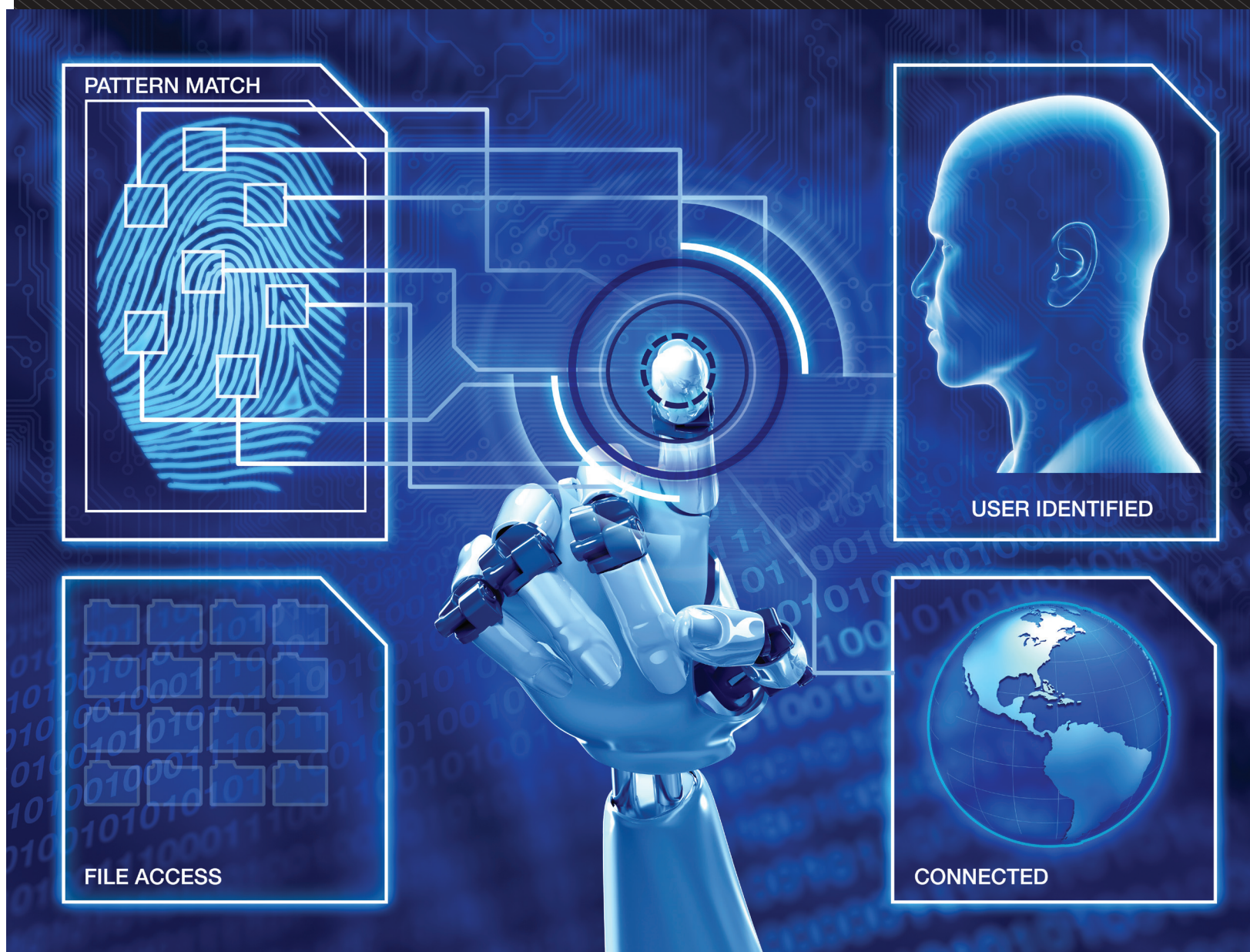




Nasjonalt ID-senter

Biometri og identitet

Utfordringer og nye muligheter for utlendingsforvaltningen



the 'information' and 'communication' fields. The 'information' field is defined as:

...the study of the processes of information production, distribution, access, use and evaluation, and the study of the social, cultural, economic and political contexts in which these processes take place. (p. 10)

The 'communication' field is defined as:

...the study of the processes of communication production, distribution, access, use and evaluation, and the study of the social, cultural, economic and political contexts in which these processes take place. (p. 10)

The 'information science' field is defined as:

...the study of the processes of information production, distribution, access, use and evaluation, and the study of the social, cultural, economic and political contexts in which these processes take place. (p. 10)

The 'information studies' field is defined as:

...the study of the processes of information production, distribution, access, use and evaluation, and the study of the social, cultural, economic and political contexts in which these processes take place. (p. 10)

The 'information technology' field is defined as:

...the study of the processes of information production, distribution, access, use and evaluation, and the study of the social, cultural, economic and political contexts in which these processes take place. (p. 10)

The 'information systems' field is defined as:

...the study of the processes of information production, distribution, access, use and evaluation, and the study of the social, cultural, economic and political contexts in which these processes take place. (p. 10)

The 'information management' field is defined as:

...the study of the processes of information production, distribution, access, use and evaluation, and the study of the social, cultural, economic and political contexts in which these processes take place. (p. 10)

The 'information policy' field is defined as:

...the study of the processes of information production, distribution, access, use and evaluation, and the study of the social, cultural, economic and political contexts in which these processes take place. (p. 10)

The 'information law' field is defined as:

...the study of the processes of information production, distribution, access, use and evaluation, and the study of the social, cultural, economic and political contexts in which these processes take place. (p. 10)

The 'information ethics' field is defined as:

...the study of the processes of information production, distribution, access, use and evaluation, and the study of the social, cultural, economic and political contexts in which these processes take place. (p. 10)

The 'information education' field is defined as:

...the study of the processes of information production, distribution, access, use and evaluation, and the study of the social, cultural, economic and political contexts in which these processes take place. (p. 10)

Sammendrag

Biometri er et viktig virkemiddel i arbeidet med å avklare identitet. Biometri er et tiltak som har blitt tatt i bruk på migrasjonsområdet i flere land. I denne rapporten har Nasjonalt ID-senter undersøkt i hvilken grad biometri kan utnyttes bedre i norsk utlendingsforvaltning. Nasjonalt ID-senters undersøkelser viser at politiet og utlendingsforvaltningen kan bruke biometri på en bedre måte enn i dag. Det er rom for å lagre biometri i større grad, og vi kan utnytte de biometriske systemene bedre. Det kan dreie seg om bedre utnyttelse av eksisterende databaser, større grad av sentral lagring av biometri og bedre opplæring i opptak, lagring og søk i biometriske systemer.

I Schengen-området er det innført flere biometriske systemer. Biometri av asylsøkere blir lagret i Eurodac, som ble opprettet i 2003. I 2010 ble det innført biometri i oppholdskort som utstedes til utlendinger som får oppholdstillatelse. Fra oktober 2011 ble fingeravtrykk og bilde av visumpliktige som reiser til Norge og 26 andre europeiske land, lagret i en sentral database i EU: Visa Information System (VIS). Nyere pass inneholder biometri i form av foto og fingeravtrykk som kan leses elektronisk (ePass).

I denne rapporten beskriver vi regelverk, rutiner og praksis i førstelinjen til politiet og utenriks tjenesten. Vi presenterer de viktigste biometriske systemene i bruk i norsk utlendingsforvaltning, ser nærmere på de tekniske aspektene, og går gjennom reglene for opptak, lagring og søk.

Vi har kartlagt praksis når det gjelder bruk av biometri for identifiserings- og verifiseringsformål gjennom intervjuer med ulike politidistrikter, særorgan og grensekontroll nasjonalt. I tillegg har vi forespurt syv internasjonale aktører om opptak og lagring av biometri i visum- og oppholdssaker. Gjennom kartleggingen har vi gjort funn som tilsier at politiet ikke fullt ut bruker den muligheten de har til å registrere og foreta søk i flere saker der identiteten ikke er fastlagt. Spesielt gjelder dette i søknader om oppholdstillatelse. Større grad av sentral lagring av biometri vil gi en gevinst i identitetsarbeidet, blant annet ved at det er lettere å kontrollere om en person oppholder seg i landet under flere identiteter. Nasjonalt ID-senter anbefaler å opprette en nasjonal database for å lagre biometri i alle utlendingssaker.

I utlendingsdatabasen (UDB) er det lagret ansiktsfoto av alle som har søkt visum, oppholdstillatelse eller beskyttelse i Norge. Nasjonalt ID-senter foreslår et pilotprosjekt for å utrede og undersøke mulighetene for å sammenligne foto i denne databasen.

De ansatte i førstelinjen ønsker seg mer opplæring og bedre rutinebeskrivelser i sakshåndtering, regelverk og bruk av utstyr. Nasjonalt ID-senter mener at opplæringsarbeidet i politiet og utenriks tjenesten bør styrkes.

Betingelsene for å kunne gjennomføre en effektiv utlendingskontroll bør bli bedre. Nasjonalt ID-senter foreslår et pilotprosjekt der man prøver ut håndholdte mobile enheter som kan brukes til å kontrollere biometri i operativ tjeneste i politiet.

Med ett overordnet register der man kan «låse» identiteten til biometri, for eksempel til personens fingeravtrykk, ville både søk og registrering blitt enklere og sikrere

Under kartleggingen nevnte et av politidistriktene et eksempel med en utlending som figurerte med flere identiteter i ulike registre: én identitet i folkeregisteret, to i det sentrale straffe- og politiopplysningsregisteret (SSP), to identiteter i politiets saksbehandlingssystem BL, og fire identiteter i den politioperative loggen (PO-loggen).

Innhold

Sammendrag	3
1 Innledning	6
1.1 Rapportens oppbygning	6
1.2 Bakgrunnen for prosjektet	6
1.3 Mandat	7
1.4 Hovedproblemstillinger og avgrensninger	7
1.5 Datagrunnlag og metode	7
2 Biometri	8
2.1 Biometri i det moderne samfunnet	8
2.2 Biometri og biometriske systemer	8
2.3 Biometri og personvern	10
2.4 Informasjonssikkerhet	11
2.5 Personvernimplikasjonene knyttet til biometriske løsninger	11
3 Biometriske systemer i utlendingsforvaltningen	13
3.1 Utlendingsdatabasen – UDB	13
3.2 Utlendingsregisteret	14
3.3 Eurodac	16
3.4 Visa Information System – VIS	17
3.5 Schengen-standardiserte oppholdskort	20
3.6 EU/Schengen Smart border system	22
4 Kartlegging – politiets arbeid med opptak av biometri, lagring og søk i registre	23
4.1 Kompetanse- og opplæringsbehov	23
4.2 Utilstrekkelige rutiner eller rutinebeskrivelser	24
4.3 Politiets utstyr	25
4.4 Systemløsninger og registerforvaltning	26
4.5 Kartlegging av praksis for opptak, lagring og søk i registre i syv land	27
5 Oppsummering og anbefalinger	29
5.1 Oversikt over anbefalinger og etatenes ansvar	29
5.2 Bruken av biometri i utlendingsforvaltningen bør utvides	30
5.3 Det bør opprettes et nytt system for opplæring	34
5.4 Tekniske løsninger og systemer	34
5.5 Pilotprosjekter	35
5.6 Politiets rutiner for samhandling internt og eksternt bør forbedres	36
Ordliste	37
Kilder	40
Figurer og tabeller	
Tabell 1	13
Tabell 2	42
Figur 1	14
Figur 2	15
Vedlegg	42

1 Innledning

1.1 Rapportens oppbygning

I kapittel 1 tar vi for oss bakgrunnen for prosjektet, med mandat, hovedproblemstillinger, avgrensninger og metode. Kapittel 2 gir en oversikt over biometriske systemer som bruker automatisert gjenkjenning for å identifisere en person eller verifisere en identitet. Vi gjør også rede for informasjonssikkerhet og personvern knyttet til bruk av biometriske løsninger. I kapittel 3 går vi nærmere inn på tekniske aspekter ved de ulike biometriske systemene i utlendingsforvaltningen.

I kapittel 4 presenterer vi funn fra en nasjonal kartlegging av hvordan biometri brukes for identifiserings- og verifiseringsformål i førstelinjen. I tillegg har vi forespurt syv internasjonale aktører om opptak og lagring av biometri i visum- og oppholdssaker. I kapittel 5 kommer vi med forslag og anbefalinger til hvordan utlendingsforvaltningen bedre kan utnytte biometri i identitetsarbeidet.

1.2 Bakgrunnen for prosjektet

Globaliseringen har gjort verden mindre ved at vi forflytter oss mer fra land til land og i et raskere tempo enn tidligere. Innrulling av mennesker i offentlige registre har spilt en viktig rolle i fremveksten av dagens velferdssamfunn. Folketrygd, skattesystemer og andre registre baserer seg på standardisering og

kvantifisering av befolkninger som basis for å hente inn informasjon, planlegge og fordele ressurser. Det oppstår derfor utfordringer i utlendingsforvaltningen og andre offentlige etater når noen mennesker forsøker å tilegne seg rettigheter de ikke har krav på. Det er viktig å arbeide med preventive tiltak for å bekjempe identitetsmisbruk. Identitetsmisbruk er et stort og voksende problem i samfunnet generelt. Utlendingsforvaltningen har behov for kontroll og bedre muligheter for å kunne vurdere identitet.

Biometri er en generisk teknologi som muliggjør en rekke teknologiske bruksområder og praksiser. Teknologien har ikke et fastlagt bruksområde, men biometriske systemer kan tas i bruk på en rekke områder, for eksempel i helsevesenet, informasjonssystemer, transportsektoren og regulering av global migrasjon.¹

Det er en stor utfordring for utlendingsmyndighetene at utlendinger som søker beskyttelse eller annen oppholdstillatelse, ankommer uten reisedokumenter. Det er derfor nødvendig å benytte andre metoder som kan forenkle og styrke identitetsarbeidet i utlendingsforvaltningen.

I dag tas det opp biometri av utlendinger i visse tilfeller, men biometrien lagres i forskjellige databaser, avhengig av sakstype. Dette gjør at en utlending som oppholder seg i Norge, kan

være registrert med forskjellige identiteter i forskjellige databaser, og på den måten kan operere med ulike identiteter i Norge. For eksempel er det mulig å lure til seg tillatelser eller velferdsgoder, eller bedrive kriminell virksomhet. Behovet for en sikker identifiserings- og verifiseringsmetode i utlendingsforvaltningen underbygges av at stadig flere blir avslørt i identitetsmisbruk. Det finnes dessverre ikke statistikk på omfanget av identitetsmisbruk, men dette er en utfordring som Nasjonalt ID-senter vil legge vekt på i tiden fremover.

Biometrisk identitetskontroll vil redusere muligheten for identitetsforveksling og identitetstyveri og forhindre at utlendinger opererer med ulike tillatelser under ulike identiteter.

På den andre siden er det en vanskelig situasjon for den som ikke kan identifisere seg, fordi identitet er et viktig bindeledd til å bli integrert i samfunnet. Å leve i et samfunn uten avklart identitet byr på utfordringer og problemer for utlendingen, som da vil ha begrensede rettigheter.

Nasjonalt ID-senter gjennomførte i 2011 et kartleggingsprosjekt der arbeidsprosessene hos aktørene i utlendingsforvaltningen⁴ ble undersøkt for å avklare aktørenes behov innen identitetsarbeidet. Aktørene som deltok i kartleggingen, ytret ønske om utvidet bruk av biometri i

1. Rommetveit (2011).

2. Bare 9 % av asylsøkerne i 2011 fremla reisedokumenter i forbindelse med asylregistreringen, ifølge Politiets utlendingsenhetens årsmelding for 2011.

3. Nasjonalt ID-senter: Kartleggingsprosjekt 2011.

4. Utlendingsnemnda (UNE), Utlendingsdirektoratet (UDI), Landinfo, Politiets utlendingsenhet (PU), Kripos, Politiets sikkerhetstjeneste (PST), Utenriksdepartementet (UD), Integrerings- og mangfoldsdirektoratet (IMDi), politidistriktene Gardermoen, Hordaland, Østfold og Øst-Finnmark.

identitetsarbeidet. En videre utredning var ønsket som et strakstiltak.

1.3 Mandat

Nasjonalt ID-senter skal styrke utlendingsforvaltningens og politiets arbeid med å avklare identiteten til utlendinger som søker seg til, kommer til eller oppholder seg i Norge.

Systemet, slik det er i dag, åpner for at utlendinger kan operere med flere identiteter. I dag tas det opp biometri for pass, reisebevis og oppholdskort, men de biometriske dataene lagres ikke i en database, de er bare lagret i selve kortet eller reisedokumentet. I de tilfellene utlendinger ikke kan dokumentere identiteten sin, eller hvis de legger frem falske dokumenter eller dokumenter med lav eller ingen notoritet (etterprøvnbarhet), er det nødvendig å finne nye metoder og verktøy. Nasjonalt ID-senter bidrar til å utvikle verktøy og metoder som kan benyttes når en utlendingsidentitet av ulike grunner ikke er dokumentert.

Noen av våre hovedoppgaver er å yte bistand og rådgivning på generelt grunnlag og i enkeltsaker. Dette innebærer blant annet å bistå departementene med analyser og koordinere fag- og metodeutviklingen knyttet til identitets- og dokumentasjonsarbeidet i utlendingsforvaltningen.

Formålet med denne rapporten er å se på om økt bruk av biometri som metode kan bedre identitetsarbeidet.

I rapporten synliggjør vi de mulighetene og begrensningene som ligger i opptak, lagring og deling av biometri når det gjelder identitetsarbeidet til aktørene i utlendingsforvaltningen.

1.4 Hovedproblemstillinger og avgrensninger

Mulighetene for bruk av biometri er omfattende. Vår avgrensning er knyttet til identitetsarbeidet i utlendingsforvaltningen. For å vise mulighetene og begrensningene som ligger i opptak, lagring og søk av biometriske data er det nødvendig å gå gjennom dagens regelverk, også knyttet til personvern. I tillegg kartlegger vi de tekniske mulighetene. Vi ser på potensialet som ligger i bruk av biometri innen utlendingsforvaltningen, og om utlendingsforvaltningen utnytter dagens muligheter for å ta i bruk biometri så langt de tekniske løsningene og gjeldende regelverk tillater det. Vi gir også en komprimert og helhetlig oversikt over hvordan biometri brukes i utlendingsforvaltningen i dag.

Vi konsentrerer oss om norske utlendingsmyndigheters bruk av biometri knyttet til utlendingsinnreise og-/eller opphold i landet. Vi har ikke vurdert politiets bruk av biometri i straffesaker.

Det er svært viktig å kontrollere underlagsdokumentasjon når man skal utstede biometriske identitetsdokumenter, siden disse har høyere legitimitet. Dette er imidlertid ikke

fokuset vårt i denne rapporten, men et arbeid som Nasjonalt ID-senter vil følge opp.

Med begrepet biometri mener vi først og fremst ansiktsfoto og fingeravtrykk.

I rapporten fokuserer vi på utfordringer knyttet til identitetsarbeidet i politiet, men disse erfaringene vil også være overførbare til førstelinjen⁵ i utlendingsforvaltningen.

1.5 Datagrunnlag og metode

Arbeidet med biometriprosjektet har siden oppstarten i januar 2012 bestått av en kvalitativ kartleggingsfase, der prosjektet har hentet inn fakta rundt praksis i førstelinjen i utlendingsforvaltningen når det gjelder bruk av biometri for identifiserings- og verifiseringsformål. Vi har kartlagt både praktiske, teknologiske og juridiske løsninger for bruk av biometri.

Vi har gjennomført kvalitative kartleggingsintervjuer med flere aktører, blant annet ulike politidistrikter, særorgan, grensekontrollører og internasjonale aktører.

Rapporten er skrevet av ansatte ved Nasjonalt ID-senter med bistand fra prosjektmedarbeider fra Justis- og beredskapsdepartementet (JD). Vi har bygget videre på funnene i Utlendingsdirektoratets rapport «Bruk av biometri i utlendingsforvaltningen».⁶

5. Førstelinjen i utlendingsforvaltningen er den første kontakten en person har med norske myndigheter i en utlendingssak. Førstelinjen veileder og jobber med forvaltningsoppgaver knyttet til søknadsbehandlingen av utlendingssaker. Disse oppgavene utføres i dag hovedsakelig av politiet, Utlendingsdirektoratet og på utenriksstasjonene.

6. Utlendingsdirektoratet, «Bruk av biometri i utlendingsforvaltningen» 2010.

2 Biometri

Ordet biometri kommer fra gresk og er en sammensetning av ordene «bios», som betyr liv, og «metron», som betyr mål. Biometriske teknologier utnytter de unike og målbare karakteristikkene hos et menneske.

International Organization of Standardization (ISO) forklarer biometrisk gjenkjenning som automatisert gjenkjenning av individer basert på deres adferdsmessige og biologiske egenskaper.⁷ Det finnes to hovedkategorier biometriske teknologier. Den første kategorien er basert på anatomiske eller fysiologiske karakteristikk. Eksempler på dette er gjenkjenning av fingeravtrykk, ansikt, iris, stemme og håndgeometri. Den andre kategorien er adferdsbasert, og teknologien måler blant annet adferd som inkluderer gjenkjenning av for eksempel håndskrift, tastodynamikk og ganglag.⁸

Skal biometri brukes til verifisering eller identifisering, må de biometriske identifikatorene oppfylle visse krav. Biometrien må være unik for personen, den må være enkel å avlese, og den må ikke endre seg mye over personens livsløp. I denne rapporten konsentrerer vi oss om to biometriske identifikatorer – ansiktsfoto og fingeravtrykk – som brukes til både identifisering og verifisering.

