

**KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2019/329****av den 25 februari 2019****om fastställande av specifikationerna för kvalitet, upplösning och användning av fingeravtryck och ansiktsbilder för biometrisk verifiering och identifiering i in- och utresesystemet**

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EU) 2017/2226 av den 30 november 2017 om inrättande av ett in- och utresesystem för registrering av in- och utreseuppgifter och av uppgifter om nekad inresa för tredjelandsmedborgare som passerar medlemsstaternas yttre gränser, om fastställande av villkoren för åtkomst till in- och utresesystemet för brottsbekämpande ändamål och om ändring av konventionen om tillämpning av Schengenavtalet och förordningarna (EG) nr 767/2008 och (EU) nr 1077/2011 <sup>(1)</sup>, särskilt artikel 36 första stycket led a och b, och

av följande skäl:

- (1) Genom förordning (EU) 2017/2226 inrättades in- och utresesystemet som ett system för elektronisk registrering av tidpunkt och plats för in- och utresa för tredjelandsmedborgare som beviljas inresa för kortare vistelse på medlemsstaternas territorium samt för beräkning av längden på denna tillåtna vistelse.
- (2) Målet för in- och utresesystemet är att förbättra förvaltningen av de yttre gränserna, förhindra irreguljär invandring och underlätta hanteringen av migrationsströmmar. In- och utresesystemet bör framför allt bidra till identifiering av personer som inte uppfyller, eller inte längre uppfyller, villkoren för den tillåtna vistelsen på medlemsstaternas territorium. Dessutom bör systemet bidra till att terroristbrott och andra grova brott förebyggs, förhindras, upptäcks och utreds.
- (3) Eftersom de biometriska uppgifternas kvalitet och tillförlitlighet är avgörande framgångsfaktorer för att in- och utresesystemet ska kunna nå sin fulla potential, är det nödvändigt att fastställa specifikationerna för både fingeravtryckens och ansiktsbildernas kvalitet, upplösning och användning för biometrisk verifiering och identifiering i in- och utresesystemet, inbegripet när de tas på plats eller hämtas elektroniskt från den elektroniska maskinläsbara resehandlingen. Eftersom kvaliteten på de registrerade fingeravtrycken kommer att ha inverkan på in- och utresesystemets funktion i årtal efter att de registrerats bör miljöfaktorer och operativa faktorer i samband med registreringen av fingeravtrycks kvalitet övervakas noggrant på lång sikt.
- (4) Detta beslut skapar inga nya standarder; det är förenligt med Icaos standarder.
- (5) På grundval av dessa åtgärder bör Europeiska byrån för den operativa förvaltningen av stora it-system inom området frihet, säkerhet och rättvisa därefter kunna fastställa utformningen av in- och utresesystemets fysiska arkitektur, inbegripet dess kommunikationsinfrastruktur och tekniska specifikationer för systemet, samt utveckla systemet.
- (6) I detta sammanhang är det därför nödvändigt att anta specifikationer för fingeravtryckens och ansiktsbildernas kvalitet, upplösning och användning för biometrisk verifiering och identifiering i in- och utresesystemet.
- (7) Detta beslut påverkar inte tillämpningen av Europaparlamentets och rådets direktiv 2004/38/EG <sup>(2)</sup>.
- (8) I enlighet med artiklarna 1 och 2 i protokoll nr 22 om Danmarks ställning, fogat till fördraget om Europeiska unionen och fördraget om Europeiska unionens funktionssätt, deltog Danmark inte i antagandet av förordning (EU) 2017/2226, som inte är bindande för eller tillämplig på Danmark. Eftersom förordning (EU) 2017/2226 utgör en utveckling av Schengenregelverket anmälde Danmark emellertid den 30 maj 2018 i enlighet med artikel 4 i det protokollet sitt beslut att genomföra förordning (EU) 2017/2226 i sin nationella lagstiftning. Danmark är därför enligt internationell rätt skyldigt att genomföra detta beslut.

<sup>(1)</sup> EUT L 327, 9.12.2017, s. 20.

<sup>(2)</sup> Europaparlamentets och rådets direktiv 2004/38/EG av den 29 april 2004 om unionsmedborgares och deras familjemedlemmars rätt att fritt röra sig och uppehålla sig inom medlemsstaternas territorier och om ändring av förordning (EEG) nr 1612/68 och om upphävande av direktiven 64/221/EEG, 68/360/EEG, 72/194/EEG, 73/148/EEG, 75/34/EEG, 75/35/EEG, 90/364/EEG, 90/365/EEG och 93/96/EEG (EUT L 158, 30.4.2004, s. 77).

