Evaluering av standardisert teknologi, biometriske verdier og utbedringspotensiale av ICAO standarden for elektroniske pass

av

Mona Forsbakk

og

Ingvar Narvestad

Masteroppgave i

informasjons- og kommunikasjonsteknologi

Høgskolen i Agder

Fakultet for teknologi

Grimstad

mai 2006

Sammendrag

En av ettervirkningene til terroraksjonen mot USA 11. september 2001 har vært et verdensomspennende syn at det tradisjonelle pass-systemet trenger en fornyelse. Det har vært enkelt å forfalske pass og dette har ført til svekket kontroll over reisende som krysser landegrenser.

FN-organisasjonen ICAO (International Civil Aviation Organization) har utarbeidet en ny internasjonal standard (Doc 9303) for elektroniske pass. Den internasjonale standarden har blitt møtt med kraftig kritikk fra sikkerhetseksperter og personvernsgrupper.

Denne studien ser på om den standardiserte lagringsteknologien og de biometriske verdiene i elektroniske pass ivaretar sikkerheten godt nok, slik at de biometriske verdiene med sikkerhet kan verifisere et menneske og at uvedkommende ikke kan lese ut informasjon fra lagringsteknologien. Det er også undersøkt hvilke muligheter som er tilgjengelig for å forbedre denne sikkerheten.

Vi mener ICAO har valgt de best egnede biometriske karakteristikkene som er bestemt skal/kan brukes i elektroniske pass. Foreløpig er ansikt et krav, mens fingeravtrykk og iris er godkjente tilleggsalternativer. Ansiktsbiometri er godt innarbeidet. FERET testen fra 2002 viste akseptable resultater, og teknologien har forbedret seg ytterligere de siste fire årene. Videre er fingeravtrykk også en teknologi som har utviklet seg mye i de seinere år. Fingeravtrykk fremstår derfor som det beste biometrien i tillegg til ansikt. Iris er den teknologien som har best potensial til identifisering, men teknologien for irisgjenkjenning er enda svært ung og ikke god nok. Ingen av de andre foreslåtte biometriske karakteristikkene har kvaliteten som kreves for sikker identifisering.

Vi har også sett på teknologiene som er spesifiseres for å beskytte denne informasjonen. Den obligatoriske beskyttelsen i form av passive autentisering er for svak og er et resultat av ICAOs ønske om å støtte begge kommunikasjonsgrensesnittene, som spesifiseres av ISO 14443, på grunn av økonomiske årsaker. For å forsterke denne bør derfor sikkerhetsprinsippene som støtter begge grensesnittene, Faraday-bur, MRZ-sammenligning og kryptering av tilleggsbiometri, gjøres obligatoriske. Samtidig bør det oppfordres til å implementere Type B med minimum grunnleggende tilgangskontroll. Ved lagring av tilleggsbiometri bør også en utvidet tilgangskontroll implementeres. Denne bør bygge på egendefinerte nøkler eller alternative protokoller Caernarvon-protokollen.

Forord

Denne rapporten er en del av masterutdanningen i Informasjons- og kommunikasjonsteknologi ved Høgskolen i Agder, Fakultetet for teknologi. Oppgaven ble gitt av Høgskolen i Agder uten involvering av eksternt firma. Arbeidet ble startet i januar 2006 og avsluttet mai 2006.

Vi ønsker å takk vår veileder, Ola Torkild Aas ved Høgskolen i Agder for veiledning og inspirasjon i løpet av arbeidet. Vi ønsker også å takke studieleder, Stein Bergsmark, for råd og anbefalinger i løpet av prosjektarbeidet.

Grimstad, mai 2006

Mona Forsbakk og Ingvar Narvestad

Innhold

1 Innledning

Det tradisjonelle pass-systemet er gammeldags og det har vært enkelt å forfalske et pass, dette har ført til svekket kontroll over reisende som krysser landegrenser. En av ettervirkningene til terroraksjonen mot USA 11. september 2001 har vært et verdensomspennende syn at systemet trenger en fornyelse.

Siden 2002 har FN-organisasjonen ICAO (International Civil Aviation Organization) utarbeidet en ny internasjonal standard for elektroniske og biometriske pass. Den internasjonale standarden har blitt møtt med kraftig kritikk fra sikkerhetseksperter og personvernsgrupper.

Denne studien vil se på om den standardiserte teknologien til lagring og behandling av biometriske verdier i pass ivaretar sikkerheten godt nok, slik at de biometriske verdiene er sikre nok for å verifisere et menneske og at uvedkommende ikke kan få tak i sensitiv informasjon om passeier. Studien vil også undersøke hvilke muligheter som er tilgjengelig for å forbedre denne sikkerheten.

Denne rapporten evaluerer den 5.versjonen av ”Machine Readable Travel Documents. Part 1.- Machine Readable Passports" (Doc 9303) som kom ut i 2003. I tillegg evaluerer oppgaven 17 dokument som i 2004 ble publisert som et supplement til standarden. Disse spesifiserer biometri og teknologi for bruk i elektroniske pass.

Bakgrunnsinformasjon om reisedokumenter og historie gir svar på hvorfor utviklingen har gått mot det elektroniske passet. Det tradisjonelle passet er grunnlaget for videre utvikling, aktuelle elementer fra de maskinlesbare passene er vikige. Både hvilke biometriske parametre, hvilken lagringsteknologi og sikkerhetselementer det elektroniske passet må inneholde vil beskrives før det dras inn teori og resultater fra annen forskning som er med på å evaluere passet med tanke på sikkerheten.

Evalueringen legger vekt på at eventuelle biometriske og tekniske løsninger vil være praktisk gjennomførbare med tanke på at passkontrollen ikke skal bli for omstendelig.

2 Bakgrunnsinformasjon

2.1 Reisedokumenter

Det finnes per i dag flere forskjellige reisedokument. De vanligste er pass, visum og nasjonale identitetskort. Doc 9303 definerer de tre i hver sin del.

2.1.1 Pass

Et pass er et formelt identifikasjons- eller sertifiseringsdokument utstedt av en nasjon eller organisasjon som identifiserer eieren som en stasborger eller medlem av organisasjonen. Passet symboliserer en anmodning på vegne av utstedende suverene stat eller organisasjon om tillatelse for passets eier til å slippe inn i et land, eller passere gjennom dette. Et pass settes også sammen med rett til rettslig beskyttelse i utlandet.

Passet regnes i de fleste tilfeller som eneste gyldige identifikasjonsbevis ved reiser eller opphold i utlandet, og utstedes av hver enkelt nasjon eller organisasjon etter standardiserte retningslinjer utarbeidet av ICAO som er en mellomstatlig organisasjon tilknyttet FN.

Det finnes i dag flere forskjellige typer pass. Mest vanlig er de ordinære passene som vanlige reisende bruker.

2.1.2 Visum

Et visum er et dokument utstedt av en suveren stat som gir eieren av visumet tillatelse til formelt å be om innreise til landet. Bakgrunnen for bruk av visum er at nasjonene vil ha kontroll på hvilke utenlandske statsborgere som befinner seg i landet, eller har tillatelse til innreise eller utreise. Derfor har de fleste land visumplikt ved innreise, mens noen også krever utreisevisum for å kontrollere hvem som får lov til å forlate landet. Visumet har alltid en begrenset gyldighetsperiode og en spesifisert hensikt. [2]

Vanligvis stemples visum på passenes papirsider eller trykkes eventuelt på egne ark som stiftes sammen med passet. Se Illustrasjon 1 for eksempler på visum stemplet i pass.

I mange tilfeller finnes overenskomster mellom to land om at respektive lands statsborgere får reise til det andre landet uten visum. Schengenavtalen[2] og Visa Waiver Program[3] er eksempler på avtaler mellom nasjoner om bortfall av behov for visum.

Illustrasjon 1: Stemplet visum for Laos, Thailand og Sri Lanka [1]

2.2 Visa Waiver Program

Visa Waiver Program(VWP) er et program som tillater statsborgere fra spesifiserte land å reise inn i U.S.A. for å reise eller drive foretninger i opp til 90 dager uten å måtte skaffe seg et visum. 27 land deltar i programmet, deriblant Norge. Det stilles nå også krav til passene for reisende selv om disse statsborgernes land er medlemmer: [4]

- Det stilles ingen krav til MRTDer utsted før 26.oktober 2005.
- For MRTDer utsted mellom 26.oktober 2005 og 25.oktober 2006 kreves et digitalt fotografi printet på datasiden eller en integrert brikke som inneholder informasjonen fra datasiden.
- For MRTDer utsted etter 26.oktober 2006 kreves en integrert brikke med informasjonen fra datasiden.

2.3 Historisk

Ulike former for pass har vært brukt for å bekrefte brukerens identitet og for diplomatisk beskyttelse ved grensekryssing eller reiser i utlandet. De eldste passene var ofte skrevet på store pergament, og var skrevet som et kongelig anbefalelsesbrev for å sørge for en sikker reise.

I middelalderens Europa ble slike dokument utstedt til reisende av lokale myndigheter og inneholdt en liste over byer den reisende hadde lov til å passere gjennom, på samme måte som dagens system med pass og visum. Dette systemet var for eksempel gjeldende til Frankrike frem til 1860-årene. Passene var generelt kun påkrevd for reise over landjorden, og var som oftest ikke nødvendig for reisende som ankom havnebyene sjøveien da havnene ofte var regnet som friplasser.

Illustrasjon 2: Pass utstedt i Montenegro i 1887 [5]

De tradisjonelle passpapirene inneholdt vanligvis personlig informasjon som navn, nasjonalitet og fødeby, i tillegg til visumdelen. Men etter hvert ble det også vanligere å inkludere en fysisk beskrivelse av passets eier. Se Illustrasjon 2 for et eksempel på et passpapir. Fotografi ble først lagt til i første halvdel av 1900-tallet.

2.4 Veien mot internasjonalisering og standardisering

Den tradisjonelle passordningen fungerte greit i en tid da internasjonal reising stort sett var begrenset til statlige representanter, handelsreisende og de privilegerte klassene, som generelt var et lavt antall samlet sett. Men utover 1800-tallet ble det stadig lettere å reise, og turismen begynte så smått å vokse frem. Etter hvert som turismen og internasjonale reiser stadig ble vanligere begynte de forskjellige regjeringene å bli bekymret for flaskehalsene som ble skapt gjennom komplekse administrative kontrollprosedyrer ved grensene, og problemet med verifisering av pass og andre identitetspapir utstedt av andre nasjoner etter forskjellige nasjonale modeller og standarder. Dette førte til at det i siste halvdel av 1800-tallet ble inngått en serie internasjonale avtaler som

begrenset, og i noen tilfeller fjernet, behovet for pass mellom nasjoner. Disse avtalene var stort sett begrenset til avtaler mellom to eller et fåtall nasjoner som delte grenser.

Forsøkene på å liberalisere passformalitetene kom forøvrig til en brå slutt da første verdenskrig brøt ut i august 1914. Krigen satte flere av avtalene kraftig tilbake, men i perioden like etter krigen ble allikevel arbeidet tatt opp igjen. I 1920 avholdt Nasjonenes forbund, populært kalt Folkeforbundet, en internasjonal konferanse der det sentrale temaet var å forenkle internasjonal passasjertrafikk, med et mål om å gjenskape de gunstige praksisene som var gjeldende før krigenes utbrudd.

Nasjonenes Forbund (eng. *"League of Nations"*), som var forløperen til FN, ble opprettet i januar 1919 på fredskonferansen i Paris, og hovedsetet lagt til Geneve i Sveits. Organisasjonen ble formelt grunnlagt gjennom Versailles-traktaten av seierherrene i 1. verdenskrig etter initiativ fra den amerikanske presidenten Woodrow Wilson[6]. USA ble forøvrig aldri medlem som en følge av at den amerikanske kongressen aldri godkjente Versailles-traktaten. I første rekke sluttet 45 land seg til traktaten, blant dem Norge. Senere kom flere land til, slik at medlemstallet på det høyeste var 60 land. Nasjonenes forbund ble forøvrig svært svekket utover 1930-tallet etter at flere land trakk seg. Mye av organisasjonens problemer skyldtes at den ikke hadde egne militære styrker, men var avhengig av stormaktene. Og etter at organisasjonen ikke klarte å forhindre 2. verdenskrig ble den i realiteten oppløst selv om den formelle oppløsningen ikke ble gjennomført før ved dannelsen av FN i 1945.

De viktigste temaene for konferansene i 1920-årene var pass, tollformaliteter og gjennomreisebilletter. Dette arbeidet fortsatte opp gjennom 1920-årene men stoppet mer og mer opp utover 1930-årene på grunn av de internasjonale spenningene og interne uenigheter innad i Nasjonenes Forbund i årene før 2. verdenskrig.

I 1945 møttes representanter for 50 nasjoner i San Francisco og la grunnlaget for FN-pakten[6]. 26. juni 1945 ble avtalen undertegnet av de 51 opprinnelige medlemsstatene og FN var dannet. Nasjonenes forbund ble samtidig formelt oppløst, og FN arvet de byrå og organisasjoner som var startet av Nasjonenes Forbund.

2.5 ICAO

4. april 1947 ble International Civil Aviation Organization (ICAO) offisielt grunnlagt, med hovedkvarter i Montreal, Canada. Se Illustrasjon 3 for logo. Organisasjonen fikk ansvaret for å utforme alle lover og regler som gjelder for sivil luftfart.

ICAOs engasjement i forhold til standardisering av pass kan spores tilbake til organisasjonens begynnelse.

Illustrasjon 3: ICAOs logo

FN innså at med bakgrunn i flere år med krig, og de politiske spenningene rundt omkring i verden, at målet om internasjonal passfrihet var langt fra virkelighet. Derfor gikk FN i et møte i 1947 inn for å anbefale en internasjonal mal for pass utviklet av Nasjonenes Forbund. I tillegg ble medlemsnasjonene oppfordret til å inngå avtaler om å gjensidig fjerne krav til pass ved reiser mellom gjeldende land.

I 1963 ble det avholdt en konferanse i regi av FN i Roma, med tema internasjonal reise og turisme. Konferansen hadde representanter fra et vidt spekter av land og organisasjoner, deriblant ICAO, med interesser innen turisme og reise. På denne konferansen ble det stadfestet retningslinjer for prosedyrer rundt utstedelse, format og innhold med tanke på pass og visum. Retningslinjene baserte seg på en revidert utgave av ICAOs tidligere arbeid og forskriftene utarbeidet av Nasjonenes Forbund.

Per i dag har ICAO 188 medlemsnasjoner.

2.5.1 Maskinlesbare Reisedokument (MRTD)

Utover 1950-tallet økte internasjonal flytrafikk veldig, mye på grunn av lanseringen av den første generasjonen av sivile jetfly[7]. I 1968 begynte derfor ICAOs avdeling for tilpasning å se på forslag til innføring av maskinlesbare pass som kunne erstatte de konvensjonelle passene. Målet var å gjøre passkontrollene raskere. Flere løsninger ble vurdert og konklusjonen ble at løsningene måtte vurderes ytterligere. I den forbindelse ble et panel nedsatt av "*The Air Transport Committee and the Council of ICAO*" i november 1968[8]. Panelet består av 8 medlemmer valgt fra ICAOs medlemsland. I tillegg deltar også "*The International Criminal Police Organization"* (INTERPOL) og *"The International Air Transport Association"* (IATA).

Panelet vurderte i løpet av 1970-tallet flere forskjellige konsept og teknologier. Hovedprinsippet var at løsningen måtte være praktisk gjennomførbar i alle land, uavhengig av språk. Panelets foretrukne løsninger endret seg etter hvert som arbeidet skred frem. De første forslagene som ble vurdert var pregede kort av plastikk som virket omtrent som dagens pregede bankkort. Denne løsningen ble avløst av forslag om plastkort med magnetstripe. Løsningen som til slutt ble foretrukket og enstemmig vedtatt av panelets 5. møte i 1978, var bruk av en spesialutviklet skrifttype kalt OCR (Optical Character Reading). Denne ble foretrukket fordi den var pålitelig og særdeles billig å implementere sammenlignet med andre teknologier.

Resultatet av panelets arbeid ble i 1980 publisert i en rapport som fikk navnet ICAO Doc 9303, *"A Passport with Machine Readable Capability"*. Dette dokumentet ble siden basis for utstedelse av maskinlesbare pass for landene Australia, Canada og USA, som var først ute med prøveprosjekter. I 1981 og 1982 adopterte også daværende EF (EU) ICAOs resolusjoner og ga medlemslandene beskjed om at europeiske pass skulle utstedes etter ICAOs Doc 9303.

2.5.2 Technical Advisory Group on Machine Readable Travel Documents (TAG/MRTD)

ICAO panelet som utarbeidet dokumentet, som senere ble Doc 9303, ble oppløst etter fullført arbeid i 1978. Men teknologien fortsatte å utvikle seg[9]. Samtidig dukket det opp problemer med den fastsatte standarden. Derfor ble det i 1984 etablert en ny gruppe med ansvar for utvikling av maskinlesbare reisedokument. Denne gruppen fikk navnet "*Technical Advisory Group on Machine Readable Travel Documents"* forkortet TAG/MRTG med hovedkvarter i Montreal, Canada. Gruppen fikk etter hvert også utvidet mandatet sitt til også å gjelde maskinlesbare visum og andre offisielle reisedokumenter i tillegg til pass.

TAG/MRTG gruppen består av delegasjoner fra 13 av ICAOs medlemsland. Disse delegasjonene består normalt av statsansatte eksperter innen områder som passkontroll, immigrasjonsmyndigheter, tollkontroll og nasjonalt politi. I tillegg består gruppen av observatører fra medlemsstater eller organisasjoner tilknyttet sivil flytrafikk, INTERPOL eller "*International Organization for Standardization"* (ISO). Særlig ISO, som er et internasjonalt organ bestående av individuelle nasjonale standardiseringsorganisasjoner (som igjen består av eksperter fra stat og industri) spiller en viktig rolle i utarbeidelsen av ICAOs standarder.

TAG/MRTD er bygget opp av tre undergrupper; EOWG, DCFWG og NTWG. Det er i disse gruppene mesteparten av TAG/MRTDs arbeid gjøres. Den samlede gruppen har kun møter for å evaluere undergruppenes arbeid.

"*The Education and Promotion Working Group"* (EOWG) er TAG/MRTGs informasjons- og implementasjonsorgan og jobber direkte mot ICAOs medlems-nasjoner. Denne hjelper nasjonene som ikke allerede utsteder maskinlesbare pass eller som ikke følger Doc 9303, og jobber med å identifisere og løse problem som hindrer overgang til Doc 9303-standard.

"The Document Content and Format Working Group" (DCFWG) evaluerer spesifikasjonene og oppdaterer disse.

"*The New Technologies Working Group"* (NTWG) har ansvaret for forskning, analysering og innrapportering i forbindelse med dagens og fremtidens teknologier tenkt brukt i maskinlesbare reisedokument. Gruppen fungerer som et forum der industrien kan presentere sine tekniske løsninger med tilknytning til maskinlesbare reisedokument.

3 Maskinlesbare Pass

Da arbeidet med maskinlesbare reisedokument begynte i 1968 var kriteriene for utformingen en helt annen enn i dag. De fleste reisende hadde bakgrunn fra vestlige land, i motsetning til dagens system der reisende er fordelt ut over verden. ICAO måtte ta utgangspunkt i at løsningene som ble valgt måtte la seg gjennomføre i hele verden, uavhengig av språk og geografi. Det var også viktig at de økonomiske rammene var tilpasset den fattige delen av verden. Et pass skal være tilgjengelig for folk flest, og da må også den økonomiske rammen være slik at folk kan ha råd til å gå til anskaffelse av pass. Samtidig må kontrollapparatet være økonomisk oppnåelig for alle land før det kan innføres i landet. Dette er også et av de sentrale kriteriene i 5. revisjon av Doc 9303 for pass.

Den teknologiske utviklingen har siden arbeidet startet opp i 1968 vært formidabel. Til tross for dette har ikke teknologien som brukes i dagens maskinlesbare pass endret seg mye siden første versjon av Doc 9303 kom i 1980. Dette skyldes at en global implementasjon av standarden tar veldig lang tid. På de 26 årene siden første utgave av standarden kom er det omkring 40 av ICAOs 188 medlemsland som fortsatt ikke har begynt å utstede kun maskinlesbare pass. ICAO har satt seg som mål at alle medlemslandene skal utstede maskinlesbare pass innen 1. april 2010. På samme måte som det tar lang tid å gjennomføre global innføring av gammel teknologi tar det også lang tid å gjennomføre større endringer i gjeldende standard. Derfor må alle endringer som gjøres også være kompatible med gammelt system i mange år etter at de første gang gjøres tilgjengelige.

ICAO forutså også at økningen i antall reisende ville vedvare konkluderte med at daværende rutiner for manuell passkontroll ville bli for tidkrevende og omstendelige. Samtidig var den politiske situasjonen slik at FNs håp om passfrihet var langt fra aktuell med det første. Løsningen ble dermed å automatisere passkontrollen mest mulig.

Den endelige standarden måtte dermed fattes ut ifra et kompromiss mellom effektivitet i forhold til utstedelse og kontrollapparat, tilgjengelig teknologi som samtidig var holdbar i mange år fremover, økonomiske rammer, og være praktisk gjennomførbar over hele verden.

Disse forutsetningene førte til at Doc 9303 inneholder en ganske løs standardisert løsning for maskinlesbare pass, der utstederne gis ganske frie tøyler for produksjonen av pass, så fremt de følger spesifiserte retningslinjer. Versjon 5 av *"Machine Readable Travel Documents. Part 1.- Machine Readable Passports"* spesifiserer disse retningslinjene.

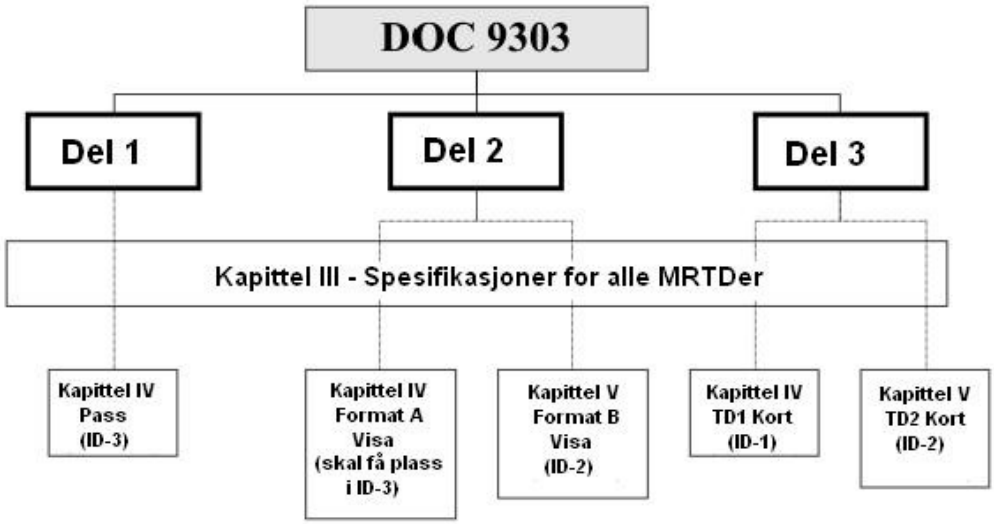
3.1 Doc 9303

Den første utgaven av Doc 9303 kom ut i 1980 under tittelen *"A Passport with Machine Readable Capability"*. Da TAG/MRTD ble opprettet fikk organisasjonen også ansvaret for Doc 9303. Da TAG/MRTDs mandat ble utvidet til å gjelde visum og andre reisedokument i tillegg til pass ble Doc 9303 delt inn i flere deler.

Arbeidet med pass ble videreført i *"Machine Readable Travel Documents. Part 1.- Machine Readable Passports. (Doc 9303)"*. En spesifikasjon for visum, kalt *"Machine Readable Travel Documents. Part 2. - Machine Readable Visas (Doc 9303)"* ble publisert i 1994, mens en spesifikasjon for andre maskinlesbare dokument, *"Machine Readable Travel Documents. Part 3. - Size 1 and Size 2 Machine Readable Official Travel Documents (Doc 9303)"* kom ut første gang i 1996.

Hver del av standarden har siden vært inne til revisjon. Del 1 – Maskinlesbare Pass foreligger per dags dato i 5. utgave som kom ut i 2003, mens Del 2 – Maskinlesbare Visum er ute i 3. ugave fra 2005, og Del 3 – Størrelse 1 og 2 Maskinlesbare Offisielle Reisedokument foreligger i 2. utgave fra 2002.

Doc 9303s oppbygging vises i Illustrasjon 4:



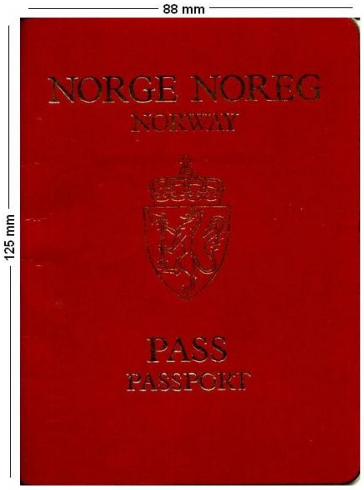
Illustrasjon 4: Oppbygningen av Doc 9303 og relasjonene mellom de tre delene.

Hver av de tre delene er bygget opp der de har en felles del som beskriver og setter opp retningslinjene for alt som er felles for reisedokument spesifisert av Doc 9303. Denne går igjen som kapittel III. Deretter følger kapittel IV og eventuelt V med spesifikke retningslinjer for det gitte reisedokumentet.

3.2 Generelt design

Maskinlesbare pass bygger videre på det tradisjonelle passet med fysiske mål 88,0 mm x 125,0 mm. Passet er bygget opp som en bok, bestående av tre deler: forsiden, datasiden og et sett papirsider for stempling av visum.

På forsiden står utstedende nasjons fulle offisielle navn og dokumenttypen, som er pass, trykket på nasjonens eget offisielle språk og et av ICAOs offisielle språk, utstedernasjons offisielle språk ikke er et av disse. I tillegg vises ofte nasjonens riksvåpen eller lignende symbol. Se Illustrasjon 5 for forsiden av et tradisjonelt pass.



Illustrasjon 5: Et tradisjonelt pass

Datasiden er den viktigste delen av alle reisedokument, og så også pass. Denne skal ligge enten på innsiden av permen, eller den tilhørende siden. De resterende papirsidene brukes til stempling av visum.

3.3 Biografisk Dataside

Den biografiske datasiden er den viktigste siden av passet. Dette er siden som inneholder all informasjon om passholderen. Datasiden skal sitte på innsiden av passets perm eller tilhørende side, og deles inn i syv soner i henhold til Tabell 1.

Tabell 1: Biografisk Dataside - Soneinndeling

Biografisk Dataside – Soneinndeling	
Sone I	Header
Sone II	Personlige dataelement (obligatoriske og valgfrie)
Sone III	Dokument dataelement (obligatoriske og valgfrie)
Sone IV	Signatur
Sone V	Identifikasjonskjennetegn
Sone VI	Valgfrie dataelement
Sone VII	Obligatorisk maskinlesbar sone (MRZ)

Sone I – VI utgjør den visuelle kontrollsonen kalt VIZ (eng. *"Vizual Inspection Zone"*) mens den maskinelt lesbar kontrollsonen (MRZ – eng. *"Machine Readable Zone"*) kun er forbeholdt maskinlesing.

3.3.1 Optisk maskinelt lesbar skrifttype – OCR

Den viktigste teknologien for maskinlesbare reisedokument spesifisert av Doc 9303 er standardisering av valg av skrifttype i forhold til systemet som skal lese tegnene. I offisielle maskinlesbare reisedokumenter benyttes den standardiserte

optisk lesbare teknologien for skrifttype OCR-B (Optical Character Reading – B), som spesifiseres av ISO/IEC 1073-2:1976 og ISO/IEC 1831:1980. OCR-B skrifttypen er en såkalt *monospace* skrifttype. Det vil med andre ord si at avstanden mellom hvert tegn er fast.

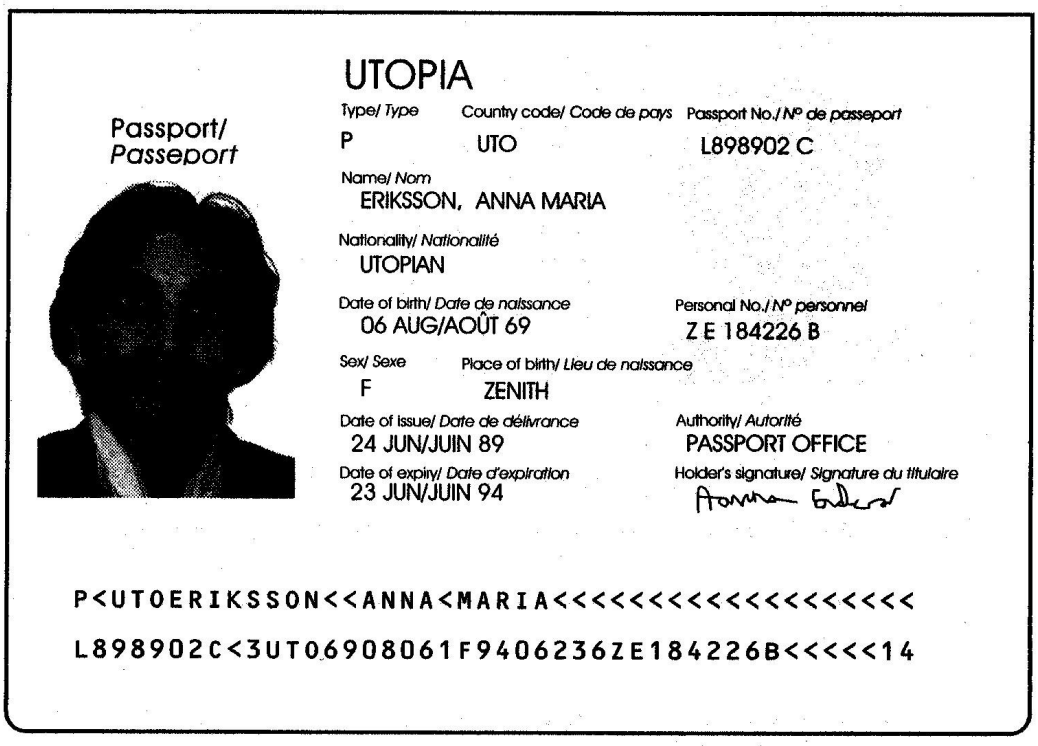
Doc 9303 setter krav til at all tekst i sone VII, det maskinlesbare feltet, skal være trykket i OCR-B, samtidig som det oppfordres til også å bruke OCR-B til teksten i den visuelle kontrollsonen.