2.1 Biometri i det moderne samfunnet

Fremveksten av velferdsstater, moderne samfunnsstrukturer og

en stadig mer mobil befolkning har skapt et behov for hjelpemidler som kan brukes til sikker og rask identifisering og verifisering av identitet.

Men globalisering og kompliserte samfunnsstrukturer gjør også samfunnet sårbart for misbruk av identitet. Personer kan misbruke identitet for å lure til seg tillatelser, godkjenninger, velferdsgoder eller som ledd i kriminell virksomhet av mer eller mindre alvorlig grad. En stor del av denne problematikken angår utlendingsmyndighetene, men en rekke andre offentlige og private aktører er også berørt.

Det er en stor utfordring for utlendingsmyndighetene at utlendinger som søker beskyttelse, ankommer landet uten reisedokumenter. Det er viktig å vite hvem som oppholder seg i landet. På den annen side skaper dette også en vanskelig situasjon for den som ikke kan identifisere seg, fordi identitet er viktig for å bli integrert i samfunnet.

Biometrisk teknologi bidrar til å verifisere og identifisere personer. De tradisjonelle metodene, derimot, omfatter noe du «vet» eller «har» (for eksempel passord, PIN-koder, fødselsnummer). Verifiseringen eller identifiseringen skjer da ved hjelp av tildelte identitetsmidler. Det som er unikt med biometriske metoder, er at de tar i bruk kroppen, noe du «er». Dette har både fordeler og ulemper. Utviklingen av teknologien gjør den

stadig mer anvendbar og brukervennlig. Så langt er den praktiske bruken av biometriske teknikker knyttet til verifisering og identifisering. Her er noen eksempler der biometri brukes til verifisering eller identifisering:

- visumsøknader
- søknader om oppholdstillatelse og beskyttelse
- automatisk grensekontroll (ePass)
- utdeling av nødhjelp
- befolkningsregistrering
- valg⁹
- adgangskontroll (PC, bygning, journaler)
- utbetaling av sosiale ytelser
- økonomiske transaksjoner
- låse bolig og kjøretøy
- arbeidstidsregistrering
- utlån av bøker på biblioteket
- rask innsjekking på flyplasser for utvalgte grupper
- etterforskning
- overvåkning

2.2 Biometri og biometriske systemer

Det finnes en rekke ulike biometriske systemer som bruker automatisert gjenkjenning for å identifisere en person eller verifisere en identitet. Ett kjent system, som er tatt i bruk i politiet og i utlendingsforvaltningen i Norge, er Automated Fingerprint Identification System (AFIS). EUs rådgivende organ for personvernsspørsmål beskriver biometriske systemer som applikasjoner som tar

7. Betegnelsen biometri på norsk refererer til to ulike fagfelt. Betegnelsen benyttes om biostatistikk, som analyserer biologiske data ved bruk av matematiske og statistiske metoder, eller om automatiserte systemer for gjenkjenning ved å ta i bruk unike målbare biologiske kjennetegn. På engelsk er det ulike betegnelser for disse to fagfeltene, henholdsvis biometry og biometrics. På norsk bruker vi bare ordet biometri.

8. Nancy Yue Lieu, 2012.

9. Biometri kan tilby løsninger for å modernisere valgprosesser, der styrking av demokrati, mer åpenhet, og kamp mot korrupsjon og svindel står sentralt. For eksempel benyttes biometri ved valg i Burkina Faso.

i bruk biometriske teknologier for automatisk identifisering og-/ eller verifisering av en person. Identifiserings- og verifiseringsapplikasjoner blir ofte brukt til ulike oppgaver, på forskjellige områder og for ulike formål.¹⁰

Proessen med å samle inn biometriske prøver fra en person og den påfølgende bearbeidingen og omgjøringen av biometriske originaldata til en mal som så lagres i et biometrisk system, kan deles inn i fire trinn: innsamling, behandling, lagring og sammenligning.¹¹ De tre første prosessstrinnene innsamling, behandling og lagring utgjør *innrulleringen*.

Innrulling

- **Innsamling:** Biometriske kjennetegn samles vanligvis inn ved hjelp av sensorer, for eksempel et kamera eller en optisk skanner.
- **Behandling:** Originaldata (foto, fingeravtrykk) blir gjort om til en mal.¹² I denne prosessen benyttes en algoritme som trekker ut et sett nøkkeldata fra de biometriske kjennetegnene, og bearbeider på den måten de biometriske kjennetegnene til en mal. Denne malen kan så i neste omgang sammenlignes med én eller flere lagrede maler. Prosessen kalles uttrekking.
- **Lagring:** Malen kan lagres lokalt på den innretningen der originaldataene blir behandlet, eller i et kort som personen kan

ha med seg, der brikken enten kan leses av ved kontakt eller fjernavleses (RFID-brikke¹³). Malen kan også lagres i en sentral database.

Algoritmen som brukes i innrulleringen, må være den samme som senere brukes til identifisering eller verifisering. Dersom originaldataene er tilgjengelige i lagringsmediet, vil et hvilket som helst biometrisk system kunne utføre en sammenligning. Biometriske teknikker forutsetter at originaldataene tilfredsstiller visse kvalitetskrav.

Sammenligning

En ny biometrisk prøve blir sammenlignet med den lagrede malen. Sammenligningen resulterer i en poengsum. En beslutning om «godkjent» eller «avvist» avhenger av om poengsummen overstiger en viss terskel. Vi skiller mellom ulike typer prosesser for sammenligning: identifisering, verifisering og screening.

- **Identifisering** er en prosess for å finne ut identiteten når den ikke er kjent. Dette er med andre ord en «én-til-mange»-sammenligning. Når biometriske systemer brukes til identifisering, vil den biometriske prøven som personen avgir på identifiseringstidspunktet, bli sammenlignet med en mengde lagrede maler. Dette forutsetter lagring i en sentral database. Etter søk i basen returnerer systemet et svar som viser at det er «søketreff» eller «ikke søketreff» på en

person som tidligere er innrullet i basen.

- **Verifisering** er en prosess for å forsikre seg om at en person er den han utgir seg for å være. Det er med andre ord en «én-til-én»-sammenligning. Når biometriske systemer brukes til verifisering, vil den biometriske prøven som personen avgir på verifiseringstidspunktet, bli sammenlignet med den lagrede malen som tilhører samme person.
- **Verifisering med *sentral database*** foregår slik at tidligere innrullede biometriske data, for eksempel fingeravtrykk som er lagret for vedkommende, blir hentet opp fra den sentrale databasen for å bli sammenlignet med fingeravtrykkene som avgis i forbindelse med en kontroll. Selve sammenligningen kan skje enten lokalt på den tekniske innretningen som brukes i kontrollen, eller i en annen teknisk innretning der fingeravtrykkene har blitt overført for sentral lagring.
- **Verifisering med en *lokal innretning*** gjøres vanligvis ved at verifiseringssystemet trekker ut de bestemte biometriske dataene, for eksempel fingeravtrykk, fra RFID-brikken for sammenligning med fingeravtrykk som avgis i en kontroll. Personaliaopplysninger kan være lagret i mikrobrikken, alternativt printet på identitets-

10. Article 29 Data Protection Working Party, wp 80, Working Document on Biometrics.

11. Article 29 Data Protection Working Party, wp 193, Opinion 3/2012 on Developments in Biometric Technologies. 00720/12/en wp 193.

12. Template på engelsk.

13. I oppholdskort, pass og reisebevis benyttes det en slik RFID-brikke, og vi vil omtale disse brikkene som RFID-brikker videre i rapporten.

kortet. Resultatet av sammenligningen vil vise om personen er den rettmessige eieren av identitetsdokumentet.

- Screening/observasjonslister: Biometri kan også brukes som et ledd i en sikkerhetsforanstaltning, med bruk av databaser og observasjonslister. Eksempelvis kan personer som er utvist, eller som skal pågripes, stå oppført på en slik liste. Alle som gjennomgår screening, avlegger en biometrisk prøve som sammenlignes med biometriske data som er lagret i observasjonslista. Personen blir da bare identifisert hvis han står på lista, og kan passere dersom søket ikke resulterer i treff. Etter kontrollen forkastes den biometriske prøven. Personer kan være gjort kjent med at det utføres screening, og den typiske situasjonen er grensepassering. Men screening kan også utføres i skjul for eksempel ved bruk av sikkerhetskamera og ansiktsgjenkjenning ved å skanne ansikter i en menneskemengde¹⁴ og undersøke om noen av dem er registrert i en observasjonsliste.

Verifisering har to feilkilder. Den første er «falsk positiv» (False Acceptance Rate, FAR), som angir sannsynligheten for at en person blir feilaktig gjenkjent av systemet. Den andre feilkilden er «falsk negativ» (False Rejection Rate, FRR), som angir sannsynligheten for at et

system mislykkes i å gjenkjenne en person som faktisk er registrert i systemet.

I kalibrering av biometriske systemer er ambisjonen å finne et nivå der både FAR og FRR ligger på et forsvarlig nivå. Dette nivået kan variere ut fra sikkerhetshensyn og behovet for effektivitet, brukervennlighet og kundeservice.

2.3 Biometri og personvern

Personvern handler om at vi har behov for en privat sfære som vi selv kontrollerer. Når vi vil uttrykke dette aspektet i personvernet, snakker vi om retten til privatlivets fred. Personvern handler også om den enkeltes personlige integritet og verdighet. Dette aspektet er knyttet til retten til å bestemme over og ha kontroll over personopplysninger om seg selv.

I menneskerettighetslovgivningen er retten til privatliv en uomtvistelig fundamental rettighet som skal beskyttes. Retten er nedfelt i FNs universelle menneskerettighetserklæring av 1948, FN-konvensjonen om sivile og politiske rettigheter, og den europeiske menneskerettighetskonvensjonen. Sistnevnte regner opp hensyn som viser at retten ikke er absolutt, og at privatlivet må vike i noen tilfeller:

Artikkel 8. Retten til respekt for privatliv og familieliv

1. *Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin*

korrespondanse.

2. *Det skal ikke skje noe inngrep av offentlig myndighet i utøvelsen av denne rettighet unntatt når dette er i samsvar med loven og er nødvendig i et demokratisk samfunn av hensyn til den nasjonale sikkerhet, offentlige trygghet eller landets økonomiske velferd, for å forebygge uorden eller kriminalitet, for å beskytte helse eller moral, eller for å beskytte andres rettigheter og friheter.*

Bestemmelsen pålegger statene å fastsette lover som verner om privatlivets fred og sikrer at integritet og ære ikke blir krenket. Plikten omfatter også ansvar for lovgivning som regulerer innsamling, behandling og utveksling/spredning av personopplysninger.

Denne plikten følges opp i lovgivningen på EU-nivå i Europaparlamentets og Europarådets personverndirektiv.¹⁵ Direktivet omhandler beskyttelse av personer i forbindelse med behandling av personopplysninger og fri utveksling av slike opplysninger. Personopplysningsloven er i hovedsak utformet etter personverndirektivet og tar opp i seg kravene i direktivet. Personverndirektivet stiller krav om at medlemsstatene fastsetter vilkår for behandling av personnummer og *andre personlige identifikatorer*.¹⁶ Dette inkluderer også biometriske identifikatorer.

Den praktiske bruken av biometri i dag er som nevnt knyttet til *verifisering og identifisering*. Det er denne bruken dagens lovgivning tar sikte

14. «Face in the crowd biometrics».

15. Direktiv 95/46/EF (personverndirektivet).

16. Personverndirektivet artikkel 8, nr. 7.

på å regulere. Bruk av biometri blir behandlet i særlovgivningen i tillegg til at personopplysningsloven legger noen føringer for adgangen til å ta i bruk biometri. Det er ikke gitt bestemmelser som eksplisitt regulerer bruk av biometriske teknikker. Personopplysningsloven § 12 regulerer imidlertid bruk av fødselsnummer og bruk av «andre entydige identifiseringsmidler». Forarbeidene nevner andre entydige identifikasjonsmidler, som fingeravtrykk og andre biometriske data.¹⁷ Det er antatt at enhver fremgangsmåte som gjør det mulig å identifisere en person, er omfattet av bestemmelsen. Et særtrekk ved biometriske identifikatorer sammenlignet med tradisjonelle identifikatorer er som tidligere nevnt at våre biometriske kjennetegn er en del av kroppen vår som ikke kan skiftes ut eller endres på.

Mens biometriske kjennetegn som ansikt og fingeravtrykk er tilgjengelige i det offentlige rom og ikke er å regne som sensitive opplysninger, vil andre biometriske data betraktes som personsensitive, blant annet dersom de inneholder informasjon om helse. Misbruket kan for eksempel bestå i å skaffe seg uautorisert adgang eller tilgang på personinformasjon. Samtidig har biometriske teknikker mange fortrinn som tilskynder bruk av teknologien, nettopp fordi biometriske teknikker gir entydig verifisering og dermed bedre sikkerhet enn tradisjonelle identifikatorer. Det er vanskeligere å låne bort fingeren sin enn å fortelle passordet sitt til en annen.

Personopplysningsloven § 12 fastsetter to vilkår som må være oppfylt for å bruke entydige identifiseringsmidler. Det må for det første være *saklig behov* for sikker identifisering, og metoden må videre være *nødvendig* for å oppnå sikker identifisering. Det er ikke gitt noen klare retningslinjer for bruken av disse skjønnsvilkårene, og det er lite rettspraksis på området. Personvernemnda har heller ikke lagt noen klare føringer i de sakene den har behandlet.

I utlendingsforvaltningen er det krav om at identiteten til utlendinger som oppholder seg i Norge, skal være kjent. Biometriske teknikker er tatt i bruk i den norske utlendingsforvaltningen etter en nøye vurdering av personvernet. Både det norske regelverket og Schengen-regelverket angir konkrete formål for bruk av biometri knyttet til de ulike sakstypene. Videre fastsettes det vilkår for lagring, og for verifisering og identitetssøk.

2.4 Informasjonssikkerhet

Argumentene for og imot å ta i bruk biometri er mange, og til dels blir de samme argumentene brukt av både entusiastene og skeptikerne. Samtidig som biometriske teknikker er positivt for informasjonssikkerheten, bør det stilles strenge krav til løsninger for lagring av biometriske opplysninger nettopp av hensyn til informasjonssikkerheten. Dette er fordi opplysningene betraktes som en spesiell form for data idet de er hentet fra menneskekroppen og dermed er uforanderlige.¹⁸

Biometriske løsninger gir entydig identifisering av en person. Dette gir

- en effektiv og brukervennlig identifisering. En begrunnelse for å ta i bruk biometriske løsninger er bekvemmelighet. Med biometrisk bruker-ID kan vi glemme passord og PIN-koder.
- økt sikkerhet. Biometri gir økt sikkerhet fordi biometriske identifikatorer er betydelig vanskeligere å stjele eller forfalske enn mer tradisjonelle identifikatorer som passord, PIN-koder og smartkort. Når biometri benyttes som en sikkerhetsforanstaltning i identitetsbevis, vil beviset være ubrukelig for den som stjeler det. Tyven kan ikke fremvise de samme biometriske kjennetegnene som er lagret i identitetsbeviset.
- økt kontroll med hvem som gjør hva. Biometri vil forhindre bruk av doble eller falske identiteter og være et tiltak mot identitetstyveri.

2.5 Personvernimplikasjonene knyttet til biometriske løsninger

Hensynet til personvernet skal vurderes i all behandling av personopplysninger. Biometri er som nevnt å betrakte som personopplysninger, og nedenfor tar vi for oss personvernimplikasjonene som har blitt diskutert i forbindelse med lagring av biometri:

- Overskuddsinformasjon: Biometrien kan være bærer av annen informasjon enn det rent

17. Se merknad til § 12 i Ot.prp. nr. 92 (1998–1999).

18. Dette er uttalt blant annet i anbefalingene om praktisering av prinsipper for personvern i «Convention for the Protection of Individuals with regard to automatic processing of personal data». Rådgivende komite Europarådet, utferdiget av rådets konsultative komite.

identifiserende. Spesielt betenkelig er det når overskuddsinformasjonen avslører sensitive personopplysninger. Biometrisk avlesning av øynene, ansiktet eller benbygningen kan for eksempel si noe om helse og etnisk bakgrunn.

- Sekundærbruk:¹⁹ Sekundærbruk som innebærer at det opprinnelige formålet med å skaffe de biometriske dataene blir utvidet til å favne andre formål enn det som var tenkt. Slik sekundærbruk kan forekomme uten at personen vet eller har samtykket til det.
- «Spoofing»: Biometriske systemer kan lures ved at biometriske kjennetegn kan kopieres og brukes til å lage gjenstander (for eksempel av fabrikkerte fingeravtrykk) som vil lure biometriske systemer. Denne typen misbruk kan motarbeides ved hjelp av gode rutiner, eller dypskannere eller liveness detection.²⁰
- Misbruk: Hvis datasikkerheten er dårlig, kan hackere eller utro tjenere lure til seg de biometriske datafilene.

Informasjonssikkerhet knyttet til lagring av biometri har fått stor oppmerksomhet. Det er derfor viktig å spørre hvorfor lagring av biometriske opplysninger stiller høyere krav til datasikkerhet enn lagring

av andre personopplysninger. Det finnes mengder av sensitive personopplysninger som lagres i databaser i dag, der sikkerhetsbrudd kan sies å innebære en vel så stor personvernrisiko. Det kan for eksempel dreie seg om spredning av helseopplysninger som kan fremkomme i utlendingssaker, og som lagres i Utlendingsdatabasen (UDB). De mest brukte biometriske karakteristika har vært fingeravtrykk og ansikt som er lett tilgjengelige ellers. Vi etterlater oss biometriske spor som fingeravtrykk, foto og DNA i en rekke sammenhenger og på ulike steder.²¹ De som har kriminelle hensikter, kan lett skaffe informasjon uten å gå veien om å bryte seg inn i systemer, noe som krever avansert teknisk kunnskap.

Når det gjelder personvernimplikasjonene knyttet til biometriske løsninger, er debatten i Vesten ofte rettet inn mot biometri som et middel for å frata borgerne rettigheter, slik som retten til personvern og fri bevegelse. India har verdens største biometriske database for nasjonale identitetskort der mer enn 200 millioner personer er registrert med fingeravtrykk. I den indiske konteksten er biometri koblet opp mot gjennomføringen av en nasjonal folketelling, og debatten synes å ha en mer positiv tone enn i Vesten: Biometri kan bidra til å gi rettigheter, for eksempel til analfabeter

og store mengder av uregistrerte personer. Borgerne må synliggjøres for staten for at den skal kunne gi rettigheter og fordele goder.²²

Den som er dataansvarlig for et biometrisk system, har ansvar for å implementere tekniske og organisatoriske tiltak på et sikkerhetsnivå som er tilpasset den risikoen som er knyttet til prosessering av ulike typer data.²³ Organisatoriske tiltak kan komme til kort, og for å redusere personvernrisikoen blir det stilt høye krav til tekniske sikkerhetsmekanismer når biometriske teknikker skal tas i bruk. Samtidig kan presset for å ta i bruk biometri bli forsterket etter hvert som det utvikler seg sikkerhetsmekanismer som hindrer uautoriserte tilgang på biometriske data.

Kryptering og bruk av digitale signaturer er sikkerhetsmekanismer som er tatt i bruk, blant annet på biometriområdet. Dette er mekanismer som skal ivareta konfidensialitet (kan ikke leses), autentisitet (kommer fra rette vedkommende) og integritet (er ikke endret). Bruk av digitalt sertifikat er en mekanisme for å sikre at krypteringsnøkler kommer fra rette vedkommende, og en PKI²⁴-infrastruktur støtter bruken av slike digitale sertifikater.

19. Ofte kalt function creep eller mission creep.

20. Målet er å oppdage om biometriske data er avgitt av en levende fysisk person.

21. For eksempel benytter Facebook ansiktsgjenkjenning for bilder, Bunnpris benytter fingeravtrykk for unge ølkjøpere, og treningssentre benytter fingeravtrykk i stedet for adgangskort.

22. Rommetveit 2011.

23. Artikkel 17 i EUs personverndirektiv.

24. PKI står for Public Key Infrastructure og er et system for identifisering, signering samt kryptering og sikkerhet innen elektronisk kommunikasjon.

3 Biometriske systemer i utlendingsforvaltningen

I utlendingsforvaltningen er det foto og fingeravtrykk som er de biometriske dataene som blir benyttet. Grunnlaget for innsamling er utlendingsloven § 100 som gir adgang til å ta fotografi og fingeravtrykk av en utlending som søker opphold, reiser inn eller oppholder seg i Norge. Bestemmelser om overføring og lagring av biometriske data til nasjonale databaser eller Schengen-sentraliserte databaser åpner i neste omgang for å bruke biometriske teknikker til å verifisere identitet og identifisering. Det er også innført oppholdskort med biometri for tredjelandborgere som innvilges oppholdstillatelse i Norge.

Under presenterer vi de viktigste biometriske systemene som er i bruk i norsk utlendingsforvaltning i dag. Samtidig går vi gjennom reglene for opptak, lagring og søk.

