EUROPÄISCHE
KOMMISSION

Brüssel, den 25.2.2019
C(2019) 1280 final

ANNEX

ANHANG

des

Durchführungsbeschlusses der Kommission

zur Festlegung der Spezifikationen für die Qualität, Auflösung und Verwendung von Fingerabdrücken und Gesichtsbildern für die biometrische Verifizierung und Identifizierung im Einreise-/Ausreisesystem (EES)

ANHANG

1. QUALITÄT

1.1. Schwellenwerte

1.1.1. Fingerabdrücke

Erfassung

Bei der Erfassung wird anhand von Version 2.0 (oder einer neueren Version) der Qualitätsmetrik für Fingerabdruckbilder (NFIQ)[1] des amerikanischen Normeninstituts NIST (National Institute of Standards and Technology) überprüft, ob die Qualität der erfassten Fingerabdruckdaten die Schwellenwerte erfüllt, die in den in Artikel 37 Absatz 1 der Verordnung (EU) 2017/2226 genannten technischen Spezifikationen festzulegen sind.
Zum Zwecke der Erfassung erfolgt die Bewertung der Qualität der Fingerabdruckdaten:

- auf nationaler Ebene durch die Mitgliedstaaten bei der Erfassung vor der Übermittlung an das EES-Zentralsystem (CS-EES), optional mithilfe eines Tools, das von eu-LISA bereitgestellt, gepflegt und aktualisiert wird, sowie
- auf zentraler Ebene.

Verifikation

Zum Zwecke der Verifikation wird empfohlen, dass die Mitgliedstaaten die Qualität der Fingerabdruckdaten zum Zeitpunkt der Erfassung vor der Übermittlung an das CS-EES entweder anhand von Version 2.0 (oder einer neueren Version) der NFIQ-Metrik (Qualitätsmetrik für die Bewertung von Fingerabdruckbildern) des NIST bewerten, oder – wenn dies technisch nicht möglich ist – anhand einer anderen Metrik, die vorzugsweise mit der NFIQ-Metrik Version 2.0 (oder einer neueren Version) korreliert werden sollte. Die Korrelation wird a priori hergestellt. Wird bei der Qualitätsmessung der Standard der NFIQ-Qualitätsmetrik Version 2.0 (oder einer neueren Version) erreicht, so muss dieses Ergebnis gleichzeitig mit den Fingerabdruckdaten an das CS-EES übermittelt werden.

1.1.2. Gesichtsbilder

Die Qualität der Gesichtsbilder, einschließlich von Nah-Infrarot-Bildern, muss die Schwellenwerte in den technischen Spezifikationen nach Artikel 37 Absatz 1 der Verordnung (EU) 2017/2226 sowie die Anforderungen an Frontalaufnahmen gemäß ISO/IEC 19794-5:2011 erfüllen. Die Bewertung der Gesichtsbildqualität erfolgt auf nationaler Ebene durch die Mitgliedstaaten zum Zeitpunkt der Erfassung vor der Übermittlung an das EES-Zentralsystem (CS-EES), optional mithilfe eines Tools, das von eu-LISA bereitgestellt, gepflegt und aktualisiert wird. Der Qualitätsprüfalgorithmus für Gesichtsbilder muss mit den in ISO/IEC 19794-5:2011 dargelegten Kriterien in Einklang stehen.

Der Schwellenwert für die Qualität der Gesichtsbilder wird unter Verwendung eines Algorithmus zur Bewertung der Gesichtsbildqualität basierend auf den Qualitätskriterien nach ISO 19794-5 festgelegt und gewährleistet Qualitätsprüfungen analog zu den im CS-EES implementierten Prüfungen.[2]

---

[1] https://www.nist.gov/services-resources/software/development-nfiq-20

[2] Wenn möglich, werden die Gesichtsbilder anhand der Kriterien unter Punkt 3.9 des ICAO-Dokuments 9303 sowie der Empfehlungen der französischen Behörden zu Anträgen für französische Visa bewertet und validiert.

1.2. Leistungswerte für die Genauigkeit biometrischer Systeme

Begriffsbestimmungen

In Artikel 3 der Verordnung (EU) 2017/2226 sind folgende Leistungswerte für die biometrische Genauigkeit definiert:

> 29. „Quote der Erfassungsfehler“ [bezeichnet] den Anteil der Registrierungen mit nicht ausreichender Qualität der biometrischen Erfassung;
>
> 30. „Quote der falsch positiven Identifizierungen“ [bezeichnet] den Anteil der Treffer bei einer biometrischen Suche, die nicht zu dem überprüften Reisenden gehören;
>
> 31. „Quote der falsch negativen Identifizierungen“ [bezeichnet] den Anteil der nicht erhaltenen Treffer bei einer biometrischen Suche, obwohl die biometrischen Daten des Reisenden registriert waren.

Die unter den Punkten 30 und 31 genannte „biometrische Suche“ ist identisch mit der biometrischen Identifizierung oder „1 bis N“-Suche.

Im Einklang mit Artikel 36 Absatz 1 Buchstabe g der Verordnung (EU) 2017/2226 können im Durchführungsrechtsakt zusätzliche Werte für die biometrische Erkennungsleistung festgelegt werden.