3.3.2 Maskinlesbar Sone (MRZ)

Doc 9303 spesifiserer ikke at hele passet skal leses maskinelt. Den visuelle kontrollsonen (VIZ) kan blant annet inneholde nasjonale tegn. Selv om informasjonen i denne også må skrives med latinsk tegnsett, og det oppfordres til å bruke den optisk maskinlesbare OCR-B fonten også her, er det kun Sone VII som er beregnet for å leses maskinelt.

Den maskinlesbare sonen, sone VII, lokaliseres nederst på datasiden[10]. Sonen består av to linjer, hver på 44 tegn, og inneholder all informasjon som er representert med tekst i den visuelt kontrollerbare sonen (VIZ). Linjene inneholder ingen tomme mellomrom. I stedet brukes et "mindre enn" -tegn, <, for å skille mellom de forskjellige elementene og fylle ut tomrom.

Doc 9303 bruker følgende eksempelpass for pass med maskinlesbar sone (MRZ) (Illustrasjon 6).



Illustrasjon 6: Datasiden i et pass, med tilhørende MRZ i bunnen

Den maskinlesbare sonen er synlig som to linjer nederst på illustrasjonen. I eksempelet over ser den slik ut:

```
P<UTOERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<<
L898902C<3UT06908061F9406236ZE184226B<<<<<14
```

Den maskinlesbare sonen kan deles inn i elementene vist i Tabell 2 og Tabell 3.

Tabell 2: Øverste linje i den maskinlesbare sonen (MRZ)

Øverste linje	Lengde	Forklaring
P<	2	P indikerer at dokumentet er et pass. < holder av en plass for å kunne benytte to tegn for identifikasjon av reisedokument.
UTO	3	Utstedende nasjons tresifrede nasjonalitetskode som spesifisert i appendiks 1 til seksjon III av Doc 9303. UTO er en fiktiv kode for Utopia.
ERIKSSON<<ANNA<MARIA<<<<<<<<<<<<<<<<<<<<<<<	39	Passholderens fulle navn. Malen er som følger: Etternavn står først skilt av <. Skillet mellom etternavn og fornavn markeres med <<. Mellomnavn følger sist. ALLE<ETTERNAVN<<FORNAVN<ALLE<MELLOMNAVN Doc 9303 spesifiserer flere regler for forkortelser dersom navnet er lengre enn den avsatte plassen. Ubrukt plass okkuperes av påfølgende <.

Tabell 3: Nederste linje i den maskinlesbare sonen (MRZ)

Nederste linje	Lengde	Forklaring
L898902C<	9	Passnummer. Eventuelle ubrukte plasser okkuperes av påfølgende <.
3	1	Kontrollsum generert av passnummeret.
UTO	3	Passholderens nasjonalitet. Denne er tatt med siden den ikke alltid er lik utstedernasjon i den øverste linjen. I situasjoner der for eksempel FN står som utsteder, vil nasjonalitetskoden avvike fra utstederkoden.
690806	6	Passholderens fødselsdag på formatet YYMMDD.
1	1	Kontrollsum basert på fødselsdato.
F	1	Kjønn. M, F eller < for uspesifisert.
940623	6	Passets utløpsdato på formatet YYMMDD.
6	1	Kontrollsum basert på utløpsdato.
ZE184226B<<<<<	14	Valgfrie data for utstedernasjon eller organisasjon. I dette tilfellet satt av til personnummer.
1	1	Kontrollsum basert på valgfrie data.
4	1	Kontrollsum basert på hele den nederste

3.3.2.1 Kontrollsum

Den nederste maskinlesbare linjen inneholder 5 kontrollsummer[10] som vist i Tabell 4.

Tabell 4: Oversikt over kontrollsummer i den maskinlesbare sonen (MRZ)

Kontrollsum	Tegnposisjoner som utgjør kontrollsummen	Kontrollsummens plassering i den laveste maskinlesbare linjen
Passnummer	1-9	10
Fødselsdato	14 – 19	20
Utløpsdato	22 – 27	28
Personnummer (evt annen personlig informasjon spesifisert av utsteder)	29 – 42	43
Sammensatt kontrollsum	1 – 10, 14 – 20, 22 – 43	44

Kontrollsummene regnes ut ved å bruke en metode som er fast i alle maskinlesbare reisedokument. Utregningen baserer seg på modulus 10 med en sammenhengende repeterende vekting av 731, med andre ord 731731731731...

Selve utregningen gjøres over 5 steg som vist i Tabell 5.

Tabell 5: Konvertering av tegn til tall i kontrollsummer

Steg 0[1]**:** Utregningene må gjøres ved tall. Derfor byttes alle bokstaver i feltet det skal lages kontrollsum av ut med tall etter følgende tabell:

Steg 1 : Går fra venstre mot høyre i tallene det skal lages kontrollsum av, og multipliserer hvert av disse med tilhørende vektet tall fra 731731731731..sekvensen.

Steg 2 : Produktene fra hver multiplikasjon adderes.

Steg 3 : Summen divideres på 10 (modulusen)

Steg 4 : Resten blir så kontrollsummen.

Under følger to eksempler på utregning av kontrollsummen fra Doc 9303 i Tabell 6 og Tabell 7.

Eksempel 1: Kontrollsum av datofelt

Bruker datoen 27. juli 1952, på etter spesifikasjonene i ISO 8601.

		Dato:	5	2	0	7	2	7						
		Vekting:	7	3	1	7	3	1						
Steg 1 :	(Multiplikasjon)	Produkt:	35	6	0	49	6	7						
Steg 2 :	(Summen av produktene)		35	+	6	+	0	+	49	+	6	+	7	= 103
Steg 3 :	(Modulusdivisjon)		$\frac{103}{10}$ = 10, rest 3											
Steg 4 :	Sjekksummen blir da resten, 3.													
	Datoen med tilhørende sjekksum skrives dermed som 5207273													

Tabell 6: Eksempel 1 på utregning av MRZ kontrollsum

Eksempel 2: Kontrollsum fra dokumentfelt

Bruker 9 felts passnummer AB2134<<<

Dataelement:			A	B	2	1	3	4	<	<	<			
Tilsvarende numerisk verdi:			10	11	2	1	3	4	0	0	0			
Vekting:			7	3	1	7	3	1	7	3	1			
Steg 1 :	(Multiplikasjon)	Produkt:	70	33	2	7	9	4	0	0	0			
Steg 2 :	(Summen av produktene)		70	+	33	+	2	+	7	+	9	+	4	+	0	+	0	+	0	= 125
Steg 3 :	(Modulusdivisjon)		$\frac{125}{10}$ = 12, rest 5											
Steg 4 :	Sjekksummen blir da resten, 5.													
	Datoen med tilhørende sjekksum skrives dermed som AB2134<<<5													

Tabell 7: Eksempel 2 på utregning av MRZ kontrollsum

1 I Doc 9303 regnes ikke dette som et eget steg i prosessen. Derfor er den gitt nummerering 0.

4 Elektroniske pass

ICAO New Technologies Working Group(NTWG) har jobbet med maskinassistert identifikasjon av personer, både når et pass utstedes og ved verifikasjon ved grensekontroll. NTWG begynte å undersøke biometri for MRTDer for ca 7 år siden. Den første oppgaven var å finne biometri som kunne anvendes i MRTDer og deretter utforske disse teknologiene. Følgende motiverte 11.september 2001 til økt aktivitet i utviklingen av biometriske studier, eksperimenter, pilotprogrammer og produkter.

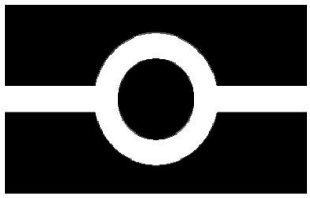
Ved siden av valgte biometriske teknologier er lagrings og kommunikasjonsteknologien det viktigste teknologien som brukes i forbindelse med elektroniske reisedokument.

ICAO har gjennom *Technical Advisory Group for Machine Readable Travel Documents* (TAG/MRTD) og *New Technologies Advisory Group* (NTGW) undersøkt flere potensielle teknologier i forhold til lagring av maskinlesbar og elektronisk informasjon.

Løsningene er vurdert ut ifra følgende hovedkriterier:

Global samspillsevne:	Løsningen må la seg innføre globalt.
Teknisk pålitelighet:	Løsningen må være stabil. Det er også viktig av den er teknisk moden og utprøvd i større omfang over lengre tid.
Praktisk:	Løsningen må være praktisk av natur. Både når det gjelder implementasjon og i forhold til kontroll av reisedokument.
Holdbarhet:	ICAO har satt 10 år som maksimum levealder for et reisedokument. De tekniske løsningene som velges for elektroniske pass må tilfredsstille denne levealderen.

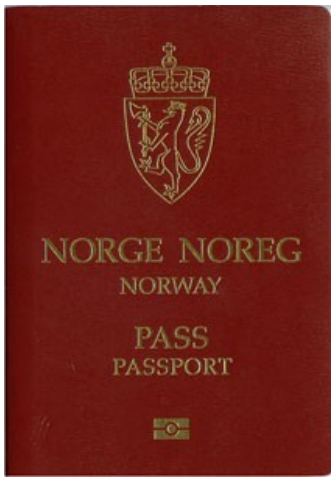
Rapporten "*Biometrics deployment of machine readable travel documents"* [11] som er hoveddokumentet for supplementene til Doc 9303, og 16 annekser til rapporten gir den viktigste støtteinformasjonen og blir oppdatert ettersom tilleggsinformasjon og nye versjoner av grunnleggende dokumenter blir tilgjengelige. Alt dette skal til slutt, etter evaluering, legges inn i en ny versjon av Doc 9303.



Illustrasjon 7: Symbolet for tråløs integrert krets(IC)

Det forslås at et pass som har lagringsbrikke med biometri bør merkes med det symbolet vist i Illustrasjon 24. Symbolet anbefales å plasseres på bunnen av forsiden til passet, under landsmerke og under navnet "*Passport*". Se hvordan dette for eksempel er gjort på norske pass i Illustrasjon 8.

I fortsettelsen av dette kapittelet beskrives valg av biometri og lagringsteknologi med tilhørende datastruktur og sikkerhetsprinsipper.



Illustrasjon 8: Et norskt pass med symbolet for trådløs IC

4.1 Biometri

Ansiktsgjenkjenning, fingeravtrykk og iris er valgt og godkjent av 13th ICAO TAG/MRTD i februar 2002 og kan brukes av en stat som en begynnelse på å innføre biometri i reisedokumenter. Ansiktsbiometri er den best egnede for reisedokuments utstedelse, men fingeravtrykk og/eller iris er også mulig å implementere. Viktige punkter ved impementasjon av biometriske standarder i MRTDer bygger på de generelle hovedkriteriene til ICAO:

- Global samspillsevne: viktighet av spesifikasjoner for hvordan biometri blir brukt på en universal måte.
- Uniformitet: begrense omfanget av spesifikk standard til å være praktisk rettet mot løsningsvarianter som kan bli tatt i bruk av de forskjellige stater.
- Teknisk pålitelighet: behovet for retningslinjer og parametere for å forsikre at landene tar i bruk teknologier som har høy sikkerhet med tanke på identitetsbekreftelse, og at statene seg imellom kan være sikker på at data de får av hverandre er av tilstrekkelig kvalitet og integritet for å gi nøyaktig verifikasjoner.
- Praktisk: behovet for å forsikre at anbefalte standarder kan bli implementert uten at de forskjellige stater må innføre en rekke ulike systemer og utstyr for å garantere at alle mulige variasjoner av tolkninger av standarden kan dekkes.
- Varighet: at systemene som introduseres vil vare de 10 år et pass varer, og at oppdateringer er bakover kompatible.

Rapporten beskriver hvilke nøkkelprosesser som utføres men hensyn på biometri og hvilke applikasjoner som finnes for biometrisystemer. I tillegg til dette må hvert land ha sine egne krav til:

1. Nøyaktighet av funksjonene for biometrisk sammenligning. Land som utsteder pass må kode en eller flere biometriske karakteristikker på MRTDer med LDS standarder eller opprette en database som er tilgjengelige for andre land. Ved bruk av ICAO standardiserte biometriske avbildinger eller maler må hvert land velge sin biometriske verifikasjonssoftware og avgjøre egen bedømming av biometri for godkjenningsrate til identitetsverifikasjon.
2. Hvor mange reisende som bør komme gjennom et biometrisk system eller hele grensekontrollen per minutt.
3. Hvorvidt en biometrisk teknologi(ansikt, finger eller øye) er hensiktsmessig i en grensekontroll.

Rapporten har også restriksjoner til biometriske løsninger:

- Det er oppdaget at leverandørers implementering for de fleste biometriske teknologier er emne for videre utvikling.
- Mange har ikke blitt testet over ti år
- Mange er ikke utprøvd på å identitet en til mange mot en stor nasjonal database.
- Teknologier endrer seg raskt. Enhver spesifikasjon må gi mulighet for og være forberedt til endringer som en følge av utbedringer i teknologien.
- Biometrisk informasjon som er lagret i pass må ikke komme i konflikt med nasjonale databeskyttelseslover, personvernslover eller kulturell praksis. PKI Technical Report[12] i samsvar med LDS Technical Report[13] spesifiserer hvordan integritet og hemmeligholdelse av data oppnås når biometri anvendes i MRTDer.

Flere beslutningsskriv er tatt med i rapporten og viser utviklingen til bestemmelsene rundt biometri i pass og begrunner valg av biometriske karakteristikker. Følgende fordeler ved å bruke ansiktet:

- Et ansiktsfotografi gir ikke ut mer informasjon om personen enn det gjøres til daglig.
- Et fotografi er allerede sosialt og kulturelt akseptert internasjonalt.
- Folk er allerede kjent med hvordan fotografiene taes og brukes ved identitetsverifisering.
- Det brukes allerede i pass etter ICAO 9303 standarden.
- Det er metode som ikke er påtrengende. Brukere trenger ikke være i fysisk kontakt med utstyr for å bli registrert.
- Det krever ikke nye og kostbare metoder/utstyr for å ta dette i bruk.
- Ansiktsfotografier kan bli tatt umiddelbart.
- Mange land har database med ansiktsfotografier som en del av den digitaliserte produksjonen av passfoto som kan bli kodet til ansiktsmaler og verifisert for identitetssammenligninger.
- En person trenger ikke være fysisk tilstede dersom et godkjent fotografi kan brukes. Dette kan brukes for barn hvis de ikke er tilstede.
- Ved bruk av observasjonsliste er fotografier som regel det eneste tilgjengelige for sammenligning.
- Menneskelig verifikasjon av denne biometriske karakteristikken mot et fotografi/en person er relativ enkel og velkjent for personell ved grensekontroll.

NTWG var derimot klar over at forskning på ansiktsgjenkjenning ikke var ferdig, men det var ikke noe som antydet at det var umulig å få til både ved passutstedelse og ved grensekontroll.

Anneksene til rapporten tar for seg behandlingen av ansiktsfotografier, alt om posisjonering av ansikt og effekter som ikke skal i bildet som skygge, uskarphet, hatt, etc. Hvordan fotografiet skal klippes til blir også utredet og forskjellige typer bildeformater og komprimeringsmetoder blir evaluert. Det forslås også en standard for utveksling av irisinformasjon i et fotografi. Når det gjelder

fingeravtrykk er det presentert tre forskjellige gjenkjenningsmuligheter; fotografi, minutiae og mønsterspektral.

4.2 Det trådløse systemet

Teknologien som har vunnet frem er trådløse smartkort. Dette er en teknologi som bygger på RFID-teknolgien. RFID (eng. *"Radio Frequency Identification"*) er en trådløs kommunikasjonsteknologi som i første rekke brukes til identifikasjon. Industrimessig er RFID i ferd med å seile opp som et reelt alternativ til strekkoder. Tradisjonell RFID er enkel i oppbyggingen og returnerer vanligvis kun en identifikator. Trådløse smartkort bygger på den samme teknologien, men utvider denne ved å implementere en integrert krets.

Løsningen som er valgt spesifiseres av den internasjonale standarden ISO/IEC 14443, *"Identification Cards – Contactless integrated circuit(s) cards – Proximity cards"* [14]. Brikkene som standardiseres av ISO/IEC 14443 er passive, de har med andre ord ingen egen energikilde. I stedet baserer de seg på å generere strøm fra signalet til leseren. Leseavstanden som spesifiseres av ISO/IEC 14443 mellom brikke og leser er omtrent 10 cm.

ISO/IEC 14443 er sist revidert i 2000 og består av fire deler:

Del 1: Physical characteristics

Del 2: Radio frequency power and signal interferance

Del 3: Initialization and anticollision

Del 4: Transmission protocol

Et RFID system består av to hovedkomponenter:

1. En transponderende enhet, i form av den trådløse integrerte kretsen.
2. Sender- og mottakerenhet, som oftest kombinert i en enhet kalt leser.

ISO 14443 bruker forkortelsen PICC (eng. *"Proximity Integrated Circuit Card"* for den trådløse-brikken og PCD (eng. *"Proximity Coupling Device"*) for leseren.

I tillegg er datasystemet som ligger bak leseren en viktig del av systemet. Dette består i de fleste tilfeller av EDGE-servere, middleware og applikasjonssoftware og er ikke standardisert på samme måte siden systemet avhenger av bruken.

Løsningen ICAO har valgt baserer seg på bruk av passive trådløse brikker som opererer på 13,56 Mhz[15] ± 7 Khz[14]. Brikken består av to hovedkomponenter: en silikonbasert integrert krets, IC (eng. *"Integrated Circuit"*) og en antenne, også kalt koplingsenhet. Den passive brikken har ingen intern energikilde og genererer strøm fra signalene som sendes fra leseren(PCD). Derfor har brikken ingen strøm når den er utenfor leserens rekkevidde, og forholder seg dermed inaktiv. Når den derimot kommer innenfor leserens signaldekningsområde og mottar riktig signal fra leseren genererer den strøm ved induktiv kopling, og den integrerte kretsen (IC) aktiveres. Den trådløse brikken (PICC) kan deretter

signalere og sende data til leseren (PCD) gjennom å svitsje en prosess som på engelsk kalles *"load modulation"*.

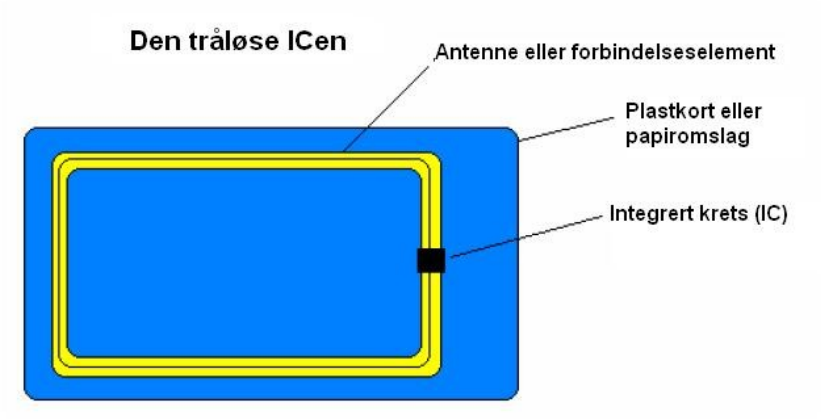
Leseren (PCD) inneholder en høyfrekvent radiomodul for sending og mottak av data, en signalprosessor og kontrollmodul, og en antenne eller koplingsenhet for den fysiske oppkoplingen. I tillegg er det vanlig med et datagrensesnitt mot datasystemet. Dette datagrensesnittet følger vanligvis RS-232 – standarden eller USB – standarden. Anneks I, *"Use of Contactless Integrated Circuit(s) in Machine Readable Travel Documents"*[15] spesifiserer kun bruk av USB. Selv om USB 1.1 tilfredsstiller dagens krav til overføringshastighet, oppfordres det til bruk av USB 2.0 for å møte fremtidige krav.

4.2.1 Den trådløse brikken

Den induktivt koblete trådløse brikken er enkel i oppbyggningen. Den består av en elektronisk integrert krets(IC) som tar seg av all databehandling, og en lang antenne, også kalt koplingsenhet som består av en metalltråd som er kveilet flere ganger rundt brikken slik Illustrasjon 9 viser.

Den viktigste delen av den trådløse-brikken er den laveffekt-integrerte koplingskretsen som styrer kommunikasjonen med leseren(PCD). I tillegg inneholder den integrerte kretsen også minne for lagring av data. Brikken består ellers av tre deler:

- *Minne*, som er en helt enkel minneenhet.
- Logikk, som inneholder minne og enkle logiske funksjoner som passordbeskyttelse.
- *Mikrokontroller*, som inneholder minne og mer avanserte funksjoner for kryptering og partisjonering av data.



Illustrasjon 9: Trådløs integrert krets (IC)

4.2.2 Plassering

Det er flere mulige lokasjoner for den trådløse IC brikken i passet, hver har sine fordeler og ulemper. Hvert land bestemmer selv hvor brikken plasseres. ICAOs forslåtte plassering er som følger:

- Datasiden – samler alle dataene og teknologien slik at polycarbonat kan taes fordel av ved innstøping av brikke og tilhørende antenne. Dette må sees i forhold til fordelen ved å separere brikken fra resterende data i passet slik at en forfalsker må endre to områder enn et.
- I senter av heftet – fordel ved at hele heftet beskytter mot slitasje når brikken er plassert i midten.
- Mellom forsatspapir og perm – gir mulighet til å sette inn brikken og antenne i løpet av motering men dette kan utsette utstyret ved gull eller plastpreging, eller ødelegges når permen presses sammen, eller forfalsking kan prøves ved oppdeling av permen fra forsatspapiret.
- Sydd inn separat i side.

Se Illustrasjon 10 for hvordan man kan se ICen i datasiden til et pass når dette gjennomlyses.

Illustrasjon 10: Et gjennomlyst pass hvor ICen ligger i datasiden

4.2.3 Induktiv kopling

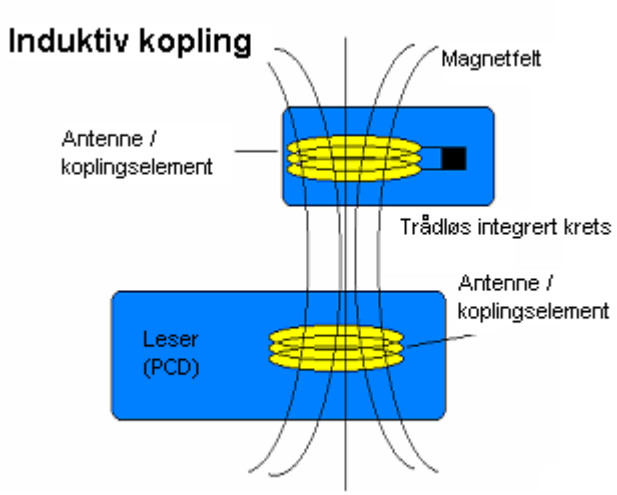
Passive trådløse smartkort, i likhet med passiv RFID, henter energien sin fra kraftfeltet som genereres av leseren. Induktiv RFID baserer seg på den elektriske resonanse effekten, og genererer strøm fra leserens sterke elektromagnetiske radiofrekvensfelt gjennom antennen. Antennen eller koplingsenheten til induktive RFID brikker er egentlig en induksjonsspole og kondensator som er sammenkoblet og designet for å gi resonans ved 13,56 Mhz[16], som er systemets operasjonsfrekvens definert i ISO/IEC 14443[14].

Bølgelengden ved 13,56 Mhz er 22,1 meter. Dette tilsvarer mangfoldige ganger avstanden mellom leser(PCD) og den trådløse brikken, som i følge spesifikasjonene i Anneks I, *"Use of Contactless Integrated Circuit(s) in Machine Readable Travel Documents"*[15] tilhørende *"Biometrics Deployment Of Machine Readable Travel Documents""*[11] som er en utvidelse av Doc 9303[17] publisert i 2004 og ISO/IEC 14443[14] er mindre enn 10 cm. Innenfor området som defineres av den korte avstanden til leseren kan derfor det elektromagnetiske feltet betraktes som et enkelt vekslende magnetisk felt, av typen som finnes i

transformatorer. Styrken til det elektromagnetiske feltet avtar raskt ved økende avstand mellom leseren (PCD) og den trådløse brikken.

Maksimumstyrken for det elektromagnetiske feltet som genereres av leseren er regulert av ISO 14443, som følge av sikkerhetshensyn, med tanke på strålingsfare. Derfor vil en leseavstand over 1 meter heller ikke være praktisk samtidig som det gir sikkerhetsfordeler i forhold til bedre kontroll over eksterne støykilder og beskyttelse av datastrømmen.

Illustrasjon 11 beskriver induktiv kopling.



Illustrasjon 11: Induktiv kopling

En del av det elektromagnetiske feltet som genereres av leseren(PCD) dekker den trådløse brikkens antenne og induserer en vekselstrømspenning (eng. *"AC – Alternating Current"*) over denne. Denne vekselstrømmen konverteres til likestrøm (eng. *"DC – Direct Current"*) og brukes til å lade kondensatoren. Kodensatorladningen brukes så til strøm for den integrerte kretsen(IC).

Over den trådløse brikkens antenne er det er det koblet til en kodensator. Verdiene til denne kapasitansen er valgt slik at den virker med induktansen til antennen og danner en parallell resonanskrets. Frekvensresonansen til denne kretsen samsvarer med den transmitterte frekvensen fra det elektromagnetiske feltet og gir maksimumspenningen til trådløse integrerte kretsen.

Dataene transmitteres fra leseren(PCD) til den trådløse brikken ved at et av det transmitterte elektromagnetiske feltets parametere, amplitude, frekvens eller fase, endres.

4.2.4 Lastmodulering

Den parallelle resonanskretsen på den trådløse brikkens integrerte krets trekker energi fra det elektromagnetiske feltet som genereres av leseren(PCD). Denne energien som trekkes kan måles på leserens antenne ved å overvåke strømmen som tilføres. Den trådløse integrerte kretsen kan svitsje en lastmotstand ved

antennen som forårsaker at energitilførselen til leseren øker eller avtar. Denne strømendringen måles så ved å måle strømtilførselen til leserens antenne. Dersom svitsjingen på den trådløse integrerte kretsens lastmotstand representerer data, betyr det at den trådløse integrerte kretsen kan sende data til leseren. Denne metoden kalles lastmodulering (eng. *"Load mudulation"*).

Den trådløse interne kretsen må svitsje lastmotstanden til en lavere frekvens enn den som genereres av leseren(PCD). Den nye frekvensen kalles en hjelpebærebølge (eng. *"subcarrier"*), og kan moduleres til digitalt datakommunikasjonsformål på flere måter, typisk ASK(eng. *"Amplitude Shift-Keying"*), FSK (eng. *"Frequency Shift-Keying"*) og BPSK (eng. *"Binary Phase Shift-Keying"*) og OOK (eng. *"On/Off-Keying"*). Modulasjonsmetodene som spesifiseres av ISO 14443 er ASK, OOK og BPSK.

4.2.5 Type A og Type B Trådløs Integrert Krets

ISO 14443[14] spesifiserer to typer kommunikasjonsgrensesnitt mellom leseren(PCD) og den integrerte kretsen i den trådløse brikken. Disse kalles Type A og Type B. I "*Biometrics Deployment Of Machine Readable Travel Documents"* spesifiseres det at alle lesere må støtte minst en av disse grensesnittene, samtidig som det oppfordres til å støtte begge to for global samspillsevne.

Type A trådløse integrerte kretser er vanligvis kretser som kun inneholder minne. Leseren(PCD) bruker 100% amplitudemodulasjon (ASK) av det elektromagnetiske feltet for å kommunisere med den trådløse integrerte kretsen. Det vil si at for å kommunisere 1ere og 0er slås det elektromagnetiske feltet på og av. Av spesifiseres av ISO/IEC 14443-2[18] som mindre enn 5%, Mens det elektromagnetiske feltet er slått av må den interne kondensatoren i den integrerte kretsen lagre nok energi til å kunne fungere til feltet slås på igjen.

Type B trådløse integrerte kretser er generelt utstyrt med en prosesserende integrert krets og er derfor i stand til å utføre flere operasjoner. Den bruker av samme grunn mer strøm enn en integrert krets av type A som er minnebasert. Derfor er ikke 100% amplitudemodulasjon til det elektriske feltet lengre praktisk, siden det vil medføre at den trådløse integrerte kretsen lades ut for hver tilføring av ny energi. Derfor bruker Type B 10% ASK-modulasjon slik at energistrømmen til den trådløse integrerte kretsen konstant opprettholdes. Med andre ord kommuniserer leseren 1ere og 0er til den trådløse integrerte kretsen ved å svitsje det elektromagnetiske feltet mellom 100% og 90% amplitude.

Hjelpebærebølgen som dannes ved modulasjonen er på 848 Khz (fc/16 = 13,56 Mhz/16). Type A bruker modifisert Millerkoding for overføringen fra leseren(PCD) til den trådløse integrerte kretsen, og OOK-modulasjon og Manchesterkoding over hjelpbærebølgen på 848 Khz for dataoverføringen fra den trådløse integrerte kretsen til leseren. Type B bruker NRZ-L (eng. *"NonReturn to Zero Level"*) koding på frekvensen begge veier mellom leseren og den trådløse integrerte kretsen og BPSK-modulasjon på hjelpebærebølgen.

4.2.6 Dataoverføringshastighet

ISO/IEC 14443-2:1999[18] definerer en dataoverføringshastighet på opptil 106 kbit/s (fc/128) begge veier mellom leseren og den integrerte kretsen. Her representerer en bit 8 Hz i hjelpebærebølgen. Dataoverføringshastighet på 212 kbit/s (fc/64), 424 kbit/s (fc/32), 848 kbit/s (fc/16) og høyere er vist i et tillegget til ISO/IEC 14443-2:2001, og Anneks I *"Use of Contactless Integrated Circuit(s) in Machine Readable Travel Documents"* [15] til *"Biometrics Deployment Of Machine Readable Travel Documents"* [11] åpner opp for å gå utover spesifikasjonene i ISO 14443 for å utnytte denne.

Forutsetningene for denne hastigheten er at det brukes BPSK-modulasjon og NRZ-L koding på hjelpebærebølgen på både Type A og Type B.

4.2.7 Kollisjonsavvergingssystem

Det er mulig å plassere to eller flere trådløse brikker innenfor det elektromagnetiske feltet til leseren samtidig. En normal situasjon vil være dersom passet inneholder en egen RFID brikke i tillegg til et visum med RFID brikke. I denne situasjonen vil begge brikkene dele på energien fra det elektromagnetiske feltet og de responderende hjelpebærebølgene vil interferere. For å unngå dette implementerer både Type A og Type B et avvergingssystem for kollisjoner.