3.1 Utlendingsdatabasen – UDB

Utlendingsdatabasen (UDB) er en database for alle saker som er behandlet etter statsborgerskap-, eller utlendingsloven som for eksempel søknad om visum, opphold, statsborgerskap og beskyttelse i Norge. Det lagres også et ansiktsfoto av søker. Dataene som lagres er hovedsakelig hentet fra søknadsskjemaet, søknadsdokumentene, vedtaksdata samt informasjon som søker oppgir under et eventuelt intervju.

I tillegg inneholder databasen informasjon om utlendinger som

oppholder seg i asylmottak.²⁵

Databasen ble tatt i bruk i 2003.

Utlendingsdirektoratet (UDI) er eier av systemet og deres Avdeling for elektronisk forvaltning er systemansvarlig for UDB.²⁶

Brukere av Utlendingsdatabasen – UDB

Følgende saksbehandlingssystemer kommuniserer med UDB:

Tabell 1:

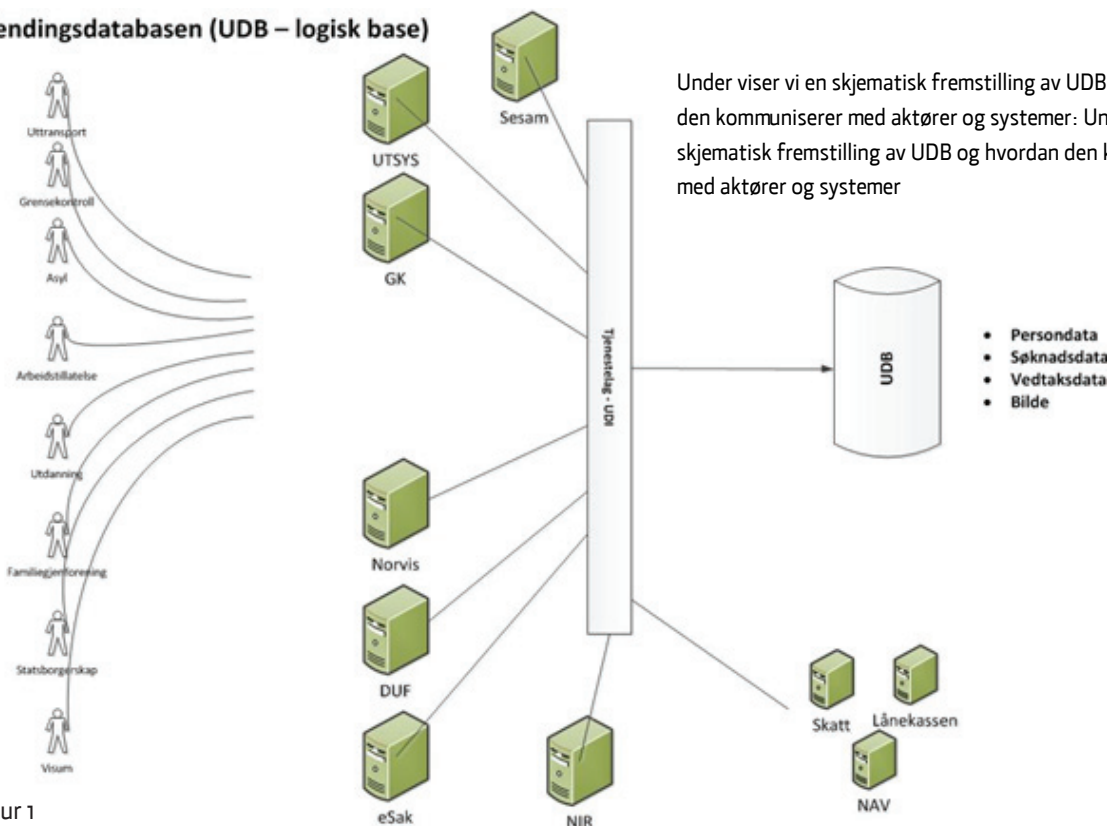
Saksbehandlingssystem	Brukere
DUF (Datasytemet for utlendings- og flyktningssaker)	UDI, UNE, politiet
Norvis (Norsk visumdatabase)	UDI, UD v/ utenriksstasjonene, (i fremtiden: politidistriktene og PU)
UTSYS (System for registrering av asylsøkere, samt uttransportering)	PU
GK (Grensekontrollapplikasjonen)	Politidistriktene
eSak (saksbehandlingssystem for elektronisk arkiv og saksbehandling)	UDI, UNE, politidistriktene, UD v/ utenriksstasjonene
SESAM («System for Elektronisk Samhandling med Asylmottakene»)	UDI og asylmottakene
NIR (Nasjonalt introduksjonsregister)	IMDi (Integrerings- og mangfoldsdirektoratet)

I tillegg foregår det noe kommunikasjon med eksterne aktører som Skatteetaten, Statens lånekasse og NAV.

25.Økonomiske ytelser, etc.

26.Utlendingsdirektoratets internmelding IM 2012-020

Utlendingsdatabasen (UDB – logisk base)



Figur 1

3.2 Utlendingsregisteret

Fingeravtrykk som opptas i forbindelse med behandling av saker om beskyttelse og utvisning, og enkelte bortvisningssaker, lagres i utlendingsregisteret.²⁷ Utlendingsregisteret er en separat fil i det alminnelige fingeravtrykksregisteret hos Kripos. Politiet benytter portalen Biometra²⁸ for å oppta og lagre fingeravtrykk i utlendingsregisteret. Formålet er å «undersøke om utlendingen allerede er registrert under samme eller annen identitet».²⁹

Biometra er en portal som politiet bruker til å oppta signalement,

personfoto og fingeravtrykk for videresendelse til Kripos via politinettet.

I Norge er følgende instanser brukere av Biometra (i utlendingsforvaltningen):

- Politiets utlendingsenhet (PU) under asylregistreringen
- politidistriktene ved ID-tvil i kontroll på territoriet
- politidistriktene ved ID-tvil i andrelinje grensekontroll

Eieren av utlendingsregisteret

Utlendingsdirektoratet er behandlingsansvarlig for utlendingsregisteret, og Kripos er databehandler.³⁰ Følgende

instanser er brukere av utlendingsregisteret:

- Politiets utlendingsenhet (PU)
- politidistriktene (grensekontroll / «GK»³¹)
- politidistriktene (kontroll på territoriet)

Fingeravtrykkene tas opp av politiet og sendes elektronisk til Kripos, som foretar søket i utlendingsregisteret. Hjemmelen for søket skal angis, og avtrykkene skal merkes med et eget referansenummer.³²

Infrastrukturen er bygd opp slik at all kommunikasjon til og fra utlendingsregisteret går via Kripos.

27. Jf. utlendingsforskriften § 18-1.

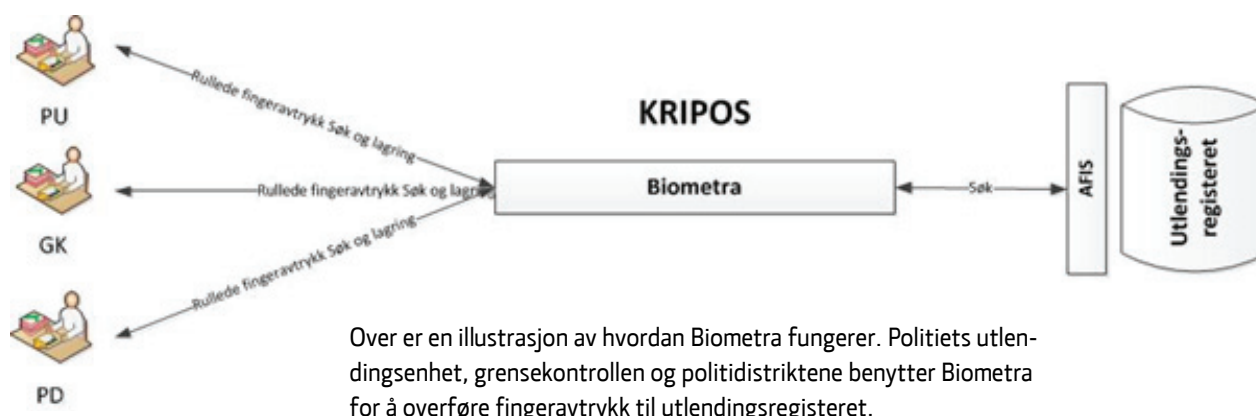
28. Biometra er en portal som politiet bruker til å oppta signalement, personfoto og fingeravtrykk som skal videresendes til Kripos via politinettet.

29. Utlendingsforskriften § 18-3, første ledd bokstav a.

30. Utlendingsforskriften § 18-2, fjerde ledd.

31. I GK registreres reisemåte, type transportmiddel og varighet av oppholdet ved innreise. Les mer om «Grensekontrollsystemet – GK» i punkt 3.4.

32. Utlendingsforskriften § 18-2, tredje ledd.



Figur 2

Opptak, lagring og søk i utlendingsregisteret

Mens utlendingsloven § 100 gir regler om når det *kan* tas fingeravtrykk og foto av utlendinger, fastsetter utlendingsforskriften § 18-1 når det rutinemessig *skal* tas fingeravtrykk.³³ Fingeravtrykkene blir lagret i utlendingsregisteret. Når fingeravtrykkene blir lagret, blir det gjennomført søk i tidligere lagrede fingeravtrykk. Fingeravtrykkene kan også oversendes til andre lands myndigheter for søk dersom det er grunn til å tro at utlendingen har søkt opphold der.³⁴ På samme måte kan fingeravtrykk mottatt fra utlandet benyttes til søk i utlendingsregisteret i Norge.³⁵

Når det skal tas fingeravtrykk etter utlendingsforskriften § 18-1, skal det også søkes i det alminnelige fingeravtrykkregisteret (der avtrykkene til de som er strafferegistrerte, er

lagret). Formålet er å undersøke om utlendinger er ettersøkt i Norge eller et annet land.

I forbindelse med kriminaletterforskningen kan politiet også søke i utlendingsregisteret, men dette gjelder bare i forbindelse med etterforskningen av én eller flere handlinger som samlet kan medføre høyere straff enn fengsel i seks måneder.³⁶

Sletting fra utlendingsregisteret

Dersom det ikke foreligger tvil om utlendingens identitet, skal fingeravtrykkene slettes fra utlendingsregisteret når vedkommende har fått innvilget en oppholdstillatelse som kan danne grunnlag for permanent oppholdstillatelse. Dersom det er tvil om utlendingens identitet, skal fingeravtrykkene beholdes inntil utlendingen innvilges permanent oppholdstillatelse / varig oppholds-

rett, eller inntil det ikke lenger er tvil om utlendingens identitet.³⁷

Dersom utlendingen ikke kan fremlegge dokumentasjon med nødvendig notoritet på identiteten sin, slettes fingeravtrykkene først når utlendingen får statsborgerskap i Norge eller et annet medlemsland i Eurodac-samarbeidet (se neste side).³⁸

Dersom utlendingen får avslag, slettes fingeravtrykkene etter fem år forutsatt at vedtaket er iverksatt.³⁹ Dette gjelder også hvis det er tatt fingeravtrykk i forbindelse med en sak om bortvisning eller utvisning. Fingeravtrykkene kan slettes før hvis utlendingen blir innvilget statsborgerskap i et annet land som deltar i Eurodac-samarbeidet.

33. Foruten personalia lagres ansiktsfoto og ti rullede fingeravtrykk av følgende, jf. utlendingsforskriften § 18-1 annet ledd: a) utlending som ikke kan dokumentere sin identitet, eller det er grunn til å mistenke at utlendingen oppgir falsk identitet; b) utlending som søker om beskyttelse etter loven; c) utlending over 18 år som søker oppholdstillatelse etter lovens kapittel 6 (familieinnvandring) som familiemedlem til en utlending som har søkt om beskyttelse; d) utlending som nevnt under bokstav b eller c som har fått avslag på sin søknad, når fingeravtrykk ikke er tatt tidligere; e) utlending som blir utvist; f) utlending som blir bortvist etter å ha blitt ilagt straff eller gitt påtaleunnlattelse; g) utlending som har oppholdt seg ulovlig i Norge.

34. Utlendingsforskriften § 18-2, tredje ledd.

35. Utlendingsforskriften § 18-3, tredje ledd.

36. Utlendingsloven § 100, andre ledd.

37. Utlendingsforskriften § 18-4, første ledd.

38. Ibid.

39. Jf. utlendingsforskriften § 18-4.

3.3 Eurodac

Eurodac ble introdusert for å lette identifiseringsarbeidet etter Dublin-regelverket.⁴⁰ Eurodac-forordningen sier følgende:

*A system known as 'Eurodac' is hereby established, the purpose of which shall be to assist in determining which Member State is to be responsible pursuant to the Dublin Convention for examining an application for asylum lodged in a Member State, and otherwise to facilitate the application of the Dublin Convention under the conditions set out in this Regulation.*⁴¹

Med Eurodac ble fingeravtrykk valgt som identifikasjonsmiddel.⁴² Norges forpliktelser til å overføre fingeravtrykk til Eurodac er regulert i utlendingsforskriften § 18-5, jf. utlendingsloven § 101.

Utlendinger som må avgi fingeravtrykk for overføring til Eurodac, omfatter personer over 14 år som søker beskyttelse, og personer over 14 år som krysser Schengen-grensen ulovlig (og ikke blir bortvist). Vi har illustrert adgangen til å bruke Eurodac og andre systemer til verifisering og identifisering i vedlegg nr. 1, tabell nr. 2.

Systembeskrivelse

Eurodac er en stor database for lagring, søk og sammenlikning av fingeravtrykk av asylsøkere, samt ulovlige immigranter i medlemslandene.

Systemet består av en sentral enhet og en «back-up» enhet. Begge databasene ligger i EU-kommisjonens lokaler i Luxemburg, men er driftet fra Tallin. I tillegg til den sentrale delen, finnes et system for elektronisk dataoverføring mellom databasen og medlemslandene. Sistnevnte har dessuten utviklet egne, nasjonale systemer for kommunikasjon med Eurodac via et kryptert nettverk.⁴³

Hvert medlemsland har nasjonale aksesspunkter som all kommunikasjon med Eurodac går gjennom. I Norge ligger dette aksesspunktet hos Kripos som også er databehandler. Utlendingsdirektoratet er behandlingsansvarlig i Norge.

Kripos kvalitetssikrer også fingeravtrykkstreffene som returneres fra Eurodac.

Data som lagres i Eurodac

Som forklart tidligere må utlendinger over 14 år som søker beskyttelse, og personer over 14 år som krysser Schengen-grensen ulovlig (og ikke blir bortvist), avgi fingeravtrykk for overføring til Eurodac.

Følgende data overføres til Eurodac:

- ti rullede fingeravtrykk
- avsenderlandet (landet som overfører dataene til databasen)
- søkerens kjønn
- sted og dato for asylsøknaden

da den ble fremmet, eller der utlendingen ble anholdt av politiet

- referansenummer
- dato for opptak av fingeravtrykk
- dato for overføring av disse dataene til databasen

Eurodac benytter rullede fingeravtrykk. Enkelte land, blant annet Sverige, har ytret ønske om å gå over til flate fingeravtrykk også i Eurodac. Dette krever en større tilpasning i Eurodac, men vil bli vurdert i fremtiden.

Grunnlag for søk i Eurodac

Det foretas bare identifiseringssøk i Eurodac og ikke verifisering, fordi hensikten er å finne ut om personen tidligere er kjent i et annet medlemsland. Politiet som utlendingsmyndighet foretar søk mot Eurodac via Biometra i følgende tilfeller:

- for å identifisere hvilket land som er ansvarlig for å behandle asylsøknaden
- ved forsøk på å fastsette identiteten til en utlending som søker beskyttelse
- ved forsøk på å fastsette identiteten til en utlending ved en irregulær grensepassering
- ved forsøk på å fastsette identiteten til en utlending ved kontroll på territoriet (ved ulovlig opphold)

Ved kontroll på territoriet kan

40. Dublin-samarbeidet går ut på at en asylsøknad bare skal behandles i ett av de 29 medlemslandene. Dublin-samarbeidet består av EU-landene, samt Norge, Sveits og Island. EUs rådsforordning nr. 343/2003/ (Dublin-forordningen)

41. Jf. Eurodac-forordningen artikkel 1.

42. I forordet i Eurodac-forordningen står det: «Fingerprints constitute an important element in establishing the exact identity of such persons. It is necessary to set up a system for the comparison of their fingerprint data. To this end, it is necessary to set up a system known as 'Eurodac'».

43. European Data Protection Supervisor, Inspection of Eurodac Central Unit Summary Report 13 June 2012: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/12-06-13_EURODAC_Inspection_EN.pdf

politiet bare foreta søk. Fingeravtrykkene skal ikke lagres. Søket kalles «hurtigsøk» og gjøres ved opptak av fire fingre (begge tomlene og begge pekefingrene). Det er ikke anledning til å utføre hurtigsøk ved asylregistrering eller ved ulovlig grensepassering.

Det kan foretas hurtigsøk i følgende tilfeller:

- hvis utlendingen opplyser at han/hun har søkt beskyttelse, men ikke til hvilket land
- hvis utlendingen ikke søker beskyttelse, men motsetter seg retur til hjemlandet fordi han/hun mener han/hun er i fare der
- hvis utlendingen forhindrer retur til hjemlandet fordi han/hun ikke samarbeider med å kartlegge identiteten, spesielt dersom utlendingen har fremvist falske identitetspapirer⁴⁴

Hver gang politiet gjør søk eller overfører data til Eurodac, skal dette registreres i DUF.⁴⁵ Det skal også registreres hjemmel for søket eller lagringen.

Sletting av data i Eurodac

Utlendingsforskriftens § 18-6 regulerer lagring og sletting i Eurodac. Data i Eurodac slettes etter ti år for asylsøkere eller når utlendingen får statsborgerskap fra et av medlemslandene.⁴⁶ Data om utlendinger som blir registrert i forbindelse med irregulære grensepasseringer, slettes etter to år fra den datoen fingeravtrykkene ble

tatt opp. Slettingen skjer umiddelbart hvis utlendingen får oppholdstillatelse eller statsborgerskap i et av medlemslandene, eller hvis vedkommende forlater Schengen-området og EU.

Ved kontroll på territoriet skal dataene som nevnt ovenfor slettes umiddelbart etter at sammenligningen av fingeravtrykkene er utført.

3.4 Visa Information System – VIS

Med innføringen av VIS ble det opprettet en ny sentral Schengen-basert fingeravtrykksdatabase. VIS er et Schengen-basert system der medlemslandene registrerer alle søknader om Schengen-visum (C-visum.)

Hensikten med VIS er å lette implementeringen av en felles visum-praksis i Schengen-området, bedre det konsulære samarbeidet og forenkle konsultasjoner mellom medlemsstatene. Databasen inneholder biometriske fingeravtrykksdata til samtlige tredjelandsborgere som søker visum til Schengen-området, og dessuten personalia og informasjon om vedtak og utstedelse. Overføring av fingeravtrykksdata til VIS er formålsbestemt i utlendingsloven § 102a (som er en gjengivelse av formålene slik de er spesifisert i VIS-forordningen, artikkel 2):

- a) forenkle visumsøknadsprosedyrene,
- b) unngå omgåelse av kriteriene som ligger til grunn for avgjørelsen av hvilken medlemsstat som er ansvarlig for å behandle søknaden,
- c) forenkle bekjempelsen av forfalskning,
- d) lette kontrollen ved medlemsstatenes yttergrenser og innenfor medlemsstatenes område,
- e) forenkle identifikasjonen av personer som ikke fyller vilkårene for innreise eller opphold på medlemsstatens territorium,
- f) lette anvendelsen av Dublin II-forordningen om fastsettelse av kriterier og prosedyrer for avgjørelse av hvilken medlemsstat som er ansvarlig for behandlingen av en asylsøknad fremsatt av en tredjelandsborger i en av medlemsstatene, og
- g) bidra til å avverge trusler mot den enkelte medlemsstats indre sikkerhet⁴⁷

Søkeadgangen i VIS blir omtalt i utlendingsloven § 102 c og e.

VIS-forordningens kapittel 3 angir nærmere den søkeadgangen som grensekontrollen og politimyndighetene har ved utlendingskontroll på grensen og på territoriet.⁴⁸

I spesielle tilfeller kan nasjonale myndigheter og Europol, etter strenge rutiner og via det sentrale aksesspunktet i hvert medlemsland, be om data fra VIS for å forhindre, oppdage og etterforske terrorisme og alvorlig kriminalitet.⁴⁹ Medlemslandene kan også innhente anonymisert statistikk fra VIS-basen.

44. UDI RS 2010-019 «Gjennomførende rutiner i tilknytningen til Eurodac-forordningen».

45. Datasystem for utlendings- og flyktningsaker. Utlendingsforvaltningen benytter DUF i saksbehandlingen. DUF ble tatt i bruk i 2003.

46. Det er Kripos som sletter dataene etter instruks fra Utlendingsdirektoratet når tidsperioden for lagring utløper.

47. Utlendingsloven § 102a.

48. Forordningen som følger som vedlegg til utlendingsforskriften § 3-4. Den angir også den søkeadgangen utlendingsmyndighetene har ved fastsettelse av ansvaret for, og behandlingen av, en søknad om beskyttelse.

