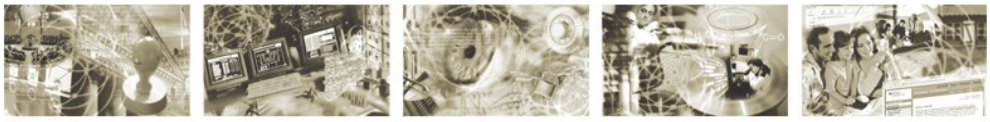
Federal Office
for Information Security



Technical Guideline TR-03121-3

Biometrics for public sector applications

Part 3: Application Profiles and Function Modules

Volume 1: Verification scenarios for ePassport and Identity Card

Version 3.0.1

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63, 53133 Bonn, Germany

Email: TRBiometrics@bsi.bund.de

Internet: https://www.bsi.bund.de

Index of contents

List of tables

List of figures

1 Introduction

This document describes Application Profiles and Function Modules in the scope of the TR Biometrics. For an overview of this guideline, consult TR-03121-1. For a definition of the software architecture component model, see TR-03121-2.

2 Application Profiles for Verification ePassport and Identity Card

2.1 Verification ePassport and Identity Card using facial biometrics

This Application Profile describes the biometric verification using facial biometrics in the context of electronic passports and identity cards.

2.1.1 Introduction

European legislation - European Regulation No. 2252/2004 - as well as national legal requirements (e.g. German PAuswG, Gesetz über Personalausweise und den elektronischen Identitätsnachweis or German Passgesetz, PaßG) mandate a facial image to be included in electronic passports or in electronic identity cards, respectively. The facial image is the primary interoperable biometric characteristic for eMRTD. Verification is typically part of border control which is performed at airports, seaports or land borders.

2.1.2 Process Overview

For biometric verification, authenticated biometric reference data (i.e. the face image of data group 2 according to the ICAO LDS Structure [ICAO_06]) is loaded from the eMRTD. Furthermore, a live image is captured from the document holder by using a capture subsystem. The live images (biometric probes) needs to be of sufficient quality for the comparison (e.g. by methods of pre-qualification) and shall be checked for any presentation attack attempt. Finally, the identity of the document holder is checked by comparing the probes to the reference image (a schematic illustration is given in figure 2-1).

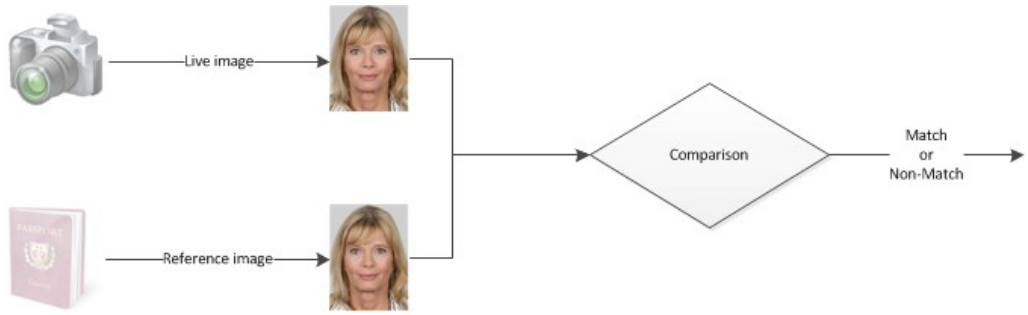


Figure 2-1: Verification ePassport and Identity Card - Facial Image

Aside from the regular verification work flow, for evaluation purposes it is required to conduct quality assurance and cross-comparison measures to get information of the biometric performance and quality of the complete process.

Therefore, an additional evaluation work flow shall be implemented, independently of the regular verification work flow. Acquired and used biometric data for this evaluation shall be safely deleted right after results of the evaluation process are available.

Details on the verification and evaluation work flows are given in the Function Module Process. Table 2-1 lists the mandatory Function Modules for this application profile.

Evaluations according to the Function Module Evaluation should be conducted by the corresponding police authority, not as part of the biometric capture and verification system itself.

2.1.3 Target Audience

The Application Profile "Verification ePassport and Identity Card using facial biometrics" is relevant for the following audience:

- (Border) police authorities
- Suppliers of hardware and software components

2.1.4 Software Architecture Overview

The following components are required by this Application Profile (see TR-03121-2 for detailed definitions of these component types):

- Verification work flow
  - a Capture BSP and a Verification Engine BSP, separating capture and verification functionality in two components, or,
  - a Verification BSP, encapsulated capture and verification functionality in one component. A Verification BSP shall be able to provide the captured live images to the evaluation work flow in an appropriate manner.
- Evaluation work flow
  - one or more QA providers for estimating quality of the processed images,
  - one or more Verification Engine BSPs for cross-comparison purposes.

The hardware functionality may be accessed directly by the BSP or as an option by using a sensor through the Biometric Sensor Function Provider Interface (BioSFPI).

2.1.5 Relevant Standards and Conditions

In addition to the legal requirements (see above), further basic directives and standards are applicable:

- ICAO Document 9303, Machine Readable Travel Documents, Part 1 – Machine Readable Passports, 6th edition, 2006 [ICAO_06]
- ICAO Document 9303, Machine Readable Travel Documents, Part 3 - Size 1 and Size 2 Machine Readable Official Travel Documents, 3rd edition, 2008 [ICAO_08]
- ISO/IEC 19784-1 „Information technology – Biometric application programming interface – Part 1: BioAPI specification“ [ISO_19784-1]
- ISO/IEC 19794-5 „Information technology – Biometric data interchange formats – Part 5: Face Image Data" [ISO_FACE]
- Technical Guideline BSI TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents, Version 2.10, 2012 [EAC]

2.1.6 Function Modules

Table 2-1 enumerates the mandatory Function Modules for this Application Profile.

Module category	*Required Function Modules*
Process	P-PH-VID
Acquisition Hardware	AH-PH-VID
Acquisition Software	AS-PH-VID
Presentation attack detection	PAD-PH-VID
Biometric Image Processing	BIP-PH-VID
Quality Assurance	QA-PH-VID (verification work flow), QA-PH-SB (evaluation work flow)
Compression	COM-PH-VID
Coding	COD-PH-VID
Operation	O-PH-VID
User Interface	UI-PH-VID
Reference Storage	-
Biometric Comparison	CMP-PH-VID
Logging	LOG-PH-VID
Coding	COD-PH-VID
Evaluation	EVA-PH-VID

Table 2-1: Application Profile Verification ePassport and Identity Card using facial biometrics

2.2 Verification ePassport and Identity Card using fingerprint biometrics

This Application Profile describes the biometric verification using fingerprint biometrics in the context of electronic passports and identity cards.

2.2.1 Introduction

European legislation - European Regulation No. 2252/2004 - as well as national legal requirements (e.g. German PAuswG, Gesetz über Personalausweise und den elektronischen Identitätsnachweis or German Passgesetz, PaßG) mandate two fingerprints to be included in electronic passports or in electronic identity cards, respectively (Note that fingerprints are voluntary in the context of the German Identity Card). The fingerprints serve as secondary biometric characteristic for eMRTD in the area of the European Union. Verification can be conducted as part of border control which is performed at airports, seaports or land borders, both in an automated self-service scenario as in a regular manual control scenario.

2.2.2 Process Overview

For biometric verification, authenticated biometric reference data (i.e. the fingerprints of data group 3 according to the ICAO LDS Structure [ICAO_06]) is loaded from the eMRTD. Furthermore, a live image is captured from the document holder by using a fingerprint scanner. The live images (biometric probes) need to be of sufficient quality for the comparison and shall be checked for any presentation attack attempt. Finally, the identity of the document holder is checked by comparing the probes to the reference image (a schematic illustration is given in figure 2-2).

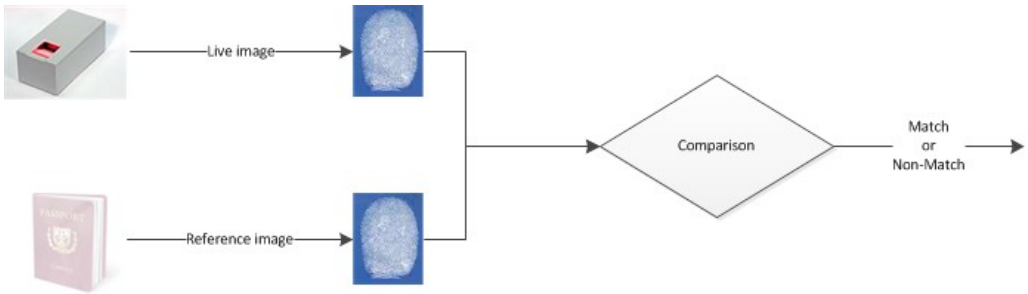


Figure 2-2: Verification ePassport and Identity Card - Fingerprints

Aside from the regular verification work flow, for evaluation purposes it is required to conduct quality assurance and cross-comparison measures to get information of the biometric performance and quality of the complete process.

Therefore, an additional evaluation work flow shall be implemented, independently of the regular verification work flow. Acquired and used biometric data for this evaluation shall be safely deleted right after results of the evaluation process are available.

Details on the verification and evaluation work flows are given in the Function Module Process. Table 2-2 lists the mandatory Function Modules for this application profile.

Evaluations according to the Function Module Evaluation should be conducted by the corresponding police authority, not as part of the biometric capture and verification system itself.

2.2.3 Target Audience

The Application Profile “Verification ePassport and Identity Card using fingerprint biometrics” is relevant for the following audience:

– (Border) police authorities

– Suppliers of hardware and software components

2.2.4 Software Architecture Overview

The following components are required by this Application Profile (see TR-03121-2 for detailed definitions of these component types):

– Verification work flow

  – a Capture BSP and a Verification Engine BSP, separating capture and verification functionality in two components, or,

  - a Verification BSP, encapsulated capture and verification functionality in one component. A Verification BSP shall be able to provide the captured live images to the evaluation work flow in an appropriate manner.

- Evaluation work flow
  - one or more QA providers for estimating quality of the processed images,
  - one or more Verification Engine BSPs for cross-comparison purposes.

The hardware functionality may be accessed directly by the BSP or as an option by using a sensor through the Biometric Sensor Function Provider Interface (BioSFPI).

Note that this application profile currently doesn't impose further restriction on the use of a QA provider as given in TR-03121-2. The choice of QA providers used in the evaluation work flow should be based on which providers are considered state-of-the-art at time of implementation.

2.2.5 Relevant Standards and Conditions

In addition to the legal requirements (see above), further basic directives and standards are applicable:

- ICAO Document 9303, Machine Readable Travel Documents, Part 1 – Machine Readable Passports, 6th edition, 2006 [ICAO_06]
- ICAO Document 9303, Machine Readable Travel Documents, Part 3 - Size 1 and Size 2 Machine Readable Official Travel Documents, 3rd edition, 2008 [ICAO_08]
- ISO/IEC 19784-1 „Information technology – Biometric application programming interface – Part 1: BioAPI specification“ [ISO_19784-1]
- ISO/IEC 19794-4 „Information technology – Biometric data interchange formats – Part 4: Finger Image Data” [ISO_FINGER]
- Technical Guideline BSI TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents, Version 2.10, 2012 [EAC]

2.2.6 Function Modules

Table 2-2 enumerates the mandatory Function Modules for this Application Profile.

Module category	*Required function modules*
Process	P-FP-VID
Acquisition Hardware	AH-FP-FTR
Acquisition Software	AS-FP-MF/AS-FP-SF
Presentation attack detection	PAD-FP-VID
Biometric Image Processing	BIP-FP-APP
Quality Assurance	-
Compression	COM-FP-WSQ
Operation	O-FP-VID
User Interface	UI-FP-VID
Reference Storage	-
Biometric Comparison	CMP-FP-VID
Logging	LOG-FP-VID
Coding	COD-FP-VID
Evaluation	EVA-FP-VID

Table 2-2: Application Profile Verification ePassport and Identity Card using fingerprint biometrics

3 Function Modules

This chapter lists all the Function Modules for the defined Application Profiles.

