COMMISSION IMPLEMENTING DECISION (EU) 2019/329

of 25 February 2019

laying down the specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Regulation (EU) 2017/2226 of the European Parliament and of the Council of 30 November 2017 establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third-country nationals crossing the external borders of the Member States and determining the conditions for access to the EES for law enforcement purposes and amending the Convention implementing the Schengen Agreement and Regulation (EC) No 767/2008 and Regulation (EU) No 1077/2011 ([1]), and in particular points (a) and (b) of Article 36 first paragraph thereof,

Whereas:

(1) Regulation (EU) 2017/2226 established the Entry/Exit System (EES) as a system which registers electronically the time and place of entry and exit of third-country nationals admitted for a short stay to the territory of the Member States and which calculates the duration of their authorised stay.

(2) The EES aims to improve the management of external borders, to prevent irregular immigration and to facilitate the management of migration flows. The EES should, in particular, contribute to the identification of any person who does not fulfil or no longer fulfils the conditions of the authorised stay on the territory of the Member States. Additionally, the EES should contribute to the prevention, detection and investigation of terrorist offences and of other serious criminal offences.

(3) As quality and reliability of biometric data are key success factors for EES to reach its full potential, it is necessary to lay down the specifications for the quality, resolution and use of both fingerprints and facial image for biometric verification and identification in the EES, including where taken live or extracted electronically from the electronic Machine Readable Travel Document (eMRTD). As the quality of registered fingerprints will have impacts years after registration on the proper functioning of the EES, environmental and operational factors of fingerprint quality registration should be closely monitored on the long run.

(4) This decision does not create any new standards; it is coherent with ICAO standards.

(5) Based on those measures, the European agency for the operational management of large-scale information systems in the area of freedom, security and justice should then be able to define the design of the physical architecture of the EES including its Communication Infrastructure, as well as the technical specifications of the system and to develop the EES.

(6) In this framework, it is thus necessary to adopt specifications for the quality, resolution and use of fingerprints and facial image for biometric verification and identification in the Entry/Exit System (EES).

(7) This Decision is without prejudice to the application of Directive 2004/38/EC of the European Parliament and of the Council ([2]).

(8) In accordance with Articles 1 and 2 of Protocol No 22 on the position of Denmark, annexed to the Treaty on European Union and to the Treaty on the Functioning of the European Union, Denmark did not take part in the adoption of Regulation (EU) 2017/2226 and is not bound by it or subject to its application. However, given that Regulation (EU) 2017/2226 builds upon the Schengen *acquis*, Denmark, in accordance with Article 4 of that Protocol, notified on 30 May 2018 its decision to implement Regulation (EU) 2017/2226 in its national law. Denmark is therefore bound under international law to implement this Decision.

([1]) OJ L 327, 9.12.2017, p. 20.

([2]) Directive 2004/38/EC of the European Parliament and of the Council of 29 April 2004 on the right of citizens of the Union and their family members to move and reside freely within the territory of the Member States amending Regulation (EEC) No 1612/68 and repealing Directives 64/221/EEC, 68/360/EEC, 72/194/EEC, 73/148/EEC, 75/34/EEC, 75/35/EEC, 90/364/EEC, 90/365/EEC and 93/96/EEC (OJ L 158, 30.4.2004, p. 77).

(9) This Decision constitutes a development of the provisions of the Schengen *acquis* in which the United Kingdom does not take part, in accordance with Council Decision 2000/365/EC ([3]); the United Kingdom is therefore not taking part in the adoption of this Decision and is not bound by it or subject to its application.

(10) This Decision constitutes a development of the provisions of the Schengen *acquis* in which Ireland does not take part, in accordance with Council Decision 2002/192/EC ([4]); Ireland is therefore not taking part in the adoption of this Decision and is not bound by it or subject to its application.