- (9) Detta beslut utgör en utveckling av de bestämmelser i Schengenregelverket i vilka Förenade kungariket inte deltar i enlighet med rådets beslut 2000/365/EG <sup>(3)</sup>. Förenade kungariket deltar därför inte i antagandet av detta beslut, som inte är bindande för eller tillämpligt på Förenade kungariket.
- (10) Detta beslut utgör en utveckling av de bestämmelser i Schengenregelverket i vilka Irland inte deltar i enlighet med rådets beslut 2002/192/EG <sup>(4)</sup>. Irland deltar därför inte i antagandet av detta beslut, som inte är bindande för eller tillämpligt på Irland.
- (11) När det gäller Island och Norge utgör detta beslut, i enlighet med avtalet mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket <sup>(5)</sup>, en utveckling av de bestämmelser i Schengenregelverket som omfattas av det område som avses i artikel 1.A i rådets beslut 1999/437/EG <sup>(6)</sup>.
- (12) När det gäller Schweiz utgör detta beslut, i enlighet med avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket <sup>(7)</sup>, en utveckling av de bestämmelser i Schengenregelverket som omfattas av det område som avses i artikel 1.A i beslut 1999/437/EG jämförd med artikel 3 i rådets beslut 2008/146/EG <sup>(8)</sup>.
- (13) När det gäller Liechtenstein utgör detta beslut, i enlighet med protokollet mellan Europeiska unionen, Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Liechtensteins anslutning till avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket <sup>(9)</sup>, en utveckling av de bestämmelser i Schengenregelverket som omfattas av det område som avses i artikel 1.A i beslut 1999/437/EG jämförd med artikel 3 i rådets beslut 2011/350/EU <sup>(10)</sup>.
- (14) När det gäller Cypern, Bulgarien, Rumänien och Kroatien kräver driften av in- och utresesystemet att passiv åtkomst till VIS har beviljats och att alla bestämmelser i Schengenregelverket som avser SIS har fått verkan i enlighet med relevanta rådsbeslut. Dessa villkor kan endast uppfyllas när verifieringen i enlighet med tillämpligt Schengenutvärderingsförfarande har slutförts framgångsrikt. Därför bör in- och utresesystemet endast drivas av de medlemsstater som uppfyller dessa villkor när systemet tas i drift. Medlemsstater som vid driftsstarten inte har tagit in- och utresesystemet i drift bör anslutas till in- och utresesystemet i enlighet med det förfarande som anges i förordning (EU) 2017/2226 så snart som alla dessa villkor är uppfyllda.
- (15) Europeiska datatillsynsmannen avgav sitt yttrande den 27 juli 2018.
- (16) De åtgärder som föreskrivs i detta beslut är förenliga med yttrandet från kommittén för smarta gränser.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

#### Artikel 1

1. Specifikationerna för fingeravtryckens kvalitet, upplösning och användning för biometrisk verifiering och identifiering i in- och utresesystemet anges i bilagan.

<sup>(3)</sup> Rådets beslut 2000/365/EG av den 29 maj 2000 om en begäran från Förenade konungariket Storbritannien och Nordirland om att få delta i vissa bestämmelser i Schengenregelverket (EGT L 131, 1.6.2000, s. 43).

<sup>(4)</sup> Rådets beslut 2002/192/EG av den 28 februari 2002 om Irlands begäran om att få delta i vissa bestämmelser i Schengenregelverket (EGT L 64, 7.3.2002, s. 20).

<sup>(5)</sup> EGT L 176, 10.7.1999, s. 36.

<sup>(6)</sup> Rådets beslut 1999/437/EG av den 17 maj 1999 om vissa tillämpningsföreskrifter för det avtal som har ingåtts mellan Europeiska unionens råd och Republiken Island och Konungariket Norge om dessa båda staters associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket (EGT L 176, 10.7.1999, s. 31).

<sup>(7)</sup> EUT L 53, 27.2.2008, s. 52.

<sup>(8)</sup> Rådets beslut 2008/146/EG av den 28 januari 2008 om ingående på Europeiska gemenskapens vägnar av avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket (EUT L 53, 27.2.2008, s. 1).

<sup>(9)</sup> EUT L 160, 18.6.2011, s. 21.

<sup>(10)</sup> Rådets beslut 2011/350/EU av den 7 mars 2011 om ingående på Europeiska unionens vägnar av protokollet mellan Europeiska unionen, Europeiska gemenskapen, Schweiziska edsförbundet och Furstendömet Liechtenstein om Furstendömet Liechtensteins anslutning till avtalet mellan Europeiska unionen, Europeiska gemenskapen och Schweiziska edsförbundet om Schweiziska edsförbundets associering till genomförandet, tillämpningen och utvecklingen av Schengenregelverket, om avskaffande av kontroller vid de inre gränserna och om personers rörlighet (EUT L 160, 18.6.2011, s. 19).

2. Specifikationerna för ansiktsbildens kvalitet, upplösning och användning för biometrisk verifiering och identifiering i in- och utresesystemet, inbegripet för ansiktsbilder som tas på plats eller hämtas elektroniskt från den elektroniska maskinläsbara resehandlingen anges i bilagan.

*Artikel 2*

Detta beslut träder i kraft den tjugonde dagen efter det att det har offentliggjorts i *Europeiska unionens officiella tidning*.

Utfärdat i Bryssel den 25 februari 2019.

*På kommissionens vägnar*

Jean-Claude JUNCKER

Ordförande

---

## BILAGA

## 1. KVALITET

## 1.1 Tröskelvärden

## 1.1.1 Fingeravtryck

## Registrering

Vid registreringen ska version 2.0 (eller senare) av Fingerprint Image Quality-måttet (NFIQ) <sup>(1)</sup> som fastställts av National Institute of Standards and Technology (NIST) användas för att verifiera att kvaliteten på fingeravtrycksuppgifterna är förenlig med de tröskelvärden som ska anges i de tekniska specifikationer som avses i artikel 37.1 i förordning (EU) 2017/2226.