Die Falschübereinstimmungsrate (False Match(ing) Rate – FMR) ist der Anteil der Täuschungsversuche („impostor attempts“), bei denen fälschlicherweise eine Übereinstimmung mit einem Template eines anderen Objekts (biometrisches Template einer Person) festgestellt wird.

Die Falschnichtübereinstimmungsrate (False Non-Match(ing) Rate – FNMR) ist der Anteil der authentischen Versuche („genuine attempts“), bei denen fälschlicherweise eine Nichtübereinstimmung mit einem Template desselben Objekts festgestellt wird.

Ein authentischer Versuch ist ein einzelner Versuch eines Nutzers, eine Übereinstimmung mit seinem eigenen gespeicherten Template zu erzielen. Ein Täuschungsversuch ist das Gegenteil: Das Template eines Nutzers weist eine Übereinstimmung mit dem Template einer anderen Person auf.

1.2.1. Quote der Erfassungsfehler

Der Zielwert für die Quote der Erfassungsfehler beträgt Null. Die Mitgliedstaaten müssen ein qualitätsorientiertes Erfassungsverfahren nutzen, um derartige Fehler zu vermeiden.

1.2.2. Genauigkeit der biometrischen Verifikation

Die Falschnichtübereinstimmungsrate (FNMR) darf bei einer Falschübereinstimmungsrate (FMR) von 0,05 % (5 pro 10 000) folgende Werte nicht überschreiten:

Art	FMR	FNMR
Fingerabdruck	0,05 %	< 0,5 %
Gesichtsbild	0,05 %	< 1 %

1.2.3. Genauigkeit der biometrischen Identifizierung

Die Quote der falsch negativen Identifizierungen (FNIR) darf bei einer Quote der falsch positiven Identifizierungen (FPIR) von 0,1 % (1 pro 1000) folgende Werte nicht überschreiten:

Art	FPIR	FNIR
Fingerabdruck	0,1 %	< 1,5 %
Gesichtsbild und Fingerabdruck (multimodal)	0,1 %	< 1 %

1.3. Überwachung der Genauigkeit der biometrischen Erkennungsleistung

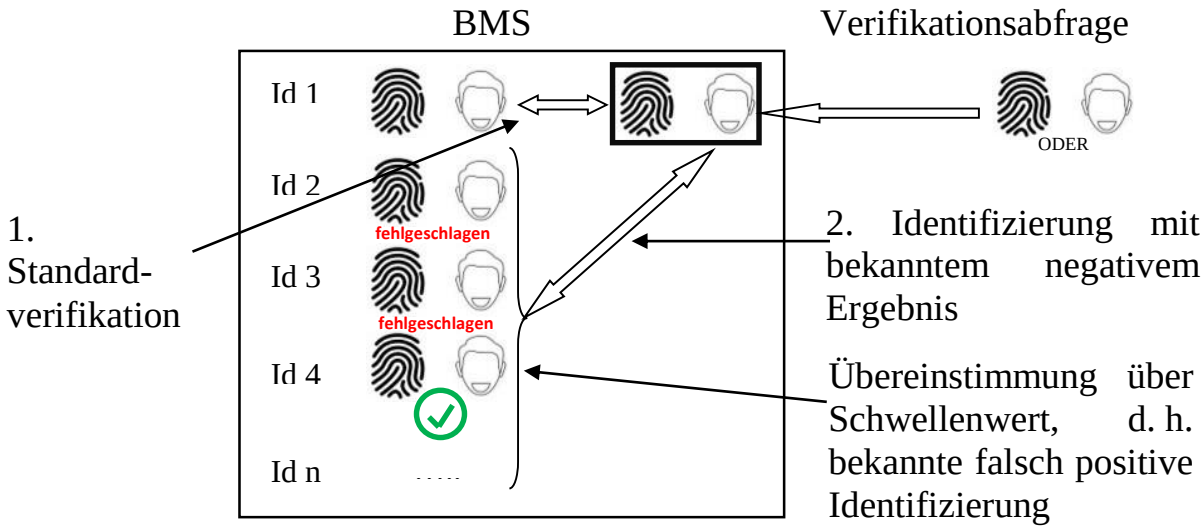
Die Genauigkeit der biometrischen Erkennungsleistung wird anhand einer repräsentativen Stichprobe authentischer Daten gemessen, die jeder einzelne Mitgliedstaat routinemäßig an ausgewählten Grenzübergangsstellen erfasst. Die Messung erfolgt zentral, vollautomatisch und erfordert keinen Zugang des Bedienungspersonals zu personenbezogenen Daten.

Die Messung der Erkennungsleistung bei Abgleichen mit biometrischem Material muss nicht kontinuierlich erfolgen: Sie kann aktiviert oder deaktiviert werden, muss von eu-LISA jedoch regelmäßig (mindestens monatlich) durchgeführt werden.

Bei der Messung der Erkennungsleistung bei Abgleichen mit biometrischem Material werden die biometrischen Daten selbst nicht verwendet. Die für die Genauigkeitsmessung verwendeten Templates von Bildern werden nach dem Bewertungsprozess automatisch gelöscht. Die Ergebnisse der Leistungsmessung dürfen keine personenbezogenen Daten enthalten.