(11) As regards Iceland and Norway, this Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the latter's association with the implementation, application and development of the Schengen *acquis* ([5]), which fall within the area referred to in Article 1, point A of Council Decision 1999/437/EC ([6]).

(12) As regards Switzerland, this Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([7]), which fall within the area referred to in Article 1, point A of Decision 1999/437/EC, read in conjunction with Article 3 of Council Decision 2008/146/EC ([8]).

(13) As regards Liechtenstein, this Decision constitutes a development of the provisions of the Schengen *acquis* within the meaning of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* ([9]) which fall within the area referred to in Article 1, point A of Decision 1999/437/EC read in conjunction with Article 3 of Council Decision 2011/350/EU ([10]).

(14) As regards Cyprus, Bulgaria, Romania and Croatia, the operation of the EES requires the granting of passive access to the VIS and the putting into effect of all the provisions of the Schengen *acquis* relating to the SIS in accordance with the relevant Council Decisions. Those conditions can only be met once the verification in accordance with the applicable Schengen evaluation procedure has been successfully completed. Therefore, the EES should be operated only by those Member States which fulfil those conditions by the start of operations of the EES. Member States not operating the EES from the initial start of operations should be connected to the EES in accordance with the procedure set out in Regulation (EU) 2017/2226 as soon as all of those conditions are met.

(15) The European Data Protection Supervisor delivered an opinion on 27 July 2018.

(16) The measures provided for in this Decision are in accordance with the opinion of the Smart Borders Committee,

HAS ADOPTED THIS DECISION:

Article 1

1. The specifications relating to the quality, resolution and use of fingerprints for biometric verification and identification in the EES are set out in the Annex

([3]) Council Decision 2000/365/EC of 29 May 2000 concerning the request of the United Kingdom of Great Britain and Northern Ireland to take part in some of the provisions of the Schengen *acquis* (OJ L 131, 1.6.2000, p. 43).
([4]) Council Decision 2002/192/EC of 28 February 2002 concerning Ireland's request to take part in some of the provisions of the Schengen *acquis* (OJ L 64, 7.3.2002, p. 20).
([5]) OJ L 176, 10.7.1999, p. 36.
([6]) Council Decision 1999/437/EC of 17 May 1999 on certain arrangements for the application of the Agreement concluded by the Council of the European Union and the Republic of Iceland and the Kingdom of Norway concerning the association of those two States with the implementation, application and development of the Schengen *acquis* (OJ L 176, 10.7.1999, p. 31).
([7]) OJ L 53, 27.2.2008, p. 52.
([8]) Council Decision 2008/146/EC of 28 January 2008 on the conclusion, on behalf of the European Community, of the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis* (OJ L 53, 27.2.2008, p. 1).
([9]) OJ L 160, 18.6.2011, p. 21.
([10]) Council Decision 2011/350/EU of 7 March 2011 on the conclusion, on behalf of the European Union, of the Protocol between the European Union, the European Community, the Swiss Confederation and the Principality of Liechtenstein on the accession of the Principality of Liechtenstein to the Agreement between the European Union, the European Community and the Swiss Confederation on the Swiss Confederation's association with the implementation, application and development of the Schengen *acquis*, relating to the abolition of checks at internal borders and movement of persons (OJ L 160, 18.6.2011, p. 19).

2. The specifications for the quality, resolution and use of the facial image for biometric verification and identification in the EES, including where taken live or extracted electronically from the eMRTD are set out in the Annex.

Article 2

This Decision shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

Done at Brussels, 25 February 2019.

For the Commission
The President
Jean-Claude JUNCKER

ANNEX

1. QUALITY

1.1. **Thresholds**

1.1.1. *Fingerprints*

Enrolment

At the moment of enrolment, the version 2.0 (or newer version) of the Fingerprint Image Quality (NFIQ) metric ([1]) defined by the National Institute of Standards and Technology (NIST) shall be used for verifying that the quality of the captured fingerprint data respects the thresholds that shall be specified in the technical specifications referred to in Article 37(1) of Regulation (EU) 2017/2226.

