

Security og biometri i transportsektoren

Kartlegging av behov for Person-ID

Desember 2005

Rapporten er finansiert med støtte fra



MODERNISERINGSDEPARTEMENTET



INNHALDSFORTEGNELSE

Forord	3
Bakgrunn	4
1 Sammendrag og anbefaling	6
2 Generelt om transportsektoren i Norge	8
3 Myndigheter og juridiske forhold og organisering	8
4 Biometriske pass	9
5 Kartlegging og områdebeskrivelse	10
5.1 Generelt	10
5.2 Behov innen grensekontroll og immigrasjon	11
Nasjonale ID-kort	
Reisepass for hund, katt og ilder	
5.3 Behov i luftfart	15
5.4 Behov innen havnesikkerhet	17
Seafarer's Identity Document (SID)	
5.5 Behov i vegtrafikk	18
5.6 Behov i forsvaret	19
5.7 Behov i helsesektoren	20
5.8 Behov i kultursektoren	21
5.9 Behov i bygg- og anleggsnæringen	21
5.10 Behov i kriminalitetsomsorgen	22
5.11 Behov i Posten	22
5.12 Behov i bankene	23
5.13 Praksis i andre land	23
6 Standardisering	24
7 Opplæring	24
8 Konsekvensvurdering og risikovurdering	24
9 Konklusjoner og Anbefaling	26
Vedlegg	27
1 Artikkel om "Biometric ID and Security Control"	28
2 ACI Europe – Position Paper 06.01.2004	31
3 Brief Summary of International Standards Activity	36
4 ILO strategy paper – Seafarer's ID (SID)	39
5 European Citizen Card – ECC	41
6. Terminologi og begreper – IT brancheforeningen i Danmark	43
7. Menneskers identitet – Noen betraktninger	44

Forord

Arbeidet med ny generasjon person-ID på kombinerte elektroniske og visuelle identitetskort har pågått i over ti år i Norge. En tidlig aktivitet var at daværende Norsk Teknologistandardisering i 1994 inviterte til et ID-forum for å kartlegge behov og vurdere mulige løsninger. Standard Norge har siden holdt i denne prosessen ved etablering av referansegrupper innen standardiseringsapparatet, tilknytning til direktiv for elektronisk signatur og ved å slå sammen tilgrensende standardiseringskomitéer til "K-188 Person-ID" for å optimalisere arbeidet. Det er imidlertid ennå et stykke fram, og det er vårt håp at foreliggende rapport kan bidra i det videre arbeidet.

ITS Norway tok opp temaet Security og Biometri tidlig i sin virksomhet. Norges Lastebileier Forbund og Avinor tok opp behovet i transportetatens "Nettverksgruppe for multimodal ITS" med ønske om å vurdere felles løsninger, standarder og mulighetene for et frivillig "borgerkort" (Citizen Card). Foreningen etablerte våren 2005 en egen faggruppe for Security og Biometri under ledelse av Avinor. Det er arrangert seminar og møter i regi av faggruppen og gruppens arbeid utgjør viktig bakgrunn for arbeidet med rapporten.

ITS Norway takker Avinor AS, Fiskeri- og kystdepartementet og Moderniseringsdepartementet som har bidratt med finansiering til utredningsarbeidet. Vi takker Steria As som har bekostet trykking. Vi takker også Leif Jansen (Kystdirektoratet), Ole Folkestad (Avinor), Odd Stormorken (Norsik), Odd H. Elness (Steria) og Ole H. Øen (Norges Lastebileier-Forbund) for verdifulle bidrag. ITS Norway har bidratt med egeninnsats for å ferdigstille prosjektet.

ITS Norway er en uavhengig medlemsorganisasjon som arbeider for å fremme kunnskap om og bruk av intelligente transportsystemer. Medlemmene kommer fra myndigheter, næringsliv, forskning og organisasjoner og representerer alle transportformer. Foreningen er et nettverk for samarbeid, utvikling og standardisering - med fremtidens transportløsninger i fokus. Målsettingen er bedre utnyttelse av transportsystemet og økte leveranser fra norske virksomheter.

Foreliggende rapport har fokus på fellesløsninger og veivalg videre for person-ID. Asbjørn Hovstø, Management IT (tidl. ErgoGroup) har vært prosjektleder. Det var planlagt et større arbeid, men til tross for stor forståelse hos mange parter har det ikke vært mulig å få til en tilstrekkelig finansiering i henhold til den opprinnelige planen. Prosjektarbeidet er derfor skalert ned tilsvarende. Vi håper likevel at rapporten skal utgjøre et verdifullt bidrag for å skape bedre forståelse for mangfoldet av behov og krav til ID og security, inklusive det åpenbare behovet for samordning. Vi tar utgangspunkt i transportsektoren, men rapporten viser at det er sammenfallende situasjon i de fleste samfunnsområder.

Oslo, 22. desember 2005

Ivar Christiansen

Daglig leder ITS Norway



Bakgrunn

Behovet for dette prosjektet om person-ID og biometri er tatt ut fra problemstillinger som er drøftet i brede lag innen transportsektoren, i Nettverksgruppen for ITS i transportetatene og i faggruppen for security og biometri i ITS Norway. Innen nettverket til ITS Norway er det foreløpig Kystverket, Avinor og Norges Lastebiler-Forbund som har påvist særlige behov for harmoniserte ID-kort løsninger for personell og publikum som utfører oppgaver og benytter tjenester.

Krav til personidentifikasjon og kontroll berører i dag mange offentlige virksomheter med ansvaret liggende hos det enkelte fagdepartement. Det er innført strengere krav til sikker person-identifikasjon på fly- og havneterminaler, for mannskap på skip, for førerkort, for grensepassering, for asyl- og visumsøknader, til forsvarets anlegg og i forbindelse med ulike typer arrangementer og hendelser.

Innen EU pågår det et omfattende arbeid for harmonisering på dette området. I Norge har Moderniseringsdepartementet en rolle for nasjonal harmonisering og PKI, mens Standard Norge har ansvar for teknisk standardisering. Det er nødvendig med et konkret initiativ for å utforme grunnlaget for en felles norsk standard for ID-kort med PKI og biometri. Det er ellers svært sannsynlig at det utvikler seg flere løsninger og regimer som ikke er kompatible og som skaper økte kostnader og begrensinger for samfunnet.

Vi ser sammenfallende utfordringer og løsninger knyttet til sikker personidentifikasjon innen flere samfunnsområder hvor fellesnevneren er forflytning av personer og gods.

Prosjektets mandat er å utføre en vurdering av dagens situasjon og foreslå tiltak som kan samordne området, herunder opplæring og standardisering. Aktivitetene i prosjektet er skalert i forhold til tilgjengelig finansiering, men dekker likevel alle de følgende områder:

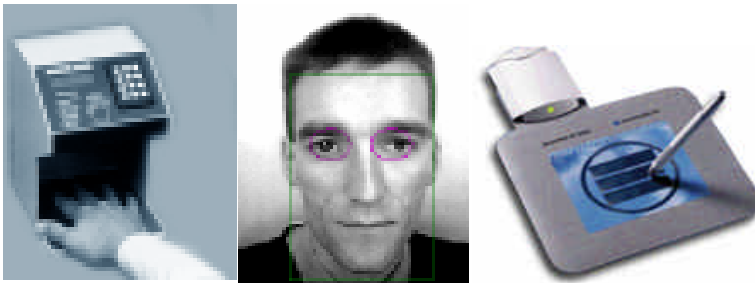
1. kartlegge dagens situasjon og behov
2. arrangere seminarer i regi av faggruppen for security og biometri
3. foreslå opplæringstiltak
4. delta i og påvirke standardiseringsarbeidet
5. lage en sluttrapport med anbefaling om videre arbeid

Et av siktemålene for denne rapporten er å påvise muligheten for å samordne behov for Person-ID fra ulike myndigheter. Avinor som flyterminal operatør og ansvarlig for fysikring har særlige behov, og her gjengis en problemstilling fra selskapet:

”Avinor har i dag løsninger som kan sjekke ”hvor plastkortene befinner seg” – om de er innenfor et visst område. En vet ikke hvem som bærer kortet. For å få til en verifisering av identitet må ”Biometri” teknologien anvendes. Det er en utfordring at teknologien er ny og at entydige standarder ikke er ferdig utviklet. Det vil medføre store ekstra kostnader ved bruk av manuell ID-sjekk. Avinor ønsker innføring av et frivillig nasjonalt ID-kort med biometri. Det forutsetter at en offentlig myndighet som politiet, er ansvarlig utsteder av kortet og at dette kan betraktes som et ”sub-sett” av et (elektronisk) pass.”

Biometri er....

Kroppens "PIN-kode" for å identifisere og verifisere påstått identitet



Eksempler:

- Iris
- Ansikt
- Fingeravtrykk
- Signatur
- Hånd

1. Sammendrag og anbefaling

Kartlegging

Det er i prosjektet foretatt en kartlegging av behov og beskrivelse av eksisterende løsninger for person-identifikasjon i Norge. Myndighetene arbeider for å få til en samordning på området og det er en positiv utvikling med f.eks. Justisdepartementets initiativ til en interdepartemental arbeidsgruppe for en utredning omkring nasjonalt ID kort (se under). Kartleggingen i kapittel 5 inneholder de mest presserende behovene i de ulike områdene.

Kartleggingen har vært utført ved intervju og informasjonsinnhenting fra nøkkelpersoner i de enkelte sektorer. Av viktige funn er erkjennelsen av at hver sektor har lagd sine egne standarder uten tanke på om standardene kan bruk på tvers.

Luftfart. Pass er i dag det eneste godkjente bevis på personidentitet for eksempel i en lufthavn. Spesielt fra brukere er det framkommet behov for et ID-kort i et mindre format som er tilpasset andre kortformat. ID-kortet må være anerkjent som et offisielt ID-dokument fra Norge.

Havn og Skipsfart. Sikkerhetsregelverket som benyttes i havner og på skip (ISPS) setter krav til kontroll med gods inn i havnen og fra havn til sjøside for videre transport. Regelverket stiller krav til kontroll og oversikt over personer i havna med krav om ID-bevis.

Som et ledd i beredskap mot terror i internasjonale sjøhavner og lufthavner stilles det krav om personkontroll ved tilgang til ulike sikkerhetssoner.

Passasjer- og personellsikring har et voksende behov i internasjonal skipsfart. En internasjonal konvensjon i regi av den internasjonale arbeidstaker organisasjonen ILO, stiller krav til et nytt og enda sikrere ID-kort for sjøfolk med deltakelse fra Norge.

Landtransport. Lastebilnæringen må forholde seg til et utall av ulike identitetsbevis og autorisasjonskort og har behov for å redusere antallet til et fåtall.

Transportoperatører utstyres publikum med et antall reisedokumenter til bruk i kollektivtrafikk, flytrafikk, grensekryssende buss- og togtrafikk, samt elektroniske billettsystemer. Publikum har behov for reisedokumenter som kan benyttes på tvers av transportformer.

Harmonisering

ITS Norway anbefaler en harmonisert norsk standardprofil for personbasert ID til bruk i transportsektoren. Profilen bør baseres på en europeisk standard for European Citizen Card (ECC) som dekker behovene i de fleste transportformer. Profilen bør også ta hensyn til ICAO-anbefalingene som er sentrale ved utvikling av maskinlesbare og biometriske pass. Profilen kan harmoniseres med Seafarer's Identity Documents (SID) som benyttes innen skipsfart.

En detaljert kravspesifikasjon bør utformes i samarbeid mellom transportoperatører og myndigheter. Siden arbeidet har en klar lovmessig side foreslås det at Justis- og politidepartementet organiserer det videre arbeidet.

Justisdepartementet bør vurdere å utstede en harmoniserte norske standardprofilen som et nasjonalt ID-kort under prosedyren knyttet til søknad om pass. Vi kjenner til at Justisdepartementet i brev av 29.11.2005 har invitert Finansdepartementet, Arbeids- og inkluderingsdepartementet, Fornyings- og administrasjonsdepartementet, Samferdselsdepartementet og Utenriksdepartementet til en arbeidsgruppe for utredning av spørsmålet om innføring av et nasjonalt ID-kort. Arbeidet skal innen 30.april 2006 legge fram et foreløpig forslag til etablering av ordning for nasjonalt ID-kort, og skal legge fram sin innstilling innen 15.september 2006.

Ansvar for internasjonale standardiseringsprosesser innen flytransport, skipsfart, havner, jernbane, veg- og lastebiltransport er idag spredt ut til ulike direktorat og tilsyn. Ansvar med spesiell vekt på sikkerhet innen disse områdene bør koordineres bedre med brukerne og én organisasjon bør settes til å koordinere dette arbeidet. Bekjentgjøring og innspill på standarder innen luftfart (ICAO), sjøfolk (ILO), maritim (IMO) og ISO/IEC bør koordineres sterkere fra en relevant brukerorganisasjon.

FOU

Det anses som sannsynlig at et videre arbeid for en harmonisert ID kan utnytte tilgjengelige FOU-midler i tillegg til egeninnsats fra ulike interessenter innen privat og offentlig sektor. Sikkerhetsområdet er et eget fagområde med mange interessenter.

Det er interesse for å få opp sertifiseringsordninger for produkter og tjenester innen Person-ID ved bruk av tjenester hos Nasjonal Sikkerhetsmyndighet (NSM). Det bør søkes å etablere en offentlig utviklingskontrakt (OFU) gjennom Innovasjon Norges virkemiddelapparat for å utvikle sikkerhetsrelaterte evalueringsprofiler for et nasjonalt ID-kort med særskilte krav til den som er utsteder.

Videreføring

ITS Norway planlegger å arrangere to seminarer eller workshops basert på denne rapporten.

- Diskusjonsmøter i Faggruppen for security og biometri i desember og januar. Deltakerne i Faggruppen får anledning til, på fritt grunnlag, å gi kommentarer til rapporten, og komme med forslag til videre arbeid, mandat for et nytt prosjekt og lignende. Det kan også være aktuelt at Faggruppen nedsetter et egnet Arbeidsutvalg for å lage forslag til en prosess for videreføring av initiativet til harmonisering. Faggruppen arrangerte et arbeidsmøte 14.desember hvor vi fikk innsyn i Justisdepartementets initiativ om en egen arbeidsgruppe for et nasjonalt ID kort (se over) og planlegger et nytt møte i februar med fokus på transportnæringen og ITS-konferansen 2006.

