



Bryssel den 29.2.2016
COM(2016) 93 final

RAPPORT FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

Tillgängligheten och driftklarheten för tekniken för identifiering av personer på grundval av fingeravtryck lagrade i andra generationen av Schengens informationssystem (SIS II)

1. INLEDNING

Det blir allt svårare att fastställa identiteten på personer på grund av att de byter namn, använder täcknamn eller förfalskade handlingar. Förfalskade handlingar används i ökande omfattning för att illegalt resa in i och röra sig inom Schengenområdet. I Frontex årliga riskanalys för 2015 rapporteras att det år 2014 upptäcktes omkring 9 400 fall av dokumentbedrägeri vid inresa till EU/Schengenområdet från tredjeland, vilket innebär en liten minskning jämfört med föregående år. Däremot har antalet rapporterade fall av rörelser i Schengenområdet inom EU ökat markant från 7 867 år 2013 till 9 968 år 2014 (+27 %).

Dokumentbedrägeri undergräver inte bara gränsskyddet utan även EU:s inre säkerhet. Personer som är eftersökta av polisen försöker ofta dölja sin identitet och använder flera täcknamn. Vissa personer som omfattas av inreseförbud till Schengenområdet kan lagligt ändra sin identitet i sitt hemland för att undvika upptäckt. Mot bakgrund av detta behövs en tillförlitlig metod för att fastställa personers identitet. Både gränskontrollpersonal och brottsbekämpande myndigheter skulle kunna använda fingeravtryck, vilket vore en effektiv metod för att identifiera personer som eftersöks av myndigheter och för att upptäcka fall av dokumentbedrägerier.

Bedrägerier med resehandlingar i samband med de nyligen inträffade terrorattackerna i Paris understryker också behovet av ett verktyg som ger möjlighet att identifiera personer med hjälp av fingeravtryck. I detta sammanhang betonades i rådets slutsatser från november 2015 vikten av att stärka övervakningen och utföra systematiska kontroller. Hittills har det i EU saknats ett övergripande system som möjliggör kontroll av personer med hjälp av fingeravtryck.

Den andra generationen av Schengens informationssystem (SIS) togs i drift den 9 april 2013. En ny funktion är lagring av fingeravtryck i det centrala systemet. För närvarande används fingeravtryck för att *bekräfta* identiteten på en person som hittats vid en sökning, oftast genom att få fram namn och födelsedatum. Detta är en sökning i förhållandet ”ett-till-ett”, dvs. den berörda personens fingeravtryck jämförs med en uppsättning fingeravtryck som finns lagrad i SIS. För att det ska bli möjligt att *identifiera* en person genom fingeravtryck behöver systemet dock utvecklas i linje med de rutiner som de brottsbekämpande myndigheterna tillämpar: en persons fingeravtryck jämförs här med samtliga uppsättningar av fingeravtryck (en sökning i förhållandet ”ett-till-många”) för att identifiera personen enbart genom fingeravtryck. För denna funktion krävs ett automatiskt fingeravtrycksidentifieringssystem (AFIS).

AFIS har använts framgångsrikt i många nationella databaser och databaser för gränsöverskridande samarbeten. Tydliga exempel inom EU är Informationssystemet för viseringar (VIS) och Eurodac.

I artikel 22 c i SIS II-beslutet¹ och i SIS II-förordningen² anges den rättsliga grunden för att använda AFIS. Innan denna funktion införs ska kommissionen lägga fram en rapport om huruvida den teknik som krävs är klar att tas i bruk och finns tillgänglig, och Europaparlamentet

¹ Rådets beslut 2007/533/RIF av den 12 juni 2007 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II).

² Europaparlamentets och rådets förordning (EG) nr 1987/2006 av den 20 december 2006 om inrättande, drift och användning av andra generationen av Schengens informationssystem (SIS II).

ska därefter höras om rapporten. Syftet med denna rapport är att tillgodose detta krav och bekräfta att tekniken för identifiering genom fingeravtryck finns tillgänglig och är klar att integreras i SIS II.

Teknikens driftklarhet och tillgänglighet måste bedömas mot bakgrund av den unika situationen kring och egenskaperna hos SIS II, vilket medför en rad tekniska och organisatoriska utmaningar som kräver lämpliga anpassade lösningar. Denna rapport, som stödjer sig på en undersökning gjord av kommissionens gemensamma forskningscentrum (JRC)³, beskriver också de tekniska och organisatoriska kraven kring SIS och i vilken typ av situationer fingeravtryck används operativt. Dessutom innehåller rapporten rekommendationer för att framgångsrikt införa en AFIS-funktion.