49. Rådsbeslutning 2008/663/JHA, samt VIS Regulations, article 3, section 1 and 2, 2008.

Systembeskrivelse

Utrulling av VIS startet 11. november 2011 i Nord-Afrika og foregår regionsvis over en periode på to til tre år. VIS består av en sentral database og medlemslandenes nasjonale systemer som kommuniserer med den sentrale databasen.

Fra oppstart av VIS skal alle visumpliktige som passerer Schengens yttergrense, verifiseres mot VIS-basen. Verifisering skal gjøres ved hjelp av to til fire fingeravtrykk, men i en overgangsperiode på tre år fra oppstartdato kan grensekontrollen velge kun å verifisere mot VIS-databasen med visumetikettnummeret. Norge har foreløpig bare denne løsningen.

Den sentrale VIS-databasen ligger i Strasbourg i Frankrike. I tillegg finnes det en parallellbase i St. Anton i Østerrike. Basen i St. Anton oppdateres kontinuerlig og tar over automatisk dersom basen i Strasbourg ikke er tilgjengelig.

VIS har, i motsetning til Eurodac og utlendingsregisteret, et moderne, hel-automatisk biometrisk matchesystem⁵⁰ for fingeravtrykk som ikke krever kunnskap om fingeravtrykk fra den som behandler søket.

EU-kommisjonen eier VIS

Samtlige medlemsland har vært med på å betale utviklingen av det sentrale systemet. På samme måte deles kostnadene for drift og vedlikehold. Den juridiske eieren av systemet er EU-kommisjonen. Medlemslandene

er interessenter. Basen driftes av EU-kommisjonen.⁵¹

I tillegg har alle de ulike medlemslandene utviklet nasjonale systemer som kommuniserer med den sentrale databasen. I Norge gjøres dette med Norvis-applikasjonen og Grensekontrollapplikasjonen (GK). Applikasjonene kommuniserer mot VIS-basen gjennom Utlendingsdirektoratets sentrale system og gjennom Schengens lukkede nettverk. Politiets utlendingsenhet og politidistriktene benytter en tilpasset versjon av Norvis. Bruken reguleres ved tilgangsstyring etter hjemlet, tjenstlig behov.

Norvis

Norvis eies og forvaltes av Utlendingsdirektoratet. Følgende instanser i Norge og utlandet er brukere av Norvis:

- Utenriksdepartementet (behandling av visumsøknader ved utenriksstasjonene)
- Utlendingsdirektoratet (behandling av visumsøknader ved visumenheten)
- Politiets utlendingsenhet (søk i VIS ved registrering av asylsøkere)
- politidistriktene (grensekontroll andrelinje og innlandskontroll)

Den største brukeren av Norvis er utenriksstasjonene, som innvilget om lag 140 000 visumsøknader til Norge i 2011.⁵² I tillegg registreres alle søknader om oppholdstillatelse som mottas ved utenriksstasjonene, i Norvis. Dataene lagres i Utlendingsdatabasen (UDB).⁵³ Med unntak

av fingeravtrykk lagres den samme informasjonen om visumsøkerne i UDB som i VIS. I tillegg lagres tilleggsinformasjon om søkeren og referansepersonen i UDB som ikke lagres i VIS. Informasjon om oppholdssøknader lagres derimot bare i UDB, ikke i VIS.

Grensekontrollsystemet – GK

GK er grensekontrollens saksbehandlingsverktøy. Et av hovedformålene med GK var å gi grensekontrollen ett system å forholde seg til i stedet for å måtte gjøre oppslag i flere ulike systemer.

GK har følgende funksjonalitet:

- skanning av pass, inkludert avlesing av maskinlesbare felter (MRZ) og RFID-brikken i dokumentet
- kontroll av visum mot UDB
- søk mot ELYS (nasjonale etterlysninger) og SIS II (etterlysninger i Schengen)
- melding om treff i søk, informasjon om gyldig/ugyldig reisedokument
- registrering av inn- og utreiseopplysninger for visumpliktige
- verifisering mot VIS, verifiseringen foretas med to fingre i Norge (grensekontrollen registrerer ingen informasjon i VIS)

I GK registreres reisemåte, type transportmiddel og varighet av oppholdet ved innreise. Systemet utfører automatiske søk mot UDB, ELYS og (N-)SIS. For at søket i GK skal fungere, må den som bruker GK, også være registrert som bruker

50. BMS/AFIS.

51. I Brussel frem til 31.11.12 og EUs nyetablerte IT-byrå i Tallin fra og med 01.12.12.

52. Utlendingsdirektoratets statistikk fra årsrapporten for 2011: <http://www.udi.no/arsrapport2011/Statistikk/>

53. Utlendingsdirektoratet behandler oppholdssøknadene i saksbehandlerverketøyet DUF og sender vedtak elektronisk gjennom eSak til den effektuerende myndighet (utenriksstasjonene eller politiet), som skriver ut avslagsbrev eller visumetikett fra Norvis/DUF.

i de systemene det søkes i.⁵⁴ Det er ingen registrering av biometri i GK.

Ved utreise registreres bare utreisedato i GK.

Bruk av VIS

Foruten lagring av data kan det foretas to typer operasjoner i VIS: identifisering (én-til-én-søk) og verifisering (én-til-mange-søk).

Identifisering

Når en søknad om et Schengen-visum fremmes ved en utenriksstasjon, skal det normalt opptas ti fingeravtrykk av søkeren over tolv år og gjøres et identifiseringssøk i VIS-databasen for å se om søkeren er registrert i basen fra før. Søket vil ta opptil tretti minutter når alle medlemslandene har kommet i normal drift over hele verden.

Dersom det ikke er mulig å ta opp fingeravtrykk,⁵⁵ skal den myndigheten som utsteder visum, foreta et alfanumerisk søk i VIS-databasen.

Dersom søkeren mangler én eller flere fingre, eller noen av fingeravtrykkene er av så dårlig kvalitet at de ikke kan brukes, skal dette registreres i Norvis på søknadstidspunktet, slik at både identifisering og verifisering kan gjøres mot de fingeravtrykkene som er av brukbar kvalitet.⁵⁶

Å foreta korrekte søk er av stor

betydning for å unngå dobbelt-registreringer og aliasføringer i systemene. Dette kan føre til at en person som har misbrukt et visum,⁵⁷ kan få nytt visum på en ny identitet i saksbehandlingssystemet.

Politiets utlendingsenhet har hjemmel for å utføre identifiseringssøk mot VIS ved asylregistreringen. Det samme har politidistriktene ved kontroll på territoriet og i grensekontrollen dersom det er identitetstvil.

Ved førstegangssøknad opprettes (automatisk) et dossier på søkeren i VIS. Ved senere søknader skal den nye søknaden linkes med tidligere søknader, uavhengig av hvilket medlemsland som har behandlet den tidligere søknaden.⁵⁸

Verifisering

Verifisering er en én-til-én-matching. Ved innreise i Schengen-området skal grensekontrollen verifisere at den reisende er rette innehaver av visumet. Dette gjøres ved å ta opp to til fire fingeravtrykk⁵⁹ og, sammen med visumetikettnummeret, verifisere dette mot VIS-databasen. Verifiseringen utføres på noen få sekunder. Dersom det er treff i VIS, får grensekontrollen mulighet til å se visse data i søknadsmappen til den reisende. Dersom grensekontrollen ikke får treff på verifisering mot VIS, kan den foreta et identifiseringssøk i andrelinjen. Det samme gjelder

kontroll på territoriet i politidistriktene.

I en overgangsperiode på tre år fra VIS' oppstartdato, altså frem til november 2014 kan grensekontrollen velge å verifisere et visum kun med visumetikettnummeret.

Hva lagres i VIS?

I VIS lagres følgende informasjon:

- alfanumeriske data om søkeren (data fra søknadsskjemaet og reisedokumentet)
- alfanumeriske data om visumet (antall dager, antall innreiser, tidsrom, etc.) som
 - det er søkt om
 - er utstedt
 - er avslått
 - er annullert
 - er tilbakekalt
 - er forlenget
- fotografi
- ti fingeravtrykk⁶⁰
- informasjon om linkede søknader

En søknad lagres i VIS i fem år. Den myndigheten som utsteder visumet, er ansvarlig for å slette søknaden. Alle søknadene skal slettes dersom søkeren blir statsborger av et medlemsland. Det medlemslandet som gir personen statsborgerskap, har ansvar for å underrette de andre landene, slik at de kan slette personens andre søknader i VIS.

54. For eksempel må man være DUF-bruker for å søke i UDB.

55. For eksempel VIPs eller personer med skadede eller manglende hender.

56. Juridisk sett kan man i et identifiseringssøk også søke på fornavn, etternavn, tidligere etternavn, kjønn, fødselsdato, fødested, fødeland, type og nummer på reisedokument, utstedende myndighet, utstedelsesdato, utløpsdato, nåværende nasjonalitet og nasjonalitet ved fødsel.

57. Ved for eksempel ikke å ha returnert når han skulle.

58. Tidlig bruk av VIS viser at ikke alle medlemslandene alltid linker søknader, noe som øker sjansen for at personer kan slippe gjennom med en ny identitet i systemet.

59. Medlemslandene kan selv bestemme hvor mange fingre de ønsker å bruke til dette formålet.

60. Det lagres færre fingeravtrykk dersom søkeren ikke har ti fingre, eller dersom avtrykkene er av så dårlig kvalitet at de ikke har noen verdi.

Schengen-regelverket åpner for at medlemslandene kan lagre en kopi av fingeravtrykkene de selv tar opp i visumsaker, i en nasjonal database. Norge gjør foreløpig ikke dette, på grunn av manglende hjemmel i vårt nasjonale regelverk. Schengen-regelverket gir imidlertid ikke tilgang til å hente fingeravtrykk fra den sentrale databasen og kopiere over i egen database.

Tilgang til VIS

Det er bare autorisert personale som kan få tilgang til VIS. Det er stasjonssjefen som avgjør hvem som autoriseres på en utenriksstasjon. Det vil si at også tredjelandsborgere i teorien kan falle inn under kategorien «autorisert personale» i VIS-sammenheng.⁶¹ I Utlendingsdirektoratet har de ansatte i visumenheten tilgang til Norvis, mens politiet selv administrerer sine brukere.

3.5 Schengen-standardiserte oppholdskort

Norge innførte Schengen-standardiserte oppholdskort i 2012. Oppholdskortet inneholder biometri i form av fingeravtrykk og ansiktsfoto. Oppholdskortet utstedes til tredjelandsborgere som får innvilget en oppholdstillatelse.

Regler for opptak og lagring

Innhenting og lagring av biometrisk personinformasjon i oppholds-kortene er regulert i utlendingsloven § 100a, mens § 100b gir hjemmel for å innhente biometrisk personinformasjon

til kontroll og sammenligning med biometrien som finnes i oppholdskortet. § 100b gir også anledning til i en kontrollsituasjon å innhente ansiktsfoto og fingeravtrykk ved tvang. Dersom utlendingen ikke medvirker til dette, kan det være grunnlag for en straffereaksjon.⁶²

Oppholdskortet er ikke et identitetskort. Formålet med oppholdskortet er å gjøre det mulig å verifisere opplysningene om oppholdsstatus. Med biometri er det etablert en mer pålitelig kobling mellom innehaveren av kortet og oppholdstillatelsen. Biometrisk data som er innhentet ved bestilling av kortet skal slettes så snart oppholdskortet er produsert. Tilsvarende skal opptak av biometri som tas i en kontrollsituasjon slettes straks verifisering er gjennomført. Schengenregelverket om opptak av biometri for lagring i oppholdskort berører ikke spørsmål om sentral lagring på nasjonalt nivå.

Teknisk beskrivelse av oppholdskortet

Oppholdskortet er et plastkort i kredittkortstørrelse som er basert på krav satt av EU og ICAO.⁶³ På kortets overflate er det et lasergravert bilde av søkeren, noe persondata, data om type tillatelse og hvor lenge tillatelsen er gyldig. Det meste av denne informasjonen er også tilgjengelig i en maskinlesbar sone (MRZ). Kortet har også et anmerkningsfelt for tilleggsinformasjon på for- og baksiden. Integrert i kortet ligger det en RFID-brikke med antenne. I denne brikken

lagres foruten informasjon trykt på forsiden av kortet, og bilde (image) av to flate fingeravtrykk.

Kortet har en rekke sikkerhetslementer for å hindre forfalskning både med hensyn til endring av data på kortets overflate, og for å hindre uautorisert avlesing av fingeravtrykk fra databrikken. For å beskytte mot uautorisert avlesning av fingeravtrykkene brukes det PKI-sertifikater⁶⁴ som den autoriserte kontrollmyndigheten må ha tilgang til for å kunne lese innholdet i databrikken. Det utstedes også sertifikater for å bekrefte dokumentets ekthet («trust»), det vil si som bekrefter at et bestemt land har utstedt dokumentet, og at dette landet kan bekrefte innholdet i dokumentet.

Bruk av oppholdskortet

Oppholdskortet er et bevis på at innehaveren har en gyldig oppholdstillatelse. Ved innreise inn i Schengenområdet og ved kontroll innenlands må eieren kunne fremlegge kortet. Tredjelandsborgere må ha et pass i tillegg. Reisedokumentet, derimot, er et dokument som gir personen mulighet til å reise utenlands.

For å kontrollere at oppholdskortet eller reisedokumentet er ekte, og at det er riktig person som fremlegger kortet, kan det tas opp fingeravtrykk av personen og sammenligne dette med fingeravtrykk som er lagret i kortet. For å gjennomføre en slik operasjon må den som kontrollerer, ha tilgang til flere typer sertifikater

61. Begrepet bør for øvrig ikke forveksles med «autorisert» og «uautorisert» bruker i Norvis, der bare Schengen-borgere kan autoriseres og fatte vedtak i en visumsak.

62. Jf. utlendingsloven § 108 annet ledd bokstav a.

63. International Civil Aviation Organization – ICAO.

64. Public Key Infrastructure – PKI. Det står mer om sertifikater side 41 under «Sikkerhetsmekanismer ved lagring av biometrisk data i oppholdskort, utlendingspass og reisebevis for flyktninger».

utstedt av norske myndigheter: én type sertifikat for å sjekke dokumentets ekthet, og en annen type sertifikat for å låse opp den delen av databrikken som inneholder fingeravtrykkene. Elektronisk avlesning av bilde og fingeravtrykk kan også brukes i forbindelse med forenklet grensekontroll og ved automatisk grensekontroll (ABC-gates⁶⁵).

Utstedelse av oppholdskort og reisedokument

Reisebevis for flyktninger og utlendingspass er internasjonale, standardiserte dokumenter for personer som av forskjellige grunner ikke kan skaffe seg nasjonale pass. Dokumentene er teknisk sett identiske med et nasjonalt pass, men har noe annet utseende og inneholder en litt annen type informasjon.

I 2005 implementerte Norge det nye nasjonale ePasset. ePasset er basert på EU-krav og ICAO 9303-standard.⁶⁶ Det har en polykarbonat personaliaside og en RFID-brikke der det blant annet lagres to flate fingeravtrykk. Norge valgte samtidig å innføre den samme standarden i reisedokumentene for utlendinger. Reisedokumentene har de samme sikkerhetselementene som oppholdskortet.

EU/Schengen-borgere som har ePass, kan benytte seg av automatisert grensekontroll (ABC-gates). Biometri lagret i passene blir da kontrollert opp mot biometri som avleses på grenseovergangsstedet for passering

av Schengens yttergrense.

Oppholdskort, utlendingspass og reisebevis utstedes etter at søkeren har fått innvilget oppholdstillatelse. Personen kalles inn til politiets førstelinje, som tar opp fingeravtrykk. Fingeravtrykkene tas opp med biometrikiosken. Prosessen styres av DUF-applikasjonen.

Når det gjelder oppholdskort, blir fingeravtrykkene som er tatt opp, samt person- og vedtaksdata fra UDB-basen, overført til en oppholdskort-modul. Denne modulen håndterer kontroll og forsendelse av data til produsenten av oppholdskortet eller reisedokumentet.

Produsenten personaliserer kortet. Dette vil si at bilde, person- og vedtaksdata printes på dokumentets overflate. I tillegg lagres person- og vedtaksdata, bilde og fingeravtrykk i RFID-brikken. Det ferdigproduserte dokumentet sendes direkte til den rette innehaveren. Deretter slettes fingeravtrykkene. De er nå bare registrert i RFID-brikken i dokumentet.

Systemeierskap og ansvarsforhold

Utlendingsdirektoratet har utviklet og er eier av systemet som tar opp og formidler data fra førstelinjen i politiet til produsenten av kortene. Politiet eier biometrikioskene som tar opp biometrien i førstelinjen. Politiets data- og materielltjeneste (PDMT) har ansvar for å utstede sertifikater (sikkerhetsmekanismene omtales nedenfor) og produsenten har

ansvaret for selve kortproduksjonen. Utlendingsdirektoratet er dataansvarlig for oppholdskortene, og politiet er databehandler.

Sikkerhetsmekanismer ved lagring av biometrisk data i oppholdskort, utlendingspass og reisebevis for flyktninger

Databrikken (RFID-brikken) i oppholdskortet, norske pass, utlendingspass og reisebevis for flyktninger har samme type sikkerhetsmekanisme. Dokumenter som inneholder data som er lagret i en databrikke, omtales ofte som ePass og eMRTD,⁶⁷ der «e» står for elektronisk lagring av data i en databrikke.

I RFID-brikken lagres stort sett den samme informasjonen som er synlig i personaliasiden i passet og på forsiden i oppholdskortet, samt fingeravtrykk. For å sikre integritet og autentisitet for dataene i databrikken benyttes det elektroniske sertifikater.

Elektroniske sertifikater produseres av landets nasjonale myndigheter og styres av en Certificate Authority (CA) som utgjør det høyeste leddet i en sertifikatkjede. I Norge er det Justis- og beredskapsdepartementet som er Certificate Authority. CA utsteder to overordnede dokumenter som forklarer hvilke reisedokumenter og oppholdskort som inngår i denne sertifikatkjeden.⁶⁸ Disse to dokumentene heter Country Signing Certificate Authority (CSCA) og Country Verifying Certificate Authority

65. Automatic Border Control

66. Biometriske pass i 2005 inneholdt bare foto. Fra 2010 ble fingeravtrykk inkludert.

67. E-Machine Readable Travel Documents.

68. Ofte kalt «chain of trust».

(CVCA). Disse betegnes ofte som rot-sertifikater.

CSCA-dokumentet beskriver hvilke reisedokumenter og oppholdskort som dekkes, og typer av underdokumenter. I Norge er det for eksempel ett felles CSCA som dekker både passene og oppholdskortene. I det samme dokumentet står det videre at under dette CSCA-dokumentet finnes det flere undertyper av reisedokumenter og oppholdskort betegnet Document Signer (DS). Her har for eksempel pass ett DS, mens oppholdskort har et annet DS. På denne måten kan et elektronisk avlesersystem, for eksempel på en grensekontroll, først lese at kortets CSCA er norsk, og at DS-typen tilsier at dette er et oppholdskort. For å kunne foreta en slik autentisering av ektheten av dokumentet avleses sertifikat-informasjonen om CVCA og DS som ligger i RFID-brikken. Dette er en «private key» som lagres ved produksjonen av dokumentet. Denne sammenlignes deretter med den informasjonen grensestasjonen har i CSCA-dokumentet som er publisert av norske myndigheter. Dette er «public key». Dersom disse to stemmer overens, er dette et ekte norsk dokument, og de vet også hvilken type dokument det er. Det finnes også mekanismer som sjekker om dataene i brikken har blitt endret.

CVCA beskriver et kontrollregime for å lese av fingeravtryksdata i databrikken. Under CVCA er det undergrupper som Document Verifier (DV) som avlesingssystemene må kjenne til for å kunne lese av dataene. Forenklet fungerer dette

på følgende måte: Informasjon om DV-sertifikatet lagres i RFID-brikken ved produksjon. Den myndigheten som skal kunne lese fingeravtrykkene i passet eller oppholdskortet, må få tilsendt et motsvarende sertifikat fra norske myndigheter. Slik utveksling av sertifikater gjøres på forespørsel og gjennom diplomatiske kanaler. Et mottatt sertifikat legges inn i landets grensekontrollsystem. Når en reisende fremlegger passet eller oppholdskortet, vil sertifikatet i RFID-brikken bli kontrollert mot sertifikatet som ligger i avlesingssystemet. Dersom disse to delene utfyller hverandre, er sikkerhetskjeden kontrollert og fingeravtryksdataene kan leses av fra RFID-brikken.

3.6 EU/Schengen Smart border system

EU/Schengen vurderer å ta i bruk biometrisk identifisering i forbindelse med EU-kommisjonens forslag om å etablere det Schengen kaller «smart border system» på grenseovergangstedene for passering over Schengens yttergrense. Det er foreslått at systemet skal bestå av to komponenter: et entry/exit-system som registrerer inn- og utreise til tredjelandborgere, og automatisert grensekontroll for bona fide-reisende (RTP, omtales nedenfor).

- **Entry/exit-systemet:**

Hovedinnholdet i forslaget om et entry/exit-system er å opprette et system for automatisk registrering av tid og sted idet visumpliktige tredjelandborgere passerer Schengens yttergrense.