- Basert på rapporten og drøftelser i Faggruppen foreslås det at berørte myndigheter inviteres til en prosess med tanke på å lage en kravspesifikasjon for et nasjonalt ID kort som spilles inn til Justisdepartementets arbeidsgruppe. ITS Norway kan som en nøytral organisasjon påta seg sekretariatsoppgaver.

2. Generelt om transportsektoren i Norge

Persontransportene har ulike behov for identifikasjon og støttesystemer avhengig av transportform. Det er nå økende muligheter for samvirkende systemer på tvers av transportformene. Dette er betalings- og informasjonssystemer som skal gjøre det lettere for passasjerene å benytte en sammenhengende transportkjede med en billett eller reisedokument. ID-kort vil bli nødvendig i en slik sammenhengende reise.

Persontransport med fly har til nå sett ulik praksis for krav om person-identifikasjon og det innføres et stadig strengere identifikasjons regime. Det innføres nye pass med biometriske kjennetegn fra 2006 (ansiktsgjenkjenning og fingeravtrykk). Det er også behov for personregistrering på passasjerbåtruter. Det er et eksempel på å benytte bankkort som registreringsenhet (elektronisk) når man går ombord i en hurtigbåt langs kysten. I kollektivtrafikken innføres i stigende grad smartkort som billettmedium. Enkelte billettyper som periodebillett og kundekort krever personinformasjon, og det er behov for et multifunksjons ID kort med billettapplikasjon. Det er også mulig at virksomheters ansattkort kan utstyres med en applikasjon for tilgang til kollektivtrafikk.

Godstransport består som oftest av en kjede av enkelttransporter, særlig når skipstransport er en del av kjeden. ISPS-regelverket innen internasjonal skipsfart har krav om fysisk sikrede havneterminaler. Personell som har oppgaver knyttet til godstransportene må bære identitetskort. Adgangskontrollsystemer og identitetskort er under løpende utvikling. Det er i dag ingen felles krav til systemer i trafikkhavner noe som kan medføre at en lastebilsjåfør må utrustes med flere kort for å kunne betjene sine leveranser noe som er en uholdbar utvikling. Det vil i økende grad bli satt sporingsbrikker på godset (RFID), f eks på en container. Det betyr at havneoperatører kan etablere en sikrere oversikt over type gods, inklusive om det er farlig gods. Dagens situasjon med beredskap for terror, menneskesmugling og annen smugling, medfører at skipets mannskap og personell på havnesiden kan kreve at egen personsikkerhet er ivaretatt.

3. Myndigheter og juridiske forhold – ansvar og organisering

Flere aktører, f.eks. Posten har tatt initiativ til å innføre et nasjonalt ID-kort som også kan benyttes for reise- og identitetskort i områder hvor det ikke stilles krav til pass (Norden og Schengen-området). Det er kun Passloven som stiller eksplisitte krav til en nasjonal ID med forankring i Pass-registeret. Justisdepartementet tok i 2003 initiativ til å utarbeide en kravspesifikasjon for biometriske pass, noe som ble fulgt opp av Politidirektoratet i 2004 med utarbeidelse av anbudsdokumenter. Leverandør ble valgt i april 2005. Utstedelse av biometriske pass startet 1.oktober 2005.

Personvern

Personopplysningsloven som forvaltes av Datatilsynet er vesenlig for arbeidet med harmoniserte løsninger, samt utstedelse og anvendelse av et nasjonalt ID-kort. I forbindelse med innføringen av biometriske pass er det tidligere reist spørsmålet overfor passmyndighetene om personvernet er tilfredsstillende ivaretatt.

Sikkerhet

Ulike problemstillinger må vektlegges i forhold til sikkerhet. Representanter for 40

europiske personvernmyndigheter (note 1) har i en felles resolusjon (note 2) reist krav om at effektive sikkerhetsforanstaltninger må settes inn på et tidlig stadium. Tidsfristen som er satt fra USA er gjentatte ganger blitt benyttet som begrunnelse for hvorfor det haster slik med den norske gjennomføringen. USA har imidlertid utsatt innføringen av biometriske pass til oktober 2006 slik at den sammenfaller med den interne fristen EU har satt for innføringen.

Justisdepartementet opplyser at ICAO-kravene som er lagt til grunn for sikkerhet er publisert på ICAOs hjemmeside og kan bestilles fra ICAO.

4. Biometriske pass

Fra 1. januar 1993 innførte Norge en ny passblankett som var i samsvar med internasjonale anbefalinger og forberedt for maskinlesbarhet. Passene fylles ut manuelt, lamineres og ferdigstilles på det enkelte passøkersted (politistasjon, lensmannskontor eller utenriksstasjon).

Siden 1997 har det pågått arbeid med å videreutvikle passet og gjøre det maskinlesbart. Det har også vært et mål å gjøre passet sikrere mot manipulasjoner.

I Justisdepartementets regi er det utviklet et pass som tilfredsstillende anbefalinger gitt av den internasjonale luftfartsorganisasjon ICAO – Doc 9303 fifth edition 2003 – maskinlesbare pass, id-kort og reisedokumenter. ICAO publiserte i 2004 tekniske rapporter for hvordan lagre ansiktsbiometri og fingeravtrykk, PKI for digital signering av datainnhold og en logisk datastruktur for en kontaktløs brikke (RFID).³

13 desember 2004 ble det vedtatt en rådsforordning om biometriske reisedokumenter i EU. Forordningen innebærer at medlemslandene og EØS-landene må ha pass der biometriske data om ansiktsform, i første omgang, er digitalt lagret. Også fingeravtrykk skal lagres, men først på et senere tidspunkt. De biometriske dataene lagres på en elektronisk brikke som kan leses av "kontaktløst". For å få til dette, bruker man en RFID-løsning som er i stand til å kommunisere med en leser over en gitt radiofrekvens. Tekniske spørsmål og kryptering er omhandlet i kapittel om Grensekontroll. Etske og lovmessige spørsmål behandles i ISO/IEC 24714, (se vedlegg 3) og i et pågående EU-prosjekt BITE⁴.

Det har de siste årene vært en sterk økning i utstedelse av ID-kort både som kundekort og som ansattkort i tillegg til bankkort. ID-kortene benyttes i varierende grad for å bekrefte egen identitet. Utviklingen har vist at mange ID-kort er produsert uten tanke på sikkerhet med liten eller ingen kopibeskyttelse. Det er utviklet metoder i kriminelle miljø internasjonalt for å "stjele" og misbruke identiteten til intetanende personer. "Tyveriene" kan forekomme ved fysisk å stjele pass og ID opplysninger på internett. Det

¹ ARTICLE 29 Data Protection Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 01/43. Website: http://europa.eu.int/comm/justice_home/fsj/privacy/index_en.htm

² 1710/05/EN WP 112 04/09/12 Opinion on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (Official Journal L 385 , 29/12/2004 p. 1 - 6) Adopted on 30 September 2005

³ Se <http://www.icao.org/mrtd/> for oppdaterte spesifikasjoner

⁴ Se <http://www.europeanbiometrics.info/> for oppdaterte opplysninger.

kan skje ved at en person oppgir informasjonen til skjulte kilder. Trusselbildet knyttet til biometriske pass dreier seg om hvorvidt en persons biometriske data kan avleses uten personens vitende, og benyttes til å skape en ny identitet basert på personens data.

Dette er en alvorlig utvikling, og med store personlige konsekvenser for den som rammes. Nasjonale ID-løsninger basert på sertifiserte produkter vil imidlertid kunne tilbakeføre identitet for personer som er rammet, og vil langt på vei legge hindringer i veien for de kriminelle miljøene.

5. Kartlegging og beskrivelser

5.1 Generelt

Personidentifikasjonsområdet har stor aktualitet med økende internasjonal reisevirksomhet, økt mobilitet og økt bruk av elektronisk identifikasjon ved forhold som elektronisk handel og e-læring, og som svar på internasjonal terrortrussel. Den akselererende utvikling av nye metoder for personidentifikasjon ved hjelp av biometriske metoder, kaller på økt ressursinnsats fra norsk side.

Personidentifikasjon og biometri har betydning når identifisering skal være sikker. Biometriske ID-kort muliggjør en automatisering av identitetskontroll og denne kan dermed skje hurtigere. Mange institusjoner burde ha interesse av å komme fram til en felles løsning - dette kan være institusjoner som er ansvarlige for utstedelse eller godkjenning av pass- og reisedokumenter, aktører i forhold til grensepassering, offentlig transport, identifisering av førere, elev- og studentidentifisering, samt identifisering ved bruk av bank- og finansapplikasjoner.

Krav fra USA til elektroniske reisedokumenter gir en mulighet til uttesting for ulike bedrifter. Utfordringene for å få på plass et reisedokumentregime, ligger i hovedsak til offentlig sektor. Amerikanske krav til identifisering av offentlig ansattes (FIPS 2) og til transportarbeideres identifisering vil stille krav til internasjonale standarder.

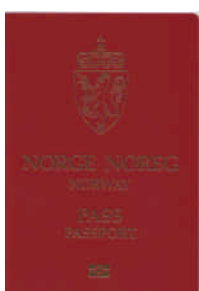
Europeisk arbeid med identifisering og et mulig kommende direktiv gjør at norske myndigheter bør være kjent med forberedende prosesser.

Av aktører som er sentrale ved personidentifikasjon nevner vi:

- Den internasjonale luftfartsorganisasjonen ICAO har gjennom fasiliteringskonferansen FAL med spesifisering av sikkerhet innen lufttransport, der TAG/MRTD er en rådgivende gruppe for å utarbeide de tekniske spesifikasjoner for maskinlesbart pass, mens New Technology Working Group (NTWG) har ansvar for å vurdere ny teknologi for pass.
- Politidirektoratet har valgt produsent av biometriske pass basert på ICAO sine anbefalinger og står foran utrulling av leseutstyr.
- Den internasjonale arbeidstakerorganisasjonen ILO har laget spesifiseringen for internasjonal sjømannsidentitet basert på fingeravtrykk som biometri. Sjøfartsdirektoratet har ansvaret for implementering i Norge.
- Den internasjonale maritime organisasjon IMO som har definert sikkerhetsregelverket for såkalte ISPS-godkjente internasjonale trafikkhavner.

- SERTIT er den norske sertifiseringsmyndigheten for IT-sikkerhet som bl.a. forestår sertifisering av IT-produkter og systemer, og som skal gjøre det enklere å tilfredsstillte forhåndsdefinerte sikkerhetskrav ved anskaffelser.⁵
- Standard Norge arbeider med standardisering generelt innen informasjonsteknologi og innen ITS. Dette betyr at organisasjonen kan tilby å koordinere og bistå norsk, og annen ekspertise innen sikkerhet og biometri. Målet for en slik innsats er å oppnå kjennskap til aktuelle standardprosesser, påvirke standardutformingen og finne samsvar mellom nasjonale spesifikasjoner og internasjonale krav – samtidig at det sørges for at arbeidet blir avstemt i standardiseringens konsensusprosesser.

5.2 Behov i grensekontroll og immigrasjon



Det er politiet som har oppgaven om å håndheve grensekontroll og i første rekke består kontrollen av å godkjenne identitetsdokumentet til den reisende. Kommer den reisende fra et Schengen-land gjelder kun kontroll av ID-dokument. For en rekke andre land – de såkalte Visa-waiver landene og land Norge har visum-fri avtale med er det tilstrekkelig med pass. Ved innreise fra alle andre land er det krav om visum som må være utstedt av norsk ambassade eller konsulat i vedkommende land.

Ved utreise er det krav om gyldig reisedokument og den reisende må identifisere seg med pass for å bevise at en er riktig innehaver av reisedokumentet.

Immigrasjonsmyndigheten i Norge er Utlendingsdirektoratet – fra 1.1.2006 underlagt Arbeids- og inkluderingsdepartementet. UDI er ansvarlig for utstedelse av en asylsøker-ID for mennesker som ankommer Norge uten identitetsdokumenter.

Det er behov for ordninger som kan bekrefte identitet og pre-klarere den reisende allerede fra avreiselandet. En rekke transportoperatører assisterer ulike lands immigrasjonsmyndigheter med ordninger for passasjer- og prosesseringsinformasjon med det mål å registrere reisende i automatiserte klareringssystemer allerede ved avreise.

Tekniske løsninger

De fleste land står foran innføring av maskinlesbare pass med biometriske kjennetegn lagret i en elektronisk brikke i passet. Norge og Sverige startet utstedelsen fra 1.oktober – på bakgrunn av opprinnelige krav fra USA om ansiktsbiometri i maskinlesbare pass fra 26.oktober 2005. Mange land har hatt problem med å møte den opprinnelige fristen, og amerikanske myndigheter besluttet i juni 2005 å forlenge fristen med ett år til 26.oktober 2006. I løpet av 2007 regner norske myndigheter å ha på plass leseutstyr i grensekontrollene for biometriske pass og visum. Noen flyselskap har allerede slikt leseutstyr på plass i Norge.

Et EU-pass vil være basert på dokumentet ”Council Regulation on standards for security features and biometrics in passports and travel documents issued by Member States” publisert i februar 2005 med følgende innhold:

- spesifikasjon for biometriske identifikatorer; ansikt og fingeravtrykk
- lagringsmedium i elektronisk brikke

⁵ Se www.sertit.no for flere opplysninger om sertifiseringsordningen.

- logisk datastruktur i elektronisk brikke
- spesifikasjon for sikkerhet knyttet til lagrede data i elektronisk brikke
- konformitetstest for elektronisk brikke og applikasjoner
- berøringsfri kompatibilitet (Radio Frequency Identifikasjon– RFID) med andre elektroniske reisedokument

Medlemslandene pålegges å integrere ansiktsbiometri innen sommeren 2006 og fingeravtrykk senest 18 måneder deretter.