2. JRC:S STUDIE OCH DESS RESULTAT

I EU:s forskningsprogram Horisont 2020 (*Horizon 2020 EU Research and Innovation Framework Program*) beskrivs teknikens driftklarhet och tillgänglighet med en 9-gradig skala⁴: nivå 1 innebär att grundläggande principer efterlevs medan nivå 9 innebär att det finns system som fungerar i en driftsmiljö. AFIS-tekniken har redan uppnått nivå 9 och används i många system över hela världen.

2.1 Översikt över AFIS-tekniken

2.1.1 Prestanda

JRC presenterade en översikt över de viktigaste oberoende prestandautvärderingarna och identifierade de initiativ som var relevanta för SIS. Tre centrala principer kunde urskiljas:

- Precisionen hos ett automatiskt fingeravtrycksidentifieringssystem är helt beroende av de data som använts för bedömningen och kvaliteten på dessa data.
- Andra faktorer som kan påverka prestandan hos ett automatiskt fingeravtrycksidentifieringssystem är storleken på databasen där sökningar görs, antal fingeravtryck som används för sökningen och förväntad svarstid.
- Vid god datakvalitet och sökningar med matchningar av 10 mot 10 avtryck visar utvärderingar att AFIS-tekniken ger mycket hög precision, med felfrekvenser på runt 0,1 %.

2.1.2 Kvalitet

Många undersökningar och mätningar har visat att prestandan hos biometriska system är beroende av kvaliteten på de prover som undersöks. Kvalitetsförbättringar kan röra teknik, standarder eller till och med metoden för hur fingeravtrycken tas, d.v.s. elektronisk avläsning

³ <http://publications.jrc.ec.europa.eu/repository/handle/JRC97779>

⁴ https://ec.europa.eu/research/participants/portal/doc/call/h2020/common/1617621-part_19_general_annexes_v.2.0_en.pdf
http://ec.europa.eu/research/participants/data/ref/h2020/other/wp/2016-2017/annexes/h2020-wp1617-annex-ga_en.pdf

(med fingeravtrycksläsare) eller manuellt tagna bläckavtryck. Elektronisk avläsning som övervakas av en erfaren operatör är att föredra för att få den bästa kvaliteten. Bläckavtryck som läses in i databasen förekommer emellertid fortfarande. Systemen bör inbegripa metoder för att upptäcka fingeravtryck med dålig kvalitet.

Man bör genomgående fokusera på kvaliteten i

- hur fingeravtrycken tas,
- den tekniska bedömningen av fingeravtryckens kvalitet,
- de systembaserade lösningar som används för att säkerställa matchning,
- användningen av de bästa fingeravtrycken,
- övervakningen av prestandan i systemet och hos de personer som använder det.

Eftersom undersökningen var omfattande tog den också upp det område som kvalitetsmässigt utgör den största utmaningen, nämligen ”latenta” fingeravtryck som hittats på en brotts- eller olycksplats.

Latenta fingeravtryck används uteslutande för sökningar. Endast fullständiga 10-fingeravtrycksuppsättningar från kända personer förväntas lagras i SIS.

I de flesta medlemsstater som besöktes hanteras kvaliteten också med hjälp av ”flerdubbla datamängder”. Om personer har fått sina fingeravtryck tagna vid flera tillfällen, t.ex. varje gång de gripits, lagras avtrycken. De enskilda fingeravtrycken i uppsättningarna kan jämföras utifrån sina kvalitetspoäng, och en sammansatt uppsättning med avtryck kan sammanställas av de tio fingeravtryck som har den högsta kvaliteten. Ett sådant tillvägagångssätt skulle också kunna användas i SIS.