For the purpose of enrolment, the quality of fingerprint data shall be assessed:

— at national level by Member States at the time of capture prior to their transmission to the EES Central System (CS-EES), optionally with the support of a tool provided, maintained and updated by eu-LISA, and,

— at central level.

Verification

For the purpose of verification, it is recommended to assess the quality of fingerprints data by Member States at the time of capture prior to their transmission to the CS-EES either by using version 2.0 (or newer version) of the NIST Fingerprint Image Quality (NFIQ) metric or, where technically impossible, by using another metric which should preferably be correlated with the NFIQ version 2.0 (or newer version). The correlation shall be derived a priori. If a NFIQ version 2.0 (or newer version) quality metric is obtained, it has to be sent at the same time as the fingerprint data to the CS-EES.

1.1.2. *Facial images*

The quality of the facial images, including near infrared ones, shall comply with the thresholds specified in the technical specifications referred to in Article 37(1) of Regulation (EU) 2017/2226 and with the image requirements of ISO/IEC 19794-5:2011 Frontal image type. The quality of the facial image shall be assessed at national level by Member States at the time of capture prior to their transmission to the CS-EES, optionally with the support of a tool provided, maintained and updated by eu-LISA. The facial quality algorithm shall be comprehensible in terms of the ISO/IEC 19794-5:2011 criteria.

The quality threshold for the facial images shall be fixed using a facial image quality assessment algorithm based on the quality measures outlined in ISO 19794-5 and provide quality checks analogous to those implemented at the CS-EES ([2]).

1.2. **Performance values for biometric accuracy**

Definitions

The performance values for biometric accuracy defined in Article 3 of Regulation (EU) 2017/2226 are:

‘(29) “Failure To Enrol Rate” (FTER) means the proportion of registrations with insufficient quality of the biometric enrolment;

(30) “False Positive Identification Rate” (FPIR) means the proportion of returned matches during a biometric search which do not belong to the checked traveller;

(31) “False Negative Identification Rate” (FNIR) means the proportion of missed matches during a biometric search even though the traveller’s biometric data were registered.’

The ‘biometric search’ referred to in points (30) and (31) is the same as a biometric identification or ‘1 to N’ search

In compliance with Article 36 first paragraph point (g) of Regulation (EU) 2017/2226 the opportunity is left to the implementing act to define additional values of biometric performance.

The False Match(ing) Rate (FMR) is the proportion of impostor attempts that are falsely declared to match a template of another object (a person’s biometric template).

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

([2]) Where possible an assessment and validation of the facial images against the criteria of ICAO document 9303 §3.9, and the French Visual and User Recommendation for French Visa Applications shall be performed.

The False Non-Match(ing) Rate (FNMR) is the proportion of genuine attempts that are falsely declared not to match a template of the same object.

A genuine attempt is a single attempt by a user to match his/her own stored template. An impostor attempt is the opposite — a user's template is matched against someone else's template.

1.2.1. *Failure To Enroll Rate*

The target value for the Failure To Enroll Rate is zero. Member States shall take care to avoid such cases by using a quality-focused enrolment process.

1.2.2. *Accuracy of biometric verification*

The maximum values of the False Non-Matching Rate (FNMR) at a False Matching Rate (FMR) = 0,05 % (5 per 10 000) are:

Type	FMR	FNMR
Fingerprint	0,05 %	< 0,5 %
Facial Image	0,05 %	< 1 %

1.2.3. *Accuracy of biometric identification*

The maximum values of the False Negative Identification Rate at a False Positive Identification Rate = 0,1 % (1 per 1 000) are:

Type	FPIR	FNIR
Fingerprint	0,1 %	< 1,5 %
Facial Image and Fingerprint (multi-modal)	0,1 %	< 1 %

