Federal Office
for Information Security

BSI Technical Guideline TR-03121-3

Biometrics for Public Sector Applications

Part 3: Application Profiles, Function Modules and Processes

Volume 1: Border Control (BCL)

Version 6.0

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn
E-Mail: trbiometrics@bsi.bund.de
Internet: https://bsi.bund.de

Table of Contents

List of Figures

1. Volume Border Control

BSI TR-03121, Volume 1 Border Control (BCL), covers the biometric processes of border control. Thereby, enrolment of the biometric subject's biometric characteristics as well as identification and verification of biometric subjects' identities with the help of biometric characteristics are subprocesses of the general border control processes. Biometric characteristics used in border control processes are facial images (FIs) and plain fingerprints (FPs).

2. Application Profiles

The following sections specify the Application Profiles of this Volume. The processes specified by the Application Profiles of this Volume support a number of border control configurations.

2.1. Application Profile Manual Border Control

This Application Profile specifies the requirements for Manual Border Control (MBC) systems equipped with a facial image acquisition system and a fingerprint acquisition system.

2.1.1. Mandatory Process

The following subsections specify the overall process of the biometric operations of the MBC and the biometric border control checks required per border control use case at the MBC.

2.1.1.1. Overview Process

Figure 2.1 depicts the general biometric process of the MBC. The ad hoc process depicted is for illustration purpose only.

At the MBC the border guard assesses alphanumeric and biometric candidate lists. In case true matches are identified, the border guard takes the necessary actions such as guiding the traveller to the second line or linking existing records. The border guard acquires missing biometric modalities or assesses the biometric modalities acquired unsupervised at a downstream system. In addition, the border guard assesses biometric verification results.

