

DÉCISION D'EXÉCUTION (UE) 2019/329 DE LA COMMISSION**du 25 février 2019****établissant les spécifications relatives à la qualité, à la résolution et à l'utilisation des empreintes digitales et de l'image faciale aux fins de vérification et d'identification biométriques dans le système d'entrée/de sortie (EES)**

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2017/2226 du Parlement européen et du Conseil du 30 novembre 2017 portant création d'un système d'entrée/de sortie (EES) pour enregistrer les données relatives aux entrées, aux sorties et aux refus d'entrée concernant les ressortissants de pays tiers qui franchissent les frontières extérieures des États membres et portant détermination des conditions d'accès à l'EES à des fins répressives, et modifiant la convention d'application de l'accord de Schengen et les règlements (CE) n° 767/2008 et (UE) n° 1077/2011 ⁽¹⁾, et notamment son article 36, premier alinéa, points a) et b),

considérant ce qui suit:

- (1) Le règlement (UE) 2017/2226 a créé le système d'entrée/de sortie (EES), qui enregistre par voie électronique le moment et le lieu d'entrée et de sortie des ressortissants de pays tiers admis pour un court séjour sur le territoire des États membres et qui calcule la durée de leur séjour autorisé.
- (2) L'EES vise à améliorer la gestion des frontières extérieures, à empêcher l'immigration irrégulière et à faciliter la gestion des flux migratoires. Il devrait, plus particulièrement, aider à identifier toute personne qui ne remplit pas, ou ne remplit plus, les conditions relatives au séjour autorisé sur le territoire des États membres. En outre, l'EES devrait contribuer à la prévention et à la détection des infractions terroristes ou d'autres infractions pénales graves, ainsi qu'aux enquêtes en la matière.
- (3) La qualité et la fiabilité des données biométriques étant déterminantes pour que l'EES atteigne son potentiel maximal, il y a lieu d'établir les spécifications relatives à la qualité, à la résolution et à l'utilisation des empreintes digitales et de l'image faciale aux fins de vérification et d'identification biométriques dans l'EES, y compris lorsque l'image faciale est prise en direct ou extraite électroniquement du document de voyage électronique lisible à la machine (DVLM-e). Étant donné que la qualité des empreintes digitales enregistrées aura des incidences sur le bon fonctionnement de l'EES pendant des années après l'enregistrement, il convient de surveiller de près, à long terme, les facteurs environnementaux et opérationnels influençant la qualité des empreintes digitales enregistrées.
- (4) La présente décision ne crée pas de nouvelles normes; elle est cohérente avec les normes de l'OACI.
- (5) À partir de ces mesures, l'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice devrait ensuite pouvoir définir la conception de l'architecture matérielle de l'EES, y compris son infrastructure de communication, ainsi que les spécifications techniques du système, et développer l'EES.
- (6) Dans ce cadre, il convient dès lors d'adopter les spécifications relatives à la qualité, à la résolution et à l'utilisation des empreintes digitales et de l'image faciale aux fins de vérification et d'identification biométriques dans le système d'entrée/de sortie (EES).
- (7) La présente décision est sans préjudice de l'application de la directive 2004/38/CE du Parlement européen et du Conseil ⁽²⁾.
- (8) Conformément aux articles 1^{er} et 2 du protocole n° 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark n'a pas participé à l'adoption du règlement (UE) 2017/2226 et n'est donc pas lié par celui-ci ni soumis à son application. Toutefois, ledit règlement développant l'acquis de Schengen, le Danemark, conformément à l'article 4 dudit protocole, a notifié le 30 mai 2018 sa décision de transposer le règlement (UE) 2017/2226 dans son droit interne. Le Danemark est donc tenu, en application du droit international, de mettre en œuvre la présente décision.

⁽¹⁾ JO L 327 du 9.12.2017, p. 20.

⁽²⁾ Directive 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres, modifiant le règlement (CEE) n° 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE (JO L 158 du 30.4.2004, p. 77).