Vid registreringen ska kvaliteten på fingeravtrycksuppgifterna bedömas

- på nationell nivå av medlemsstaterna vid den tidpunkt då de tas och innan de överförs till in- och utresesystemets centrala system, eventuellt med stöd av ett verktyg som tillhandahålls, upprätthålls och uppdateras av eu-LISA, och
- på central nivå.

## Verifiering

För verifieringen rekommenderas att medlemsstaterna bedömer kvaliteten på fingeravtrycksuppgifterna vid den tidpunkt då de tas och innan de överförs till in- och utresesystemets centrala system, antingen genom att använda version 2.0 (eller senare) av NIST Fingerprint Image Quality (NFIQ)-måttet eller, om det är tekniskt omöjligt, genom att använda ett annat mått som helst ska korrelera med NFIQ version 2.0 (eller senare). Korrelationen ska fastställas på förhand. Om ett kvalitetsmått enligt NFIQ version 2.0 (eller senare) erhålls ska det skickas till in- och utresesystemets centrala system på samma gång som fingeravtrycksuppgifterna.

## 1.1.2 Ansiktsbilder

Kvaliteten på ansiktsbilderna, även sådana som är i nära infrarött, ska stämma överens med de tröskelvärden som fastställs i de tekniska specifikationer som avses i artikel 37.1 i förordning (EU) 2017/2226 och med bildkraven i ISO/IEC 19794-5:2011 Frontal image type. Kvaliteten på ansiktsbilden ska bedömas på nationell nivå av medlemsstaterna vid den tidpunkt då den tas och innan den överförs till in- och utresesystemets centrala system, eventuellt med stöd av ett verktyg som tillhandahålls, upprätthålls och uppdateras av eu-LISA. Kvalitetsalgoritmen för ansiktsbilden ska förstås enligt kriterierna för ISO/IEC 19794-5:2011.

Kvalitetströskeln för ansiktsbilderna ska fastställas med hjälp av en kvalitetsbedömningsalgoritm för ansiktsbilder som baserar sig på de kvalitetsmått som beskrivs i ISO 19794-5 och sörja för kvalitetskontroller som motsvarar de som genomförs i in- och utresesystemets centrala system <sup>(2)</sup>.

## 1.2 Prestandavärden för biometrisk noggrannhet

## Definitioner

De prestandavärden för biometrisk noggrannhet som definieras i artikel 3 i förordning (EU) 2017/2226 är följande:

29. *andel registreringsfel*: andelen registreringar med otillräcklig kvalitet vad gäller biometrisk registrering.
30. *andel felaktig positiv identifiering*: andelen visade träffar vid biometrisk sökning som inte avser den kontrollerade resenären.
31. *andel felaktig negativ identifiering*: andelen träffar som missas vid biometrisk sökning trots att biometriska uppgifter har registrerats för resenären."

Den "biometriska sökning" som avses i punkterna 30 och 31 är liktydig med biometrisk identifiering eller en "1 till n"-sökning.

I artikel 36 första stycket led g i förordning (EU) 2017/2226 lämnas möjligheten öppen att i genomförandeakten definiera ytterligare värden för biometrisk prestanda.

False Match(ing) Rate (FMR) är den andel falska försök som felaktigt bedöms vara en träff mot en mall av ett annat objekt (en persons biometriska mall).

<sup>(1)</sup> <https://www.nist.gov/services-resources/software/development-nfiq-20>

<sup>(2)</sup> När det är möjligt ska ansiktsbilderna bedömas och valideras mot kriterierna i §3.9 i Icaos dokument 9303 och de franska användnings- och bildrekommendationerna för franska viseringsansökningar.

False Non-Match(ing) Rate (FNMR) är den andel genuina försök som felaktigt inte ger en träff mot en mall av samma objekt.

Ett genuint försök är en användares försök att matcha sin egna lagrade mall. Ett falskt försök är det motsatta, dvs. en användares mall matchas mot någon annans mall.

### 1.2.1 Andel registreringsfel

Målvärdet för andelen registreringsfel är noll. Medlemsstaterna ska anstränga sig för att undvika sådana fall genom att använda en kvalitetsinriktad registreringsprocess.

### 1.2.2 Den biometriska verifieringens noggrannhet

Det maximala värdet av False Non-Matching Rate (FNMR) vid en False Matching Rate (FMR) på 0,05 % (5 per 10 000) är följande:

Typ	FMR	FNMR
Fingeravtryck	0,05 %	< 0,5 %
Ansiktsbild	0,05 %	< 1 %

### 1.2.3 Den biometriska identifieringens noggrannhet

Det maximala värdet av andelen felaktig negativ identifiering vid en andel felaktig positiv identifiering på 0,1 % (1 per 1 000) är följande:

Typ	Andel felaktig positiv identifiering	Andel felaktig negativ identifiering
Fingeravtryck	0,1 %	< 1,5 %
Ansiktsbild och fingeravtryck (multimodal)	0,1 %	< 1 %