1.3. **Monitoring of biometric accuracy performance**

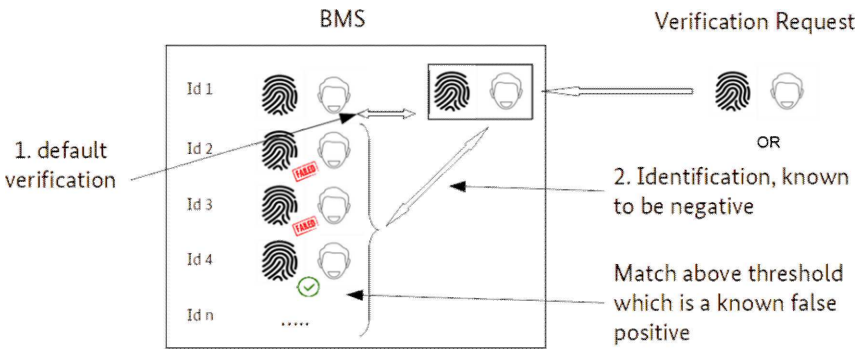
Biometric accuracy performance shall be measured on the actual data captured by each Member State based on a representative sample of cases on a daily basis at border crossing points of choice. The measurement is managed centrally, fully automated and does not require the access to personal data by the operator.

The measurement of biometric performance does not need to be done continuously: it may be disabled or enabled but shall be carried out by eu-LISA on a regular basis (at least monthly).

The measurement of biometric performance does not use biometric data itself. The templates of images used for the accuracy measurement are automatically deleted after execution of the evaluation process. All results of the performance measurement shall not contain personal information.

1.3.1. *Measurement of the FPIR (False Positive Identification Rate)*

The following figure shows that the templates for the biometric sample of both fingerprints and facial image are contained in the Biometric Matching System for a number 'n' of identities.



The measurement process shall be as follows:

1. A person subject to registration in the EES submits a sample of one or both of the two biometric modalities (fingerprints and facial image).

2. The biometric verification is conducted with the biometric reference data corresponding with the identity of the person (step 1 of the figure called 'default verification').

3. For a continuous sample set, the second biometric modality is obtained from the same person (either was submitted together with step 1 or it can be extracted from the biometric reference data corresponding to the identity of the person). The combined biometrics are used to run an identification on the complete gallery size excluding the biometrics of the person to whom the biometric sample belongs (step 2 of the figure called 'identification known to be negative'). This identification process is expected to yield a zero result as the matching biometric sample has been voluntarily removed from the comparison.

   In the event the modality used in step 2 corresponds to the fingerprint, an identification (to evaluate the fingerprint identification accuracy) is carried out under the same conditions mentioned in the first subparagraph.

4. In the case where the biometric identification returns a biometric sample (indicated as 'match above threshold') this is a known false *positive* identification (another person than the expected one is returned).

Steps 1 and 2 belong to the identity verification process that is part of the EES. Steps 3 and 4 do not belong to the identity verification process and are done for measuring the biometric accuracy performance.

The FPIR (False Positive Identification Rate) is computed as:

$$FPIR = \frac{Number\ of\ identifications\ where\ an\ identifier\ is\ returned}{Number\ of\ all\ known\ negative\ identification\ transactions}$$

1.3.2. *Measurement of FNIR (False Negative Identification Rate)*

The figure in point 1.3.1 applies to the description that follows.

The measurement process shall apply the following logic where the first two steps are always the same as they belong to the identity verification process that is part of the EES:

1. A person subject to registration in the EES submits a sample of one or both of the two biometric modalities.

2. The biometric verification is conducted with the biometric reference data corresponding with the identity of the person (step 1 of the figure called 'default verification').

3. For a continuous sample set, a second biometric modality is obtained either from the same person in the case both biometric modalities were submitted in step 1 or from another person for whom steps 1 and 2 of this process were triggered). The combined biometrics are used to run an identification on the complete gallery size including the biometrics of the person(s) to whom the biometric sample belongs. This identification process is expected to yield the known result as the matching biometric sample is included in the comparison.