1.3.1. Messung der FPIR (Quote der falsch positiven Identifizierungen)

Die nachfolgende Abbildung zeigt, dass im biometrischen Abgleichsystem (BMS – Biometric Matching System) Templates für das biometrische Sample der Fingerabdrücke sowie des Gesichtsbilds für eine Anzahl „n“ von Identitäten vorhanden sind.



Beschreibung des Messverfahrens:

1. Eine der Erfassung im EES unterliegende Person stellt ein Sample einer oder beider der zwei biometrischen Modalitäten (Fingerabdrücke und Gesichtsbild) zur Verfügung.

2. Die biometrische Verifikation erfolgt anhand der biometrischen Referenzdaten, die der Identität der Person entsprechen (Schritt 1 in der Abbildung: „Standardverifikation“).

3. Um einen zusammenhängenden Sample-Satz zu erhalten, wird die zweite biometrische Modalität derselben Person verwendet (die entweder zusammen mit Schritt 1 zur Verfügung gestellt wurde oder aus den biometrischen Referenzdaten, die der biometrischen Identität der Person entsprechen, extrahiert werden kann). Anhand der kombinierten biometrischen Daten wird eine Identifizierung basierend auf allen biometrischen Referenzbildern – ohne die biometrischen Daten der Person, zu der das biometrische Sample gehört – durchgeführt (Schritt 2 der Abbildung: „Identifizierung mit bekanntem negativem Ergebnis“). Bei diesem Identifizierungsverfahren ist das erwartete Ergebnis Null, da das richtige biometrische Sample absichtlich aus dem Vergleich entfernt wurde.

   Wenn die in Schritt 2 verwendete Modalität mit dem Fingerabdruck übereinstimmt, so wird eine Identifizierung (zur Bewertung der Genauigkeit der Fingerabdruckidentifizierung) unter denselben Bedingungen wie in Unterabsatz 1 durchgeführt.

4. Wird bei der biometrischen Identifizierung ein biometrisches Sample als Treffer gemeldet (mit der Angabe „Übereinstimmung über dem Schwellenwert“), ist dies eine bekannte falsch *positive* Identifizierung (das Ergebnis ist eine andere als die erwartete Person).

Die Schritte 1 und 2 sind Teil des Verfahrens zur Identitätsverifikation im EES. Die Schritte 3 und 4 sind nicht Teil des Verfahrens zur Identitätsverifikation und dienen der Messung der Genauigkeit der biometrischen Erkennungsleistung.

Die FPIR (Quote der falsch positiven Identifizierungen) wird wie folgt berechnet:

$$FPIR = \frac{\textit{Anzahl der Identifizierungen, bei denen eine Kennzeichnung rückgemeldet wird}}{\textit{Anzahl aller bekannten Identifizierungstransaktionen mit negativem Ergebnis}}$$

1.3.2. Messung der FNIR (Quote der falsch negativen Identifizierungen)

Die Abbildung unter Punkt 1.3.1 veranschaulicht nachfolgende Ausführungen.

Das Messverfahren folgt der nachstehenden Logik, wobei die ersten beiden Schritte stets dieselben sind, da sie Teil des Verfahrens zur Identitätsverifikation im EES darstellen.

1. Eine der Erfassung im EES unterliegende Person stellt ein Sample einer oder beider der zwei biometrischen Modalitäten zur Verfügung.

2. Die biometrische Verifikation erfolgt anhand der biometrischen Referenzdaten, die der Identität der Person entsprechen (Schritt 1 in der Abbildung: „Standardverifikation“).

3. Um einen zusammenhängenden Sample-Satz zu erhalten, wird eine zweite biometrische Modalität entweder von derselben Person verwendet – wenn beide biometrische Modalitäten in Schritt 1 zur Verfügung gestellt wurden – oder von einer anderen Person, für die die Schritte 1 und 2 dieses Verfahrens durchgeführt wurden. Anhand der kombinierten biometrischen Daten wird eine Identifizierung basierend auf allen biometrischen Referenzbildern – einschließlich der biometrischen Daten der Person(en), zu der (denen) das biometrische Sample gehört – durchgeführt. Bei

diesem Identifizierungsverfahren wird erwartet, dass eine Übereinstimmung erzielt wird, da das übereinstimmende biometrische Sample im Vergleich enthalten ist.

4. Wenn die in Schritt 2 verwendete Modalität mit dem Fingerabdruck übereinstimmt, so wird eine Identifizierung (zur Bewertung der Genauigkeit der Fingerabdruckidentifizierung) unter denselben Bedingungen wie in Absatz 3 durchgeführt.