3.1 Process

The module Process describes the modality of how the different Function Modules have to be called and combined in order to achieve the objective of the Application Profile. Any alternative call of modules (e.g. for conformance testing) is specified with additional information.

3.1.1 P-FP-VID

This function block describes the overall acquisition software process for verification of an identity based on the comparison of a live captured fingerprint and a stored reference.

Requirements

General requirements

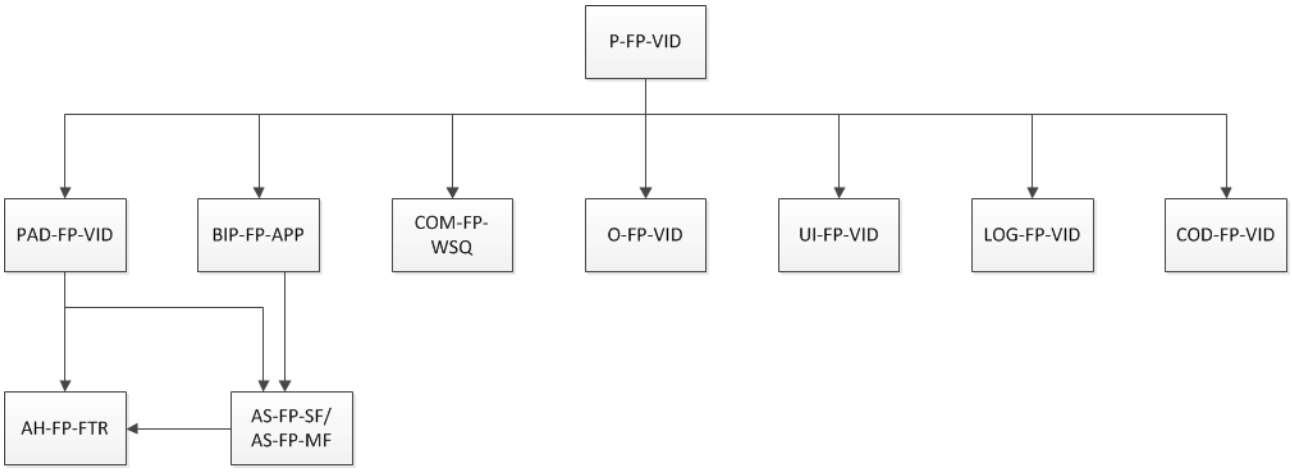


Figure 3-1: Relevant Function Modules for the verification of fingerprint images

Figure 3-1 gives an overview of the required function modules. Multiple lossy compressions shall not occur within the overall process.

The whole process consists of the standard verification work flow and the evaluation work flow. The evaluation work flow shall be executed independently after the standard verification work flow. Both work flows return separate logging data according to FM COD-FP-VID. Verification and evaluation logging data shall be linked by means of the provided transaction identifiers. Figure 3-2 shows a general overview over the complete process with both work flows.

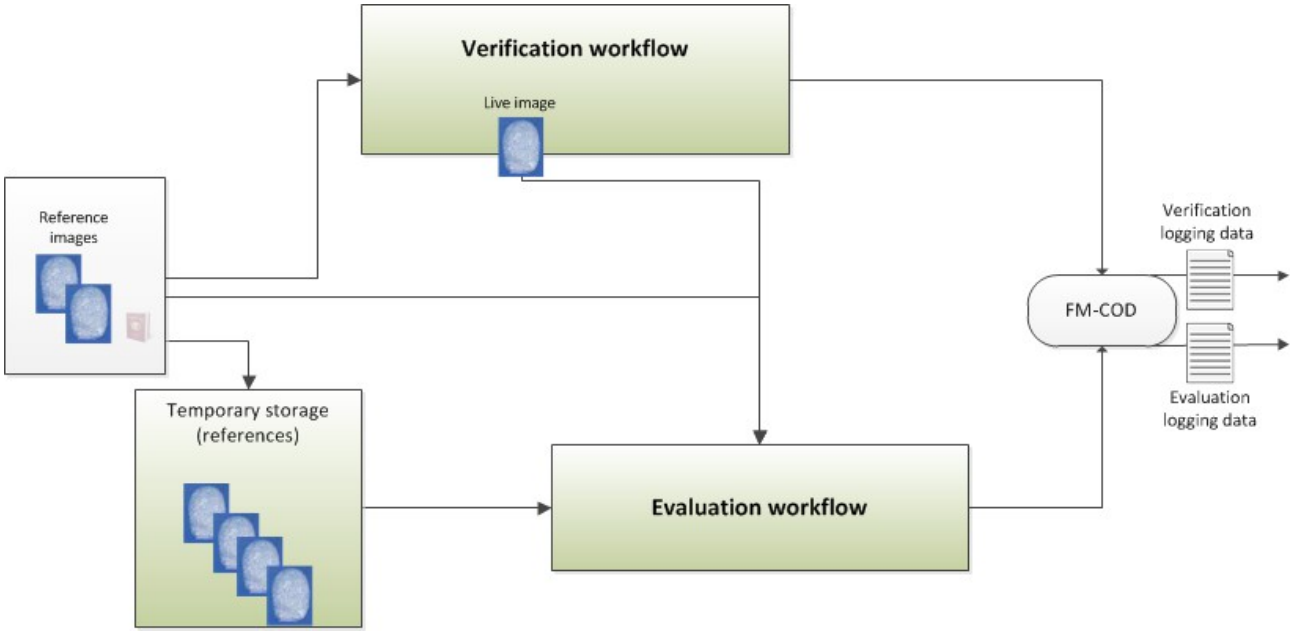


Figure 3-2: Overall work flow of verification ePassport and identity card

Standard verification work flow

An overview of the standard verification work flow is given in figure 3-3.

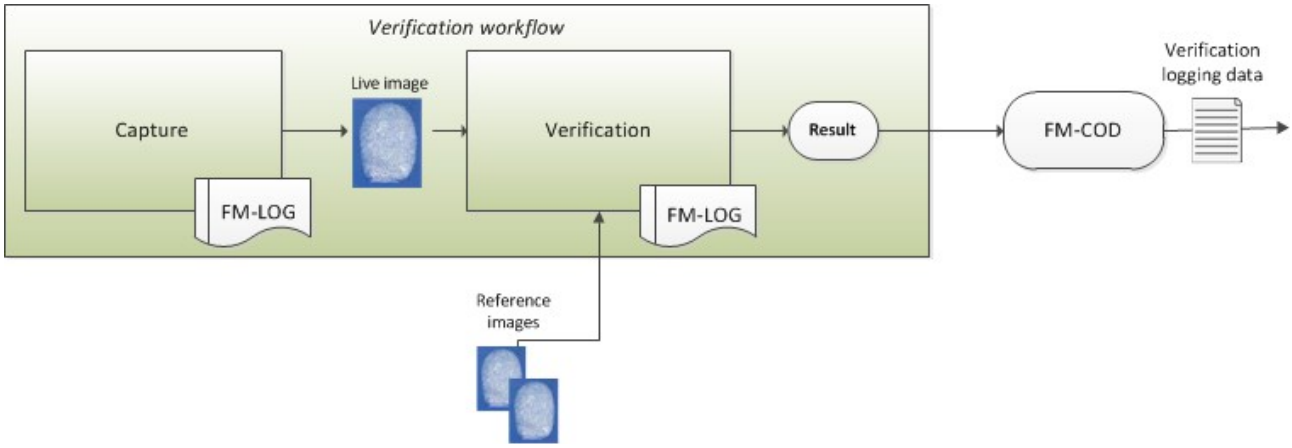


Figure 3-3: Verification work flow of verification ePassport and identity card

The full process of provision of the reference images (candidates), acquisition of the fingerprint with verification afterwards is presented in figure 3-4. The following steps shall be performed:

1. The reference images (DG3) stored in the eMRTD are read and the images are extracted. Note that typically two images are encoded in DG3, it is also possible that only one finger is present or none at all. In case no finger is present, the verification shall fail.
Furthermore, live image data (probe) is captured from a fingerprint scanner with respect to AH-FP-FTR, AS-FP-SF or AS-FP-MF, PAD-FP-VID and BIP-FP-APP. Live image data may optionally be compressed according to COM-FP-WSQ.
In case of multi-finger scanners, the process may capture multiple fingers (e.g. a complete right hand slap) and use the relevant segmented fingers for comparison.

2. If the candidates as well as the probes are available a verification according to CMP-FP-VID shall be performed. In case of doubt about which hand or finger was placed on the scanner, multiple cross comparisons to establish the right finger are permitted.

3. If the comparison process described in step 2 is successful the process ends with a successful verification. In the unsuccessful case an exit condition is checked. If the specified time-out is not reached a new probe is captured (see also UI-FP-VID for necessary user guidance) and again the verification is started. If the time-out is reached the process ends with an non-match decision. All gathered information is then logged and coded according to FM LOG-FP-VID and FM COD-FP-VID.

By means of PAD-FP-VID the officer shall receive a warning when the PAD subsystem detects a spoofing attack. Typically PAD data does not apply directly to a specific image, therefore, the biometric component shall be able to correlate an image that was used for verification with the corresponding PAD information. It is recommended that the biometric subject is checked again manually in case of a PAD warning.

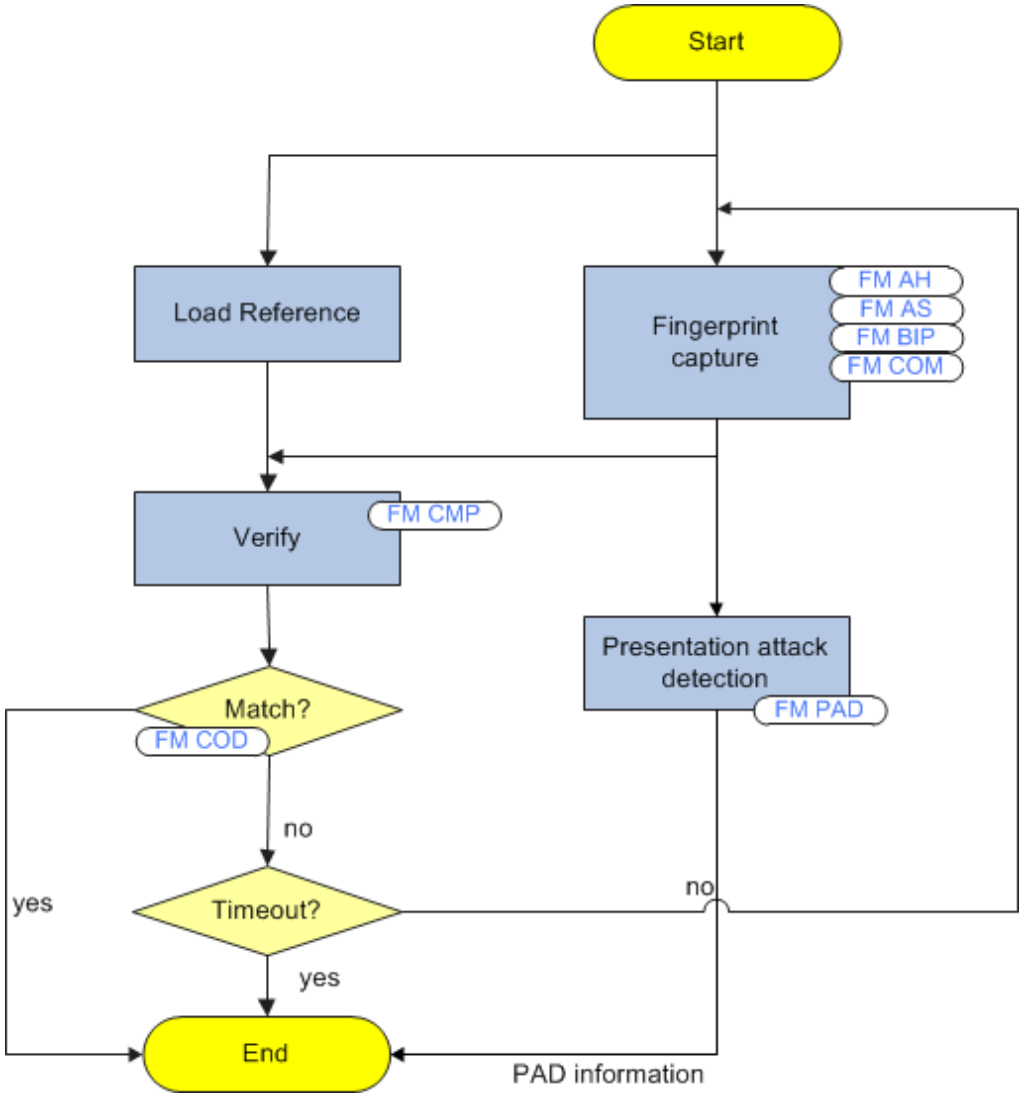


Figure 3-4: Detailed acquisition and comparison work flow

Evaluation work flow

For further evaluation purposes, the candidates are added to a temporary list of previous candidates. This is needed for an evaluation work flow which is conducted to get information about the quality and security level of the overall verification process. The probe and the last few candidates shall be used for quality assurance checks and cross-comparison tasks within the evaluation work flow only. Images shall be deleted immediately after template generation, templates shall be deleted within 24 hours.