Det är viktigt att införa mekanismer för kvalitetsmätning i ett automatiskt fingeravtrycksidentifieringssystem för att förbättra dess prestanda. När det gäller kvalitet måste sex centrala principer beaktas:

- Prestandan hos ett automatiskt fingeravtrycksidentifieringssystem är helt beroende av kvaliteten på de data (d.v.s. fingeravtrycken) som matas in i systemet.
- Det finns många omständigheter som kan påverka fingeravtryckens kvalitet. Vissa kan kontrolleras (t.ex. att sensorn hålls ren) medan andra inte kan det (t.ex. att den person som införts i systemet har fingertoppar som nötts av manuellt arbete).
- Automatiska mekanismer för verifiering av kvaliteten på fingeravtryck spelar en viktig roll för att kontrollera kvaliteten på de data som läggs in i ett automatiskt fingeravtrycksidentifieringssystem.
- Olika typer av fingeravtryck har olika kvalitetsnivåer. De huvudtyper som ett automatiskt fingeravtrycksidentifieringssystem behöver kunna hantera är: bläckavtryck/elektroniskt avlästa, rullade/platta/latenta.
- Den största utmaningen för prestandan i ett automatiskt fingeravtrycksidentifieringssystem är data med latent fingeravtryck, eftersom deras kvalitet inte går att kontrollera.

- Även om det finns inte finns någon standard för mätning av fingeravtrycks kvalitet har *NFIQ* och *NFIQ-II* (*NIST Fingerprint Image Quality*) som utvecklats av NIST (*American National Institute for Standards and Technology*) blivit standarder som tillämpas i praktiken på grund av att de uppvisat mycket hög prestanda och tillgänglighet.

2.2 Gemensam användning av nationella AFIS

I undersökningen beskrevs de typiska användningsfallen för fingeravtryck. De fall som är viktigast för SIS syften gäller personer som är närvarande då fingeravtrycken tas, t.ex. när misstänkta har gripits. Två parametrar måste definieras:

- Lägsta förväntade precision i matchningsprocessen.
- Maximal tillåten svarstid.

Som exempel kan tas en misstänkt som gripits och förts till en polisstation där hans eller hennes fingeravtryck tas. Uppsättningen med tio fingeravtryck används för att söka i den centrala fingeravtrycksdatabasen. En matchande uppsättning med tio fingeravtryck hittas. Dessa fingeravtryck togs när den misstänkte greps vid ett tidigare tillfälle. Personen var närvarande när båda uppsättningarna med fingeravtryck togs, vilket innebär att en hög kvalitet kan förväntas. Eftersom den berörda personen kan kvarhållas under flera timmar är en snabb svarstid inte nödvändig.

Som ett motsatt exempel kan tas en snabbkontroll vid t.ex. säkerhetskontroller på flygplatser, där kanske bara två fingrar läses av.

Precisionen förväntas vara lägre vid denna kontroll, men man har fortfarande betydande kontroll över hur de två fingeravtrycken tas och vilka fullständiga uppsättningar med tio fingeravtryck som används som jämförelse. Eftersom personen inte är gripen förväntas en snabb responstid, troligen några sekunder snarare än minuter. Om en matchning görs kan en fördjupad kontroll utföras genom en fullständig sökning med tio fingeravtryck.

2.3 Eurodac och VIS

För att inhämta eventuella lärdomar som kan tillämpas i SIS undersöktes två befintliga EU-system som använder AFIS.

I eu-LISAs årsredovisning för 2014 anges att Eurodac innehöll sammanlagt 2,7 miljoner fingeravtrycksposter (10-fingeravtrycksuppsättningar), och totalt 756 368 transaktioner ägde rum. På grund av inbyggda kvalitetsrutiner underkändes 4,49 % som undermåliga, vilket innebär att de behövde tas om och läggas in på nytt. Databasens storlek ligger nära kapacitetsgränsen för SIS, men antalet transaktioner är mycket mindre och svarstiderna mycket längre än vad som skulle krävas för SIS – en brådskande jämförelse i Eurodac utförs inom en timme medan förväntad tid i SIS skulle vara några sekunder p.g.a. att användningssituationerna är helt annorlunda.

VIS innehåller runt 20 miljoner fingeravtrycksposter (10-fingeravtrycksuppsättningar). VIS används normalt för identitetskontroll vid gränser, d.v.s. är denna person den ursprungliga viseringssökanden? Men VIS används också för att utföra en-till-många-sökningar för nya viseringssökande och vid fördjupade gränskontroller med fullständiga 10-fingeravtryckssökningar. I genomsnitt görs 20 000 till 30 000 sådana identifieringar varje dag med en toppbelastning på 3 000/timme. Den förväntade svarstiden för en identifiering är mindre än tjugo minuter (mindre än tre sekunder för en ett-till-ett-kontroll med avtryck från ett till fyra fingrar vid en typisk gränskontroll).