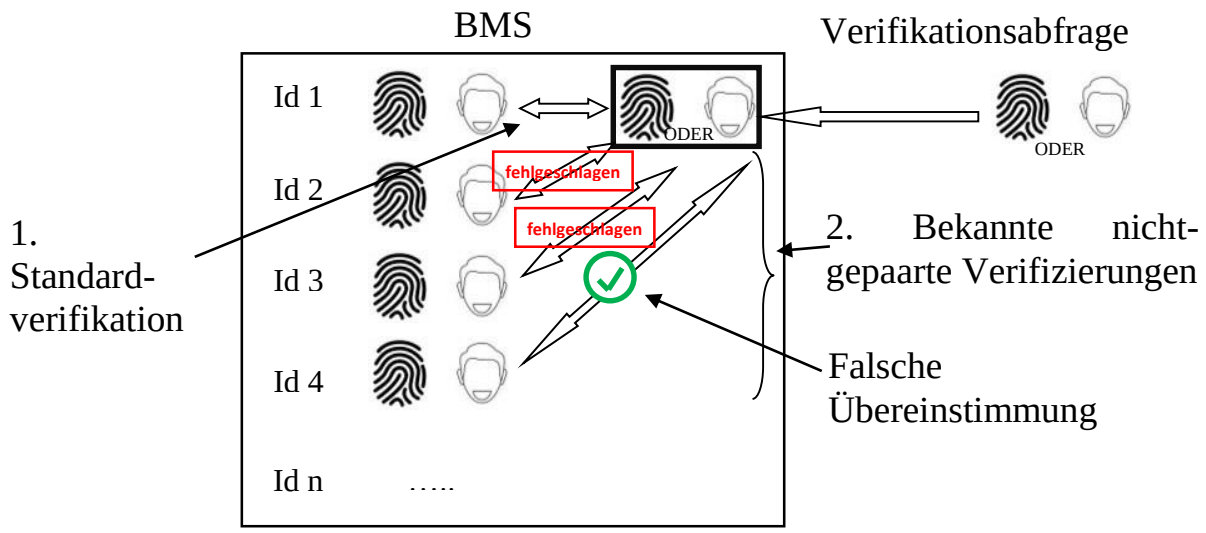
5. Wenn bei der biometrischen Identifizierung das erwartete biometrische Sample nicht in der Trefferliste erscheint (mit der Angabe „Übereinstimmung über dem Schwellenwert“), handelt es sich um eine bekannte falsch *negative* Identifizierung.

Die Schritte 1 und 2 sind Teil des Verfahrens zur Identitätsverifikation im EES. Die Schritte 3 und 4 sind nicht Teil des Verfahrens zur Identitätsverifikation und dienen der Messung der Genauigkeit der biometrischen Erkennungsleistung.

Die FNIR (Quote der falsch negativen Identifizierungen) wird wie folgt berechnet:

$$FNIR = \frac{\textit{Anzahl der Identifizierungen, bei denen die korrekte Kennzeichnung des biometrischen Subjekts nicht rückgemeldet wird}}{\textit{Anzahl aller Identifizierungstransaktionen}}$$

1.3.3. Messung der Genauigkeit der biometrischen Erkennungsleistung zum Zwecke der Verifikation (Falschübereinstimmungsrate und Falschnichtübereinstimmungsrate)



Das Messverfahren folgt nachstehender Logik:

1. Eine der Erfassung im EES unterliegende Person stellt ein Sample einer der beiden biometrischen Modalitäten zur Verfügung.

2. Die biometrische Verifikation erfolgt anhand der biometrischen Referenzdaten, die der Identität der Person entsprechen (Schritt 1 in der Abbildung: „Standardverifikation“).

Die Schritte 1 und 2 sind Teil des Verfahrens zur Identitätsverifikation im EES. Im nächsten Schritt wird die Genauigkeit der biometrischen Erkennungsleistung gemessen.

3. Die Verifikation des biometrischen Samples erfolgt anhand einer Reihe anderer biometrischer Samples, die nach dem Zufallsprinzip aus den biometrischen Referenzbildern ausgewählt werden und keine biometrischen Daten der betroffenen Person enthalten. Das erwartete Ergebnis ist, dass die Verifikationen keine Übereinstimmung ergeben (siehe Punkt 2 der Abbildung „bekannte nicht-gepaarte Verifizierungen“). Jede Übereinstimmung wäre eine falsche Übereinstimmung.

Schritt 3 ermöglicht die Berechnung der **Falschübereinstimmungsrate** (Übereinstimmung mit einer anderen Person als dem Inhaber der Daten):

$$FMR = \frac{\textit{Trefferzahl bei nicht-gepaarten Vergleichen}}{\textit{Anzahl der nicht-gepaarten Vergleiche}}$$

Anmerkung: Die Zahl der nicht-gepaarten Vergleiche ist die Anzahl der unter Schritt 3 durchgeführten Vergleiche.

Schritt 2 ermöglicht wie folgt die Berechnung der **Falschnichtübereinstimmungsrate** (die Übereinstimmung wird nicht mit dem Inhaber der biometrischen Daten erzielt), wenn die Identität auf andere Weise bestätigt wurde:

$$FNMR = \frac{\textit{Anzahl der Vergleiche mit fehlenden Treffern}}{\textit{Anzahl der angenommenen gepaarten Vergleiche}}$$

Anmerkung: Die Anzahl der gepaarten Vergleiche wird als „angenommen“ bezeichnet, da es keine absolute Gewissheit gibt, dass sich im Satz der Identitäten, auf denen der Vergleich basiert, kein Impostor befindet.