The evaluation work flow consists of two processes:

– quality assurance on probe and candidate images

– cross-comparison: genuine comparison of probe and given candidates, imposter comparisons of given probe with non-mated candidates.

An overview of the evaluation work flow is given figure 3-5.

Quality assurance is conducted by a QA provider which implements the quality assessment algorithm for fingerprint images.

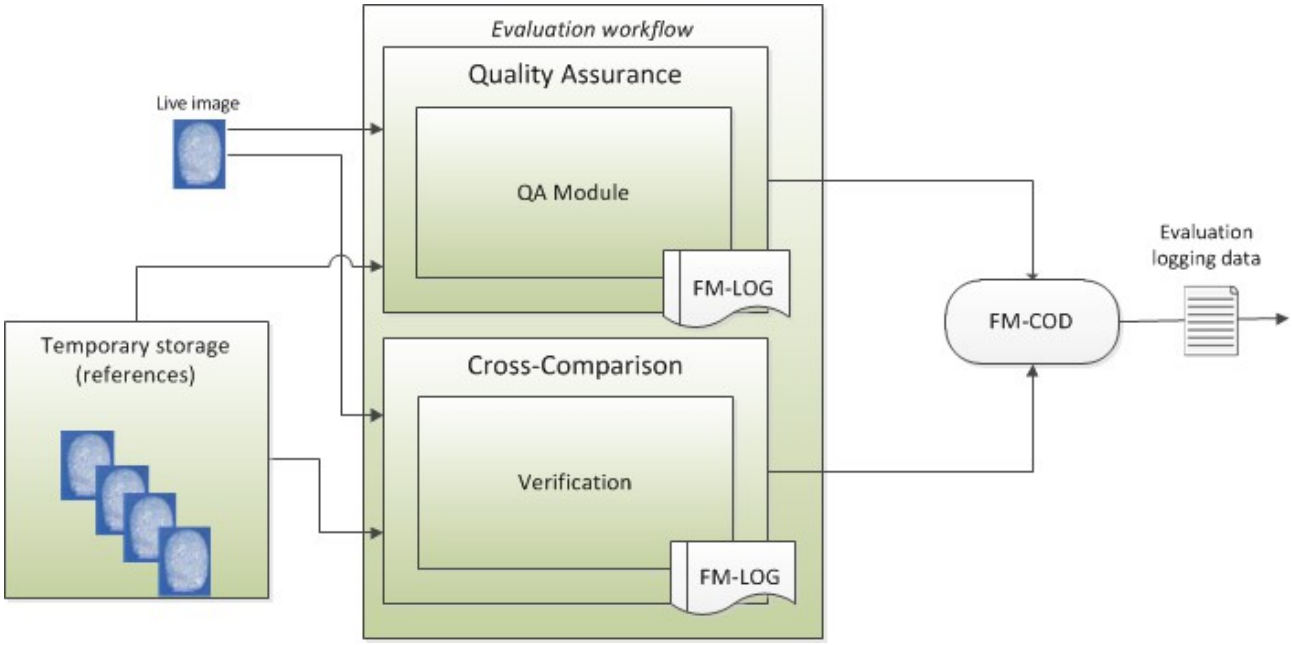


Figure 3-5: Evaluation work flow of verification ePassport and identity card

Cross-comparison is conducted for the probe and the last few candidates of the temporary list. It is intended to produce several imposter comparison scores and results for evaluating and determining the biometric performance of the used (or even more) verification algorithms.[1] Furthermore, at least one genuine comparison of the probe and the according candidate is made. A BioAPI compliant Verification Engine BSP is used for comparing probes and candidates. Results of cross-comparison are logged and finally combined with all other logging data of the evaluation work flow within the Function Module Coding (FM COD-FP-VID).

In detail, the following approach has to be implemented for cross-comparison. For the assessment of the performance of the complete biometric system genuine comparisons of the candidate from the document and the captured probe as well as comparisons with candidates of not identical people are calculated. For that purpose, the following procedure has to be applied:

1. The probe is compared against the candidate (genuine comparison). As typically two candidates are available from the subject's eMRTD, only the one yielding the higher score shall be considered as genuine comparison. In addition to the comparison in the standard verification work flow, additional verification algorithms can be used here.
2. The probe from the verification process is compared against the other non-mated candidates in the list and the comparison score is saved (imposter comparisons).
3. The candidate is added to the dynamic list.

1 Typically, one verification algorithm is used for the main verification work flow, and a second one is used in addition, on the evaluating back-end system. This allows – at least partially - for filtering out “false imposters” at a later evaluation stage.

4. The oldest candidate in the list and the probe are discarded.

It is assumed that the candidate fingerprint templates of the last present passport verifications are saved anonymously in a dynamic list.

Only one probe from the standard verification work flow shall be used in the evaluation work flow. The selected probe is the one which was used for successful comparison, or, if no successful comparison was conducted, the one with the best prequalification value.

The application shall ensure that a candidate is added only once to the list to avoid false imposter comparisons.

3.1.2 P-PH-VID

This function block describes the overall acquisition software process for verification of an identity based on the comparison of a live captured facial image and a stored reference.

Requirements

General requirements

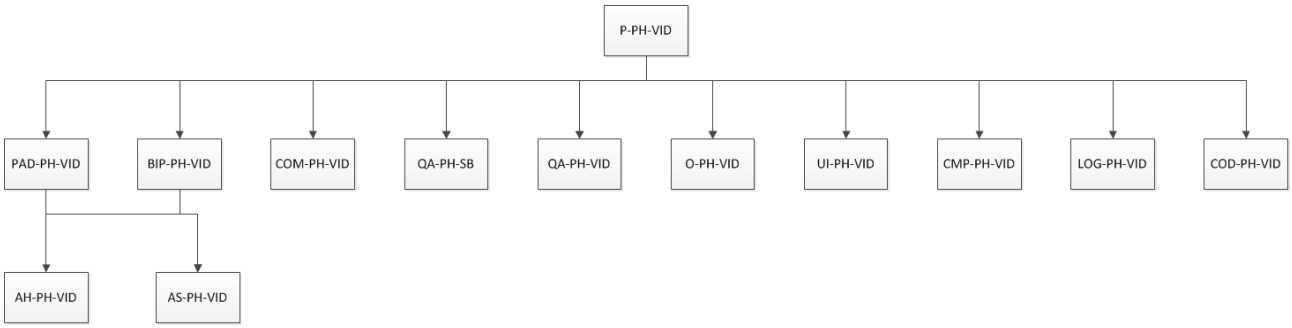


Figure 3-6: Relevant Function Blocks for the verification of facial images

Figure 3-6 gives an overview of the required function modules. Multiple lossy compressions shall not occur within the overall process.

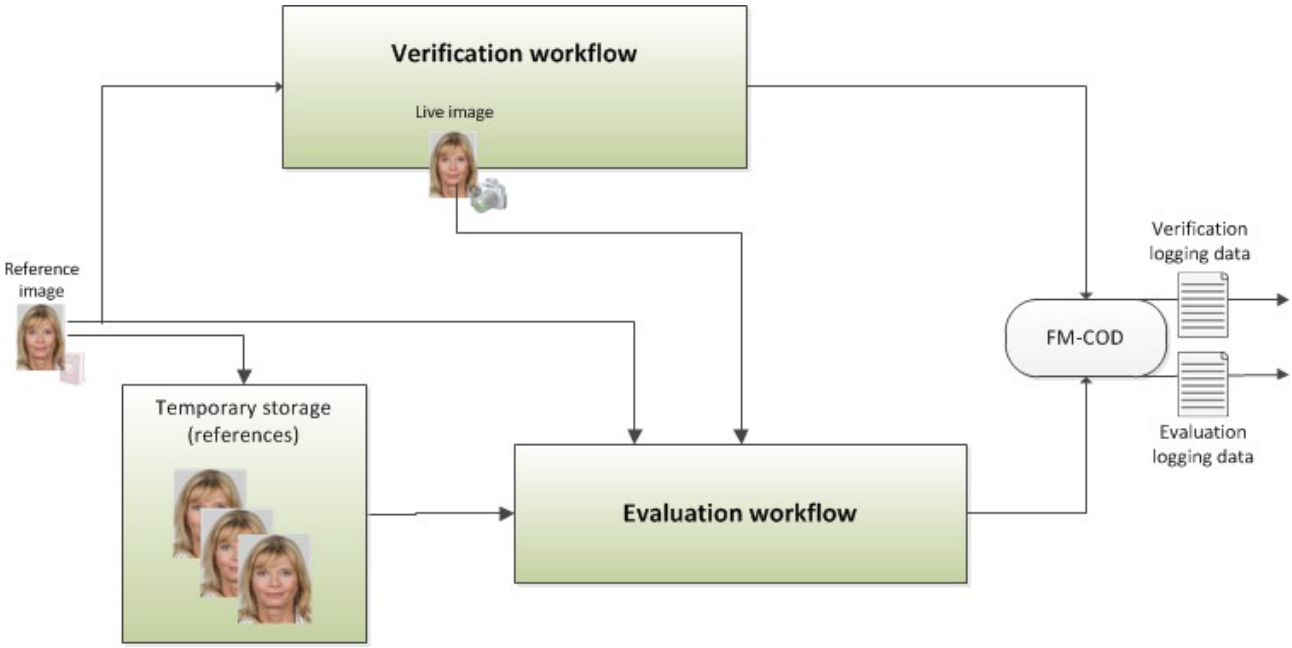


Figure 3-7: Overall work flow of verification ePassport and identity card

The whole process consists of the standard verification work flow and the evaluation work flow. The evaluation work flow shall be executed independently after the standard verification work flow. Both work flows return separate logging data according to FM COD-PH-VID. Verification and evaluation logging data shall be linked by means of the provided transaction identifiers. Figure 3-7 shows a general overview over the complete process with both work flows.

Standard verification work flow

An overview of the standard verification work flow is given Figure 3-8.