Samtidig skal det være mulig å oppta biometri for sammenligning med biometrien som er lagret i VIS. Dette vil gjelde tredjelandborgere som skal oppholde seg på territoriet for en kort periode (inntil tre måneder). Hensikten er å bekjempe ulovlig opphold og sikre muligheten for å kunne identifisere og iverksette tiltak mot tredjelandborgere som ikke forlater territoriet innen utreise Fristen. For visumfrie tredjelandborgere må biometri tas opp på grenseovergangstedet. Dette krever et system for å registrere opplysningene om tid og sted for grensepassering og videre for opptak og lagring av biometri til ikke-visumpliktige tredjelandborgere. Systemet vil være basert på den samme tekniske plattformen som VIS.

- **The Registered Traveller Program (RTP):**

For lavrisikoreisende tredjelandborgere blir det foreslått en ordning, omtalt som the Registered Traveller Program (RTP), som gjør at disse kan benytte seg av automatisert grensekontroll. Lavrisikoreisende tredjelandborgere kan søke om å få forhåndsgodkjent status som registrerte reisende. Lavrisikoreisende som ikke er visumpliktige, og som derfor heller ikke vil være registrert med biometri i VIS, kan oppnå en slik status ved en frivillig forhåndsscreening der de også avgir biometri.

4 Kartlegging – politiets arbeid med opptak av biometri, lagring og søk i registre

Nasjonalt ID-senter utførte i perioden mai-juni 2012 syv intervjuer med seks ulike politidistrikter samt sårorganet Politiets utlendingsenhet. Vi stilte spørsmål rundt tre kjerneområder: bruk av biometri i politiet (praksisen), politiets utstyr for opptak, lagring og søk av fingeravtrykk og ansiktsfoto, samt regelverket for dette.

Under kartleggingen fremkom det at de ulike politidistriktene ofte meldte om samme utfordringer når det gjaldt identitetsarbeid med utlendinger. Funnene i denne kartleggingen har vi plassert i fire kategorier. Det er behov for følgende:

- kompetanse og opplæring
- bedre rutiner for bruk av biometri til verifisering og identifisering i utlendingsaker
- utstyr for å sikre bedre utnyttelse av biometri
- bedre og helhetlige systemløsninger og registerforvaltning

Når det gjelder mangelfull opplæring, fremkom det ønsker og behov om mer opplæring i både taktisk og teknisk identitetskontroll, inkludert opplæring i bruk av kontrollutstyr. Videre ble det påvist at kunnskapen om hjemmelsgrunnlaget for opptak av biometri (foto og fingeravtrykk) i forvaltningssaker ikke alltid var til stede, og at mye var uklart når det gjaldt grenseoppgangene mellom straffe- og forvaltningssaker.

Utilstrekkelige rutiner dreier seg først og fremst om ønsker og behov for mer helhetlige, tilgjengelige og pålitelige datasystemer og -registre. Manglende ressurser handler i hoved-

sak om ønsker og behov for mer og nytt utstyr, og sist, men ikke minst, bemanning og tid.

4.1 Kompetanse- og opplæringsbehov

Samtlige politidistrikter pekte på mangelfull kunnskap og opplæring om utlendingskontroll, både teknisk dokumentkontroll og taktisk identitetskontroll.

Når det gjelder teknisk dokumentkontroll, er det mange som for eksempel ikke vet hva de skal se etter av sikkerhetslementer i pass og andre identitetsdokumenter. Det ble hevdet at den vanlige politibetjenten «... ikke vet noe som helst om kontroll av dokumenter», blant annet fordi dette ikke inngår i undervisningen på Politihøgskolen. Manglende kompetanse i dokumentkontroll fører til at kontrollene ikke blir foretatt slik de burde. Hvis ikke tjenestemannen kan gi konkrete holdepunkter for identitetstvil og dokumentmisbruk, er det ikke mulig for påtalemyndigheten å vurdere tiltale.

Flere av utlendingsseksjonene påpekte viktigheten av at politipatroljer burde ha et større fokus rettet mot identitetsrelaterte spørsmål ved utlendingskontroller. Det var derfor nødvendig med bevisstgjøring om identitetsarbeid hos politiet generelt, ikke bare hos de som jobber med utlendingsaker.

Når det gjelder kjennskap til regler for bruk av fingeravtrykk, var de fleste politidistriktene kjent med disse. Kunnskapen var god – særlig i

de større politidistriktene. Distriktene som hadde mindre erfaring, rapporterte at de var mer usikre når det gjaldt regelverket for bruk av fingeravtrykk, og da spesielt i bortvisnings- og utvisningssaker.

Praksis for opptak av fingeravtrykk i oppholdssaker (familieinnvandring) er imidlertid varierende. Dette skyldes blant annet uklarheter om reglene for opptak av fingeravtrykk for tredjelandsborgere.⁶⁹

Usikkerhet om regelverket ble oppgitt som en grunn til at det ikke alltid blir tatt fingeravtrykk, selv om reglene tilsier at det skal gjøres.

Det ble videre påpekt at regelverk, rundskriv og instruksjoner om bruk av fingeravtrykk i utlendingsaker var uoversiktlig. Dette gjaldt særlig grenseflatene mellom straffe- og forvaltningssaker. Det ble rapportert at straffesaker og forvaltningssaker ble blandet i regelverksformuleringene. Det var derfor ønskelig med en klarere oversikt over hjemler om bruk av fingeravtrykk i utlendingsaker.

Begrenset kunnskap om de ulike saksbehandlingssystemene som benyttes, og hvilken informasjon som er tilgjengelig i de ulike systemene, hemmer også effektiv utlendingskontroll. Det skortet dessuten på kompetanse i bruk av utstyr for opptak av fingeravtrykk og foto.

Politiets utlendingsenhet pekte ikke på et tilsvarende opplæringsbehov, men ga uttrykk for å ha god kunnskap og praksis for identitetsundersøkelser og teknisk dokumentkontroll. På

⁶⁹ Se også punkt 5.2. om «Opptak av biometri fra alle tredjelandsborgere» for nærmere omtale av utlendingsforskriften. § 18-1.

intervjutidspunktet hadde Politiets utlendingsenhet tre dokumentgranskere på andrelinjenivå⁷⁰ som sjekket flertallet av originale identitetsdokumenter i asylsaker.

4.2 Utilstrekkelige rutiner eller rutinebeskrivelser

Det ble også påpekt utfordringer knyttet til utlendingskontroll i forbindelse med andre typer politioppdrag. Eksempelvis når politiet påtreffer utlendinger i et narkotikabeslag som de da sjekker identiteten på. Dette er altså ikke en planlagt utlendingskontroll, men kan være et hvilket som helst politioppdrag.

Den spesialkompetansen som trengs, varierer i distrikter som ikke kommer opp i slike kontrollsituasjoner med jevne mellomrom. Politidistriktene ønsket klarere retningslinjer og rutinebeskrivelser, gjerne i form av enkle tiltakskort.⁷¹ Det ble kartlagt et behov for rutinebeskrivelser på flere områder: dokument- og personkontroll, registersøk, opptak, søk og registrering av fingeravtrykk, dessuten tekniske instruksjoner for hvordan man skal gjøre opptak av foto for registrering i DUF.⁷² Videre blir bilder ikke alltid tatt og lagt inn i DUF, ettersom mange ikke vet hvordan man gjør det, eller fordi utstyret ikke virker. Erfarne tjenestemenn påpeker at det er viktig å gjøre parallelle undersøkelser, og ikke eksempelvis

bare stole blindt på hurtigsøk.

Betydningen av å samtale med utlendingen ble fremhevet i tillegg til å søke i ulike politiregistre, som politiets straffesaksregister (Strasak) og politiets kriminaletterretningsregister (Indicia). Hurtigsøk var den metoden som oftest ble nevnt brukt for å innhente informasjon om identiteten til en utlending. Det ble påpekt at rutinene for hurtigsøk og andre undersøkelser ikke er optimale. Noen distrikter oppga at hurtigsøk ikke alltid ble foretatt i saker der det forelå tvil om identitet.

Distriktene (og Politiets utlendingsenhet) ga uttrykk for å være gode på å undersøke person og bagasje (ransaking). Samtidig ble det sagt at det var en del å hente når det gjaldt undersøkelser ved utlendingskontroll på territoriet. Spesielt når utlendingen ikke blir innbrakt på politistasjonen for hurtigsøk, mente tjenestemennene at undersøkelser burde vært utført i større grad, som for eksempel undersøkelse av bopel.

Kripos' patruljehåndbok for å utføre dokumentkontroll ble ikke nevnt, ei heller Politiets utlendingsenhets «Veileder for verifiseringsarbeid».

Opptak, søk og registrering av biometri

Ved asylregistrering hos Politiets utlendingsenhet er det rutine for å

gjøre opptak av foto og fingeravtrykk. Politiets utlendingsenhet søker i Eurodac og utlendingsregisteret, og resultatet av søket registreres i DUF.

I de tilfellene der en person melder seg som asylsøker i et politidistrikt, skal søkeren overføres til Politiets utlendingsenhet for registrering. Praksisen for slik overføring synes å være uklare.⁷³ Noen distrikter signalerer⁷⁴ og registrerer sak i DUF hvis utlendingen søker asyl. Andre politidistrikter har utarbeidet samarbeidsrutiner for overføring av asylanter til Politiets utlendingsenhet, men signalerer ikke personen og oppretter heller ikke noen sak i DUF.

Praksisen i bortvisnings- og utvisningssaker er ulik i politidistriktene, men trenden synes å være at det i stor grad blir tatt opp foto og fingeravtrykk i bortvisningssaker, mens dette gjøres i mindre grad i utvisningssaker.

Distrikter som har mindre erfaring med slike saker, synes imidlertid i større grad å unnlate å oppta biometri i form av foto og fingeravtrykk. Politidistrikter kan også velge å nedprioritere bortvisning, mens det har vært økt fokus rettet mot utvisning av straffedømte den siste tiden.

Noen politidistrikter forklarte at de ikke alltid signalerte i utvisningssaker.

En grunn til dette var mangel på

70. Dette er høyt kvalifiserte dokumentgranskere med avansert utstyr for ekthetsvurdering og tilgang på referansedokumenter. Andrelinje finnes hos Politiets utlendingsenhet, større politidistrikter og på enkelte flyplasser. De samarbeider ofte tett med førstelinjen.

71. Tiltakskort er en standardisert sjekkliste/handlingsplan/huskeliste for tiltak som skal settes i gang ved spesielle situasjoner. Disse blir brukt innen offentlig sektor, spesielt i HMS- og beredskapsarbeid.

72. DUF er utlendingsforvaltningens datasystem for utlendings- og flyktningssaker.

73. Dette er regulert i Politidirektoratets rundskriv 2012/005: «Politiets arbeid med søknader om beskyttelse (asyl), identifisering og uttransportering av utlendinger etter utlendingsloven».

74. Signalementsrapportering i politiet viser til registrering av persondata og opptak av foto og fingeravtrykk.

utstyr. Med håndholdt mobilt fingeravtrykksutstyr i patruljebilene ville det vært en mye enklere oppgave å oppta fingeravtrykk. Da ville patruljen slippe å ta inn personen til arrest eller politistasjon eller et annet sted med fingeravtrykksutstyr.

En annen grunn til manglende signalering i en utvisningssak er at personen som oftest allerede er signalert i straffesaken. På den annen side ble det også påpekt at dersom straffesaken ble henlagt, ville avtrykkene etter en viss periode bli slettet.

Politiet erfarer at hvis det ikke tas fingeravtrykk straks utlendingen blir utvist eller når det foreligger bortvisningsvedtak, blir dette heller ikke etterregistrert. Dette forklares med at politiet ikke alltid har kunnskap om hvor personen befinner seg. Men selv når politidistriktet har kontroll på personen i en utvisningssak, blir det heller ikke alltid tatt fingeravtrykk når det foreligger vedtak.

Politidistriktene oppga i intervjuene at biografisk førstehåndsinformasjon som tjenestemenn får i forbindelse med en utlendingskontroll, eller når en utlending søker asyl, sjeldent blir registrert noe annet sted enn i PO-loggen.⁷⁵ Dermed blir opplysninger om person og situasjon som kan være viktige for identitetsarbeidet, ikke kjent for aktørene i utlendingsforvaltningen som skal håndtere saken videre.

Samarbeid

Politipatruljene bruker som oftest egne operasjonssentraler og utlendingsseksjoner når de trenger bistand.

Videre ga de ulike politidistriktene uttrykk for at de stort sett brukte de samme kontaktene innenfor politiet: Gardermoen, Desken Kripos, Sirene Kripos og Politiets utlendingsenhet.⁷⁶ Desken i Politiets utlendingsenhet stenger kl. 23 på hverdager og kl. 19 i helgen, og det er bare Gardermoen og Desken Kripos som har døgnbemanning. Gardermoen fortalte at de ble brukt svært mye, og at stort sett hele Politi-Norge ringte inn for å be dem om råd.

Spesielt arrestforvarerne ga uttrykk for at de er avhengige av å ringe rundt til andre aktører, som oftest Politiets utlendingsenhet og Gardermoen. Grunnen til dette er at arrestforvarerne sjelden har tilgang til de ulike systemene.

Manglende ressurser

Mangel på ressurser ble omtalt som en stor utfordring i politiets arbeid med utlendingskontroll. Blant annet bemerket skrankepersonell at de bruker for kort tid per klient på grunn av lav bemanning. Oslo politidistrikt anslo at det blir brukt om lag 15 minutter per tredjelandsborger, og bare ti minutter hvis personen var en EU-/EØS-borger. Dette er altfor liten tid til å gjøre en god nok vurdering av personens identitet, samtidig som man utfører en rekke registreringer i systemet. Videre forklarer politidistrikter som har

egne dokumentgranskere, at andre oppgaver ofte fører til at arbeid med dokumentkontroll nedprioriteres.

4.3 Politiets utstyr

Mangelen på utstyr, både for enkel kontroll og mer sofistikerte metoder, ble fremhevet av alle intervjuobjektene.

Biometrikiosken

Flere politidistrikter ga uttrykk for et ønske om utvidet bruk av biometrikioskene. I tillegg til opptak og lagring av fingeravtrykk burde den også bli tilrettelagt for søk opp mot utlendingsregisteret og Eurodac. Ettersom lagringsmulighetene er der, burde også søkemulighetene være det, mente mange.

Én-fingeravtrykksleser

Samtlige politidistrikter fikk i 2011 utlevert én-fingeravtrykkslesere i verifiseringøyemed. Dette utstyret er ikke i bruk, og hos ett av distriktene som Nasjonalt ID-senter besøkte, fikk vi beskjed om at åtte slike fingeravtrykkslesere lå «stuet bort i kjelleren». Én-fingeravtrykksleserne skulle brukes til å verifisere pass i GK-systemet,⁷⁷ men dette viste seg å ikke være tekniske mulig. Avleserne kan imidlertid benyttes til verifisering opp mot VIS-basen. En ulempe er imidlertid at VIS krever to fingre slik at man må gjøre to opptak to ganger.

Lumidigm

Politiets utlendingsenhet nevnte at de gjerne ville ha nye fingeravtrykkskannere av merket Lumidigm.

75. Politioperativ logg, et internt datasystem og arbeidsredskap.

76. Andre støttespillere for politidistriktene var Skatteetaten, Arbeidstilsynet og Tollvesenet. Øst-Finnmark politidistrikt rapporterte også at de har et godt samarbeid med Forsvaret og Mattilsynet. Skatteetaten ble fremhevet som en etat som satset på arbeidet med utlendingers identitet.

77. GK er grensekontrollens saksbehandlingssystem/grensekontrollapplikasjon.

Lumidigm er en dypskannervariant som leser flate fingeravtrykk, også i de tilfellene der avtrykk av ulike årsaker blir dårlige, for eksempel ved slpite fingertupper. Sverige har gode erfaringer med dette utstyret.⁷⁸

Håndholdte mobile enheter

Videre var det et sterkt ønske fra flere om håndholdte mobile enheter med applikasjoner for bruk av fingeravtrykk og bilde som biometriske identifikatorer. Det er kjent at andre lands utlendingsmyndigheter benytter smart-telefoner til å oppta bilde i et format som kan benyttes til ansiktsgjenkjenning opp mot databaser. Flere av respondentene ønsket at politiet i Norge også fikk dette verktøyet. Håndholdte mobile løsninger vil effektivisere politiarbeidet blant annet ved at patruljer ikke behøver å ta inn utlendingen til politistasjonen for biometrisk søk.

Det ble også sagt at håndholdte mobile løsninger for verifisering og identifisering av personer vil bli enda mer relevant nå som det er innført Schengen-standardiserte oppholdskort med biometri.

Verktøy for ansiktsgjenkjenning

I dag har politiet i hovedsak ikke annen mulighet enn manuell sammenligning av enten foto mot foto eller foto mot person. Ofte sendes foto via mobiltelefon til operasjonssentralen, som foretar manuelle sammenligninger i politiets

foto-register eller DUF. En slik sammenligning er ofte svært vanskelig, på grunn av dårlig bildekvalitet, eller personforandringer som vektøkning, aldring eller misdannelser i ansiktet.

Respondentene var positive til å utvikle et verktøy for ansiktsgjenkjenning i utlendingssaker. Flere anså identifisering- og verifisering opp mot lagrede foto i UDB-basen som nyttig, både i førstelinjen og i det videre arbeidet med identitetsfastsettelse.

4.4 Systemløsninger og registerforvaltning

En utfordring ved systemene er mangelen på helhetlige løsninger. Det ble ytret ønske om en løsning som gjorde at flere søk kunne foretas simultant, i ulike baser. Ett opptak kunne brukes til automatisert søk basert på standardiserte innlagte kriterier.

Politisystemene

De fleste respondentene fremhevet utfordringen med ustabile datasystemer. Det er stor frustrasjon over dårlig internettforbindelse og politiets datasystemer og nettverk ble beskrevet som «trege, utdaterte og upålitelige». Det ble uttrykt et sterkt behov for mer driftssikre systemer.

I dag kan én person bli registrert med ulike identiteter i de ulike registrene.

Et politidistrikt nevnte som eksempel en kriminell iraker som figurete med

én identitet i folkeregisteret, to identiteter i SSP,⁷⁹ to identiteter i BL⁸⁰ og fire identiteter i PO-loggen, som er et internt datasystem og arbeidsredskap.

Hvis politiet hadde hatt ett felles identitetsregister basert på biometri, ville ikke dette vært mulig.⁸¹

VIS

Verifisering mot VIS-basen kan foreløpig bare gjøres alfanumerisk, ikke med fingeravtrykk av politiet (grensekontroll, kontroll på territoriet og Politiets utlendingsenhet) i Norge. Det er et sterkt ønske om å legge til rette for bruk av fingeravtrykk mot VIS så raskt som mulig.

Referansedatabaser og tilganger

Flere ønsker seg tilganger til politisystemer for å kunne foreta identitetsvurderinger i utlendingssaker. Etterretningsregisteret Indicia ble nevnt spesielt. Politiets tilgang til utlendingsforvaltningens datasystemer er også begrenset for enkelte tjenestemenn. Noen arrestforvarere nevnte at tilgangen deres til DUF ble sperret etter 14 dager uten bruk, mens andre politidistrikter opplyser at deres arrestforvarere ikke har tilgang til DUF i det hele tatt. Dette førte ofte til at det ikke ble gjort søk i DUF.

Biometra

Flere bemerket at på grunn av bemanningssituasjonen hos Kripes

78. Etter vårt intervju med PU tok de i bruk Lumidigm sommeren 2012. Med noen meget få unntak blir nå alle fingeravtrykk godkjent, og de som tidligere ikke hadde blitt godkjent i Eurodac på grunn av skade eller sliping, har blitt hentet inn til nye avtrykk.

79. I SSP (Det sentrale straffe- og politiopplysningsregisteret) registrerer politiet og påtalemakten personopplysninger i forbindelse med forebygging og etterforskning av lovbrudd og straffefølgelse av lovbrutere.

80. BL er et lokalt saksbehandlingssystem i politiet og står for «Basisløsninger». I BL registreres opplysninger som er nødvendige ved behandlingen av en straffesak, helt fra en sak er anmeldt til den er avsluttet.

81. Politiets utlendingsenhet kom etter vårt intervju i gang med en prøveordning med å søke biometrisk i VIS.

fikk de ikke alltid svar på søk i helgene. Dette problemet er siden kartleggingen løst ved innføring av Biometra II som sender et foreløpig svar på søket automatisk. Det foreløpige svaret som politiet mottar er tilstrekkelig for å kunne gå videre med saken selv om det er helg.

Det ble videre rapportert at det er uheldig at Biometra aksepterer fingeravtrykk av for dårlig kvalitet ved opptak. Politidistriktene ønsket dessuten tilbakemeldinger fra Kripos om kvaliteten på fingeravtrykksarbeidet.

Det ble også nevnt at systemet med registrering av fingeravtrykk i dag førte til mye dobbeltarbeid, ettersom personer blir signalert etter både straffeloven og utlendingsloven. Det var ønskelig med en avhukingsknapp i Biometra der man kunne markere at det skulle lagres både i henhold til utlendingsloven og straffeloven når dette er lovpålagt. Ettersom Biometra er tilrettelagt for søk i både kriminalregisteret og utlendingsregisteret, lurte flere politidistrikt på hvorfor man ikke kunne oppta og lagre fingeravtrykk i begge registrene samtidig.