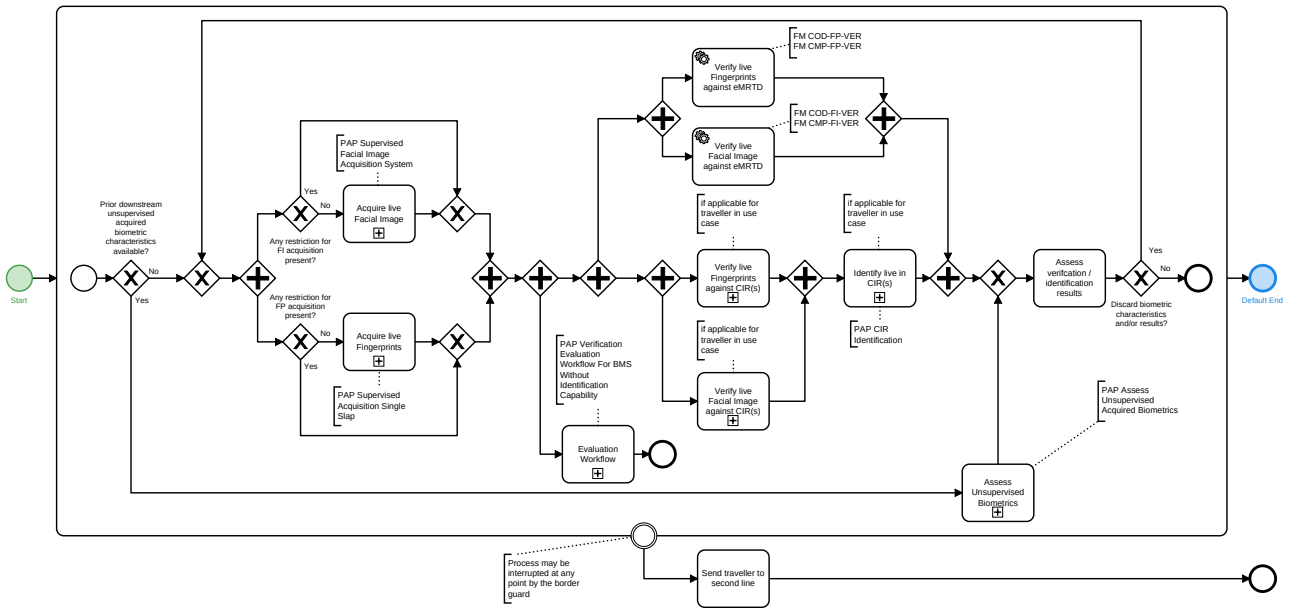

Figure 2.1. Overview Process Manual Border Control

2.1.2. Mandatory Function Modules

All Function Modules which SHALL be applied for this Application Profile are listed in Table 2.1. All listed Function Modules (separated by commas) are mandatory for this Application Profile unless specified other-

wise. Function Modules separated by slash are alternatives to each other. Function Modules in brackets are RECOMMENDED.

Module Category	Required Function Modules
Acquisition Hardware	▸FM AH-FP-OPT
Acquisition Software	▸FM AS-FP-MF, ▸FM AS-FP-SLP
Biometric Image Processing	▸FM BIP-FP-APP
Quality Assessment	▸FM QA-FP-APP
Presentation Attack Detection	▸FM PAD-FP-APP1
Compression	▸FM COM-FI-GENERIC, ▸FM COM-FI-BCL, ▸FM COM-FP-WSQ, ▸FM COM-FP-BCL
Operation	▸FM O-ALL-LNK
User Interface	▸FM UI-FI-OP, ▸FM UI-FP-OP
Reference Storage	▸FM REF-FP-EES, ▸FM REF-FI-EES
Biometric Comparison	▸FM CMP-FI-VER, ▸FM CMP-FP-VER
Logging	▸FM LOG-ALL-GENERIC, ▸FM LOG-ALL-BCL, ▸FM LOG-FI-GENERIC, ▸FM LOG-FP-GENERIC
Coding	▸FM COD-ALL-BCL, ▸FM COD-FI-VER (for FI verification logging), ▸FM COD-FI-EES (for FI data to CS EES), ▸FM COD-FP-EES (for FP data to CS EES), ▸FM COD-FP-VER
Evaluation	-

Table 2.1 Required Function Modules Application Profile Manual Border Control

2.1.3. Mandatory Application Profiles

For the acquisition of facial images, the ▸Application Profile Facial Image Acquisition System Manual Border Control SHALL be applied by this Application Profile.

2.1.4. Mandatory Partial Application Processes

All Partial Application Processes and Tasks which SHALL be applied for this Application Profile are listed in ▸Table 2.2. All listed Processes (separated by commas) are mandatory for this Application Profile unless specified otherwise. Processes separated by slash are alternatives to each other.

No.	Required Partial Application Process
1	▸PAP ASS-B-USV-1: Assess Unsupervised Acquired Biometrics
2	▸PAP ID-1: CIR Identification
3	▸PAP EVA-VER-nCIR-1: Verification Evaluation Workflow for BMS without Identification Capability
4	▸PAP ACQ-FPS-SV-1: Supervised Acquisition Single Slap

Table 2.2 Required Partial Application Processes Application Profile Manual Border Control

2.2. Application Profile Facial Image Acquisition System Manual Border Control

This Application Profile specifies a facial image acquisition system for manual border control booths. The facial image acquisition system is used to automatically acquire or manually capture facial images for enrolment, verification or identification purposes.

2.2.1. Mandatory Process

The following subsection specifies the overall process of the biometric operations of a facial image acquisition system used at the MBC.

2.2.1.1. Overview Process

▸Figure 2.2 depicts the general biometric process of the facial image acquisition system. Note, that ▸PAP ACQ-FI-SV-5: Supervised Facial Image Acquisition System is used here.