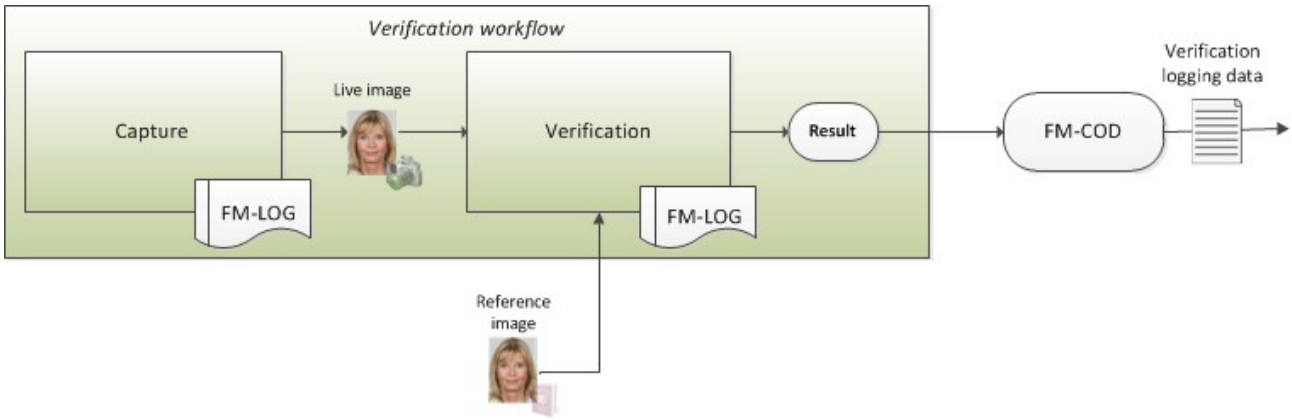


Figure 3-8: Verification work flow of verification ePassport and identity card

The full process of provision of the reference image (candidate), acquisition of the facial image with verification afterwards is presented in figure 3-9. The following steps shall be performed:

1. The reference (DG2) stored in the eMRTD is read and the image is extracted.
Furthermore, live image data (probe) is captured with respect to AH-PH-VID, AS-PH-VID, PAD-PH-VID and BIP-PH-VID. Prequalification (as defined by FM QA-PH-VID) ensures that only images of sufficient quality are taken.
Live image data may be compressed according to COM-PH-VID.

2. If the candidate as well as the probe are available a verification according to CMP-PH-VID shall be performed.

3. If the comparison process described in step 2 is successful the process ends with a successful verification. In the unsuccessful case an exit condition is checked. If the specified time-out is not reached a new probe is captured and again the verification is started. If the time-out is reached the process ends with an non-match decision. All gathered information is then logged and coded according to FM LOG-PH-VID and FM COD-PH-VID.

During the complete transaction of acquisition and verification the border control officer should ensure that the document holder does not try to illegally bypass the border control by using fake biometrics or other mechanisms. By means of PAD-PH-VID the officer can receive a warning when the PAD subsystem detects a spoofing attack. Typically PAD data does not apply directly to a specific image, therefore, the biometric component shall be able to correlate an image that was used for verification with the corresponding PAD information.

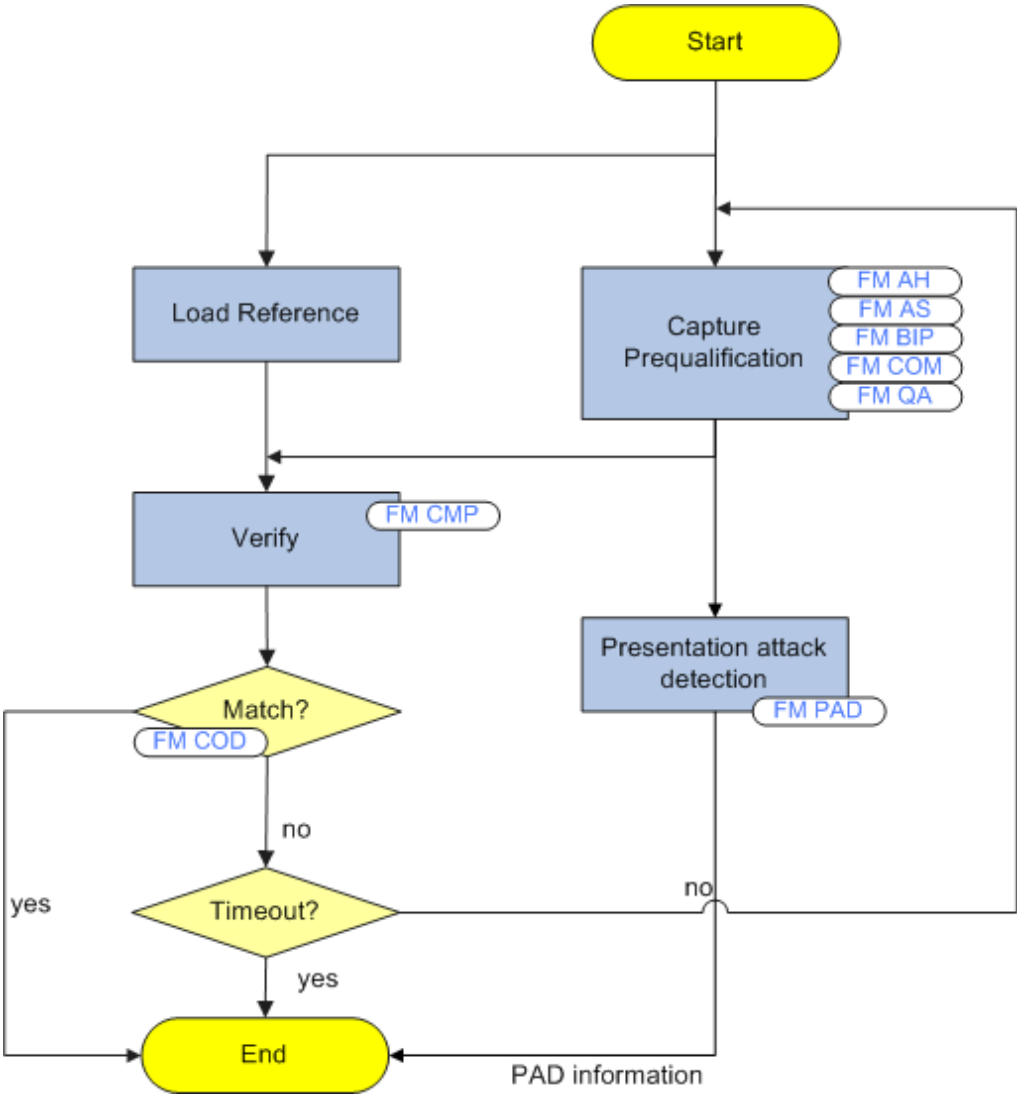


Figure 3-9: Detailed acquisition and comparison work flow

Evaluation work flow

For further evaluation purposes, the candidate is added to a temporary list of reference images. This is needed for an evaluation work flow which is conducted to get information about the quality and security level of the overall verification process. The probe and the last few candidates shall be used for quality assurance checks and cross-comparison tasks within the evaluation work flow only. Images shall be deleted immediately after template generation, templates shall be deleted within 24 hours.

The evaluation work flow consists of two processes:

– quality assurance on probe and candidate images

– cross-comparison: genuine comparison of probe and given candidate, imposter comparisons of given probe with non-mated candidates.

An overview of the evaluation work flow is given figure 3-10.

Quality assurance for evaluation purposes shall be conducted according to FM QA-PH-SB. Quality assurance is conducted by a QA provider which implements the quality assessment algorithm for facial images.

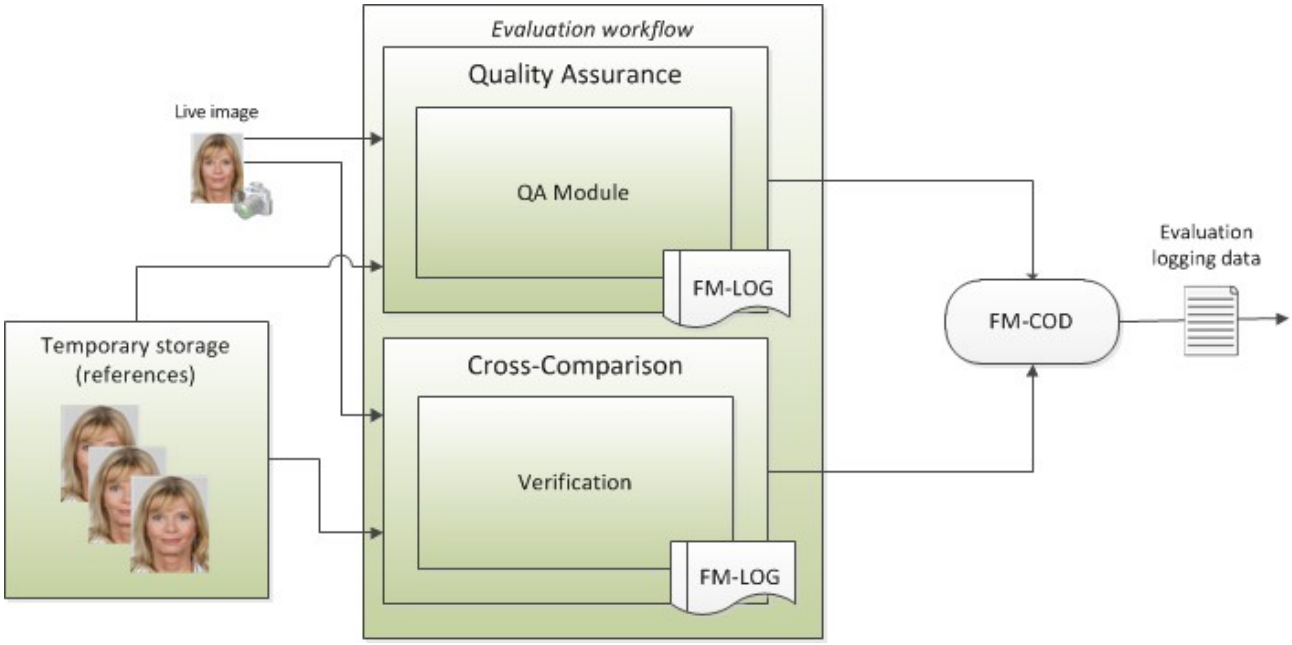


Figure 3-10: Evaluation work flow of verification ePassport and identity card

Cross-comparison is conducted for the probe and the last few candidates of the temporary list. It is intended to produce several imposter comparison scores and results for evaluating and determining the biometric performance of the used (or even more) verification algorithms.[2] Furthermore, at least one genuine comparison of the probe and the according candidate is made. A BioAPI compliant Verification Engine BSP is used for comparing probes and candidates. Results of cross-comparison are logged and finally combined with all other logging data of the evaluation work flow within the Function Module Coding (FM COD-PH-VID).

In detail, the following approach has to be followed for cross-comparison. For the assessment of the performance of the complete biometric system genuine comparisons of the candidate from the document and the captured probe as well as comparisons with candidates of not identical people are calculated. For that purpose, the following procedure has to be applied:

1. The probe is compared against the candidate (genuine comparison). In addition to the comparison in the standard verification work flow, additional verification algorithms can be used here.
2. The probe from the verification process is compared against the other non-mated candidates in the list and the comparison score is saved (imposter comparisons).
3. The candidate is added to the dynamic list.
4. The oldest candidate in the list and the probe are discarded.

2 Typically, one verification algorithm is used for the main verification work flow, and a second one is used in addition, on the evaluating back-end system. This allows – at least partially - for filtering out “false imposters” at a later evaluation stage.

It is assumed that the candidate templates of the last present passport verifications are saved anonymously in a dynamic list.

Only one probe from the standard verification work flow shall be used in the evaluation work flow. The selected probe is the one which was used for successful comparison, or, if no successful comparison was conducted, the one with the best prequalification value.

The application shall ensure that a candidate is added only once to the list to avoid false imposter comparisons.

3.2 Acquisition Hardware

Devices that are used for digitising physical, representable biometric characteristics are called acquisition hardware. Scanners for capturing photographs, digital cameras to capture images of the face, fingerprint sensors, or signature tablets can be named as examples.