- (9) La présente décision constitue un développement des dispositions de l'acquis de Schengen auxquelles le Royaume-Uni ne participe pas, conformément à la décision 2000/365/CE du Conseil ⁽³⁾; le Royaume-Uni ne participe donc pas à l'adoption de la présente décision et n'est pas lié par celle-ci ni soumis à son application.
- (10) La présente décision constitue un développement des dispositions de l'acquis de Schengen auxquelles l'Irlande ne participe pas, conformément à la décision 2002/192/CE du Conseil ⁽⁴⁾; l'Irlande ne participe donc pas à l'adoption de la présente décision et n'est pas liée par celle-ci ni soumise à son application.
- (11) En ce qui concerne l'Islande et la Norvège, la présente décision constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord conclu par le Conseil de l'Union européenne, la République d'Islande et le Royaume de Norvège sur l'association de ces deux États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen ⁽⁵⁾, qui relèvent du domaine visé à l'article 1^{er}, point A, de la décision 1999/437/CE du Conseil ⁽⁶⁾.
- (12) En ce qui concerne la Suisse, la présente décision constitue un développement des dispositions de l'acquis de Schengen au sens de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen ⁽⁷⁾, qui relèvent du domaine visé à l'article 1^{er}, point A, de la décision 1999/437/CE, lue en liaison avec l'article 3 de la décision 2008/146/CE du Conseil ⁽⁸⁾.
- (13) En ce qui concerne le Liechtenstein, la présente décision constitue un développement des dispositions de l'acquis de Schengen au sens du protocole entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen ⁽⁹⁾, qui relèvent du domaine visé à l'article 1^{er}, point A, de la décision 1999/437/CE, lue en liaison avec l'article 3 de la décision 2011/350/UE du Conseil ⁽¹⁰⁾.
- (14) En ce qui concerne Chypre, la Bulgarie, la Roumanie et la Croatie, la mise en œuvre de l'EES requiert l'octroi d'un accès passif au VIS et la mise en application de toutes les dispositions de l'acquis de Schengen relatives au SIS conformément aux décisions pertinentes du Conseil. Ces conditions ne pourront être remplies qu'une fois que la vérification prévue par la procédure d'évaluation de Schengen applicable aura été réalisée avec succès. En conséquence, l'EES ne devrait être mis en œuvre que par les États membres qui remplissent ces conditions au moment de sa mise en service. Les États membres qui ne mettent pas en œuvre l'EES à partir de sa mise en service initiale devraient y être connectés, dans le respect de la procédure prévue par le règlement (UE) 2017/2226, dès que toutes ces conditions seront remplies.
- (15) Le Contrôleur européen de la protection des données a rendu son avis le 27 juillet 2018.
- (16) Les mesures prévues par la présente décision sont conformes à l'avis du comité des frontières intelligentes,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

1. Les spécifications relatives à la qualité, à la résolution et à l'utilisation des empreintes digitales aux fins de vérification et d'identification biométriques dans l'EES figurent en annexe.

⁽³⁾ Décision 2000/365/CE du Conseil du 29 mai 2000 relative à la demande du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord de participer à certaines dispositions de l'acquis de Schengen (JO L 131 du 1.6.2000, p. 43).

⁽⁴⁾ Décision 2002/192/CE du Conseil du 28 février 2002 relative à la demande de l'Irlande de participer à certaines dispositions de l'acquis de Schengen (JO L 64 du 7.3.2002, p. 20).

⁽⁵⁾ JO L 176 du 10.7.1999, p. 36.

⁽⁶⁾ Décision 1999/437/CE du Conseil du 17 mai 1999 relative à certaines modalités d'application de l'accord conclu par le Conseil de l'Union européenne et la République d'Islande et le Royaume de Norvège sur l'association de ces deux États à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (JO L 176 du 10.7.1999, p. 31).

⁽⁷⁾ JO L 53 du 27.2.2008, p. 52.

⁽⁸⁾ Décision 2008/146/CE du Conseil du 28 janvier 2008 relative à la conclusion, au nom de la Communauté européenne, de l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen (JO L 53 du 27.2.2008, p. 1).

⁽⁹⁾ JO L 160 du 18.6.2011, p. 21.

⁽¹⁰⁾ Décision 2011/350/UE du Conseil du 7 mars 2011 relative à la conclusion, au nom de l'Union européenne, du protocole entre l'Union européenne, la Communauté européenne, la Confédération suisse et la Principauté de Liechtenstein sur l'adhésion de la Principauté de Liechtenstein à l'accord entre l'Union européenne, la Communauté européenne et la Confédération suisse sur l'association de la Confédération suisse à la mise en œuvre, à l'application et au développement de l'acquis de Schengen en ce qui concerne la suppression des contrôles aux frontières intérieures et la circulation des personnes (JO L 160 du 18.6.2011, p. 19).

2. Les spécifications relatives à la qualité, la résolution et l'utilisation de l'image faciale aux fins de vérification et d'identification biométriques dans l'EES, y compris lorsque l'image faciale est prise en direct ou est extraite électroniquement du DVLM-e, figurent en annexe.

Article 2

La présente décision entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 25 février 2019.

Par la Commission
Le président
Jean-Claude JUNCKER

ANNEXE

1. QUALITÉ

1.1. **Seuils**1.1.1. *Empreintes digitales*

Enregistrement

Au moment de l'enregistrement, la version 2.0 (ou une version plus récente) de la métrique *Fingerprint Image Quality* (NFIQ) ⁽¹⁾ définie par le National Institute of Standards and Technology (NIST) est utilisée pour vérifier si la qualité des données dactyloscopiques capturées respecte les seuils qui seront précisés dans les spécifications techniques visées à l'article 37, paragraphe 1, du règlement (UE) 2017/2226.

Aux fins de l'enregistrement, la qualité des données dactyloscopiques est évaluée:

- au niveau national, par les États membres au moment de la capture préalable à la transmission des données au système central de l'EES («CS-EES»), éventuellement à l'aide d'un outil fourni, géré et actualisé par l'eu-LISA, et
- au niveau central.