2.4 AFIS i medlemsstater och tredjeland

Undersökningen visade att ett automatiskt fingeravtrycksidentifieringssystem som används av nationell kriminalpolis i medlemsstaterna kan vara mer omfattande än den förväntade storleken på det automatiska fingeravtrycksidentifieringssystemet i SIS, eftersom en stor mängd registerposter sparas där. De två systemen som undersöktes i USA innehåller tiotals miljoner poster. SIS kan bara lagra fingeravtryck för personregistreringar. Den 1 januari 2015 fanns det strax under 800 000 personregistreringar i SIS.

2.5 Utmaningar vid införandet av AFIS-teknik

Utmaningarna vid införandet av AFIS-teknik kan sammanfattas som följer:

- användningsfall
- prestanda
- kvalitet
- hastighet (svarstid)
- databasstorlek
- matchningskapacitet
- antal transaktioner/matchningar vid toppbelastning
- strategi för att hantera frågor
- format för datautbyte
- systemarkitektur: centraliserad eller lokaliserad på flera platser
- typ av data som behandlas – fingeravtrycksformat
- latent fingeravtryck

2.6 Slutsatser

Som anges i inledningen av detta kapitel finns tekniken tillgänglig och är redo att tas i bruk. Kommissionen har också lyft fram de utmaningar som behöver hanteras. Rekommendationerna för ett framgångsrikt införande och för att möta dessa utmaningar beskrivs i kapitel 4.

3. AFIS I SIS

Det automatiska fingeravtrycksidentifieringssystem som införs i SIS måste kunna hantera alla typer av fingeravtrycksregistreringar som kommer att utföras. Dessa registreringar omfattar följande:

- platta och rullade fingeravtryck,
- snabbkontroller där t.ex. endast två fingrar avläses,
- latent fingeravtryck som samlats in på en brottsplats.

3.1 Uppgiftsskydd

Behandling av fingeravtryck i SIS II, inklusive lagring och användning i identifieringssyfte, måste uppfylla de relevanta bestämmelser om uppgiftsskydd som finns i rättsakterna för SIS II och i tillämpliga nationella bestämmelser om uppgiftsskydd i koppling till dataskyddsdirektivet 95/46/EG⁵ och rambeslut 2008/977/RIF⁶. Båda rättsakterna är tillämpliga i fråga om behandling av fingeravtryck av såväl medborgare från tredjeland som medborgare i EU. Samtliga användningssyften för fingeravtryck ska vara godkända enligt unionsrätten eller lagstiftningen i medlemsstaterna. I enlighet med syftesprincipen måste syftet med fingeravtrycken i SIS II tydligt definieras, liksom även sättet att använda dem. Fingeravtryck ska inte bearbetas utöver vad som är nödvändigt för det allmänintresse som eftersträvas. Dessutom ska bearbetningen av fingeravtryck vid behov vara föremål för lämpliga skyddsåtgärder. Vid införandet av dessa nya funktioner i SIS II bör bestämmelserna för uppgiftsskydd följas rent standardmässigt, liksom även i fråga om principerna för hur de berörda funktionerna utformas.

3.2 Användningssituationer för fingeravtryck i SIS

Två typer av fingeravtryckstransaktioner kan förutses i SIS:

- En registrering skapas/uppdateras och fingeravtryck läggs till.
- En sökning görs i SIS-databasen med hjälp av fingeravtryck i stället för namn och födelsedatum. En sådan sökning sker också innan en ny registrering utförs för att kontrollera om personen redan finns i någon annan registerpost i SIS.

Fingeravtryck måste bifogas till SIS-registreringen om de finns tillgängliga. De situationer då fingeravtryck kan påträffas i SIS anges i underavsnitten nedan. Varje enskilt fall jämfördes med liknande ”användningsfall” som redan hanterats i medlemsstaternas automatiska fingeravtrycksidentifieringssystem. Beroende på användningssituation ingår dessa fall i huvudsak i JRC:s undersökning om de användningsfall där ”10-mot-10”-fingeravtryckskontroller beskrivs.

⁵ Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

⁶ Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete.

Med undantag för sådana fall där operativa utmaningar framhävs, är kvaliteten på fingeravtrycken i allmänhet hög. Det beror på att både nytagna fingeravtryck från de berörda personerna och de fingeravtrycksuppsättningar som lagrats i databasen har tagits under kontrollerade förhållanden med möjlighet att underkänna fingeravtryck med låg kvalitet och ta dem på nytt.