1.4. Ersetzen biometrischer Daten (zu Qualitätsverbesserungszwecken oder zur Ersetzung eines aus dem eMRTD extrahierten Lichtbildes durch eine Live-Gesichtsbildaufnahme aus den CS-EES-Referenzbildern)

Biometrische Daten dürfen nur nach erfolgreicher biometrischer Identitätsverifikation ersetzt werden.

1.4.1. Ersetzen gespeicherter Fingerabdruckdaten

Das Verfahren für das Ersetzen gespeicherter Fingerabdruckdaten, die nicht den Qualitätsanforderungen entsprechen, wird in dem in Artikel 71 der Verordnung (EU) 2017/2226 genannten Handbuch festgelegt.

Werden die Daten der linken Hand durch Daten der rechten Hand ersetzt (oder umgekehrt), wird anhand der neu erfassten Fingerabdrücke eine Identifizierung durchgeführt, um sicherzustellen, dass es keine Übereinstimmung mit einer anderen, bereits im System registrierten Identität gibt.

1.4.2. Ersetzen gespeicherter Gesichtsbilder

Das Verfahren für das Ersetzen eines gespeicherten Gesichtsbildes, das nicht den Qualitätsanforderungen entspricht oder das vom Chip des elektronischen maschinenlesbaren

Reisedokuments extrahiert wurde, wird in dem in Artikel 71 der Verordnung (EU) 2017/2226 genannten Handbuch festgelegt.

2. AUFLÖSUNG

2.1. Fingerabdrücke

Die für das CS-EES bestimmten Fingerabdruckdaten müssen eine Nennauflösung von 500 oder 1000 ppi (zulässige Abweichung +/- 10 ppi) mit 256 Graustufen aufweisen.

Die Fingerabdruckdaten sind gemäß dem Standard ANSI/NIST-ITL 1-2011, aktualisierte Version 2015 (oder neuere Version), und nach Maßgabe der technischen Spezifikationen nach Artikel 37 Absatz 1 der Verordnung (EU) 2017/2226 zu übermitteln.

2.2. Gesichtsbilder

2.2.1. Definition

Die für das CS-EES bestimmten Live-Gesichtsbildaufnahmen (Hochformat) müssen eine Auflösung von mindestens 600 x 800 Pixel und höchstens 1200 x 1600 Pixel aufweisen.

Das Gesicht muss innerhalb des Bildes ausreichend Platz einnehmen, sodass der Abstand der Augenmittelpunkte mindestens 120 Pixel beträgt.

2.2.2. Farben

Live-Gesichtsbildaufnahmen müssen Farbbildaufnahmen sein. In Ausnahmefällen, in denen keine Farbbildaufnahme möglich ist, kann eine Graustufen- oder ein Nah-Infrarot-Aufnahme verwendet werden. Weist das Graustufen- oder Nah-Infrarot-Bild eine ausreichende Qualität auf, kann es zur Verifikation oder Identifizierung, jedoch nicht zur Erfassung verwendet werden. Für die Erfassung sind Graustufenbilder nur dann zugelassen, wenn sie vom Chip des Reisedokuments extrahiert wurden.

Spezifische Vorschriften für Nah-Infrarot-Gesichtsbilder werden im Einklang mit Artikel 71 der Verordnung (EU) 2017/2226 im Handbuch festgelegt.

3. VERWENDUNG BIOMETRISCHER DATEN

3.1. Eingabe und Speicherung

3.1.1. Fingerabdrücke

Im CS-EES werden die Daten von vier flach[3] aufgenommenen Fingerabdrücken gespeichert. Sofern möglich, werden die Fingerabdrücke folgender Finger der rechten Hand verwendet: Zeigefinger, Mittelfinger, Ringfinger, kleiner Finger.

Wenn es nicht möglich ist, von den genannten Fingern der rechten Hand Fingerabdrücke abzunehmen, werden die vier Fingerabdrücke – soweit möglich – von der linken Hand erfasst. Ist es nur vorübergehend nicht möglich, vier Fingerabdrücke der rechten Hand zu erhalten, werden die Fingerabdruckdaten ausdrücklich gekennzeichnet; wenn der vorübergehende Hinderungsgrund nicht mehr besteht, werden die Fingerabdruckdaten der rechten Hand im Einklang mit den technischen Spezifikationen nach Artikel 37 Absatz 1 der Verordnung (EU) 2017/2226 (vorübergehende Unmöglichkeit) bei der Ausreise oder der folgenden Einreise erfasst.

[3] Der Begriff „flat“ (flach) entspricht der ISO/IEC-Terminologie und wird synonym zu „plain“ (flach) gemäß dem ANSI//NIST-Standard verwendet.

Um den geltenden Schwellenwert zu erfüllen, sollte die Fingerabdruckdatenerfassung bei jeder betroffenen Person erforderlichenfalls zweimal wiederholt werden (d. h. insgesamt sollten drei Erfassungsversuche stattfinden). Bei den Wiederholungsversuchen sollten die gleichen Finger wie beim ersten Versuch herangezogen werden.