Vérification

Aux fins de la vérification, il est recommandé que les États membres évaluent la qualité des données dactyloscopiques au moment de la capture préalable à leur transmission au CS-EES, en utilisant soit la version 2.0 (ou une version plus récente) de la métrique *Fingerprint Image Quality* (NFIQ) du NIST soit, lorsque c'est techniquement impossible, une autre métrique qui sera, de préférence, corrélée avec la version 2.0 (ou une version plus récente) de la NFIQ. La corrélation est déduite a priori. Si une métrique de la version 2.0 (ou une version plus récente) de la NFIQ est obtenue, elle doit être envoyée en même temps que les données dactyloscopiques au CS-EES.

1.1.2. *Images faciales*

La qualité des images faciales, y compris celles dans le proche infrarouge, doit respecter les seuils précisés dans les spécifications techniques visées à l'article 37, paragraphe 1, du règlement (UE) 2017/2226 et les exigences fixées pour les images par la norme ISO/IEC 19794-5:2011 Frontal image type. La qualité de l'image faciale est évaluée au niveau national par les États membres, au moment de la capture préalable à la transmission de l'image au CS-EES, éventuellement à l'aide d'un outil fourni, géré et actualisé par l'eu-LISA. L'algorithme pour la qualité faciale doit être complet en ce qui concerne les critères de la norme ISO/IEC 19794-5:2011.

Le seuil de qualité pour les images faciales sera fixé au moyen d'un algorithme d'évaluation de la qualité des images faciales basé sur les mesures de qualité décrites dans la norme ISO 19794-5 et il assurera des contrôles de qualité analogues à ceux appliqués dans le CS-EES ⁽²⁾.

1.2. **Valeurs de performance pour l'exactitude biométrique**

Définitions

L'article 3 du règlement (UE) 2017/2226 définit les valeurs de performance suivantes pour l'exactitude biométrique:

- «29) "taux d'échec à l'enregistrement", la proportion d'enregistrements pour lesquels l'enregistrement biométrique est de qualité insuffisante;
- 30) "taux de fausses identifications positives", la proportion de concordances constatées lors d'une recherche biométrique qui ne correspondent pas au voyageur soumis à vérification;
- 31) "taux de fausses identifications négatives", la proportion de concordances non constatées lors d'une recherche biométrique bien que les données biométriques du voyageur aient été enregistrées.»

La «recherche biométrique» mentionnée aux points 30) et 31) est identique à l'identification biométrique ou à la recherche «1 à N».

En application de l'article 36, premier alinéa, point g), du règlement (UE) 2017/2226, l'acte d'exécution peut définir des valeurs de performance biométrique supplémentaires.

Le taux de fausses correspondances (FMR) est la proportion de tentatives d'imposteurs qui sont déclarées à tort correspondre au gabarit d'un autre objet (gabarit biométrique d'une personne).

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

⁽²⁾ Lorsque c'est possible, il sera réalisé une évaluation et une validation des images faciales au regard des critères fixés au point 3.9 du document 9303 de l'OACI et dans les recommandations des autorités françaises pour les demandes de visa français.

Le taux de fausses non-correspondances (FNMR) est la proportion de tentatives légitimes qui sont déclarées à tort ne pas correspondre au gabarit du même objet.

Une tentative légitime est une tentative unique, faite par un utilisateur, de trouver une correspondance avec son propre gabarit stocké. Une tentative d'imposteur est l'inverse - le gabarit d'un utilisateur est comparé avec le gabarit d'une autre personne.

1.2.1. Taux d'échec à l'enregistrement

La valeur cible pour le taux d'échec à l'enregistrement est zéro. Les États membres veillent à éviter de tels cas en appliquant un processus d'enregistrement axé sur la qualité.

1.2.2. Exactitude de la vérification biométrique

Les valeurs maximales du taux de fausses non-correspondances (FNMR) à un taux de fausses correspondances (FMR) = 0,05 % (5 pour 10 000) sont les suivantes:

Type	FMR	FNMR
Empreintes digitales	0,05 %	< 0,5 %
Image faciale	0,05 %	< 1 %

1.2.3. Exactitude de la vérification biométrique

Les valeurs maximales du taux de fausses identifications négatives (FNIR) à un taux de fausses identifications positives (FPIR) = 0,1 % (1 pour 1 000) sont les suivantes:

Type	FPIR	FNIR
Empreintes digitales	0,1 %	< 1,5 %
Image faciale et empreintes digitales (multi-modal)	0,1 %	< 1 %

1.3. Contrôle de performance de l'exactitude biométrique

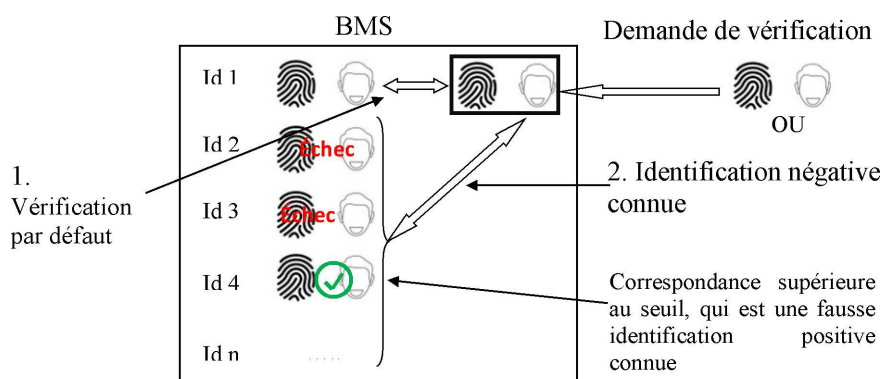
La performance de l'exactitude biométrique se mesurera sur les données réelles capturées par chaque État membre, sur la base d'un échantillon représentatif quotidien de cas, à des points de passage frontaliers sélectionnés. La mesure est gérée au niveau central, est totalement automatisée et ne nécessite pas l'accès de l'opérateur à des données à caractère personnel.