## 1.3 Övervakning av bietrisk noggrannhet

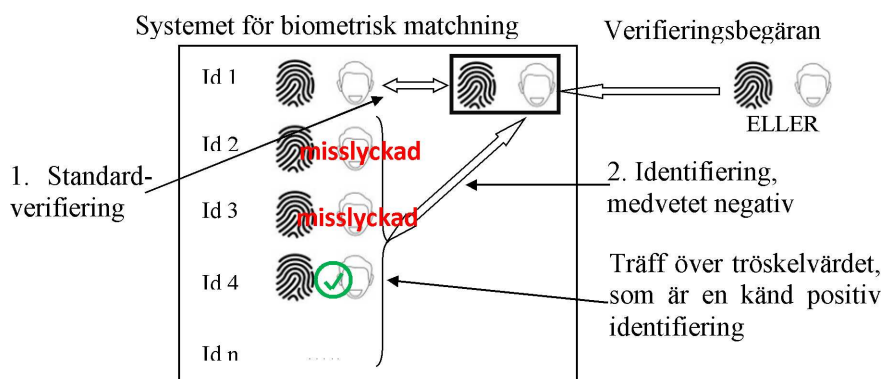
Den biometriska noggrannheten ska mätas utifrån faktiska data som inhämtas dagligen av varje medlemsstat på grundval av ett representativt urval ärenden vid valfria gränsövergångsställen. Mätningen förvaltas centralt, på ett fullständigt automatiserat sätt och kräver inte att operatören har åtkomst till personuppgifter.

Mätningen av bietrisk prestanda måste inte göras fortlöpande: den kan inaktiveras eller aktiveras men ska regelbundet utföras av eu-LISA (minst en gång i månaden).

Vid mätningen av bietrisk prestanda används inte själva de biometriska uppgifterna. De mallar av bilderna som används för noggrannhetsmätningen raderas automatiskt efter genomförandet av utvärderingen. Resultaten av prestandamätningen ska inte innehålla personuppgifter.

### 1.3.1 Mätning av andelen felaktig positiv identifiering

Följande figur visar att mallarna för de biometriska proven av både fingeravtryck och ansiktsbild ingår i systemet för bietrisk matchning för "n" stycken identiteter.



Mätningen ska ske enligt följande:

1. En person som ska registreras i in- och utresesystemet lämnar ett prov av en eller båda av de två biometriska typerna (fingeravtryck och ansiktsbild).
2. Den biometriska verifieringen utförs med de biometriska referensdata som motsvarar personens identitet (steg 1 i figuren, "standardverifiering").
3. För en kontinuerlig uppsättning prov erhålls den andra biometriska typen från samma person (lämnas antingen samtidigt med steg 1 eller extraheras från de biometriska referensdata som motsvarar personens identitet). Kombinationen av biometriska uppgifter används för att köra en identifiering mot det fullständiga galleriet, med undantag för de biometriska uppgifterna för den person som det biometriska provet tillhör (steg 2 i figuren, "identifiering, medvetet negativ"). Denna identifieringsprocess förväntas leda till ett nollresultat eftersom det matchande biometriska provet med avsikt har tagits bort från jämförelsen.

Om den typ som används i steg 2 motsvarar fingeravtrycket utförs en identifiering (för att utvärdera identifieringens noggrannhet) med samma villkor som anges i första stycket.

4. Om den biometriska identifieringen ger ett biometriskt prov som resultat (anges som "träff över tröskelvärdet") är detta en känd felaktig *positiv* identifiering (resultatet är en annan person än den förväntade).

Steg 1 och 2 är en del av identitetsverifieringen i in- och utresesystemet. Steg 3 och 4 hör inte till identitetsverifieringen, utan görs för att mäta den biometriska noggrannheten.

Andelen felaktig positiv identifiering beräknas på följande sätt:

$$\text{Andel felaktig positiv identifiering} = \frac{\text{Antal identifieringar som ger en identifierare i resultat}}{\text{Antal kända negativa identifieringar}}$$

### 1.3.2 Mätning av andelen felaktig negativ identifiering

Figuren i punkt 1.3.1 illustrerar den beskrivning som följer.

Mätningsprocessen ska tillämpa följande logik, där de första två stegen alltid är desamma eftersom de är en del av identitetsverifieringen i in- och utresesystemet:

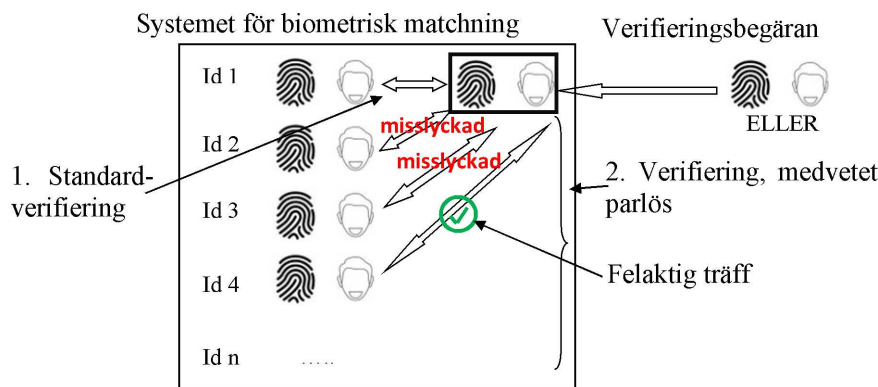
1. En person som ska registreras i in- och utresesystemet lämnar ett prov av en eller båda av de två biometriska typerna.
2. Den biometriska verifieringen utförs med de biometriska referensdata som motsvarar personens identitet (steg 1 i figuren, "standardverifiering").
3. För en kontinuerlig uppsättning prov erhålls den andra biometriska typen antingen från samma person (om båda biometriska typerna lämnades i steg 1) eller från en annan person för vilken steg 1 och 2 i denna process har inletts. Kombinationen av biometriska uppgifter används för att köra en identifiering mot det fullständiga galleriet, inklusive de biometriska uppgifterna för den eller de personer som det biometriska provet tillhör. Denna identifieringsprocess förväntas leda till det kända resultatet eftersom det matchande biometriska provet ingår i jämförelsen.
4. Om den typ som används i steg 2 motsvarar fingeravtrycket utförs en identifiering (för att utvärdera identifieringens noggrannhet) med samma villkor som anges i tredje stycket.
5. Om den biometriska identifieringen inte ger det förväntade biometriska provet som resultat (anges som "träff över tröskelvärdet") i listan över träffar, är detta en känd felaktig *negativ* identifiering.

Steg 1 och 2 är en del av identitetsverifieringen i in- och utresesystemet. Steg 3 och 4 hör inte till identitetsverifieringen, utan görs för att mäta den biometriska noggrannheten.

Andelen felaktig negativ identifiering beräknas på följande sätt:

$$\text{Andel felaktig negativ identifiering} = \frac{\text{Antal identifieringar som inte ger den biometriska registrerades korrekta identifierare som resultat}}{\text{Antal identifieringar totalt}}$$

### 1.3.3 Mätning av verifieringens biometriska noggrannhet (False Matching Rate och False Non Matching Rate)



Vid mätningen ska följande logik tillämpas:

1. En person som omfattas av in- och utresesystemet lämnar ett prov på en av de två biometriska typerna.
2. Den biometriska verifieringen utförs med de biometriska referensdata som motsvarar personens identitet (steg 1 i figuren, "standardverifiering").

Steg 1 och 2 är en del av identitetsverifieringen i in- och utresesystemet. Mätningen av bietrisk noggrannhet inleds här.

3. Det biometriska provet verifieras mot ett antal andra biometriska prov som slumpmässigt hämtats från det biometriska galleriet och som inte innefattar de biometriska uppgifter som lämnats. Det förväntade resultatet är att verifieringen misslyckas (punkt 2 i figuren, "verifiering, medvetet parlös"). Om en träff fås är den felaktig.

Steg 3 möjliggör beräkning av **False Matching Rate** (en träff fås på en annan person än den person som uppgifterna tillhör):

$$FMR = \frac{\text{Antal framgångsrika parlösa jämförelser}}{\text{Antal parlösa jämförelser}}$$

Anmärkning: Antalet parlösa jämförelser är antalet jämförelser enligt steg 3.

Steg 2 möjliggör beräkning av **False Non Matching Rate** (ingen träff fås mot den person som de biometriska uppgifterna tillhör), om identiteten har bekräftats på annat sätt, enligt följande:

$$FNMR = \frac{\text{Antal misslyckade jämförelser}}{\text{Antal jämförelser som antas ha ett par}}$$

Anmärkning: Det anges att jämförelserna "antas" ha ett par eftersom det inte råder någon absolut säkerhet om att en bedragare inte ingår i den grupp identiteter jämförelsen görs med.

### 1.4 Ersättande av biometriska uppgifter för att förbättra kvaliteten eller för att ersätta en bild som har hämtats från den elektroniska maskinläsbara resehandlingen med en ansiktsbild som tagits på plats och ingår i galleriet i in- och utresesystemets centrala system

Biometriska uppgifter får endast ersättas när en positiv bietrisk verifiering av identiteten har gjorts.

#### 1.4.1 Ersättande av lagrade fingeravtrycksuppgifter

Förfarandet för att ersätta lagrade fingeravtrycksuppgifter som inte uppfyller kvalitetskraven ska beskrivas i den handbok som avses i artikel 71 i förordning (EU) 2017/2226.

Om vänster hand ersätts med höger hand (eller vice versa) ska en identifiering med de nytagna fingeravtrycken inledas för att garantera att de inte motsvarar en annan identitet som redan har registrerats i systemet.

#### 1.4.2 Ersättande av lagrade ansiktsbilder

Förfarandet för att ersätta en lagrad ansiktsbild som inte uppfyller kvalitetskraven, eller som har hämtats från chippen i den elektroniska maskinläsbara resehandlingen, ska beskrivas i den handbok som avses i artikel 71 i förordning (EU) 2017/2226.

## 2. UPPLÖSNING

### 2.1 Fingeravtryck

In- och utresesystemets centrala system ska ta emot fingeravtrycksuppgifter med en upplösning på antingen 500 eller 1 000 ppi (godtagbar avvikelse på +/- 10 ppi) med 256 grånivåer.