Den nye generasjon maskinlesbare pass (MRTD) blir således utstyrt med berøringsfri elektronisk brikke som inneholder digitalisert biometri til innehaver. Data som lagres på elektronisk brikke må tilfredsstillende sikkerhetskrav til autentisitet (inkl. integritet), originalitet og konfidensialitet. Derfor har ICAO spesifisert mekanismer for passiv autentisering, aktiv autentisering og aksesskontroll:

Mekanisme	Beskyttelse	Kryptografisk teknikk
Passiv autentisering	Autentisitet	Digital signatur
Aktiv autentisering	Orginalitet	Challenge-Respons
Aksesskontroll	Konfidensialitet	Autentisering & Secure Channels

Passiv autentisering sikrer at reisedokumentet er autentisk, uendret og utstedt og digitalt signert av angitt myndighet med dennes offentlige nøkkel (PKI). Passiv autentisering er påkrevet, men sikrer ikke mot urettmessig kopiering av innhold i den elektroniske brikken eller mot at en elektronisk brikke er erstattet med en annen elektronisk brikke. For å sikre seg mot dette må Aktiv autentisering benyttes. Ved autentisering via maskinlesbar sone (MRZ) kan det verifiseres at rett elektronisk brikke er identifisert og lest fra. Aksesskontroll sikrer kommunikasjonen mellom pass og leserutstyr med kryptering med den hensikt å beskytte personvern og ivareta retten til den reisende om slik beskyttelse. Aktiv autentisering og Aksesskontroll er begge to svært viktige ingredienser for et sikkert maskinlesbart reisedokument (MRTD).⁶ Aktiv autentisering og aksesskontroll er begge valgfrie sikkerhetsmekanismer. Slike sikkerhetsmekanismer er svært sentralt for EU og forventes å inngå i et EU-pass og den endelige spesifikasjon vil være tilgjengelig mot slutten av 2005.



Nasjonale ID-kort

I Europa innen Schengen-området er det ikke lenger grensekontroll innenfor området. Det er likevel nødvendig å ha med seg et ID-kort eller pass som legitimasjon. Alle hoteller og overnattingssteder har plikt til å kreve ID-dokument i Schengen-området.

Ved reiser utenfor Schengen som til Storbritania og Irland samt resten av verden er det passet som gjelder som gyldig legitimasjon.

I Norge anerkjenner NyeKripos også ID-kort som reisebevis fra alle tidligere EU-land og 8 av 10 nye EU-land når personer fra ulike nasjoner passerer norsk grensekontroll.

⁶ Federal Office for Information Security (BSI), Bonn, Tyskland, Advanced Security Mechanisms for Machine Readable Travel Documents

Det er et økende behov for oversikt, informasjon og opplæring i ulike lands ID-kort løsninger. Det er ikke bare krav til selve dokumentet, men også til hvilke prosedyrer kortene er utstedt under for å bl.a. å redusere risiko for å få utstedt ID-dokument på andre enn personen selv. Hvert land som utsteder nasjonale ID-kort bør ha en egen brosjyre som beskriver sikkerhetselement og registrerings- og utleveringsprosedyrer.



Eksempel på et typisk europeisk lands nasjonale ID-kort, der forsiden inneholder kortholders signatur og foto, samt kortholder-navn, kortholders nasjonale ID-nummer, kortholders fødselsdato, kortholders kjønn, kortholders statsborgerskap, kortnummer samt kortets gyldighetsperiode.



Kortets bakside på det nasjonale ID-kort inneholder data om kortinnehavers fødested, kortets utstedelsesdato, oppholdstillatelse (om nødvendig), samt kortet og kortinnehavers data i maskinlesbart format iht ICAO-9303 standarden – lesbar tekst med OCR-B type font.

Alle visuelle data på kortet er også offentlig tilgjengelig

elektronisk med unntak av foto og håndskrevet signatur. I tillegg inneholder kortet to elektroniske sertifikater med tilhørende hemmelige nøkler og PIN-koder. Sertifikatet inneholder kun innehaverens navn og nasjonalt fødselsnummer. I tillegg inneholder autentiseringssertifikatet kortinnehavers offentlig tildelt email adresse i formatet firstname.lastname.NNNN@utsteder.land, der NNNN består av 4 tilfeldige tall som er nødvendig for å tildele en unik email-adresse til personer med samme navn. Adressen endres ikke, men garanteres som personens email adresse livet ut. Estlands nasjonale ID-kort koster 10 Euro inkludert programvare, med tillegg av kortleser fra 6 Euro. Neste utgave av ID-kortet vil leveres med berøringsfri elektronisk brikke og logisk datastruktur med biometriske data i henhold til ICAO-standard.

Reisepass for hund, katt og ilder

Fra 2005 er det påbudt at hund, katt eller ilder som reiser i europeiske land har sitt eget pass. I Norge erstatter passet det gamle veterinærsertifikatet som var et krav ved innførsel av dyr. Reisepasset er kommet i stand som følge av EU-forordning nr.998/2003 som Norge også er pålagt gjennom EØS-avtalen.

Passene utstedes av veterinærer med tillatelse og det er Mattilsynet som autoriserer veterinærene til å utstede pass for hund, katt og ilder.

Hvert pass har et unikt nummer som tildeles av passprodusentene VESO og Euro-Pharma. Den enkelte veterinær skal føre fortegnelser over hvilket passnummer det enkeltedyr har fått.

Passet skal inneholde all dokumentasjon som er nødvendig for innførsel og tilbakeførsel av hund, katt og ilder til Norge fra EU-land og for reise fra Norge til EU-land. Passet kan også benyttes til dyr som ikke reiser, hvis f.eks. eier ønsker å samle opplysninger om vaksinasjoner og behandlinger på ett sted.

I passet er det også plass til å fylle ut eierskifte, vaksinasjon og blodprøvetaking, siste rabiesvaksinasjon med siste frist for revaksinasjon. Det er ikke tillatt å fjerne eller legge til sider i passet og nytt pass må utstedes om det ikke er mer plass til attestasjoner.

Nedenfor et norsk pass godkjent for EU-området med en sprøyte som skyter inn en microchip i dyrets venstre skulder, samt et halsmerke for å vise at dyret er merket og identiteten kan leses av med en liten scanner.

Veterinærer tar fra kr.150 for å utstede pass og merke dyret.



5.3 Behov i luftfart



Luftfart er en internasjonal næring hvor sikkerhetskravene i stor grad blir definert av ICAO (International Civil Aviation Organization). ICAO er et overnasjonalt organ hvor medlemsstatene er forpliktet til å følge pålegg gitt av organisasjonen. I Norge er det Luftfartstilsynet som gjennom forskrifter og lover implementerer påleggene.

Innenfor luftfart har security lenge vært et fokusområde. Etter 9.11 ble fokuset ytterligere skjerpet, både overfor ansatte innen luftfarten og reisende. Rett etter 9.11 ble det innført krav til identitetskontroll av alle reisende. Kravet falt bort etter en tid, men er nå på vei til å bli gjeninnført. Pr 01.07.05 ble det innført krav til identitetskontroll av passasjerer med innsjekket bagasje på utenlandsreise. Håndheving av kravet til identitetskontroll av alle reisende medfører store ekstrakostnader for flyselskapene pga økt bemanning i skranke og ved "gate"ene.

Pass er det eneste ID-beviset som er godkjent internasjonalt. Nasjonalt kan man i tillegg til pass godkjenne flere typer ID-bevis, og i Norge er førerkort og bankkort også godkjent. ICAO har under utarbeidelse en standard for både hvordan ID-bevis skal være utformet, og hvordan prosessene rundt utstedelse av disse skal være. Det internasjonale bankvesen og internasjonale vegmyndigheter har utarbeidet likeartede standarder.

De senere årene har automatiserings- og selvbetjeningsgraden i tilknytning til innsjekking og boarding av fly økt betraktelig. Denne utviklingen har skjedd blant annet for å redusere kø-tiden for den reisende og dermed gjøre reiseopplevelsen mer behagelig, samt å redusere kostnadene for flyselskapene. Målinger viser at stadig flere benytter automater eller foretar innsjekking via Internet. Skal utviklingen føres videre, vil det kreve innføring av biometrisk ID-kontroll. Alternativet er manuell kontroll med tidstap for reisende og flyselskapene.

Innføring av krav til ID-kontroll av reisende, *uten* en nasjonal standard for ID-bevis kan reversere denne utviklingen. Et viktig prinsipp i lufthavner er at utstyr som benyttes til innsjekking, boarding mv skal være av såkalt "Common Use" type. Det betyr at ulike operatører benytter samme utstyr. En innsjekkingskranke og en "gate" kan for eksempel både benyttes av SASBraathens og Norwegian om hverandre.

I og med at det ikke finnes noen standard for verken utstyr til bruk for automatisert identitetskontroll eller biometriske reisedokumenter, er det grunn til å frykte at de ulike operatørene vil installere ulikt utstyr ved for eksempel "gate"en.

Behovet: Innføring av et nasjonalt biometrisk ID-kort som følger ICAO standard vil sørge for at flyselskapene ikke behøver å innføre sine egne biometriske ID-kort og løsninger for å lese dem automatisk. Det siste ville være en løsning som ikke er til det beste for den reisende eller selskapene, og som kan komme til å redusere sikkerheten.

På en lufthavn er det behov for ulike ID-løsninger avhengig av hvilke risikoområder man beveger seg i. De ulike områdene er

- Landsiden – del av lufthavnen som er åpen for alle
- Kontrollert område – etter sikkerhetskontroll og før flyside åpent for alle

- Flyside (Security Restricted Area (SRA)) – del av lufthavnen med begrenset tilgang, normalt for flygende personell (med adgangskort og flysertifikat), utvalg av ansatte på lufthavnen, politi, toll og GA-personell
- Høyrisiko-sone (Critical Security Restricted Area (CSRA)) – område rundt fly, drivstoff installasjoner, bakkeradar, sentrale dataanlegg, der adgangen er basert på funksjon

I et åpent område i lufthavnen for både publikum, besøkende, personell og reisende vil det ikke være hensiktsmessig å adgangskontrollere. Så lenge Norge ikke har et nasjonalt ID-kort, vil det ikke være hensiktsmessig å kreve ID-kort i disse åpne publikums-områdene.

I kontrollert område – innenfor sikkerhetskontrollen – vil det være adgang med begrensninger. Reisende med gyldig billett vil være et typisk adgangsdokument som gir tilgang til kontrollert område. Ved behov bør den reisende ha med seg en gyldig legitimasjon som kan vises på forespørsel.

I område Flyside vil det kun være personell ansatt ved lufthavnen, i samarbeidende virksomheter eller i flyselskapene som har tilgang. Ansattkort, crew-kort eller andre dokumenter som knytter de ansatte til samarbeidende virksomhet bør kreves her.

I høyrisiko-områdene – rundt flyene, ved drivstoff installasjonene, områder i tilknytning til bakkeradar og sentrale dataanlegg – bør det stilles strenge krav til ID-kort og kun ID-kort utstedt av lufthavnen selv. Biometriske ID-kort kan her bidra til å øke sikkerhet ved personverifisering. Biometri vil knytte kortinnehaver med personens fysiske kjennetegn, gjerne med bruk av en PIN-kode i tillegg. 3-faktor⁷ autentisering må være et minimumskrav og dører med sluseløsning som sikrer at kun den identifiserte personen slipper gjennom.

Behovet: Det er stort behov for en samordning spesielt knyttet til personell med en sekundær tilknytning til lufthavnen, slik som transportører, service-personell mm. En typisk problemstilling er hvilken part skal stå for utstedelsen. Siden lufthavnen står ansvarlig for sikkerheten i lufthavnen er det mest naturlig at den selv står for innhenting av personalopplysninger ("enrollment"), utstedelse av ID-kortet, tilbaketrekking av ugyldige og mistede kort, samt aktivering av kort mot soner og dørkort-lesere.

ACI Europe er en brukerorganisasjon som organiserer lufthavnene i Europa. ACI Europe har laget et eget dokument om problemstilling ID-kort og biometri (se vedlegg 2).

Ved store flyplasser med mange internasjonale flyselskap og hyppige ankomster er der innført egne gater hvor det flygende personell registrerer seg med sitt Air Crew Card og fingeravtrykk eller ansikt som biometri med åpning av dør/port ved gyldig adgang. Til venstre et bilde fra Smartgate ved Kingsford Airport i Sydney, Australia. Automaten leser ansiktsbiometri fra kortet med tre kamera og åpner gate hvis faktisk bilde stemmer med bilde lagret på kortet.



⁷ 3-faktor autentisering – noe du vet f.eks. PIN-kode, noe du har f.eks. et ID-kort og noe du er f.eks. verifisering med biometri mot ID-kortet eller mot database med tillatte brukere.

5.4 Behov ved havnesikkerhet

FNs sjøfartsorganisasjon IMO vedtok i desember 2002 et nytt internasjonalt regelverk om sikkerhetstiltak om bord på skip og i havneanleggene.

Dette er inntatt som et nytt kapittel XI-2 i "The international convention for the Safety Of Life At Sea (SOLAS-konvensjonen). SOLAS kapittel XI-2 om "Special measures to enhance maritime security" og den tilhørende ISPS-koden (International Ship and Port Facility Security-Code) inneholder en rekke myndighetskrav og krav til konkrete sikkerhetstiltak som skal iverksettes om bord på skip i internasjonal fart og i havneanlegg som betjener slike skip. Målet er å forhindre terroranslag mot internasjonal skipsfart.

Kystdirektoratet er myndighet for implementering av regler for havnesikkerhet. ISPS – koden består av to deler: "Part A" - obligatoriske krav og "Part B" som er anbefalinger. ISPS-regelverket er implementert for havner som har tillatelse til å betjene internasjonal trafikk. Fiskeri- og kystdepartementet har for implementering av ISPS-koden i norske havner delegert Kystdirektoratet en rekke oppgaver og myndighet. Sjøfartsdirektoratet er ansvarlig for å implementere sikkerhetsregelverket som skal gjelde om bord i skip.