4. In the event the modality used in step 2 corresponds to the fingerprint, an identification (to evaluate the fingerprint identification accuracy) is carried out under the same conditions mentioned in paragraph 3.

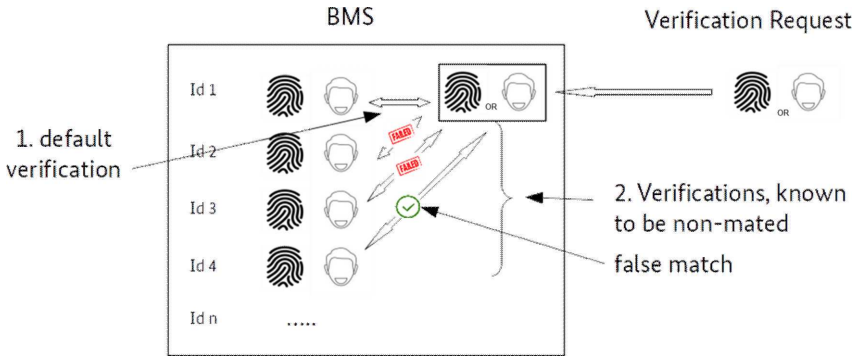
5. In the case where the biometric identification does not return the expected biometric sample (indicated as 'match above threshold') in the hit list, this is a known false *negative* identification.

Steps 1 and 2 belong to the identity verification process that is part of the EES. Steps 3 and 4 do not belong to the identity verification process and are done for measuring the biometric accuracy performance.

The FNIR (False Negative Identification Rate) is computed as:

$$FNIR = \frac{Number\ of\ identifications\ where\ the\ biometric\ subject's\ correct\ identifier\ is\ not\ returned}{Number\ of\ all\ identification\ transactions}$$

1.3.3. *Measurement of the biometric accuracy for verification (False Matching Rate and False Non Matching Rate)*



The measurement process shall apply the following logic:

1. A person to whom the EES applies submits a sample of one of the two biometric modalities.
2. The biometric verification is conducted with the biometric reference data corresponding with the identity of the person (step 1 of the figure called 'default verification').

   Steps 1 and 2 belong to the identity verification process that is part of the EES. The measurement of the biometric accuracy starts from here.
3. The verification of the biometric sample is executed vs a number of other biometric samples randomly taken from the biometric gallery which do not include the biometrics provided. The expected result is that the verifications will fail (this refers to point 2 of the figure 'verifications known to be non-mated'). Any match would mean a false match.

Step 3 allows the calculation of the **False Matching Rate** (the match occurs with another person than the owner of the data):

$$FMR = \frac{Number\ successful\ non\ mated\ comparisons}{Number\ of\ non\ mated\ comparisons}$$

Note: The number of non mated comparisons is the number of comparisons done under step 3)

Step 2 allows the calculation of the **False Non Matching Rate** (the match does not occur with the owner of the biometrics), in the case the identity has been confirmed by other means, on the basis of

$$FNMR = \frac{Number\ of\ failed\ comparisons}{Number\ of\ assumed\ mated\ comparisons}$$

Note: The number of mated comparisons is called 'assumed' as there is no absolute certainty that an impostor is not included in the set of identities the comparison is made with.

1.4. **Replacement of biometrics to improve the quality or to replace a picture which was extracted from the eMRTD with a live capture facial image of the CS-EES gallery**

Replacement of biometrics shall only occur upon successful biometric verification of the identity.

1.4.1. *Replacement of the stored fingerprint data*

The procedure for replacement of stored fingerprint data, which does not reach the required quality, shall be described in the practical handbook referred to in Article 71 of Regulation (EU) 2017/2226.

In the case of replacement of the left hand by the right hand (or vice versa), an identification with the newly captured fingerprints shall be launched to guarantee it does not correspond to another identity already registered into the system.