Type A implementerer "*Binærsøketre"* (eng. *"Binary search tree"*), mens Type B implementerer *"Slotted Aloha."* Begge avvergingssystemene for kollisjoner er spesifisert i ISO/IEC 14443-3[19].

4.2.8 Lagringskapasitet

I den tekniske rapporten "*Biometrics Deployment Of Machine Readable Travel Documents*" spesifiseres det at den trådløse brikken må ha minimum lagringskapasitet på 32 Kilobytes. Dette som som et minimum for å lagre den obligatoriske informasjonen.

4.3 Logisk datastruktur

En standardisert logisk datastruktur (eng. *"Logical Data Structure"*, LDS) er nødvendig for global samspillsevne. Den logiske datastrukturen beskriver strukturen på informasjonen som lagres på den trådløse brikken. Dette spesifiseres i *"Development of a Logical Data Structure – LDS – for Optical Capacity Expansion Technologies"* [13]. Tabell 8 gir en oversikt over den viktigste strukturen.

LOGISK DATASTRUKTUR (LDS)

			DATA GRUPPE	DATAELEMENT		Element nummer
Obligatorisk informasjon	Data kontrollert av utstedende nasjon eller organisasjon	Detaljer fra MRZ	DG 1	Dokumenttype		1
				Utstedernasjon eller org.		2
				Passholders navn		3
				Passnummer		4
				Sjekksum Passnummer		5
				Nasjonalitet		6
				Fødselsdato		7
				Sjekksum Fødselsdato		8
				Kjønn		9
				Passets utløpsdato		10
				Sjekksum utløpsdato		11
				Utsteders valgfrie data		12
				Sjekksum valgfrie data		13
				Sjekksum Fødselsdato		14
				Sjekksum over hele MRZ		15
Valfri informasjon	Data kontrollert av utstedende nasjon eller organisasjon	Krypterte identifikasjons-kjennetegn	DG 2	Globalt utvekslbare kjennetegn	Kryptert ansikt	1 – 3
			DG 3	Tilleggs-kjennetegn	Krypterte fingre	1 – 3
			DG 4		Krypterte øyne	1 – 3
		Synlige identifi-kasjons-kjennetegn	DG 5	Passbilde		1 – 2
			DG 6	Reservert for fremtidig bruk		Ubestemt
			DG 7	Pass-signatur		1 – 2
		Krypterte sik-kerhets-innslag	DG 8	Datainformasjon (Udefinert)		1 – 3
			DG 9	Strukturinformasjon (Udefinert)		1 – 3
			DG 10	Substansinformasjon (Udefinert)		1 – 3
			DG 11	Personlig tilleggsinformasjon		1 – 14
			DG 12	Tilleggsinformasjon dokument		1 – 10
			DG 13	Utsteders valgfrie data		1
			DG 14			Ubestemt
			DG 15	Offentlig Nøkkel for Autentisering		
			DG 16	Pårørende		1 – 5
Valgfri informasjon	Data Mottaker-nasjon eller godkjent mottaker-organisasjon					Element nummer
			DG 17	Automatisk grenseklarering, Detaljer		Ubestemt
			DG 18	Elektronisk(e) visum, Detaljer		Ubestemt
			DG 19	Reiseprotokoll(er), Detaljer		Ubestemt

Tabell 8: Logisk datastruktur

Strukturen deles inn i to hoveddeler, obligatorisk og valgfri informasjon. Informasjonen ICAO spesifiserer som obligatorisk er kun den samme

informasjonen som er tilgjengelig gjennom den maskinlesbare sonen (MRZ), som spesifiseres i datagruppe 1 i Illustrasjon 12. Dette er informasjonen som strengt tatt må være med i elektroniske pass. I tillegg oppfordres det som et minimum å også ta med Datagruppe 5, en digital kopi av passbildet, og Datagruppe 7, en digital kopi av signaturen. Et fotografi av ansiktet regnes som offentlig og all denne informasjonen er allerede tilgjengelig via den maskinlesbare sonen(MRZ) og den visuelle sonen(VIZ) og trenger derfor ikke å krypteres.

I tillegg oppfordres det sterkt til å legge inn en elektronisk digital mal (eng. "*template")* av ansiktsformene i datagruppe 2. ICAO bestemte i Berlin resolusjonen fra 28. juni 2002[11] at ansiktsgjenkjenning skal være den internasjonale fellesfaktoren i maskinell identifiseringshjelp for maskinlesbare reisedokument. I New Orleans resolusjonen fra 21. mars 2003[11], oppfordres det også til å lagre digitale maler av fingeravtrykk og iris i henholdsvis datagruppe 3 og datagruppe 4. Denne informasjonen regnes forøvrig som personlig. Derfor settes det krav til at datagruppe 2-4 krypteres for å hindre at utenforstående får tak den. Det samme gjelder datagruppe 8-10 som omhandler informasjon om fremtidige sikkerhetsforanstaltninger. Grunnen til at ikke all informasjon i datastrukturen krypteres er at spesifikasjonene i størst mulig grad skal være kompatible med de trådløse integrerte kretsene Type A og Type B, som spesifiseres av ISO/IEC 14443[18]. Type A er kun en minnebrikke og er ikke like avansert som Type B, og støtter ikke like mange operasjoner. Operasjonene som ikke støttes er i tilknyttning til krypteringsmetodene.

I tillegg åpnes det opp for at utstedende nasjoner og land kan legge inn ekstra informasjon om passinnehaveren (Illustrasjon 12), dokumentet (Illustrasjon 13), pårørende (Illustrasjon 14) og eventuell annen valgfri informasjon (Illustrasjon 15). Dette legges i datagruppene 11, 12, 13-14 og 16.

DATA GRUPPE	Personlig tilleggsinformasjon	Element nummer
DG 11	Passholders navn	1
	Andre navn	2
	Personnummer	3
	Fødselssted	4
	Full fødselsdato	5
	Adresse	6
	Telefonnummer	7
	Yrke	8
	Tittel	9
	Personlig sammendrag	10
	Statsborgerbevis	11
	Antall andre gyldige reisedokument	12
	Annen gyldig reisedokumentasjon	13
	Rullebladsinformasjon	14

Illustrasjon 12: LDS Datagruppe 11 - Personlig Tilleggsinformasjon

DATA GRUPPE	Tilleggsinformasjon dokument	Element nummer
DG 12	Utstedelsesautoritet	1
	Utstedelsesdato	2
	Antall personer som er innkludert	3
	Andre personer som er innkludert i det maskinlesbare reisedokumentet	4
	Tilleggsinformasjon	5
	Utreisekrav	6
	Bilde av reisedokumentets forside	7
	Bilde av reisedokumentets bakside	8
	Tidspunkt for personaliseringen	9
	Maskin som er brukt til personaliseringen	10

Illustrasjon 13: LDS Datagruppe 12 - Tilleggsinformasjon dokument

DATA GRUPPE	Utsteders valgfrie data
DG 13	Valgfritt
DG 14	Valgfritt

Illustrasjon 14: LDS Datagruppe 13 & 14 - Utsteders valgfrie data

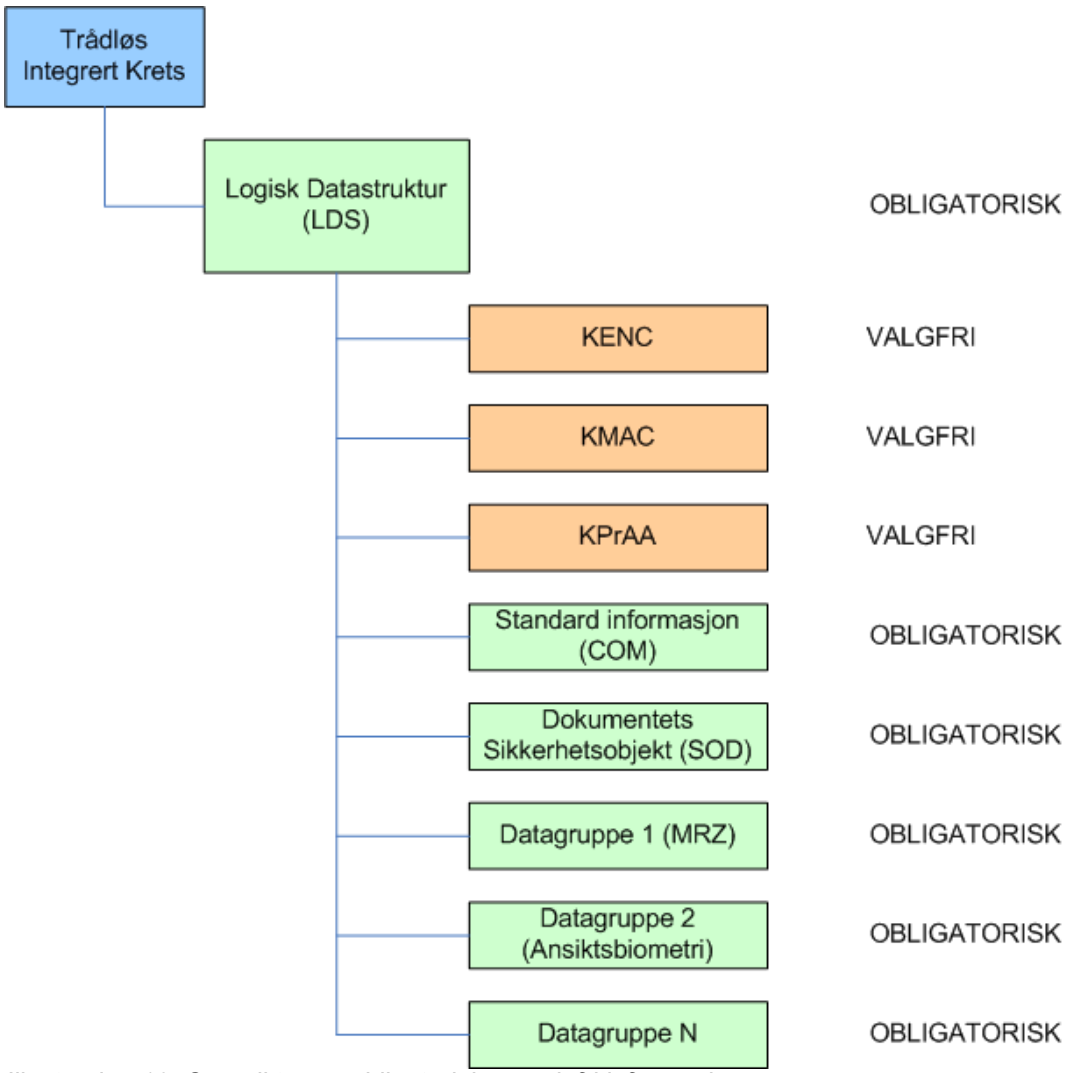
DATA GRUPPE	Pårørende	Element nummer
DG 16	Antall pårørende	1
	Dato for registreringen	2
	Navn	3
	Telefonummer	4
	Adresse	5

Illustrasjon 15: LDS Datagruppe 16 -Pårørende

Datagruppe 15 er forbeholdt den offentlige nøkkelen for dekryptering av de krypterte datagruppene (DG 2 – 4 og 8 – 9).

Informasjonen i datagruppene 1 – 16 kontrolleres av utstedende nasjon eller organisasjon og kan ikke endres av andre utstedende nasjoner, da denne låses som en del av produksjonsprosessen. Datagruppe 17 – 19 er imidlertid satt av til informasjon fra mottakernasjonen eller godkjente mottakerorganisasjoner. Denne er også frivillig å implementere og er ikke ferdig spesifisert enda. Datagruppe 17 omhandler automatiske grenseklareringer, datagruppe 18 visum og datagruppe 19 omhandler reiselogger.

I tillegg spesifiseres blant annet bitstørrelser og inndatamasker i *"Development of a Logical Data Structure – LDS – for Optical Capacity Expansion Technologies"* . Hvordan den logiske datastrukturen skal implementeres på trådløse integrerte kretser spesifiseres i *"Annex A – Normative Mapping of LDS [Version 1.7] Using Random Access File Representation to Integrated Circuits (IC(s))"*.



Illustrasjon 16: Oversikt over obligatorisk og valgfri informasjon

Illustrasjon 16 viser rekkefølgen informasjonen lagres i den logiske datastrukturen(LDS).

4.4 Sikkerhetsprinsipper

ICAO definerer flere teknikker for beskyttelse av innholdet i elektroniske reisedokument samt verifisering av informasjonen i den maskinlesbare sonen (MRZ) og den visuelle sonen (VIZ). Disse teknikkene bygger i hovedsak på bruken av digitale signaturer, kryptografi og digitale sertifikat.

Teknikkene spesifiseres i dokumentene *"PKI Digital Signatures For Machine Readable Travel Documents"* [20]og *"PKI for Machine Readable Travel Documents offering ICC Read-Only Access"* [12].

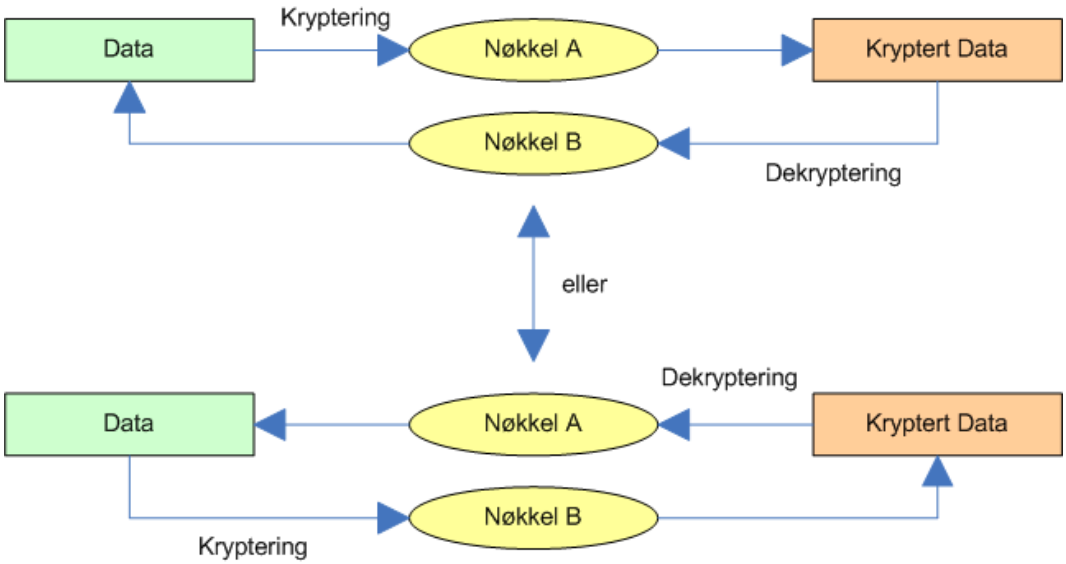
4.4.1 Offentlig nøkkel kryptografi

Et sentralt begrep i ICAOs sikkerhetsløsning er offentlig nøkkel kryptografi (eng. *"public key cryptography"*). I tradisjonell kryptografi, som kalles symmetrisk kryptografi, brukes den samme nøkkelen til både kryptering og dekryptering (Illustrasjon 17).

Illustrasjon 17: Tradisjonell symmetrisk kryptering

Dette forutsetter at både sender og mottaker kjenner nøkkelen, og brukes for det meste i intern og privat kryptering.

Offentlig nøkkel kryptografi, som kalles asymmetrisk kryptografi , benytter seg av matematiske algoritmer, som i motsetning til tradisjonell kryptografi bruker to adskilte, men matematisk beslektede nøkler (Illustrasjon 18). Informasjon som er kryptert med den ene nøkkelen kan kun dekrypteres med den andre nøkkelen, og motsatt.



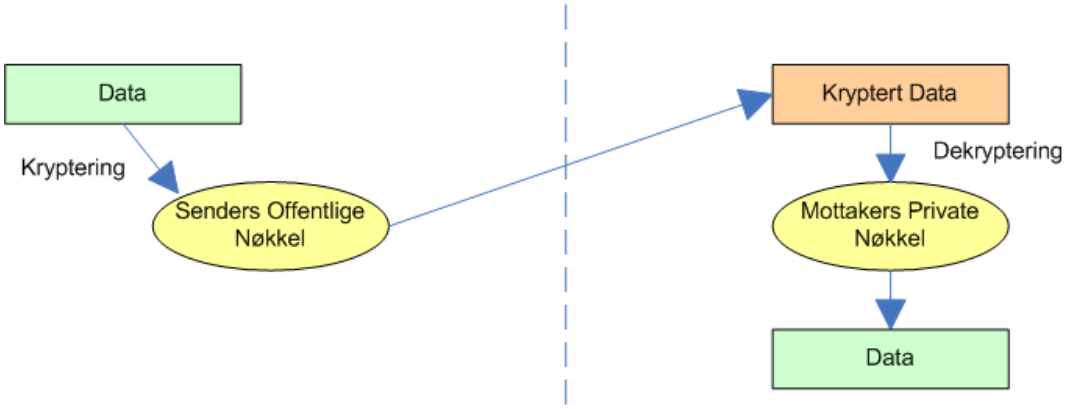
Illustrasjon 18: Asymmetrisk offentlig nøkkel kryptering

En annen fordel med offentlig nøkkel kryptografi er at de to nøklene i nøkkelparet i praksis ikke kan utledes av hverandre ved bruk av en nøkkel av en viss lengde. Nøklene deles så i to, der den ene av nøklene blir privat hemmelig nøkkel, mens den andre brukes som offentlig nøkkel som gjøres tilgjengelig for alle parter ved behov.

På denne måten kan data krypteres med den offentlige nøkkelen og kun åpnes av den som har den private hemmelige nøkkelen. Dermed sikres dataenes konfidensialitet.

Eventuelt så kan informasjon krypteres med den private nøkkelen og alle som har den offentlige nøkkelen har en garanti for at informasjonen er kryptert av eieren av den private nøkkelen, og ikke endret av andre, noe som sikrer dataenes integritet.

Ved denne metoden, som kalles sikker meldingsutveksling (Illustrasjon 19), kan to parter utveksle kryptert informasjon uten å avsløre noen av de private nøklene. Dette gjøres ved at begge parter har hvert sitt nøkkelpar, og utveksler de offentlige nøklene. Informasjonen krypteres så med mottakers offentlige nøkkel og sendes.



Illustrasjon 19: Sikker meldingsutveksling

4.4.2 Digitale signaturer

"PKI Digital Signatures for Machine Readable Travel Documents" [20] spesifiserer bruk av digitale signaturer som en moderne erstatning for den om enn marginale sikkerheten i håndskrevne signaturer på tradisjonelle reisedokument.

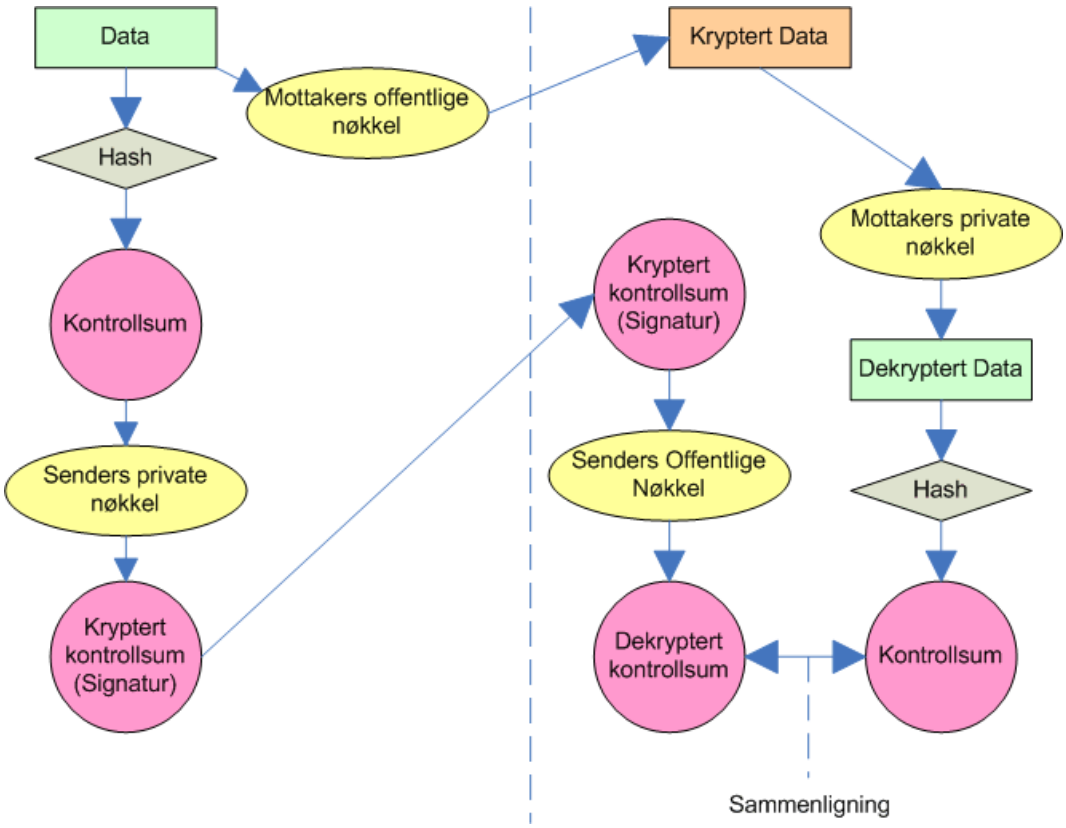
Digital signatur er en teknikk for å elektronisk signere data som i seg selv ikke nødvendigvis er kryptert. Digitale signaturer sertifiserer med andre ord at dataene kommer fra riktig avsender. Samtidig kan ikke avsender senere nekte for å ha signert informasjonen. Den digitale signaturen sikrer med andre ord autorisering ved at den forteller hvorvidt dataene er signert av avsender eller

ikke. Samtidig avslører den digitale signaturen hvorvidt dataene er de samme som signaturen ble generert ut ifra, eller om de har blitt byttet ut på veien.

Digitale signaturer baserer seg på *"hashing"* (eng.) teknikk. Det vil si at spesifikke matematiske operasjoner utføres på dataene. Dette gir ut en bitstreng, som kun kan dannes av den spesifikke algoritmen som er brukt på de spesifikke dataene. Bitstrengen som kalkuleres er ikke helt ulik kontrollsummene som kalkuleres for MRZ-feltet i kapittel 3.3.2, bare mer avansert. Når bitstrengen er kalkulert krypteres den med senderens private nøkkel. Den digitale signaturen sendes så med dataene den beskytter til mottakeren.

Mottakeren kan så verifisere hvorvidt dataene faktisk er sendt fra den riktige senderen ved å dekryptere bitstrengen med senderens offentlige nøkkel. Deretter genererers ny bitstreng fra dataene som er mottat ved å bruke den samme hash-algoritmen. Deretter sammenligners den dekrypterte bitstrengen med den egengenererte bitstrengen. Dersom disse er eksakt like er dataene signert av avsender.

Illustrasjon 20 viser en overføring av asynkront kryptert data beskyttet med senderens digitale signatur.



Illustrasjon 20: Autentisering ved digital signatur

Bitstrengen som brukes i maskinlesbare reisedokument til å lage den digitale signaturen lages ut fra den maskinlesbare sonen (MRZ) på datasiden. Denne krypteres så med en av utstedernasjonens private nøkler.

4.4.3 PKI Sertifikat

Et av de største problemene i forhold til offentlig nøkkel kryptografi og digitale signaturer er problemet med å verifisere nøklenes og signaturenes eiere. Dette løses normalt ved at uavhengige organisasjoner kalt CA (eng. *"Certificate Authoroty"*) utsteder egensignerte sertifikat som verifiserer mottakeren. I mange tilfeller utsteder de også egne nøkkelpar tilhørende sertifikatet.

Disse sertifikatene inneholder stort sett følgende informasjon:

- Sertifikatets serienummer
- Utsteder (CA)
- Gyldig fra / til
- Sertifikatholders navn
- Sertifikatholders offentlige nøkkel
- Digital signatur over all informasjonen innsatt av CA

Disse organisasjonene må så verifiseres av en CA hakket over i hierarkiet, helt opp til øverste "Rot-CA". Videre kryssverifiserer forskjellige CA-hierarkier hverandre.

Denne tradisjonelle PKI Sertifikat strukturen er rimelig kompleks og uoversiktlig. I den kommersielle verden, der sertifikat og nøkler endres hyppig kreves det hyppige oppslag i CA-databasene for verifisering. Samtidig er det også behov for lister, såkalte CRL (eng. *"Certificate Revocation List"*), over sertifikat som ikke lengre er gyldige.

4.4.4 ICAO/TAG Digital Signatur Infrastruktur

Miljøet ICAO opererer i er veldig forskjellig fra det kommersielle internett. Selv om alle 188 av ICAO medlemsland opererer med flere forskjellige nøkler vil det likevel være relativt få nøkler som vil være rimelig statiske i forhold til utskiftning. Derfor har ICAO gått inn for en forenklet løsning i forhold til tradisjonell PKI (eng. *"Public Key Infrastructure"*).

Av sikkerhetsmessige grunner er det ikke ønskelig at ICAO utsteder eller innehar enhver nasjons hemmelige private nøkler. Med dette som bakgrunn er det utarbeidet en todelt løsning:

1. Nasjonene(/Organisasjonene) genererer sine egne nøkkelpar. Disse nøklene brukes så til å kalkulere den digitale signaturen som brukes når reisedokumentet utstedes.

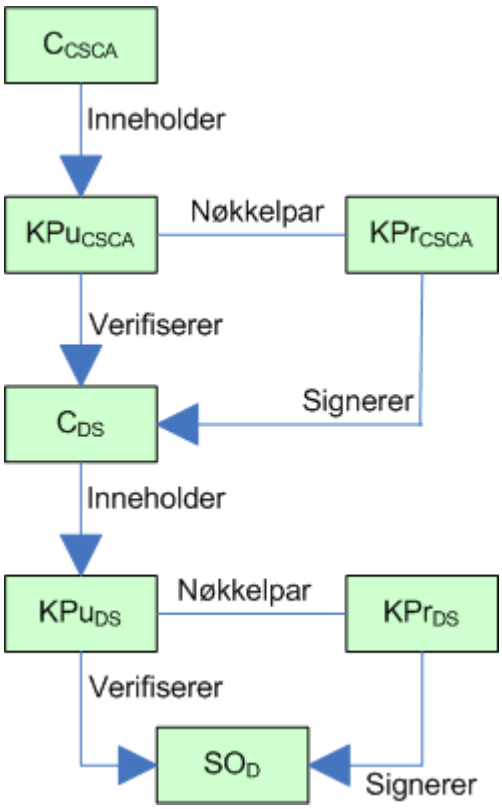
2. ICAO oppretter en katalogtjeneste (eng. *"Public Key Directory, PKD"*) som brukes til å effektivt dele de tilhørende offentlige nøklene til alle

medlemslandene. Dette er en enkel tjeneste som mottar informasjon om nye offentlige nøkler, lagrer dem, og sprer informasjonen om den nye nøkkelen til de andre nasjonene som overfører den til sine grensekontrollsystem.

ICAO erkjenner også en annen og potensielt bedre løsning for spredning av offentlige nøkler. Det vil være å lagre dem på hvert enkelt reisedokument. Derfor er det satt av plass på den trådløse brikken til å lagre denne informasjonen. Dette er løsningen som anbefales implementert som den beste av ICAO. Den er forøvrig ikke gjort obligatorisk på grunn av kravet om at løsningene må tilfredsstille både kommunikasjonsgrensesnitt type A og type B som defineres av ISO 14443[14]. Type A, som kun er minnebasert, er ikke kompleks nok til å kunne foreta sikker autentisering og det er derfor ikke ønskelig at nøkkelen skal ligge fritt tilgjengelig. Type B er derimot i stand til sikker autentisering og det anbefales derfor at innhenting av nøkkel fra selve reisedokumentet brukes som primær nøkkelkilde for reisedokument av type B og kontrollsystem som støtter dette. Katalogtjenesten ICAO PKD vil dermed fungere mer som en sikkerhetskopi med mulighet for bekreftelse av nøkkelens integritet.

4.4.5 Hierarkisk infrastruktur

I mange land med mange innbyggere vil det ofte være praktisk å utstede(trykke) reisedokumentene på forskjellige steder internt i landet. Derfor legger ICAO opp til at hver nasjon/organisasjon skal kunne ha et eget nøkkelpar for kryptering($KPr_{DS\ og}$ KPu_{DS}) for hver lokasjon som utsteder offisielle elektroniske reisedokument. Den private nøkkelen KPrDS signerer dokumentsikkerhetsobjekt (eng. *"Document Security Object, SO_D"*), mens den offentlige nøkkelen KPu_{DS} verifiserer dokumentsikkerhetsobjektets autentisitet(Illustrasjon 21). KPu_{DS} autentisitet bekreftes gjennom dokumentsigneringssertifikatet C_{DS} som utstedes av et sentralt nasjonalt organ for nøkkelutstedelse (eng. *"Country Signing CA, CSCA"*) til hver enkelt dokumentutstedende lokasjon. Dette sertifikatet (C_{DS}), lagres i det maskinlesbare reisedokumentets trådløse brikke eller lastes over i hvert enkelt lands inspeksjonssystem gjennom ICAOs katalogtjeneste PKD (eng. *"Public Key Directory"*). Sertifikatet C_{DS} inneholder den offentlige nøkkelen KPu_{DS}, og er igjen signert med den utstedernasjonens private nøkkel KPr_{CSCA}. C_{DS} verifiseres av den tilhørende offentlige nøkkelen KPu_{CSCA} som ligger utstedende nasjons sertifikat C_{CSCA}. Dette sertifikatet er utstedt og selvsignert av utstedernasjonen og må spres til alle andre ICAO medlemsnasjoner gjennom et lignende system som ICAO PKD.