La mesure de la performance biométrique ne doit pas nécessairement être continue: elle peut être désactivée ou activée, mais l'eu-LISA doit la réaliser de manière régulière (au moins une fois par mois).

La mesure de la performance biométrique ne repose pas sur les données biométriques mêmes. Les gabarits d'images utilisés pour mesurer l'exactitude biométrique sont automatiquement supprimés après l'exécution du processus d'évaluation. Aucun résultat de la mesure de performance ne peut contenir d'informations à caractère personnel.

1.3.1. Mesure du FPIR (taux de fausses identifications positives)

La figure suivante indique que les gabarits destinés à l'échantillon biométrique des empreintes digitales et des images faciales se trouvent dans le système d'établissement de correspondances biométriques pour un nombre «n» d'identités.



La mesure est réalisée comme suit:

- 1) une personne à enregistrer dans l'EES soumet un échantillon de l'une ou des deux modalités biométriques (empreintes digitales et image faciale);
- 2) La vérification biométrique est réalisée avec les données biométriques de référence correspondant à l'identité de la personne (étape 1 de la figure, appelée «vérification par défaut»).
- 3) Pour disposer d'un ensemble d'échantillons cohérent, la seconde modalité biométrique est obtenue auprès de la même personne (soit elle a été soumise simultanément à l'étape 1 soit elle peut être extraite des données biométriques de référence correspondant à l'identité de la personne). Les données biométriques combinées servent à réaliser une identification sur la galerie complète, en excluant les données biométriques de la personne à laquelle appartient l'échantillon biométrique (étape 2 de la figure, appelée «identification négative connue»). Ce processus d'identification doit donner un résultat nul puisque l'échantillon biométrique correspondant a été volontairement exclu de la comparaison.

Dans le cas où la modalité utilisée à l'étape 2 correspond à l'empreinte digitale, une identification (pour évaluer l'exactitude de l'identification des empreintes) a lieu dans les mêmes conditions que celles mentionnées au premier alinéa.

- 4) Si l'identification biométrique a pour résultat un échantillon biométrique (qualifié de «correspondance supérieure au seuil»), il s'agit d'une fausse identification *positive* connue (le résultat est une personne autre que celle attendue).

Les étapes 1 et 2 font partie du processus de vérification de l'identité inclus dans l'EES. Les étapes 3 et 4 n'en font pas partie et servent à mesurer la performance de l'exactitude biométrique.

Le FPIR (taux de fausses identifications positives) est calculé comme suit:

$$FPIR = \frac{\text{Nombre d'identifications ayant pour résultat un identifiant}}{\text{Nombre total d'opérations d'identification négatives connues}}$$

1.3.2. Mesure du FNIR (taux de fausses identifications négatives)

La figure du point 1.3.1 s'applique à la description ci-après.

Le processus de mesure appliquera la logique suivante, selon laquelle les deux premières étapes sont toujours les mêmes parce qu'elles font partie du processus de vérification de l'identité inclus dans l'EES:

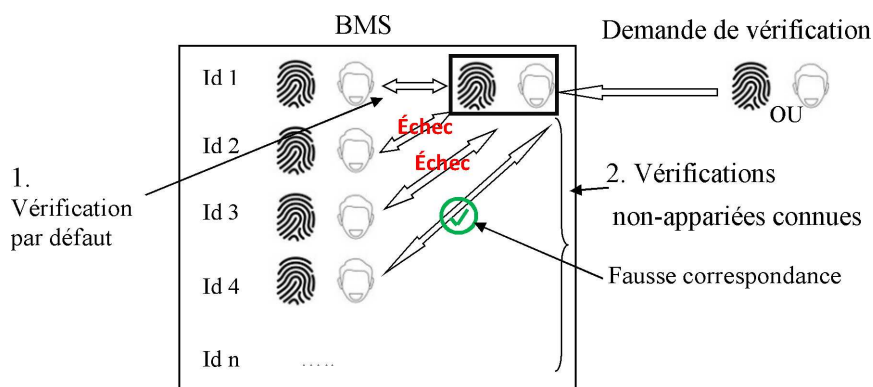
- 1) une personne à enregistrer dans l'EES soumet un échantillon de l'une ou des deux modalités biométriques.
- 2) La vérification biométrique est réalisée avec les données biométriques de référence correspondant à l'identité de la personne (étape 1 de la figure, appelée «vérification par défaut»).
- 3) Pour disposer d'un ensemble d'échantillons continu, une seconde modalité biométrique est obtenue soit auprès de la même personne, si les deux modalités biométriques ont été soumises à l'étape 1, soit auprès d'une autre personne pour laquelle les étapes 1 et 2 de ce processus ont été lancées. Les données biométriques combinées servent à réaliser une identification sur la galerie complète, y compris les données biométriques de la ou des personnes auxquelles appartient l'échantillon biométrique. Ce processus d'identification doit donner le résultat connu puisque l'échantillon biométrique correspondant est inclus dans la comparaison.
- 4) Dans le cas où la modalité utilisée à l'étape 2 correspond à l'empreinte digitale, une identification (pour évaluer l'exactitude de l'identification des empreintes) a lieu dans les mêmes conditions que celles mentionnées au point 3).
- 5) Si, lors de l'identification biométrique, l'échantillon biométrique attendu (qualifié de «correspondance supérieure au seuil») ne figure pas dans la liste des résultats positifs, il s'agit d'une fausse identification *négative* connue.