Fingeravtrycksuppgifterna ska lämnas i enlighet med standarden ANSI/NIST-ITL 1-2011 Update 2015 (eller senare) och enligt de tekniska specifikationer som avses i artikel 37.1 i förordning (EU) 2017/2226.

### 2.2 Ansiktsbilder

#### 2.2.1 Upplösning

In- och utresesystemets centrala system ska ta emot ansiktsbilder som tas på plats i en upplösning (i stående format) på minst 600 × 800 pixlar och högst 1 200 × 1 600 pixlar.

Ansiktet ska uppta en så stor del av bilden att det garanterat finns minst 120 pixlar mellan ögonens mittpunkter.

#### 2.2.2 Färger

Ansiktsbilder som tas på plats ska vara färgbilder. I undantagsfall, när det inte går att ta en färgbild, får gråskala eller nära infraröd teknik användas. I sådana fall får bilden i gråskala eller nära infrarött, om kvaliteten är tillräcklig, användas för verifiering eller identifiering men inte för registrering. Bilder i gråskala godtas för registrering endast när de hämtas från chippet i resehandlingen.

Särskilda regler om ansiktsbilder i nära infrarött ska beskrivas i den handbok som avses i artikel 71 förordning (EU) 2017/2226.

## 3. ANVÄNDNING AV BIOMETRISKA UPPGIFTER

### 3.1 Införande och lagring

#### 3.1.1 Fingeravtryck

In- och utresesystemets centrala system ska lagra fingeravtrycksuppgifterna från fyra platta fingeravtryck<sup>(?)</sup>. När de finns tillgängliga ska fingeravtrycken från följande fingrar på höger hand användas: pekfinger, långfinger, ringfinger och lillfinger.

När det är omöjligt att ta fingeravtryck med de nämnda fingrarna på höger hand ska de fyra fingeravtrycken tas från vänster hand, om det är möjligt. Om det endast tillfälligt är omöjligt att erhålla fyra fingeravtryck från höger hand ska fingeravtrycksuppgifterna uttryckligen markeras och, om det tillfälliga hindret inte längre existerar, ska fingeravtrycksuppgifterna från höger hand tas vid utresa eller nästa inresa i enlighet med de tekniska specifikationer som avses i artikel 37.1 i förordning (EU) 2017/2226 (tillfälligt hinder).

För att uppnå det tillämpliga tröskelvärdet bör man ta om fingeravtryck två gånger, om så krävs, för varje registrerad (dvs. totalt tre försök att ta fingeravtryck bör göras). Omtagningsförsöken bör göras med samma fingrar som det ursprungliga försöket.

För fingeravtrycksuppgifter som inte uppfyller den tillämpliga kvalitetströskeln gäller följande:

1. De ska lagras i in- och utresesystemets centrala system.
  - a) Biometrisk verifiering ska göras mot dessa uppgifter.
  - b) Biometrisk identifiering ska inte göras mot fingeravtryck som inte uppfyller kvalitetströskeln förutom för brottsbekämpande ändamål.
2. Uppgifterna ska flaggas i det nationella systemet i enlighet med de tekniska specifikationer som avses i artikel 37.1 i förordning (EU) 2017/2226 (teknisk omöjlighet) så att de kan tas vid nästa gränspassage.

(?) Termen "platt" motsvarar termen "flat" i ISO/IEC-lexikonet och "plain" i ANSI/NIST-standarderna.



Den NIST-fil som skickas från de nationella systemen till in- och utresesystemets centrala system och lagras där ska också innehålla villkoren för registrering av fingeravtryck, inklusive den nivå av övervakning som genomförts av myndigheterna och den metod som använts för att ta fyra platta fingeravtryck, i enlighet med standarden ANSI/NIST-ITL 1-2011: Update 2015 <sup>(4)</sup> (eller senare).

### 3.1.2 Ansiktsbild

In- och utresesystemets centrala system ska lagra den ansiktsbild som tagits på plats vid gränsövergångsstället och överförs som en del av en NIST-behållare till in- och utresesystemets centrala system i enlighet med ANSI/NIST-ITL 1-2011: Update 2015 (eller senare).

I undantagsfall, när det är omöjligt att ta en ansiktsbild av tillfredsställande kvalitet av en person på plats, begärs registrering från dokumentchippet i en elektronisk maskinläsbar resehandling, när det är tekniskt möjligt, och efter en positiv elektronisk verifiering i enlighet med den process som ska beskrivas i den handbok som avses i artikel 71 i förordning (EU) 2017/2226.

Bilder som skannas från den biografiska sidan i resehandlingen ska inte användas och ska inte överföras till in- och utresesystemets centrala system.

De fotografier av viseringssökande som lagras i Informationssystemet för viseringar (VIS), inrättat enligt Europaparlamentets och rådets förordning (EG) nr 767/2008 <sup>(5)</sup>, ska inte användas för att utföra någon elektronisk biometrisk verifiering eller identifiering med in- och utresesystemets centrala system.

Av praktiska skäl är kvalitetströskeln inte obligatorisk för ansiktsbilder som tas på plats enbart för verifiering mot bilder i in- och utresesystemets centrala system. Positiv verifiering enligt de överenskomna tröskelvärdena för träffar skulle dock kräva bilder med tillräcklig kvalitet även i dessa fall.