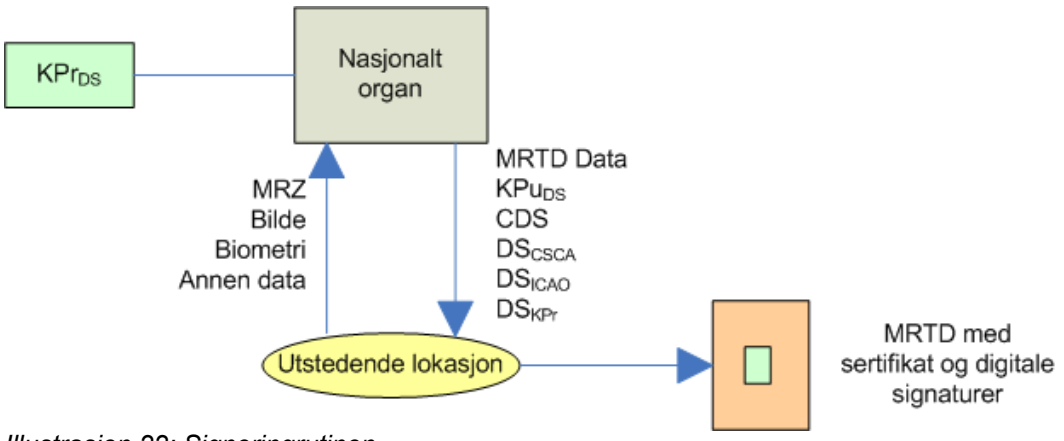


Illustrasjon 21: Nøkkelhierarkiet

Både den nasjonale hemmelige private nøkkelen KPr_{CSCA} og hver enkelt av de nasjonale utstedelseslokasjonenes hemmelige private nøkler KPr_{DS} oppbevares hos det sentrale nasjonale organet, mens de offentlige nøklene KPu_{CSCA} og KPu_{DS} legges i hvert av sertifikatene C_{CSCA} og C_{DS} som begge spres til andre nasjoners inspeksjonssystem via ICAO PKD eller en lignende løsning. C_{DS} kan også legges i den trådløse brikken.

4.4.6 Utstedelsesprosedyren

Når så et reisedokument skal utstedes lages det fysiske reisedokumentet på en av lokasjonene nasjonen har spesifisert. Deretter sendes all informasjon som skal krypteres og digitalt signeres til det sentrale nasjonale organet (Illustrasjon 22). Her krypteres biometriske data med krypteringsteknologien valgt av utstedende nasjon. Deretter returneres informasjonen som ble sendt inn sammen med utstedende nasjonale lokasjons offentlige nøkkel (KPr_{DS}) lagt inn i utstedende lokasjons sertifikat (C_{DS}). Dette er igjen signert at den nasjonale hemmelige private nøkkelen (KPr_{CSCA}), som igjen eventuelt er signert av ICAOs hemmelige nøkkel (kapittel 4.4.7 Nøkkelutveklsling). All denne informasjonen er deretter signert med de utstedende lokasjons hemmelige private nøkkel (KPr_{DS}).



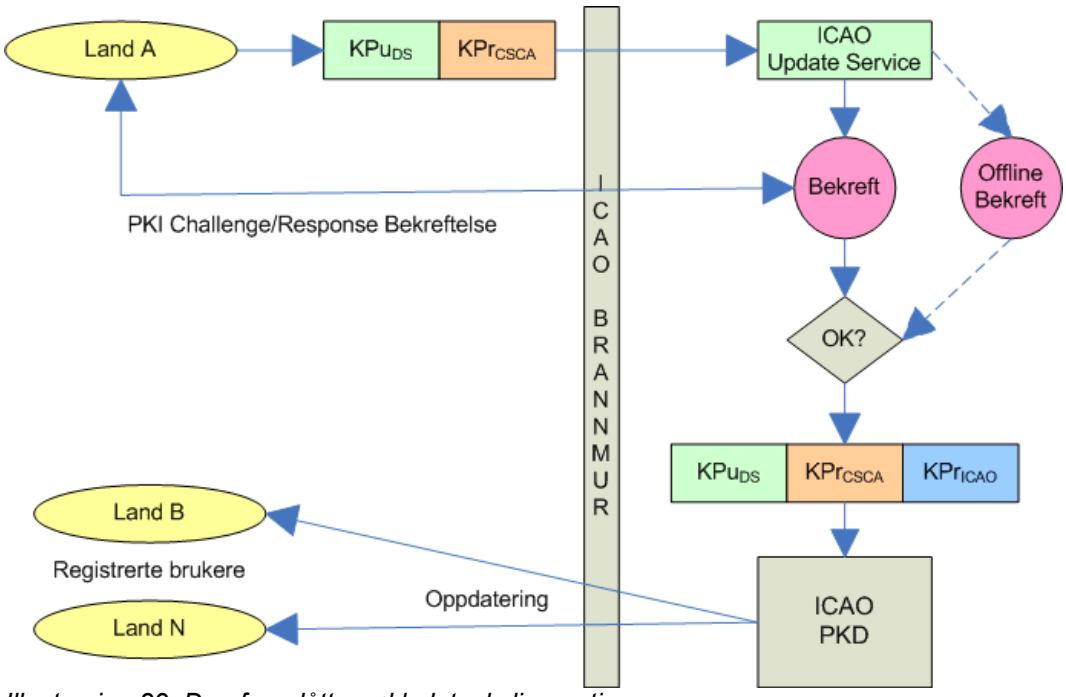
Illustrasjon 22: Signeringrutinen

Informasjonen fra den maskinlesbare sonen (MRZ) og et digitalt fotografi, der begge er signert med utstedende lokasjons hemmelige private nøkkel (KPr_{DS}) regnes som det absolutte minimumskrav i forhold til hva som må implementeres dersom kun den maskinlesbare sonen (MRZ) og digitalt bilde skal lagres i den trådløse brikken.

4.4.7 Nøkkelutveksling

I tillegg er det åpnet opp for at dokumentsigneringssertifikatet, $C_{DS,}$ også kan signeres med ICAO sin hemmelige nøkkel for å tilfredsstille kravene for digitale sertifikat. Denne informasjonen må i så fall sendes til ICAO PKD som signerer og sender tilbake. Informasjonen som da lagres i det elektroniske reisedokumentet vil dermed bli lik informasjonen som lagres i ICAO PKD.

Oversendelse av nøkler mellom en nasjons sentrale organ og ICAO PKD finner sted på følgende forenklede måte (Illustrasjon 23). Utstedende lokasjons offentlige nøkkel, KPu_{DS}, signeres med utstedende nasjons private sertifikatnøkkel (Kpr_{CSCA}). Denne strukturen kalles et dokumentsigneringssertifikat (eng. *"Document Signer Certificate, C_{DS}"*) og sendes til ICAO Update Service. ICAO har den offentlige delen av sertifikatnøkkelparet og kan verifisere sertifikatet. ICAO krypterer så informasjonen med sin egen hemmelige nøkkel og returnerer denne til avsenderlandet.



Illustrasjon 23: Den foreslåtte nøkkelutvekslingsrutinen

Avsenderlandet har ICAO sin offentlige nøkkel og kan dekryptere og verifisere denne signaturen. Deretter krypteres informasjonen med ICAO sin offentlige nøkkel og sendes tilbake til ICAO som dekrypterer og sammenligner de to mottatte meldingene. På denne måten garanteres det at informasjonen som ble sendt til ICAO kommer fra riktig land og er uendret. Samtidig får landet en garanti for at informasjonen kom uendret frem til ICAO PKD. Deretter signerer ICAO den opprinnelige meldingen med sin egen hemmelige nøkkel og lagrer denne i katalogstrukturen og informerer de andre nasjonene.

4.4.8 Tilgangskontroll

Det spesifiseres to valgfrie tilgangskontroller, en grunnleggende og en utvidet tilgangskontroll.

4.4.8.1 Grunnleggende tilgangskontroll

"PKI for Machine Readable Travel Documents offering ICC Read-Only Access" [12] åpner for en frivillig implementasjon av en grunnleggende tilgangskontrollmekanisme (eng. "*basic access control mechanism"*). Denne mekanismen skal hindre tilgang til brikkens innhold, med mindre inspeksjonssytemet kan bevise at det er autorisert til å få tilgang til brikken. Dette beviset ved en anrop-svar (eng. "*challenge-response*") protokoll, der inspeksjonssytemet beviser kjennskap til brikkeindividuelle grunnleggende dokumenttilgangsnøkler (eng. "*Document Basic Access Keys*"), K_{ENC} og K_{MAC} som genereres ut fra hvert reisedokuments maskinlesbare sone (MRZ).

Inspeksjonssystemet må inneha denne informasjonen før brikken kan leses. Derfor leses den optisk eller visuelt fra det maskinlesbare reisedokumentet, fra den maskinlesbare sonen (MRZ). Denne informasjonen kan enten leses maskinelt gjennom den optisk lesbare skrifttypen OCR-B eller skrives manuelt inn av en inspektør. Informasjonen sendes så til den trådløse brikken. En brikke som innehar den grunnleggende tilgangskontrollen vil kun svare "*Security status not satisfied"* dersom et system prøver å iverksette annen kommunikasjon uten at tilgangskontrollen er gjennomført.

Til utregning av K_{ENC} og K_{MAC} brukes den symmetriske blokk-krypteringsteknologien 3DES (eng. "*Triple Data Encryption Standard"*) som spesifiseres i "*NIST Special Publication 800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher"* [21] på følgende måte:

Lesesystemet henter ut en sammentrekking av dokumentnummeret, fødselsdatoen og utløpsdatoen, med tilhørende kontrollsummer. Så lages det en SHA-1 hash-sum av denne informasjonen, hvorav de første 32 bitene av hash-summen danner en tallrekke kalt K_{seed}. Denne brukes så som input i en ny SHA-1 hash-sum sammen med en av de 32 bits verdiene 0x 00 00 00 01 eller 0x 00 00 00 02, der 1 brukes for å generere krypteringsnøkkelen K_{ENC}, mens 2 brukes for å generere den tilhørende autentiseringsnøkkelen K_{MAC}. De første 16 bytene av hver av hash-summene som genereres utgjør henholdsvis K_{ENC} og K_{MAC}.

Inspeksjonssystemet genererer disse nøklene ved hver eneste passkontroll, mens den trådløse brikken har disse ferdig utregnet og lagret i den logiske datastrukturen, da nøklene utregnes under utstedelsesprosessen.

Selve tilgangskontrollprosessen foregår på følgende måte:

Inspeksjonssystemet sender en "GET CHALLENGE" kommando til den trådløse brikken. Brikken genererer så et tilfeldig generert tall (8 bytes), *RND.ICC*, som den sender til leseren. Leseren generer deretter et eget tilfeldig tall (8 bytes), RND.IFD, og en nøkkel (16 bytes) K.IFD. Deretter grupperer inspeksjonssystemet de tilfeldige tallene, RND.IFD og RND.ICC, og nøkkelen K.IFD i et kryptogram, E_{IFD}, som krypteres med krypteringsnøkkelen K_{ENC}. Deretter genereres det en kontrollsum, M_{IFD}, av kryptogrammet (E_{IFD}) som krypteres med autentiseringsnøkkelen K_{MAC}.

Deretter sendes en MUTUAL_AUTHENTICATE melding bestående av kryptogrammet (E_{IFD}) og den tilhørende kontrollsummen (M_{IFD}) til den trådløse brikken. Brikken verifiserer så kontrollsummen (M_{IFD}) med autentiseringsnøkkelen K_{MAC} som ligger i brikkens logiske datastruktur (LDS) og dekrypterer kryptogrammet (E_{IFD}). Deretter kontrolleres det at inspeksjonssytemet returnerte den korrekte RND.ICC.

Så generer den trådløse brikken en egen tilfeldig valgt nøkkel(16 bits), K.ICC og grupperer denne, RND.INF og RND.ICC i kryptogrammet E_{ICC}, som krypteres med K_{ENC}. Så lager den en kontrollsum M_{ICC} av kryptogrammet E_{ICC} og krypterer denne med K_{MAC}. Deretter sendes E_{ICC} og M_{ICC} tilbake til inspeksjonssytemet,

som dekrypterer kontrollsummen med K_{MAC} og verifiserer denne. Så krypteres E_{ICC} med K_{ENC} og det kontrolleres at brikken har returnert den riktige RND.IFD.

Nå genererer både inspeksjonssystemet og den trådløse brikken de unike sesjonsnøklene (16 bytes) KS_{ENC} og KS_{MAC}. Dette gjøres ved at den logiske operasjonene XOR kjøres på K_{IFD} og K_{ICC}. Så brukes hver av XOR-verdiene sammen med K_{SEED} som inndata for å generere to nye SHA-1 hashsummer. De 16 første bytene fra hver av SHA-1 resultatene brukes så til nøklene KS_{ENC} og KS_{MAC}.

KS_{ENC} og KS_{MAC} brukes så som sesjonsnøkler for 3DES krypteringen som brukes i den videre kommunikasjonen.

4.4.8.2 Utvidet tilgangskontroll

For stater som ønsker en annen tilgangskontroll enn den generelle som tilbys av ICAO gjennom "P*KI for Machine Readable Travel Documents offering ICC Read-Only Access"* [12] legges det også opp til en utvidet tilgangskontroll (eng. "*Extended Access Control"*). Denne innehar mye likheter med den grunnleggende tilgangskontrollen men de grunnleggende dokumenttilgangsnøklene, K_{ENC} og K_{MAC}, er byttet ut med et annet sett nøkler. Dette nøkkelparet er det opp til hver enkelt utstedende nasjon/organisasjon å velge. Disse kan enten være symmetriske nøkler utledet fra den maskinlesbare sonen (MRZ) og en nasjonal masternøkkel, eller asymmetriske nøkkelpar.

4.4.9 Autentisering

"PKI for Machine Readable Travel Documents offering ICC read-only access" [12] spesifiserer to autentiseringsmekanismer.

4.4.9.1 Passiv Autentisering

I tillegg til datagruppene som spesifiseres i *"Development of a Logical Data Structure – LDS – for Optional Capacity Expansion Technologies, Revision 1.7"* [13] inneholder brikken også et dokumentsikkerhetsobjekt (eng. *"Document Security Object, SO_D"*). Dette objektet er digitalt signert av utstedende nasjonale lokasjon og inneholder en hash-sum kalkulert ut i fra innholdet i den logiske datastrukturen(LDS). Et inspeksjonssystem som allerede har utstederlokasjons offentlige nøkkel, KPu_{DS}, eller har lest dokumentsigneringssertifikatet, C_{DS}, fra det maskinlesbare reisedokumentet, vil være i stand til å verifisere dokumentsikkerhetsobjektet(SO_D). På denne måten, gjennom SO_D, autentiseres innholdet i den logiske datastrukturen (LDS).

Fordi denne metoden ikke krever noen prosessering på den trådløse brikken på det maskinlesbare reisedokumentet kalles den passiv autentisering, og er lagt inn som et minimumskrav for autentisering i *"PKI for Machine Readable Travel Documents offering ICC read-only access"* [12].

Passiv autentisering kontrollerer at innholdet i dokumentsikkerhetsobjektet(SO_D) og den logiske datastrukturen(LDS) er autentisk og ikke endret. Det forhindrer forøvrig ikke eksakt kopiering av innholdet eller utbytte av hele databrikken i

reisedokumentet. Derfor bør bruk av passiv autentisering kombineres med en fysisk kontroll av selve reisedokument.

4.4.9.2 Aktiv Autentisering

ICAO spesifiserer også en metode for å unngå mulighet for at hele databrikken er byttet ut. Denne metoden er valgfri, men anbefales å brukes.

Aktiv autentisering baserer seg på en anrop-svar (eng. *"challenge-response"*) protokoll mellom leseren og reisedokumentets trådløse brikke. Ved bruk av denne metoden innføres et ekstra aktivt nøkkelpar for autentisering (eng. *"Active Authentication Key pair"*) kalt KPr_{AA} og KPu_{AA}. Datagruppe 15 er forbeholdt den offentlige nøkkelinformasjonen KPu_{AA} som lagres i denne. Deretter kalkuleres en kontrollsum av datagruppe 15. Denne lagres i dokumentsikkerhetsobjektet(SO_D) og er derfor autentisert av utsteders digitale signatur. Den tilhørende private nøkkelen (KPr_{AA}) lagres i brikkens sikre minne.

Systemet kan så verifisere at dokumentsikkerhetsobjektet (SO_D) er lest fra den genuine brikken som sitter i det genuine maskinlesbare reisedokumentet ved følgende metode:

Systemet verifiserer at dokumentsikkerhetsobjektet (SO_D) er lest fra den genuine brikken i det genuine maskinlesbare reisedokumentet ved å kombinere autentisering av den visuelle maskinlesbare sonen (MRZ) gjennom en kontrollsum av den maskinlesbare sonen (MRZ) som ligger lagret i dokumentets sikkerhetsobjekt (SO_D), og anrop-svar metoden som bruker det aktive nøkkelparet for autentisering, KPr_{AA} og KPu_{AA}. Denne metoden beskrives i anneks D.2 i "*PKI for Machine Readable Travel Documents offering ICC read-only access"* [12].

Aktiv autentisering forutsetter forøvrig at databrikken har prosesseringsegenskaper. Den støttes altså bare av kommunikasjonsgrensesnitt type B fra kapittel 4.2.5 som spesifiseres i ISO 14443 [14].

4.4.10 Algoritmer

"PKI Digital Signatures For Machine Readable Travel Documents" [20] foreslår tre signeringsalgoritmer for digitale signaturer. Det legges opp til at hver enkelt nasjon kan velge selv hvilken av disse de vil implementere. Alle tre signeringsalgoritmene beskrives mer inngående i *"NIST Special Publication 800-57 Recommendation for Key Management – Part 1: General"* [22] av Barker et al.

4.4.10.1 DSA

DSA (eng. *"Digital Signature Algorithm"*) spesifiseres i *"FIPS 186-2, Federal Information Processing Standards (FIPS PUB) 186-2(+ Change Notice), Digital Signature Standard (DSS)"* [23]. Denne algoritmen, som er en variant av El Gamal Digital Signatur, baserer seg på det diskrete logaritmeproblemet [24] og ble utviklet for den amerikanske statens digitale signaturer.

I *"PKI Digital Signatures for Machine Readable Travel Documents"* anbefales det en modulig for nøkkelgenerering på 1024 bits og 160 bits, som produserer en digital signatur på 320 bits (40 bytes). Algoritmen krever en offentlig nøkkel på minimum 1024 bits for å være sikker.

Anbefalingen fra ICAO bygger på FIPS 186-2 [23] fra 2000. Denne standarden støtter bare nøkler på opptil 1024 bits. En ny utgave *"FIPS 186-3, Federal Information Processing Standards (FIPS PUB) 186-3, Digital Signature Standard (DSS)"* [25]. Dette standardutkastet støtter en sterkere kryptering og det anbefales derfor en minimumsstørrelse på moduli, 2048 bits og 224 bits for nøklene, KPr_{DS} og KPu_{DS} som brukes av den nasjonale lokaliseringenes signaturer.

Videre anbefales det at det nasjonale nøkkelparet, KPr_{CSCA} og KPu_{CSCA}, bruker moduli på 3072 bits og 256 bits. Dette nøkkelparet skal normalt ha en lang levetid, og byttes ut sjeldnere enn hvert 5. år og må følgelig være sikre i hele denne tiden.

Videre anbefales det at et eventuelt aktivt nøkkelpar for autentisering, KPr_{AA} og KPu_{AA} , bruker en moduli på minimum 1024 bits og 160 bits. Denne trenger ikke et like høyt sikkerhetsnivå fordi all prosesseringen skjer internt i den trådløse brikken.

4.4.10.2 RSA

RSA, *Rivest Shamir Adleman*, algoritmen spesifiseres i *"RFC3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"* [26]. Denne algoritmen er meget sterk, men er relativt langsom i signeringene, men er tilsvarende rask i verifiseringen.

RFC 3447 spesifiserer to signaturmekanismer: RSASSA-PSS og RSASSA-PKCS1_v15. Standarden anbefaler bruk av RSASSA-PSS, men åpner også opp for at begge bør støttes av alle utstedende og inspiserende system. RSASSA-PSS regnes som arvtakeren etter RSASSA-PKCS1_v15.

For å tilfredsstille sikkerhetskravene kreves det i *"PKI Digital Signatures for Machine Readable Travel Documents"* [20] at modulusen som brukes for å generere nøkkelparene for signering på minimum 2048 bits, noe som produserer en digital signatur på 1024 bits som krever en offentlig nøkkel på 1088 bits. I den nyere *"PKI for Machine Readable Travel Documents offering ICC Read-Only Access"* [12] videreføres anbefalingen om 2048 bits nøkler, KPr_{DS}, for signering av dokumentenes sikkerhetsobjekt, SO_D.

For det nasjonale nøkkelparet for sertifisering KPr_{CSCA} og KPu_{CSCA}, anbefales det en minimumsstørrelse på modulus på 3072 bits, mens et eventuelt aktivt nøkkelpar for autentisering ,KPr_{AA} og KPu_{AA} , bør bruker en modulus på minimum 1024 bits. Denne trenger ikke et like høyt sikkerhetsnivå fordi all prosesseringen skjer internt i den trådløse brikken.

4.4.10.3 ECDSA

ECDSA (eng. *"Elliptical Curve Digital Signature Algorithm"*) spesifiseres i *"American National Standard X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)" [27]*. Denne algoritmen anses som veldig sterk med korte nøkkellengder og relativt rask signaturverifikasjon. *"PKI Digital Signatures for Machine Readable Travel Documents"* [20] anbefaler en nøkkellengde på kun 160 bits, som produserer en digital signatur på 320 bits (40 bytes). Den offentlige nøkkelen er også bare på 161 bits (21 bytes).

I den oppdaterte *"PKI for Machine Readable Travel Documents offering ICC Read-Only Access"* [12] fra 2004 anbefales det å bruke en 224 bits streng til den nasjonale lokaliseringens private hemmelige nøkkel, KPr_{DS}.

Videre anbefales det at nøkkelen, KPr_{CSCA}, som brukes til å signere utstedende lokasjoners sertifikat C_{DS}, bruker 256 bits, mens det for et eventuelt aktivt nøkkelpar for autentisering, KPr_{AA} og KPu_{AA}, anbefales det å opprettholde nøkkelen på 160 bits som spesifiseres i *"PKI Digital Signatures for Machine Readable Travel Documents"* [20].

4.4.10.4 Secure Hash Algorithm (SHA)

I tillegg til disse tre foreslåtte krypteringsteknologiene er SHA (eng. *"Secure Hash Algorithm"*), som spesifiseres i *"FIPS 180-2, Federal Information Processing Standards Publication (FIPS PUB 180-2, Secure Hash Standard (SHS)"* [28] valgt som teknologi for beregning av selve kontrollsummene i de digitale signaturene. *"PKI Digital Signatures for Machine Readable Travel Documents"* [20] spesifiserer kun bruk av SHA-1 for å unngå behovet for å spesifisere hvilken algoritme som er brukt. I *"PKI for Machine Readable Travel Documents offering ICC Read-Only Access"* [12] er denne utvidet til å også åpne for bruk av SHA-224, SHA-256, SHA-384 og SHA-512. Disse kalles ofte kollektivt for SHA-2.

Riktig hash algoritme må velges ut i fra hvilken signaturalgoritme som er valgt.

4.4.11 Tilleggskryptering

I tillegg til sikkerhetsmekanismene som tilbys åpnes det også for at utstedende nasjoner/organisasjoner selv kan kryptere deler av informasjonen som lagres i elektroniske passet slik som biometriske data og utsteders egen valgfrie informasjon. Her står nasjonene fritt til selv å velge sikkerhetsprinsipp og algoritmer. Nøkler for dekryptering og informasjon om algoritmer som er brukt må i så fall implementeres gjennom reisedokumentet eller ved en tjeneste av typen ICAO PKD eller lignende.

5 Teknisk evaluering

ICAO spesifiserer flere forskjellige sikkerhetsteknikker for beskyttelse av innholdet på den trådløse brikken. Disse deles inn i obligatoriske og valgfrie teknikker. De obligatoriske kravene er forøvrig begrenset av ICAOs valg om å støtte både Type A og Type B kommunikasjonsgrensesnittene som spesifiseres av ISO 14443 [14]. Type A er kun en minnebrikke uten intern prosesseringsegenskaper, og setter derfor begrensninger på hva slags sikkerhetsteknikker som lar seg innføre. Derfor er alle prosesseringskrevende teknikker gjort valgfrie. Dette har ført til at sikkerheten i reisedokument som kun følger minimumskravene er rimelig svak. Samtidig har de valgfrie sikkerhetsteknikkene også vist seg å være rimelig begrenset.

5.1 Obligatoriske spesifikasjoner

Den eneste obligatoriske sikkerthetsteknikken som spesifiseres av ICAO er passiv autentisering.

5.1.1 Passiv autentisering

Denne teknikken sikrer at innholdet i den trådløse brikkens logiske datastruktur, LDS, er autentisk og ikke er endret.

Dette gjøres ved at det genereres en hash-sum av hver av datagruppene som er benyttet i den logiske datastrukturen (LDS). Hash-summene lagres så i en del av den logiske datastrukturen som kalles dokumentsikkerhetsobjektet (SO_D), som er en del av den logiske datastrukturen. Deretter signeres hele dokumentsikkerhetsobjektet, med utsteders private nøkkel. Når inspeksjonssytemet så skal foreta en passiv autentisering laster det over både datagruppene og dokumentsikkerhetsobjektet fra den logiske datastrukturen. Deretter verifiserer systemet signaturen over dokumentsikkerhetsobjektet ved hjelp av dekryptering med utsteders offentlige nøkkel. Så genererer systemet hash-summer fra datagruppene med samme algoritme som er brukt av utsteder. De genererte hash-summene sammenlignes så med hash-summene fra den logiske datastrukturen. Dersom disse er like er det verifisert at innholdet av dokumentsikkerhetsobjektet og innholdet i datagruppene er autentisk og ikke er endret.

ICAOs opprinnelig utkast til passiv autentiseringsmetode, som ble spesifisert gjennom "*A Proposed Methodology for an ICAO KPI Infrastructure for Implementation of Digital Signatures on Machine Readable Travel Documents*" [29] og "*Development of a Logical Data Structure (LDS) for Optional Capacity Expansion Technologies*" [13] fra 2003, inneholdt et stort sikkerhetsproblem. Denne foreslo at hash-summene fra den personlige informasjonen fra Datagruppe 1 og de biometriske datagruppene skulle legges i datasikkerhetsobjektet (SO_D) og signeres hver for seg. Dette åpnet for et alvorlig sikkerhetsproblem da seperate signaturer la til rette for forfalskning av reisedokumentene.

Angrepet foregår ved at angriperen får tak et pass med sin egen identitet og biometri. Deretter lytter han på kommunikasjonen av et annet gyldig pass og får tak i en kopi av personens digitalt signerte identitet. Deretter lager angriperen et nytt smartkort med angriperens biometri, men der angriperens identitet er byttet ut med den andre personens identitet. Hver signatur vil så bli kontrollert av inspeksjonssytemet men angrepet vil ikke la seg avsløre. Dette angrepet vil forøvrig kun la seg gjennomføre dersom både angripers og offers reisedokument er utstedt av samme utsteder, da det kreves samme offentlige nøkkel for å verifisere de digitale signaturene.

I de oppdaterte utgavene av "*PKI Digital Signatures For Machine Readable Travel Documents*"[20] og "Readable Travel Documents offering ICC Read-Only Access"[12] fra 2004 løses dette problemet ved at identiteten kryptografisk bindes til biometrien ved at alle hash-summene lagres i dokumentsikkerhetsobjektet (SO_D) og at utsteder deretter digitalt signerer hele dokumentsikkerhetsobjektet, inkludert alle hash-summene. Ved å kryptografisk binde identiteten og biometrien sammen blir angrepet over umulig siden hash-summen i dokumentets sikkerhetsobjekt ikke vil stemme overens med hash-summen som er generert av inspeksjonssytemet ut fra datagruppene i den logiske datastrukturen (LDS). Dersom angriperen prøver å endre hash-summen i tillegg til identiteten vil dette føre til at verifikasjonen av den digitale signaturen feiler.

Selv om dette sikkerhetsproblemet er rettet i 2004-spesifikasjonene gir passiv autentisering fortsatt lite beskyttelse. Metoden beskytter bare innholdet av den logiske datastrukturen. Den binder på ingen måte brikken til selve reisedokumentet og hindrer derfor ikke eksakt kopiering eller utskiftning av brikke. Derfor spesifiserer "*PKI for Machine Readable Travel Documents offering ICC Read-Only Access"* [12] at kontrollen bør kombineres med en ekstra fysisk kontroll av reisedokumentet. Med bakgrunn i at en av grunnene for etablering av elektroniske pass var at forfalsknerne blir stadig mer teknologisk avanserte, gir heller ikke dette tilstrekkelig sikkerhet.

Passiv autentisering har også andre svakheter. Autentiseringsteknikken hindrer ikke uautorisert tilgang til kommunikasjonen mellom inspeksjonssytemet og reisedokumentet, da det er systemet som verifiserer brikkens dataintegritet etter at den er oversendt. Brikken foretar ingen autentisering av inspeksjonssystemet før informasjonen sendes. Passiv autentisering alene gir derfor ingen beskyttelse mot hemmelige avlesninger, såkalte skummingsangrep (eng. "*Skimming'"*). Skimming-angrep vil si angrep der en uautorisert leseenhet aktivt iverksetter kommunikasjonen med brikken for å få tak i informasjon. Dette gjøres ved at den uautoriserte leseren utstråler energi mot brikken for å iverksette kommunikasjonen, på samme måte som en autorisert leser gjør ved normal kommunikasjon. Dette angrepet begrenses delvis av at trådløse brikker som følger ISO 14443-standarden kun har en maksimal leseavstand på opptil 10 cm. Men det finnes også situasjoner der angriper kan komme innenfor 10 cm og gjennomføre et angrep uten at passholderen er klar over dette. Et slikt eksempel kan være der angriper er plassert ved siden av passholderen i et tog eller fly.

Dersom passholderen oppbevarer passet i en lomme vil det være fullt mulig for angriper å ha en leser i sin egen lomme like ved siden av.

Avstanden mellom leser og brikke er også mulig å øke noe ved at leseren sender sterkere signaler enn det som spesifiseres som lovlige verdier i ISO 14443. Dette begrenser seg forøvrig til at brikkens signalstyrke synker proporsjonalt med at avstanden økes etter formelen

$$a = \sqrt[6]{b}$$

,der a er brikkens strømtilgang og b er avstanden mellom leseren og brikken. Til tross for denne begrensningen viser Kfir og Wool i "*Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems"* [30] hvordan avstanden mellom leseren og kortet femdobles til omtrent 50 cm. Ved denne avstanden økes angripers muligheter for hemmelige angrep betraktelig. Dersom lesesystemets leserenhet og senderenhet splittes opp til to fysisk mindre enheter, kan senderen befinne seg lengre unna og kompensere med sterkere signal, mens mottakeren ligger skjult i brikkens nærhet. Skimmingangrep medfører flere potensielle farer, som identitetstyveri eller sporing. Et annet potensielt angrep kan være en bombe utstyrt med en skimmingsleser som går av når en spesifisert statsborger eller person kommer innenfor leserens kraftfelt og brikken leses.