Seafarer's Identity Document (SID)

Kravet om bedre sikkerhet og trygghet på skip har kommet fram etter 11. september 2001. Den internasjonale maritime organisasjon IMO og den internasjonale arbeiderorganisasjonen ILO har studert dette problemet nærmere og samarbeidet har resultert i ILO konvensjon 185. Konvensjonen etterspør et nytt og enda sikrere ID-kort for sjøfolk og gjør det samtidig klart at bare bruk av biometri kan tilfredsstillende strenge krav til sikkerhet ombord i skip og i havneanlegg og samtidig gjøre det enklere for sjøfolk til å reise til et land med fly og mønstre på i en havn – og mønstre av i et annet lands havn og returnere hjem fra landets flyplass uten bruk av visum. SID skal være tilstrekkelig for å bekrefte personens arbeidsmessige tilhørighet i skipsfart.



Hvert lands maritime myndighet vil være ansvarlig for å utstede disse nye ID-kortene. Kortene erstatter tidligere identifikasjonsdokument som sjømannsboka og reduserer behov for visum, uten å være en erstatning for passet men et tillegg.⁸

Kortet vil være unikt for hver enkelt kortholder siden fingeravtrykket skannes og opptrer som en to-dimensjonal barkode på baksiden av ID-kortet. Ved kontroll kan kortholder plassere fingeren på en skanner som sjekker om fingeravtrykket tilsvarer den kode som er lagret i kortet. En ny ISO-standard 24713-3, Biometric Profiles for Interoperability and Data Interchange – Part 3: Seafarer's ID vil være tilgjengelig i 2007.

Andre yrkesgrupper som havnearbeidere, kranførere og lastebilsjåfører har behov for et tilsvarende ID-kort i en ISPS-godkjent havn.

⁸ Norge vil være første land i Europa som står for utstedelse av Seafarer's Identity Document i 2006.

5.5 Behov i vegtrafikk

Identifikasjonsbehovene er mange i vegtrafikken. Hovedgruppene for disse behovene gjelder identifikasjon av sjåfør, kjøretøyet, selve lasten og lastebæreren. En kort gjennomgang er nevnt nedenfor.⁹

Sjåføren har behov for:

- Pass (ved internasjonal transport), utsteder Politiet
- Sertifikat, utsteder Statens vegvesen
- Del av vognkortet som identifiserer eieren og oppbevares av denne.
- Helseattest (hvis sjåfør er 70 år eller eldre, utsteder: legekantorene)
- Tachograf sjåførkort, utsteder Statens vegvesen
- ADR-kompetansebevis, utsteder Statens vegvesen v/trafikkstasjonene
- Diverse ID-kort for adgangskontroll i sikkerhetsklarerte havner med internasjonal trafikk (ISPS-regelverket), utsteder den enkelte havn
- Diverse ID-kort for adgangskontroll hos private virksomheter (f.eks. Statoil sine oljeraffinerier)
- Diverse kompetansebevis som bevis for dyretransport, truck- og kranførerbevis (utsteder Sentralregisteret for yrkesbevis, Våler i Hedmark),

Kjøretøyet har også identitetsbehov. De viktigste er:

- Vognkort, utsteder Statens vegvesen
- Godsløyve, utsteder Fylkeskommunen
- Grønt forsikringskort for internasjonal transport, utsteder forsikringsselskapene
- Fellesskapstillatelse for kjøretøy i internasjonal transport, utsteder Statens vegvesen
- Digital tachograf
- AutoPass-brikke, utsteder lokal bomselskap i Norge
- Ferjebetalingskort, utsteder ferjerederiene
- Motorvegkredittkort, bl.a. for motorveger i Italia, Spania m.fl.
- Kort for betaling av lastebilavgiften Maut i Tyskland
- Kort for drivstoff (Statoilkort, og lignende)
- Kort for betaling/kreditt, diverse

Identitetsbehov for selve lasten:

- Tolldeklarasjonspapirer, utsteder: tollmyndighetene
- Fraktbrev, utsteder: avsender
- CMR-fraktbrev ved int. transport, utsteder: Avsender eller speditør

⁹ Kilde: Norges Lastebileier Forbund

- RFID-brikker for last og gods (kommer i nær framtid)

Identitetsbehov for selve lastbæreren

- RFID-brikker for lastbærere – paller og containere (kommer senere)

Denne listen, som antakelig ikke er komplett, er allerede lang nok til at denne rapportens formål vedr. behov for harmonisering av ID-kort "floraen" forhåpentlig kommer tydelig fram.

Førerkort er en internasjonal de facto standard for personidentifikasjon. Nye standarder for internasjonale førerkort vil i hovedsak følge retningslinjene til nye elektroniske pass med tillegg av elektronisk lagring av bilde, fingeravtrykk, iris og andre biometriske data.

I Storbritania er det UK Driver and Vehicle Licence Association i Swansea, Wales som står for organiseringen.

Her er det ting som tyder på at førerkortet vil være det de facto nasjonale ID-kortet for de personer som har rett til å benytte kortet. Et EU-direktiv for førerkort forutsetter

introduksjon av elektroniske enheter for å kunne avlese og autentisere kortet. Flere land er i ferd med å introdusere førerkortet som smartkort. Imidlertid fjerner et nytt EU-

direktiv denne restriksjonen. EU-kommisjonen har etablert en ny ekspertgruppe for å tilpasse såkalte LEP-kort til smartkort-funksjonalitet. Tachograf-kort som innføres i hele Europa for å kontrollere hvilebestemmelsene ved yrkestransport har et behov for å kunne lagre tid for kjøring i smartkortet. I Norge skal tachograf-kortet innføres fra 2006. Politiet vil således ha et stort behov framover for å sjekke gyldighet og innhold i kortene via mobile enheter fra veggside.



5.6 Behov i Forsvaret

Det er et stigende behov for identifikasjon med høy sikkerhet for adgang til militære områder og andre områder som krever høy beskyttelse. Forsvarsdepartementet har derfor sett behovet for å ha kontroll med utstedelse av egne ID-kort for forsvaret.

Forsvaret har valgt å erstatte både "Kongeriket Norge-kortet" for befal og ansatte og "vernepliktsboka for soldater" med et standard ID-kort. Kortet har en grunndesign som gjør at det skal gjenkjennes som Forsvarets kort, men inneholder også design-elementer som viser noe om innehaverens rolle i organisasjonen. Kortene blir utstedt på grunnlag av Forsvarets egen personliddatabase og er tilknyttet et bestillings- og kortadministrasjonssystem. Bestillingssystemet er hel-elektronisk og bygget opp slik at ingen kan utføre hele bestillingsprosessen alene. Bestillingsenhetene er skilt fra den sentrale produksjonen, og produksjonen er også modulert bygget opp. Det er således lagt stor vekt på sikkerhet og kontroll i prosessene. Selve kortet inneholder også flere

sikkerhetslementer, noe som gjør det svært vanskelig å endre eller totalforfalske kortet. Kortet brukes som et visuelt ID-kort og det er tatt høyde for at det skal ha stor slitestyrke. I tillegg har det en strekkode og magnetstripe, noe som gjør at det kan utnyttes i administrative systemer. Kortet er også forberedt for senere å kunne ha elektronisk brikke. Løsningen må sies å være velbalansert og at de ulike elementene henger sammen på en god måte. Samtidig er løsningen bygget for å kunne utvikles videre og tilpasses framtidens behov.

Bildet nedenfor viser korttypene som ble benyttet i en testfase.



5.7 Behov i helsesektoren

Helsepersonell-kort



Rikstrykdeverket inngikk i 2001 en rammeavtale om bruk av PKI og smartkort for helsesektoren, der legene får utstedt kort og kode for digital signatur på sykmelding, resept og oppgjørmelding. Av totalt 8.000 privatpraktiserende leger har vel 3.000 valgt å bestille smartkortet bl.a. for også å få tilknytning til Nasjonalt helsenett og bredbåndstjenesten. Et aktuelt problem med å håndtere roller gjelder fornying – hvordan skal

sertifikatets gyldighetsperiode utvides uten å måtte få utstedt nytt kort og hvordan skal et utgått kort nektes brukt.

Europeisk helsetrygdkort

Alle som er medlem av norsk folketrygd har rett til å få utstedt et europeisk helsetrygdkort. Europeisk helsetrygdkort er et plastkort på størrelse med et vanlig bankkort. Kortet dokumenterer at vedkommende har rett til nødvendig helsehjelp under midlertidig opphold i et annet [EØS-land](#), på lik linje med oppholdslandets egne statsborgere for dekning av nødvendig medisinsk hjelp. Ordningen omfatter også familiemedlemmer, det vil si ektefelle og barn under 25 år, uavhengig av statsborgerskap. Kortet erstatter den tidligere blankett E 111 man måtte få på trygdekontoret for hvert utenlandsopphold.



Pasientkort

Det foreligger ingen pasientkort i kommersiell bruk, men det er utført forsøk

med slike kort, bl.a. som et gravidekort med registrering av alle undersøkelser under svangerskapet (lege, helsestasjon, sykehus) og som medisinkort med registrering av alle resept-pålagte medisiner pasienten gis i forbindelse med resepter.

5.8 Behov i kultursektoren

Siden år 2000 har Norsk Tipping drevet statens forsøk og kommersiell bruk av smartkort med elektronisk ID for å forenkle innlegging av spill hos kommisjonær og på internett. Smartkortet utstedes etter strenge prosedyrer for kvalifisert, elektronisk signatur under kontroll av Post- og teletilsynet. Annen generasjon smartkort av spillerkortet er nå på markedet og kan også benyttes i andre sammenhenger som krever sterk autentisering, bl.a.hos Skattedirektoratet ved innlevering av moms-oppgaver og selvangivelse. I følge planen skal 2 millioner smartkort utstedes til erstatning for dagens magnetstripe-kort.



5.9 Behov i bygg- og anleggsnæringen

I forskrift nr.377 av 7.oktober 2004 om sikkerhet, helse og arbeidsmiljø på bygge- og anleggsplasser stilles det strengere krav for bygge- og anleggsplasser” hvor det sysselsettes mer enn fem arbeidstakere skulle fra årsskiftet 2005/2006 pålegge alle arbeidsgivere innen bygg- og anleggsbransjen å utstyre sine arbeidstakere med egne identitetskort, som en oppfølging av tiltak mot sosial dumping, som følge av utvidelsen av EU/EØS østover. ID-kortet skulle inneholde navn, bilde, foretaksnummer, navn på virksomheten de er ansatt i og gyldighetsdato. ID-kortet skal i følge §10 være i hendig format og være vanskelig å forfalske. Det er også innført krav til hovedentreprenør om føring av mannskapslistor.

I statsråd 9.desember 2005 besluttet regjeringen å utsette ikrafttreddelsen av de vedtatte identitetskortene for byggebransjen og ba samtidig om en utredning om hvordan ID-kortene kan gjøres sikrere og bli et godt verktøy mot sosial dumping.

Regjeringen begrunner dette med at tiltak som gjennomføres mot sosial dumping er målrettede og effektive. Et godt system for id-kort på byggeplasser vil være et viktig virkemiddel for å hindre useriøse firmaer i å få innpass i byggebransjen, og et nødvendig bidrag i kampen mot sosial dumping, sier arbeids- og inkluderingsministeren.

ID-kort vil også kunne lette myndighetenes arbeid med å kontrollere at f.eks. helse-, miljø- og sikkerhetskrav på byggeplassene ivaretas. Men forutsetningen for at id-kortene skal få en slik gunstig effekt, må være at kortene har stor tillit og vanskelig å forfalske.

En utredning forventes å foreligge i løpet av seks til tolv måneder med anbefaling om skjerpede krav til ID-kortene.

5.12 Behov i bankene

Bankene har i flere tiår utstedt bankkort som i tillegg til autentisering mot bankkonto også i utstrakt grad benyttes som ID-kort. Et bankkort kan være knyttet til en Bank-ID som er en elektronisk sertifikat for identifisering og signering på internett og tilbys gjennom de fleste banker bl.a. for pålogging til nettbanken.

5.13 Praksis i andre land og verdensdeler

Flere land har startet utvikling og gjennomført utrulling av ”Borgerkort” for hele eller deler av sin befolkning. Det er i hovedsak frivillig å anskaffe kortet og det er ingen land som har regelverk med krav om å bære ID kort for sporadisk kontroll.

Følgende land og praksis nevnes i denne forbindelsen:

- Sverige: utsteder fra 1.oktober 2005 både biometriske pass og ID-kort og benytter samme registrerings- og utleveringsprosess.
- Finland: har hatt et borgerkort i 6 år, og har hatt en sen utrullingstakt på grunn av manglende elektroniske tjenester. I dag koster kortet 40 euro med en levetid på fem år.¹⁰
- Estland innførte i 2002 et obligatorisk borgerkort i den hensikt å få på plass et nasjonalt ID-kort og kortet kan også benyttes som elektronisk identitet på internett og for digital signering av dokumenter.¹¹ De tre baltiske landene forbereder i fellesskap bruk av biometri i nye ID-kort og pass for bruk i Schengen-området.
- I Nederland ved lufthavnen Schiphol tilbys alle reisende et medlemskort for hurtig grensepassering med bruk av biometri og iris kontroll.
- Frankrike: Til tross for å være smartkortets hjemland har landet ennå ikke planene klare, men vil trolig følge den europeiske standarden European Citizen Card
- Malaysia: har hatt et borgerkort i 5 år med samme informasjon som på passet
- USA: biometriske pass kommer på plass i løpet av 2006 Homeland Security har spesifisert såkalte personal identity verification (PIV) ID ansattekort som er utgitt som FIPS 201 standard og også spilt inn til ISO 24727-standard.¹²

¹⁰ <http://vrk.fineid.fi/default.asp?todo=setlang&lang=uk>

¹¹ <http://www.id.ee/pages.php/030301>

¹² <http://csrc.nist.gov/piv-program/>

6 Standardisering

Standard Norge deltar i flere tekniske komiteer som arbeider med teknologiutvikling til støtte ved personidentifikasjon. I hovedsak foregår biometriarbeidet i ISO/IEC JTC1/SC37 Biometrics (se vedlegg 3), men etter avtale mellom ulike komiteer ligger også arbeidsoppgaver i ISO/IEC JTC1/SC27 IT-sikkerhetssystemer og i ISO/IEC JTC1/SC 17 Personidentifikasjon (for kortteknologi), der

- ICAOs arbeid med reisedokumenter utgjør en undergruppe 3 (WG3),
- arbeidet med berøringsfri kortteknologi utgjør gruppe 8
- Homeland Security sine krav utgjør en vesentlig del av arbeidet i gruppe 9 (WG9)
- standardisering av førerkort utgjør gruppe 10 (WG10)

Europeisk direktivutforming følges standardiseringsmessig opp av den felles europeiske standardiseringsorganisasjonen, CEN. Internasjonalt engasjement er nødvendig for å ivareta og opprettholde medlemskap i internasjonale komiteer. Internasjonalt arbeid er ressurskrevende og for å påvirke standardene må det påregnes arbeids- og koordineringsinnsats.