Les étapes 1 et 2 font partie du processus de vérification de l'identité inclus dans l'EES. Les étapes 3 et 4 n'en font pas partie et servent à mesurer la performance de l'exactitude biométrique.

Le FNIR (taux de fausses identifications négatives) est calculé comme suit:

$$FNIR = \frac{\text{Nombre d'identifications pour lesquelles l'identifiant correct du sujet ne s'affiche pas}}{\text{Nombre total d'opérations d'identification}}$$

1.3.3. Mesure de l'exactitude biométrique pour la vérification (taux de fausses correspondances et taux de fausses non-correspondances)



Le processus de mesure appliquera la logique suivante:

- 1) une personne concernée par l'EES soumet un échantillon de l'une des deux modalités biométriques.
- 2) La vérification biométrique est réalisée avec les données biométriques de référence correspondant à l'identité de la personne (étape 1 de la figure, appelée «vérification par défaut»).

Les étapes 1 et 2 font partie du processus de vérification de l'identité inclus dans l'EES. La mesure de l'exactitude biométrique commence à partir de là.

- 3) La vérification de l'échantillon biométrique est réalisée par rapport à un certain nombre d'autres échantillons biométriques pris au hasard dans la galerie biométrique et ne comportant pas les données biométriques fournies. La vérification doit normalement aboutir à un échec (voir le point 2 de la figure, «vérifications non appariées connues»). Toute correspondance serait une fausse correspondance.

L'étape 3 permet de calculer le taux de fausses correspondances (FMR) (la correspondance est établie avec une autre personne que le propriétaire des données):

$$FMR = \frac{\text{Nombre de comparaisons non appariées réussies}}{\text{Nombre de comparaisons non appariées}}$$

Remarque: Le nombre de comparaisons non appariées est le nombre de comparaisons réalisées à l'étape 3.

L'étape 2 permet de calculer le taux de fausses non-correspondances (FNMR) (la correspondance avec le propriétaire des données ne s'établit pas), dans le cas où l'identité a été confirmée par d'autres moyens, selon la formule suivante:

$$FNMR = \frac{\text{Nombre de comparaisons ayant échoué}}{\text{Nombre de comparaisons appariées supposées}}$$

Remarque: Les comparaisons appariées sont qualifiées de «supposées» car il n'est pas totalement certain qu'aucun imposteur ne figure dans le groupe d'identités avec lesquelles la comparaison est réalisée.

1.4. Remplacement de données biométriques pour en accroître la qualité ou pour remplacer une photo extraite du DVLM-e par une image faciale capturée en direct provenant de la galerie du CS-EES

Le remplacement de données biométriques n'a lieu qu'en cas de réussite de la vérification biométrique de l'identité.

1.4.1. Remplacement des données dactyloscopiques stockées

La procédure de remplacement des données dactyloscopiques stockées qui ne présentent pas la qualité requise est décrite dans le manuel pratique visé à l'article 71 du règlement (UE) 2017/2226.

En cas de remplacement de la main gauche par la main droite (ou vice versa), une identification est lancée avec les nouvelles empreintes digitales capturées, pour garantir que la main ne correspond pas à une autre identité déjà enregistrée dans le système.

1.4.2. Remplacement des images faciales stockées

La procédure de remplacement d'une image faciale stockée qui ne présente pas la qualité requise ou qui a été extraite de la puce du document de voyage électronique lisible à la machine est décrite dans le manuel pratique visé à l'article 71 du règlement (UE) 2017/2226.

2. RÉSOLUTION

2.1. Empreintes digitales

Le CS-EES recevra des données dactyloscopiques d'une résolution nominale de 500 ou 1 000 ppi (l'écart maximal toléré étant de +/- 10 ppi) avec 256 niveaux de gris.

Ces données seront transmises conformément à la norme ANSI/NIST-ITL 1-2011 Update 2015 (ou une version plus récente) et ainsi qu'il est mentionné dans les spécifications techniques visées à l'article 37, paragraphe 1, du règlement (UE) 2017/2226.