Om en medlemsstat har gjort en registrering men saknar fingeravtryck för att slutföra den kan en annan medlemsstat som redan har hanterat personen ha fingeravtrycken i sitt nationella AFIS. Sirenehandboken⁷ beskriver hur sådana fingeravtryck som ska läggas till i registreringen får skickas. Eftersom fingeravtrycken kan ha tagits i ett annat system bör det säkerställas att de innehåller uppgifter om avtryckens ”kvalitetspoäng”, så att de använts på ett genomtänkt sätt.

3.2.1 Nekad inresa eller vistelse (förordning, artikel 24)

Denna personregistrering är den överlägset vanligaste. Om man antar att den medlemsstat som utför registreringen har tillgång till den person som ska registreras i SIS (registrerad person) tas en uppsättning med tio fingeravtryck som läggs till i registreringen och därefter jämförs med de 10-fingeravtryckskort som redan finns i SIS. Kopplingar till andra registreringar kan då hittas.

3.2.2 Gripande för överlämnande eller utlämning (beslut, artikel 26)

Den registrerade personen kan vara otillgänglig vid tidpunkten för registreringen och fingeravtryck finns inte tillgängliga. Den medlemsstat som utför registreringen kanske dock redan har den berörda personens fingeravtryck i sitt nationella AFIS och kan slutföra registreringen. En uppsättning med tio fingeravtryck tas, läggs till i registreringen och jämförs med de 10-fingeravtryckskort som redan finns i andra registreringar i SIS.

3.2.3 Försvunna personer (beslut, artikel 32)

Fingeravtryck från dessa personer är inte alltid tillgängliga när registreringen utförs. Om det finns ett nationellt register och lagstiftningen medger det, kan dock fingeravtryck därifrån i vissa fall läggas till i registreringen.

Under utredningens gång kan latent fingeravtryck från den berörda personen användas för att söka i SIS (men dessa fingeravtryck skulle inte behållas och lagras i databasen). Om så sker rör det sig inte om en registrering utan en sökning.

3.2.4 Personer som söks för att delta i ett rättsligt förfarande (beslut, artikel 34)

Fingeravtryck är kanske inte alltid tillgängliga. En medlemsstat kan emellertid slutföra en registrering med fingeravtryck från sitt nationella AFIS om detta är tillåtet.

⁷ Bilaga till kommissionens genomförandebeslut 2013/115/EU om antagande av Sirenehandboken och övriga genomförandeåtgärder avseende andra generationen av Schengens informationssystem (SIS II).

3.2.5 Diskreta eller särskilda kontroller (beslut, artikel 36)

Det kan finnas fall där fingeravtryck inte finns tillgängliga. Kontrollerna är sådana till sin natur att fingeravtryck sannolikt inte kommer att finnas tillgängliga i ett senare skede. Den medlemsstat som utför registreringen kanske dock redan har den berörda personens fingeravtryck i sitt nationella AFIS och kan slutföra registreringen. Polis-/gränskontroller är en möjlighet att göra sökningar mot dessa fingeravtryck.

3.2.6 Missbruk av identitet (förordning, artikel 36; beslut, artikel 51)

Med samtycke av offret vars identitet har missbrukats kan medlemsstaterna lägga till hans eller hennes fingeravtryck till registreringen av den person som missbrukat identiteten. Denna åtgärd innebär en ”uppdatering” av registreringen, inte en ”nyregistrering”. Det ger myndigheterna möjlighet att identifiera både bedragare och offer, eftersom offret vid behov kan bevisa sin identitet. Efter en träff på en sökning på namn och födelsedatum i samband med primärkontrollen vid gränsen kan offrets identitet verifieras i en fördjupad kontroll.

3.3 Bestämning av storleken på AFIS i SIS

Vid tidpunkten för undersökningen fanns omkring 5 500 fingeravtrycksposter i SIS. Medlemsstaterna bekräftade att avsaknaden av AFIS var en faktor som begränsande möjligheterna att lägga in fingeravtryck i SIS.