Innenfor fagområdet personidentifikasjon/biometri har Standard Norge opprettet en nasjonal speilkomiteé (K188 Person-ID) for å samordne arbeidet i tre ISO-komiteer og i en CEN-komite. De som arbeider med problemstillingene i internasjonal standardisering, er medlemmer av denne komiteen. I tillegg deltar aktuelle brukermiljø og interesserte under implementeringen av standarder i Norge. Komiteen tar standpunkt til arbeidsforslag og til det reelle innholdet i standardforslagene.

Oversikt over standardene finnes i vedlegg 4 og vedlegg 6.

7. Opplæring

Denne rapporten kan vanskelig gi noen klare føringer for hvordan opplæring innen feltet bør foregå siden det er så mange parter involvert. Imidlertid er mange fagfelt og sektorer berørt av biometri. I politiets arbeid vil biometri bli viktig framover. Derfor anbefales det Politihøgskolen om å ta et særskilt ansvar for opplæring innen justisområdet.

Transportsektoren har ved denne rapporten tatt tak i problemstillinger som er felles for en rekke sektorer. Transport består av ulike modaliteter som bane, vei, luft og sjø, og det vil det være naturlig å videreføre en koordinert opplæring innen transportsektoren. ITS-Norway anbefales å ta et grep her og gjennomføre opplæringstiltak i sine nasjonale konferanser og i regi av faggruppen for Security og Biometri.

8. Konsekvensvurdering og risikovurdering

Det er kun rom for en kortfattet konsekvensvurdering i denne rapporten.

Harmonisering av Person-ID

Dagens utvikling øker behovet for en harmonisert person-ID. Det reisende publikum vil benytte elektroniske løsninger av denne for ulike formål som identifisering ved

flyavgang og på hurtigbåter. Konsekvensen ved å unngå harmonisering medfører at den personlige "floraen" av kort øker videre. Tidspunkt for en gunstig mulig harmonisering er når "noen" (som Arbeids- og inkluderingsministeren) stopper opp og spør om hensikten med *nok et ID-kort* uten sikkerhet. På det nåværende tidspunkt har enkeltinstanser stor forståelse for behovet for harmonisering og en eventuelt norsk standard på området. Det vil bli langt vanskeligere og mer kostnadskrevende om konsekvensen blir at harmoniseringsarbeidet blir utsatt i tid.

Personvernet ved en harmonisert løsning

Utstedelse av ID kort handler om trygghet for den enkelte og kunne stole på den som utsteder løsningen. Publikum kan velge mellom ulike løsninger med ulike tillitsnivå. Personvernet ivaretas spesielt ved at utsteder er sertifisert av relevant myndighet (sivil og/eller militær). Publikum må instrueres med tydelig personlig ansvar for bruken av kortet. Personvernet kan gjøres til et spesielt tema ved harmonisering: Harmonisering fremmer personvernet. Det kan bli et sterkere personvern hvis mange går sammen om omforente løsninger og tilstrekkelig tillitsnivå. Det blir et svakere personvern hvis det blir mange ulike løsninger og et svakere sikkerhets regime for enkelte av disse løsningene.

Et nasjonalt ID-kort med støtte for nasjonal PKI og biometriske elementer kan være en stamme i et identifikasjonssystem som igjen er grunnlaget for at folk kan velge å få utstedt andre ID-kort og identitetspapirer (som bankkort, studentbevis, månedskort osv.).

Økonomiske forhold

Harmonisering vil bli av høyest mulig kvalitet om myndighetene står bak nødvendig kravspesifisering. ITS Norway vil arbeide for at myndighetene tar ansvaret for spesifisering og videre forvaltning av spesifikasjonen. Det finns lignende ordninger for andre systemer som har allmenn anvendelse. Vi kan nevne Håndbok 206 for elektronisk billettering. Det er en av Vegvesenets manualer som er laget for harmonisering av viktige deler for billett transaksjoner, standarder mv. der smartkort benyttes. Spesifikasjonen som er laget for samvirke er fritt tilgjengelig for kommersielle operatørselskaper, og er bekostet av det offentlige. Systemene blir derved tilgjengelig og blir brukt. Det er et økonomisk løft som er tatt av det offentlige og en god modell også for ID området. Det er også gjenbruksmuligheter for ulike delsystemer for eksempel fra Håndbok 206.

Standardisering

Det er ikke et alternativ å søke prosesser som unngår nasjonal og internasjonal standard på dette feltet. Mindre anvendelse av standardisering kan ha fatale følger for ID systemene på lengre sikt. Standardisering på dette feltet er en forsikring for at person ID vil holde internasjonale krav til sikkerhet og funksjonalitet, og at kostnadene ved systemene kan kontrolleres og holdes på et rimelig nivå.

Hvilke umiddelbare konsekvenser ser vi hvis et harmonisert kort ikke innføres i Norge?

For transportsektoren kan det føre til at tendensen som vi ser til mer ukontrollerte leverandør -og spesifikasjonsarbeider vil holde fram. Ulike havner (kommunale og private innkjøp) vil benytte lokale forhandlere (laveste pris, vedlikehold mv). Det er viktig at spesifiseringsprosessen følges opp, og at interesseforeninger søker å presse på slik at myndighetene legger føringer på hvordan innkjøp skal foretas for å ivareta harmonisering.

Risikovurdering for person ID kortet i Norge

Det ligger ikke innenfor rammen av foreliggende rapport å foreta en risikovurdering for etablering av et harmonisert ID-kort i Norge. Dette vil bli utført som en naturlig del av en videreføring.

9 Konklusjoner og anbefalinger

Det er i dette prosjektet foretatt en kartlegging over ulike behov og eksisterende løsninger for person identifikasjon i Norge. Det er også kommet fram i løpet av prosjektet at ulike myndigheter ennå ikke samarbeider i en grad som kan være ønskelig for framdrift for å få fram gode og praktiske løsninger på området.

ITS Norway anbefaler at det utvikles en norsk standardprofil for personbasert ID som er harmonisert med de behov som stilles i transportsektoren.

Standardprofilen må baseres på European Citizen Card og må ta hensyn til ICAO-anbefalingene utgitt av den internasjonale luftfartsorganisasjonen ICAO. ICAO er det sentrale organ på utvikling av maskinlesbare pass til biometriske pass. Politi- og lufthavnmyndighetene i alle land støtter denne standarden.¹³ Profilen kan harmoniseres med Seafarer's Identity Documents (SID).

European Citizen Card som nå er under sluttvotering i den europeiske standardiseringsorganisasjonen. CEN vil ha profiler for et Schengen reise- og identitetsbevis.

Profilen bør harmoniseres med NS 9200 for visuell utforming av ID på et kortformat.

Profilens sertifikatformat bør harmoniseres med de norske "SEID"-spesifikasjonene for Standardisert Elektronisk ID til bruk i PKI.

En detaljert kravspesifikasjon bør utformes på en slik måte at transportoperatører og myndigheter kan benytte denne ved forespørsler om tilbud på ID-kort.

Justisdepartementet bør vurdere å utstede en harmonisert norsk standardprofil som et nasjonalt ID-kort under prosedyren knyttet til søknad om pass.

Produkter som gjør bruk av denne profilen bør vurdere evaluering etter sertifiseringsnivå 14 hos SERTIT – den norske sertifiseringsmyndighet for IT-sikkerhet, underlagt Nasjonal Sikkerhetsmyndighet (NSM). Se www.nsm.stat.no

Dagens praksis med utstedelse av ID-kort basert på "usikre" identitetsdokumenter må snus. Et grunnregister som Passregisteret med kopling til Folkeregisteret bør være basis for å få utstedt andre identitetsdokument (vedlegg 7). Passregisteret bør inneholde utvidet personinformasjon med PKI og biometri iht ICAO logisk datastruktur (LDS) – hver person sin entydige identitet – for blant annet å møte trusselen om identitetstyveri.

Gjennom pågående arbeid og bearbeide konklusjoner fra denne prosjektrapporten bør det interdepartementalt etableres et Nasjonalt ID-kort.

¹³ ICAO Doc 9303 Machine Readable Travel Documents består av 3 deler; del 1: Machine Readable Passports Volume 1; without additional storage, del 2: Machine Readable Passports Volume 2; Specification for Electronically Enabled Passports with Biometric Identification Capability, del 3: Size 1 and size 2 Machine readable Official Travel Documents – seventh edition som utgis årsskiftet 2005/2006. Ved bruk av sixth edition fra 2002 må tillegg av tekniske rapporter for PKI, logisk datastruktur og biometri, publisert i 2004 benyttes.

¹⁴ I henhold til Common Criteria (ISO 15408) Evaluation Assurance Level 4 (EAL 4)

Vedlegg

Vedlegg 1 – Artikkel fra ITS Norway Members Directory & Handbook 2005-2006

“Security and Biometrics – a requirements analysis”

by Ole Folkestad, Avinor and Asbjørn Hovstø, ITS Norway

The demand for better security and safety in transport stems from the new terror situation that has arisen after 11 September 2001.

Main threat is in particular air transport but also sea transport, border control, license to drive a vehicle and access to secure areas have special needs.

Introduction

Authentication using biometrics is the automatic recognition of individual persons based on distinguishing biological (usually anatomical) or behavioral traits. The field is a subset of the broader field of human identification science. Example technologies include, among others: fingerprinting, face recognition, hand geometry, speaker recognition and iris recognition.

At the current level of technology, DNA analysis is a laboratory technique not fully automated and requiring human processing, so it not considered “biometric authentication” under this definition (it is not currently automatic and fast, but may become so in the near future).

Some techniques (such as iris recognition) are more biologically-based, some (such as signature recognition) more behaviourally based, but all techniques are influenced by both behavioural and biological elements.

ITS project

The result of the project is a survey of requirements for ID-documents and biometrics within the transport area thus suggesting actions for harmonisation, education and need for standards.

The survey includes:

- Passports, identification of air crew, seafarers and truck drivers
- Border control
- Security and safety in ports
- Transport of persons
- Access control to highly secured areas

Area descriptions

Increase in travelling, mobility and digital authentication require new methods for person identification. Most countries around the world participate in specification work for person identification using biometrics.

The US-government requires electronic travel documents for visa-free border-crossing. Also government employees and transport workers require stronger schemes for identification and international standards are highly needed.

Preparatory work is done in Europe for a new directive for identification and authentication. New European standards for

“Identification card systems - European Citizen card” a 3-part standard are emerging and ready for final voting.

The international Civil Aviation Organisation (ICAO) is issuing standards for interoperability and security through their bi-annual publication Doc 9303; 6th

edition is to be published including biometrics, PKI and security. All countries in the world must issue Machine Readable Passports compliant to Doc 9303 within the year 2010. From October 1st 2005 Norwegian and Swedish citizens can order ePassports i.e. biometric passports.

The International Labour Organisation (ILO) and International Maritime Organisation (IMO) have published ILO Convention 185 which calls for new and more secure ID cards for seafarers. Only a biometric solution can satisfy the stricter demands for security on board ships and in ports, while at the same time make it simpler to travel to and from ships for seafarers.

Conceptual diagram of a general biometric system

Given the variety of applications and technologies, it might seem difficult to draw any generalizations about biometric systems. All such systems, however, have many elements in common. Biometric samples are acquired from a subject by a sensor. The sensor output is sent to a processor which extracts the distinctive but repeatable measures of the sample (the “features”), discarding all other components. The resulting features can be stored in the database as a “template”, or compared to a specific template, many templates or all templates already in the database to determine if there is a match. A decision regarding the identity claim is made based upon the similarity between the sample features and those of the template or templates compared.

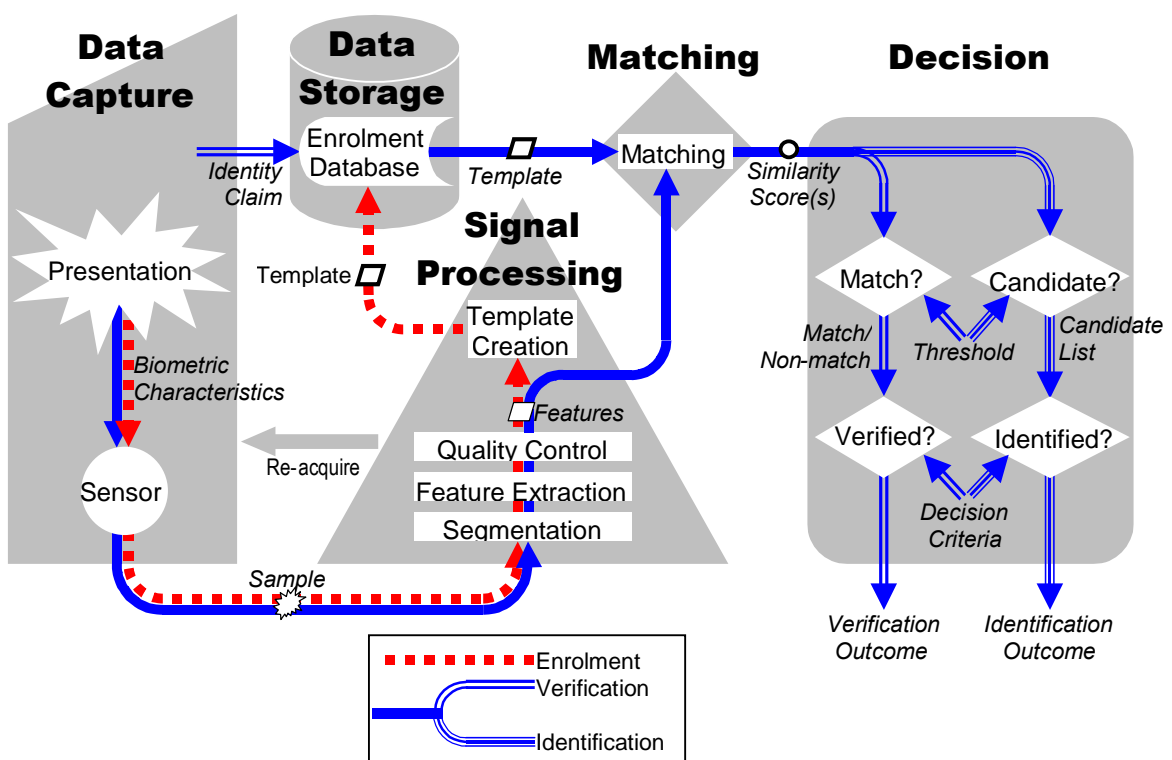


Figure 1 — Components of a general biometric system

Figure 1 illustrates the information flow within a general biometric system, showing a general biometric system consisting of *data capture*, *signal processing*, *storage*, *matching* and *decision* subsystems. This diagram illustrates both enrolment, and the operation of verification and identification systems. In any real biometric system, these

conceptual components may not exist or may not directly correspond to the physical components.