2.2. Images faciales

2.2.1. Définition

Le CS-EES recevra des images faciales capturées en direct d'une résolution (en mode portrait) de 600 pixels par 800 pixels au minimum et de 1 200 pixels par 1 600 pixels au maximum.

Le visage doit occuper, à l'intérieur de l'image, un espace suffisant pour qu'il y ait, au minimum, 120 pixels entre les centres des yeux.

2.2.2. Couleurs

Lorsqu'une image faciale est capturée en direct, elle doit être en couleur. Dans les cas exceptionnels où une image en couleur ne peut être capturée, une capture en niveaux de gris ou dans le proche infrarouge est autorisée. Le cas échéant, si la qualité de l'image en niveaux de gris ou dans le proche infrarouge est suffisante, elle peut servir à la vérification ou à l'identification, mais pas à l'enregistrement. Les images en niveaux de gris ne sont acceptées pour l'enregistrement que si elles sont extraites de la puce du document de voyage.

Des règles particulières concernant les images faciales dans le proche infrarouge sont décrites dans le manuel visé à l'article 71 du règlement (UE) 2017/2226.

3. UTILISATION DES DONNÉES BIOMÉTRIQUES

3.1. Saisie et stockage

3.1.1. Empreintes digitales

Le CS-EES stockera les données dactyloscopiques de quatre doigts à plat⁽³⁾. Lorsqu'elles sont disponibles, les empreintes digitales des doigts de la main droite suivants seront utilisées: l'index, le majeur, l'annulaire et l'auriculaire.

Lorsqu'il est impossible d'obtenir une quelconque empreinte digitale des doigts de la main droite susmentionnés, les quatre empreintes sont capturées sur la main gauche, si c'est possible. Lorsque l'impossibilité d'obtenir quatre empreintes digitales de la main droite est temporaire, une mention expresse est inscrite dans les données dactyloscopiques et, lorsque l'impossibilité a disparu, les données dactyloscopiques de la main droite sont prises à la sortie ou lors d'une entrée ultérieure, en respectant les spécifications techniques visées à l'article 37, paragraphe 1, du règlement (UE) 2017/2226 (impossibilité temporaire).

Pour respecter le seuil applicable, une nouvelle capture des données dactyloscopiques devrait avoir lieu, si nécessaire, deux fois pour toute personne concernée (c'est-à-dire que trois tentatives de capture devraient être effectuées au total). Les nouvelles tentatives de capture doivent se faire avec les mêmes doigts que la tentative initiale.

Les données dactyloscopiques qui ne respectent pas le seuil de qualité applicable:

- 1) sont stockées dans le CS-EES;
 - a) des vérifications biométriques sont réalisées par comparaison avec ces données;
 - b) aucune identification biométrique n'est réalisée par comparaison avec des empreintes digitales qui ne respectent pas le seuil de qualité, sauf à des fins répressives;
- 2) sont signalées par le système national conformément aux spécifications techniques visées à l'article 37, paragraphe 1, du règlement (UE) 2017/2226 (impossibilité technique), pour permettre la capture de ces données au prochain passage frontalier.

⁽³⁾ L'expression «à plat» («flat») est employé conformément au dictionnaire ISO/IEC et est équivalent au terme «plain» employé dans la norme ANSI/NIST (en anglais uniquement).

Le dossier NIST transmis par les systèmes nationaux au CS-EES et stocké dans ce dernier mentionnera aussi les conditions d'enregistrement des empreintes digitales, y compris le niveau de contrôle exercé par les autorités et la méthode employée pour obtenir les images de quatre doigts à plat, ainsi qu'il est spécifié dans la norme ANSI/NIST-ITL 1-2011: Update 2015 ⁽⁴⁾ (ou une version plus récente).

3.1.2. Image faciale

Le CS-EES stockera l'image faciale capturée en direct au point de passage frontalier et soumise dans un container NIST au CS-EES, ainsi qu'il est spécifié dans la norme ANSI/NIST-ITL 1-2011: Update 2015 (ou une version plus récente).

Dans des cas exceptionnels, lorsqu'il est impossible d'obtenir une image faciale de qualité suffisante à partir de la personne présente, l'enregistrement à partir de la puce d'un document de voyage électronique lisible à la machine (DVLM-e) est demandé, si la puce est techniquement accessible et après une vérification électronique réussie, réalisée conformément au processus qui sera décrit dans le manuel pratique visé à l'article 71 du règlement (UE) 2017/2226.

Les images scannées à partir de la page du document de voyage comportant les informations personnelles ne peuvent être utilisées ni transmises au CS-EES.

Les photographies des demandeurs de visa stockées dans le système d'information sur les visas (VIS) créé en application du règlement (CE) n° 767/2008 du Parlement européen et du Conseil ⁽⁵⁾ ne peuvent servir à la vérification ni à l'identification biométrique sous forme électronique avec le CS-EES.

Pour des raisons pratiques, le seuil de qualité des images faciales capturées en direct sur des personnes aux seules fins d'une vérification par comparaison avec celles stockées dans le CS-EES n'est pas obligatoire. Une vérification réussie, respectant les seuils de taux de correspondance convenus, requiert cependant des images d'une qualité suffisante, même dans ces cas.