För att uppnå den fastställda kvalitetströskeln, i synnerhet när det är omöjligt att elektroniskt hämta en ansiktsbild från chippet i den elektroniska maskinläsbara resehandlingen <sup>(6)</sup>, ska följande åtgärder gälla:

1. Om den enhet som tar ansiktsbilder registrerar bilder i en jämn ström ska omtagning göras under en tillräckligt lång tid, så att bästa möjliga bild som erhålls inom tagningsströmmen överförs till in- och utresesystemets centrala system. Om det prov som översänds är av sämre kvalitet ska det flaggas som sådant av in- och utresesystemets centrala system i enlighet med de tekniska specifikationer som avses i artikel 37.1 i förordning (EU) 2017/2226.
2. Om den enhet som tar ansiktsbilder registrerar statiska enskilda bilder då en operatör aktiverar den, ska tillräckligt många omtagningar göras så att den optimala bilden överförs till in- och utresesystemets centrala system. Om det prov som översänds är av sämre kvalitet ska det flaggas som sådant i in- och utresesystemets centrala system i enlighet med de tekniska specifikationer som avses i artikel 37.1 i förordning (EU) 2017/2226.

Riktlinjer för bästa praxis som ska följas vid tagning av ansiktsbilder i enlighet med de föregående två punkterna ska ingå i den handbok som avses i artikel 71 i förordning (EU) 2017/2226.

### 3.1.3 Bildkomprimering

#### Fingeravtrycksbilder

Den komprimeringsalgoritm som ska användas ska följa NIST-rekommendationerna. Följaktligen ska fingeravtrycksuppgifter med en upplösning på 500 ppi komprimeras med WSQ-algoritmen (ISO/IEC 19794) medan fingeravtrycksuppgifter med en upplösning på 1 000 ppi ska använda bildkomprimeringsstandarden och kodsystemet JPEG 2000 (ISO/IEC 15444-1). Den eftersträvade komprimeringsgraden är 15:1.

#### Ansiktsbilder

Bilder som komprimeras med bildkomprimeringsstandarden och kodningssystemet JPG (ISO/IEC 10918) eller JPEG 2000 (JP2) (ISO/IEC 15444-1) ska lämnas till in- och utresesystemets centrala system i enlighet med de tekniska specifikationer som avses i artikel 37.1 i förordning (EU) 2017/2226. Den maximala tillåtna bildkomprimeringsgraden är 1:20.

<sup>(4)</sup> Standarden ANSI/NIST-ITL 1-2011 *Data Format for the Interchange of Fingerprint, Facial, Scar Mark & Tattoo (SMT) Information*, tillgänglig på: <https://www.nist.gov/publications/data-format-interchange-fingerprint-facial-other-biometric-information-ansinist-itl-1-1>.

<sup>(5)</sup> Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen) (EUT L 218, 13.8.2008, s. 60).

<sup>(6)</sup> Detta kan t.ex. vara fallet om resenären inte har en elektronisk handling eller om deras resehandling innehåller en "facial image token" i stället för själva bilden, vilket är tillåtet enligt Icaos dokument 9303.

## 3.2 Biometrisk verifiering

### 3.2.1 Fingeravtryck

In- och utresesystemets centrala system ska kunna utföra biometrisk verifiering med en, två eller fyra platta fingeravtryck.

När fyra platta fingeravtryck används ska fingeravtrycksuppgifter från följande fingrar användas: pekfinger, långfinger, ringfinger och lillfinger.

När ett eller två platta fingeravtryck används ska följande fingrar ska användas som standard:

- a) Ett finger: pekfinger.
- b) Två fingrar: pekfinger och långfinger.

Alternativt kan följande fingrar användas:

- a) Ett finger: det första tillgängliga fingret i följande ordningsföljd – pekfinger, långfinger, ringfinger, lillfinger.
- b) Två fingrar: de första två tillgängliga fingrarna i följande ordningsföljd – pekfinger, långfinger och ringfinger. Lillfingret kan också övervägas som (endast) det andra fingret för verifiering om det är den enda möjligheten.

I samtliga fall:

- a) Fingeravtrycksuppgifterna ska tas från den hand som användes för registreringen.
- b) Det ska för varje enskild fingeravtrycksbild anges vilket finger det rör sig om, i enlighet med standarden ANSI/NIST-ITL 1-2011: Update 2015 (eller senare).
- c) En verifiering som baserar sig på permutation<sup>(7)</sup> säkerställer att fingeravtryck från båda uppsättningarna matchas mot varandra, oavsett deras position i uppsättningen. Det ska vara möjligt att aktivera eller inaktivera denna funktion på central nivå, så att det påverkar alla användare.

I fall där det permanent eller tillfälligt är fysiskt omöjligt att lämna fingeravtryck ska fingeravtrycken alltid anges i enlighet med standarden ANSI/NIST-ITL 1-2011: Update 2015 (eller senare) och dokumentet för gränssnittskontroll för in- och utresesystemet.

### 3.2.2 Ansiktsbild

In- och utresesystemets centrala system ska utföra biometrisk verifiering med ansiktsbilder som tagits på plats.