3.3.1 Storlek

Antalet personregistreringar i SIS är relativt stabilt. Antalet kan komma att öka som följd av att förslag framlagts om att lägga till registreringar vid beslut om återvändande och relaterade inreseförbud. Även om storleken på AFIS ökar i SIS, förväntas databasen ändå vara mindre än en större medlemsstats och utgör därför inte något tekniskt problem vad gäller dimensionering.

3.3.2 Antal transaktioner

Det finns tre typer av transaktioner som bör beaktas:

- **Frågor/sökningar.** Det är framför allt frågor/sökningar som kommer att behöva hanteras i SIS. År 2014 ställdes nästan två miljarder frågor i alla registreringskategorier i SIS, antingen i nationella kopior eller i det centrala systemet. Frågorna/sökningarna kommer att innefatta sökningar som redan gjorts i SIS och som kommer att få uppbackning när ett automatiskt fingeravtrycksidentifieringssystem införs. Visumansökningar via VIS bör kontrolleras mot SIS. Varje dag ställs upp emot 20 000 till 30 000 identifieringsfrågor. Eurodac hanterade 750 000 transaktioner år 2014. Innan dessa transaktioner genomförs måste sökningar göras i VIS och SIS för att förebygga, upptäcka och utreda terroristbrott och andra allvarliga brott. Fingeravtryckskontroller väntas också utföras. Kontroller vid Schengengränserna utförs med hjälp av namn och födelsedatum. I framtiden planeras att fingeravtryckskontroller kommer att utföras för tredjelandsmedborgare. Alla registreringar kommer inte att innehålla fingeravtryck, så alla personfrågor kommer inte att kunna ställas på det här sättet. Många kontroller kommer fortsättningsvis att göras

med hjälp av namn och födelsedatum. Alla åtkomstpunkter till SIS kan inte ställa frågor baserade på fingeravtryck.

- **Skapa, uppdatera och radera registreringar.** Det utfördes 1,4 miljoner transaktioner för att skapa, uppdatera eller radera registreringar år 2014. Av dessa rörde 780 000 skapande och uppdatering av personregistreringar och skulle därför kunna innebära att fingeravtryck lagts till. Radering bör vara en process som utförs automatiskt vid radering av en registrering, men naturligtvis bör bearbetningskrav tillgodoses.

Det är viktigt att säkerställa att korrekt statistik finns tillgänglig så att dimensioneringen av AFIS blir den rätta i SIS. Kunskaper som inhämtats vid utvecklingen av nationella AFIS kan användas för SIS.

3.3.3 Standarder för utbyte av fingeravtryck

NIST-standarderna och Interpols riktlinjer för bästa praxis utgör en lämplig grund för sådant utbyte.

3.3.4 Systemarkitektur

SIS arkitektur omfattar följande delar:

- Ett centralt system som hanterar 20 % av transaktionerna – fem medlemsstater använder det centrala systemet direkt.
- Nationella kopior (80 % av transaktionerna), som kan vara
 - ”partiella” (endast uppgifter som utgörs av ord och siffror – nio medlemsstater har sådana kopior),
 - ”fullständiga” (uppgifter som utgörs av ord och siffror plus bilder och fingeravtryck – sexton medlemsstater har sådana kopior).

Ett centralt AFIS behövs för att ge service till medlemsstater som saknar en nationell kopia, medlemsstater med en partiell nationell kopia och även medlemsstater som har problem med den tekniska tillgängligheten till sin fullständiga nationella kopia.

Alla transaktioner för att skapa, uppdatera eller radera registreringar involverar det centrala systemet. För att tillägga fingeravtryck i en registrering kommer det att krävas en kvalitetskontroll i det centrala systemets automatiska fingeravtrycksidentifieringssystem.

Efter att transaktioner för att skapa, uppdatera eller radera registreringar skickats till det centrala systemet, sänds de inom tre minuter ut till de nationella kopiorna. Ett centralt AFIS kommer att krävas för att stödja dessa transaktioner.

Enligt rättsakterna för SIS II måste en sökning i en nationell kopia ge samma resultat som en sökning i SIS-databasen. Detta efterlevnadskrav tillämpas för sökningar på namn och siffror och kommer också att behöva tillämpas för fingeravtryckssökningar.

Om en medlemsstat inför ett eget AFIS som en del av sin nationella kopia, måste detta AFIS ha samma identifieringsprestanda som det centrala AFIS. Det är tekniskt och juridiskt möjligt att ha ett AFIS som en del av en nationell kopia, men att producera likvärdiga resultat blir en utmaning.

