemførende stat at definere dette "Document Extended Access Key"-sæt (som er forskelligt fra chip til chip). "Document Extended Access Key"-sættet kan enten bestå af symmetriske nøgler, som f.eks. afledes af det maskinlæsbare felt og en "National Master key", eller af et asymmetrisk nøglepar med et tilsvarende kortcertifikat. Men der er stadig mange detaljer i forbindelse med disse sikkerhedsordninger, som ikke er afklaret.

Udvidet adgangskontrol er et fremskridt med hensyn til sikkerhedsforanstaltninger, men denne sikkerhedsordning er ligesom BAC ikke obligatorisk²⁴. Hertil kommer, at det er et åbent spørgsmål, om udvidet adgangskontrol vil blive anvendt af tredjelande. Europa-Kommissionen og medlemsstaterne bør sikre, at EU-borgeres pas, som indeholder fingeraftryksdata, ikke kan læses af læsere, der ikke er kompatible med udvidet adgangskontrol.

3. Konklusioner

Indførelsen af biometriske identifikatorer i pas, andre rejsedokumenter og id-kort rejser en række etiske, juridiske og tekniske spørgsmål. Gruppen peger således på følgende aspekter:

1. Inden der indføres biometriske identifikatorer i pas, andre rejsedokumenter eller id-kort, skal der gennemføres en tilbundsgående diskussion i samfundet. I den forbindelse er det nødvendigt at afvente resultaterne af BITE-projektet.
2. For at begrænse de risici, som ligger i selve biometriens natur, må der på et tidligt tidspunkt indføres effektive garantier. I den forbindelse skal det udvalg, som er nedsat ved artikel 5 i forordning (EF) nr. 2252/2004, der skal bistås af eksperter, som er udpeget af Artikel 29-Gruppen, fremlægge en beskyttelsesprofil (Protection Profile).
3. Det skal sikres, at der foretages en klar sondring mellem biometriske data, som indsamles og lagres til offentlige formål (f.eks. grænsekontrol) på grundlag af retlige forpligtelser, og biometriske data, som med de pågældendes samtykke indsamles og lagres på grundlag af en kontrakt.
4. Anvendelsen af biometriske identifikatorer i pas og identitetskort skal med tekniske midler begrænses til kontrolformål, hvor man sammenligner dataene i dokumentet med de data, som indehaveren fremlægger, når han foreviser dokumentet.

²³ ICAO Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, offentliggjort den 1. oktober 2004, s. 17.

²⁴ ICAO Technical Report: PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, offentliggjort den 1. oktober 2004, s. 17, 21 og 22.

5. Europa-Kommissionen og medlemsstaterne bør garantere, at EU-borgernes pas, som indeholder fingeraftryksdata, ikke kan læses af læsere, der ikke er kompatible med udvidet adgangskontrol (Extended Access Control).

6. Det skal sikres, at det kun er de kompetente myndigheder, der kan få adgang til de data, som er lagret på chippen. Medlemsstaterne skal oprette et register over de kompetente myndigheder.

Udfærdiget i Bruxelles, den 30. september 2005.

For Artikel 29-Gruppen
Peter Schaar
Formand