## 3.3 Biometrisk identifiering och sökning

### 3.3.1 För de ändamål som anges i kapitel 3 i förordning (EU) 2017/2226

För andra ändamål än brottsbekämpning ska flera sökkonfigurationer vara tillgängliga. Det ska finnas åtminstone en sökkonfiguration som uppfyller de krav som definieras i kommissionens genomförandebeslut om fastställande av prestandakrav för in- och utresesystemet<sup>(8)</sup> och ytterligare möjliga sökkonfigurationer som har olika specifikationer för noggrannhetsprestanda (mindre strikta och mer strikta).

Användning av fingeravtryck

För andra ändamål än brottsbekämpning ska in- och utresesystemets centrala system utföra biometrisk identifiering och sökning antingen med fyra platta fingeravtryck eller med fyra platta fingeravtryck kombinerade med den ansiktsbild som tagits på plats, och endast med biometriska uppgifter som uppfyller de tillämpliga kvalitetströsklarna. Den biometriska identifieringen ska utföras med fingeravtrycksuppgifterna med högst en bild per fingertyp (NIST-identifikation 1–10).

Fingeravtrycksuppgifter från följande fingrar ska användas: pekfingret, långfingret, ringfingret och lillfingret. Fingeravtryck från samma hand ska användas, företrädesvis den högra handen.

Fingeravtrycksuppgifterna ska åtföljas av en korrekt angivelse av vilket finger de avser. Vid permanent eller tillfälligt fysiskt hinder ska detta alltid anges för fingeravtrycken i enlighet med standarden ANSI/NIST-ITL 1-2011: Update 2015<sup>(9)</sup> (eller senare) och eventuella resterande fingrar ska användas.

<sup>(7)</sup> Permutation är en särskild konfigureringsmetod i systemet för biometrisk matchning, som säkerställer att fingeravtryck från båda uppsättningarna matchas mot varandra, oavsett deras position i uppsättningen. Detta garanterar att potentiella mänskliga misstag undviks vad gäller fingrarnas ordningsföljd och säkrar största möjliga biometriska noggrannhet vid verifieringen.

<sup>(8)</sup> C(2019) 1260.

<sup>(9)</sup> Se ovan.

Om identifieringen sker inom ett annat sammanhang än in- och utresekontroller ska in- och utresesystemets centrala system kunna godta rullade fingeravtryck från myndigheter med åtkomst till in- och utresesystemet och som har rätt att använda även rullade fingeravtryck enligt annan EU-lagstiftning. Om myndigheten utför en identifiering med fingrar från båda händerna, ska in- och utresesystemets centrala system utföra två identifieringar: en med högra handens fingrar och en med vänstra handens fingrar.

#### Användning av ansiktsbilden

In- och utresesystemets centrala system ska utföra biometriska sökningar med ansiktsbilder som tas på plats i kombination med fingeravtrycksuppgifter i enlighet med de regler som anges i ovanstående avsnitt "Användning av fingeravtryck".

#### 3.3.2 För brottsbekämpande ändamål

Sökningar får, endast för brottsbekämpande ändamål, utföras med följande biometriska uppgifter:

- Uppsättningar fingeravtrycksuppgifter som innehåller minst ett fingeravtryck.
- Rullade och osegmenterade "slap"-fingeravtrycksuppgifter.
- Fingeravtrycksspår.
- Ansiktsbild i kombination med fingeravtrycksuppgifter.
- Endast ansiktsbild.

När det gäller sökningar på fingeravtryck ska permutation<sup>(10)</sup> av händer utföras inom ramen för sökningar för brottsbekämpande ändamål. Användningen av permutation av händer ska kunna konfigureras (aktiveras/inaktiveras) centralt, så att det påverkar alla användare.

Identifiering för brottsbekämpande ändamål med fingeravtryck ska utföras mot alla lagrade fingeravtryck utan beaktande av fingeravtryckens kvalitet, eller endast mot sådana som uppfyller en viss kvalitetströskel som fastställs i den användarsökkonfiguration som används för en sökning. In- och utresesystemets centrala system ska tillhandahålla matchande biometriska uppgifter till den begärande medlemsstaten tillsammans med en angivelse om kvaliteten på de hämtade fingeravtrycken. Vid en träff mot fingeravtryck av låg kvalitet ska den brottsbekämpande myndigheten underrättas om att ytterligare verifiering krävs för att bekräfta träffen. De tröskelvärden som anger "låg uppgiftskvalitet" och kräver ytterligare verifiering ska fastställas i de tekniska specifikationer som avses i artikel 37.1 i förordning (EU) 2017/2226.

Biometriska sökningar med endast ansiktsbildsfunktionen får uteslutande göras för det syfte som anges i artikel 32.2 i förordning (EU) 2017/2226. I det fallet ska användaren ange en begränsning av antalet potentiella träffar. Det högsta antalet resultat är fyrahundra. I första steget ska användaren få åtkomst till de tvåhundra närmaste träffarna. Om det är nödvändigt ska systemet ge åtkomst till de återstående tvåhundra akterna, om användaren bekräftar att den första sökningen inte ledde till en träff.

---

<sup>(10)</sup> Permutation av händer gör det möjligt att jämföra ena handens fingeravtryck med andra handens fingeravtryck. Detta förbättrar träffnoggrannheten när det inte är känt vilken hand provet kommer från.