Main threats to security in travel documents

The following list of threats to document security identifies ways in which the document, its issuance and use may be fraudulently attacked.

- Counterfeiting a complete travel document
- Photo-substitution
- Deletion/alteration of text in the visual or machine readable zone of the Machine Readable Travel Document (MRTD)
- The construction of a fraudulent document using material from legitimate documents
- Removal and substitution of entire page(s) of a Machine Readable Passport (MRP) or visas
- Deletion of entries on visa pages and the Observations Page of an MRP
- Theft of genuine document blanks
- Impostors (assumed identity; altered appearance)

To provide protection against these threats and others a travel document requires a range of security features and techniques combined in an appropriate way within the document. Although some features can offer protection against more than one type of threat, no single feature can offer protection against them all. Likewise, no security feature is 100% effective in eliminating any one category of threat. The best protection is obtained from a balanced set of features and techniques providing multiple defences of security in the document that combine to deter or defeat attacks.

Vedlegg 2 ACI – Airports Council International

Introduction

Biometrics is a generic term used to refer to a physiological or behavioural characteristic that can be measured and used to identify an individual. Physiological biometrics measure a part of an individual's anatomy, e.g. fingerprint, hand, face, and iris; and behavioural biometrics measure an action performed by an individual, e.g. voice, signature.

ACI EUROPE position

Position of Europe's airport industry on the application of biometrics for:

Border control

- Europe's airports support the use of an internationally standardised globally interoperable biometric for Machine Readable Travel Documents (MRTDs) and standardised formats for biometric data.
- Europe's airports call for a harmonised approach, building upon ICAO recommendations, for the use of biometric identifiers in MRTDs.
- Biometric systems implemented for border control must not impact negatively on passenger flows through the airport.
- The introduction of biometrics in MRTDs is a national security and immigration issue and consequently the costs of adapting infrastructure at airports in order to be able to accept these new documents must be borne by governments.

Passenger Facilitation

- Europe's airports see merit in the integration of biometrics for the purpose of border control procedures with air carrier check-in and boarding processes, and thus urge air carriers, regulators, and border control authorities to work together with airports to ensure that the goals of enhancing passenger security and facilitating quicker passenger flows are realised.
- Europe's airports strongly encourage the use of common user systems by air carriers in order to avoid the proliferation of dedicated biometric systems for self service check-in points and for check-in and boarding check points. Such proliferation will be avoided by the adoption of a common use biometric template in MRTDs.

Staff access control

- Europe's airports call upon national and EU regulators to take into account the potential benefits of implementing biometrics systems for enhancing security at airports. The implementation of other security measures must not preclude the use of biometrics technologies where they can deliver tangible benefits.
- Europe's airports consider that regulators must simply determine the security objectives and leave airport operators to investigate and implement the biometric technology that best suits the local conditions that characterise each individual airport.

Understanding biometrics

1. The principle of using any biometric for the purpose of identification is the same. Enrolment process: the individual provides a sample of the biometric which is captured by a device (e.g. a camera or a scanner). Information is extracted from this sample to create a template which is recorded on a storage medium (e.g. chip or barcode). Authentication process: The individual provides a sample of the biometric previously

recorded on the storage medium. The template created from this sample is compared to the (stored) reference template. As no two templates are exactly identical, the authentication process must determine whether the samples are a close match.

2. In terms of the main objective of biometrics systems, i.e. the authentication process, the challenge is to achieve a high level of accuracy in the identification of any given individual. This involves developing a system that overcomes two key problems: 1) incorrectly matching a sample template of one individual with the reference template for another individual (False Acceptance Rate), and 2) failing to recognise a match between a sample template of an individual with the reference template of that same individual (False Rejection Rate).

Requirements for the use of biometrics

Performance

3. The performance of biometric systems must improve the rigour of passenger and airport employee checks in a significant manner, ease the fluidity of processing and at the same time reduce costs by automation of the operations. To reach this objective, the adopted technologies must display the following characteristics: high level of performance measured in operational conditions and on a large scale, ease of use and acceptance by the users, protection against fraud, and reduced processing time.

4. The issue of biometric performance however is often subjective depending on the source. Even when comparing biometric technologies using False Acceptance Rates and False Rejection Rates, the result can often still be inconclusive. This is why it is important to develop standards for the use of biometrics, so that their application in the airport environment, for security or facilitation purposes, can be executed with a high degree of confidence in the system.

Standards

5. Taking the diversity of the technologies and manufacturers into account, the deployment of biometric systems must be in line with international standards, as much for the transfer and storage of information as for the measurement of performance, so as to guarantee market access (competition), interoperability between suppliers and the capacity for deploying biometrics over the whole employee and passenger processing chain (border control, boarding checks, access checks, etc.). This condition is essential for the continuity of the biometric systems deployed and for the upgradeability of the technologies. The European Union should take a lead role in the development of such standards.

ICAO recommendations

6. Regarding the choice of technology, the direction given by the ICAO (face recognition - as the primary biometric interoperable identifier - and one or two additional, but optional, biometric identifiers - fingerprint and/or iris) must not lead to an increase in the number of technologies, as this risks making the systems more complex, both for passengers and operators, and risks increasing the cost. The choice of two biometric technologies for passports seems to be a good compromise between the required global interoperability and the complexity of the systems, including other requirements such as passenger security profiling.

Technology

7. From a commercial perspective, it would be desirable for a number of biometric technologies to be selected, thus avoiding a single vendor taking advantage of their monopolistic position. The 'desirable' solution would be where a single technology infrastructure supported multiple biometric acquisition technologies seamlessly and transparently. The reality is that this is not possible without significant development effort by – one would assume – an independent technology integration company. However, in principle, this goal is achievable with the correct level of investment and sponsorship.

Cost

8. The costs of a biometric system, apart from the investment in equipment, equally concern:

- Its integration in the operational employee and passenger processing procedure (interfaces);
- The infrastructure required for enrolment and control, particularly at airports where the availability in space is often limited; and
- The costs of qualified personnel, including training and maintenance.

9. National governments must take on the financing of biometric systems which contribute to the implementation of the tasks on which it is incumbent for them to do, particularly border control. The source of the financing should not be limited to the strict basis of air passengers, as the biometric systems, to fully reach their assigned objective, should be extended in parallel with other forms of transport (road, maritime) in a coordinated manner.

Application of biometrics

Border control

10. The case for border control is relatively simple and straightforward. As ICAO has recently determined a standard for the use of biometrics in Machine Readable Travel Documents (MRTDs) it seems only wise to accept ICAO's decision and prepare a standpoint on the use of biometrics for border control at airports. The fact that the introduction of biometrics in MRTDs is a pure government issue implies that the costs of adapting the passport control booths at airports to be able to accept these new documents must be borne by governments.

11. Due to ICAO resolutions and the European Commission proposals on biometrics requirements for travel documents, soon all European airports will have to install and to manage biometrics systems to complement the more traditional identification procedures at airports. ACI EUROPE welcomes the fact that the European Commission's recent proposals on biometrics for visas and residence permits for third-country nationals are consistent with the ICAO approach.

Passenger Facilitation

12. The use of biometrics for passenger facilitation will mainly benefit air carriers (through frequent flier programmes) or, in most EU Member States, government authorities (as discussed above). Airport operators will only have secondary benefits from the use of biometric systems in passenger handling, since passengers will be handled more conveniently and quickly, which will certainly have an impact on the image of the airport.

13. Checking that a passenger's identity is consistent across all the processes - check-in, border crossing, passenger security check and boarding the aircraft - is key for ensuring

that the right person is boarding the right aircraft and that the person boarding is also the same person who has undergone all of the earlier processes. If the passenger uses the same 'token' in all these processes, it is quite obvious that there are benefits to be gained.

14. As the use of a travel document is quite widespread in other processes at airports and even within airline processes, it can be foreseen that MRTDs with biometric identifiers will swiftly be incorporated into these processes. The normal chain of processes that a passenger undergoes at an airport shows that a passport is not only used for border control; the check-in process has a link with the passport as does the boarding process. Airport operators and air carriers should work together to ensure that regulators apply the same biometric identifiers for border control as for the check-in and boarding processes in order to facilitate quicker passenger flows.

15. In terms of air carrier frequent flier programmes, airport operators encourage air carriers to employ common user systems to avoid the proliferation of biometric systems at dedicated self service check-in points and dedicated check-in and boarding check points. The use of common biometric templates for air carrier frequent flier programmes should be considered. The integration of MRTDs into the airline process may render redundant the need to use an additional frequent flier card.

Security access control

16. In its most basic form, airport security managers are looking for a solution which ensures that flight crew and airport personnel are positively identified or verified and granted appropriate access into security restricted areas. Until now, airport security for staff access has been reliant on a series of tried and tested procedures coupled with conventional token or PIN-based access control security solutions. With the recent emergence of biometric identification technology a new capability is introduced, enabling security managers to allow access to secure areas on the basis of who an individual is as opposed to what they are carrying or what they know.

17. The performance of the biometric application for access control is extremely important since, unlike the passenger handling process, access control points for employees can be automated and therefore do not necessarily have to be manned by security staff, unless otherwise required by national law.

18. Biometric technology for security access control in airports has been applied relatively slowly due to three key factors: 1) over-promise and under-delivery of biometric technology vendors 2) fast progress of biometric technology capabilities and 3) the lack of a cohesive approach from regulating bodies.

19. The first problem has already started to dissipate as vendors become wise to the fact that for a technology to be adopted on a mass scale, the 'customer' must be made aware of the strengths as well as the weaknesses of the technology they represent; all too often trials dash the expectations set of security managers. The second factor is being mitigated as the leading biometric contenders for various application areas become apparent; however, an element of risk – albeit an informed risk – will always exist in the selection decision. The third factor is the biggest cause for concern as this is where the greatest single influence resides: without the appropriate level of steer from regulators, airports will remain intransigent on the decision of adopting biometric technology.

20. Regarding the last point, it is a concern of some airport operators that the use of biometric systems for controlling access of employees to the security restricted area of an airport only makes sense if 'critical parts' – to be defined in accordance with the EU

Regulation 2320/2002 on civil aviation security – apply to the terminal area only. This is because, access control points to these critical parts must be occupied by security staff that must screen personnel for prohibited items and can therefore also identify staff instead of a biometrics system. Biometric systems can help security staff to perform effectively staff identification in the same way as practiced for border control.

21. For the reasons above, Europe’s airports consider that the role of national and EU regulators must be to simply determine the security objectives, whilst taking into account the potential benefits of biometrics systems for enhancing security. The choice and application of biometrics for security at airports, however, must be left to airport operators. Airport operators must be able to investigate and implement the biometric technology that best suits each individual airport, and furthermore must be able to determine whether the implementation of biometrics technologies can deliver tangible benefits, as opposed to other security measures.

Airports Council International (ACI) is the only worldwide professional association of airport operators. ACI EUROPE represents over 450 airports in 45 European countries. Member airports handle 90% of commercial air traffic in Europe, welcoming over a billion passengers each year.

Vedlegg 3 – Brief summary of International Standards activity Background on Biometrics standardization

Much of biometrics standardisation was initiated in the USA, but in 2002 a new ISO/IEC JTC1 Sub-committee was established - SC37, and first met in Orlando in December 2003. The following is from the SC37 Web site.

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National Bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity.

ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, government and non-governmental, in liaison with ISO and IEC also take part in the work.

In the field of information technology, ISO and IEC have established a Joint Technical Committee 1: ISO/IEC JTC1 on Information Technology. In June 2002, JTC1 established a new Subcommittee 37 on Biometrics. The goal of this new JTC1 SC is to ensure a high priority, focused, and comprehensive approach worldwide for the rapid development and approval of formal international biometric standards. These standards are necessary to support the rapid deployment of significantly better, open systems standard-based security solutions for purposes such as homeland defence and the prevention of ID theft.

The intended area of work is the standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects.

Layers or areas of biometric standardization and Working Groups

There is not yet an agreed layered model for the SC 37 biometrics work (but see clauses 2 and 3 for a model of a biometric system), but the following is proposed in this tutorial. For a slightly different layered relationship of SC 37 standards, please refer to ISO/IEC 24713-1: Biometric Profiles for Interoperability and Data Interchange: Biometric Reference Architecture (see A.27 below).

For the purposes of this tutorial, we recognise four levels of biometric standardisation, plus other areas related to societal and privacy issues. The layering is largely based on dependencies for implementation of the Standards, with implementation of those in a higher layer dependent on implementation understanding or implementation of a lower layer Standard. Societal and privacy issues are outside this layering structure.