3.2.1 AH-FP-FTR

This function block describes the requirements for high quality fingerprint scanners (single finger and multi finger).

Requirements

For the acquisition of the fingerprints, optical sensors using the principle of frustrated total reflection (FTR live scanner) according to setting level 31 or 41 in table 1 of [ISO_FINGER] (especially this means a resolution of 500 ppi or 1000 ppi) have to be used exclusively.

For the acquisition of the fingerprints, only devices are permitted which meet the following requirements (in analogy to [EBTS/F]). Notwithstanding, a capturing area of at minimum 16 mm width and 20 mm height is required (deviating from table F 1 in [EBTS/F]) for single finger scanners.

Grayscale linearity

When measuring a stepped series of uniform target reflectance patches (“step tablet”) that substantially covers the scanner’s gray range, the average value of each patch shall be within 7.65 gray-levels of a linear, least squares regression line fitted between target reflectance patch values (independent variable) and scanner output gray-levels of 8 bit resolution (dependent variable).

Resolution and geometrical accuracy

Resolution: The scanner’s final output fingerprint image shall have a resolution, in both sensor detector row and column directions, in the range: (R – 0.01R) to (R + 0.01R). The magnitude of R is either 500 ppi or 1000 ppi; a scanner may be certified at either one or both of these resolution levels. The scanner’s true optical resolution shall be greater than or equal to R.

Across-Bar geometric accuracy: When scanning a 1.0 cy/mm, multiple parallel bar target, in both vertical bar and horizontal bar orientations, the absolute value of the difference (D), between the actual distance across parallel target bars (X), and the corresponding distance measured in the image (Y), shall not exceed the following values, for at least 99% of the tested cases in each print block measurement area and in each of the two directions

- for 500 ppi scanners:
  $D \leq 0.0007$, for $0.00 < X \leq 0.07$ and
  $D \leq 0.01X$, for $0.07 \leq X \leq 1.50$
- for 1000 ppi scanners:
  $D \leq 0.0005$, for $0.00 < X \leq 0.07$ and
  $D \leq 0.0071X$, for $0.07 \leq X \leq 1.50$

where $D = |Y-X|$, X = actual target distance, Y = measured image distance (D, X, Y are in inches)

Along-Bar geometric accuracy: When scanning a 1.0 cy/mm, multiple parallel bar target, in both vertical bar and horizontal bar orientations, the maximum difference in the horizontal or vertical direction, respectively, between the locations of any two points within a 1.5 inch segment of a given bar image, shall be less than 0.016 inches for at least 99% of the tested cases in each print block measurement area and in each of the two orthogonal directions.

Contrast transfer function

The spatial frequency response shall be measured using a binary grid target (Ronchi-Grating), denoted as contrast transfer function (CTF) measurement. When measuring the bar CTF, it shall meet or exceed the minimum modulation values defined by equation [EQ 1] or equation [EQ 2], in both the detector row and detector column directions, and over any region of the scanner's field of view. CTF values computed from equations [EQ 1] and [EQ 2] for nominal test frequencies are given in the following table. None of the CTF modulation values measured at specification spatial frequencies shall exceed 1.05. The output bar target image shall not exhibit any significant amount of aliasing.

Frequency [cy/mm]	*Minimum Modulation for 500 ppi scanners*	*Minimum Modulation for 1000 ppi scanners*	*Maximum Modulation*
1.0	0.948	0.957	1.05
2.0	0.869	0.904	1.05
3.0	0.791	0.854	1.05
4.0	0.713	0.805	1.05
5.0	0.636	0.760	1.05
6.0	0.559	0.716	1.05
7.0	0.483	0.675	1.05
8.0	0.408	0.636	1.05
9.0	0.333	0.598	1.05
10.0	0.259	0.563	1.05
12.0	---	0.497	1.05
14.0	---	0.437	1.05
16.0	---	0.382	1.05
18.0	---	0.332	1.05
20.0	---	0.284	1.05

Table 3-1: Minimum and maximum modulation

It is not required that the bar target contain the exact frequencies listed in table 3-1, however, the target does need to cover the listed frequency range and contain bar patterns close to each of the listed frequencies. The following equations are used to obtain the minimum acceptable CTF modulation values when using bar targets that contain frequencies not listed in table 3-1:

– 500 ppi scanner, for f = 1.0 to 10.0 cy/mm:
  CTF = 3.04105E-04 * f2 - 7.99095E-02 * f + 1.02774 [EQ 1]

– 1000 ppi scanner, for f = 1.0 to 20.0 cy/mm:
  CTF = - 1.85487E-05*f3 +1.41666E-03*f2 - 5.73701E-02* f +1.01341 [EQ 2]

For a given bar target, the specification frequencies include all of the bar frequencies which that target has in the range 1 to 10 cy/mm (500 ppi scanner) or 1 to 20 cy/mm (1000 ppi scanner).

Signal-to-noise ratio and the gray–level uniformity

The white signal-to-noise ratio (SNR) and black SNR shall each be greater than or equal to 125.0, in at least 97% of respective cases, within each measurement area.

The gray level uniformity is defined for the three following cases:

- Adjacent row, column uniformity: At least 99% of the average gray-levels between every two adjacent quarter-inch long rows and 99% between every two adjacent quarter-inch long columns, within each imaged area, shall not differ by more than 1.0 gray-levels when scanning a uniform low reflectance target, and shall not differ by more than 2.0 gray-levels when scanning a uniform high reflectance target.
- Pixel to pixel uniformity: For at least 99.9% of all pixels within every independent 0.25 inch by 0.25 inch area located within each imaged area, no individual pixel's gray-level shall vary from the average by more than 22.0 gray-levels, when scanning a uniform high reflectance target, and shall not vary from the average by more than 8.0 gray-levels, when scanning a uniform low reflectance target.
- Small area uniformity: For every two independent 0.25 inch by 0.25 inch areas located within each imaged area, the average gray-levels of the two areas shall not differ by more than 12.0 graylevels when scanning a uniform high reflectance target, and shall not differ by more than 3.0 gray-levels when scanning a uniform low reflectance target.

Gray scale range of fingerprint images

A fingerprint scanner operating at 500ppi or 1000ppi, has to perform the following sets of live scans:

- For a standard roll and plain finger live scanner: capture a complete set of fingerprints from each of 10 subjects; i.e., 10 rolls (all 5 fingers from each hand), 2 plain thumb impressions, and 2 plain 4-finger impressions.
- For a palm scanner component of a live scan system: capture left and right palms from each of 10 subjects.
- For an identification flats live scanner: capture left and right 4-finger plain impressions and dual thumb plain impressions from each of 10 subjects.

Within the histogram of each image all gray values with at least 5 Pixels in this image are counted. The histogram has to show no break and no other artefact. At least 80% of the captured individual fingerprint images shall have a gray-scale dynamic range of at least 200 gray-levels, and at least 99% shall have a dynamic range of at least 128 gray-levels.

3.2.2 AH-PH-VID

This function block describes the requirements for integrated camera systems that are used to obtain digitised face images. Specific requirements apply to e-gate scenarios.

Requirements

General requirements

For integrated camera systems the following general requirements have to be met:

- the minimum physical resolution of the camera video stream should be at least 640 x 480 pixels,
- the camera system shall adapt automatically to the height of the person standing in front of it,
- the camera system shall cover at least a range of 140cm to 200cm of a person's body height (if standing in front of the camera system). It is recommended that the camera system covers the range of 120cm to 220cm of the person's body height (if standing in front of the camera system),
- the camera shall be able to capture a frontal image of the person if the person is looking straight to the camera,
- the camera system shall use active diffuse lighting to ensure a uniform illumination of the captured face image and to be independent of external lighting; mirroring effects of glasses have to be avoided,
- the camera system shall guarantee the sharpness of the captured image within the designated capture area,
- the camera system shall minimise the distortion of the captured face within the whole capture area.

Specific requirements for e-gate scenarios

For the usage in e-gate scenarios the following additional requirements have to be met:

- the camera system shall be designed to be placed in the moving direction of the person (sideways attached camera units which require a rotation of the moving person shall not be used); it is recommended that at a distance of 70cm before the end of the gate (typically the exit door), the necessary rotation of the person shall be less than 15 degrees,
- persons have to be captured within a typical range of at least 200cm with sufficient sharpness and with minimized distortion of the captured face,
- the camera system shall provide a feedback screen for displaying the camera live stream (digital mirror)[3]; if the person is looking straight to the feedback screen the viewing direction of the person shall be frontal.

3 This feedback screen is typically used also for user information and guidance.

3.3 Acquisition Software

Acquisition Software contains all functionality regarding image processing except for biometric purposes. Therefore, this module usually contains device driver software for the Acquisition Hardware or, in general, software that is very close to the physical hardware such as firmware. Furthermore, colour management and image enhancement mechanisms are part of this software layer.

3.3.1 AS-FP-MF

This function block describes the requirements and interfaces for Acquisition Software for multi finger scanners.

Requirements

The image provided by Acquisition Software has to meet the criteria of fingerprints as described in [ISO_FINGER] (particularly chapter 7 "Image acquisition requirements"). The requirements according to setting level 31 or 41 from table 1 in [ISO_FINGER] are in force.

For the acquisition process, a pre-qualification of the fingerprints to prefer high quality has to be used. The activation of the acquisition has to occur automatically. The capture should prefer the highest quality image of a sequence, at least the last captured image (after time-out) of a sequence. It is possible that this functionality is part of the hardware firmware and may not be available as separate software component.

3.3.2 AS-FP-SF

This function block describes the requirements and interfaces for Acquisition Software for single finger scanners.

Requirements

The image provided by Acquisition Software has to meet the criteria of fingerprints as described in [ISO_FINGER] (particularly chapter 7 "Image acquisition requirements"). The requirements according to setting level 31 or 41 from table 1 in [ISO_FINGER] are in force.

For the acquisition process, a pre-qualification of the fingerprints to prefer high quality has to be used. The activation of the acquisition has to occur automatically. The capture should prefer the highest quality image of a sequence, at least the last captured image (after time-out) of a sequence. It is possible that this functionality is part of the hardware firmware and may not be available as separate software component.

If the sensor was not able to capture an image (e.g. because no finger was placed on it), it is not required to return an image after time-out. In this case, an adequate error code has to be returned.

3.3.3 AS-PH-VID

This function block describes the requirements and interfaces for Acquisition Software used for integrated camera systems in order to obtain digitised face images.

Requirements

The acquisition software of the camera system shall provide uncompressed image data for further processing. It shall either provide raw uncompressed image data (e.g. YUV422, RGB) or use a lossless image container format (e.g. BMP, TIFF).

3.4 Presentation attack detection

The objective of the module Presentation Attack Detection is to avoid presentations with the goal to subvert an enrolment, verification of identification process.

3.4.1 PAD-FP-VID

This function block describes requirements for presentation attack detection in the context of the acquisition of fingerprint biometrics. This function module is especially relevant for use cases where no direct observation of the acquisition process by an official is possible (e.g. in self-service scenarios).

Requirements

General requirements

The capture system shall contain a presentation attack detection subsystem detecting spoofing attempts using artefacts by which an attacker is trying to establish a different biometric characteristic as probe in the verification or identification process.

The presentation attack detection subsystem may consist of hardware and software (e.g. the used fingerprint scanner may have additional sensors designed for this purpose).

Typical artefacts consist of fake fingers (e.g. silicone, gelatine based). The presentation attack detection subsystem shall be able to detect all well-known attack types.

Integration requirements

The presentation attack detection subsystem shall be independent of the regular capture subsystem, i.e. it shall not inhibit capturing image data in case of a suspected attack. It shall signal its detection results in the form of a presentation attack detection score to the calling application.[4] It may additionally provide detailed information about the results of the presentation attack detection.