Für Fingerabdruckdaten, die den geltenden Qualitätsschwellenwert nicht erfüllen, gilt:

(1) Sie werden im CS-EES gespeichert;

a) anhand dieser Daten werden biometrische Verifikationen durchgeführt;

b) anhand von Fingerabdrücken, die den Qualitätsschwellenwert nicht erfüllen, werden – außer zu Gefahrenabwehr- und Strafverfolgungszwecken – keine biometrischen Identifizierungen durchgeführt;

(2) Sie werden vom nationalen System im Einklang mit den technischen Spezifikationen nach Artikel 37 Absatz 1 der Verordnung (EU) 2017/2226 (technische Unmöglichkeit) gekennzeichnet, damit diese Daten beim nächsten Grenzübertritt erfasst werden können.

In der NIST-Datei, die von den nationalen Systemen an das CS-EES übermittelt und dort gespeichert wird, muss zudem erfasst sein, unter welchen Bedingungen die Fingerabdruckregistrierung erfolgt ist, u. a. in wieweit der Vorgang von den Behörden überwacht wurde und welche Methode für die Erfassung flacher Abdrücke von vier Fingern gemäß dem Standard ANSI/NIST-ITL 1-2011, aktualisierte Version 2015[4] (oder neuere Version) verwendet wurde.

3.1.2. Gesichtsbild

Das CS-EES speichert die Live-Gesichtsbildaufnahme, die an der Grenzübergangsstelle erstellt und gemäß dem Standard ANSI/NIST-ITL 1-2011, aktualisierte Version 2015 (oder neuere Version), als Teil eines NIST-Containers an das CS-EES übermittelt wurde.

In Ausnahmefällen, wenn es unmöglich ist, eine Live-Gesichtsbildaufnahme von ausreichender Qualität zu erhalten, wird der Chip des elektronischen maschinenlesbaren Ausweisdokuments (eMRTD) für die Erfassung herangezogen, sofern technisch Zugang dazu besteht und die Daten nach dem im Handbuch nach Artikel 71 der Verordnung (EU) 2017/2226 festgelegten Verfahren erfolgreich verifiziert wurden.

Von der Personaldatenseite des Reisedokuments gescannte Bilder dürfen nicht verwendet und an das CS-EES übermittelt werden.

Lichtbilder von Visumantragstellern, die in dem nach Maßgabe der Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates eingerichteten Visa-Informationssystem (VIS)[5] gespeichert sind, dürfen nicht für elektronische biometrische Verifikationen oder Identifizierungen mit dem CS-EES herangezogen werden.

Aus praktischen Gründen ist der Qualitätsschwellenwert, der für Live-Gesichtsbildaufnahmen ausschließlich zu Zwecken der Verifikation anhand der im CS-EES gespeicherten Bilder gilt, nicht verbindlich. Für eine erfolgreiche Verifikation unter Berücksichtigung der vereinbarten

[4] Standard ANSI/NIST-ITL 1-2011 „Data Format for the Interchange of Fingerprint, Facial, Scarmark & Tattoo (SMT) Information“, abrufbar unter: https://www.nist.gov/publications/data-format-interchange-fingerprint-facial-other-biometric-information-ansinist-itl-1-1.

[5] Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung) (ABl. L 218 vom 13.8.2008, S. 60).

Schwellenwerte für die Übereinstimmung wären jedoch auch in diesen Fällen Bilder von ausreichender Qualität erforderlich.

Um sicherzustellen, dass der festgelegte Qualitätsschwellenwert erreicht wird, insbesondere wenn es nicht möglich ist, ein Gesichtsbild aus dem Chip eines eMRTD[6] elektronisch zu extrahieren, ist folgendermaßen vorzugehen:

(1) In Fällen, in denen die für Gesichtsbildaufnahmen zuständige Stelle Bilder in einer kontinuierlichen Serie erfasst, erfolgt die erneute Bilderfassung über einen ausreichenden Zeitraum hinweg, damit das optimale Bild aus dem Erfassungsstrom an das CS-EES übermittelt wird. Wird ein Sample mit niedriger Qualität übermittelt, so wird dieses durch das CS-EES nach Maßgabe der technischen Spezifikationen nach Artikel 37 Absatz 1 der Verordnung (EU) 2017/2226 als solches gekennzeichnet.

(2) In Fällen, in denen die für Gesichtsbildaufnahmen zuständige Stelle statische, manuell aufgenommene Einzelbilder erfasst, wird die Erfassung ausreichend oft wiederholt, sodass ein optimales Bild an das CS-EES übermittelt werden kann. Wird ein Sample mit niedriger Qualität übermittelt, so wird dieses im CS-EES nach Maßgabe der technischen Spezifikationen nach Artikel 37 Absatz 1 der Verordnung (EU) 2017/2226 als solches gekennzeichnet.

Es wird ein Leitfaden mit bewährten Verfahren in das Handbuch nach Artikel 71 der Verordnung (EU) 2017/2226 aufgenommen, der bei Gesichtsbildaufnahmen gemäß den zwei vorstehenden Punkten dieses Absatzes zu berücksichtigen ist.