This tutorial recognises layer 1 as BDB (Biometric Data Block) format standards, layer 2 as CBEFF (Common Biometric Exchange Formats Framework) data elements and BIR formats, layer 3 as the BioAPI (Biometrics Application Programming Interface) architecture and standard interfaces for a biometric system, and layer 4 as the BIP (Biometric Interworking Protocol) for interchanges between biometric systems.

This tutorial also identifies other areas (related to societal and privacy issues) in which standards or technical reports are being produced, but which do not fit naturally into the above layering.

The work is organized into the following Working Groups:

WG1 - Harmonized Biometric Vocabulary and Definitions

WG2 - Biometric Technical Interfaces (Layer 2, 3, and 4 Standards)

WG3 - Biometric Data Interchange Formats (Layer 1 Standard)

WG4 - Study Group on Profiles for Biometric Applications

WG5 - Biometric Testing and Reporting

WG6 - Study Group on Cross-Jurisdictional and Societal Aspects

Layer 1 Standards (approved or in preparation for initial standards)

19794-1: Biometric Data Interchange Format: Framework

19794-2: Biometric Data Interchange Format: Finger Minutiae Data

19794-3: Biometric Data Interchange Format: Finger Pattern Spectral Data

19794-4: Biometric Data Interchange Format: Finger Image Data

19794-5: Biometric Data Interchange Format: Face Image Data

19794-6: Biometric Data Interchange Format: Iris Image Data

19794-7: Biometric Data Interchange Format: Signature/Sign Behavioral Data

19794-8: Biometric Data Interchange Format: Finger pattern Skeletal Data

19794-9: Biometric Data Interchange Format: Vascular Biometric Image Data

19794-10: Biometric Data Interchange Format: Hand Geometry Silhouette Data

19794-11: Biometric Data Interchange Format: Signature/Sign processed dynamic data

Layer 2 Standards (approved or in preparation for initial standards)

19785-1: Common Biometric Exchange Formats Framework (CBEFF): Data Element Specification

19785-2: Common Biometric Exchange Formats Framework (CBEFF): Procedures for the Operation of the Biometrics Registration Authority

19785-3: Common Biometric Exchange Formats Framework (CBEFF): Patron Format Specifications

Layer 3 Standards (approved or in preparation for initial standards)

19784-1: BioAPI - Biometric Application Programming Interface: BioAPI Specification

19784-2: BioAPI - Biometric Application Programming Interface: Biometric Archive Function Provider Interface

24709-1: BioAPI Conformance Testing: Methods and Procedures

24709-2: BioAPI Conformance Testing: Test Assertions

24722: Multi-Modal Biometric Fusion

Layer 4 Standards (approved or in preparation for initial standards)

24708: Biometric Interworking Protocol (BIP)

Other Standards and Technical Reports (approved or in preparation for initial standards)

Harmonized Biometric Vocabulary

Biometric Vocabulary Corpus

19795-1: Biometric Performance Testing and Reporting: Principles and Framework

19795-2: Biometric Performance Testing and Reporting: Testing Methodologies

19795-3: Biometric Performance Testing and Reporting: Specific Testing Methodologies

19795-4: Biometric Performance Testing and Reporting: Specific Test Programmes

24713-1: Biometric Profiles for Interoperability and Data Interchange – Part 1: Biometric Reference Architecture

24713-2, Biometric Profiles for Interoperability and Data Interchange – Part 2: Physical Access Control for Employees at Airports

24713-3, Biometric Profiles for Interoperability and Data Interchange – Part 3: Seafarer's ID

24714: Multi-part Technical Report on Cross Jurisdictional and Societal Aspects of Biometric Technologies

Vedlegg 4 – ILO strategy paper – Seafarer’s ID (SID)

The International Labour Organization, established in 1919, is a specialized agency of the United Nations (UN). It is a tripartite organization in which representatives of governments, employers and workers take part with equal status. In the wake of the terrorist attacks of 11 September 2001, the International Labour Organization took steps to revise its 1958 Convention on seafarers’ identity documents (also known as “seafarers’ IDs” or “SIDs”), under an accelerated procedure. The new Convention, the Seafarers’ Identity Documents Convention (Revised), 2003 (No. 185), which was adopted by the International Labour Conference in June 2003, introduced modern security features into the seafarers’ ID to help to resolve the urgent question of seafarers being refused admission into the territory of countries visited by their ships for the purposes of shore leave and transit and transfer to join or change ships. One of those security features is a fingerprint biometric template, which shall be printed as numbers in a PDF417 bar code “conforming to a standard to be developed” (Convention No. 185, Annex I).

In a resolution adopted by the International Labour Conference in June 2003, the ILO Director-General was requested to take urgent measures “for the development by the appropriate institutions of a global interoperable standard” for the biometric template referred to above, particularly in cooperation with the International Civil Aviation Organization (ICAO). At a meeting held at the ILO in September 2003, which was attended by representatives of Governments, Shipowners, Seafarers, ICAO and ISO, it became clear that ICAO, which was proceeding with a recommendation for a different biometric solution (see below) as the standard for machine-readable passports, was not in a position to take an active part in the development of the template required by the new seafarers’ ID. It was also noted that the urgent time frame required for the entry into operation of Convention No. 185 precluded a resort to the normal procedures for the development of such a template in the framework of the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC).

The ILO has consequently commissioned this technical report to reflect the requirements generated by the seafarers’ IDs Convention in 2003, which outlined highlevel requirements for biometric-based personal identification of the international seafarer community. The authors submit this technical report, ILO SID-0002 rev. 02, in the form of a biometric profile defining the standard for generating and storing minutiae-based fingerprint templates on the PDF417 2-D bar code of the next-generation SID and in the Member’s national electronic databases (Convention No. 185, Annex I and Annex II, respectively). This biometric profile is organized in near-ISO-standard-compliant form that can be matured into a standard and then into a procurement document following international discussion and harmonization of the requirements.

Various studies, experiments, pilot programmes and products have been developed in recent years in attempts to expedite the inspection process at border management points. Many efforts will incorporate biometric technology into next-generation travel documents and international identification documents. The ILO drafted and approved Convention No. 185 to define requirements for the next-generation seafarers’ IDs, which will incorporate biometric-based personal identification for the seafarer (document holder) and store biometric templates in a bar code printed on the SID.

Prior to 11 September 2001, the biometrics industry had initiated several standards development projects to facilitate the development of interoperable biometrics products and systems, as well as the interchange of biometrics data objects between products and systems and requirements for ensuring the integrity and privacy of biometric data.

✍ ISO/IEC FCD 19784 – Information technology – Biometric application programme interface (BioAPI) (ISO/IEC JTC 1 SC37 N number 55, 1 dated 17 December 2002), which provides an application programming interface that assures that conforming products and systems can interoperate with each other. (This is also a final American

National Standards Institute/International Committee for Information Technology Standards standard: ANSI/INCITS 358:2002 – Information technology – BioAPI specification).

✍ ISO/IEC CD 19785 – Information technology – Common biometric exchange formats framework (CBEFF) (ISO/IEC JTC1 SC37 N 208, dated 14 July 2003).

✍ ISO/IEC CD 19794-2 – Biometric data interchange formats – Part 2: Finger minutiae data (ISO/IEC JTC 1 SC37 N 340, dated 7 October 2003).

✍ The International Civil Aviation Organization (ICAO) standard (document 9303) for machine-readable travel documents (MRTDs), commissioned by ISO/IEC JTC1 SC17.

Note: The latest recommendation of ICAO is to include contactless smart card technology in next-generation travel documents and to include one or more biometrics (the facial biometric is required by the ICAO MRTD standard and either fingerprint or iris recognition systems could also be incorporated). While the ILO seafarers' ID is an identity document (and not a travel document), the ILO will attempt to follow the ICAO-proposed standard for next-generation MRTD where possible. It is important to note that the next-generation ILO seafarers' ID will use bar code technology to store biometric data (not the embedded chip technology recommended by ICAO's MRTD standard). This difference significantly impacts the SID biometric profile. While bar code storage is less expensive than embedded chip storage, there is significantly less storage capacity available on the SID PDF417 bar code than there is in ICAO recommended embedded chip storage.

Because the next-generation ILO seafarers' IDs will use bar code technology to store biometric data and support the ILO's international interoperability requirements of the SID, this biometric profile defines the format for PDF417 bar code storage of fingerprint templates. Consequently, ISO/IEC 15438:2001 (PDF417 bar code symbology) and ISO/IEC FDIS 15415 (PDF417 bar code print quality) are fundamentally applicable to this biometric profile.

Together the standards ISO/IEC 15438:2001, ISO/IEC FDIS 15415, ISO/IEC CD 19794-2 and ICAO 9303, represent the foundation upon which the biometric capabilities of the seafarers' ID systems will be built. Other standards either already developed (such as ANSI/INCITS 358:2002 – Information technology – BioAPI specification) or being developed in parallel with this one, such as the ISO/IEC WD 19794-4 – Biometric data interchange formats – Part 4: Finger image-based interchange format (ISO/IEC JTC 1 SC37 N 341, dated 7 October 2003) will also be relevant as incorporated below.

Determination of the SID fingerprint biometric technology option

ILO Convention No. 185 requires that the SID be internationally interoperable. The Convention precludes the use of fingerprint images. Therefore, the ILO had to choose between finger minutiae-based or finger pattern-based templates as the basis of procurement for the next-generation seafarer's ID. This report, ILO SID-0002, represents the technical requirements for the finger minutiae-based biometric option, which has been selected as the best solution for the ILO SID implementation.

ISO/IEC 24713-3, Biometric Profiles for Interoperability and Data Interchange – Part 3: Seafarer's ID vil være den nye standarden på området.

Vedlegg 5 – European Citizen Card – ECC

CEN TC224: Identification card systems . European Citizen Card.

Part 1: ECC Physical, Electrical and Transport Protocol Characteristics

Part 2: Logical data structures and card services

Part 3: Management of the card and services

The documents specify the logical characteristics and security features at the card/system interface for the European Citizen Card.

The European Citizen Card is a smart card with Identification, Authentication and electronic Signature (IAS) services. Therefore:

- The supported services are specified
- The supported data structures as well as the access to these structures are specified
- The command set is defined

The document has the objective of ensuring the interoperability at card/system interface in the usage phase. In order to reach the interoperability objective, IAS services are compliant to CWA 14890 part 1 and part 2. As the CWA documents offer options, this specification fully defines a complete profile. This specification also provides other features not defined in the CWA documents (biometric on card matching, command chaining, role authentication).

This specification is also compliant with ICAO specification (authentication methods, basic access control).

This specification does not mandate the use of a particular technology, and is intended to allow both Native and Java card technologies.

This specification encompasses mandatory and optional features. Optional features make up a toolbox of modular options from which issuers can pick up the necessary protocols to fulfil the requisites of their use cases. Mandatory features are necessarily to be implemented for a smart card to be compliant to this specification. Two IAS-enabled smart cards issued by two different issuers, and compliant with this specification but implementing different modular options out of this specification, can interoperate with a terminal provided such a terminal supports both options. Therefore, interoperability requires a specific agreement between issuers/Governments in order to determine which cross-border services are to be shared, and consequently which protocols are to be supported by the terminals in each country.

All the APDU commands described in this document are in accordance with ISO/IEC 7816 Part 4 or Part 8.

They are fully described here in order to provide the settings adopted by this specification and to prevent any ambiguity in case of several possible interpretations of the standards.

For physical, electrical and transport protocol characteristics, refer to Part-1 of this specification. An informative annex illustrates three different profiles corresponding to two usage profiles for the ECC considered representative of the real operation of the card:

- Profile 1 - an ECC National ID card with only a contact interface;
- Profile 2 - an ECC Daily Life card with a dual interface;
- Profile 3 - an ECC issued as a Visa Schengen Card.

Tests which include cycles designed according to this informative annex are not intended to replace ordinary tests such as qualification or functional performance ones.

It is noted that logical testing are out the scope of this Informative annex.

Normative references

ISO/IEC 7810, Identification cards - Physical characteristics
ISO/IEC 7812, Identification cards - Identification of issuers
ISO/IEC 7816-1, Identification cards - Integrated circuit(S) card(S) with contacts - Part 1 : physical characteristics
ISO/IEC 7816-2, Identification cards - Integrated circuit(s) cards with contacts - Part 2 : Dimensions and location of the contacts
ISO/IEC 7816-3, Identification cards - Integrated circuit(S) cards with contacts - Part 3 : electronic signals and transmission protocols
ISO/IEC 7816-4, Identification cards - Integrated circuit(S) cards with contacts - Part 4 : interindustry commands for interchange
ISO/IEC 7816-5, Identification cards - Integrated circuit(s) cards with contacts - Part 5 : numbering system and registration procedure for application identifiers
ISO/IEC 7816-6, Identification cards - Integrated circuit(s) cards with contacts - Part 6 : interindustry data elements
ISO/IEC 7816-8, Identification cards - Integrated circuit(s) cards with contacts - Part 8 : security related interindustry commands
ISO/IEC 7816-9, Identification cards - Integrated circuit(s) cards with contacts - Part 9 : additional interindustry commands and security attributes
ISO/IEC 7816-11, Identification cards - Integrated circuit(s) cards with contacts - Part 11: Personal verification through biometric methods
ISO/IEC FDIS 7816-12, Identification cards - Integrated circuit(s) cards with contacts - Part 12 : USB electrical Interface and operating procedure
ISO/IEC 7816-15, Identification cards - Integrated circuit(s) cards with contacts - Part 15: Cryptographic information application
ISO/IEC 10373-3, Identification cards - Test methods - Part 3 : integrated circuit(s) cards with contacts and related interface devices
ISO/IEC 10373-6, Identification cards - Test methods - Part 6 : proximity cards
ISO/IEC 14443-1, Identification cards. Contactless integrated circuit(s) cards. Proximity cards. Part 1:Physical characteristics.
ISO/IEC 14443-2, Identification cards. Contactless integrated circuit(s) cards . Proximity cards. Part 2: Radio frequency power and signal interface.
ISO/IEC 14443-3, Identification cards. Contactless integrated circuit(s) cards. Proximity cards. Part 3:Initialization and anticollision.
ISO/IEC 14443-4, Identification cards. Contactless integrated circuit(s) cards . Proximity cards. Part 4: Transmission protocol..
FDIS ISO 18013-1 Personal Identification-ISO compliant Driving Licence-Part 1: Physical characteristics and basic data set – Part 2: Biometrics profile
ISO/IEC 24727 – Identification Cards – Integrated circuit card programming interfaces; part 1: Architecture – Part 2: Generic Card Interface – Part 3: Application Interface – Part 4: API Administration – Part 5: Testing
ICAO 9303 sixth edition part 1 Volume 1 Machine Readable Passports without additional data storage
ICAO 9303.sixth edition part 1 Volume 2 Specifications for Electronically Enabled Passports with Biometric Identification Capability
CWA 15264 Parts 1,2,3
UTI X 509v3, Key Infrastructure Certificate and CRL profile
CWA 14890 parts 1 and 2
CWA 14169
European Parliament and the Council of 13 December. Directive 1999/93 EC on a Community framework for electronic signatures
European Parliament and the Council of 12 July. Directive 2002/58 EC on privacy and electronic Communications
European Parliament and the Council of 24 October 1995 - Directive 95/46/EC on data protection

Vedlegg 6 – Terminologi og begrep – Danmark

IT Brancheforeningens Biometri-ordbog

Kilder: International Association for Biometrics (iAfB) Findbiometrics.com
Redigeret november 2005 / Flemming Rud, DURCOM

INDLEDNING

Denne ordbog har til formål at opstille de biometriske kendetegn og teknologier, der arbejdes med i dag samt forklare de termer og sproglige udtryk der anvendes indenfor området. Ordbogen er udarbejdet af biometrisk udvalg under IT-Brancheforeningen.