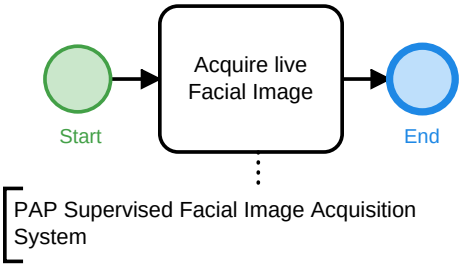

Figure 2.2. Overview Process Facial Image Acquisition System at MBC Border Crossing

2.2.2. Mandatory Function Modules

All Function Modules which SHALL be applied for this Application Profile are listed in ▸Table 2.3. All listed Function Modules (separated by commas) are mandatory for this Application Profile unless specified otherwise. Function Modules separated by slash are alternatives to each other. Function Modules in brackets are RECOMMENDED.

Module Category	Required Function Modules
Acquisition Hardware	▸FM AH-FI-ICS, ▸FM AH-FI-BCL
Acquisition Software	▸FM AS-FI-ICS, ▸FM AS-FI-ICS3
Biometric Image Processing	▸FM BIP-FI-APP
Quality Assessment	▸FM QA-FI-PRE, ▸FM QA-FI-GENERIC, ▸FM QA-FI-BCL
Presentation Attack Detection	-
Compression	▸FM COM-FI-GENERIC, ▸FM COM-FI-BCL
Operation	▸FM O-ALL-USV, ▸FM O-FI-ALL, ▸FM O-FI-DC
User Interface	▸FM UI-FI-BSJ
Reference Storage	-
Biometric Comparison	-
Logging	▸FM LOG-ALL-BCL, ▸FM LOG-FI-GENERIC
Coding	▸FM COD-ALL-EES, ▸FM COD-FI-GENERIC
Evaluation	-

Table 2.3 Required Function Modules Application Profile Facial Image Acquisition Manual Border Control

2.2.3. Mandatory Partial Application Processes

All Partial Application Processes and Tasks which SHALL be applied for this Application Profile are listed in ▸Table 2.4. All listed Processes (separated by commas) are mandatory for this Application Profile unless specified otherwise. Processes separated by slash are alternatives to each other.

No.	Required Partial Application Process
1	▸PAP ACQ-FI-SV-5: Supervised Facial Image Acquisition System
2	▸PAP ACQ-FI-AUTO-1: Automated Facial Image Acquisition

Table 2.4 Required Partial Application Processes Application Profile Facial Image Acquisition Manual Border Control

2.3. Application Profile Mobile Manual Border Control

This Application Profile specifies the requirements for a mobile manual border control with handheld devices. It will be amended in a future version of this Technical Guideline (TR).

2.4. Application Profile Semi-Mobile Manual Border Control

This Application Profile specifies the requirements for semi-mobile MBC systems equipped with a facial image camera and a fingerprint acquisition system.

2.4.1. Mandatory Process

▸Figure 2.3 depicts the acquisition process at the semi-mobile manual border control. Semi-mobile equipment is meant to be portable (e.g. placed within in a suit-case), but is not hand-held.

In general, the biometric data of the biometric subject SHALL be captured sequentially. Depending on the use case it is required to acquire fingerprints and / or a facial image of the biometric subject. For all acquisitions enrolment quality SHALL be used in order to simplify the over all processes (e.g. a facial image that has been used for a verification is not needed to be recaptured for an enrolment).

In the end the acquired biometrics are used for enrolment, verifications and / or identifications within one or multiple Central Indentity Registers (CIRs).