1.4.2. *Replacement of the stored facial images*

The procedure for replacement of a stored facial image, which does not reach the required quality, or which was extracted from the chip of the electronic Machine Readable Travel Document, shall be described in the practical handbook referred to in Article 71 of Regulation (EU) 2017/2226.

2. RESOLUTION

2.1. **Fingerprints**

The CS-EES shall receive fingerprint data of a nominal resolution of either 500 or 1 000 ppi (with an acceptable deviation of +/– 10 ppi) with 256 grey levels.

The fingerprint data shall be submitted in accordance with the ANSI/NIST-ITL 1-2011 Update 2015 standard (or newer version) and as specified in the technical specifications referred to in Article 37(1) of Regulation (EU) 2017/2226.

2.2. **Facial images**

2.2.1. *Definition*

The CS-EES shall receive live facial images at a resolution (in portrait mode) of minimum of 600 pixels by 800 pixels and maximum of 1 200 pixels by 1 600 pixels.

The face shall occupy a sufficient space within the image so as to ensure that there is a minimum of 120 pixels between the centres of the eyes.

2.2.2. *Colours*

When a facial image is taken live, it shall be a colour image. In exceptional cases when a colour image cannot be captured, grayscale or near infrared capture may be used. In such a case, if the quality of the grayscale or near infrared image is sufficient, it may be used for verification or identification but not for enrolment. Grayscale images are accepted for enrolment only when they are extracted from the chip of the travel document.

Specific rules concerning the near infrared facial images shall be described in the handbook in accordance with Article 71 of Regulation (EU) 2017/2226.

3. USE OF BIOMETRICS

3.1. **Entry and Storage**

3.1.1. *Fingerprints*

CS-EES shall store the fingerprint data from four fingers flat ([3]). When available, fingerprints from the following fingers of the right hand shall be used: the index finger, middle finger, ring finger, little finger.

Where it is impossible to obtain any fingerprint using the mentioned fingers of the right hand, the four fingerprints shall be captured from the left hand, where available. In such cases where the impossibility to obtain four fingerprints of the right hands is of a temporary nature, the fingerprint data shall be explicitly marked and, if the temporary impossibility does not exist anymore, the fingerprint data of the right hand shall be taken on exit or at subsequent entry in accordance with the technical specifications referred to in Article 37(1) of Regulation (EU) 2017/2226 (temporary impossibility).

In order to meet the applicable threshold, the re-capture of fingerprint data should be undertaken, if necessary, twice for any particular data subject (i.e. a total of three capture attempts should be made). Re-capture attempts should involve use of all fingers as initially attempted.

Fingerprint data that do not meet the applicable quality threshold:

(1) shall be stored in the CS-EES;

   (a) biometric verifications shall be done against those data;

   (b) biometric identifications shall not be done against fingerprints not meeting the quality threshold except in the case of law enforcement purposes;

(2) shall be flagged by the national system in accordance with the technical specifications referred to in Article 37(1) of Regulation (EU) 2017/2226 (technical impossibility) to allow their capture at the next border crossing.

([3]) The term 'flat' is used in accordance with the ISO/IEC dictionary and is the same as the term 'plain' used in the ANSI//NIST standard.

The NIST file sent by national systems to CS-EES and stored there, shall also contain the conditions of fingerprint registration including the level of monitoring carried out by the authorities and the method used for acquiring four finger flat images, as specified by the ANSI/NIST-ITL 1-2011: Update 2015 standard ([4]) (or newer version).

3.1.2. *Facial Image*

CS-EES shall store the live facial image captured at the border crossing point and submitted as part of a NIST container to the CS-EES as specified by the ANSI/NIST-ITL 1-2011: Update 2015 standard (or newer version).

In exceptional cases, where it is impossible to obtain a facial image of sufficient quality from the live subject, enrolment from the document chip of an electronic Machine Readable Travel Document (eMRTD) is requested, where it is technically accessible and after successful electronic verification according to the process that shall be described in the practical handbook referred to in Article 71 of Regulation (EU) 2017/2226.