4.5 Kartlegging av praksis for opptak, lagring og søk i registre i syv land

Nasjonalt ID-senter forespurte medlemmer i IGC-nettverket om opptak og lagring av biometri i visumsaker og oppholdssaker. Intergovernmental Consultations on Migration, Asylum and Refugee (IGC) er et forum der medlemmene

kan konsultere hverandre i spørsmål knyttet til migrasjon. Under oppsummerer vi raskt noen viktige punkter i de ulike landenes arbeid med biometri i deres respektive utlendingsforvaltninger.

Finland

Finland opptar og lagrer fingeravtrykk nasjonalt av personer over seks år som søker om beskyttelse, familiegjenforening, av kvoteflyktninger, personer som er nektet innreise / utvist fra landet og ved identitetstvil. Fingeravtrykk som er opptatt til Schengens VIS-base, lagres ikke nasjonalt.

Registeret kan bare brukes av immigrasjonsmyndighetene, politiet, grensekontrollen eller utenriksstasjonene. Formålet er å undersøke oppholdsstatus og for å verifisere identiteten til eieren av et oppholdskort, eller i saker knyttet til inn- og utreise, opphold og arbeid, samt av hensyn til nasjonal sikkerhet og i forbindelse med sikkerhetsklarering. Det kan søkes opp mot politiets systemer⁸² ved grensekontroll, men kun dersom fingeravtrykkene er knyttet til et lovbrudd der strafferammen er på minst ett år ubetinget fengsel.

New Zealand

New Zealand registrerer bare fingeravtrykk av asylsøkere. Fra november 2013 vil ansiktsbiometrien til alle som søker visum og oppholdstillatelse,⁸³ bli registrert, mens opptak av fingeravtrykk vil være risikobasert. New Zealand deltar i et multinasjonalt samarbeid om sikkerhet med myndighetene i Canada, USA,

Australia og Storbritannia. Samarbeidet åpner for at immigrasjonsmyndighetene kan dele biometriske data når de skal undersøke identiteten til innvandrere og besøkende.

Tyskland

Fingeravtrykk som er opptatt for lagring i Schengens VIS-base lagres ikke nasjonalt. Ellers blir foto lagret i den nasjonale visumdatabase som er tilknyttet det nasjonale utlendingsregisteret. Fingeravtrykkene til utlendinger som søker nasjonalt visum,⁸⁴ blir lagret sentralt i den nasjonale fingeravtrykksdatabase. Fingeravtrykk som er opptatt til produksjon av oppholdskort, lagres ikke nasjonalt. Fingeravtrykk som er lagret i oppholdskortet, brukes utelukkende til å verifisere identiteten til bæreren av dokumentet.

Sveits

Fingeravtrykk som er opptatt til Schengens VIS-base lagres ikke i nasjonalt register. Det opptas heller ikke fingeravtrykk i forbindelse med utstedelse av D-visum. Fingeravtrykk som er opptatt for søknad om oppholdstillatelse og for utstedelse av oppholdstillatelse, lagres derimot i et nasjonalt register. Lagrede biometriske data brukes bare til å utstede nye oppholdstillatelser (fornyelser) i løpet av de påfølgende fem årene fra opptaket.

Storbritannia

I Storbritannia tas det opp fingeravtrykk i alle utlendingssaker. Samtlige fingeravtrykk, uansett sakstype (visum, oppholdstillatelse, asyl og utlendinger som har brutt

82. Systemet PATJA.

83. Både såkalt long-stay og short-stay visa.

84. Kategori D

immigrasjonslovgivningen), lagres i et sentralt fingeravtrykkregister og er innbyrdes søkbare. Fingeravtrykk kan også sjekkes mot politiets fingeravtrykksregister for kriminalsaker. Fingeravtrykkene slettes etter ti år, eller når utlendingen får britisk statsborgerskap. Dersom fingeravtrykkene kun er registrert av identifiseringshensyn, slettes de så snart identiteten er fastslått.

Australia

Det opptas fingeravtrykk i alle utlendingssaker der det søkes om beskyttelse og visum (inkludert studieopphold og varig opphold). Fingeravtrykkene kontrolleres mot, og lagres i, en nasjonal fingeravtrykksdatabase.

Nederland

Fingeravtrykk som er opptatt til Schengens VIS-base lagres ikke i et nasjonalt register. Utenriksstasjonene opptar fingeravtrykk ved innlevering av søknad om oppholdstillatelse. Fingeravtrykkene overføres hjem til Nederland for produksjon av oppholdskort. Oppholdskortene brukes som innreisebevis. Fingeravtrykkene som er opptatt i oppholdssaker, lagres ikke nasjonalt.

Nederland utreder nå et forslag om å oppta og lagre ti fingeravtrykk for alle tredjelandsborgere, inkludert barn over fire år ved søknad om beskyttelse og seks år ved andre typer oppholdssøknader. Grunnlaget er å bruke registeret i arbeidet med å verifisere identiteten til utlendinger som søker seg til Nederland. Det er også ønskelig å kunne benytte registeret i kriminalsaker, og forslaget

åpner for søk ved nærmere bestemte tilfeller: som en siste utvei, etterforskning, eller ved mistanke om alvorlige lovbrudd, terrorisme og lignende. Fingeravtrykkene foreslås slettet ti år etter at tillatelsen har løpt ut, eller når personen har forlatt Nederland.

Sverige

Fingeravtrykk som er opptatt til Schengens VIS-base og for utstedelse av oppholdskort lagres, ikke i et nasjonalt register. Ved søknad om beskyttelse derimot opptas det og lagres fingeravtrykk i et nasjonalt register. Dette fingeravtrykkregisteret ligger hos politiet. Fingeravtrykkene slettes etter ti år, eller når utlendingen blir svensk statsborger.

Danmark

I Danmark registreres fingeravtrykk i et særskilt EDB-register (B-filen), som Rigspolitichefen er ansvarlig for. I henhold til dansk utlendingslov § 40a, nr. 5, skal disse fingeravtrykkene slettes ti år etter registreringen. I Danmark finnes det ingen ytterligere regulering av sletting av fingeravtrykk i den såkalte B-filen.

5 Oppsummering og anbefalinger

I punkt 5.1 har vi laget en oversikt over anbefalinger og hvem vi mener har ansvaret for å følge dem opp. I rapporten har vi pekt på at opplæring er et viktig område, og at Nasjonalt ID-senter har en sentral rolle og ansvar. Dette arbeidet er prioritert og opplæringstilbudet fra Nasjonalt ID-senter vil styrkes i 2013. I tillegg til ordinær opplæring vil vi utvikle nye e-læringstjenester på NID-portalen for førstelinjen i politiet og utenriks tjenesten knyttet til blant annet opptak av biometri.

I resten av kapittelet har vi oppsummert og begrunnet anbefalingene i oversikten nedenfor.

5.1 Oversikt over anbefalinger og etatenes ansvar

Justis- og beredskapsdepartementets ansvar

- avklare ansvar, policy og regelverk for implementering av biometri som følge av Schengen-avtalen.
- sørge for at bruken av biometri i utlendingsforvaltningen utvides, herunder:
 - opprette en felles nasjonal database for opptak og lagring av biometri i alle typer utlendings-saker
 - flytte opptak av biometri til utenriksstasjonene i de sakene der det er aktuelt
 - innføre biometri-søk som første obligatoriske trinn i saks-behandling i utlendings saker
 - gi mulighet til å benytte hele databasen ved identifisering og verifisering uansett sakstype

Politidirektoratets og Politiets data- og materiell tjenestes ansvar

- tydeliggjøre prioritering og strategi for politiets bruk av biometri i identitetsarbeidet i styringsdialogen med politidistriktene
- innføre ID- og dokumentkontroll som fag på Politihøgskolen
- utbedre og oppgradere de tekniske systemene, blant annet:
 - bedre integrasjonen mellom systemene slik at politiet får færre og bedre systemer å forholde seg til
 - prioritere å legge til rette for tilgang til å verifisere med fingeravtrykk mot VIS for Politiets utlendingsenhet, grensekontrollen og politidistriktene
 - gjennomføre pilotprosjekt på håndholdt mobilt utstyr for biometri i samarbeid med Nasjonalt ID-senter og Politiets data- og materiell tjeneste
- omorganisere den systematiske opplæringen i utlendingsforvaltningen, blant annet:
 - utarbeide instruks for å opprette rollene «opplæringsansvarlige» og «superbrukere» innen identitetsfeltet i hvert politidistrikt
- sette av midler til regionale samlinger innen identitetsfeltet for «opplæringsansvarlige» og «superbrukere» i politidistriktene og Politiets utlendingsenhet

Politidistriktenes ansvar:

- følge opp Politidirektoratets omorganisering- og innføring av nytt opplæringssystem i utlendingsforvaltningen med rollene «opplæringsansvarlige» og «superbrukere» innen identitets-

feltet i hvert politidistrikt

- prioritere identitetsarbeidet i førstelinjen
- sette av tid til identitets- og dokumentkontroll ved mottak av søknader

Utenriksdepartementets ansvar:

- innføre et nytt opplæringssystem for utenriksstasjonene med rollene «opplæringsansvarlig» og «superbruker» innen identitetsfeltet blant de lokalt ansatte
- prioritere identitetsarbeidet i førstelinjen
- sette av tid til identitets- og dokumentkontroll ved mottak av søknader

Nasjonalt ID-senters ansvar:

- prioritere opplæring i ID- og dokumentkontroll i politidistriktene
- utarbeide og implementere et godt opplæringsprogram innen identitetsfeltet, i samarbeid med blant annet Utenriksdepartementet, Politidirektoratet, Utlendingsdirektoratet, Romerike politidistrikt, Kripos og Politiets utlendingsenhet som inkluderer:
 - generell ID-kunnskap
 - taktisk identitetskontroll av person og dokument
 - teknisk dokumentkontroll
 - opptak av biometri
 - rutiner, lover, regler
- gi opplæring til utlendingsforvaltningen i identitetsspørsmål og dokumentkontroll
- være en aktiv del av kontaktnettet til «opplæringsansvarlige» og «superbrukere» i utlendingsforvaltningen

- delta i pilotprosjekter:
 - pilotprosjekt om ansikts-gjenkjenning i samarbeid med Utlendingsdirektoratet, Politiets Sikkerhetstjeneste, Kripos og Politiets data- og materielltjeneste
 - pilotprosjekt om håndholdte enheter for biometri i samarbeid med Politiets data- og materielltjeneste

5.2 Bruken av biometri i utlendingsforvaltningen bør utvides

Det er nødvendig med økt bruk av sentral lagring av biometri i en felles nasjonal base, videre skal identiteten låses til personens biometri og gjøre verifisering mulig. Søk i identifiserings- eller verifiseringsøyemed forutsetter at biometriske data lagres. I dag lagres biometri i norske utlendingsaker på flere ulike steder:

- innvilgelse av oppholdstillatelse – RFID-brikke i oppholdskortet
- søknad om Schengen-visum (innvilgelse og avslag) – VIS
- søknad om beskyttelse (innvilgelse og avslag) – Eurodac
- søknad om beskyttelse, samt utvisningssaker – Utlendingsregisteret

Dette innebærer at utlendingen kan bli registrert med én identitet i VIS og en annen i oppholdskortet. På samme måte kan en utlending få avslag på et Schengen-visum på én identitet, og få innvilget oppholdstillatelse på en annen identitet.⁸⁵ Dette ville ikke vært en problemstilling dersom biometri i alle typer utlendingssaker ble lagret i én felles database, eventuelt at databasene i større grad kunne utveksle

informasjon seg i mellom.

Behov for sikker identifisering og verifisering

Sentral lagring av biometriske data er en forutsetning for med sikkerhet å kunne kontrollere om utlendingen tidligere har blitt registrert under en annen identitet. Biometri er en sikker identifiseringsmetode som kan avsløre identitetsmisbruk. Systemet vi har i dag, åpner for at utlendinger relativt enkelt kan operere med flere identiteter.

På samme måte er lagring, enten i et kort eller i en nasjonal database, en forutsetning for å kunne verifisere at utlendingen er rette innehaver av tillatelsen eller visumet.

Formålene med opprettelse av en sentral database med biometriske data vil være avgjørende for hvilken behandling det er adgang til å foreta og bør fremgå direkte av lovgivningen som hjemler opprettelsen av databasen.

Opptak og lagring av biometri ved første anledning

Fingeravtrykk og foto må opptas og lagres første gang utlendingen søker om en form for oppholdstillatelse i Norge. I de fleste tilfeller vil dette være ved utenriksstasjonene. For utlendinger som er unntatt fra visumplikten, vil politiet i grensekontrollen være førstelinje. Og for den som registreres for første gang med en utvisningssak vil det være politiet.

I dag opptas biometrien først etter at utlendingen har ankommet Norge, og dette gjør systemet sårbart. For eksempel kan én person søke, og få

innvilget en tillatelse, og en annen person som ligner på søkeren, kan reise inn til Norge. Dette kan være en person som ikke ville fått innvilget en tillatelse med sin egen identitet. Når biometri så avlegges etter ankomst, vil den i slike tilfeller bli knyttet til feil person.

Nasjonalt ID-senter anbefaler derfor at opptak av biometri i form av foto og fingeravtrykk bør skje ved første mulige anledning.

All saksbehandling bør starte med et biometrisøk

All saksbehandling i utlendingssaker bør starte med et biometrisøk mot den nasjonale fingeravtrykksdatabasen. Dette vil gjøre at vi kan koble eventuelle gamle saker til nye, og vi kan avsløre eventuell misbruk av identitet. Ettersom identitet skal vurderes i alle sakstyper, er det formålstjenlig å utføre denne kontrollen før de andre vilkårene eventuelt vurderes. Tiltaket kan både sikre kvalitet og være ressursbesparende.

D-visum

Det finnes to hovedtyper D-visum (innreisevisum),⁸⁶ og i dag tas det ikke opp biometri i disse sakene. De to typene er:

- D-visum som utstedes av en utenriksstasjon etter at Utlendingsdirektoratet eller Utlendingsnemnda har innvilget oppholdstillatelse.
- D-visum som innvilges i visse tilfeller, av en utenriksstasjon (eventuelt av Utlendingsdirektoratet eller Utlendingsnemnda) til utlendinger slik at de kan oppholde seg i Norge mens søknaden om oppholdstillatelse er til behandling

85. Det er ikke adgang til å søke i VIS-basen i forbindelse med behandlingen av en søknad om oppholdstillatelse (med unntak av søknad om beskyttelse).

86. Jf. utlendingsloven § 12, jf. utlendingsforskriften § 3-13.

Slike visa er et nasjonalt anliggende og fingeravtrykkene kan ikke opptas og lagres i VIS-basen. Dette betyr at så lenge denne typen visum benyttes for innreise, vil vi ikke kunne kontrollere om det er samme person som har fått oppholdstillatelsen, som reiser inn i landet. Dersom D-visum lagres i en nasjonal base, vil vi kunne gjøre oppslag på grensen ved innreise til Norge og verifisere fingeravtrykkene.

I de tilfellene der utlendingen har fått innvilget en oppholdstillatelse, bør oppholdskortet sendes til den norske utenriksstasjonen der utlendingen har søkt, og benyttes av utlendingen for innreise til Schengen i stedet for D-visum. På den måten vil også grensekontrollen i andre Schengen-land kunne verifisere utlendingens oppholdsstatus i Norge⁸⁷ når utlendingen velger å reise inn til Norge via et annet Schengen-land. En slik fingeravtrykksverifikasjon forutsetter som nevnt⁸⁸ at visse sikkerhetsmekanismer må være på plass.

Nasjonal lagring av biometri som er tatt opp i forbindelse med søknad om Schengen-visum

VIS-forordningen åpner for at fingeravtrykk som er opptatt til VIS på en utenriksstasjon, også kan lagres nasjonalt og benyttes for internt bruk.

I VIS er søk begrenset til visumsaker, identitetstvil og ved søknad om beskyttelse.⁸⁹ Dersom disse fingeravtrykkene lagres nasjonalt, kan de benyttes til identitetsfastsetting ved

alle typer søknader. Dette forutsetter en ny lovhjemmel. Nasjonalt ID-senter vurderer det slik at kontrollhensynene ikke er mindre i en sak om oppholdstillatelse enn i en sak om beskyttelse. Altså bør fingeravtrykkene lagres for å kunne undersøke om personen tidligere kan ha søkt visum under en annen identitet.

Opptak av biometri fra alle tredjelandsborgere

Utlendingsdirektoratet har fremmet ønske om at det rutinemessig gjøres opptak og lagring av biometri av alle tredjelandsborgere i samtlige sakstyper.⁹⁰ Dette er tilsvarende kontrollhensynet som ligger til grunn for dagens adgang til søk i utlendingsregisteret jf. utlendingsforskriften § 18-3, jf. § 18-1 bokstav g, og søk i VIS-basen i identifiseringsøyemed, jf. VIS-forordningen artikkel 20. Dersom opptak av fingeravtrykk utvides til å rutinemessig omfatte tredjelandsborgere som søker oppholdstillatelse, vil grunnlaget for søk bli betydelig utvidet. En kontroll vil da kunne avdekke om utlendingen har oppholdt seg ulovlig i Norge, for eksempel etter avslag på en søknad om fornyelse.

Nasjonalt ID-senter støtter dette forslaget. Identitetsmisbruk er en stor utfordring, ikke bare for utlendingsforvaltningen, men også for samfunnet for øvrig. Misbruk av identitet kan bety at personer får ytelser eller rettigheter de ikke har krav på. Videre er identitetsmisbruk som ledd i annen kriminell aktivitet en utfordring

Et alternativ kunne være at alle som er visumpliktige, må registreres med biometri ved en søknad om oppholdstillatelse. Nasjonalt ID-senter anser at det mest hensiktsmessige vil være om alle behandles likt, og anbefaler derfor at alle tredjelandsborgere må avlegge biometri.

I dag er vilkårene for opptak av biometri at utlendingen ikke kan dokumentere sin identitet, eller det er grunn til å mistenke at utlendingen oppgir falsk identitet.⁹¹ Dette gjelder også oppholdssaker og visumsaker. Fingeravtrykkene i beskyttelsesaker, oppholdssaker og visumsaker blir dermed søkbare opp mot hverandre ved lagring i utlendingsregisteret, jf. utlendingsforskriften § 18-3.

Søkere som er visumfri, vil ikke bli avkrevd biometriske data i motsetning til visumpliktige, som avgir fingeravtrykk og foto for lagring i VIS. En delvis utvidelse i bruk av biometri, ut fra vurderingene i avsnittet ovenfor, er å gjøre opptak av biometri i oppholdssaken dersom personene er visumpliktige.

En forutsetning for å kunne gjøre opptak av fingeravtrykk etter utlendingsforskriften § 18-1 er at utlendingen «ikke kan dokumentere sin identitet», mens utlendingsforskriften § 18-4 om sletting av fingeravtrykk slår fast at avtrykkene ikke skal slettes for «fremleggelse av dokumentasjon med nødvendige notoritet eller utlendingen innvilges statsborgerskap i Norge eller i et annet land som deltar i Eurodac-samarbeidet». Det

87. Ved hjelp av fingeravtrykkene som er lagret i RFID-brikken i kortet.

88. Se punkt 3.5 om «Sikkerhetsmekanismer ved lagring av biometrisk data i oppholdskort, utlendingspass og reisebevis for flyktninger».

89. Jf. artikkel 22 i VIS-forordningen

90. Utlendingsdirektoratet: «Rapport om utvidet bruk av biometri i utlendingsforvaltningen», 2010.

91. Jf. utlendingsloven § 100 første ledd, bokstav a.

har vært uklarheter i praktiseringen av utlendingsforskriften § 18-1.

Nasjonalt ID-senter oppfatter dette som et dokumentasjonskrav som krever nærmere utdyping i retningslinjer.

Sentral lagring av biometri til bruk i utreisekontroll

For en utlending som har fått avslag på søknad om beskyttelse, gjelder en plikt til utreisekontroll.⁹²

Utlendingsdirektoratet stiller spørsmål i sin rapport om det i den forbindelse bør innføres fingeravtrykkskontroll.⁹³

Utlendingsdirektoratet foreslår at ordningen også skal omfatte andre tredjelandsborgere som får avslag på sin søknad om fornyelse av oppholdstillatelse.

Planen med innføring av et entry/exit-system i Schengen⁹⁴ vil innebære at det skal gjennomføres søk i VIS-basen med påfølgende registrering av visumpliktiges inn- og utreise.

Innføring av tilsvarende fingeravtrykkskontroll når tredjelandsborgere som ikke har en oppholdstillatelse i Norge reiser ut av landet, forutsetter en utvikling av grensekontroll-applikasjoner og søk-funksjonalitet opp mot lagrende biometriske data. Det er for øvrig ingen grunn til å vektlegge kontroll med utreise i mindre grad enn kontroll med innreise.

Registrering av identitet når dokumentasjonen har lav notoritet

I saker om beskyttelse hender det ofte at søkeren ikke har dokumentasjon

på identitet, eller at den dokumentasjonen som legges frem har for lav notoritet til å kunne benyttes. Dokumentasjon med lav notoritet forekommer også i visum- og oppholdssaker. I slike tilfeller bør utlendingsmyndighetene kunne registrere den oppgitte identiteten til søkeren, slik de gjør i dag, og knytte denne til søkerens biometri. Dersom personen senere forsøker å endre opplysningene, vil man unngå dobbelt- og alias registreringer, og stå igjen med bare ett individ som har flere navn⁹⁵ knyttet til seg, eventuelt flere måter å transkribere det samme navnet på.