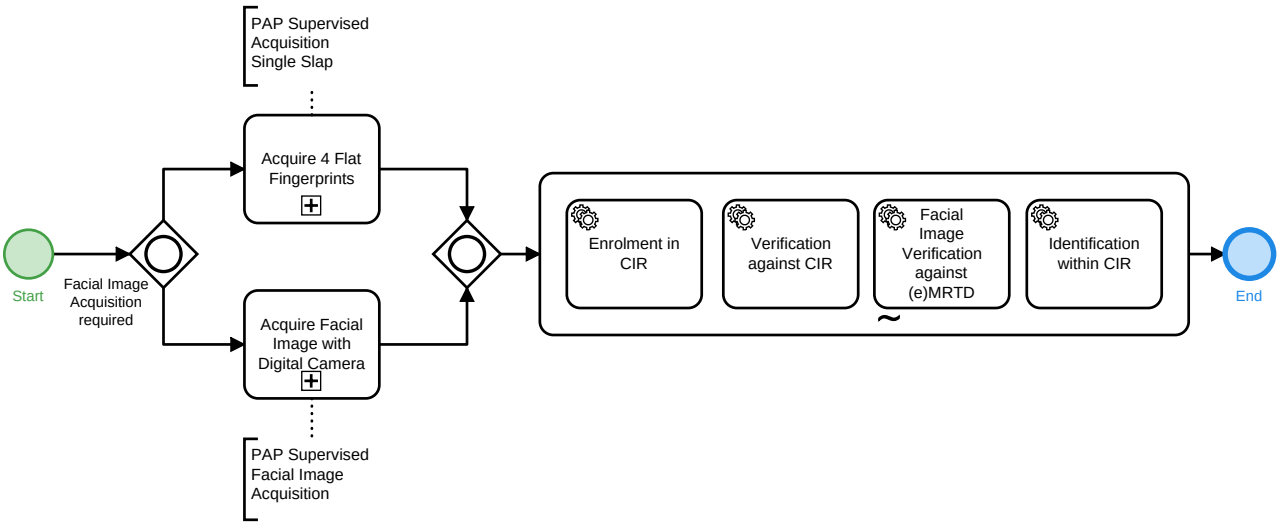

Figure 2.3. Overview Process at Semi-Mobile Manual Border Control

2.4.2. Mandatory Function Modules

All Function Modules which SHALL be applied for this Application Profile are listed in ▸Table 2.5. All listed Function Modules (separated by commas) are mandatory for this Application Profile unless specified otherwise. Function Modules separated by slash are alternatives to each other. Function Modules in brackets are RECOMMENDED.

Module Category	Required Function Modules
Acquisition Hardware	▸FM AH-FI-DC, ▸FM AH-FP-OPT
Acquisition Software	▸FM AS-FI-DC, ▸FM AS-FP-MF, ▸FM AS-FP-SLP
Biometric Image Processing	▸FM BIP-FI-APP, ▸FM BIP-FP-APP
Quality Assessment	▸FM QA-FI-GENERIC, ▸FM QA-FI-BCL, ▸FM QA-FP-APP
Presentation Attack Detection	▸FM PAD-FP-APP1
Coding	▸FM COD-ALL-BCL, ▸FM COD-ALL-EES, ▸FM COD-FI-GENERIC, ▸FM COD-FI-EES, ▸FM COD-FP-EES
Compression	▸FM COM-FI-GENERIC, ▸FM COM-FI-BCL, ▸FM COM-FP-BCL, ▸FM COM-FP-WSQ
Operation	▸FM O-FI-ALL, ▸FM O-FI-DC, ▸FM O-FP-ALL
User Interface	▸FM UI-FI-OP, ▸FM UI-FP-OP
Reference Storage	-
Biometric Comparison	-
Logging	▸FM LOG-ALL-GENERIC, ▸FM LOG-ALL-BCL, ▸FM LOG-FI-GENERIC, ▸FM LOG-FP-GENERIC
Evaluation	-

Table 2.5 Required Function Modules Application Profile Semi-Mobile Manual Border Control

2.4.3. Mandatory Partial Application Processes

All Partial Application Processes and Tasks which SHALL be applied for this Application Profile are listed in ▸Table 2.6. All listed Processes (separated by commas) are mandatory for this Application Profile unless specified otherwise. Processes separated by slash are alternatives to each other.