Images scanned from the biographic page of the travel document shall be not used and shall not be transmitted to the CS-EES.

The photographs of visa applicants stored in the Visa information System (VIS) established pursuant to Regulation (EC) No 767/2008 of the European Parliament and of the Council ([5]) shall not be used for carrying out any electronic biometric verification or identification with the CS-EES.

Due to practical reasons, the quality threshold of facial images captured from live persons solely for the purposes of verification against those stored in the CS-EES are not compulsory. Successful verification according to the agreed matching score thresholds would however require images with sufficient quality even in these cases.

In order to meet the set quality threshold, particularly when it is impossible to extract electronically a facial image from the chip of an electronic eMRTD ([6]), the following measures shall apply:

(1) In cases where the face capture unit enrols images in a continuous stream, re-capture shall be taken over sufficient amount of time, so that the optimal image obtained within the capture stream is transmitted to the CS-EES. A lower-quality sample sent shall be flagged as such by the CS-EES as specified in the technical specifications referred to in Article 37(1) of Regulation (EU) 2017/2226.

(2) In cases where the face capture unit enrols static single images upon activation by an operator, a sufficient amount of recaptures shall be taken, so that the optimal image obtained is transmitted to the CS-EES. A lower-quality sample transmitted shall be flagged as such to the CS-EES as specified in the technical specifications referred to in Article 37(1) of Regulation (EU) 2017/2226.

A best practice guide to be followed for capturing facial images referred to in the previous two points of this paragraph shall be included in the practical handbook referred to in Article 71 of Regulation (EU) 2017/2226.

3.1.3. *Image compression*

Fingerprint images

The compression algorithm to be used shall follow the NIST recommendations. As a result, the fingerprint data with a resolution of 500 ppi shall be compressed using the WSQ algorithm (ISO/IEC 19794) while 1 000 ppi fingerprint data shall use the JPEG 2000 image compression standard (ISO/IEC 15444-1) and coding system. The target compression ratio is 15:1.

Facial images

Images compressed with JPG (ISO/IEC 10918) or JPEG 2000 (JP2) (ISO/IEC 15444-1) image compression standard and coding system shall be submitted to the CS-EES as specified in the technical specifications referred to in Article 37(1) of Regulation (EU) 2017/2226. The maximum allowed image compression rate is 1:20.

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

([5]) Regulation (EC) No 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation) (OJ L 218, 13.8.2008, p. 60).

([6]) This may be the case when the traveler does not possess an electronic document, or in instances when their travel document contains a facial image token rather than the image itself, as permitted by ICAO Document 9303, for example.

3.2. **Biometric verifications**

3.2.1. *Fingerprints*

CS-EES shall be able to perform biometric verifications using one, two or four fingers flat.

In the case where four fingers flat are used, fingerprint data from the following fingers shall be used: the index finger, middle finger, ring finger, little finger.

In the case where one or two fingers flat are used, the following fingers shall be used by default:

(a) one finger: index finger;

(b) two fingers: index finger and middle finger.

Alternatively, the following fingers may be used:

(a) One finger: the first finger available for acquisition by the following order — index finger, middle finger, ring finger, little finger.

(b) Two fingers: the first two fingers available for acquisition by the following order — index finger, middle finger and ring finger. Little finger may be also considered as a second one (only) for verification, should no other possibility exist.

In all cases:

(a) The fingerprint data shall be captured from the hand used for the enrolment.

(b) The finger-position shall be identified for each individual fingerprint image as specified by the ANSI/NIST-ITL 1-2011: Update 2015 standard (or newer version).

(c) A verification based on permutation ([7]) ensures that fingerprints from each of the two sets are matched against each other, regardless of their position in the set. It shall be possible to enable or disable this functionality at central level, impacting all users.