En centraliserad systemarkitektur är lättare att hantera från kvalitetssynpunkt men måste klara av den belastning som den kommer att utsättas för. En systemarkitektur som består av ett centralt AFIS tillsammans med andra AFIS i fullständiga nationella kopior fördelar belastningen men behöver också kunna hantera den utmaning som beskrivs ovan. Utmaningen skulle kunna hanteras genom att alla sådana AFIS använder samma mjukvara.

När en övergripande systemarkitektur har fastställts bör det övervägas om alla användningsfall ska hanteras på samma sätt eller om skillnader i volymer eller svarstider talar för parallella arbetsflöden eller delsystem inom AFIS.

Vissa brottsbekämpnings- eller gränskontrolloperationer kommer att kräva en svarstid på under 30 sekunder, men på ett konsulat skulle svarstiden kanske endast behöva vara under fem minuter.

I kontrollerade situationer på en polisstation kan det krävas en svarstid på under 10 minuter. Det är viktigt att utvärdera den arbetsbelastning som anges i dessa användningsfall och definitionen av prioriteringar för hanteringen av förfrågningar. Användning av filter, såsom ålder och kön, kan minska det antal poster som jämförs och därmed förbättra svarstiden.

Avslutningsvis måste AFIS i SIS ingå i de utvärderings- och rapporteringsförfaranden som fastställs i rättsakterna för SIS II.

4. REKOMMENDATIONER

De föregående kapitlen bekräftar att AFIS-tekniken finns tillgänglig och är klar att tas i bruk. Dessutom anser kommissionen att genomförandet av följande 19 rekommendationer bör anses stödja en framgångsrik installation och användning av ett automatiskt fingeravtrycksidentifieringssystem i SIS:

1. **Behov av kompletterande statistik** – om antalet sökningar per år på personer och deras operativa sammanhang för en korrekt bedömning av det automatiska fingeravtrycksidentifieringssystemets storlek och bearbetningskapacitet.
2. **Främjande av bästa praxis** – för AFIS i SIS baserat på kunskaper som inhämtats då nationella AFIS utvecklats och förvaltats.
3. **Gemensam standard för datautbyte** – NIST-containerfiler utgör en lämplig grund för utbyte av fingeravtrycksdata. En automatisk kontroll av genomförandet bör utvecklas
4. **Kompletterande förhållande mellan Prüm och SIS II** – det kompletterande förhållandet mellan Prüm-mekanismen och AFIS i SIS bör förtydligas för att undvika överlappning⁸.

⁸ De fingeravtryck som lagras i SIS II är kopplade till registreringar och SIS II används vid gränskontroller och kontroller som utförs av brottsbekämpande myndigheter. Genom beslut 2008/615/RIF ger Prüm-mekanismen

möjlighet att söka i nationella AFIS som används för brottsbekämpning. Till skillnad från SIS II föreskriver Prüm

5. **Särskilda delsystem** – på grund av skillnaderna mellan de olika användningsfallen, särskilt i fråga om volym och svarstider, bör parallella arbetsflöden eller särskilda delsystem övervägas.
6. **Hög kvalitet i registreringsprocessen** – i registreringsfasen bör elektronisk avläsning och erfarna operatörer användas.
7. **Lagring av flerdubbla datamängder** – för att stödja en sammansatt matchningsstrategi.
8. **Kontrollerad överföring av data** – i AFIS i SIS ska fingeravtryck som skapats i andra system kunna användas förutsatt att systemparametrarna från dessa system finns kvar i de data som läggs in vid registreringen.
9. **Punkter som rör inläsningskvalitet:**
 - a. **Övervakning av en operatör** – lämplig utbildning för registreringsarbete.
 - b. **Lämplig sensor** – enheter för elektronisk avläsning är att föredra.
 - c. **Förbättrat grafiskt användargränssnitt (GUI)** – för att ge feedback i realtid om inlästa data.
 - d. **Lämplig användarinteraktion** – registreringen bör vara användarvänlig.
 - e. **Lämplig miljö** – belysning, temperatur och bakgrund.
 - f. **Sensorunderhåll** – bör vara regelbundet och systematiskt.
10. **Kvalitetsbedömningsalgoritmer:**
 - a. **Efterlevnad av standarder** – användning av erkända kvalitetsmått.
 - b. **Korrigerande åtgärder** – för att få fingeravtryck med tillfredsställande kvalitet.
11. **Identifieringssystemens kvalitet:**
 - a. **Kvalitetsbaserad bearbetning** – inklusive användning av kompletterande verktyg såsom alternativa funktioner för särdragsdetektion och processspecifika matchningsalgoritmer.
 - b. **Kvalitetsbaserad sammanslagning** – olika fingeravtrycksinläsningar kombineras så att sammansatta kontroller kan göras.
 - c. **Mallersättning/malluppdatering** – de bästa fingeravtrycksregistreringarna används när mallar för ett AFIS skapas.
 - d. **Övervakning** – statistik skapas för varje typ av program, varje webbplats, enhet och operatör.
12. **Fall med barn** – i synnerhet när det gäller försvunna personer ska SIS automatiska fingeravtrycksidentifieringssystem kunna anpassa matchningsprocessen när det är uppenbart att barnet har vuxit efter att fingeravtrycken togs.
13. **Central tjänst för kvalitetskontroll** – för att kontrollera fingeravtryckskvaliteten mot kvalitetsmåten i SIS automatiska fingeravtrycksidentifieringssystem.