Et annet angrep mot passiv autentisering er tyvlytting på den lovlig iverksatte kommunikasjonen mellom brikken og leseren. Dette foregår ved at angripers leser plasseres innenfor området som defineres som kommunikasjonsfeltet mellom den legitime leseren og passet. I motsetning til skimmingangrep er ikke angriperens leser en aktiv deltaker i kommunikasjonen. Den lytter kun på informasjonsstrømmen og kan kopiere denne. Informasjonsstrømmen kan deretter avspilles mot inspeksjonssytemet og lure dette til å tro at det kommuniserer med et legitimt reisedokument.

Kfir og Wool viser også et angrep der avstanden mellom inspeksjonssytemet og den legitime brikken kan økes betraktelig. Dette gjøres ved hjelp av et slags relé, bestående av to enheter. Disse kalles ghost og leech, og plasseres mellom brikken og inspeksjonssytemet. Mellom disse er det en rask digital kommunikasjonskanal. Angrepet gjennomføres så ved at leech, som er en leseenhet av samme type som brukes i inspeksjonssystemet, induserer strøm til brikken og dermed igangsetter kommunikasjonen. Brikken svarer så i den tro at den kommuniserer med en legitim leser. Dette svaret fanges så opp av leech og sendes via den digitale linjen til ghost. Ghost bringer så informasjonen videre til den legitime leseren som dermed lures til å tro at den kommuniserer direkte med brikken. Den største forskjellen er at ghost ikke er avhengig av å generere strøm fra leserens induksjonsfelt. Ved hjelp av en egen strømkilde kan derfor avstanden mellom ghost og den autentiserte leseren økes ved at signalstyrken økes. Kfir og Wool viser hvordan avstanden mellom ghost og leseren kan være opptil 50 meter, mens avstanden mellom leech og brikken kan være opptil 50 cm. Denne avstanden kan også økes ved høy overføringshastighet mellom ghost

og leech. Potensielt kan man da lure en passkontroll som kun implementerer passiv autentisering med et forfalsket pass uten innebygget brikke, for så å kringkaste informasjonen fra et annet pass som ikke befinner seg i umiddelbar nærhet.

5.2 Valgfrie spesifikasjoner

ICAO spesifiserer også flere metoder for hvordan beskyttelsen av reisedokumentets informasjon kan beskyttes bedre utover beskyttelsen som tilbys gjennom passiv autentisering. Et par av disse er universelle og er tilpasset reisedokument som følger begge kommunikasjonsgrensesnittene som spesifiseres av ISO 14443. Men flesteparten krever kommunikasjonsgrensesnitt B og brikker med logiske prosesseringsegenskaper.

5.2.1 Faraday-Bur

En av de universelle metodene som spesifiseres av ICAO er bruk av et såkalt Faraday-bur (eng. "*Faraday-cage"*) til å skjerme den trådløse brikken fra inngående induksjon og signalering uten passinnehavers godkjennelse. Et Faraday-bur går ut på at brikken pakkes inn i metall, ofte aluminium. Frekvensen, 13,56 Mhz, som spesifiseres av ISO 14443 og som brukes i maskinlesbare reisedokument, er ikke i stand til å trenge gjennom metaller og absorberes. Dersom en metallflate implementeres i passets perm vil denne dermed beskytte brikken mot skimmingangrep, for eksempel dersom innehaveren har passet i en lomme. For at den trådløse brikken skal kunne induseres og utveksle informasjon må passboken forevises ved at den åpnes.

Faraday-bur sikrer dermed delvis reisedokumentets datakonfidensialitet, gjennom å forhindre skimmingangrep. Forøvrig tilbyr den ingen beskyttelse mot tyvlyttingsangrep, da disse baserer seg på angrep etter at kommunikasjonen er igangsatt ved at passboken er forevist.

Foreløpig er denne metoden kun spesifisert som frivillig, men med anbefaling av ICAO om bruk. Til tross for dette, har flere land gått i gang med utstedelse av elektroniske reisedokument uten bruk av Faraday-bur.

5.2.2 MRZ-sammenligning

En annen av de universelle metodene for utbedring av sikkerhet er sammenligning av den konvensjonelle maskinlesbare sonen (MRZ) som leses fra datasiden gjennom OCR-B teknologien og kopien av den maskinlesbare sonen som ligger lagret i datagruppe 1 i den trådløse brikkens logiske datastruktur (LDS). ICAO-spesifikasjonene sier at den maskinlesbare sonen skal kontrolleres, men lar det være opp til inspiserende nasjon å selv velge om denne informasjonen skal hentes fra den maskinlesbare sonen eller fra den trådløse brikkens logiske datastruktur. Følgelig er ingen sammenligning mellom disse påkrevd, selv om den anbefales implementert.

Denne metoden forutsetter forøvrig at MRZ-informasjonen leses fra både dokumentet og den trådløse brikken og sammenlignes av inspeksjonssytemet. Dermed bindes den spesifikke fysiske brikken til et spesifikt fysisk

reisedokument. Metoden forhindrer forøvrig ikke en samlet kopiering av både den trådløse brikken og det konvensjonelle passet.

5.2.3 Grunnleggende tilgangskontroll

Alternativet til bruk av Faraday-bur er den grunnleggende tilgangskontrollen, som også hindrer skimmingangrep. Men i motsetning til Faraday-bur tilbyr denne også beskyttelse mot tyvlytting dersom den implementeres med kryptering av informasjonskanalene i tillegg til autentiseringen av inspeksjonssytemet.

Den grunnleggende tilgangskontrollen hindrer systemet tilgang til informasjonen på den trådløse brikken med mindre inspeksjonssystemet beviser sin legitime tilgang.

Dette gjøres ved at inspeksjonssystemet leser den maskinlesbare OCR-B baserte sonen (MRZ) fra reidesokumentets dataside. Denne kan eventuelt også skrives inn i systemet manuelt dersom den OCR-B leseren av en eller annen grunn ikke fungerer eller ikke er implementert. MRZ informasjonen brukes så til å generere et sett med brikkeindividuelle nøkler, K_{ENC} og K_{MAC}. K_{ENC} og K_{MAC} ligger allerede lagret i den trådløse brikkens logiske datastruktur (LDS) fra da reisedokumentet ble utstedt. Brikken og inspeksjonssystemet bruker så nøklene til å utveksle verifiserende informasjon.

Denne informasjonen kan så brukes videre til å generere unike sesjonsnøkler for 3DES kryptering av informasjonene som utveksles, og forhindre tyvlytting på kommunikasjonskanalene.

Grunnen til at det brukes informasjon fra reisedokumentets dataside som grunnlag for nøkkelgenereringen er at man vil begrense tilgangen kun til personer som har blitt forevist passet av passholderen. Dette gjør den grunnleggende tilgangskontrollen er effektiv mot skimmingsangrep på tilfeldige forbipasserende siden angriper ikke har noe informasjon om offeret. Dermed har han ingen informasjon om innholdet i den maskinlesbare sonen (MRZ) og vil derfor i praksis ikke ha noen mulighet til å finne de kryptografiske nøklene, K_{ENC} og K_{MAC}.

En angriper som vet noe om offeret vil derimot ha en større mulighet. MRZ-informasjonen som brukes som bakgrunn for genereringen av K_{ENC} og K_{MAC} er passets serienummer, passholderens fødselsdato og utløpsdatoen, med tilhørende kontrollsummer. I motsetning til skimmingangrep på tilfeldige forbipasserende vil blant annet fødselsdatoen i mange tilfeller være kjent ved et angrep mot en kjent person. Ved de fleste angrep vil fødselsdatoen i alle fall la seg bestemme innforbi et 5 til 10 års intervall. Videre tildeles passnummerne vanligvis i rekkefølge, og derfor vil også utstedelsesdatoer og utløpsdatoen være mulig å prøve seg frem til. Dette er et problem som ICAO selv fremhver i "*PKI for Machine Readable Travel Documents offering ICC Read-Only Access*" [12]. Rapporten konkluderer med at denne metoden ikke er sikker nok til å hindre et seriøst brute-force (eng.) angrep der angriperen forsøker å gjette serienummeret og utløpsdatoen. Rapporten konkluderer forøvrig med at dette ikke er et reellt

stort proplem siden det finnes andre lettere måter å skaffe seg informasjonen som lagres i passet.

Dette er forsåvidt rett, men rapporten overser det faktum at den biometriske informasjonen som ligger lagret er digitalt signert av utsteder. Den digitale signaturen gir informasjonen en ekstra troverdiget og dermed også verdien. Rapporten behandler heller ikke problemstillingen der angriper har veldig lang tid til å gjennomføre brute-force angrepet, dersom han for eksempel sitter ved siden av offeret på et tog, slik det spesifiseres av Kfir og Wool [30].

Marc Witteman viser i "*Attacks on Digital Passports*" [31] hvoran et brute-force angrep på en nederlandsk implementasjon av den grunnleggende tilgangskontrollen, kan knekkes på under to timer med en vanlig PC. Gjennom undersøkelse av gjennomsnittelig antall passutgivelser daglig og den nederlanske prosedyren for generering av passnummer, oppdaget han en effektiv bitstyrke på kun 35 bits.

Et eksempel på et tidligere ikke omtalt angrep kan være å utsette passet for et brute-force angrep mot den grunnleggende tilgangskontrollen i løpet av utstedelsesprosessen. Et eksempel her er den norske prosedyren for passutstedelse. Norske pass sendes til mottakeren som A-post i delvis anonymiserte konvolutter. Men dersom angriper selv har mottatt et pass i posten vil han lett kunne gjenkjenne konvolutter som potensielt inneholder pass, på utseende og returadressen. Se Illustrasjon 24 for konvolutten norske pass blir sendt i.

Illustrasjon 24: Konvolutten norske pass sendes ut i

En angriper som jobber innen postdistribusjonsbransjen, eller som innehar viten om at offeret har bestilt nytt pass, vil derfor kunne luke ut potensielle passkonvolutter i forsendelsesprosessen eller fra mottakers postkasse. Fordi Norge ikke bruker Faraday-bur (Illustrasjon 10 side 25) vil et brute-force angrep kunne gjennomføres uten at konvolutten må åpnes. Dermed kan konvolutten sendes tilbake i lerveringsprosessen uten at mottaker får vite om angrepet. På grunn av varierende leveringstider vil det i mange tilfeller gå opptil flere dager før

passets eier vil savnet dette, noe som gir en angriper tid til å gjennomføre brute-force angrep selv med lite eller ingen bakgrunnsinformasjon. Forøvrig vil angriper i dette tilfellet kunne beregne seg frem til utstedelsesdatoen med tilhørende kontrollsum med kun et par dagers feilmargin ut i fra viten om at passet er nyutstedt. Dette vil eliminere antall brute-force kombinasjoner kraftig.

Det norske datatilsynet har påpekt at denne praksisen kan innebære en sikkerhetsrisiko, og har etterlyst en risikovurdering av denne. [32] Dette har foreløpig ikke blitt gjort.

Gaurav S. Kc og Paul A. Karger viser i "*Preventing Attacks on Machine Readable Travel Documents"* [33] et større sikkerhetsproblem enn brute-force angrep. Den grunnleggende tilgangskontrollen baserer seg på at datasiden og den maskinlesbare sonen (MRZ) vises til legitime kontrollører i passkontrollen. Pass brukes forøvrig i mange andre sammenhenger der MRZen blir forevist et antall andre personer som ikke skal ha tilgang til biometrien som er lagret i passet. Dette kan gjelde annet personell på flyplassen, bankpersonale eller hotellpersonale. I mange tilfeller tar også hotellekspeditøren en fotokopi av passet ved innsjekk, eller man må legge passet i hotellresepsjonene under oppholdet. Enkelte nasjoner, blant annet Storbritannia, har også lansert planer om å utvide passet til å bli et slags nasjonalt ID-kort der man kan kombinere for eksempel pass, førerkort og medisinske data. Da i henhold til spesifikasjonene i "*Doc 9303 Part 3: Size 1 and Size 2 Machine Readable Official Travel Documents"*. Dette vil i såfall medføre at enda flere uautoriserte får tilgang til informasjonen fra datasiden, som for eksempel bilutleiefirma eller farmasøyter. Dette vil igjen øke den reelle faren for identitetstyveri som følge av for dårlig beskyttelse av informasjonen som lagres i elektroniske reisedokumenter.

Selv om den grunnleggende tilgangskontrollen til en viss grad hindrer skimmingangrep og tyvlytting, gir den ingen sikkerhet mot kopiering av reisedokumentet, så fremt både brikken og dokumentet kopieres.

Den grunnleggende tilgangskontrollen er også avhengig av en prosessor som er i stand til å utføre logiske operasjoner for identifisering av inspeksjonssystemet og utregning av sesjonsnøklene. En implementasjon av den grunnleggende tilgangskontrollen forutsetter derfor bruk av minnebrikker som følger spesifikasjonene av Type B kommunikasjonsgrensesnittet som spesifiseres i ISO 14443.

5.2.4 Aktiv autentisering

"PKI for Machine Readable Travel Documents offering ICC Read-Only Access" [12] spesifiserer også en alternativ metode for den passive autentiseringesteknikken, kalt aktiv autentisering. Denne metoden kommer i tillegg til den obligatoriske passive autentiseringen og bygger videre på denne.

Metoden går ut på at den maskinlesbare sonen (MRZ) leses fra datasiden (med mindre den allerede er lest som følge av den grunnleggende tilgangskontrollen). Denne sammenlignes så med datagruppe 1 i den trådløse brikkens logiske datastruktur (LDS). Den logiske datastrukturens integritet er allerede verifisert

gjennom den passive autentisering. Ved implementasjon av den aktive autentiseringen, ligger den offentlige aktive autentiseringsnøkkelen KPu_{AA}, lagret i datagruppe 15 i den logiske datastrukturen. Gjennom den passive autentiseringen har også integriteteten av denne blitt verifisert. Den private aktive autentiseringsnøkkelen, KPr_{AA}, er verifisert ved at den i utstedelsesprosessen er signert av utsteders hemmelige nøkkel og lagret i brikkens skjulte minne. Dette nøkkelparet brukes så til en toveis challenge-response signalering.

Aktiv autentisering utvider den passive autentiseringen ved å hindre kopiering av dokumentets sikkerhetsobjekt (SO_D) og beviser at SO_D har blitt lest fra den autentiske trådløse brikken. Samtidig bindes brikken til det autentiske passet gjennom sammenligningen med datasidens maskinlesbare sone (MRZ). Denne metoden krever en prosesserende brikke, og støtter derfor kun implementasjoner som følger kommunikasjonsgrensesnitt Type B i henhold til ISO 14443 [14].

ICAO bekrefter forøvrig et potensielt sikkerhetsproblem med den aktive autentiseringen. Dette angrepet går ut på at det plasseres falske brikker mellom inspeksjonssystemet og den legitime trådløse brikken. Disse falske brikkene fungerer så som relé som videreformidler informasjonen. Angrepet kalles "Grandmaster Chess Attack" og tilsvarer i stor grad angrepet som skisseres av Kfir og Wool i "*Picking virtual pockets using relay attacks on contactless smartcard systems"* [30]. Grandmaster Chess Attack er også en vanlig legitim tunnellerings teknikk for sending av kryptert informasjon over nettverk. Et slikt angrep kan derfor være vanskeligere å oppdage i inspeksjonssystemene.

5.2.5 Utvidet tilgangskontroll

ICAO anerkjenner at biometriske verdier utover det spesifiserte bildet trenger bedre sikkerhet enn det den grunnleggende tilgangskontrollen kan tilby. Derfor åpnes det også opp for at utsteder kan implementere egengenererte nøkler i stedet for K_{ENC} og K_{MAC} som brukes i den grunnleggende tilgangskontrollen.

Denne implementasjonen er forøvrig ikke spesifisert utover dette. Dermed oppstår det potensielle problemer der forskjellige utstedende nasjoner eller organisasjoner implementerer forskjellige ukompatible mekanismer, eller implementerer tilleggsbiometri uten noen form for tilgangskontroll i det hele tatt.

En vellykket utvidet tilgangskontroll som baserer seg på egengenererte nøkler i stedet for K_{ENC} og K_{MAC} vil hindre uautorisert tilgang til tilleggsbiometrien, og hindre angriper i å få tak i biometriske verdier ved skimmingangrep. Metoden krever forøvrig en logisk prosesseringsenhet som samsvarer med kommunikasjonsgrensesnitt type B som spesifiseres av ISO 14443 [14].

5.2.6 Tilleggskryptografi

Den andre løsningen ICAO åpner for om beskyttelse av biometriske verdier utover minimumskravet om bilde, er kryptering av informasjonen. Denne metoden vil, forutsatt at krypteringsteknologien som brukes er sikker, beskytte informasjonen. Når informasjonen krypteres som en del av utstedelsesprosessen og kun lagres på brikken til den hentes over på inspeksjonssystemet og

kontrolleres der, krever den heller ikke en prosesserende brikke, og støtter derfor kommunikasjonsgrensesnitt type A i henhold til ISO 14443 [14] spesifikasjonene.

5.3 Signeringsalgoritmer

"PKI for Machine Readable Travel Documents Offering ICC Read-Only Access" [12] spesifiserer frivillig bruk av følgende algoritmer for digitale signaturer: DSA, RSA og ECDSA. Disse beskrives mer inngående i *'"IST Special Publication 800-57 Recommendation for Key Management – Part 1: General"'* [22] av Barker et al. Her sammenlignes blant annet styrken til både symmetriske og asymmetriske krypteringsalgoritmer ut i fra bitstyrke. Nøkkelstørrelsene som spesifiseres her oppfyller kravene om en sikker levetid på maksimalt 10 år, der levetiden anbefales satt til 5 år. Tabell 9 viser forholdet mellom signaturalgoritmer, hash algoritmer og bitstyrke.

Styrke	Forventet sikker levetid	DSA	RSA	Elliptic Curve DSA	HASH
> 80	> 2010	Minimum: L = 1024 N = 160	Minimum: K = 1024	Minimum: F = 160	SHA – 1 SHA – 224 SHA – 256 SHA – 384 SHA – 512
> 112	< 2030	Minimum: L = 2048 N = 224	Minimum: K = 2048	Minimum: F = 224	SHA – 224 SHA – 256 SHA – 384 SHA – 512
> 128	> 2030	Minimum: L = 3072 N = 256	Minimum: K = 3072	Minimum: F = 256	SHA – 256 SHA – 384 SHA – 512

Tabell 9: Algoritmenes bitstyrke med tilhørende hash-algoritme

5.3.1 DSA

"PKI for Machine Readable Travel Documents Offering ICC Read-Only Access" [12] anbefaler bruk av en nøkkel på minimum 2048 bits for generering av den nasjonale lokaliseringens nøkler, KPr_{DS} og KPu_{DS}. I følge "*NIST Special Publication 800-57 Recommendation for Key Management – Part 1: General*" [22] gir en DSA kryptering på 2048 bits en bitstyrke på 112 bits og en sikker levetid frem til 2030. Dette er godt innenfor ICAOs krav om en sikker levetid på maksimalt 10 år, der 5 år anbefales som levetid.

For det nasjonale nøkkelparet, KPr_{CSCA} og KPu_{CSCA}, anbefales det en nøkkelstørrelse på minimum 3072 bits. Dette nøkkelparet skal normalt ha en lang levetid, og byttes ut skjeldnere enn hvert 5. år. En 3072 bits DSA kryptering har en bitstyrke på 128 bits og en forventet sikker levetid til etter 2030 [22].

Videre anbefales det at et eventuelt aktivt autentiseringsnøkkelpar ,KPr_{AA} og KPu_{AA} , bruker en nøkkel på minimum 1024 bits. Dette gir en styrke på 80 bits og en forventet sikker levetid frem til 2010 [22]. Denne trenger ikke et like høyt sikkerhetsnivå fordi all prosesseringen skjer internt i den trådløse brikken.

5.3.2 RSA

I den nyere "P*KI for Machine Readable Travel Documents offering ICC Read-Only Access'"* [12] videreføres anbefalingen fra "P*KI Digital Signatures for Machine Readable Travel Documents"* [20] om bruk av minimum 2048 bits nøkler, KPr_{DS}, for signering av dokumentenes sikkerhetsobjekt, SO_D.

For det nasjonale sertifiseringsnøkkelparet KPr_{CSCA} og KPu_{CSCA}, anbefales det en minimum nøkkelstørrelse på 3072 bits. En 3072 bits RSA-kryptering har en bitstyrke på 128 bits og en forventet sikker levetid til etter 2030 [22].

Videre anbefales det at et eventuelt aktivt autentiseringsnøkkelpar ,KPr_{AA} og KPu_{AA} , bruker en minimum nøkkelstørrelse på 1024 bits. Dette gir en bitstyrke på 80 bits og en forventet sikker levetid frem til 2010 [22]. Denne trenger ikke et like høyt sikkerhetsnivå fordi all prosesseringen skjer internt i den trådløse brikken.

5.3.3 ECCDA

"PKI for Machine Readable Travel Documents offering ICC Read-Only Access" [12] fra 2004 anbefaler en minimum nøkkelstørrelse på 224 bits streng til den nasjonale lokaliseringens private hemmelige nøkkel, KPr_{DS}. Dette gir en bitstyrke på 112 bits og en forventet sikker levetid frem til 2030 [22].

Videre anbefales det at nøkkelen, KPr_{CSCA}, som brukes til å signere utstedende lokasjoners sertifikat C_{DS}, er på 256 bits. Dette gir en styrke på 128 bits og en forventet sikker levetid til etter 2030 [22].

Til et eventuelt eventuelt aktivt autentiseringsnøkkelpar, KPr_{AA} og KPu_{AA}, anbefales det å opprettholde nøkkelen på 160 bits som spesifiseres i "*PKI Digital Signatures for Machine Readable Travel Documents"* [20]. Denne gir en bitstyrke på 80 bits og en forventet sikker levetid frem til etter 2010 [22]. Dette er nok fordi nøkkelen kun brukes til prosessering internt i brikken.

5.3.4 Secure Hash Algorithm

"PKI Digital Signatures for Machine Readable Travel Documents'" [20] utpeker SHA-1 som eneste lovlige hashingalgoritme. "*PKI for Machine Readable Travel Documents offering ICC Read-Only Access"* åpner for utvidelse av spesifikasjonen til også å gjelde SHA-224, SHA-256, SHA-384 og SHA-512, kollektivt kalt SHA-2. Eksemlene og spesifikasjonene som følger "*PKI for Machine Readable Travel Documents offering ICC Read-Only Access"* omhandler forøvrig kun SHA-1 algoritmen. I "*Collision search attacks on SHA1*" [34] fremhever forøvrig Wang et al. flere svakheter med denne algoritmen. National Institute of Science and Technologies (NIST) er i tillegg i ferd med å

fase ut SHA-1 protokollen og anbefaler bruk av SHA-2 familien. Derfor bør spesifikasjonene også oppdateres til å basere seg på disse.

5.4 Andre sikkerhetsspørsmål

Det finnes også en del andre sikkerhetsspørsmål som vil berøre temaet elektroniske reisedokument. Eksempler på dette kan være tjenestenektangrep (eng. "*Denial of Service attack, DoS attack*") mot ICAOs katalogtjeneste for utveksling av nøkler (ICAO PKD). Implementasjoner som baserer seg på spredning av offentlige nøkler gjennom ICAO PKD, i stedet for gjennom reisedokumentets trådløse brikke, vil derfor få problemer med passkontrollen.

5.5 Alternative sikkerhetsimplementasjoner

ICAOs spesifikasjoner av den utvidete tilgangskontrollen åpner for implementasjon av valgfrie eksterne algoritmer. Dette har ført til at blant annet EU har utviklet sin egen tilgangskontroll som er utviklet av Dennis Kügler og spesifiseres i "*Advanced Security Mechanisms for Machine Readable Travel Documents*" [35]. Denne baserer seg på tre hovedsteg:

1. Den grunnleggende tilgangskontrollen
2. Brikkeautentisering
3. Terminalautentisering

Etter den grunnleggende tilgangskontrollen får inspeksjonssystemet tilgang til de digitale signaturene i dokumentets sikkerhetsobjekt, SO_D. Leseren autentiserer så brikken gjennom bruk av den kryptografiske nøkkelen som kalkuleres av den grunnleggende tilgangskontrollen. Så utledes det en sterk sesjonsnøkkel fra et Diffie-Hellman nøkkelpar. Denne brukes så til å overføre det biometriske bildet fra brikken. Først når bildet har blitt kontrollert mot passholderens ansikt og inspeksjonssystemet har blitt autentisert får brikken gjennom en challenge-respons protokoll, overfører brikken annen biometrisk informasjon, som for eksempel fingeravtrykk.

Denne protokollen tilbyr en sikrere dataoverføring enn den grunnleggende tilgangskontrollen. Men fordi den i den innledende kommunikasjonen baserer seg på den grunnleggende tilgangskontrollen vil MRZ-informasjon og det biometriske bildet være like utsatt for angrep som den grunnleggende tilgangskontrollen. Men den biometriske informasjonen forblir beskyttet.

Kc og Karger viser i "*Preventing Attacks on Machine Readable Travel Documents"* [33] til autentiseringsprotokollen Caernarvon som unngår dette problemet ved å bruke Diffie-Hellman sesjonsnøkler fra begynnelsen på kommunikasjonsstrømmen som erstatning for den grunnleggende tilgangskontrollen. Brikken utleverer ingen informasjon før den har verifisert inspeksjonssystemet.

Både Caernarvon og Küglers protokoll er avhengig av en brikke med logiske prosesseringsegenskaper og vil følgelig kun være kompatibel med ISO 14443 type B kommunikasjonsgrensesnitt.

5.6 Forskjellige lagringsteknologier

Her prensteres forskjellige lagringsteknologier til bruk i elektroniske pass.

5.6.1 Optisk minne

Ved bruk av optisk minne lagres data på et optisk medium(for eksempel CD) og leses av med en laser stråle. Optiske minne kort kan lagre opp til 4MB data, men data kan ikke endres eller slettes etter de er skrevet på et optisk medium. [36] Disse type kort er ideelle til journalføring, for eksempel for medisinske filer eller kjørejournal. Optiske kort er foreløpig upraktiske for pass og andre reisedokumenter og er i tillegg relativt dyre, selv om de tilbyr stor lagringskapasitet i sammenligning med andre teknolgier.

5.6.2 Magnetstripe

En magnetisk stripe er et bånd av magnetisk metaloksid som brukes for å lagre data til for eksempel kredittkort. Stripen leses av ved fysisk kontakt og dras forbi et lesehode. Lagringskapasiteten til kort med magnetstripe som følger ISO 7811 er 1288 bits fordelt på tre dataspor.

Data på den magnetiske stripen kan bli ødelagt av magnetiske felt, så kortene må behandles forsiktig. Manipuleringer ved å overskrive lagret data på en magnestisk stripe kan ikke forhindres, mens noen modifikasjoner kan oppdages av kryptografisk tilkytning av data på magnetstripen til annen informasjon på dokumentet. Fordelen med magnetisk stripe i forhold til datalagring som bruker integrerte kretser(IC) er den lave enhetsprisen. Men på grunn av den begrensede levedtiden og svakheten for feil og modifikasjoner, burde ikke kort med magnetstripe brukes for ID dokumenter som skal vare i ti år.

5.6.3 Intergrerte kretser

Intergrerte kretser(IC) er datalagring ved bruk av ROM, EEPROM eller permanentlagrings RAM. Det finnes både kontaktbaserte og trådløse ICer. De kontaktbaserte kan være smartkort. De trådløse er ofte referert til som RFID transponder. Begge disse typene kan både ha bare minne funksjonalitet eller avanserte prosess muligheter.

5.6.3.1 Kontaktbaserte ICer

Kontaktbaserte ICer er standardiserte i ICO/IEC 7816 og brukes til for eksempel telefonkort, sikkerhetsbevis ved autentisering og til lagring av digitale signaturer. ICene til forskjellige formål er svært forskjellig i minnekapasitet, prosesskraft og sikkerheten mot fysisk angrep. Lagringskapasiteten kan være på flere hundre kilobytes av EEPROM. Utrustet med tilstrekkelig logisk sikkerhet forhindrer de uautoriserte personer fra å lese eller endre lagrede data. ICer har også prosesskraft til å utføre kraftig kryptering.

De fleste kontaktbaserte ICer må monteres på et slags plastikkort, det forhindrer de å bli implemetert i dagens reisedokumenter. En fordel med kontaktbaserte ICer i forhold til RFID transpondere er at den kontaktbaserte ikke kan leses ubemerket og kommunikasjon mellom IC og leser er vanskeligere å tyvlytte til

enn RFID transpondere. Kontaktbasert datakommunikasjon er også mer robust mot blokkering av kommunikasjon.

5.6.3.2 RFID transponder

De fleste RFID transpondere nå er passive. Med det menes at de ikke har egen strømforyning og at de får den nødvendig elektriske energien via induksjon fra leseren. Det finnes tre forskjellige typer transpondere som er anerkjente i henhold til leseavstand: nær, fjern og nærhetsforbindelse[2].

Mangfoldet i tråløse ICer er bra. Noen brikker har kraft til å utføre avanserte krypteringsalgoritmer og har lagringskapasitet på flere Kbytes. På grunn av at trådløse ICer er små og flate kan de legges inn i pass.

RFID transpondere har det generelle problemet for trådløs kommunikasjon: avlytting av dataoverføring. Hvis det ikke er implementert aksesskontroll, kan transpondere bli lest ubemerket innenfor den standardiserte avstanden. Det første problemet kan løses ved bare å sende krypterte data. ICAO anbefaler å legge inn elektronisk skjermende materiale(for eksempel aluminiumsfolie) i omslaget til passet, slik at ICen ikke kan leses når passet er lukket. Å velge RFID standard med korte leseavstander kan begrense faren for at den trådløse ICen leses av ubemerket.

2 Nærhetsforbindelses transpondere er definert i ISO 10536 og skal fungere innen 1cm rekkevidde. ISO 14443 definerer kommunikasjon innen 15cm rekkevidde. Hvis ISO 15693 følges fungerer de innen 1.5m.