In cases of permanent or temporary physical impossibility to be fingerprinted, the fingerprints shall always be identified as specified by the ANSI/NIST-ITL 1-2011: Update 2015 standard (or newer version) and the EES Interface Control Document

3.2.2. *Facial Image*

CS-EES shall perform biometric verifications using live captured facial images.

3.3. **Biometric identifications and searches**

3.3.1. *For the purposes defined in the Chapter 3 of Regulation (EU) 2017/2226*

For purposes other than law enforcement multiple search configurations shall be available. There shall be at least one search configuration fulfilling the requirements defined in the Commission Implementing Decision laying down performance requirements of the Entry/Exit System (EES) ([8]) and further possible search configurations having different accuracy performance specifications (less strict or stricter).

Using fingerprints

For purposes other than law enforcement, CS-EES shall perform biometric identifications and searches either with four fingers flat, or with four fingers flat combined with the live captured facial image and only on biometric data which meet the applicable quality thresholds. The biometric identification shall be performed using the fingerprint data with at most one image per finger type (NIST identification 1 to 10).

Fingerprint data from the following fingers shall be used: the index finger, middle finger, ring finger, little finger. Fingerprints from the same hand shall be used, starting with the right hand.

The fingerprint data shall be correctly labelled as to which finger it relates. In cases of permanent or temporary physical impossibility, the fingerprints shall always be identified accordingly as specified by the ANSI/NIST-ITL 1-2011: Update 2015 standard ([9]) (or newer version) and the remaining fingers, if any, shall be used.

([7]) Permutation is a specific configuration mode of the biometric matching system, which ensures that fingerprints from each of the two sets are matched against each other, regardless of their position in the set. This ensures the elimination of potential human errors in regards to the order of the fingers as well as the highest possible biometric accuracy for verification.
([8]) C(2019) 1260.
([9]) Idem.

In the case where identifications are performed in a scope other than border checks, the CS-EES shall be capable to accept rolled fingerprints from authorities with access to EES allowed to use also rolled fingerprints under a different European regulation. If the authority performs an identification with fingers of both hands, the CS-EES shall perform two identifications, one with the fingers of the right hand and one with the fingers of the left hand.

Using the facial image

CS-EES shall perform biometric searches using live captured facial image in combination with fingerprint data in accordance with the rules defined in the above section 'Using fingerprints'

3.3.2. *For Law Enforcement Purposes*

Only for law enforcement purposes, searches may be performed on the basis of the following biometric data:

— fingerprint data sets containing at least one fingerprint;

— rolled and unsegmented slap fingerprint data;

— latent fingerprints;

— facial image in combination with fingerprint data;

— facial image only.

In case of fingerprints searches, permutation ([10]) of hands shall be performed in the scope of law enforcement searches. The use of permutation of hands shall be configurable (enable/disable) on central side, impacting all users.

Identification for law enforcement purposes with fingerprints shall be conducted on all stored fingerprints without account to fingerprint quality, or only on those meeting a certain quality threshold defined in the user search configuration used for the search. The CS-EES shall provide the matching biometric data to the requesting MS together with the indication of the quality of the retrieved fingerprints. In the event of a match with fingerprints of low quality, the law enforcement authority shall be informed that additional verifications are required in order to confirm the match. The tresholds indicating 'low data quality' requiring additional verifications shall be specified in the technical specifications referred to in Article 37(1) of Regulation (EU) 2017/2226.

Biometric searches using only the facial image modality may be executed for the sole purpose of Article 32(2) of Regulation (EU) 2017/2226. In that case the user shall specify the capping value of the number of returned candidate matches. The maximum number of returned files is four hundred. In a first step, the user shall gain access to two hundred best matching files. If necessary, the access to the remaining two hundred files shall be granted by the system, if the user confirms that the initial search did not lead to a successful match.

([10]) Permutation of hands allows for comparing fingerprints of one hand with the one of the other hand. This is improving the matching accuracy in the case the sample hand is not known.