Pour respecter le seuil de qualité fixé, notamment lorsqu'il est impossible d'extraire, par un moyen électronique, une image faciale de la puce d'un DVLM-e ⁽⁶⁾, les mesures suivantes s'appliquent:

- 1) si l'unité de capture du visage enregistre des images en flux continu, une nouvelle capture doit être réalisée sur une durée suffisamment longue pour que l'image optimale obtenue dans le flux de capture soit transmise au CS-EES. Un échantillon de qualité inférieure envoyé sera signalé comme tel par le CS-EES, ainsi qu'il est précisé dans les spécifications techniques visées à l'article 37, paragraphe 1, du règlement (UE) 2017/2226;
- 2) si l'unité de capture du visage enregistre des images individuelles statiques lors de l'activation par un opérateur, un nombre suffisant de nouvelles captures sera réalisé, pour que l'image optimale obtenue soit transmise au CS-EES. Un échantillon de qualité inférieure transmis sera signalé comme tel au CS-EES, ainsi qu'il est précisé dans les spécifications techniques visées à l'article 37, paragraphe 1, du règlement (UE) 2017/2226.

Un guide de bonnes pratiques à suivre pour capturer les images faciales visées aux deux points précédents du présent paragraphe sera inclus dans le manuel pratique visé à l'article 71 du règlement (UE) 2017/2226.

3.1.3. Compression d'images

Images dactyloscopiques

L'algorithme de compression à utiliser suit les recommandations du NIST. Ainsi, les données dactyloscopiques d'une résolution de 500 ppi seront comprimées au moyen de l'algorithme WSQ (ISO/IEC 19794), tandis que la norme de compression d'images et le système de codage JPEG 2000 (ISO/IEC 15444-1) seront appliqués pour celles d'une résolution de 1 000 ppi. Le taux de compression à atteindre est 15:1.

Images faciales

Les images comprimées selon la norme de compression d'images et le système de codage JPG (ISO/IEC 10918) ou JPEG 2000 (JP2) (ISO/IEC 15444-1) sont soumises au CS-EES ainsi qu'il est précisé dans les spécifications techniques visées à l'article 37, paragraphe 1, du règlement (UE) 2017/2226. Le taux maximal de compression autorisé est 1:20.

⁽⁴⁾ Norme ANSI/NIST-ITL 1-2011 «Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information», disponible sur: <https://www.nist.gov/publications/data-format-interchange-fingerprint-facial-other-biometric-information-ansinist-itl-1-1>

⁽⁵⁾ Règlement (CE) n° 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS) (JO L 218 du 13.8.2008, p. 60).

⁽⁶⁾ Ce peut être le cas lorsque le voyageur ne possède pas de document électronique ou que le document de voyage contient une image faciale jeton au lieu de l'image elle-même, ainsi que le permet le document 9303 de l'OACI, par exemple.

3.2. Vérifications biométriques

3.2.1. Empreintes digitales

Le CS-EES doit être en mesure d'effectuer des vérifications biométriques au moyen d'un, de deux ou de quatre doigts à plat.

Lorsqu'il s'agit de quatre doigts à plat, les données dactyloscopiques des doigts suivants sont utilisées: l'index, le majeur, l'annulaire et l'auriculaire.

Lorsqu'il s'agit d'un ou de deux doigts à plat, les doigts suivants sont utilisés par défaut:

- a) un doigt: l'index;
- b) deux doigts: l'index et le majeur;

À titre d'alternative, les doigts suivants peuvent être utilisés:

- a) un doigt: le premier doigt disponible pour l'acquisition de données, dans l'ordre suivant - index, majeur, annulaire, auriculaire;
- b) deux doigts: les deux premiers doigts disponibles pour l'acquisition de données, dans l'ordre suivant: index, majeur, annulaire, auriculaire. L'auriculaire peut aussi être considéré comme un deuxième doigt (uniquement) à des fins de vérification, s'il n'existe pas d'autre possibilité.

Dans tous les cas:

- a) les données dactyloscopiques seront capturées sur la main utilisée pour l'enregistrement;
- b) la position du doigt sera identifiée pour chaque image individuelle conformément aux spécifications de la norme ANSI/NIST-ITL 1-2011: Update 2015 (ou une version plus récente);
- c) une vérification basée sur une permutation ⁽⁷⁾ permet de comparer entre elles des empreintes digitales provenant de chacun des deux ensembles, quelle que soit leur position dans l'ensemble. Il doit être possible d'activer ou de désactiver cette fonction au niveau central, pour atteindre tous les utilisateurs.

En cas d'impossibilité physique, permanente ou temporaire, de relever des empreintes, ces dernières sont toujours identifiées conformément à la norme ANSI/NIST-ITL 1-2011: Update 2015 (ou une version plus récente) et au document de contrôle des interfaces de l'EES.

3.2.2. Image faciale

Le CS-EES effectuera des vérifications biométriques en utilisant des images faciales capturées en direct.