6 Biometri

6.1 Generell innføring

Biometrisk gjenkjennelse referer til den automatiske gjenkjenningen av personer basert på deres fysiske og/eller atferdskarakteristikker. En biometrisk mal er den maskinkodede framstillingen av en karakteristikk laget av en software algoritme som gir mulighet for sammenligning av karakteristikker. Biometriske karakteristikker innehar et kraftfullt potensial ved å tilby ytterligere sikkerhet i flere sammenhenger. [37] Ved å bruke biometri er det mulig å bekrefte personers identitet basert på personlige kjennetegn som for eksempel et fingeravtrykk, i stede for at personen må inneha et ID-kort eller må huske et passord. Kroppskarakteristikker som ansikt, stemme og ganglag er bruk i tusener av år for å gjenkjenne personer. Først på slutten av 1800-tallet ble fingeravtrykk oppdaget og tatt i bruk. Selv om biometri ble størst utstrakt for å identifisere kriminelle er det nå økende i bruk for å gjenkjenne personer i et stort antall sivile anvendelser. Følgende krav stilles til biometriske karakteristikker:

- Universalitet: alle personer må ha karakteristikken.
- Særegenhet: to tilfeldige personer skal ha tilstrekkelig forskjell i karakteristikken.
- Holdbarhet: karakteristikken skal være tilstrekkelig uforanderlig.
- Innsamlbar: karakteristikken skal kunne bli målt kvantitativt.

Derimot er det også andre punkter å ta i betraktning i et biometrisk system.

- Utførelse: mulig nøyaktighet og hastighet til gjenkjenning, ressurser til å oppnå dette, og driftsmessige og miljømessige faktorer i henhold til dette.
- Akseptabilitet: hvorvidt folk aksepterer bruken av den bestemte biometriske karakteristikken.
- Bedrageri: hvor lett er det for systemet å bli lurt av falske metoder.

Et biometrisk system bør følge spesifikasjoner for nøyaktighet, hastighet, ressurs krav, være harmløs og akseptert for tilsiktede brukere og være tilstrekkelig motstandsdyktig mot forskjellige falske metoder og angrep på systemet. [38]

De viktigste delene i et biometrisk system er innsamling, utvinning, opprette mal og sammenligning.

- Innsamling er når det ubearbeidet biometriske materiale leses inn.
- Ved utvinning konverteres det biometriske materiale til en mellomform.
- Malen opprettes ved konvertering av mellomformen.
- Sammenligning gjøres med informasjonen i en referansemal.

Disse prosessene involverer:

- Registrering er innsamlingen av det ubearbeidet biometriske materiale. For hver person samles det inn biometrisk materiale og det opprettes det en ny mal. Innsamlingen gjøres automatisk ved hjelp av en

innlesningsenhet som for eksempel en fingeravtrykksskanner, en fotografiskanner, et digitalt kamera eller et zoomingkamera for å ta bilde av iris. Hver innlesningsenhet har forskjellige krav og prosedyrer definert for sin innlesning, for eksempel skal ansiktsfotografering gjøres i rett positur og øyne skal være helt åpne ved irisinnlesning.

- Når malen lages bevares det særskilte og de biometriske egenskapene som er mulig å gjenta fra det innsamlede biometriske materiale. Dette skjer via en softwarealgoritme som trekker ut malen fra det innsamlede bildet. Følgende kan malen og et nytt innsamlet bilde av biometrisk materiale sammenlignes og en komparativ bedømmelse gjøres. Selve algoritmen innehar kvalitetskontroll gjennom noen mekanismer som gir hver innsamling en kvalitetsverdi. Kvalitetsstandarden må være så høy som mulig siden all sammenligning er avhengig av kvaliteten til den tidligere lagrede malen. Hvis kvaliteten ikke er god nok må innsamlingen gjentas.
- Identifikasjonsprosessen tar en ny innsamling og sammenligner den til de lagrede malene av godkjente brukere for å bestemme om brukeren har vært godkjent i systemet før, og hvorvidt med samme identitet.
- Verifikasjonsprosessen tar en innsamling av en passholder og sammenligner den med en tidligere mal lagret av passholderen. Dette for å bestemme hvorvidt passholder har samme identitet som tidligere. [39]

Hovedoppgaven for et biometrisk system i en passkontroll er å knytte et MRTD til den som innehar MRTDen. Flere forskjellige typiske applikasjoner for biometri brukes når et MRTD skal utstedes:

1. Søkerens biometriske mal(er) som blir laget ved innskrivningen kan sjekkes mot biometriske databaser for å finne ut om personen for eksempel har et pass med annen identitet, har kriminell bakgrunn eller har pass fra et annet land.
2. Når søkeren henter passet kan biometriske data innhentes igjen og verifisert mot den lagrede malen.
3. Identiteten til personale kan bli verifisert for å sikre at det er autorisert personell som utgir passene. Dette kan inkludere biometriautentisering for å innføre digitale signaturer på logger slik at biometri linker personell med den aktivitet i prosessen de er ansvarlige for.

Det er også typiske applikasjoner for biometri ved en grensekontroll:

1. Hver gang reisende kommer inn i eller drar ut av et land kan identiteten verifiseres mot bildene eller malene som ble laget når de fikk MRDTen utstedt. Dette vil effektivisere et avansert passasjer informasjonssystem. Ideelt sett bør biometri lagres i passet slik at personers identitet kan bli verifisert der hvor en sentral database ikke er tilgjengelig, eller steder hvor lagring av biometri i databaser er uakseptabelt.
2. Toveiskontroll: den reisendes nylig innsamlede biometri sammenlignes med biometri i passet eller i en sentral database for å bekrefte at passet ikke er endret.

3. Treveiskontroll: den reisendes nylig innsamlede biometri, biometri lagret i passet og biometri lagret i den sentrale databasen sammenlignes for å bekrefte at passet ikke er endret.
4. Fireveiskontroll: En fjerde kontrollmulighet er en visuell sammenligning at treveiskontrollen mot fotografiet på datasiden i passet.[39]

Selv om biometri kan forsterke sikkerhet i en mengde tilfeller, er biometriske systemer, som alle andre sikkerhets systemer, sårbare for angrep. Den økende bruken av biometri til sikkerhet har skapt stor interesse for forskning og testing av metoder som kan lure et biometrisk system. [37]

Et biometrisk verifikasjonssystem kan gjøre to typer feil:

1. Godkjenne biometriske målinger fra to forskjellige personer, som om de var fra samme person (false match).
2. Underkjenne to biometriske målinger fra samme person, som om de var fra to forskjellige personer (false nonmatch).

Disse to typene av feil betegnes ofte som falsk godkjenning og falsk avvisning. Det er et forhold mellom FMR(false match rate) og FNMR(false nonmatch rate) i et hvert biometrisk system. Hvis man ønsker at systemet skal være vanskeligere å lure(lav FMR), kan det gjøre det vanskeligere for godkjente personer å bli verifisert(høy FNMR). En akseptabel feilrate for de to ratene må bli funnet i forholdet.

Biometriske karakteristikker har en fordel overfor passord og verifikasjonskort fordi de ikke kan bli glemt, selv om de kan mistes. (Personer kan miste en finger i en ulykke, eller man kan miste stemmen ved sykdom.) Hvis en nøkkel eller kode mistes, er det enkelt å bytte ut låsen eller koden og igjen ha et sikkert system. Derimot om noen stjeler en biometrisk karakteristikk, tar opp en stemme på bånd eller kopierer en database med en elektronisk iris skanning, da er et vanskelig løsbart problem oppstått. Problemet med biometriske karakteristikker er at de ikke er noen hemmelighet selv om de er unike identifikatorer på en person. Fingeravtrykk legges igjen overalt, og noen kan lett ta et fotografi av et øye. [40]

Multimodale biometriske systemer undersøker flere biometriske verdier på hver person, dette gjør de mer pålitelige. Det blir vanskeligere å lure systemet fordi man for eksempel både må godkjennes i ansiktsgjenkjenning og gjennom en fingeravtrykksleser. Systemet må også forholde seg til flere forskjellige applikasjoner som har sine strenge krav til utførelse. Selv om de multimodale systemene er sikrere, fører de til økte kostnader og lengre verifikasjonstid. [41]

Angrep på en biometrisk enhet og systemer kan opptre i tre forskjellige kategorier, angrep der biometri leses inn, angrep i prosessering og overføring av biometri eller angrep i lagringsenheten. Hvis en av flere karakteristikker i et biometrisk system blir lett å endre eller overføre til annen person, er graden av sikkerhet betraktelig redusert. Følsomheten, til et biometrisk system, for et angrep er stor bekymring for nye anvendere av slike systemer. [37]

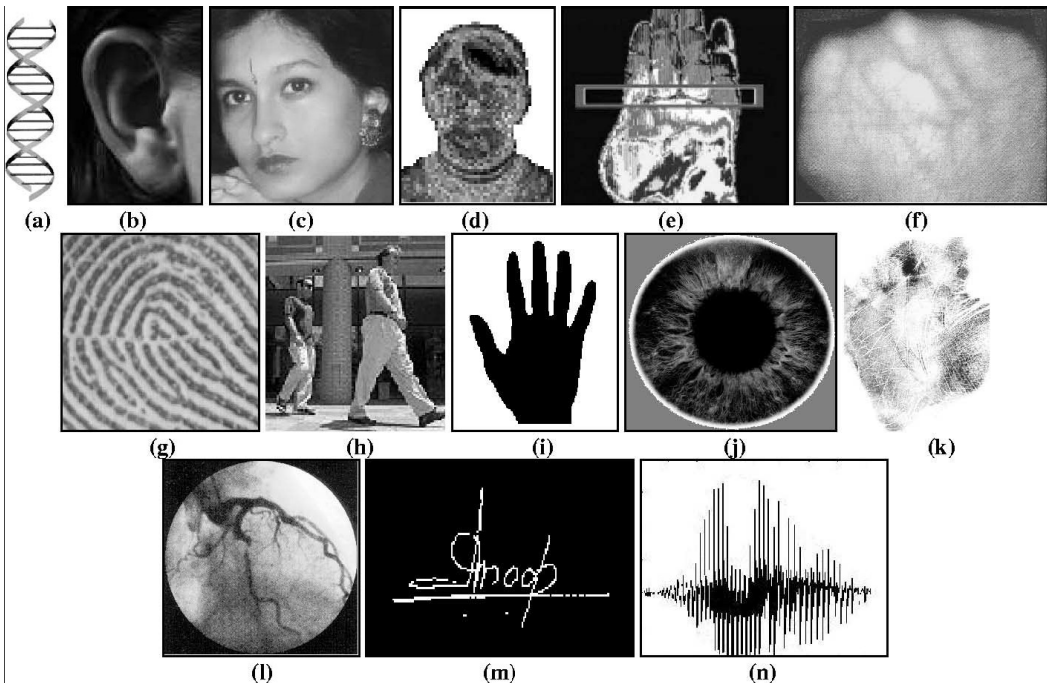
Biometriske systemer forsøker å minske faren for å bli lurt gjennom å teste på om den biometriske karakteristikken er levende/tilhører en levende person. Metoder for dette er spesifikke for de forskjellige gjenkjenningsenhetene.

En ny teknikk fra IBM som brukes for å beskytte biometriske systemer kalles annullering av biometriske karakteristikker. Når et bilde blir tatt enten av et ansikt eller en finger blir ikke det originale bildet lagret noe sted, men en algoritme lager en forvrengning som lagres isteden. Hvis en tyv sjeler forvrengningen, kan denne slettes og det kan lages en ny. Så lenge algoritmene for forvrengning beskyttes og varieres, er dette med på å gjøre det vanskeligere å benytte stjålne bilder av biometriske karakteristikker fra en database. Hvis alle som driver med biometri åpent og kontinuerlig identifiserer svakheter for å finne metoder for å forbedre, vil hele det internasjonale samfunn tjene på det. [37]

6.2 Presentasjon av forskjellige biometriske karakteristikker

Et flertall biometriske karakteristikker eksisterer og er i bruk i forskjellige applikasjoner. Hver av dem har sine styrker og svakheter, og hvilke man velger av disse kommer an på hva man skal bruke det til. Ingen biometrisk verdi forventes å møte alle kravene til en applikasjon, med andre ord finnes det ingen optimal biometrisk verdi.

De mest kjente biometriske verdiene er ansikt, fingeravtrykk, signatur, håndgeometri, stemme, iris, retina, DNA, håndens blodårer, ansiktstermogram, håndtermogram, øre, avtrykk av håndflaten, ganglag, tasttrykk og lukt. Se Illustrasjon 25 for eksempler av de biometriske karakteristikkene. I ICAO standarden er det gjort et utvalg av disse som er godkjent til bruk i pass, foreløpig er ansikt, fingeravtrykk og iris godkjent. Det er også lagt inn plass for å mulig ta i bruk ved senere anledning; håndgeometri, stemme og retina. Her følger en uttredelse av de kjente biometriske verdiene, med vekt på de som er valg i standarden.



Illustrasjon 25: Eksempler på biometriske karakteristikker: (a) DNA, (b) øre, (c) ansikt, (d) ansiktstermogram, (e) håndtermogram, (f) blodårer i hånden, (g) fingeravtrykk, (h) ganglag, (i) håndgeometri, (j) iris, (k) avtrykk av håndflaten, (l) retina, (m) signatur og (n) stemme. [38]

6.2.1 Ansiktskarakteristikk

Ansiktsgjenkjenning har blitt populært i de senere år, fra ca midt på 90-tallet, og er tidlig i utviklingsfasen i forhold til andre biometriske karakteristikker, som for eksempel fingeravtrykk. Mens andre biometriske karakteristikker trenger medvirkning av en person for utførelse, har ansiktsgjenkjenning en fordel ved at et fotografi kan taes uten samarbeid eller viten og brukes til gjenkjenning. Ved en undersøkelse gjort av International Biometric Group foretrekkes det derimot av folk å få innlest fingeravtrykket sitt enn å bli tatt bilde av. Dette kan ha en sammenheng med at mange ikke liker å bli tatt bilde av, folk synes ansiktet er personlig og at vi ser på oss selv som unike individer. [42]

Vi kjenner alle til et gjenkjenningssystem som har imponerende ytelse under alle forhold, menneskets visuelle system. Hvis vi kan klare det, burde en datamaskin klare det samme. Problemet for oss er å finne ut hvordan, det er forsket på nå i snart 30 år. Ansiktsgjenkjenning har vært og vil fremdeles være et utfordrende og vanskelig problem derfor er samarbeid mellom forskningsgrupper viktig.

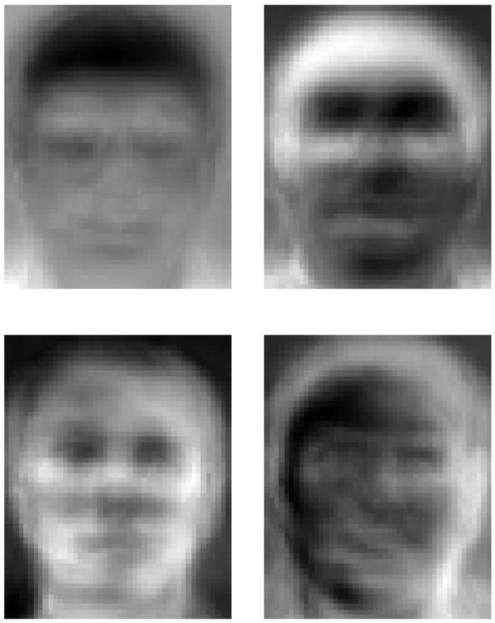
Det finnes flere forskjellige hensyn å ta når ansikter skal gjenkjennes, for eksempel under hvilke forhold fotografiet er tatt, at menn er lettere å gjenkjenne enn kvinner og at man må ha tilstrekkelig kunnskap om de svakheter og styrker metoden som velges for gjenkjenning har.

Den mest vanlige metoden er å sammenligne spesielle egenskaper i ansiktet ved hjelp av et todimensjonalt kart. Nyere metoder bruker nå tredimensjonale kart. Bilder fra foto- eller videokameraer lager et digitalt bilde av en person som lagres for sammenligninger.

Kvaliteten til det digitale bildet varierer etter hvilke forhold bildet er tatt under. ICAO standarden krever at passbilder er tatt med tilstrekkelig og jevnt lys slik at hud får naturlig farge, og at det blir minimalt med skygge og refleksjoner. En ensfarget bakgrunn skal benyttes for å få en kontrast til ansiktet. Dette blir gode bilder som er av de enkleste å gjøre gjenkjenning på ved de forskjellige metodene.

I en passkontroll vil et bilde taes av passholder som enten sammenlignes med bildet i passet eller bilder lagret i en database. Populære gjenkjenningsalgoritmer som brukes i ansiktsgjenkjenning er eigenface, fisherface, Hidden Markov model og Dynamic Link Matching. Men den nye trenden er nå tredimensjonal ansiktsgjenkjenning og en teknikk som bruker de visuelle detaljene i huden. Tester på FERET [43], en database som brukes til testing av gjenkjenningsalgoritmer, viste at den siste metoden er mer pålitelige enn tidligere algoritmer. [44]

Eigenfaces:
Eigenfaces er et sett egenvektorer som brukes når en datamaskin prøver å gjenkjenne ansikter. Metoden kalles også eigenimage siden teknikken også har blant annet blitt brukt for gjenkjenning av håndskrift og stemme. For å generere et sett av eigenfaces blir digitaliserte foto tatt under samme lysforhold normalisert for å tegne opp øyne og munn. Fotografiene blir så gjort like i pikselstørrelse(*m*n*) og behandlet som *mn*-dimensjonale vektorer hvor komponentene er verdiene til pikslene. Egenvektorene av kovariansmatrisen av den statistiske distribusjonen av ansiktsfotovektorene blir så pakket ut. Dette er de samme egenvektorene som fra en prinsipiell komponentanalyse, den statistiske metoden hvor eigenimaging er utledet fra. Se Illustrasjon 26 for eigenfaces. [45]



Illustrasjon 26: Eksempler på Eigenfaces

Fisherface:
Denne metoden prosjekterer fotografier av ansikter inn i et tredimensjonalt lineært underrom basert på Fisher's Linear Discriminant. Den er konkludert til å være bedre enn Eigenface metoden når det gjelder å håndtere variasjon i lyssetting og variasjon i ansiktsuttrykk. En begrensning med metoden er at den

trenger atskillige fotografier av hver person ved øvelse i gjenkjenning. Shan et al. Beskriver i “Extended fisherface for face recognition from a single example image per person” [46] hvordan man kan løse dette ved å utlede flere fotografier fra et enkelt ansiktsfotografi.

Hidden Markov model:
En hidden Markov modell er en statistisk modell hvor system som blir modulert etter antatt å være en Markov prosess med ukjente parametere. Parametrene bestemmes ut ifra de observerte parametrene i forhold til at det antas å være en Markov prosess. Modell parametrene kan da brukes til videre analyser, for eksempel i mønstergjenkjenningsapplikasjoner. Flere har inkludert hidden Markov i sine ansiktsgjenkjenningsalgoritmer som Nefian et.al i ”Hidden Markov Models For Face Recognition” [47], Bicego, et.al i ”Using Hidden Markov Models and Wavelets for face recognition” [48] og Othman et.al i ” Low Complexity 2-D Hidden Markov Model for Face Recognition” [49].

Dynamic Link Matching:
Denne gjenkjenningsmetoden er basert på selvorganisering av en 1-1 kartlegging mellom korresponderende punkter i et fotografi og en modell. Dynamiske linker veksler raskt synapser hvor dynamikken er kontrollert ved samarbeid fra nabo synapser. I seg selv er DLM treg og trenger mange gjentakelser. Derimot ved utvidelse ved å tillate systemdynamikk, som i Zhu, J., og von der Malsburg, C. rapport ”Object recognition by Dynamic Link Matching in biologically realistic time” [50] forbedrer dette metoden. Flere andre har brukt DLM sammen med andre metoder for å få et optimalt gjenkjenningssystem.

FRVT, Face Recognition Vendor Test, [43] er en test av kommersielt tilgjengelig ansiktsgjenkjenningssystemer. Testen ble sist utført i 2002 og flere føderale selskaper støtter den. FRVT 2002 ble designet slik at så mange som mulig av forskningsgrupper og selskaper kan ta del i den, og den er ment som hjelp for staten U.S. og andre som driver med rettshåndhevelse når de skal velge hvor og hvordan ansiktsgjenkjenning bør anvendes. Testen består av to deler for å oppfordre til bred deltagelse i evalueringen. De to delene er en høy matematisk intensitetstest (HCInt) og medium matematisk intensitetstest (MCInt). HCInt evaluerer systemenes ytelse i ekstremt utfordrende virkelighetsnære problemer, mens MCInt tester systemenes kapasitet når det gjelder å håndtere forskjellige formater ved varierende forutsetninger. Tekniske spesifikasjoner finnes på internettsidene. Resultater viser følgende hovedtrekk:

- Ved normal endring i lysforhold når fotografiene er tatt innendørs er det ikke noen særlig innvirkning på ytelsen til gjenkjenningen. Gjenkjenning ble gjort i 90% av tilfellene ved 1% falsk akseptrate av det beste systemet.
- Utviklingen har gått rett vei fra år 2000 til 2002, systemene har hatt en 50% reduksjon i feilrate. Bruken av 3-dimensjonale morphable modeller har betydelig forbedret gjenkjenningen for ansikter som ikke er tatt rett forfra.
- For hver dobling av databasestørrelse ansiktene skal sjekkes mot synker ytelsen med 2-3% poeng. Ytelsen minker lineært i forhold til logaritmen til

databasens størrelse. Det samme forholdet ved bruk av en observasjonsliste for å utelukke spesielle personer.

- De beste systemene hadde 6-9% poeng større gjenkjenningsrate på menn i forhold til kvinner, og gjenkjenningsraten for eldre mennesker var høyere enn for yngre. For hver tiende år økning i alder, økte gjennomsnittet til gjenkjenningen med cirka 5% fram til 63 år. Tilpasninger burde gjøres i forhold til demografisk informasjon siden alder og kjønn har en vesentlig effekt på ytelsen til gjenkjenningssystemene.

FRVT 2006 startet 30.januar i år og vil måle framgang siden FRVT 2002. Testen utføres av National Institute of Standards and Technology(NIST) og deltagerne leverer utstyret til testing. Et standard datasett og test metoder blir brukt slik at de forskjellige systemene blir likeverdig evaluert. Antall deltakere og omfanget av testen avgjør når resultatene kommer.

Ansiktsgjenkjenningssystemer kan bli lurt av fotografier eller masker. [37] Så lenge passkontrollen har tilsyn av personell vil det kun være mulig å lure ansiktsgjenkjenningen med en naturtro ansiktsmaske. Systemene kan kreve bevegelse av hode, lepper, eller endring av ansiktsuttrykk for å minske faren for å bli lurt.

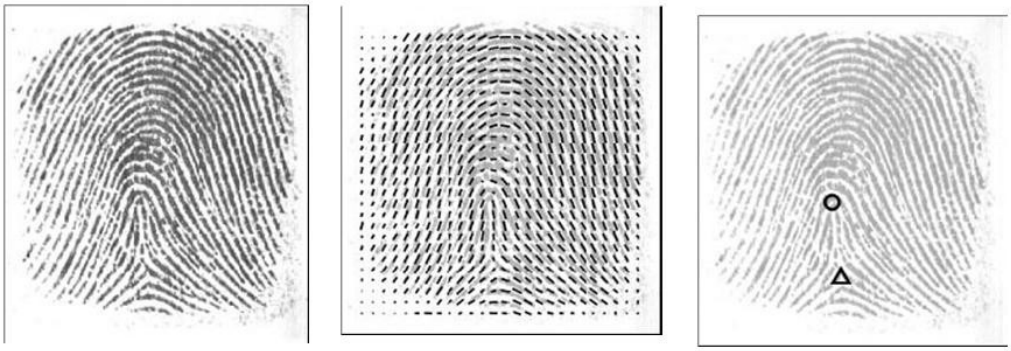
6.2.2 Fingeravtrykk

Overflaten på innsiden av fingre hos mennesker har et linjemønster som er svært stabilt gjennom hele livet. Dette mønsteret utvikles de første syv månedene i et menneskets liv. Etter automatiske datasammenligninger av mange milliarder mennesker er det aldri oppdaget to personer med samme mønster, derfor kan man med stor sikkerhet si at fingeravtrykk er unike for hvert enkelt menneske. Fingeravtrykk til identiske tvillinger er forskjellige, t.o.m. avtrykk av hver finger fra en og samme person. Dette gjør at fingeravtrykk egner seg godt til å verifisere identiteten til en person.

I forhistorisk tid ble fingeravtrykk satt på leirtavler for foretningskontrakter(antikkens Babylon) og på forseilinger av leire(antikkens Kina). Argentinsk politi gjorde den første kriminelle fingeravtrykksidentifikasjonen i 1892 og siden den gang har fingeravtrykk vært et fundament for identifisering av kriminelle. Nå brukes fingeravtrykk også til verifisering av personer, mest vha mønstergjenkjenning eller minutiaeanalyse. [51]

Minutiaeanalyse:
I fingeravtrykk er det spesielle punkter hvor linjer splittes eller ender, et slikt punkt kalles en minutiae. Mulige minutiae er når en linje ender, når en linje splittes, korte linjer, eller linjer som er innkapslet. De kan også referere til små og ellers tilfeldige detaljer. Et avtrykk har ca. hundre minutiae, og når et avtrykk er skannet av en sensor har bildet 30-40 minutiae. I rettssaker trengs 12 minutiae for å identifisere et fingeravtrykk. Det er basert på en antagelse om at to personer ikke vil ha 12 identiske minutiae i fingeravtrykkene sine, selv med sammenligninger med titalls millioner mennesker. De fleste kommersielle fingeravtrykksskannere godkjenner når 8 minutiae er identiske.

Mønstergjenkjenning:
Mønstergjenkjenning er en mer global metode i forhold til minutiae analyse, for å identifisere fingeravtrykk. Her fokuseres det mer på gjenkjenning i mønstre ved å se på retninger og flyt. Kjerne- og deltapunkter som vises klart i mønsteret blir brukt til identifisering. Se Figur 3 for eksempel på mønstergjenkjenning



Illustrasjon 27: Et fingeravtrykk(til venstre), retningsflyt(i midten) og kjerne og deltapunkter(til høyre).

Fingeravtrykkssensorer er de som har blitt mest testet for angrep, ikke minst på grunn av mangfoldet av kommersielle produkter som er tilgjengelige for alle. Kjente metoder for å lure et fingeravtrykkssystem er følgende:

- Naturtro protese laget i en støpeform av en godkjent finger
- Høyoppløselig foto av en godkjent finger
- Et godkjent fingeravtrykk hentet opp med tape på en blank overflate
- Gjenværende fingeravtrykk på skanneren som settes i live når overflaten til skanneren blir sprayet med kjemikalier. [37]

Det finnes flere forskjellige typer fingeravtrykkssensorer; optiske, ultrasoniske, silikon-, trykk-, temperatur-, kapasitetssensorer og sensorer som har elektrisk felt. Optiske sensorer har en plate som opplyses av LED lys. Et CMOS-kamera tar bilde gjennom et prisme og et system av linser. Ultrasoniske sensorer måler forskjellen i akustisk impedans mellom furene og luften i dalene mellom disse. Silikonsensorer kombinerer både silikonbaserte optiske CMOS-kameraer med kapasitetssensorer. Silikonsensorene ser på det levende laget like under huden der furene og dalene har sitt utgangspunkt. Trykksensorer har en elastisk overflate som inneholder trykksensitive elementer som skiller mellom trykket fra furer og daler. Denne informasjonen bygger opp et bilde av avtrykket. Temperatursensorer er tilstandssensorer som bruker et rutenett av temperatursensitive sensorer i pikselstørrelse. Disse måler temperaturforskjellene i furene og dalene i huden og lager et mønster som representerer fingeravtrykket. Sensorer med et elektrisk felt er også en tilstandssensor som også består av mange sensorer i pikselstørrelse. Alle sensorene foretar uavhengige målinger av variasjoner i tykkelsesforskjellen mellom furene og dalene. I rapportene vi har hentet resultater fra er optiske, silikon- og kapasitetssensorer og sensorer med elektrisk felt testet.

I desember 2002 publiserte Schuckers en rapport med tittel “Spoofing og Anti-Spoofing Measures” [52]. Former ble laget av voks, silikon og plastikk og falske fingre av silikon og gelatin. I tillegg viser hun til former av plastilin og falske fingre av tannlegeprodukter. Schuckers har også testet fingeravtrykksensorene opp mot fingre av lik. Sensortypene som ble testet var optisk, kapasitet, elektrisk felt og sensorer med elektrisk optisk teknologi. Resultatene viste at fingrene fra lik hadde en sannsynlighet på opptil 90% for å lure leserne. Plastilinforsøkene lurte systemet fra 45% - 90% av tilfellene mens vannbasert leire varierte helt mellom 10% - 90%.

I oktober 2003 publiserte Blommé [53] en oppgave der han hadde testet ut en optisk sensor fra produsenten Identrix og to silikonbaserte lesere fra Precise og Targus. Blommé laget en gelatinfinger i en støpeform av silikonpasta og alle tre leserne ble grundig lurt. Den optiske leseren kom best ut men ble lurt i 67% av tilfellene, de to silikonbaserte leserne ble lurt i 68% (Precise) og 94% (Targus) av tilfellene. I gjennomsnitt kom Targus ut med en feilaksepteringsrate på 55,4% mens Identrix og Precise kom ut med henholdsvis 24,0% og 34,4%.

Sandström publiserte i juni 2004 en omfattende avhandling med tittelen “Liveness Detection in Fingerprint Recognition Systems” [54]. Fingeravtrykk ble hentet fra en glassflate ved hjelp av askeblanding, børste laget av ekornhår og tape. Avtrykkene ble så fotografert og prosessert i Adobe Photoshop. En utskrift av avtrykkene på transparens ble overført til et kretskort ved hjelp av blant annet UV-lys. Dette ble så brukt som støpeform for å lage gelatinfingre. Gelatinfingrene ble testet opp mot 9 forskjellige autoriseringssystem for fingeravtrykk ved varemessen CeBit i Hanover, Tyskland i 2004. Samtlige av de 9 systemene hvorav to var optiske og de resterende syv var halvledende ble lurt av minst en av de to falske fingrene som ble testet. Grundigere tester ble senere utført på to halvledersensorer (elektrisk felt) og en optisk sensor. I første testrunde førte dette til at sensorene ble lurt av den falske fingeren i 67% av tilfellene mens den nådde helt opp i 86% i andre testrunde.

I desember 2004 testet Wiehe et al. [55] en optisk og en silikonbasert sensor. Gelatin og silikon i kombinasjoner med støpeformer av plastilin, stearin, leire, varmt lim og blekk på transparent papir ble forsøkt laget falske fingre av. Resultatene viste at silikonfingre laget av former av plastilin, stearin og leire klarte å lure den optiske sensoren. De resterende kombinasjonene klarte ikke å lure den optiske sensoren, mens ingen av delene klarte å lure silikonsensoren.