3.1.3. Bildkompression

Fingerabdruckbilder

Der zu verwendende Kompressionsalgorithmus muss den NIST-Empfehlungen entsprechen. Somit werden Fingerabdruckdaten mit einer Auflösung von 500 ppi mit dem WSQ-Algorithmus (ISO/IEC 19794) komprimiert. Bei Fingerabdruckdaten mit 1000 ppi hingegen finden JPEG 2000 (ISO/IEC 15444-1) Bildkompressionsstandard und Kodierungssystem Anwendung. Die Zielkompressionsrate beträgt 15:1.

Gesichtsbilder

Mit JPG (ISO/IEC 10918) oder JPEG 2000 (JP2) (ISO/IEC 15444-1) Bildkompressionsstandard und Kodierungssystem komprimierte Bilder werden nach Maßgabe der technischen Spezifikationen nach Artikel 37 Absatz 1 der Verordnung (EU) 2017/2226 an das CS-EES übermittelt. Die maximal zulässige Bildkompressionsrate beträgt 1:20.

3.2. Biometrische Verifikationen

3.2.1. Fingerabdrücke

Das CS-EES muss in der Lage sein, biometrische Verifikationen anhand von einem, zwei oder vier flach aufgenommenen Fingerabdrücken durchzuführen.

Werden flache Abdrücke von vier Fingern herangezogen, sind die Fingerabdruckdaten folgender Finger zu verwenden: Zeigefinger, Mittelfinger, Ringfinger, kleiner Finger.

[6] Die kann der Fall sein, wenn der Reisende kein elektronisches Dokument besitzt oder beispielsweise sein Reisedokument – was gemäß ICAO-Dokument 9303 zulässig ist – ein Gesichtsbild-Token statt des eigentlichen Bildes enthält.

Werden flache Abdrücke von einem Finger oder zwei Fingern herangezogen, sind folgende Finger zu verwenden:

a) Ein Finger: Zeigefinger;

b) Zwei Finger: Zeigefinger und Mittelfinger.

Alternativ können folgende Finger verwendet werden:

a) Ein Finger: erster verfügbarer Finger in folgender Reihenfolge – Zeigefinger, Mittelfinger, Ringfinger, kleiner Finger.

b) Zwei Finger: erste beide verfügbare Finger in folgender Reihenfolge – Zeigefinger, Mittelfinger und Ringfinger. Der kleine Finger kann (ausschließlich) für die Verifikation als zweiter Finger herangezogen werden, falls keine andere Möglichkeit besteht.

In allen Fällen gilt:

a) Die Fingerabdruckdaten werden von der Hand genommen, die für die Erfassung verwendet wird.

b) Die Fingerposition wird für jedes einzelne Fingerabdruckbild nach dem Standard ANSI/NIST-ITL 1-2011, aktualisierte Version 2015 (oder neuere Version), angegeben.

c) Anhand einer Verifikation nach dem Permutationsverfahren[7] wird sichergestellt, dass die Fingerabdrücke von jedem der beiden Sätze unabhängig von ihrer Position im Satz miteinander abgeglichen werden. Diese Funktion muss auf zentraler Ebene aktiviert oder deaktiviert werden können und wirkt sich auf alle Nutzer aus.

Ist die Abnahme von Fingerabdrücken dauerhaft oder vorübergehend physisch nicht möglich, werden die Fingerabdrücke stets nach dem Standard ANSI/NIST-ITL 1-2011, aktualisierte Version 2015 (oder neuere Version), und der Dokumentation zur Schnittstellenansteuerung für das EES (EES Interface Control Document) angegeben.

3.2.2. Gesichtsbild

Das CS-EES führt biometrische Verifikationen anhand von Live-Gesichtsbildaufnahmen durch.

3.3. Biometrische Identifizierungen und Suchen

3.3.1. Für die in Kapitel III der Verordnung (EU) 2017/2226 genannten Zwecke

Für Zwecke, die nicht der Gefahrenabwehr und Strafverfolgung dienen, müssen Mehrfachsuchkonfigurationen zur Verfügung stehen. Es muss mindestens eine Suchkonfiguration geben, die die im Durchführungsbeschluss der Kommission zur Festlegung der Leistungsanforderungen für das Einreise-/Ausreisesystem (EES)[8] definierten Kriterien erfüllt, sowie weitere mögliche Suchkonfigurationen, für die hinsichtlich der Genauigkeit der Erkennungsleistung andere (weniger strikte oder striktere) Spezifikationen gelten.

Verwendung von Fingerabdrücken

[7] Permutation ist ein spezifischer Konfigurationsmodus des Systems für den Abgleich biometrischer Daten, mit dem sichergestellt wird, dass die Fingerabdrücke von jedem der beiden Sätze unabhängig von ihrer Position im Satz miteinander abgeglichen werden. Dadurch werden potenzielle menschliche Fehler hinsichtlich der Reihenfolge der Finger eliminiert und größtmögliche biometrische Genauigkeit bei der Verifikation sichergestellt.

[8] C(2019)1260.