Maintainance requirements

As new technologies and new attack mechanisms are developed over time, it is recommended that the presentation attack detection subsystem is regularly updated and re-evaluated.

Certification requirements

To ensure comparable performance of presentation attack detection subsystems, the system shall be certified under the Common Criteria Agreement according to one of following Protection Profiles:

– BSI-CC-PP-0063-2010: Fingerprint Spoof Detection Protection Profile (FSDPP)

4 Currently, there exists no standard for the interoperable definition of presentation attack detection scores.

– BSI-CC-PP-0062-2010: Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP)

3.4.2 PAD-PH-VID

This function block describes requirements for presentation attack detection in the context of the acquisition of facial biometrics. This function module is especially relevant for use cases where no direct observation of the acquisition process by an official is possible (e.g. in self-service scenarios).

Requirements

General requirements

The capture subsystem shall contain a presentation attack detection subsystem detecting spoofing attempts using artefacts by which an attacker is trying to establish a different biometric characteristic as probe in the verification or identification process.

The presentation attack detection subsystem may consist of hardware and software (e.g. the used camera system may have additional sensors designed for this purpose).

Well-known artefacts are:

– photographs printed on paper or textile,

– photographs displayed on electronic devices (e.g. phones, tablets, laptops),

– videos displayed on electronic devices, especially showing motion of the biometric subject,

– 3D masks (paper based or other materials).

The presentation attack detection subsystem shall be able to detect all well-known attack types.

Integration requirements

The presentation attack detection subsystem shall be independent of the regular capture subsystem, i.e. it shall not inhibit capturing image data in case of a suspected attack. It shall signal its detection results in the form of a presentation attack detection score to the calling application.[5] It may additionally provide detailed information about the results of the presentation attack detection.

Maintenance requirements

As new technologies and new attack mechanisms are developed over time, it is recommended that the presentation attack detection subsystem is regularly updated and re-evaluated.

5 Currently, there exists no standard for the interoperable definition of presentation attack detection scores.

3.5 Biometric Image Processing

The module Biometric Image Processing provides the extraction of all relevant biometric information from the data which is provided by the Acquisition Hardware or the Acquisition Software layer. Thus, a proprietary data block is transformed to a digital image of a biometric characteristic. In general, specific image processing for biometrics is addressed here.

3.5.1 BIP-FP-APP

This function block describes requirements and interfaces for the Biometric Image Processing to provide up to four single finger images for the subsequent reference storage or biometric comparison.

Requirements

The resolution of the fingerprint image has to be 500 ppi corresponding to table 1 in [ISO_FINGER] and, therefore, may differ from the scan resolution.

Depending on the call to capture one, two, three or four fingerprints, this number of individual fingerprints have to be extracted from the input image and provided as single fingerprints.

Note: Segmentation for single finger scanner is optional.

For this segmentation process, the following requirements have to be fulfilled:

- Ability to accept rotated fingerprints in the same direction up to 45°
- Rotated fingerprints in the same direction have to be corrected to be vertical
- Segment the first part over the finger (fingertip)
- Segmentation has to occur on uncompressed data

3.5.2 BIP-PH-VID

This function block describes requirements and interfaces for Biometric Image Processing with respect to the output of integrated camera systems to obtain a facial image that fulfils the requirements for being used within automated facial verification.

Requirements

The biometric image processing shall implement the following requirements:

- colour depth 24 bit RGB or 8 bit grey scale,
- the face shall be fully visible in the foreground of the provided image,
- the minimum distance between both eyes for capture positions of the passenger in the preferred area of the camera range shall be at least 120 pixels.
  For the usage in e-gate scenarios it is allowed to have a lower distance between both eyes (e.g. if the passenger is moving towards the e-gate). This requirement shall be applied at least for the designated area where the passengers stops at the end of the gate.

Recommendations

The biometric image processing should implement the following requirements:

– The face should be cropped and de-rotated from the overall scene in the captured image.
– The size of the face within the image should be according to the geometric requirements of [ISO_FACE].

3.6 Quality Assurance

This module contains all kinds of mechanisms and procedures to check the quality of the biometric data or to select the best quality data out of multiple instances.

3.6.1 QA-PH-SB

This function block describes requirements and interfaces for software that is used for Quality Assurance of digital images to ensure compliance with [ISO_FACE].

Requirements

The Quality Assurance module is used for the software-based automatic check of the conformance of the picture to [ISO_FACE] after the digitisation. Thereby, the geometric properties of the picture as well as the digital parameters of the image are analysed and rated.

The standard which is relevant for the quality of facial images [ISO_FACE] hierarchically describes requirements to the facial images as shown in figure 3-11. In the following, full frontal images are expected.

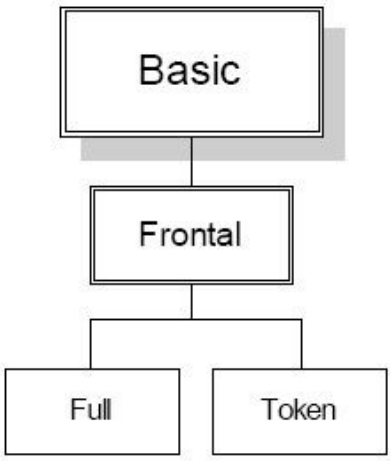


Figure 3-11: Image types and their dependencies according to [ISO_FACE]

The QA module has to analyse and to evaluate all of the quality criteria listed in table 3-2. For the criteria marked with "M", the quality values must be provided while quality values for the criteria marked with "O" may be provided in the defined format according to the respective criteria.

A criterion is fulfilled if its calculated value is in the given threshold boundaries.

Based on the results of all provided quality criteria the QA module rejects or approves the picture. The total result is true if every single quality criteria is fulfilled.

A QA module shall provide an interface for conformance testing where a single image can be processed and the calculated values and configuration data are returned.

ID	*Criterion*	*ISO-Ref.*[6]	*M/O*[7]	*Unit/Range*
		Pose of the head		
1.1	Yaw, neck axis	7.2.2	O	Degrees
1.2	Pitch, ear axis	7.2.2	O	Degrees
1.3	Roll, nose axis	7.2.2	M	Degrees
		Facial expression		
2.1	Neutral expression	7.2.3	O	Arbitrary units
2.2	Mouth closed	7.2.3	M	Arbitrary units
2.3	No raised eyebrows	7.2.3	O	Arbitrary units
		Eyes		
3.1	Eyes open	7.2.3	O	Arbitrary units
3.2	No occlusion (glasses, hair, eye patch)	7.2.11 7.2.12	O	Arbitrary units
3.3	Eyes looking to the camera	7.2.3	O	Arbitrary units
		Background		
4.1	Uniformity (plainness, no textures, colour)	7.2.6 A.2.4.3	O	Arbitrary units
4.2	No shadows	7.2.6 A.2.4.2	O	Arbitrary units
4.3	No further people / objects	7.2.4 A2.3	O	Arbitrary units
		Geometry		
5.1	Image height	8.3.5 A.3.1.1 A.3.2.1	M	In pixel
5.2	Image width	8.3.4 A.3.1.1 A.3.2.1	M	In pixel

6 Compare [ISO_FACE]
7 Mandatory/Optional

ID	*Criterion*	*ISO-Ref.*	*M/O*	*Unit/Range*
5.3	Ratio: Head width / image width	8.3.4	M	As ratio between 0 and 1
5.4	Ratio: Head height / image height	8.3.5	M	As ratio between 0 and 1
5.5	Vertical position of the face	8.3.3	M	As ratio between 0 and 1
5.6	Horizontally centred face	8.3.2	M	As ratio between 0 and 1
5.7	Eye distance	8.4.1 A3.1.1	M	In Pixel
Subject lighting				
6.1	Equally distributed lighting	7.2.7	O	Arbitrary units
6.2	No shadows over the face nor in the eye-sockets	7.2.8 7.2.9	O	Arbitrary units
6.3	No hot spots on skin	7.2.10	O	Arbitrary units
6.4	No effects on glasses	7.2.11	O	Arbitrary units
Image characteristics				
7.1	Proper exposure	7.3.2	M	Arbitrary units
7.2	Focus and depth of field	7.3.3	M	Arbitrary units
7.3	No unnatural colours	7.3.4	O	Arbitrary units
7.4	No red eyes	7.3.4	O	Arbitrary units
7.5	Colour space	7.4.2.3	M	RGB-24bit, YUV422, 8bit-grey scale
7.6	Grey scale density and colour saturation	7.4.2.1 7.4.2.2	M	Counted numbers of intensity values existing within the image
7.7	Compression artefacts		O	Arbitrary units
7.8	Compression level		M	As ratio between 0 and 1

Table 3-2: Mapping of relevant quality criteria

3.6.2 QA-PH-VID

This function block describes quality requirements for a digital live face image that is used for automated face recognition.

Requirements

It is required to use a pre-qualification of captured live face images from the acquisition stream. Images shall be ranked according to the conducted pre-qualification and passed to the verification stage as indicated by the rank.

Pre-qualification shall be conducted at least according to the following criteria:

- Pose of the head,
- illumination of the face
- position of the eyes.

3.7 Compression

The objective of the module Compression is to keep the biometric data below a feasible size without losing too much quality for a biometric verification or identification.

3.7.1 COM-FP-WSQ

This function block describes requirements and interfaces for the compression of fingerprint images that are used for reference storage or identity checks.

Requirements

As compression method for fingerprint images WSQ is used. A bit rate of 0.75 must be used as compression parameter. This is equivalent to a compression factor of approximately 1:15[8] (according to [ISO_FINGER]).

The implementation of the used WSQ algorithm has to be certified by the FBI and has to be referenced by the respective certificate number (coded in the WSQ header).

Within the Compression Module multiple lossy compressions are not allowed.

3.7.2 COM-PH-VID

This function block describes requirements and interfaces for the compression of live images used for face recognition.

Requirements

Depending on the implementation, compression can be used or not. If compression is used, the compression method for facial images shall be either JPEG 2000 (compare [ISO_15444]) or JPEG (compare [ISO_10918-1]). Multiple lossy compressions are not allowed.

The minimal file size according to table 3-3 shall be met.

8 For estimation of compression factor it is allowed to crop to the minimum size containing the fingerprint defined in FM AH-FP-FTR if a sensor is used with a larger capturing area than this minimum.

Compression algorithm	*Minimal file size*
JPEG2000	75 kB[9]
JPEG	75 kB

Table 3-3: Minimal size requirements for compression of live images

For conformance testing the software component encapsulating the compression has to provide an interface that accepts predefined test data instead of performing the regular process.

3.8 Operation

Within the module Operation, the working process is specified for the respective operator. All steps that have to be executed are described sequentially and in more detail. This also includes descriptions of how to proceed in error cases.

3.8.1 O-FP-VID

This function block describes requirements to be observed by the operator who handles the verification process using fingerprint images.

Requirements

Operation of Devices

The following operational requirements shall apply:

– The operator is responsible for an adequate cleanliness of all capture hardware components. Fingerprint scanners have to be cleaned regularly to provide good probe images.

– The fingerprint scanner shall be regularly calibrated (e.g. once a day). The operator shall ensure that the sensor platen is clean before calibration to reduce the risk of ghost images.

Organisational Requirements

The following requirements shall be met to ensure the proper operation of the verification process:

– The official must assure that only one person at the time is entering the e-gate for verification.[10]

Environmental requirements

The following requirements for infrastructure and environment shall be met:

– The operator shall ensure that different environmental lighting conditions caused by direct or indirect sunlight and different seasons of the year shall not influence the scanner capture process.

– Direct and cross irradiation of lighting on the sensor platen shall be avoided completely.

9 1 kB equals 1024 bytes.

10 The operator can be assisted in this requirement by corresponding sensors in the e-gate.

3.8.2 O-PH-VID

This function block describes requirements to be observed by the operator who handles the verification process using facial images.