14. **Rapportering om fingeravtryckskort med lägre kvalitet** – när data som registreras eller läggs till i en registrering inte har den kvalitetsnivå som krävs för registreringar eller fingeravtryckskort i SIS automatiska fingeravtrycksidentifieringssystem.
15. **Databasens integritet** – användning av bästa praxis för att minska risken för inkonsekvens eller felaktiga data, inklusive fingeravtryck, som registrerats i databasen.
16. **Sökning:**
 - a. **Förbättrad upplösning (1000 dpi⁹)** – för att göra det möjligt att lagra bilder av fingeravtryck med högre upplösning i de fall där medlemsstaterna har uppgraderat sina avläsningsenheter.
 - b. **Platta och rullade fingeravtryck** – medlemsstaterna bör få begränsa insamlingen av fingeravtryck till platta avtryck men endast för sökändamål.
 - c. **Snabbkontroll av två fingrar** – möjlighet att utföra snabbsökningar.
17. **Anpassade svarstider** – för att klara tre riktmärken för svarstider baserade på olika användningssituationer: a) mycket kort (d.v.s. under 30 sekunder), b) medium (d.v.s. under fem minuter), c) längre (d.v.s. upp till tio minuter).
18. **Frågeprioritering** – definitionen av prioritetsnivåer för bearbetning av frågor för att AFIS i SIS bättre ska kunna hantera belastningen på systemet.
19. **Prestandamätningar** – där det övervägs i ett tidigt skede hur prestandautvärderingar av AFIS i SIS ska schemaläggas.

5. NÄSTA STEG – HANDLINGSPLAN

Genomförandet av undersökningen och framläggandet av denna rapport för samråd med Europaparlamentet är de första stegen mot att tillhandahålla AFIS-funktionen i SIS-miljön. I praktiken kan de åtgärder som nu behöver genomföras på högre nivå tillsammans med eu-LISA och medlemsstaterna sammanfattas på följande sätt:

- (1) Fastställ kraven för den särskilda kvalitetskontrollen för att säkerställa att en minimistandard uppnås i fråga om datakvalitet. Specifikationerna bör ingå i ett genomförandebeslut från kommissionen.
- (2) Fastställ användarkrav för och dimensionering av det system som krävs.
- (3) Bestäm arkitekturen för det system som krävs. Detta bör ingå i ett genomförandebeslut från kommissionen.
- (4) Fastställ de tekniska specifikationerna och tidsplanen för införandet.
- (5) Genomför det projekt som leder till införandet av AFIS i SIS.

⁹ Punkter per tum.

6. SLUTSATS

AFIS-funktionen är redan nära knuten till databaser för brottsbekämpning och gränskontroll. SIS är en sådan databas och personregistreringar kommer att uppnå sin fulla potential och användbarhet med stöd av ett automatiskt fingeravtrycksidentifieringssystem.

Mot bakgrund av den analys och de synpunkter som sammanfattats i denna rapport konstaterar kommissionen att AFIS-tekniken har nått en tillräcklig teknisk mognad och tillgänglighet för att integreras i SIS. Denna rapport ger också en översikt över kommissionens förslag som kommer att beaktas i samband med införandet och användningen av SIS automatiska fingeravtrycksidentifieringssystem i en driftsmiljö.