Bedre kvalitet på registreringene i UDB

Sentral lagring av biometri vil kunne forbedre kvaliteten på registreringene i UDB. Slik vil man kunne avsløre om personer opererer med eller er registrert med flere identiteter i UDB som nevnt i avsnittet over. Dette kom også frem som et ønske i kartleggingen Nasjonalt ID-senter gjorde hos politiet.

Ved å ta i bruk biometriske teknikker vil utlendingsmyndighetene lettere kunne finne igjen tidligere navne-registreringer med tilknyttede saker. Transkribering av navn er et eksempel på en faktisk og praktisk utfordring som kan innebære at tidligere saker som er registrert på personen, ikke blir gjenfunnet. I tillegg kan det forekomme feilregistreringer. Tidligere sakshistorikk er også viktig fordi opplysningene ofte vil være av betydning for utfallet av neste sak. Sentral lagring av biometri vil

forbedre kvaliteten på registreringene i UDB og dermed bidra til økt rettssikkerhet for søkerne.

Svakhetsmomenter ved lagring kun i oppholdskortet

Som tidligere nevnt opptar vi i dag biometri for produksjon av pass, reisebevis og oppholdskort, men denne biometrien lagres ikke i noen database. Den er kun lagret i RFID-brikken på selve kortet eller i reise-dokumentet.

Biometri som er lagret i VIS, kan etter endt utrulling verifiseres ved Schengens yttergrense. I saker der utlendinger har fått innvilget oppholdstillatelse, har man i dag ingen mulighet for å verifisere med fingeravtrykk ved grensen. Det åpner for at en person kan søke om en tillatelse, og en annen person kan reise inn til Norge (bare de ligner på hverandre).

Uten lagring i en database har man heller ingen mulighet for å verifisere om utlendingen er den rette innehaveren av tillatelsen, hvis kortet eller RFID-brikken går i stykker eller ødelegges. Dette gir muligheter for misbruk ved at flere personer kan oppholde seg i Norge på samme identitet, uten oppholdstillatelse. Kort som er meldt tapt uten at de egentlig er det, kan også tas med ut av Norge av en tredjepart og selges eller lånes ut til en annen person for innreise til Norge eller Schengen.

Det at vi ikke vet hvem disse menneskene er, utgjør naturligvis en sikkerhetsrisiko,⁹⁶ men selv mennesker

92. Jf. utlendingsloven § 90, jf. utlendingsforskriften § 17-14a.

93. Utlendingsdirektoratet: «Rapport om utvidet bruk av biometri i utlendingsforvaltningen», 2010.

94. Som forklart i punkt 3.6.

95. Det kan også dreie seg om nasjonalitet, fødselsdato og lignende.

96. Terrorisme, alvorlig kriminalitet, etc.

som ikke omfattes av den kategorien, vil kunne åpne bankkonto, studere, ta arbeid, motta sosiale ytelser og lignende, til tross for at de ikke har lovlig opphold i Norge.

Alternative tekniske løsninger

Nasjonalt ID-senter mener at det finnes to alternativer for lagring av fingeravtrykk som er tatt opp i oppholds- og visumsaker: i dagens utlendingsregister eller i en ny database. Uansett hvor dataene lagres, må databasen være i stand til å lagre om lag 250 000 – 350 000 fingeravtrykk per år og utføre raske søk på samme antall saker og eventuelt grensepasseringer, noe som krever en relativ kraftig søkemotor.

For å oppnå en effektiv bruk av systemet må søkene gjøres automatisk, og svaret må lagres i saken og synliggjøres for saksbehandleren. Dagens utlendingsregister har trolig ikke kapasitet til å håndtere en slik mengde data og er heller ikke bygd for denne typen automatikk. Det er per i dag heller ikke datakommunikasjon mellom Utlendingsdirektoratets systemer og politiets portal Biometra, som styrer trafikk til utlendingsregisteret, og AFIS.

Det er kjent at politiets AFIS skal moderniseres, men det er per i dag ikke kjent hvor stor kapasitet det nye systemet får, og i hvilken grad systemet kan behandle søk automatisk.

Dagens utlendingsregister inneholder data som er tatt opp for bruk i

utlendingssaker, men politiet kan benytte seg av det under spesielle vilkår. Utlendingsregisteret ligger i samme database som politiets kriminalregister, men i separate filer. Som nevnt tidligere er Utlendingsdirektoratet behandlingsansvarlig, og Kripos er databehandler. Kripos drifter registrene og AFIS. Dette betyr at det er to dataansvarlige i samme database, Utlendingsdirektoratet for forvaltningsdataene og Kripos for kriminaldataene. Dette er i utgangspunktet ikke god databaseforvaltning.

Dersom fingeravtrykk fra oppholds- og visumsaker skal registreres i en sentral database, bør det derfor vurderes om det er hensiktsmessig å skille forvaltningsdelen fra kriminaldelen og etablere to separate systemer under hver av de dataansvarlige, Utlendingsdirektoratet og Kripos. Dette vil gjøre drift og ansvarsforhold enklere.

En slik deling vil ikke medføre dårligere tilgang, men vil gi et mer ryddig eierforhold og en bedre tilgangsstyring basert på hjemmel i regelverket.

Dersom en ny database for fingeravtrykk i forvaltningssaker etableres i regi av Utlendingsdirektoratets, må det vurderes i hvilken grad dagens eksisterende forvaltningsdata i utlendingsregisteret også bør flyttes over til den nye databasen, slik at vi får én felles database for forvaltningssaker under Utlendingsdirektoratet.

Et moderne biometrisk søkesystem vil være basert på å levere tjenester

til brukerne. For å få adgang må «kallene» som ber om tjenestene være i tråd med de spesifikasjonene som systemeieren har satt. Systemeieren vil på denne måten ha god styring over bruken av basen og dermed sikre at bare autoriserte brukere og systemer kan gjennomføre søk.

Type fingeravtrykk

Når det gjelder visum- og oppholdsaker, er kravet fra Schengen i dag at to flate fingeravtrykk skal tas opp og lagres i oppholdskortet. Dersom fingeravtrykkene skal lagres i en sentral forvaltningsdatabase under Utlendingsdirektoratet som vi diskuterer over, anbefaler Nasjonalt ID-senter at det opptas og lagres ti flate fingeravtrykk, der to brukes til produksjon av oppholdskortene. Dersom ti flate fingeravtrykk tas opp, kan man benytte samme system og standard som allerede er etablert for VIS-systemet. Dette vil forenkle opptak og systemutvikling. I tillegg vil ti fingeravtrykk gi mer informasjon, noe som medfører bedre muligheter for gjenfinning i databasen.

Dagens internasjonale trend innen fingeravtrykksbaser (VIS-basen og visum, oppholdskort og i det kommende Smart border-systemet⁹⁷⁾ er at det i utlendingssaker opptas flate fingeravtrykk. Dette står i motsetning til politisystemene, som er basert på rullede fingeravtrykk. Utlendingsregisteret har rullede fingeravtrykk.⁹⁸ Fingeravtrykkene som skal lagres og søkes i Eurodac, må også være rullede i henhold til Eurodac-forordningen.⁹⁹ Det er fremmet

97. Se punkt 3.6.

98. Dette er et frivillig valg for Norge.

99. Council Regulation (EC) No 407/2002 of 28 February 2002 – Laying down certain rules to implement Regulation (EC) No 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, article 1.2.

ønske fra flere Schengen-land om å endre Eurodac, slik at systemet kan bruke flate fingeravtrykk. Dette er gjort for å forenkle systemutvikling og anskaffelse av opptakssystemer blant Schengen-medlemslandene.

Dersom utlendingsregisteret flyttes over i et nytt fingeravtrykksregister hos Utlendingsdirektoratet, bør fingeravtrykkene i utlendingsregisteret sannsynligvis konverteres til flate fingeravtrykk, slik at fingeravtrykkene blir tilnærmet like med fingeravtrykkene fra VIS og oppholdskortene. Dette vil forenkle det biometriske søkesystemet.

En slik løsning, der det opptas flate fingeravtrykk i Utlendingsdirektoratets forvaltningssaker, vil medføre at politiet må ta opp to sett fingeravtrykk, ett sett som skal lagres og søkes mot Eurodac, og ett sett som lagres og søkes mot det nye registeret. Et alternativ er at politiet bare tar opp rullede fingeravtrykk og at fingeravtrykkene reduseres når de skal søke/lagre mot Utlendingsdirektoratets forvaltningsbase.

Et tredje alternativ er at biometrikiosken tilpasses slik at den kan ta opp både flate og rullede fingeravtrykk suksessivt, i samme operasjon uten at man må logge seg inn i et nytt system og gjøre nye registreringer for å få tatt opp biometri.

5.3 Det bør opprettes et nytt system for opplæring

Den identiteten som biometrien skal knyttes opp mot, må kontrolleres grundig. Dersom en utlending fremviser

falsk legitimasjon eller legitimasjon med lav notoritet, kan det senere vise seg at personen ikke er den han eller hun utga seg for å være. Dette krever at førstelinjetjenesten, enten det er politiet eller ansatte på norske utenriksstasjoner, har høy kompetanse for å foreta identitetsvurderinger, slik at personinformasjonen knyttet til biometrien blir nøyaktig og korrekt.

I kartleggingen kom det frem at mange ønsker seg mer og bedre opplæring. De vi intervjuet, kom inn på opplæring på en rekke områder, inkludert dokumentundersøkelser og identitetsarbeid. For dette prosjektets del kan vi trekke ut at kunnskapen omkring opptak og bruk av fingeravtrykk og foto var tilfredsstillende. Likevel var det en del usikkerhet om hva som lagres hvor, samt regelverket rundt fingeravtrykk og foto.

Noen ønsket bedre opplæring i å ta gode fingeravtrykk, slik at kvaliteten på opptaket blir så bra som mulig. Enkelte var usikre på når man har hjemmel til å ta fingeravtrykk, samt i hvilke systemer det er mulig å søke. Vi la for eksempel merke til at kjennskapen til VIS var svært lav. Det ble også bemerket at identitetsarbeid ikke er et tema man får undervisning i på Politihøgskolen.

Med nytt utstyr må det følge god opplæring. Vi har sett at utstyr i dag ikke blir brukt, fordi de ansatte ikke er sikre på hvordan det skal brukes. På grunn av stor mobilitet enkelte steder, både i politiet og i førstelinjen for øvrig, er det viktig at denne informasjonen ikke bare ligger hos én person.

Nasjonalt ID-senter anbefaler derfor at det opprettes et nytt opplærings-system i utlendingsforvaltningen som også ivaretar opplæring innen biometri, regelverk og utstyr. Ansvaret bør plasseres i én funksjon eller rolle hos de ansatte.

I tillegg kan det for eksempel avholdes jevnlig regionale samlinger i Norge slik at flest mulig av de som arbeider et sted, får anledning til å delta i sitt nærmiljø. Dette vil også kunne bidra til at de ansatte i førstelinjen får et bedre kontaktnett som de kan bruke i tvils-saker.

Når det gjelder utenriksstasjoner, er det viktig at spesielt de lokalt ansatte får god opplæring. Lokalsatte ved norske utenriksstasjoner bytter sjeldnere jobb enn de norske utsendte diplomatene.

Det kan gjerne benyttes e-læring eller ressurser på Internett, fortrinnsvis på lukkede områder, for eksempel portalen KO:DE¹⁰⁰ for politiets del, Nasjonalt ID-senters portal¹⁰¹ for hele utlendingsforvaltningen eller Utenriksdepartementets hjemmesider.

Samtidig er det svært viktig at de ansatte i førstelinjen gis den tiden som er nødvendig for å foreta denne kontrollen.

5.4 Tekniske løsninger og systemer

Det bør legges til rette for bedre og færre systemer for politiet å forholde seg til, og integrasjonen mellom systemene bør bli bedre. I kartleggingen kom det frem at politiet har svært

100. Kompetansedelingsportalen for politiet – KO:DE.

101. www.nidsenter.no

mange systemer å forholde seg til. De må logge seg inn i flere systemer for å få utført ulike oppgaver i forbindelse med behandling av en og samme sak. I tillegg til at dette naturligvis oppleves ineffektivt og frustrerende i en travel arbeidshverdag, byr det også på utfordringer i form av kompetanse og opplæring. For å begrense opplærings- og kompetansebehovet noe anbefaler Nasjonalt ID-senter at systemene bak grensesnittene integreres bedre, slik at man for eksempel kan foreta søk i ulike registre fra samme grensesnitt, både når det gjelder straffesaker og forvaltningssaker. Dette avhenger av at det gis hjemler for tilgangsstyring.

Nytt utstyr og bedre utnyttelse av eksisterende utstyr

For å kunne utnytte biometri som allerede er lagret, og for å kunne gjennomføre punktene over, er det avgjørende at politiet og førstelinjetjenesten for øvrig får tilstrekkelig, og godt utstyr.

Som nevnt i kapittel 4 vil det være mulig å ta opp fingeravtrykk av bedre kvalitet ved å benytte dyp-skanningsutstyr, for eksempel det tidligere omtalte Lumidigm. Lumidigm benytter en såkalt MSI-teknologi (Multispectral Fingerprint Image Aquisition) som tar flere bilder av fingeren med lys på forskjellige bølgelengder og fra ulike vinkler. I Sverige benytter de dette hvis de ikke får gode nok fingeravtrykk med det vanlige utstyret de bruker. Migrationsverket har lagt frem tall som viser at de med vanlig utstyr får beskjed fra Eurodac om at fingerav-

trykkene var for dårlige til å kunne utføre søk, i 10 % av sakene. I disse sakene tas fingeravtrykkene opp på nytt med Lumidigm, og de får da god nok kvalitet i 85 % av sakene som tidligere ikke ville gjennomgått søk i Eurodac.¹⁰²

I kartleggingen kom det frem et ønske om at biometrikioskene kunne brukes til både opptak og søk av biometri. Ettersom utstyret allerede fungerer for opptak av fingeravtrykk, kunne det være hensiktsmessig om det ble tilrettelagt ytterligere funksjoner slik at det var mulig å søke opp mot Eurodac, VIS og utlendingsregisteret og eventuelt andre registre. Det vil også være bedre kundeservice om politiet kunne benytte biometrikioskene til fingeravtrykkssøk i stedet for å ta den som skal kontrolleres, med til arresten, der de har det rette utstyret.

I kartleggingen så vi også at systemene er lagt opp på en måte som medfører en del dobbeltarbeid. Ettersom søket via Biometra går både til kriminalregisteret og utlendingsregisteret, burde det være mulig å oppta fingeravtrykkene bare én gang for å søke i begge registrene.

Politiet har som nevnt flere hjemler for identifisering og verifisering med fingeravtrykk mot VIS, men de mangler utstyr og integrasjon for å utføre dette i dag. Nasjonalt ID-senter anbefaler derfor at arbeidet med denne tilgangen blir prioritert og at dette implementeres så raskt som mulig.

5.5 Pilotprosjekter

Pilotprosjekt om bruk av ansiktsgjenkjenning for verifisering og identifisering

Nasjonalt ID-senter anbefaler at det gjennomføres et pilotprosjekt om bruk av ansiktsgjenkjenning for verifisering og identifisering. Ved ansiktsgjenkjenning benyttes metoden for sammenligning som ble forklart i punkt 2.2.

I dag foregår alle sammenligninger av foto i utlendingssaker manuelt. Som vi så i kapittel 4, benyttes enkelte ganger kommersielle programmet for ansiktsgjenkjenning i straffesaker, men dette kan ikke tillegges avgjørende vekt og benyttes kun som en hjelp i videre etterforskning.

Kripos kan benytte seg av et ansiktsgjenkjenningssystem i straffesaker, men det er ikke anledning til dette i forvaltningssakene. Kripos fremmer et forslag om muligheten for bruk av ansiktsgjenkjenning også i forvaltningssaker.

Ettersom det tas eller innleveres foto i alle utlendingssaker, finnes det allerede et stort datamateriale som kan benyttes i et pilotprosjekt.

Ansiktsgjenkjenning vil kunne benyttes for identifisering ved å ta et foto av en utlending, og benytte dette for søk i UDB. Ved treff vil man kunne knytte vedkommende til én eller flere identitet(er) som tidligere er innrullert i databasen.

102. Jan Westmar. Presentasjon for Sverige, GDISC-møtet, Paris 22.03.12.

103. Dobbelgjenger eller «look-alike». En person som ligner på, og utgir seg for å være, en annen.

Et ansiktsgjenkjenningsprogram vil også kunne avsløre en imposter¹⁰³ ved verifisering. I en grensekontroll eller kontroll på territoriet er man ofte mest opptatt av å undersøke om den personen som står foran en, er den han sier han er. Da vil man sjekke om ansiktet på identitetsbeviset og ansiktet på personen er det samme. Dette kan være vanskelig å se, og da er det greit å ha en automatisk tilleggskontroll som utfører ansiktsgjenkjenning. Denne teknologien benyttes i dag i såkalt ABC – automatisk grensekontrollsystem. Det vil være mulig å knytte et slikt system opp mot en database, slik at man kan identifisere personer. Systemet kan også være frittstående og benyttes utelukkende til verifisering på stedet.

Det tyske «Federal Office for Information Security» presenterte på Norsk Biometriforum en oversikt over åtte europeiske land som benytter slik ABC i dag. Av disse var det bare ett som kun benyttet fingeravtrykk, resten benyttet ansiktsgjenkjenning for verifisering. Estland brukte begge identifikatorene.¹⁰⁴ På Oslo Lufthavn Gardermoen gjennomfører Politiets data- og materiellteneste et pilotprosjekt med ABC i grensekontrollen for kontroll av statsborgere fra Schengen-området. I pilotprosjektet blir verifiseringen gjennomført ved automatisk sammenligning av person og bilde lagret i RFID-brikken i passet.

Pilotprosjekt eller utredning om bruk av håndholdt mobilt utstyr ved utlendingskontroll

Man ville oppnådd enda bedre service og effektivitet dersom patruljer

hadde håndholdt utstyr for opptak av for eksempel fingeravtrykk og foto. Da ville man både kunne kontrollere flere, samtidig som opplevelsen av å bli kontrollert kunne blitt bedre. Som vi viste i kapittel 4, vil en patrulje som skal foreta en identitetskontroll av en utlending som ikke kan legitimere seg, ofte ta et bilde av den som kontrolleres, med en mobiltelefon. Dette bildet sendes deretter til operasjonssentralen som slår opp personen i et system, for eksempel DUF. Sentralen gjør så et alfanumerisk søk og søker med de personalia han eller hun opplyser å være registrert med. Dersom de finner en person med disse personalia i UDB, vil de så sammenligne mobilbildet og bildet i UDB, og vurdere om det er samme person.

Ved å knytte identiteten til biometri ville det være tilstrekkelig å ta opp fingeravtrykket i kontrollen og deretter søke opp mot et system. Det samme gjelder dersom man kunne benytte ansiktsgjenkjenning for verifisering og identifisering.

Nasjonalt ID-senter anbefaler at det gjennomføres et pilotprosjekt eller en utredning om bruk av håndholdt mobilt utstyr ved utlendingskontroll. Utstyret bør ha en søkefunksjon som kan utnytte biometri for søk opp mot blant annet utlendingsregisteret, UDB og folkeregisteret.

5.6 Politiets rutiner for samhandling internt og eksternt bør forbedres

Ut fra funnene i kartleggingen anbefaler Nasjonalt ID-senter at politiets rutiner for samhandling

internt og eksternt forbedres og kodifiseres. Vi ser at særlig desken og SIRENE-kontoret på Kripos, desken i Politiets utlendingsenhet og Romerike politidistrikt Gardermoen benyttes mye for å gi informasjon og assistanse til politidistrikter over hele landet. I tillegg benyttes samarbeidspartnere som Tollvesenet, Skatteetaten og andre. Denne kontakten er viktig fordi mange aktører som ikke selv har spisskompetanse på utlendingskontroll, er de som faktisk påtreffer utlendingen. Det er derfor svært viktig at rutinene rundt kontakten er gode. Nasjonalt ID-senter anbefaler at rutinene for samarbeid konkretiseres i form av rundskriv eller instruksjer. Rutinene bør ta for seg eksternt og intern samhandling for utlendingsmyndighetene ved utlendingskontroll.

104. Mark Nuppency, presentasjon på Norsk Biometriforum 08.11.12.

Ordliste

Alfanumerisk søk: Dette er et søk gjort med både tall og bokstaver, for eksempel navn og fødselsdato.

Alias(registrering): Dette viser til registrering av én person flere ganger i et system ved at personen har oppgitt ulike navn (alias). Årsaken til dette kan være at personen oppgir ulike navn og nasjonaliteter ved ulike anledninger.

Andrelinje (dokumentkontroll): Andrelinjen er høyt kvalifiserte dokumentgranskere med avansert utstyr for ekthetsvurdering og tilgang på referansedokumenter. Det finnes andrelinje hos Politiets utlendingsenhet, større politidistrikter og på enkelte flyplasser. De samarbeider ofte tett med førstelinjen.

Autentisering: Autentisering viser til en del av samhandlingen mellom datasystemer i en verifiseringsprosess.

Bona fide: Bona fide betyr i god tro; ærlig og redelig. Uttrykket brukes ofte i utlendingssaker der det absolutt ikke er grunn til tvil.