Requirements

Operation of Devices

The operator is responsible for an adequate cleanliness of all capture hardware components.

Organisational Requirements

The following requirements shall be met to ensure the proper operation of the verification process:

- The official must assure that only one person at the time is entering the e-gate for verification.[11]
- The official should assure that the applicant does not conduct a presentation attack. In conjunction with the information delivered by the PAD function module, the official should be able to decide whether a presentation attack is conducted.[12]

Environmental requirements

The following requirements for infrastructure and environment shall be met:

- As the capturing process shall be independent of external lighting sources, the operator shall ensure that different environmental lighting conditions caused by direct or indirect sunlight and different seasons of the year shall not influence the proper and uniform lighting of the captured face image.
- Direct and cross irradiation of lighting shall be avoided.

11 The operator can be assisted in this requirement by corresponding sensors in the e-gate.
12 This is typically used in conjunction with additional video surveillance.

3.9 User Interface

It is the task of the User Interface to display and visualise the respective information that is obtained from the underlying Function Modules.

3.9.1 UI-FP-VID

This function block describes requirements for the user interface for verification of fingerprint images.

Requirements

Visual feedback of the verification process shall be provided for the operator. At least the (boolean) result of the verification has to be displayed to the operator.

Recommendations

The following recommendations should be met for the user interface in an e-gate:

- a visualization which fingerprint / hand to place on the sensor,
- an indicator showing the capture status should be displayed to the passenger,
- an indication when the capture process has finished or the capture process has to be retried,
- information about the successful or failed verification process should be displayed,
- graphics should avoid multiple colours or harsh contrast.

3.9.2 UI-PH-VID

This function block describes requirements for the user interface for verification of facial images.

Requirements

Visual feedback of the verification process shall be provided for the operator. At least both images (live and reference) and the (boolean) result of the verification have to be displayed to the operator.

Recommendations

The following recommendations should be met for the user interface in an e-gate:

- an indicator showing the capture status should be displayed to the passenger,
- information about the successful or failed verification process should be displayed (e.g. by using green ticks or green frames around the captured live image to mark a successful verification),
- graphics should avoid multiple colours or harsh contrast.

3.10 Biometric Comparison

The module Biometric Comparison encloses the mechanisms and algorithms to verify or identify an identity based on a 1:1 or 1:many biometric comparison between reference data and a current biometric sample (usually a live presented image) regardless of where the reference is stored (e.g. passport, identity card, AFIS, database, ...).

3.10.1 CMP-FP-VID

This function block contains requirements for the verification of an identity in relation to stored reference fingerprint images.

Requirements

Requirements on the algorithm performance

The following requirements shall be met for a fingerprint verification algorithm:

- The fingerprint verification algorithm has to be configured at a security level (threshold) guaranteeing a maximum false match rate (FMR) of 0.1% (1:1000) in conjunction with a false non-match rate (FNMR) less than 2%.
- The threshold shall be configurable to allow for stricter settings when necessary.
- Furthermore, the overall system has to be calibrated for the security level set within this specific scenario of verification. The vendor of the verification algorithm has to provide calibration data based on the actual verification performance.
- The output of the algorithm shall be a comparison score[13] and the result of the verification (the achieved FMR and an indication whether the threshold has been reached) depending on the chosen security level (threshold) of the algorithm.

To ensure validity of proclaimed values, a vendor shall provide test results that support the designated claim. The following requirements apply to those test results:

- The vendor shall provide a DET curve of the algorithm performance,
- such performance shall be on the basis of images of comparable characteristic (e.g. images in size and resolution and pose variation of a typical ePassport deployment).

Requirements on the system performance

The following requirements shall be met for the system performance (including failure to enrol (FTE) and failure to acquire (FTA) rates):

- The false reject rate (FRR) shall be less than 4% at a false accept rate (FAR) of 0.1%.

3.10.2 CMP-PH-VID

This function block contains requirements for the verification of an identity in relation to a stored reference facial image.

13 Typically a vendor-specific uncalibrated raw score.

Requirements

Requirements on the algorithm performance

The following requirements shall be met for a face verification algorithm:

- The face verification algorithm has to be configured at a security level (threshold) guaranteeing a maximum false match rate (FMR) of 0.1% (1:1000) in conjunction with a false non-match rate (FNMR) less than 2%.
- The threshold shall be configurable to allow for stricter settings when necessary.
- Furthermore, the overall system has to be calibrated for the security level set within this specific scenario of verification. The vendor of the verification algorithm has to provide calibration data based on the actual verification performance.
- The output of the algorithm shall be a comparison score[14] and the result of the verification (the achieved FMR and an indication whether the threshold has been reached) depending on the chosen security level (threshold) of the algorithm.

To ensure validity of proclaimed values, a vendor shall provide test results that support the designated claim. The following requirements apply to those test results:

- The vendor shall provide a DET curve of the algorithm performance,
- such performance shall be on the basis of images of comparable characteristic (e.g. images in size and resolution and pose variation of a typical ePassport deployment).

Requirements on the system performance

The following requirements shall be met for the system performance (including failure to enrol (FTE) and failure to acquire (FTA) rates):

- The false reject rate (FRR) shall be less than 4% at an false accept rate (FAR) of 0.1%.

3.11 Logging

The module Logging contains requirements as to which data has to be logged for a specific modality.

3.11.1 LOG-FP-VID

This function block contains requirements for the logging of information regarding the verification process.

Requirements

General requirements

Verification and evaluation work flow independently provide logging data according to the coding requirements of the Coding Function Module.

Within both work flows, the following data shall be collected:

14 Typically a vendor-specific uncalibrated raw score.

- A unique transaction identifier of the current verification process (distinguishable for every verification attempt during the whole border control process)
- A test flag
- A time stamp of the verification process
- Information about the used software (the top layer of the software stack)
- Information about the duration of the whole process.
- Information about the location where the process was conducted.
- Error code[15]

Verification work flow logging data

In addition, the verification work flow shall log the following data:

- Information about all loaded reference fingerprint images (image type and image format)
- Information about the read document (document type and issuing state)
- Demographic data of the document holder (gender, age class and nationality)
- For the capture process:
  - Duration of capture for each captured image that was used as probe afterwards.
  - Information about the used capture software and hardware
- Information about the probe images (size and type)
- For each captured image used for a verification attempt:
  - Duration of the verification
  - Information about the software used for verification
  - Configured threshold of the verification software
  - Result of the genuine comparison (result, score and achieved FMR)

Verification results shall be provided for every candidate image.

Evaluation work flow logging data

In addition, the evaluation work flow shall log the following data:

- A reference to the transaction identifier of the corresponding verification work flow
- Quality analysis results for every candidate and probe image
  - Information about the software used for quality analysis
  - Duration of the quality assurance check
  - Obtained results of the quality check

15 Error codes are not defined in the scope of this guideline. An implementer using this field should inform the consumers of the logging data of the exact semantics of this field.

  - Information of the image source used for quality assurance (live or reference image)
- Cross-comparison results
  - Information about the software used for cross-comparison
  - Duration of the cross-comparison process
  - Configured threshold of the verification software
  - Results and scores obtained from genuine and impostor comparisons.

    Comparison scores shall be calculated for all candidate images.

3.11.2 LOG-PH-VID

This function block contains requirements for the logging of information regarding the verification process.

Requirements

General requirements

Verification and evaluation work flow independently provide logging data according to the coding requirements of the Coding Function Module.

Within both work flows, the following data shall be collected:

- A unique transaction identifier of the current verification process (distinguishable for every verification attempt during the whole border control process)
- A test flag
- A time stamp of the verification process
- Information about the used software (the top layer of the software stack)
- Information about the duration of the whole process.
- Information about the location where the process was conducted.
- Error code[16]

Verification work flow logging data

In addition, the verification work flow shall log the following data:

- Information about the loaded reference image (image type and image format)
- Information about the read document (document type and issuing state)
- Demographic data of the document holder (gender, age class and nationality)
- For the capture process:
  - Duration of capture for each captured image that was used as probe afterwards.
  - Information about the used capture software and hardware

16 Error codes are not defined in the scope of this guideline. An implementer using this field should inform the consumers of the logging data of the exact semantics of this field.

- Information about the probe images (size and type)
- For each captured image used for a verification attempt:
  - Duration of the verification
  - Information about the software used for verification
  - Configured threshold of the verification software
  - Result of the genuine comparison (result, score and achieved FMR)

Evaluation work flow logging data

In addition, the evaluation work flow shall log the following data:

- A reference to the transaction identifier of the corresponding verification work flow
- Quality analysis results
  - Information about the software used for quality analysis
  - Duration of the quality assurance check
  - Obtained results of the quality check
  - Information of the image source used for quality assurance (live or reference image)
- Cross-comparison results
  - Information about the software used for cross-comparison
  - Duration of the cross-comparison process
  - Configured threshold of the verification software
  - Results and scores obtained from genuine and impostor comparisons

3.12 Coding

This module contains the procedures to encode quality data as well as biometric data in defined formats. Interoperability is provided by means of standard compliant coding.

3.12.1 COD-FP-VID

This function block describes requirements for the coding used during the verification process of fingerprint images.

Requirements

The result data of the verification process is collected from different components. The verification and the evaluation work flow return separate logging data:

- All results of the verification work flow are encoded in XML as „fp-vid-verify“.
- All results of the evaluation work flow are encoded in XML as „fp-vid-eval“.

The XML encoding is defined by the XML schema definition in „fp-vid.xsd“. Examples can be found in „fp-vid-verify.xml“ and „fp-vid-eval.xml“.

3.12.2 COD-PH-VID

This function block describes requirements for the coding used during the verification process of facial images.

Requirements

The result data of the verification process is collected from different components. The verification and the evaluation work flow return separate logging data:

- All results of the verification work flow are encoded in XML as „ph-vid-verify“.
- All results of the evaluation work flow are encoded in XML as „ph-vid-eval“.

The XML encoding is defined by the XML schema definition in „ph-vid.xsd“. Examples can be found in „ph-vid-verify.xml“ and „ph-vid-eval.xml“.

3.13 Evaluation

Methods and interfaces which are used in the scope of evaluation are the content of this Function Module.

3.13.1 EVA-FP-VID

This function block contains requirements for the evaluation of information regarding the verification process of fingerprint images.

Requirements

Evaluations can be performed based on logging data that is collected in the verification and the evaluation work flow.

Filtering of the defined evaluations shall be possible with regard to a selected time frame (e.g. only verifications from year 2009) and/or the issuing state of the ePassport or identity card (e.g. only verifications of German passports).

Biometric performance

EVA-FP-VID.1: Detection error trade-off (DET) curve
All results of the cross comparison conducted within the evaluation work flow may be used for generating False Accept Rates (FAR) and False Reject Rates (FRR). Due to the fact of multiple possible verifications within the whole verification process not all live images shall be used for calculating error rates. The FAR and FRR shall be calculated by using the best result within in the complete verification process. As, typically, multiple candidate images are available as reference, only the verification with the highest verification result score shall be considered as a possible genuine verification for determining the DET curve. Other comparison results shall not be used (also not as imposter scores).

Table 3-4: Evaluation EVA-FP-VID.1

EVA-FP-VID.2: Influence of image quality on biometric performance
All results of the quality assurance and cross comparison conducted within the evaluation work flow may be used for generating False Accept Rates (FAR) and False Reject Rates (FRR). Two different sets of images shall be generated. Set one consists of images with good quality (“easy set”), set two consists of images of bad quality (the other images, “difficult set”). Afterwards, the biometric performance is calculated for both sets.[17]

Table 3-5: Evaluation EVA-FP-VID.2

17 Other partitions are possible.

Error code evaluations

EVA-FP-VID.3: Error reasons from the local acquisition process
This evaluation shows the percentage of all error codes that have occurred during the local acquisition process and have been encoded and logged.