Noen fingeravtrykkssensorer undersøker fargen til den fingeren som leses av, slik at for eksempel sorte gummifingre ikke skal bli godkjent. Det forskes også på andre metoder, blant annet spektroskopi og målinger av svette, hvor begge har vist å være noe effektive i laboratorietesting. Forskere ved Lumidigm [56] har brukt 32 røde, grønne og blå lysdioder som kan sende lys på bølgelengder mellom 395nm og 940nm, når fingeren skal leses inn på sensoren penetrerer mange forskjellige bølgelengder fingerens hud på forskjellige punkter. Spektrale målinger blir da tatt av melanin, hemoglobin, kollagen, bilirubin og strukturen i hudlaget til fingeren. Disse målingene blir brukt til å lage særegne spektral signaturer for hver person, og de kan også brukes til å bestemme om det er dødt

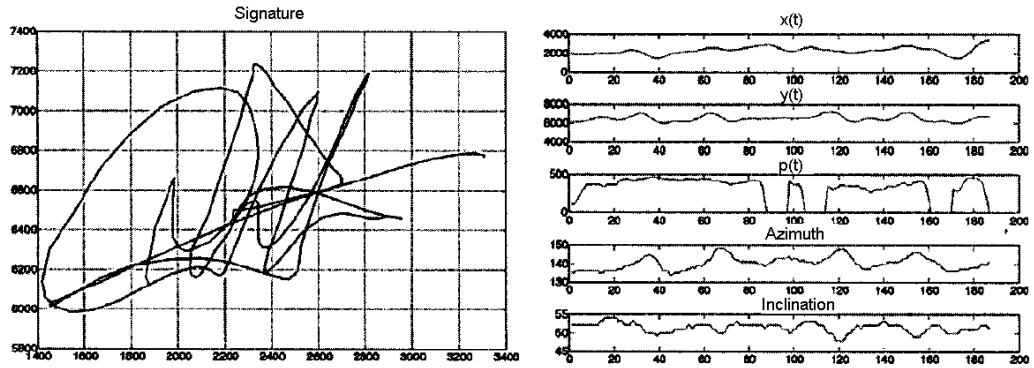
eller kunstig vev. Komposisjonen i vev blir raskt lavere når vev dør, og egenskapene til kunstig vev er forskjellig fra levende menneskehud.

Når det gjelder svettermålinger har forskere ved Clarkson Univerity og West Virgina University oppdaget en metode for å fastslå om en finger er levende som bygger på bestemte optiske, elektrooptiske eller faststoffssensorer. Disse sensorene har kapasitet til å analysere graden av fuktighet på en persons hud som er et resultat av svette fra et normalt menneske. Ved målinger tatt i intervaller på null, to og fem sekunder hvor det er forventet endring i mengde svette, forbedrer systemet evnen til å detektere om en finger er levende. [37]

6.2.3 Signatur

Hvordan er person signerer navnet sitt er også kjent som en biometrisk karakteristikk. En signatur er en atferdskarakteristikk som endres over tid ved innflytelse av både fysiske og emosjonelle forutsetninger. Signaturgjenkjenning kan deles i to kategorier, statisk og dynamisk. Ved statisk signaturgjenkjenning blir signaturen skrevet på papir før en optisk skanner eller et kamera leser signaturen og lagrer et grafisk bilde av den. Gjenkjenningen gjøres da på bakgrunn av signaturens form. Metoden kalles også offline signatur gjenkjenning. Dynamisk signaturgjenkjenning måler hvordan signaturen blir signert på en digitalisert grafisk plate ved hjelp av sensorer som registrerer en rekke tendenser som rytme, akselerasjon, vinkler, press mot skriveflaten og flyt. En penn kan også ha sensorer som kan registrere det samme. [57] Et annet navn på dynamisk signaturgjenkjenning er online signaturgjenkjenning.

Dynamisk signaturgjenkjenning:
Når signaturen skrives leses den dynamiske informasjonen inn ved hjelp av den grafiske plate eller pennen. Egenskaper fra de dynamiske systemene kan bli sortert i statiske og dynamiske trekk. De statiske trekkene taes ut fra hele prosess ved signering, som maksimum, minimum, og gjennomsnittlig



Illustrasjon 28: En signatur med tilhørende dynamisk informasjon

skrivehastighet, forhold mellom lang og korte pennestreker, segmentlengder, osv. Sammenkoblingen av alle disse målingene former en N-dimensjonal egenskapsvektor, hvor N er antall målinger. Disse egenskapene kalles også parametere. De dynamiske egenskapene er utviklingen av gitte parametere som funksjon av tid f(t), som noen vist i Illustrasjon 28. Eksempler er posisjon x(t),

y(t), hastighet v(t), akselerasjon a(t), trykk p(t), tangential akselerasjon ta(t), krumningsradius cr(t), normal akselerasjon na(t), osv. Disse egenskapene er også kalt funksjoner. [58] Funksjonene blir sendt til generering av mal. Ved gjenkjenning måles likheten mellom lagret mal og malen til den nye signaturen som blir lest inn. Når dynamiske egenskaper benyttes må en slags lengde normalisering brukes fordi en person skriver signaturen sin med ulik lengde for hver gang. Tre metoder kan brukes ved gjenkjenning:

1. Mønstergjenkjenningsmetode: Når mønstergjenkjenningsmetoden brukes sammenlignes input og signaturmodellen ved hjelp av avstandsmåling mellom dem. Den mest suksessfulle metoden for dette er Dynamic Time Warping (DTW). I DTW skjer sammenligningen ved bruk av en dynamisk programmeringsstrategi som takler variasjon i signaturenes lengde.
2. Stokastiske modeller: Egenskapene som trekkes ut fra signaturene former en statistisk modell. Ved testing blir likhetene mellom input og signaturmodellen etablert. Den mest populære metoden for dette er Hidden Markov Models (HMM) som skrevet om under avsnittet om ansiktsgjenkjenning. HMM sannsynlighetstetthetsfunksjonen er assosiert med hver tilstand. Tilstandene er koblet sammen ved overgangssannsynlighet. Sannsynligheten at en sekvens av egenskapsvektorer ble generert av denne modellen kan finnes ved Baum-Welch dekoding. HMM håndterer signaler med forskjellige varighet.
3. Nervenettverk: Periodisk nervenettverk, tidsforsinkede nervenettverk og hybridnettverk kan brukes for å anvende de dynamiske karakteristikkene. Nervenettverk har vist muligheter når det gjelder generalisering, men krever store mengder ekte og falske signaturer som ikke alltid er lett å få tak i.

Signaturverifikasjon har flere styrker. På grunn av den store mengder funksjoner presentert i en mal for en signatur, og vanskeligheten i å etterligne atferden ved signering, er metoden høyst motstandsdyktig mot forfalskninger. Som et resultat av lav falsk godkjenningsrate, kan anvendere stole på at de som blir godkjent er hvem de påstår å være. Signaturverifikasjon drar også nytte av å påvirke eksisterende prosesser og hardware som digital signaturplate og systemer basert på public key infrastructure(PKI), en populær metode for kryptering av data. Teknologien regnes også for å være mindre invasiv enn andre biometrier, siden folk er kjent med å underskrive avtaler etc. Men signaturverifikasjon har også noen svakheter:

- Noen personer har for stor variasjon i signaturen sin og får problemer med å registreres og verifiseres.
- Personer kan ha muskelsykdommer som fører til problemer ved registrering/verifisering.
- Signaturer utvikles over tid og blir påvirket av både fysiske og følelsesmessige omstendigheter.
- Mange brukere vil ikke være vant til å skrive på en grafisk plate, dette kan gi avvikende signaturer fra papirskrevne.

A.R.Baig og M.Hussain viser i ”Online Signature Recognition and Writer Identification by Spatial-Temporal Neural Processing” en metode som baserer seg på nerve arkitektur [59]. De oppnådde et resultat på 92% for signaturgjenkjenning og 94% for skriftgjenkjenning.

Online signaturgjenkjenning er mer robuste mot etterligninger enn andre biologiske egenskaper på grunn av den dynamiske karakteristikken i tillegg til de morfologiske karakteristikkene mens andre generelt bare benytter de morfologiske karakteristikkene. [60] J.Yi et.al i “Online signature verification using temporal shift estimated by the phase of Gabor filter” [60] har introdusert en ny metode for dynamisk tidsvridning for å kompensere ikke-lineære lokal tidsforskyvinger. Eksperimenter viste at antall innleste signaturer per person ga best resultat ved 20 stk signaturer med 6 % feilrate, mens for 3 stk signaturer 11 % feilrate. Og ved å innføre ISODATA, en algoritme som samler signaturer i grupper, ble feilratene reduserte. Ved 20 stk signaturer 2,5 % feilrate, mens ved 3 stk 9 % feilrate.

Flere produsenter har prøvd seg på introdusere dynamiske gjenkjenningssystemer for håndskrifter men foreløpig har ingen av dem blitt kommersielt suksessfulle. Derimot finnes potensial hvor skriftelige signaturer allerede er i bruk for eksempel formelle avtaler, kontraktinngåelse, kvitteringer ved mottagelse av tjenester og aksess til kontrollerte dokumenter.

6.2.4 Håndgeometri

Gjenkjenningssystemer for håndgeometri bruker et optisk kamera for å ta et 3D bilde av hånden. Algoritmer konverterer bildet til matematiske verdier. Over 90 dimensjonale målinger blir gjort, inkludert størrelsen på håndflaten, lengde, vidde og høyde på fingrene, og avstander mellom ledd og knokler. Se for hvordan en håndgeometrileser ser ut og for hvordan hånden skal plasseres i leseren.

Illustrasjon 29: Håndgeometrileser

Malen som lages av en hånd er ekstremt liten, bare 9 bytes. Til sammenligning krever fingeravtrykk 250-1000 bytes. Teknikken for gjenkjenning er veldig enkel, relativt enkel å bruke og rimelig i pris. Miljøforhold som lite luftfuktighet, støv og tørr hud ser ikke ut til å ha negativ effekt på verifiseringen til disse systemene. Selv om størrelsen på hendene til menneske er relativt stabile er derimot geometrien ikke kjent for å være særegen, slik at systemet ikke kan identifisere en person ut i fra en stor populasjon, men er begrenset til 1-til-1 verifikasjon.

Geometrien til en barnehånd er også stadig i vekst og ikke egnet til gjenkjenning uten hyppige oppdateringer. Ingersoll Rand [61] hevder de har løst den problematikken ved at systemet oppdaterer en lagret hånd ved hver gang den blir godkjent. En person kan da for eksempel legge på seg, naturlig eldre, og man slipper å registrere brukere på nytt. Brukeren må også i dette systemet

identifisere seg ved et id-nummer, slik at hånden sjekkes opp mot en bestemt lagret hånd.

Håndgeometri er ventet å være en av de sakte voksende biometriske karakteristikkene, og forventes å utgjøre ca 3.3% av hele det biometriske markede i 2008. Dette fordi håndgeometri typisk begrenset til aksesskontroll og tid og tilsyn. [62]

Håndgeometrisystemer kan lures ved hjelp av en modellhånd, men dette vil være vanskelig og tidkrevende.

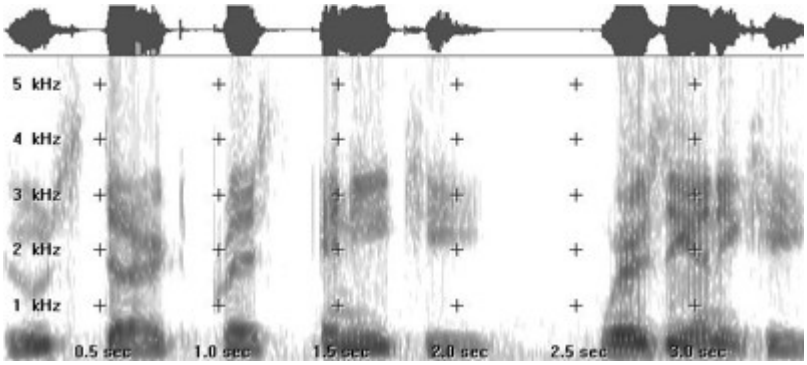
Illustrasjon 30: Hvordan hånden plasseres i en leser for håndgeometri.

6.2.5 Stemmekarakteristikk

Stemmekarakteristikk er en biometrisk verdi som er kombinert av fysiologi og atferd. Egenskapene til en persons stemme er avhengig av de fysiologiske delene som stemmeorganet, munnen, nesa og leppene. Atferdsdelen av stemmen til en person endres over tid i forhold til alder, medisinsk og følelsesmessig tilstand. En stemme er ikke særlig særegen og er ikke godt egnet til identifikasjon i stor målestokk. Stemmebasert identifisering brukes oftest hvor stemmen er det eneste biometriske alternativet, over telefon. Det er en enkelt å bruke og en akseptert metode siden det krever lite av en bruker. Stemmegjenkjenningssystemene kan deles inn i flere områder:

- Er systemet designet for en bruker eller flere?
- Kan systemet gjenkjenne kontinuerlig tale eller må brukerne atskille ordene?
- Er systemet tiltenkt tydelig talemateriale, eller tåler det bakgrunnsstøy?
- Er systemets ordforråd lite(titalls/hundretalls ord) eller stort(tusener ord)?
- Tekstavhengig eller tekstuavhengig?

Et tekstavhengig stemmegjenkjenningssystem er avhengig av en forhåndsdefinert frase som skal leses inn og gjenkjennes, mens et tekstuavhengig stemmegjenkjenningssystem gjenkjenner uavhengig av hva som sies. Det tekstuavhengig systemet er mye vanskeligere å designe enn det tekstavhengige, derimot er dette vanskeligere å lure fordi man ikke vet på forhånd hva som skal sies.
Stemmeinnlesninger blir digitalisert og en modell lagret. Ved verifisering sammenlignes innlesningen mot tidligere lagret modell av stemmen. Modellene kan vises i et lydspektrogram. En graf som viser lydens frekvens på vertikal akse og tid på horisontal akse. Se Illustrasjon 31 for et spektrogram av en stemme. [63] Forskjellige stemmelyder lager forskjellige former på grafen. Spektrogrammer bruker også farger eller skygger for å representere den akustiske kvaliteten av lyden.



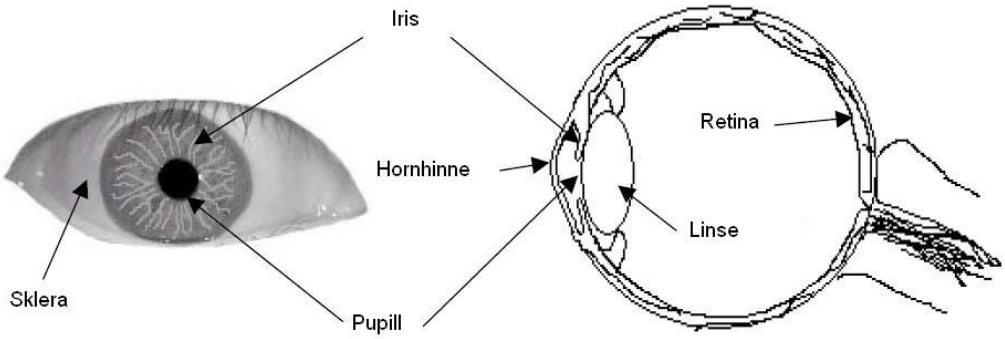
Illustrasjon 31: Opptak av en stemme vist i et spektrogram

Ulemper ved stemmebasert gjenkjenning:

- Taleutstyr er fintfølende for bakgrunnsstøy.
- En persons stemme kan endres ved sykdom, for eksempel forkjølelse.
- Stemmegjenkjenningssystemer kan bli lurt av digitale opptak av en godkjent person. [64][37]

6.2.6 Øyemønster

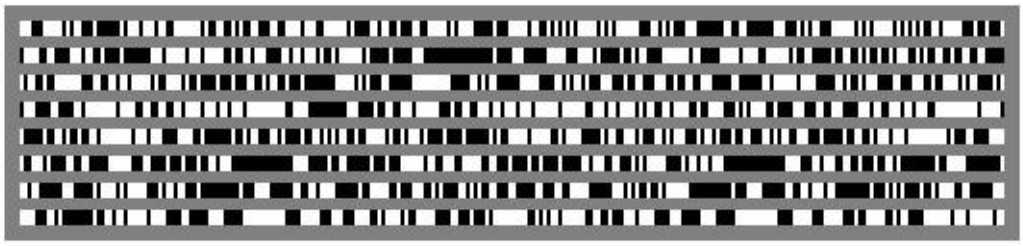
Av øyemønster har vi både iris og retina, begge er gitt som alternativer ved øyemønster i ICAO standarden. Se Illustrasjon 32 for hvor disse befinner seg i øyet.



Illustrasjon 32: Et øye vist forfra og i profil

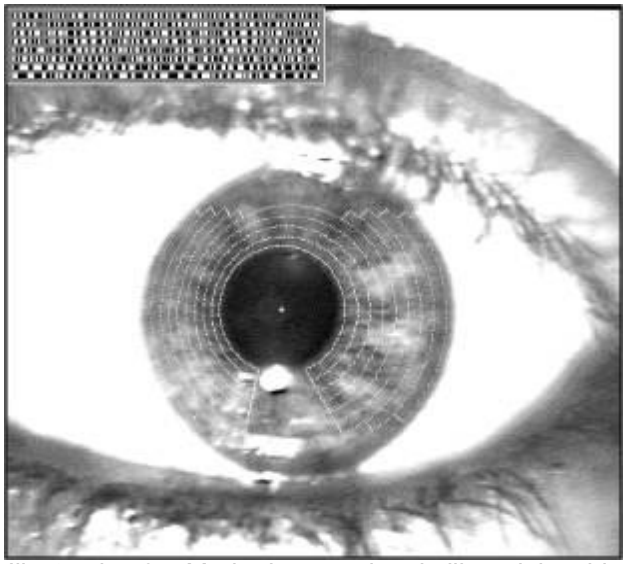
6.2.6.1 Iris

Den ringformede regionen som er avgrenset av pupillen og sklera(det hvite i øyet) på hver side i øyet er iris/regnbuehinnen. Per i dag påståes iris å være den mest nøyaktige, ikke-invasive og enkle biometriske verdien å bruke for sikker identifikasjon. Iris utvikles i løpet av de to første årene av et menneskets liv og den komplekse visuelle strukturen er særegen, selv for eneggede tvillinger og ulik på hvert øye for samme person. De synlige karakteristikkene konverteres som en fase sekvens til en 512 byte IrisCode™, en mal som lagres for gjenkjenning. Se Illustrasjon 33 for bilde av en iriskode.



Illustrasjon 33: Bilde av en iriskode (eng. "IrisCode")

Når bilde av iris skal taes må kamera ikke være lengre unna enn ca 90cm. Kameraet finner øynene og en algoritme snevrer inn fra venstre og høyre slik at ytterkantene på iris er funnet. Den horisontale tilnærming tar høyde for øyelokkene. Samtidig lokaliseres pupillen og det sees bort ifra de nedre 90^{o} på grunn av fuktighet og lys.



Illustrasjon 34: Markeringene viser hvilken del av iris som brukes til iriskoden.

Det monokrome kameraet bruker både visuelt og infrarødt lys, det siste i den lavere skalaen(700-900nm) av IR. Ved lokasjonen av iris bruker en algoritme 2-D Gabor wavelets til å filtrere og kartlegge segmenter av irisen til hundrevis av vektorer. Waveletene av forskjellig størrelse tilegnes verdier ut fra orientering og spatialfrekvens i bestemte områder. Dette former iriskoden. Ikke hele irisen brukes pga øyelokk og kameralys refleksjoner, se Illustrasjon 34. Denne teknologien gir eksepsjonelle detaljer, mye mer enn hva andre illustrasjoner eller punktbaserte presentasjoner kan tilby. Ved gjenkjenning sammenlignes den heksadesimale presentasjonen etter wavelet filtrering og kartlegging. [65]

Selv om iris er en av de senest biometriske teknologiene som har kommet, er irisgjenkjenning forventet å øke betraktelig i bruk de neste årene. Irisgjenkjenning har lav FMR(falsk godkjenning) og er det eneste alternative til fingeravtrykk i sikker 1-til-mange applikasjoner. Irisbaserte gjenkjenningssystemer er allerede tatt i bruk på flere flyplasser(Canada, Nederland og De forente arabiske emirater) for grensekontroll, begrenset adgang og forenklet passasjerreise. Ved grensekontroll med irisgjenkjenning kan passasjerer som har registrert iris, slippe omstendelig kontroll og de sikkerhetsansvarlige kan konsentrere seg om ukjente reisende. Et tilpasset

kamera tar bilde av begge iris og identifiserer på under 2 sekunder avhengig av hvor vanskelige forhold bildet taes under og hvor stor databasen den må søke i er. [66]

Irisgjenkjenningsteknologi har tradisjonelt blitt anvendt ved høysikkerhets fysisk aksess implementasjoner, men allerede i 2002 så man eksempler på høyprofilerte irisgjenkjenninger i nye applikasjoner. Iridian Technologies jobber for å få teknologien mer brukt i mindre bedrifter og i privat bruk, og har hatt noe suksess i logisk aksess i småskala. Det mest fremtredende nylig anvendelsen er passasjerautentisering ved flyplassene i U.S., U.K., Amsterdam og Island. Teknologien brukes også til å identifisere fanger i U.S. Flere av utviklingslandene vuderer iristeknologi i pass. [67]

Irisgjenkjenning krever en kontrollert og sammarbeidsvillig bruker de sekundene det tar å ta bilde av irisen. Dette kan være krevene for en uerfaren bruker. Nøyaktigheten assosiert med iris som gjenkjenningsteknologi kan overdrive virkeligheten til teknologiens effektivitet. Virkelige resultater lever ikke opp til de astronomiske projeksjonene leverandører hevder teknologien har fordi feilrate er beregnet utifra bedømmelse og gjenkjenning av ideelle irisfotografier. Siden iristeknologien er designet til å være en identifikasjonsteknologi, er reserveløsningene kanskje ikke så fullt utviklet som for verifikasjonsanvendelse(brukere vant til identifikasjon har kanskje ikke med nødvendig ID for eksempel). Dette reduserer ikke effektiviteten til irisgjenkjenning men kan være faktorer til at iristeknolgi ikke lever helt opp til forventningene.

Irisgjenkjenningssystemer må være i stand til å hamle opp med glass øyne, videoavspilling av iriser, høyoppløselige foto og kontaktlinser med påtrykte irismønstre. [37] Resultater av Matsumotos forskning som ble presentert i oktober 2004 viste at to kommersielle irisgjenkjenningsenheter ble lurt i 100% av testtilfellene, mens 50% for et annen type. Det ble brukt falske iris; papir med påtrykket ensformige fargemønstre lik iris basert på foto tatt av øyet med spesielt iriskamera eller et vanlig infrarødt kamera. Dette viser nødvendigheten av å teste på om en iris er levende. [68]

Alle leverandører av irisgjenkjenningssystemer hevder å kunne detektere om irisen er levende, selv om metodene deres sjeldent er offentlig tilgjengelige. [37]

Professor John Daugman ved Cambridge University som var pioneren av utvikling av iris gjenkjenningsalgoritmer har foreslått fire overordede tiltak for å sikre irisgjenkjenningssystemer.

1. Tiltak mot fotografier og spektrografi.
   Dette er relatert til spektroskopiteknikkene brukt ved fingeravtrykksgjenkjenning. Vev, blod, fett og melaninpigmenter i øyet oppfører seg annerledes når de er testet av forskjellige bølgelengder, og dette kan gi tegn på om irisen er ekte. 2D Fourierteknikker kan identifisere kontaktlinser med falske påtrykk av iris. Å undersøke om man kan få røde øyne, et resultat av refleksjon av retina, kan også brukes.

2. Tiltak mot atferd.
   Dette er basert på analyse av frivillig og ufrivillig atferd, som endring i pupillstørrelse ved forskjellige lysnivåer, deteksjon av bevegelse av pupillen og øyet og blunking. Videre forskning av mikrobevegelser kan også karakterisere et levende øye.
3. Tiltak mot analoge fysiske angrep.
   Dette kan bli brukt til å detektere høyoppløsningsfotografier eller kontaktlinser med påtrykket iris. Disse teknikkene kan oppdage punktmatriser og fargestoffer i noen trykketeknikker, eller de kan oppdage krumninger til en kontaktlinse i forhold til en ekte iris. Teknikkene kan også evaluere refleksjoner fra et levende øye man ikke vil få fra et fotografi.
4. Tiltak mot digitale avspillingsangrep.
   Fordi alle IrisCodes er identiske i størrelse og bruker samme kodingsstruktur uavhengig av underliggende karakteristikker, kan tilfeldige bytesammensetninger gi et tilnærmet uendelig antall mønster med forskjellige kombinasjoner. Hvis ikke den godkjente iris som er lagret og den presenterte ikke er kodet ved hjelp av den samme teknikken, vil en digital avspilling av en iris være ubrukelig.

International Biometric Group satt i gang en forskningsprosjekt Independent Testing of Iris Recognition Technology(ITIRT) i 2005 for å teste irisgjenkjenningsteknologi. [69] Registrering og gjenkjenningssoftware fra Iridian og utstyr fra LG, OKI og Panasonic ble testet:

- Vellykket registrering/innlesning skjedde i 98,39% av tilfellene for LG, 97,47% for OKI og 92,95 for Panasonic.
- Å registrere to iris tok 32s for LG, 48s for OKI og 35s for Panasonic.
- Gjennomsnittstiden for suksessfull gjenkjenning tok 1,92s for LG, 5,05s for OKI og 3,58s for Panasonic.
- Optimal var FNMR så lav som 0,5%, men kombinasjon av noe utsyr ga FNMR over 11%. LG hadde høyest FMR og FNMR. Panasonic hadde mer robust gjenkjenning mens relativ høy rate for mislykkede registreringer.

Miyazawa et al demonstrerte i 2005 at det kan benyttes lik fasebasert bildesammenligningsmetode for fingeravtrykk som for iris, slik at en kan implementere felles hardware/software for multimodale biometriske systemer med både iris og fingeravtrykksgjenkjenningsmuligheter. [70]

6.2.6.2 Retina

Regina gjenkjenning består av å ta bilde av og analysere mønsteret av blodkar på den tynne nerven bakerst i øyeeple som prosesserer lyset som slipper inn gjennom pupillen. Den vaskulære netthinna har en rik struktur og er en unik karakteristikk av hver person og hvert øye, t.o.m. for identiske tvillinger som nevnt for flere av de biometriske karakteristikkene. Retinamønsteret forblir normalt stabilt gjennom et menneskets liv, men kan bli berørt av sykdommer som grønn stær, diabetes, og høyt blodtrykk. Retina er påstått å være den mest sikre biometriske karakteristikken siden den ikke er lett å endre eller duplisere. Et bilde

taes i et okular, og man må ha øyets fokus på et spesielt punkt for at retina kan bli avbildet. Avbildingen krever stor samarbeidsvillighet fra den avbildede og bildet kan avsløre de medisinske tilstandene nevnt over. Dette taler mot bruk av retina i offentlige sammenhenger. [71]

6.2.7 Termogrammer: Ansikt, hånd og blodårer i hånden

Et infrarødt kamera kan ta bilde av varmen et menneske utstråler, dette gir et mønster som kan brukes til sammenligning. Teknologien krever ikke en samarbeidsvillig bruker og kan benyttes hvor gjenkjenning bør være hemmelig. Derimot kan teknologien ha problemer i ukontrollerte omgivelser hvor andre overflater utstråler varme (for eksempel varmeovner) i nærheten av hvor bilene taes.

En lignende teknologi bruker tilnærmet infrarød avbilding for å få tak i strukturen til blodårene på oversiden av en knyttet neve.

6.2.8 DNA

Deoksyribonukleinsyre (DNA) er den viktigste delen i kromosomene, menneskets gener er bygget opp av dette. Det kalles ofte "arvemolekylet" på grunn av at foreldre overfører kopi av DNAet sitt til barna sine ved reproduksjon. Et menneskets DNA kan man finne i blod, sæd, spytt, hår eller hud. Det er unikt for hvert menneske, bortsett fra at identiske tvillinger har like DNA mønstre. En DNA analyse sammenligner to DNA profiler mot hverandre. For 10 år siden kostet det over ti tusen kroner og tok måneder å få en analyse gjort, nå koster dette ca 1500kr og tar dager. DNA analyser brukes mest i rettsvitenskapen og er en av de mest pålitelige metodene for å identifisere kriminelle. [72]

6.2.9 Ganglag

Ganglag er menneskers måte å gå på, den er ikke særlig særegen men tilstrekkelig ulik nok til å brukes som verifikasjon i applikasjoner med lav sikkerhet. Ganglaget er en atferdskarakteristikk som kan endre seg, særlig over lang tid på grunn av forandring i vekt, eller på grunn av en alvorlig kneskade, hjerneskade eller på grunn av rus. Systemer som baserer seg på ganglag bruker videoopptak av et menneskets gange for å måle forskjellige bevegelser i hvert ledd. [38]

6.2.10 Lukt

Det er kjent at hvert menneske svetter ut en lukt som er karakteristisk i dens kjemiske sammensetning. En rekke kjemiske sensorer som er sensitive til spesielle aromatiske sammensetninger kan måle hvilke sensorer som reagerer og lage en mal av dette. Lukten er særegen for hvert menneske. Det er ikke kjent hvorvidt kroppslukten kan måles om en person har på seg deodorant og om miljøet rundt vil påvirke et måleresultat. [38]

6.2.11 Tasttrykk

Det er antatt at hver person har sin spesielle måte å skrive på et tastatur. Teknologien er enda ung og lite forsket på. Denne atferdskarakteristikken er ikke

forventet å være unik for hver person men gir tilstrekkelig informasjon til identifikasjons verifisering.

Det måles hvor lenge en tast holdes inn og hvor lang tid mellom hvert tastetrykk. En bruker velger et ord på minst åtte tegn som skrives inn i tillegg til brukernavn. Ved registrering kan en bruker måtte skrive inn brukernavn og ordet sitt 15 ganger, dette kan oppleves som mye arbeid.

Personer som brukere touchmetoden vil skrive mest konsist, men det vil også være vanskeligere å skille fra hverandre personer fordi flere bruker samme skrivemetode. For noen kan man forvente store variasjoner i tastingen.

Teknologien arver mange svakheter fra systemer som bruker passord.