Ordbogen er inddelt i tre afsnit; Biometriske kendetegn, Biometriske teknologier, Biometriske termer

Hele ordboken kan finnes og lastes ned fra

<http://www.itb.dk/sw8738.asp>

Vedlegg 7 – Menneskers identitet – Noen betraktninger

av Odd Stormorken

Innledning

De fleste mennesker i den utviklede verden vil trolig være enig i at det er en fordel at alle borgere har en og kun en identitet, og at denne er entydig bestemt. Samtidig vil de være opptatt av at de på en enkel og pålitelig måte, i alle situasjoner, kan bevise sin identitet overfor andre borgere og myndigheter, og at andre på samme måte kan bevise sin identitet overfor dem. Sist, men ikke minst, vil borgerne være opptatt av at ingen, myndighetene inkludert, kan misbruke identiteten deres.

Det antas videre at det er viktig for myndighetene i et land at de har oversikt over hvem som er statsborgere og/eller har andre plikter eller rettigheter i forhold til å betale skatt, motta ytelser, stemme ved valg og andre tilsvarende forhold. I dag ivaretas basisfunksjonene i registreringen av Folkeregisteret, og trolig er det helt avgjørende at det finnes ett slik felles basisregister som grunnlag for borgernes identitetsfastsettelse. Det at alle borgere er registrert i dette registeret, og samtidig registret kun en gang, antas også å være viktig.

Det at informasjonen som er registrert i dette sentrale registeret danner grunnlag for utstedelsen av et instrument som borgerne kan benytte til å bevise sin identitet, anses som en forutsetning om det skal være sammenheng i systemet. Som en følge av dette må også instrumentet tilbakekalles og endres om det innholdet i registeret som inngår i instrumentet senere skal endres. I praksis blir det tilnærmet bare ved navneendringer dette blir aktuelt, men noen andre sjeldne tilfeller kan tenkes.

Samtidig som man avgjør hvordan et ID-instrumentet blir utstedt til innehaveren, må man også diskutere og lage regler for videre bruk av dataene og registrering i den forbindelse. Det vil med andre ord være et prosessuelt skille mellom hvordan en persons identitet bestemmes, registreres i basisregisteret og ID-instrumentet utstedes, og på den andre siden, hvordan identiteten og dataene deretter brukes i det daglige liv.

Det ID-instrumentet som beskrives her vil aldri kunne benyttes i alle sammenhenger der innehaveren har et behov for å legitimere seg. Det er både teknologiske, praktiske og etiske grunner til det. Det vil imidlertid kunne tjene som basis når innehaveren henvender seg til firma og/eller tjenesteytere for å få utstedt andre instrumenter til bruk i andre systemer, gitt at slike systemer setter krav til identitetsopplysninger.

Frivillighet er også et tema for diskusjon. At det skal være frivillig å bære det på seg er nok selvsagt i Norge. Frivilligheten til registrering er noe annet. Det er definitivt ikke frivillig å stå i folkeregisteret, men kanskje skal det være frivillig å registrere seg med biometriske data. Det blir imidlertid da et problem med å få pass.

Nasjonal infrastruktur

Det ID-instrumentet som utstedes til borgerne, trolig i noen få varianter over en felles lest, bør betraktes som en del av en nasjonal infrastruktur som myndighetene stiller til rådighet. Naturlig nok vil dette måtte koste borgerne noe, på samme måte som andre offentlige tjenester, men i dagens og framtidens samfunn vil vi alle ha behov for et slik

instrument. De metoder og systemer for identifisering som har vært brukt til nå, holder ikke mål lenger. Utviklingen av et mer globalisert levesett, mindre generell tillit til medmennesker og ikke minst den virtuelle verden vi nå etter hvert tilbringer mye tid i via digitale nettverk, er hovedgrunnene for dette.

Dette er også hovedgrunnen til at ID-instrumenter utstedt av kommersielle firma eller organisasjoner og som ikke har noe formelt myndighetsstempel, ikke vil kunne tjene samme hensikt. Disse har rett og slett ikke det nødvendige tillitsfundament som vil kreves. Det at de også som regel har utsteders firmanavn etc. som en del av designen, er også med på å slå bena unna den generelle aksepten som ID-instrument. Det blir rett og slett konseptuelt feil å signere et offentlig dokument eller en forretningsavtale, krysse en grense, "logge seg inn" i et helseforetak eller utføre andre tilsvarende handlinger med et ID-instrument man har fått utstedt av et kommersielt firma i en helt annen hensikt.

Reisedokumenter

Reisedokumenter, primært pass, utstedes av landets myndigheter for sine borgere. I Norge er det politiet som utsteder pass (Utenriksdepartementet utsteder diplomatpass, spesialpass og servicepass, mens Utlendingsdirektoratet i samarbeid med politiet utsteder utlendingspass og reisebevis.) I dag kan man søke om pass hos alle politi- og lensmannsenheter, ca. 400 steder i landet. Passregisteret er politiets eget register, og ansvaret for dette ligger dermed under Justisdepartementet. Folkeregisteret brukes for oppslag ved utstedelsen.

For reisedokumenter kommer det nå betydelig høyere teknologiske krav i form av bl.a. biometriske data som skal lagres inn i en kontaktløs chip i dokumentet. Disse kravene er basert på internasjonale standarder som Norge må tilpasse seg. Dette betyr at innregistrering og kontroll i denne forbindelsen må bygges ut. Trolig vil politikerne innse, før det er for sent, at det å bygge ut dette på rundt 400 steder er illusorisk. Hovedsakelig på grunn av kostnadene, men også på grunn av at de som skal betjene det nye systemet må ha kontinuerlig trening i å operere det. Bestiller de pass til noen få personer i året, noe som er situasjonen på små bestillersteder i dag, er det lite trolig de vil få og beholde tilstrekkelig operasjonell kunnskap og erfaring.

Trolig ender vi med at man kan bestille pass fra 50-80 politienheter på landsbasis. Disse vil bli bygget ut med nødvendig teknisk utrustning, og bemannet med personell som er spesialister på det å fastsette/registrere identitet og igangsette utstedelse av ID-dokumenter. Profesjonell utførelse av denne jobben er helt avgjørende for kvaliteten på det dokumentet som kommer ut, og dermed tilliten til systemet totalt sett.

Register og registrering

Folkeregisteret bør organiseres på en måte slik at det blir et felles ID-register for hele samfunnet. Den informasjonen som i dag ligger i passregisteret må også inkluderes i Folkeregisteret for at dette skal bli komplett. Dette betyr med andre ord at registerets oppgaver og innhold blir utvidet. Om dette betyr at registeret organisatorisk bør ligge et annet sted enn under Skattedirektoratet/Finansdepartementet som i dag, eller det må gjøre andre organisatoriske grep, må vurderes av noen som kjenner dagens system godt.

Poenget med en slik utvidelse av Folkeregisteret er at registeret blir basissystemet for alle ID-instrumenter i Norge. Derfor må de elementene som knytter en fysisk person til hans eller hennes personalia - bilde, signatur og biometriske data - registreres sammen med disse personaliene.

Innføring i registeret vil skje i minimum to steg. Første steg vil bli en basisregistrering med tildeling av fødselsnummer og registrering av data for nyfødte og innflyttede fra utlandet. I tillegg må de som skal innføres i registeret gjennom en sekundær prosess der den fysiske personen blir knyttet til identiteten ved at foto, signatur og biometriske data legges til. Trolig vil basisregistreringen og den sekundære registreringen skje med noe tids mellomrom. Dette kan dreie seg om flere år for nyfødte og mindreårige.

I dag finnes det systemer som fanger opp det som ovenfor kalles basisregistrering. Det samme gjelder for endringer av basisdata etter første gangs registrering, og denne type endringer vil sjelden innvirke på utstedte ID-instrumenter. Trolig kreves det derfor ikke store endringer for å videreføre denne basisprosessen.

Denne sekundære prosessen bør skje hos politiet. Det er flere grunner til det, men stordriftsfordelen og rasjonaliteten i å gjenbruke utstyr, systemer og trent personell som uansett kreves til reisedokumenter (pass) er den viktigste grunnen. Trolig vil terskelen for å "prøve seg" med noe hos politiet også være høyere enn på et "vanlig" offentlig kontor, noe som er en annen grunn for å utnytte politiet. Kvaliteten på data i systemet blir dermed bedre.

En følge av at politiet brukes til den sekundære registreringsprosessen er at det må lages organisatoriske avtaler mellom Folkeregisteret og politiet, eventuelt at enhetene slås sammen på et vis. Dette er også nevnt ovenfor.

Om det skal være noe krav til når en mindreårig må være registrert i den sekundære prosessen, og at dermed bilde, signatur og biometriske data blir lagt til personaliene i Folkeregisteret, er et tema for diskusjon. En løsning ville være å si at det skal gjøres innen man fyller 16 år. Uansett ville registrering skje ved utstedelse av pass, så derfor er det i praksis neppe mange igjen på 15 år som ikke er registrert allerede.

Problemområder

Med en løsning som skissert ovenfor vil Folkeregisteret bli inneholdende bilde, signatur og biometriske data for personen, og spørsmålet er om det er et problem? Etter mitt skjønn er det ikke det, for om man legger sammen Folkeregisteret og dagens eller fremtidens passregister, så har man alt disse dataene uansett. Politiet bruker dette allerede. Dette er også grunnen til at det bør vurderes om Folkeregisteret burde ligge under justissektoren og ikke under finanssektoren som i dag.

Det man kan diskutere er hvilke og hvordan biometriske data skal lagres i registeret, enten som et komplett datasett eller som en template (et datakonstruert "utdrag") der det komplette grunnlaget ikke kan gjenskapes ved å reversere beregningsprosessen. Her er det argumenter for begge alternativene. Videre kan det diskuteres hvem som skal ha adgang til dataene i Folkeregisteret, men dette er et spørsmål man må finne svar på i dag også. Problemet blir dermed neppe annerledes enn det er nå.

Konklusjonen blir dermed at det er vanskelig å se at det skulle bli spesielle problemer relatert til å utvide datainnholdet i Folkeregisteret.

ID-instrument

Hva skal så ID-instrumentet inneholde og se ut? Det kan tenkes flere varianter, men basisen bør være et kort i kredittkortformat. Innholdet er det følgende:

- Personalia, bilde og signatur til bruk for visuell identifisering.
- Kontaktbasert chip med elektronisk ID for bruk i den virtuelle verden på nett, inkludert mot offentlige portaler/tjenester.
- En funksjon i chipen der basisdata for innehaverens identitet kan hentes ut via en enkel kortleser ved oppmøte på offentlige kontorer og i helsevesenet. (En parallell til tyskernes enkle helsekort som har spart dem for store kostnader i form av mindre feil i registreringer som må rettes senere.) Funksjonen bør kunne brukes mot private aktører også, gitt at innehaveren ønsker det.

Kortet kan også inneholde en OCR-tekst på baksiden og kontaktløs chip, tilsvarende pass, og dermed kunne tjene som maskinlesbart reisedokument i de land som kan lese dette. Dette er ikke avgjørende for utstedelsen av kortet, men kan være en praktisk tilleggfunksjon på mange måter. En slik funksjon vil i noen grad fordyre kortet.

Sikkerhetsmekanismer i kortet nevnes ikke spesielt her, men forutsettes å tilpasses bruken og utvikling over tid. Det samme gjelder design.

Om det også skal være mulig å legge til flere funksjoner etter hvert kan diskuteres senere, men det som er nevnt ovenfor vil dekke borgernes basisbehov. Dette vil også dekke behovet for de fleste offentlige formål og også for et næringsliv som skal samhandle elektronisk med sine kunder. De fleste næringsdrivende vil ikke kunne utstede egne løsninger uansett, men vil være godt hjulpet av en myndighetsutstedt og myndighetsgodkjent løsning. Løsningen åpner store muligheter for små aktører.

Kostnader

Gitt at man gjenbraker registreringssystemet og bygger passregisteret sammen med Folkeregisteret, noe som i seg selv vil koste noe, kostnader som i stor grad kommer likevel, er kostnaden for utsteder (det offentlige) for et nasjonalt ID-kort som beskrevet ovenfor i området 50 – 100 kr. pr. kort. Med andre ord er det snakk om ca. 300 – 500 millioner kr. for hele befolkningen.

Avsluttende kommentar

Dette notatet skraper i overflaten av temaet rundt menneskers identitet og tilhørende dokumentasjon. Argumentasjonene og utredningene kan og bør senere trekkes mye lengre. Imidlertid beskriver dette et konsept som vil holde vann, som er praktisk og rasjonelt lagt opp og som bør være framtidrettet.