C-visum: Schengen-visum, jf. utlendingsloven § 10.

Dobbeltregistrering: Dette viser til registrering av én person flere ganger i et system på grunn av feilregistrering. Årsaken kan for eksempel være at man transkriberer et navn ulikt: Mohammad/Muhamed.

Dublin-samarbeidet: Dublin-samarbeidet går ut på at en asylsøknad bare skal behandles i ett av de 29 medlemslandene: Belgia, Bulgaria, Danmark, Estland, Frankrike, Finland, Hellas, Irland, Island, Italia, Kypros, Latvia, Litauen, Luxemburg, Malta, Nederland, Norge, Polen, Portugal, Romania, Slovakia, Slovenia, Spania, Storbritannia, Sverige, Tsjekkia, Tyskland, Ungarn og Østerrike. Asylsøknaden fra en tredjelandsborger skal behandles av det medlemslandet der søkeren først har søkt asyl, fått oppholdstillatelse, fått visum eller er tatt for ulovlig grensepassering.

D-visum: Dette er et innreisevisum, jf. utlendingsloven § 12. Norge gir D-visum til personer som har fått innvilget en søknad om oppholdstillatelse, og som skal reise til Norge. Dette visumet er gyldig i inntil 90 dager. D-visum kan også gis til enkelte søkere som skal oppholde seg i Norge mens de venter på at en søknad om oppholdstillatelse skal behandles.

E-pass: Dette er nyere elektroniske pass som inneholder biometri i form av foto og fingeravtrykk som kan leses elektronisk.

Førstelinje: Førstelinjen i utlendingsforvaltningen er den første kontakten en person har med norske myndigheter. Førstelinjen veileder og jobber med forvaltningsoppgaver knyttet til søknadsbehandlingen av utlendingssaker.

Disse utføres i dag hovedsakelig av politiet, Utlendingsdirektoratet og på utenriksstasjonene.

Hurtigsøk: Dette er et søk i Eurodac som gjøres ved opptak av fingeravtrykkene på fire fingre, begge tomlene og begge pekefingrene. Søket sendes til Eurodac, og fingeravtrykkene skal ikke lagres. Det er ikke anledning til å utføre hurtigsøk ved asylregistrering eller ved ulovlig grensepassering.

ICAO (International Civil Aviation Organization):

Den internasjonale organisasjonen for sivil luftfart er en organisasjon som er opprettet av FN. ICAO er en styrende myndighet innen luftfart og sørger for å utvikle luftfarten på en sikker og effektiv måte. ICAO er ansvarlig for å utarbeide og følge opp standardisering innen luftfart. Et av ICAOs ansvarsområder har vært å utarbeide en standard for maskinlesbare pass.

Identifisering: Identifisering er en prosess for å finne ut av identiteten til en person når den ikke er tilkjennegett. Dette er med andre ord en «én-til-mange»-sammenligning.

Imposter: Dette viser til en dobbeltgjenger eller «look-alike», altså en person som ligner på, og utgir seg for å være, en annen.

Innrulling: I vår sammenheng viser innrulling til prosessen med å samle inn biometriske prøver fra en person og den påfølgende bearbeidingen og omgjøringen av biometrisk originaldata til en mal som så lagres i et biometrisk system. Prosessen kan deles inn i fire trinn: innsamling, behandling, lagring og sammenligning. Det er de tre første prosessstrinnene innsamling, behandling og lagring som utgjør innrulling.

ISO (International Organization of Standardization):

ISO er en internasjonal standardiseringsorganisasjon som utgir standarder på en rekke områder.

Lumidigm: Dette er en dypskannervariant som leser flate fingeravtrykk, også når avtrykkene av ulike årsaker blir dårlige, for eksempel ved slpite fingertupper. Lumidigm benytter en såkalt MSI-teknologi (Multispectral Fingerprint Image Acquisition), som tar mange bilder av fingeren med lys på forskjellige bølgelengder og fra ulike vinkler.

MRZ (Machine Readable Zone): Dette er den

maskinlesbare sonen i dokumenter. Sonen kan skannes og kontrolleres automatisk.

Notoritet: Notoritet er det samme som etterprøvbarehet. Et dokument som utstedes på bakgrunn av gode rutiner, og som inneholder etterprøvbare opplysninger, har notoritet.

Oppholdskort: Det Schengen-standardiserte oppholdskortet er et bevis på oppholdstillatelse.

PKI (Public Key Infrastructure): PKI er et rammeverk for identifisering, signering samt kryptering og sikkerhet innen elektronisk kommunikasjon.

Reisebevis: Reisebevis for flyktninger gis til en utlending som har fått oppholdstillatelse og flyktningstatus i Norge.

RFID (Radio Frequency Identification / radiofrekvensidentifikasjon): Data lagres i en brikke som kan avleses enten ved kontakt eller fjernavleses. RFID-brikker brukes i oppholdskort, pass og reisebevis.

Signalering: Signalering er signalementsrapporteringen i politiet som innebærer registrering av persondata og opptak av foto og fingeravtrykk.

Template (mal): Biometrisk informasjon kan lagres i form av en template. Dette er en kodebasert representasjon av materialet, i stedet for å lagre en hel måling (for eksempel et fullt bilde av fingeravtrykket) med alle detaljer.

Tiltakskort: Tiltakskort er en standardisert sjekkliste/handlingsplan/huskeliste for tiltak som skal settes i gang ved spesielle situasjoner. Kortene blir brukt innen offentlig sektor, spesielt i HMS- og beredskapsarbeid.

Tredjelandsborger: Begrepet viser til en person som kommer fra et land utenfor EU-, EØS- eller EFTA-området.

Utlendingspass: Dette er et reisedokument som gis til en utlending med oppholdstillatelse i Norge, men som ikke har fått flyktningstatus.

Verifisering: I vår sammenheng viser verifisering til en prosess for å forsikre seg om at en person er den han eller hun utgir seg for å være. Dette er med andre ord en «én-til-én»-sammenligning.

Systemer:

AFIS (Automated Fingerprint Identification System): AFIS er et dataverktøy for å automatisk gjenkjenne og sjekke fingeravtrykk opp mot fingeravtrykk som er lagret i en database. De fleste land har nasjonale databaser der fingeravtrykk lagres.

Biometra: Biometra er en portal som politiet bruker til å oppta signalement, personfoto og fingeravtrykk som videresendes til Kripos via politinettet.

BL: BL står for basisløsninger. BL er et saksbehandlingssystem i politiet. I BL registreres opplysninger som er nødvendige ved behandlingen av en straffesak, helt fra en sak er anmeldt, til den er avsluttet. Alle opplysninger tjenestemennene produserer i saken, skal registreres i BL. Personopplysninger som ligger i systemet, er søkbare, og en bruker får tilbakemelding dersom flere saker er registrert på samme person. BL er i et lokalt register. En del av informasjonen overføres imidlertid til de sentrale registrene Strasak, Elys og Bot.

DUF: Dette er et datasystem for utlendings- og flyktningsaker. Utlendingsforvaltningen benytter DUF i saksbehandlingen. DUF ble tatt i bruk i 2003 og erstattet det gamle systemet FREMKON.

ELYS II: Dette er politiets sentrale etterlysningsregister som blant annet omfatter etterlyste personer, kjøretøy, kjennetegn, våpen, pass, båter og båtmotorer.

Eurodac: Eurodac er et sentralt elektronisk fingeravtrykkregister over utlendinger (hovedsakelig asylsøkere) som er registrert i et land som deltar i Dublin-samarbeidet. Registeret gir bare mulighet til å sammenligne fingeravtrykk etter Dublin II-forordningen. Formålet med registeret er å finne ut om en asylsøker tidligere har søkt beskyttelse i et annet land som er tilknyttet Eurodac. Eurodac ble opprettet etter rådsforordning nr. 2725/2000.

Europol (European Police Office): Europol er den europeiske unions organisasjon for politisamarbeid i EU for å bekjempe internasjonal organisert kriminalitet og terrorisme. Organisasjonens hovedmål er å bistå de nasjonale politimyndighetene ved å utveksle etterretningsrapporter og bistå med analyse og faglig ekspertise. Europol samarbeider med en rekke organisasjoner og land utenfor EU, blant annet Norge.

Fingeravtrykkregisteret: Politiets alminnelige fingeravtrykkregister er delt inn i utlendingsregisteret og det kriminale fingeravtrykkregisteret. I utlendingssaker blir

fingeravtrykkene registrert i utlendingsregisteret, mens en person som blir dømt til straff, registreres i det kriminale fingeravtrykkregisteret. Kripes er databehandler.

GDISC (General Directors' Immigration Service Conference): GDISC er et nettverk med 33 medlemsland i Europa, se www.gdisc.org.

GK (Grensekontrollsystemet): GK er grensekontrollens saksbehandlingssystem eller grensekontrollapplikasjon. I GK kan man blant annet kontrollere både passet og visumet, undersøke om den som kontrolleres, er etterlyst i Norge eller Schengen-området, registrere inn- og utreise for visumpfiktige reisende og verifisere Schengen-visumet i VIS.

Indicia: Dette er politiets kriminaletterretningsregister. Politidirektoratet og Kripes har delt behandlingsansvar for registeret. Indicia erstatter de gamle systemene Krimsys og Usys samt de lokale etterretningsregistre i politidistriktene.

KO:DE: Dette er politiets kompetansedelingsportal.

NORVIS: Norvis er utlendingsforvaltningens visumsystem. Systemet benyttes av utenriksstasjonene og Utlendingsdirektoratet for saksbehandling av visumsaker. Norvis er integrert i SIS og vil bli integrert i Schengens VIS-system. Norvis er registreringsverktøyet for data som lagres i den nasjonale visumdatabasen.

Pass Web: Dette er en saksbehandlingsskript som der data for passøknader sendes til produksjon av pass og for lagring i passregisteret.

PO-logg: PO-loggen er politioperativ logg – et internt datasystem og arbeidsredskap.

SIS II (Schengen Information System): SIS II er et felles elektronisk informasjonssystem som skal sikre en rask og sikker utveksling av opplysninger mellom Schengen-landene. Informasjonssystemet er todelt. Det består dels av en sentral base og teknisk støttefunksjon lokalisert i Strasbourg i Frankrike (C-SIS), dels av nasjonale registre som opprettes og drives av det enkelte Schengen-landet.

SSP (det sentrale straffe- og politiopplysningsregisteret): I SSP registrerer politiet og påtalemakten personopplysninger i forbindelse med forebygging og etterforskning av lovbrudd og straffefølgelse av lovbrøyttere. Registeret gir et overblikk over følgende:

- straffereaksjoner som er gitt, gjennomføring av straff og andre reaksjoner
- pågripelser, varetekt og løslatelser

- hvem som er registrert med fingeravtrykk, foto og DNA, og signalementet til de som er registrert

Strasak: Dette er politiets sentrale straffesaksregister, som inneholder alle registrerte straffbare handlinger, eventuelt med navn på mistenkte, fornærmede osv. Strafferegisteret inneholder navn med reaksjon på alle som er domfelt eller bøtelagt for en forbrytelse.

UDB (Utlendingsdatabasen): Dette er en database for alle saker som gjelder søknad om besøk og opphold i Norge samt om de som oppholder seg i asylmottak. Databasen oppdateres av og gir data til flere datasystemer, blant annet DUE, GK og NORVIS.

Utlendingsregisteret: Dette er en separat fil i det alminnelige fingeravtrykkregisteret der man registrerer fingeravtrykkene til utlendinger som søker om beskyttelse i Norge, utlendinger som ikke kan dokumentere sin identitet, eller de det er grunn til å mistenke at oppgir falsk identitet, og utlendinger som blir utvist eller bortvist fra Norge. Utlendingsdirektoratet er behandlingsansvarlig for utlendingsregisteret, og Kripes er databehandler.

VIS (Visa Information System): VIS er forkortelsen for Schengens visum informasjonssystem. VIS består av to hoveddeler, et sentralt system (CS-VIS) med en database i Strasbourg, og medlemsstatenes nasjonale systemer (N-VIS), som kommuniserer med det sentrale VIS-systemet. Norvis er Norges N-VIS-system.

Kilder

Bok

Liu, Nancy Yue. (2012) Privacy regulations and the challenge of biometrics. Oxon. Routhledge.

Lover

Utlendingsloven (2008) Lov om utlendingers adgang til riket og deres opphold her.

Personopplysningsloven (2001) Lov om behandling av personopplysninger.

Forskrifter

Utlendingsforskriften (2010) Forskrift om utlendingers adgang til riket og deres opphold her.

Stortingsmelding

Justis- og beredskapsdepartementet (2010) Norsk flyktning- og migrasjonspolitik i et europeisk perspektiv. St.meld. nr. 9 (2009–2010). Oslo. Justis- og beredskapsdepartementet. Tilgjengelig på www.regjeringen.no.

Rundskriv

Utlendingsdirektoratets rundskriv, RS 2010-019. Gjennomførende rutiner i tilknytning til Eurodac-forordningen.

Tilgjengelig på www.udiregelverk.no.

Departementenes rundskriv G-16/2010. Ikraftttredelse – endring av utlendingsforskriften § 18-4 om sletting av fingeravtrykk (2010).

Politidirektoratets rundskriv 2012/005: Politiets arbeid med søknader om beskyttelse (asyl), identifisering og uttransportering av utlendinger etter utlendingsloven.

Direktiv

EUs personverndirektiv (95/46/EF).

Forordninger

Dublin II-forordningen, EUs rådsforordning nr. 343/2003/EF.

Eurodac-forordningen, EUs rådsforordning nr. 2725/2000/EC.

Visumforordningen, Europaparlamentets- og Rådsforordning (EF) nr. 810/2009.

VIS-forordning 767/2008: Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation).

Ot.prp.

Ot.prp. nr. 92(1998–1999). Om lov om behandling av personopplysninger. Personopplysningsloven.

Rådsbeslutning

Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention,

detection and investigation of terrorist offences and of other serious criminal offences.

Council Regulation No 2725/2000 of 11 December 2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention, Article 5.

Konvensjoner

Europarådets konvensjon om personvern i forbindelse med elektronisk behandling av personvernopplysninger (1981) (Convention for the Protection of Individuals with regard to automatic processing of personal data).

Upublisert materiale/rapport

Utlendingsdirektoratet (UDI). 2010 Rapport om utvidet bruk av biometri i utlendingsforvaltningen.

Westmar, Jan. Migrationsverket. Presentasjon for Sverige, GDISC-møtet. Paris, 22.03.2012.

Nuppeney, Mark. Norsk Biometriforum. Presentasjon. Oslo, 08.11.2012.

Nettsider

Utlendingsdirektoratets internmelding IM 2012-020.

<https://www.udiregelverk.no/no/rettskilder/udi-interne-meldinger/im-2012-020/> [Lastet ned 15.januar 2013].

Nasjonalt ID-Senter. Kartleggingsprosjektet. Tilgjengelig på https://www.nidsenter.no/Global/Dokumenter/Sluttrapport_kartleggingsprosjektet2011.pdf. [Lastet ned 02.01.13.]

Nasjonalt ID-senters instruks: Tilgjengelig på <http://www.nidsenter.no/Global/Om%20NID/Endelig%20NID-instruks%2015.11.2010.pdf> [Lastet ned 14.01.13].

Politiets utlendingsenhetens årsmelding 2011. Tilgjengelig på https://www.politi.no/vedlegg/lokale_vedlegg/politiets_utlendingsenhet/Vedlegg_1800.pdf [Lastet ned 02.01.13].

Rommetveit, Kjetil: "Biometri" (Sist oppdatert: 16.11.11). De nasjonale forskningsetiske komiteer. Tilgjengelig på <http://www.etikkom.no/FBIB/Temaer/Forholdet-forskningssamfunn/Biometri/>. [Lastet ned 18.12.12].

Andre EU-dokumenter

European Data Protection Supervisor, «Eurodac». Tilgjengelig på: <http://www.edps.europa.eu/EDPSWEB/edps/Supervision/Eurodac/> [Lastet ned 25.01. 2013].

European Data Protection Supervisor, Inspection of Eurodac Central Unit Summary Report 13 June 2012. Tilgjengelig på: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/12-06-13_EURODAC_Inspection_EN.pdf Lastet ned 25.01.13].

Article 29 Data Protection Working Party, Working Document on Biometrics (wp80) 12168/02/En wp 80.

Article 29 Data Protection Working Party, wp 193, Opinion 3/2012 on Developments in Biometric Technologies. 00720/12/en wp 193.

Vedlegg

Tabell 2

Tabellen gir en oversikt over gjeldende regler for søk eller verifisering basert på fingeravtrykk. Samtidig angis den applikasjonen som brukes for å ta opp og sende data til den aktuelle databasen.

SØK ADGANG ----- Applikasjon	OPPHOLDSØKNAD Utenriksstasjonene	VISUMSØKNAD Utenriksstasjonene	GRENSEKONTROLL PD i funksjon grensekontroll	INNLANDSKONTROLL PD	ASYLSØKNAD PU (PD hvis søknad fremmes lokalt eller på grensa)
UTLENDINGS- REGISTERET	utl. § 100 jf. utf. § 18-3 jf. § 18-1 bokstav a, b og d. For identifisering Applikasjon: BIOMETRA Ikke tilrettelagt for utenriksstasjonene	Ikke adgang	utl. § 15 og utf. § 18-3 jf. § 18-1 bokstav a. For identifisering	utl. § 21 og utf. § 18-3 jf. § 18-1 bokstav a, e, f og g. For identifisering	utl. § 100 og utf. § 18-3 jf. § 18-1 bokstav a og b. For identifisering
EURODAC	Ikke adgang	Ikke adgang	Ikke adgang til søk jf. EURODAC- forordningen art. 9. Kun mulig å overføre og lagre data utelukkende for sammenligning av fingeravtrykk dersom utlendingen senere skulle søke asyl	EURODAC- forordningen art. 11 og utl. § 21. For identifisering	EURODAC- forordningen art. 4 og utl. 15. For identifisering
VIS	Ikke adgang	VIS-forordningen art. 15. For identifisering	VIS-forordningen art. 18 For verifisering, art. 20 For identifisering	Applikasjon: BIOMETRA	
				VIS-forordningen art. 19 For verifisering, art. 20 For identifisering	VIS-forordningen art. 21 og 22.
		Applikasjon: NORVIS (Tilrettelagt, men ikke tatt i bruk)			
SCHENGEN- STANDARDISERT OPPHOLDSKORT	utl. § 100 a og b	Lite praktisk	utl. § 100 b første ledd jf. § 15. For verifisering av person opp mot kortdata	utl. § 100 b første ledd jf. 21. For verifisering av person opp mot kortdata	utl. § 100 b. For verifisering av person opp mot kortdata
			Applikasjon: DUF		

the 1990s, the number of people in the UK who are employed in the public sector has increased by 1.5 million (from 2.5 million in 1980 to 4 million in 1999). The public sector has also become an important employer of people with disabilities, with 1.5 million people with disabilities employed in the public sector in 1999, compared with 1.2 million in 1980.

There are a number of reasons why the public sector has become an important employer of people with disabilities. One reason is that the public sector has a long history of employing people with disabilities. In the 19th century, the public sector employed people with disabilities in a number of different roles, including as clerks, typists, and stenographers. In the 20th century, the public sector continued to employ people with disabilities in a variety of roles, including as teachers, nurses, and social workers.

Another reason why the public sector has become an important employer of people with disabilities is that it has a number of advantages over the private sector. For example, the public sector is often able to offer people with disabilities a more stable and secure employment environment than the private sector. This is because the public sector is often able to offer people with disabilities a more predictable and stable income, and a more secure job.

There are also a number of other reasons why the public sector has become an important employer of people with disabilities. For example, the public sector often has a number of policies in place that are designed to support people with disabilities in the workplace. These policies can include things like flexible working hours, and the provision of special equipment and facilities.

Overall, the public sector has become an important employer of people with disabilities in the UK. This is due to a number of factors, including its long history of employing people with disabilities, its advantages over the private sector, and its policies designed to support people with disabilities in the workplace.

There are a number of challenges that the public sector faces in its role as an employer of people with disabilities. One challenge is that the public sector often has a limited budget, which can make it difficult to provide the support and resources that people with disabilities need in the workplace. Another challenge is that the public sector often has a high level of turnover, which can make it difficult to build a stable and experienced workforce.

Despite these challenges, the public sector remains an important employer of people with disabilities in the UK. This is because the public sector has a number of advantages over the private sector, and it has a number of policies in place that are designed to support people with disabilities in the workplace. As a result, the public sector is likely to continue to be an important employer of people with disabilities in the future.

There are a number of ways in which the public sector can continue to improve its role as an employer of people with disabilities. One way is to increase its budget, so that it can provide the support and resources that people with disabilities need in the workplace. Another way is to reduce its level of turnover, so that it can build a stable and experienced workforce.

Overall, the public sector has a number of advantages over the private sector, and it has a number of policies in place that are designed to support people with disabilities in the workplace. As a result, the public sector is likely to continue to be an important employer of people with disabilities in the future.

Nasjonalt ID-senter

Besøksadresse: Møllergata 39

Postadresse: Postboks 8102 Dep, 0032 Oslo

Telefon: 22 69 90 22

E-post: postmottak@nidsenter.no

www.nidsenter.no

Org. nr: 996 879 828