Table 3-6: Evaluation EVA-FP-VID.3

Quality evaluations

EVA-FP-VID.4: Distribution of quality values
All results of the performed quality assurance shall be used to show a distribution of all available criterion and quality factors.

Table 3-7: Evaluation EVA-FP-VID.4

Timing evaluations

EVA-FP-VID.5: Average capture and verification process duration
The evaluation shows the average time in seconds needed to verify a holder of an identity document. It shall evaluate capture, verification and total duration.

Table 3-8: Evaluation EVA-FP-VID.5

EVA-FP-VID.6: Distribution of verification attempts per transaction
The evaluation shows the distribution of verification attempts needed to pass the border control successfully or until the exit condition is reached.

Table 3-9: Evaluation EVA-FP-VID.6

EVA-FP-VID.7: Cumulative representation of verification duration
The evaluation shows a cumulative representation of verification transactions that were completed within a given time frame of at least 15 seconds. Cumulative values should be calculated in an interval of one second.

Table 3-10: Evaluation EVA-FP-VID.7

EVA-FP-VID.8: Developments of average verification duration over time
The evaluation shall display developments of the average verification duration over time. For every month, the average verification duration shall be obtained from logged information.[18]

Table 3-11: Evaluation EVA-FP-VID.8

18 This information should also be evaluated specifically to certain locations.

Issuing states evaluations

EVA-FP-VID.9: Distribution of issuing states
The evaluation shows the distribution of all issuing states occurred during verification of ePassports and identity cards.

Table 3-12: Evaluation EVA-FP-VID.9

Demographic data evaluations

EVA-FP-VID.10: Distribution of gender
The evaluation shows the percentage of male, female and unknown gender.

Table 3-13: Evaluation EVA-FP-VID.10

EVA-FP-VID.11: Distribution of age group
The evaluation shows the percentage of all age groups that have occurred within the verification process.

Table 3-14: Evaluation EVA-FP-VID.11

3.13.2 EVA-PH-VID

This function block contains requirements for the evaluation of information regarding the verification process of facial images.

Requirements

Evaluations can be performed based on logging data that is collected in the verification and the evaluation work flow.

Filtering of the defined evaluations shall be possible with regard to a selected time frame (e.g. only verifications from year 2009) and/or the issuing state of the ePassport or identity card (e.g. only verifications of German passports).

Biometric performance

EVA-PH-VID.1: Detection error trade-off (DET) curve
All results of the cross comparison conducted within the evaluation work flow may be used for generating False Accept Rates (FAR) and False Reject Rates (FRR). Due to the fact of multiple possible verifications within the whole verification process not all live images shall be used for calculating error rates. The FAR and FRR shall be calculated by using the best result within in the complete verification process.

Table 3-15: Evaluation EVA-PH-VID.1

EVA-PH-VID.2: Influence of image quality on biometric performance

All results of the quality assurance and cross comparison conducted within the evaluation work flow may be used for generating False Accept Rates (FAR) and False Reject Rates (FRR). Two different sets of images shall be generated. Set one consists of images with good quality ("easy set"), set two consists of images of bad quality (the other images, "difficult set"). Afterwards, the biometric performance is calculated for both sets.[19]

Table 3-16: Evaluation EVA-PH-VID.2

Error code evaluations

EVA-PH-VID.3: Error reasons from the local acquisition process
This evaluation shows the percentage of all error codes that have occurred during the local acquisition process and have been encoded and logged.

Table 3-17: Evaluation EVA-PH-VID.3

Quality evaluations

EVA-PH-VID.4: Distribution of quality values
All results of the performed quality assurance shall be used to show a distribution of all available criterion and quality factors.

Table 3-18: Evaluation EVA-PH-VID.4

Timing evaluations

EVA-PH-VID.5: Average capture and verification process duration
The evaluation shows the average time in seconds needed to verify a holder of an identity document. It shall evaluate capture, verification and total duration.

Table 3-19: Evaluation EVA-PH-VID.5

EVA-PH-VID.6: Distribution of verification attempts per transaction
The evaluation shows the distribution of verification attempts needed to pass the border control successfully or until the exit condition is reached.

Table 3-20: Evaluation EVA-PH-VID.6

EVA-PH-VID.7: Cumulative representation of verification duration
The evaluation shows a cumulative representation of verification transactions that were completed within a given time frame of at least 15 seconds. Cumulative values should be calculated in an interval of one second.

19 Other partitions are possible.

Table 3-21: Evaluation EVA-PH-VID.7

EVA-PH-VID.8: Developments of average verification duration over time
The evaluation shall display developments of the average verification duration over time. For every month, the average verification duration shall be obtained from logged information.[20]

Table 3-22: Evaluation EVA-PH-VID.8

Issuing states evaluations

EVA-PH-VID.9: Distribution of issuing states
The evaluation shows the distribution of all issuing states occurred during verification of ePassports and identity cards.

Table 3-23: Evaluation EVA-PH-VID.9

Demographic data evaluations

EVA-PH-VID.10: Distribution of gender
The evaluation shows the percentage of male, female and unknown gender.

Table 3-24: Evaluation EVA-PH-VID.10

EVA-PH-VID.11: Distribution of age group
The evaluation shows the percentage of all age groups that have occurred within the verification process.

Table 3-25: Evaluation EVA-PH-VID.11

20 This information should also be evaluated specifically to certain locations.

4 Changelog of XML schemata

This chapters lists the main changes in TR-03121 XML schemata between different versions.

4.1 Changes from version 3.0 to 3.0.1

- All schemata
  - Use new type type.trbio.schema.version.values to enumerate all valid schema version numbers
  - Use xs:appinfo/sinceSchemaVersion to indicate the earliest version this element is available
- fp_visa.xsd
  - new optional element ErrorCode in type.function.module.fp.verification
  - new optional element ErrorCode in type.function.module.fp.identification
- types.xsd
  - new type for type.trbio.schema.version.values
  - new type.external.key
  - add elements for external keys to type.transaction
  - Duration is now optional in type.comparison
  - qa is now optional in type.qa.results
  - attribute total is now optional in type.qa.results
  - new optional element Duration in type.fingerprint.quality.results
  - new optional element ErrorCode in type.fingerprint.quality.results
  - new optional element ErrorCode in type.uniqueness.check
  - new optional element ErrorCode in type.cross.comparison
  - change type.uniqueness.check/@result to optional for coding undetermined results
  - change restriction of type.age.class to a pattern based approach to allow for more flexible coding of age classes
- trbio.xsd
  - version is now 2
    Note: If you use elements that are only present in version 2, your document must indicate this in the schemaVersion root attribute.

5 List of abbreviations

Abbreviation	*Description*
ACQ	Acquisition
AD	Acquisition Device
AFIS	Automated Fingerprint Identification System
AH	Acquisition Hardware
ANSI	American National Standards Institute
AP	Application Profile
APP	Application
AS	Acquisition Software
BEA	Biometric Evaluation Authority
BioAPI	Biometric Application Programming Interface
BioSFPI	Biometric Sensor Function Provider Interface
BioSPI	BioAPI Service Provider Interface
BIP	Biometric Image Processing
BMS	Biometric Matching System
BMP	Windows Bitmap version 3
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
BFP	Biometric Function Provider
BSFP	Biometric Sensor Function Provider
BSP	Biometric Service Provider
CMP	Biometric Comparison
COD	Coding

COM	Compression
CRM	Cross-matching
CTS	Conformance test suite
DC	Digital camera
DET	Detection error trade-off
eID	Electronic identity document
ePass	Electronic passport
EU	European Union
EVA	Evaluation
FAR	False accept rate
FBS	Flat bed scanner
FM	Function Module
FMR	False match rate
FNMR	False non-match rate
FP	Fingerprint
FRR	False reject rate
FTR	Frustrated total reflection
GID	German Identity Document
ICAO	International Civil Aviation Organization
ID	Identity
JPG	JPEG
JP2	JPEG 2000
LOG	Logging
MF	Multi finger

NCA	National Central Authority
NIST	National Institute of Standards and Technology
O	Operation
P	Process
PG	Photo Guideline ("Fotomustertafel”)
PH	Photo
PT	Photo Template ("Lichtbildschablone”)
QA	Quality Assurance
REF	Reference Storage
SB	Software based
SDK	Software Development Kit
SF	Single finger
TC	Test Case
TR	Technische Richtlinie (Technical Guideline)
UI	User Interface
VAPP	Visa Application
VBIC	Visa Basic Identity Check
VEIC	Visa Extended Identity Check
VIC	Visa Identity Check
VID	Verification Identity Document
VIS	Visa Information System
WSQ	Wavelet Scalar Quantisation
WSQR	Wavelet Scalar Quantisation for reference storage

6 Bibliography

[ANSI_NIST] ANSI/NIST-ITL 1-2000, American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information, available at: http://www.itl.nist.gov/ANSIASD/sp500-245-a16.pdf

[CBEFF] ISO/IEC 19785-1:2006 "Information technology - Common Biometric Exchange Formats Framework - Part 1: Data element specification"

[EAC] Technical Guideline BSI TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents, Version 2.10, 2012

[EBTS/F] FBI Electronic Biometric Transmission Specification Version 8, Appendix F, September 2007.

[EC_767_2008] 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)

[EC_296_2008] Regulation (EC) No 296/2008 of the European Parliament and of the Council of 11 March 2008 amending Regulation (EC) No 562/2006 establishing a Community Code on the rules governing the movement of persons across borders (Schengen Borders Code), as regards the implementing powers conferred on the Commission

[EC_2252/2004] Regulation (EC) No 2252/2004 of the European Parliament and of the Council of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

[EC_648_2006] Commission Decision of 22 September 2006 laying down the technical specifications on the standards for biometric features related to the development of the Visa Information System

[ICAO_06] ICAO Document 9303, Machine Readable Travel Documents, Part 1 – Machine Readable Passports, 6th edition, 2006

[ICAO_08] ICAO Document 9303, Machine Readable Travel Documents, Part 3 – Size 1 and Size 2 Machine Readable Official Travel Documents, 3rd edition, 2008

[ISO_19784-1] ISO/IEC 19784-1:2006 “Information technology – Biometric application programming interface – Part 1: BioAPI specification”

[ISO_19784-4] ISO/IEC 19784-4:2011: “Information technology – Biometric application programming interface – Part 4: Biometric sensor function provider interface”

[ISO_FACE] ISO/IEC 19794-5:2005 “Information technology - Biometric data interchange formats - Part 5: Face image data”

[ISO_FINGER] ISO/IEC 19794-4:2005 “Information technology - Biometric data interchange formats - Part 4: Finger image data”

[ISO_10918-1]	ISO/IEC 10918-1:1994: “Information technology – Digital compression and coding of continuous-tone still images: Requirements and guidelines”
[ISO_15444]	ISO/IEC 15444-1:2004 “Information technology - JPEG 2000 image coding system: Core coding system”
[ISO_19785-3]	ISO/IEC 19785-3:2007 “Information technology – Common Biometric Exchange Formats Framework – Part 3: Patron format specification”
[ISO_24709-1]	ISO/IEC 24709-1: 2007 “Information technology – Conformance testing for the biometric application programming interface (BioAPI) – Part 1: Methods and procedures”
[ISO_24709-2]	ISO/IEC 24709-2: 2007 “Information technology – Conformance testing for the biometric application programming interface (BioAPI) – Part 2: Test assertions for biometric service providers”
[NBIS]	http://fingerprint.nist.gov/NBIS/index.html
[NFIS]	http://fingerprint.nist.gov/NFIS/index.html
[PhotoGuide]	Photo guideline ("Fotomustertafel")
[RFC2119]	RFC 2119: Key words for use in RFCs to Indicate Requirement Levels.
[Template]	Photo template ("Lichtbildschablone")
[VIS-ANSI_NIST]	VIS-ANSI/NIST, European Commission Directorate-General Justice, Freedom and Security – Visa Information System – NIST Description, Version 1.23, 2009