Für Zwecke, die nicht der Gefahrenabwehr und Strafverfolgung dienen, führt das CS-EES biometrische Identifizierungen und Suchen entweder anhand der flachen Abdrücke von vier Fingern oder mit den flachen Abdrücken von vier Fingern in Kombination mit der Live-Gesichtsbildaufnahme durch, wobei nur biometrische Daten herangezogen werden, die die geltenden Qualitätsschwellenwerte erfüllen. Für die biometrische Identifizierung anhand der Fingerabdruckdaten wird höchstens ein Bild pro Finger (NIST-Kennzeichnung 1 bis 10) verwendet.

Dabei werden Fingerabdruckdaten folgender Finger verwendet: Zeigefinger, Mittelfinger, Ringfinger, kleiner Finger. Es werden die Fingerabdrücke derselben Hand verwendet, beginnend mit der rechten Hand.

Die Fingerabdruckdaten müssen die jeweils korrekte Fingerbezeichnung enthalten. Bei einem dauerhaften oder vorübergehenden physischen Hinderungsgrund werden die Fingerabdrücke stets nach dem Standard ANSI/NIST-ITL 1-2011[9], aktualisierte Version 2015 (oder neuere Version), angegeben und die vorhandenen Finger verwendet.

In Fällen, in denen Identifizierungen nicht im Rahmen von Grenzübertrittskontrollen durchgeführt werden, muss das CS-EES in der Lage sein, von Behörden mit Zugang zum EES, die gemäß anderer europäischer Rechtsvorschriften gerollte Fingerabdrücke verwenden dürfen, solche Fingerabdrücke zu akzeptieren. Führt die Behörde eine Identifizierung mit Fingern beider Hände durch, so nimmt das CS-EES zwei Identifizierungen vor, d. h. eine mit den Fingern der rechten Hand und eine mit den Fingern der linken Hand.

Verwendung des Gesichtsbildes

Das CS-EES führt nach Maßgabe der im vorstehenden Abschnitt „Verwendung von Fingerabdrücken“ festgelegten Regeln biometrische Suchen anhand von Live-Gesichtsbildaufnahmen in Kombination mit Fingerabdruckdaten durch.

3.3.2. Für Gefahrenabwehr- und Strafverfolgungszwecke

Suchen anhand folgender biometrischer Daten dürfen nur für Gefahrenabwehr- und Strafverfolgungszwecke durchgeführt werden:

- Fingerabdruck-Datensätze mit mindestens einem Fingerabdruck;
- gerollte und nicht segmentierte Slap-Fingerabdruckdaten;
- latente Fingerspuren;
- Gesichtsbild in Kombination mit Fingerabdruckdaten;
- nur Gesichtsbild.

Bei Fingerabdruck-Suchen, die zu Gefahrenabwehr- und Strafverfolgungszwecken durchgeführt werden, werden die Hände dem Permutationsverfahren[10] unterzogen. Die Verwendung der Hand-Permutationsfunktion muss auf zentraler Ebene konfiguriert (aktiviert/deaktiviert) werden können und wirkt sich auf alle Nutzer aus.

Bei Identifizierungen anhand von Fingerabdrücken zu Gefahrenabwehr- und Strafverfolgungszwecken werden entweder alle gespeicherten Fingerabdrücke ungeachtet ihrer Qualität herangezogen oder nur diejenigen, die einen bestimmten

[9] Ebenda.

[10] Die Hand-Permutation ermöglicht den Abgleich von Fingerabdrücken der einen Hand mit denen der jeweils anderen Hand. Dies verbessert die Übereinstimmungsgenauigkeit für den Fall, dass die Hand, von der das Sample stammt, nicht bekannt ist.

Qualitätsschwellenwert gemäß der für die Suche verwendeten Nutzerkonfiguration erfüllen. Das CS-EES übermittelt dem ersuchenden Mitgliedstaat die übereinstimmenden biometrischen Daten zusammen mit Angaben zur Qualität der gefundenen Fingerabdrücke. Im Falle einer Übereinstimmung mit Fingerabdrücken von geringer Qualität wird die für die Gefahrenabwehr bzw. Strafverfolgung zuständige Behörde darüber informiert, dass zur Bestätigung der Übereinstimmung weitere Verifikationen erforderlich sind. Die Schwellenwerte für „geringe Datenqualität“, die weitere Verifikationen erfordern, sind in den technischen Spezifikationen nach Artikel 37 Absatz 1 der Verordnung (EU) 2017/2226 anzugeben.

Biometrische Suchen, bei denen nur das Gesichtsbild verwendet wird, dürfen ausschließlich für den in Artikel 32 Absatz 2 der Verordnung (EU) 2017/2226 genannten Zweck durchgeführt werden. In diesem Fall gibt der Nutzer an, wie viele Personenübereinstimmungen höchstens rückgemeldet werden sollen. Die Höchstzahl beträgt vierhundert. In einem ersten Schritt erhält der Nutzer Zugang zu zweihundert Treffern mit der höchsten Übereinstimmung. Falls erforderlich, gewährt das System Zugang zu den restlichen zweihundert Treffern, wenn der Nutzer bestätigt, dass die ursprüngliche Suche keine genaue Übereinstimmung ergeben hat.