En slik teknologi vil kunne overvåke uten personers viten mens disse skriver inn informasjon. [38] [73]

6.2.12 Øre

Det er forelått at formen til et øre og strukturen av brusk og vev i ytterøret er karakteristiske. I en øregjenkjenning vil fremtredende punkter i ytterøre sammenlignes. Egenskapene til et øre er derimot ikke forventet å være særegne når identifikasjon skal gjøres. [38]

7 Diskusjon

Det finnes flere alternative teknologier for implementasjon av biometriske kontrollmetoder for reisedokument. Av disse er det i tråd med ICAOs beslutninger trådløse smartkort som egner seg best som teknologi, på grunn av sin omgjengelighet, raske overføring og akseptable lagringskapasitet. En annen teknologi som også er godkjent for bruk til elektroniske reisedokument er optiske smartkort. Denne har større lagringskapasitet enn trådløse smartkort, men er utsatt for slitasjeskader.

Den trådløse teknologien er forøvrig ikke designet med hovedvekt på sikkerhet og det eksisterer derfor flere sikkerhetsproblem knyttet til implementasjonen.

Den eneste obligatoriske sikkerhetsmekanismen, passiv autentisering, gir en minimal beskyttelse. Den hindrer kun at informasjonen i brikken endres. Metoden hindrer ikke uautorisert tilgang og kopiering eller utskiftning av brikken. I tillegg er den utsatt for skimming- og lytteangrep fra større avstander.

ICAO spesifiserer også flere alternative sikkerhetsmekanismer for å forhindre denne type angrep.

Aktiv autentisering er en utvidelse av den passive autentiseringen og hindrer kopiering av dokumentets sikkerhetsobjekt (SO_D) samtidig som den beviser den logiske datastrukturens og reisedokumentets integritet. Metoden kan forøvrig utsettes for "Grandmaster Chess" angrep og lures til å gi fra seg informasjon til feil leseenhet.

Den grunnleggende tilgangskontrollen skal hindre skimmingangrep og tyvlytting på kommunikasjonskanalen, men hindrer ikke kopiering av hele reisedokumentet. Denne metoden er forøvrig utsatt for forskjellige brute-force angrep, spesielt siden deler av nøkkelinformasjonen kan la seg utlede.

Utvidet tilgangskontroll utvider den grunnleggende tilgangskontrollen, ved bruk av egendefinerte nøkler eller alternative algoritmer, og skal hindre tilgang til biometriske verdier. Implementasjoner som baserer seg på den generelle tilgangskontrollen vil forøvrig ikke nødvendigvis beskytte all informasjonen i brikken. En alternativ protokoll som Caernarvon kan brukes for å øke denne sikkerheten.

Alle de overnevnte frivillige sikkerhetsprinsippene er avhengige av kommunikasjonsgrensesnitt type B, som tillater en prosesserende integrert trådløs krets. En av grunnene til at den obligatoriske sikkerhetsspesifikasjonen er så svak er at ICAO av økonomiske årsaker også har bestemt seg for at kommunikasjonsgrensesnitt type A også skal støttes. Dette utelukker alle sikkerhetsprinsipp som baserer seg på en prosesserende integrert trådløs krets. Det finnes også frivillige sikkerhetsteknikker som støtter type A.

Faraday-bur kan brukes for å hindre skimmingangrep, mens sammenligning av den maskinlesbare sonen (MRZ) kan sammenlignes med MRZ som ligger lagret

i den logiske datastrukturen (LDS) for å forsikre at brikken tilhører reisedokumentet.

Kryptering av den biometriske informasjonen kan erstatte eller utfylle den utvidede tilgangskontrollen.

Så ser vi på de biometriske karakteristikkene som er godkjente av ICAO standarden for bruk i MRTDer.

Det ble bestemt at ansiktet fremdeles skulle være den primære identifikator for MRTDer og utvide dette til å gjelde et digitalt lagret fotografi for maskinassistert identitetsverifisering. En stor fordel med dette valget er at et fotografi av ansiktet allerede er i bruk i pass og folk er vant til det. Registreringsprosessen blir den samme ved at fotografi taes og verifiseres rutinemessig ved produksjon, nye og kostbare metoder trengs ikke i registreringsprosessen. Ansiktet brukes ikke bare i pass, men også på bankkort, id-kort og førerkort for å forenkle daglige identifiseringer. Et ansiktsfotografi avslører heller ikke noe mer enn hva vi daglig viser allmennheten. Det er lett å anskaffe og kan registreres med et godkjent fotografi uten at personen fysisk er tilstede. Når det gjelder biometri er det også snakk om grad av påtrengenhet, hvorvidt en bruker må ta på eller samhandle med teknisk utstyr for å bli registrert eller verifisert. Dette taler til fordel for bruk av ansiktet siden ansiktsfotografier kan taes litt på avstand, også uten en brukers viten om dette skulle være nødvendig. Det er også praktisk for å utelukke spesielle personer. Hvis personer er etterlyst er det som oftest ansiktet som er den eneste biometriske karakteristikken som er tilgjengelig.

Selv om utviklingen har gått rett vei med ansiktsgjenkjenningsteknologien, fra år 2000 til 2002 hadde systemene 50% reduksjon i feilrate, blir ikke gjenkjenning gjort i mer enn 90% av tilfellene med en falsk godkjenningsrate på 1%, og det er av det beste systemet. Dette er resultater fra den siste ansiktsgjenkjenningstesten FRVT 2002. En ny test gjøres nå i disse tider og resultater derfra vil vise om systemene har bedret seg enda mer. Dagens mulige plastiske operasjoner og profesjonelle maskører kan omforme et ansikt. Dette har vi sett i filmer og på tv. Har man tid og ressurser får man endret utseende om man vil. Hvis man ønsker å ligne en spesiell person er det heller ikke vanskelig å fotografere noen usett for å ha en mal.

På grunn av at bruken av ansikt allerede er godt innarbeidet i pass og siden det var stor forbedring av ansiktgjenkjenningsteknologien på bare to år, fra år 2000 til 2002, tror vi mye har skjedd siden da. Resultatet fra år 2002 var akseptabelt på det beste, og vi mener nå at ansiktgjenkjenningssystemene er gode nok til å taes inn som maskinassistert gjenkjenning av ansikter.

Fingeravtrykk er sikker i 1-til-mange gjenkjenning på grunn av det særegne ved hvert enkelt fingeravtrykk. Det er også en av de eldst biometriske karakteristikkene som er forsket på og testet for angrep, særlig etter kommersialiseringen av fingeravtrykksenheter. Dette har bidratt til at flere svakheter ved systemene allerede er eliminert og kvaliteten på sensorer som gjenkjenner avtrykk generelt er blitt bedre. Mangfoldet av sensorer er også blitt

stort og anerkjente tester burde være med på å avgjøre hvilken sensor som velges. Det er også forsket på flere metoder for hvordan man undersøker om en finger er levende som bidrar til forbedringer av systemet.

I sluttet av år 2000 ble en av de første publikasjonene om fingeravtrykkssensorer som ble lurt av falske fingre utgitt. En rekke publikasjoner er utgitt etter dette, de fleste har klart å lure sensorene. For eksempel ble en optisk sensor lurt av silikonfingre i desember 2004, mens en silikonsensor ikke ble lurt i samme forsøk. Det finnes flere metoder for å lage falsk fingeravtrykk, både metoder som benytter mer avansert utstyr og ikke fullt så tilgjengelig materialer og metoder som benytter utstyr og materiale som er lett tilgjengelig for alle. Dette gjør at hvem som helst kan lage falske fingeravtrykk. Fingeravtrykk kan finnes hvor som helst, vi legger dem igjen overalt og på glatte overflater er det lett å kopiere et avtrykk. Det vil være en enkel sak å få tak i fingeravtrykk til en bestemt person. De gode egenskapene gelatin har for å simulere menneskevev taler også mot fingeravtrykksteknologien.

Siden fingeravtrykksensorene er en av de biometriske systemene som er mest testet på og forsøkt lurt, og forskning gjøres på metoder som bestemmer om en finger er levende, mener vi også dette er en av de beste tilgjengelig biometriske karakteristikkene.

Teknologien for iris er foreløpig det eneste alternativet til fingeravtrykk i 1-til-mange gjenkjenning, den er særegen, selv ulik for hvert av øynene. Iris er også tatt i bruk ved flere flyplasser som gjør at teknologien blir testet ut og utbedrelser vil bli gjort. Men foreløpig er teknologien enda ung og lite testet på. Glassøyne, videoavspilling av iris, høyoppløselig foto og kontaktlinser med påtrykket irismønstre er mulig måter å lure et gjenkjenningssystem på. I oktober 2004 lurte Matsumoto irisgjenkjenningsenheter ved hjelp av papir med påtrykket iris. Den ene enheten ble lurt i 100% av tilfellene, en annen type i 50% av tilfellene. International Biometric Group testet gjenkjenningsenheter i 2005. Testen viste varierende kvalitet fra de forskjellige produsentene og sammenheng mellom høyere falsk godkjenning(FMR) og falsk avvisning(FNMR) og god gjenkjenningsrate, og lavere FMR og FNMR og dårligere gjenkjenningsrate. I tillegg krever innlesning en kontrollert og samarbeidsvillig bruker de sekundene det tar, en prosess som kan være krevende for en uerfaren bruker.

På grunn av International Biometric Groups test på teknolgien for iris som viser at kvaliteten er varierende og ingen har både god feilrate og gjenkjenningsrate mener vi iris ikke bør brukes. Derimot ser vi at karakteristikken har potensial på grunn av særegenheten og vil utvikles siden den allerede er tatt i bruk på flere flyplasser.

Videre ser vi på de andre biometriske teknologiene som er tatt med som mulige alternativer i MRTD.

Signaturgjenkjenningsteknologien er høyst motstandsdyktig mot forfalskninger når vi ser på den dynamiske signaturgjenkjenningen. Det regnes som umulig å etterligne menneskers måte å skrive signaturen sin på, med alle de målinger av

trykk, akselerasjon, hastighet og posisjoner som gjøres. Problemer med teknologien er at den krever gjerne 20stk signaturer innskrevet og lagret for å gi en sikker gjenkjenning med lav feilrate. Vi skriver nemlig ikke signaturen vår likt hver gang, noen personer kan ha problemer med å bli registrert i det hele tatt. Det er for eksempel uvanlig å skrive på en grafisk plate, dette krever trening, og personer kan ha muskelsykdommer som gjør signaturer skrevet etter hverandre svært forskjellige.

Håndgeometri bruker en enkel teknologi til gjenkjenning, flere målinger av hånden gjøres og lagres i en mal på bare 9 bytes. Hvis lagringsplass er et problem er denne metoden verdt å ta med. Geometrien til hånden er derimot ikke særlig særegen og gjenkjenning kan kun gjøres i 1-til-1. Dessuten kan det skape problemer med å gjenkjenne en hånd etter for eksempel vektøkning.

Stemmegjenkjenning er enkelt å bruke og krever lite av en bruker. Derimot er en stemme ikke særlig særegen og endres ved for eksempel en forkjølelse. Taleutstyr er også ofte finfølende for bakgrunnsstøy og kan lures av digitale opptak.

ICAO Standarden har også åpnet for at retina kan brukes som alternativt øyemønster. Retina er en unik karakteristikk for hver person og forblir stabil gjennom hele livet, men vil kunne bli berørt ved sykdommer som grønn stær, diabetes og høyt blodtrykk. På grunn av mulig avsløring av overnevnte sykdommer og at avbildningen av retina krever stor samarbeidsvillighet av bruker, taler dette mot retina brukt i offentlige sammenhenger.

Av de fire mulige alternativene til elektroniske pass kommer håndgeometri best ut, men kun som et tillegg til de tre biometriske karakteristikkene som er godkjente siden den ikke er særlig særegen. Ellers er signaturen litt for tungvinn på grunn av det store antallet signaturer som må registreres. Stemmen er altfor lite særegen og retina kan avsløre sykdommer og krever stor samarbeidsvillighet.

Vi har også sett på de mest kjente biometriske karakteristikkene som det ikke er åpnet for i standarden. Ingen av dem bør vurderes å taes med i pass foreløpig på grunn av at ingen av dem har særlige gode egenskaper egnet for pass. Her er noen grunner til dette:

- Termogrammer er følsomme for utstråling av varme fra omgivelsene
- DNA har en for omfattende sammenligningsprosess
- Ganglaget til mennesker er ikke særlig særegen og kan endres over tid
- Det er usikkert om lukten fra mennesker påvirkes av deodorant/parfyme/omgivelser
- Tastetrykk er for lite særegent for et menneske og arver svakheter fra passordbaserte systemer
- Øre er ikke særlig særegent. Da foretrekkes heller for eksempel ansikt som baserer seg på lignende gjenkjenningsmetode.

Ved å bruke multimodale systemer, systemer som sjekker flere biometriske karakteristikker før en person godkjennes, vil sikkerheten økes i et system. Det er vanskelig og tidkrevende å kopiere flere biometriske karakteristikker og man forholder seg til forskjellige applikasjoner som har sine strenge krav til godkjenning. Derimot vil en passkontroll ta lengre tid hvis flere biometriske karakteristikker skal undersøkes, og innkjøp av mer utstyr vil gjøre kostnadene større.

Generelt sett er det varierende kvalitet på utstyr til bruk i biometriske systemer. Vi mener det er viktig å la seg veilede av anerkjente tester før en velger produsent til hvilken som helst biometrisk karakteristikk som skal gjenkjennes.

Uansett hvor sikkert et biometrisk system er, kommer en feil til å skje. Enten på grunn av et angrep eller at en naturlig feil skjer. Ingen biometriske systemer er motstandsdyktige mot angrep. Enten skjer angrep der hvor biometri leses inn, i prosessering og overføring, eller i lagringsenheten. Et eksempel er overbelastning av innlesningsenheten en mulighet for å frambringe feil. Hurtig blinkende sterkts lyst mot optiske fingeravtrykkssensorer og ansiktsavbildningsenheter kan avbryte korrekte funksjoner. Silikonsensorer kan lett ødelegges ved å kortslutte dem eller dyppe dem i vann. Mange biometriske systemer er avhengig av sensitivt utstyr som lett kan bli ødelagt, enten ved at brukere forårsaker feil eller det skjer en systemsvikt. Uansett må systemet være designet slik at basisfunksjonene fremdeles fungerer ved feil, eller hvis utstyret ikke kan gjøre sin påtenkte funksjon må det finnes en reserveløsning. En person kan forårsake feil fordi han/hun vet at en ubevoktet dør vil bli benyttet som et alternativ. Sikkerhetssystemer må være beredt til potensielle funksjonsfeil i biometriske systemer og ha en tilstrekkelig reserveløsning.

Andre svakheter i biometrisk systemer kan være ved overførsel av biometriske verdier mellom leser og der verdiene prosesseres, og i selve prosesseringsleddet til systemet. De fleste biometriske systemer krypterer data ved sending, men ikke alle applikasjoner og enheter er enkle å benytte ved kryptering. Ansvaret for å implementere kryptering legges over på de som skal anvende utstyr og designe systemet. IBMs teknikk som forvrenger originale bilder og lagrer forvrengingen i stede for originalen beskytter biometri lagret i databaser selv om de skulle bli stjålet.

8 Konklusjon

Vi har i denne oppgaven evaluert de biometriske verdiene og teknologiene som spesifiseres av ICAO til bruk i elektroniske pass.

I løpet av vårt arbeid har vi konkludert med at ICAO har funnet fram til de best egnede biometriske karakteristikkene til bruk i reisedokument. FERET testen fra 2002 viste akseptable resultater for ansiktsgjenkjenning, og teknologien har forbedret seg ytterligere de siste fire årene. Videre er fingeravtrykk også en teknologi som har utviklet seg mye i de seinere år. Fingeravtrykk fremstår derfor som den beste biometrien i tillegg til ansiktsbiometri. Iris er forøvrig den teknologien som har mest potensial til sikker identifisering, men teknologien for irisgjenkjenning er fortsatt svært ung og ikke god nok enda. Ingen av de andre undersøkte biometriske karakteristikkene har kvaliteten som kreves for sikker identifisering.

Det viktigste er å teste på flere biometriske karakteristikker; å bruke et multimodalt system for å øke sikkerheten.

Vi har også sett på alternative lagringsteknologier. Her kan vi konkludere med at trådløse smartkort er den beste teknologien til implementasjon av elektroniske reisedokument.

Rapporten legger stor vekt på analyse av sikkerheten i metodene som spesifiseres for å beskytte den biometriske informasjonen. Ut i fra dette arbeidet kan vi trekke følgende konklusjon: Den obligatoriske beskyttelsen i form av passive autentisering er for svak og er et resultat av ICAOs ønske om å støtte begge kommunikasjonsgrensesnittene, som spesifiseres av ISO 14443. Bakgrunnen for dette er økonomiske kostnader og kravet om at den obligatoriske løsningen må være relativt billig å innføre. For å forsterke sikkerheten i den obligatoriske løsningen bør derfor sikkerhetsprinsippene som støtter begge grensesnittene, Faraday-bur, MRZ-sammenligning og kryptering av tilleggsbiometri, gjøres obligatoriske. Også de alternative løsningene ICAO spesifiserer for kommunikasjonsgrensesnitt type B kan utsettes for angrep. Derfor bør det oppfordres til å implementere Type B med minimum grunnleggende tilgangskontroll i implementasjoner som følger minstekravene for informasjonen som lagres. Ved lagring av tilleggsbiometri bør også en utvidet tilgangskontroll implementeres. Denne bør bygge på egendefinerte nøkler eller alternative løsninger som Caernarvon-protokollen.

Selvkritikk
Vi evaluerer kun standarden slik den spesifiserer. Den totale løsningen i henhold til pass er opp til hvert enkelt land eller organisasjon å utarbeide. Det finnes veldig mange forskjellige måter å implementere en løsning. Vi har ikke fordypet oss i de forskjellige implementasjonene. En kritikk av systemet vil derfor ikke nødvendigvis være berettiget.

Sikkerhet i reisedokument er et stort og omfattende tema bestående av mange prosesser. Den endelige sikkerheten avhenger av det svakeste leddet. Vi har

ikke lagt vekt på produksjonen og selve passkontrollen da dette vil avhenge av implementasjonen.

Vårt arbeid baserer seg på Doc 9303 fra 2003 og tilhørende uformelle supplement fra 2004. Neste utgave av Doc 9303 er ventet i første halvdel av 2006. Da vår rapport ble publisert var denne enda ikke utgitt. Det må derfor taes forbehold om at en eventuell kritikk i denne rapporten blir rettet opp i versjon 6 av Doc 9303.

Forslag til videre arbeid
Evaluering i et eventuelt videre arbeid bør ta hensyn til den nye versjonen av Doc 9303 som kommer i første halvdel av 2006.

Appendiks

A1 Glossar & forkortelser

Bilirubin:	Gallen inneholder blant annet fargestoffer. Et av disse fargestoffene er bilirubin som dannes ved nedbrytning av hemoglobin
Doc 9303:	Standard for offisielle reisedokument
Hemoglobin:	fargestoffet i røde blodlegemer
IC:	Integrated Circuit. Integrert krets / databrikke.
ICAO:	International Civil Aviation Organization
Induksjon:	det dannes elektrisk strøm i en gjenstand ved påvirkning av magnetisme
ISO:	International Organization for Standardization
Kohesiv:	noe som er kohesivt består av deler som passer godt sammen for å gi en helhet
Kollagen:	viktig protein i vev
LDS	Logic Data Structure. Logisk datastruktur for lagring av informasjon i RFID-brikken og overførsel mellom leseren(PCD) og brikken. Spesifisert i *"Development of a Logical Data Structure – LDS for Optional Capacity Expansion Technologies"* [13].
Melanin:	brunt fargestoff i hud
Monokrom:	en(s)farget
Morfologi:	å studere enkelt cellenes utforming [http://biologi.uio.no/mbot/]
MRP:	Maskinlesbare pass (Machine Readable Passports)
MRTD:	Maskinlesbare reisedokument (Machine Readable Travel Documents)
MRZ:	Machine Readable Zone
OCR-B:	Tegnsett for optisk tegngjenkjenning (Optical Character Recognition)

PCD: Proximity Coupling Device. Lese-/Skriveenhet for PICC, spesifisert av ISO 14443.

PICC: Proximity Integrated Circuit Card. RFID-brikke spesifisert av ISO 14443.

RFID: Radio Frequency Identification. Trådløs identifiseringsbrikke.

Spektroskopi: en fellesbetegnelse på målemetoder som baserer seg på at atomer kan ta opp og sende fra seg elektromagnetisk energi.

Synapse: to nervecellers berøringssted

TAG/MRTD: Technical Advisory Group on Machine Readable Travel Documents

VIZ: Visual Inspection Zone

A2 Referanser

1: Wikipedia.org, Visa,
http://en.wikipedia.org/wiki/Visa_(document),2006

2: Europakommisjonen, Schengenavtalen,
http://www.europakommisjonen.no/tema/jai/schengen.htm

3: 106th U.S. Congress, Visa Waiver Permanent Program Act,
http://www.usdoj.gov/eoir/vll/legislation/HR3767.pdf, 2000

4: U.S Department of State, Visa Waiver Program,
http://travel.state.gov/visa/temp/without/without_1990.html, 2005

5: Wikipediar.org, Passport, ,
http://en.wikipediar.org/wiki/Passport, 2006

6: United Nations, Basic Facts About the United Nations,
http://www.un.org/aboutun/history.htm, 2000

7: International Civil Aviation Organization, The Need for MRTD,
http://www.icao.int/mrtd/guidance/HistNeed.cfm, 2006

8: International Civil Aviation Organization,
The ICAO Panel on Passport Cards, 1968-1978,
http://www.icao.int/mrtd/guidance/HistIcaoPanel.cfm, 2006

9: International Civil Aviation Organization, Establishment of the Technical Advisory Group on MRTD,
http://www.icao.int/mrtd/guidance/HistEstablishment.cfm, 2006

10: Technical Advisory Group on Machine Readable Passports (TAG/MRTD), Doc 9303 Part1, Section IV: Technical Specifications Unique To Machine Readable Passports, 2003

11: International Civil Aviation Organization Technical Advisory Group for Machine Readable Travel Documents / New Technologies Working Group (ICAO TAG MRTD/NTWG), Biometrics Deployment Of Machine Readable Travel Documents,
http://www.icao.int/mrtd/download/documents/Biometrics%20deployment%20of%20Machine%20Readable%20Travel%20Documents%202004.pdf, 2004

12: International Civil Aviation Organization Technical Advisory Group for Machine Readable Travel Documents / New Technologies Working Group (ICAO TAG MRTD/NTWG), PKI for Machine Readable Travel Documents offering ICC Read-Only Access,

,http://www.icao.int/mrtd/download/documents/TR-PKI%20mrtds%20ICC%20read-only%20access%20v1_1.pdf, 2004

13: International Civil Aviation Organization Technical Advisory Group for Machine Readable Travel Documents / New Technologies Working Group (ICAO TAG MRTD/NTWG), Development of a Logical Data Structure – LDS – for Optional Capacity Expansion Technologies, http://www.icao.int/mrtd/download/documents/LDS-technical%20report%202004.pdf, 2004

14: International Organization for Standardization (ISO) / InternationalElectrotechnical Commission (IEC), ISO/IEC 14443: Identification cards – Contactless integrated circuit(s) cards - Proximity cards, ,http://www.iso.org/, 2005

15: International Civil Aviation Organization Technical Advisory Group for Machine Readable Travel Documents / New Technologies Working Group (ICAO TAG MRTD/NTWG), Use of Contactless Integrated Circuits In Machine Readable Travel Documents, http://www.icao.int/mrtd/download/documents/Annex%20I%20-%20Contactless%20ICs.pdf, 2004

16: UPM Rafsec, Tutorial overview of inductively coupled RFID Systems, http://www.rafsec.com/rfidsystems.pdf, 2003

17: International Sivil Aviation Organization (ICAO), Doc 9303, Annex to Section III: Security Standards for Machine Readable Travel Documents, 2003

18: International Organization for Standardization (ISO) / InternationalElectrotechnical Commission (IEC), ISO/IEC 14443: Identification cards – Contactless integrated circuit(s) cards - Proximity cards - Part 2: Radio Frequency Power Signal Interface, http://www.iso.org/, 2005

19: International Organization for Standardization (ISO) / InternationalElectrotechnical Commission (IEC), ISO/IEC 14443: Identification cards – Contactless integrated circuit(s) cards - Proximity cards – Part 3: Initialization and anticollision, http://www.iso.org/, 2005

20: International Civil Aviation Organization Technical Advisory Group for Machine Readable Travel Documents / New Technologies Working Group (ICAO TAG MRTD/NTWG), PKI Digital Signatures For Machine Readable Travel Documents, http://www.icao.int/mrtd/download/documents/PKI%20Digital%20Signatures.PDF, 2003

21: William C. Barker, NIST Special Publication 800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA)

Block Cipher, ,http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf, 2004

22: E. Barker, W. Barker, W. Burr, W. Polk og M. Smid, NIST Special Publication 800-57 Recommendation for Key Management – Part 1: General, http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part1.pdf, 2005

23: National Institute of Standards and Technology, FIPS 186-2, Federal Information Processing Standards (FIPS PUB) 186-2(+ Change Notice), Digital Signature Standard (DSS), http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf, 2000

24: Matt Bishop, Computer Security – Art and Science, 2003 ,Addison-Wesley,ISBN 0-201-44099-7.

25: National Institute of Standards and Technology (NIST), FIPS 186-3, Federal Information Processing Standards (FIPS PUB) 186-3, Digital Signature Standard (DSS), ,http://csrc.nist.gov/publications/drafts/fips_186-3/Draft-FIPS-186-3%20_March2006.pdf, 2006

26: J. Johnsson og B. Kalinski, RFC3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf, 2003

27: Accredited Standards Committee, American National Standard X9.62-2005, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005

28: Federal Information Processing Standards Publications (FIPS PUBS), FIPS 180-2, Federal Information Processing Standards Publication (FIPS PUB 180-2, Secure Hash Standard (SHS), http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf, 2002

29: David Clark, A propsed methodology for an IACO PKI infrastructure for implemetation of digital signatures on MRTDs, 2003

30: Z. Kefir og A. Wool, Picking virual pockets using relay attacks on contactless smartcard systems, 2005

31: Marc Witteman, Attacks on Digital Passports, 2005

32: Georg Apenes, Hanne P. Gulbrandsen og Atle Årnes, Endelig rapport fra tilsyn Politidirektoratet Saksnummer: 2005/1363 , 2006

33: Gaurav S. Kc og Paul A. Karger, Preventing Attacks on Machine Readable Travel Documents, 2005

34: Xiaoyun Wang, Yiqun Lisa Yin og Hongbo Yu, Collision search attacks on SHA1, 2005

35: Dennis Kügler, Advanced Security Mechanisms for Machine Readable Travel Documents, 2005

36: Sun Microsystems, Inc., Smart Card Overview, http://java.sun.com/products/javacard/smartcards.html, 2006

37: International Biometric Group, Vulnerabilities of Biometric Technologies, 2005

38: Jain, A.K, Ross, A, Prabhakar, S., An introduction to biometric recognition, 2004

39: ICAO TAG MRTD/NTWG, Biometrics deployment of Machine Readable Travel Documents, 2004

40: The History of Fingerprints, http://onin.com/fp/fphistory.html, 2005

41: Anil K. Jain, Biometric Recognition: How Do I Know Who You Are?", 2005

42: International Biometric Group , User Perceptions, 2006

43: FERET, 2006

44: Wikipedia, Facial recognition system, http://en.wikipedia.org/wiki/Facial_recognition_system, 2006

45: Wikipedia, Eigenface, http://en.wikipedia.org/wiki/Eigenface, 2006

46: Shiguang Shan, Bo Cao, Wen Gao, Debin Zhao., Extended Fisherface for face recognition from a single example image per person, 2002

47: Nefian, A.V.; Hayes, M.H., III, Hidden Markov models for face recognition, 1998

48: M. Bicego, U. Castellani, V. Murino, Using Hidden Markov Models and Wavelets for face recognition, 2003

49: Otluman, H.; Aboulnasr, T., Low complexity 2-D Hidden Markov Model for face recognition, 2000

50: Zhu, J., & von der Malsburg, C. , Object recognition by Dynamic Link Matching in biologically realistic time, 2003

51: Bruce Sneider, Beyond Fear: Thinking Sensibly about Security in an Uncertain World, 2003

52: Stephanie A. C. Schuckers, Spoofing and Anti-Spoofing Measures, 2002

53: Johan Blommé, Evaluation of biometric security systemsagainst artificial fingers, 2003

54: Marie Sandström, Liveness Detection in FingerprintRecognition Systems, 2004

55: Anders Wiehe, Torkjel Søndrol, Ole Kasper Olsen, Fredrik Skarderud, Attacking Fingerprint Sensors, 2004

56: Lumidigm, http://www.lumidigm.com/, 2005

57: Wikipedia, Handwriting recognizer, http://en.wikipedia.org/wiki/Handwriting_recognizer, 2006

58: Marcos Faundez-Zanuy, Signature Recognition State-of-the-Art, 2005

59: A. Rauf Baig og Masroor Hussain, Online Signature Recognition and Writer Identification by Spatial-Temporal Neural Processing, 2004

60: Jonghyon Yi, Chulhan Lee, Jaihie Kim, Online signature verification using temporal shift estimated by the phase of Gabor filter, 2005

61: Ingersoll Rand, http://www.irsecuritytechnologies.nl/, 2004

62: International Biometric Group , Hand Geometry Market Size, http://www.biometricgroup.com/reports/public/reports/hand-scan_market.html, 2006

63: Voiceprints, http://computer.howstuffworks.com/biometrics4.htm, 2006

64: Wikipedia, Voice recognition, http://en.wikipedia.org/wiki/Voice_recognition, 2006

65: International Biometric Group, Iris Recognition: How it Works, http://www.biometricgroup.com/reports/public/reports/iris-scan_tech.html, 2006

66: Iridian technologies, http://www.iridiantech.com/, 2003

67: International Biometric Group, Typical Iris Recognition Applications, http://www.biometricgroup.com/reports/public/reports/iris-scan_applications.html, 2006

68: Tsutomu Matsumoto, Gummy Finger and Paper Iris: An Update, 2004

69: International Biometric Group, Independent Testing ofIris Recognition Technology, 2005

70: Miyazawa, K. Ito, K. Aoki, T. Kobayashi, K. Nakajima, H., An Efficient Iris Recognition Algorithm Using Phase-Based Image Matching, 2005

71: Retina and Iris Identification, http://www.globalsecurity.org/security/systems/eye_scan.htm, 2005

72: Wikipedia, DNA, ,http://en.wikipedia.org/wiki/DNA,2006
Nanavati, Samir., Thieme, Michael., Nanavati, Ray., Biometrics - Identity Verification in a Networked World, 2002,John Wiley & Sons, Inc.,0471099457.

A3 Illustrasjoner

A4 Tabelliste