3.3. Identifications et recherches biométriques

3.3.1. Aux fins définies au chapitre 3 du règlement (UE) 2017/2226

Pour les finalités autres que l'action répressive, des configurations de recherche multiples seront disponibles. Il existera au moins une configuration de recherche remplissant les exigences fixées dans la décision d'exécution de la Commission établissant les exigences de performance applicables au système d'entrée/de sortie (EES) ⁽⁸⁾, et d'autres configurations de recherche possibles, soumises à des spécifications de performance différentes pour l'exactitude biométrique (plus strictes ou moins strictes).

Par les empreintes digitales

Pour les finalités autres que l'action répressive, le CS-EES effectuera des identifications et recherches biométriques soit au moyen de quatre doigts à plat, soit au moyen de quatre doigts à plat combinés avec l'image faciale capturée en direct et uniquement sur des données biométriques qui respectent les seuils de qualité applicables. L'identification biométrique sera réalisée au moyen des données dactyloscopiques, avec au maximum une image par type de doigt (identification 1 à 10 du NIST).

Les données dactyloscopiques des doigts suivants seront utilisées: l'index, le majeur, l'annulaire et l'auriculaire. Il convient d'utiliser les empreintes digitales d'une même main, en commençant par la main droite.

Les données dactyloscopiques doivent correctement préciser dans leur intitulé à quel doigt elles se rapportent. En cas d'impossibilité physique, permanente ou temporaire, les empreintes sont toujours identifiées conformément à la norme ANSI/NIST-ITL 1-2011: Update 2015 ⁽⁹⁾ (ou une version plus récente) et les éventuels doigts restants sont utilisés.

⁽⁷⁾ La permutation est un mode de configuration particulier du système d'établissement de correspondances biométriques, qui permet de comparer entre elles des empreintes digitales provenant de chacun des deux ensembles, quelle que soit leur position dans l'ensemble. On élimine ainsi les éventuelles erreurs humaines relatives à l'ordre des doigts, et la plus grande exactitude biométrique possible est assurée pour la vérification.

⁽⁸⁾ C(2019) 1260.

⁽⁹⁾ Idem.

Dans le cas d'identifications effectuées dans un cadre autre que les vérifications aux frontières, le CS-EES doit avoir la capacité d'accepter les empreintes digitales roulées transmises par les autorités ayant accès à l'EES et autorisées, par une réglementation européenne différente, à utiliser également ce type d'empreintes. Si l'autorité procède à une identification avec les doigts des deux mains, le CS-EES effectue deux identifications, l'une avec les doigts de la main droite et l'autre avec les doigts de la main gauche.

Par l'image faciale

Le CS-EES effectuera des recherches biométriques au moyen d'images faciales capturées en direct, combinées avec des données dactyloscopiques, conformément aux règles définies dans la section susmentionnée «Par les empreintes digitales».

3.3.2. À des fins répressives

À des fins exclusivement répressives, des recherches peuvent être effectuées au moyen des données biométriques suivantes:

- des ensembles de données dactyloscopiques contenant au moins une empreinte,
- des données dactyloscopiques roulées et des données dactyloscopiques non segmentées des quatre doigts ensemble,
- des empreintes digitales latentes,
- une image faciale combinée avec des données dactyloscopiques,
- une image faciale uniquement.

En cas de recherche par les empreintes digitales, une permutation ⁽¹⁰⁾ des mains doit avoir lieu pour les recherches à des fins répressives. La permutation des mains doit pouvoir être configurée (activer/désactiver) au niveau central, pour atteindre tous les utilisateurs.

L'identification à des fins répressives par les empreintes digitales sera réalisée sur toutes les empreintes stockées, sans tenir compte de leur qualité, ou seulement sur celles respectant un certain seuil de qualité défini dans la configuration de recherche choisie par l'utilisateur pour la recherche. Le CS-EES fournira à l'EM requérant les données biométriques correspondantes, avec l'indication de la qualité des empreintes extraites. En cas de correspondance avec des empreintes digitales de mauvaise qualité, l'autorité répressive sera informée du fait que des vérifications supplémentaires sont nécessaires pour confirmer la correspondance. Les seuils indiquant une «mauvaise qualité de données» qui impose des vérifications supplémentaires seront précisés dans les spécifications techniques visées à l'article 37, paragraphe 1, du règlement (UE) 2017/2226.

Les recherches biométriques au moyen de la seule image faciale peuvent être exécutées aux seules fins de l'article 32, paragraphe 2, du règlement (UE) 2017/2226. Dans un tel cas, l'utilisateur précisera la valeur limite du nombre de correspondances à afficher comme résultat. Le nombre maximal de dossiers affichés est de quatre cents. Dans un premier temps, l'utilisateur aura accès aux deux cents fichiers offrant la meilleure correspondance. Si nécessaire, l'accès aux deux cents fichiers restants sera accordé par le système, si l'utilisateur confirme que la recherche initiale n'a abouti à aucune correspondance.

⁽¹⁰⁾ La permutation des mains permet de comparer les empreintes digitales d'une main avec celles de l'autre main. Elle améliore l'exactitude de la correspondance lorsque la main échantillon n'est pas connue.