No.	Required Partial Application Process
1	▸PAP ACQ-FI-SV-4: Supervised Facial Image Acquisition
2	▸PAP ACQ-FPS-SV-1: Supervised Acquisition Single Slap

Table 2.6 Required Partial Application Processes Application Profile Semi-Mobile Manual Border Control

2.5. Application Profile Automated Border Control (Face-Verification Only)

This Application Profile specifies the requirements for integrated two-step man trap Automated Border Control (ABC) (Face-Verification Only) which are equipped with a facial image acquisition system inside the man trap and a document reader at the entrance of the system.

2.5.1. Mandatory Process

The following subsections specify the overall process of biometric operations of the ABC (Face-Verification Only) and the biometric border control checks required per border control use case at the ABC (Face-Verification Only).

Note, this is an one modality system with a facial image camera for face verification with Presentation Attack Detection (PAD) only. The acquired images in this system do not have enrolment quality.

2.5.1.1. Overview Process

Figure 2.4 depicts the general biometric process of the ABC (Face-Verification Only).

If the candidate's facial image is not available or an PAD alarm is triggered, the situation MUST be checked by a border guard.

Also, if any verification fails, the situation MUST be checked by a border guard.

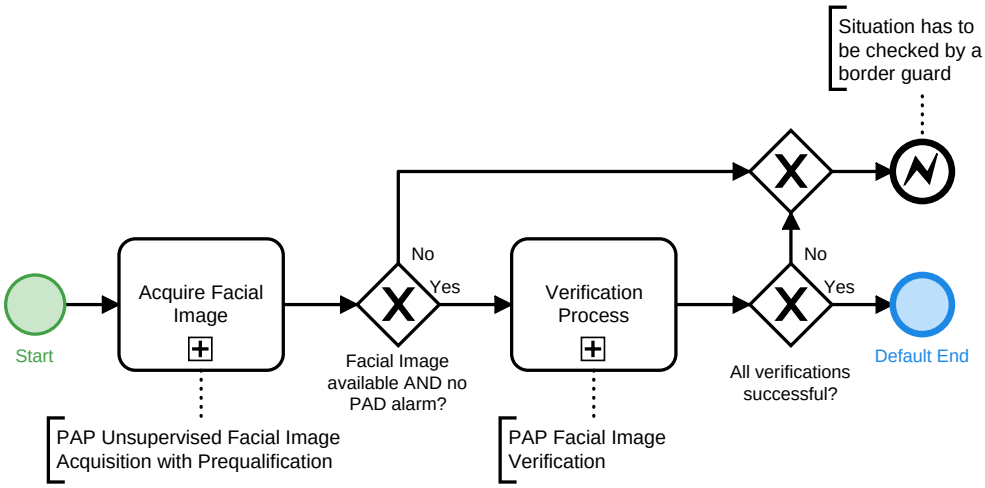

Figure 2.4. Overview Process ABC (Face-Verification Only) Border Crossing

2.5.2. Mandatory Function Modules

All Function Modules which SHALL be applied for this Application Profile are listed in Table 2.7. All listed Function Modules (separated by commas) are mandatory for this Application Profile unless specified otherwise. Function Modules separated by slash are alternatives to each other. Function Modules in brackets are RECOMMENDED.

Module Category	Required Function Modules
Acquisition Hardware	FM AH-FI-EGT, FM AH-FI-ICS
Acquisition Software	FM AS-FI-ICS
Biometric Image Processing	FM BIP-FI-APP
Quality Assessment	FM QA-FI-PRE
Presentation Attack Detection	FM PAD-FI-APP
Compression	FM COM-FI-GENERIC, FM COM-FI-BCL
Operation	FM O-ALL-USV, FM O-FI-DC
User Interface	FM UI-FI-OP, FM UI-FI-BSJ
Reference Storage	-
Biometric Comparison	FM CMP-FI-VER
Logging	FM LOG-ALL-GENERIC, FM LOG-ALL-BCL, FM LOG-FI-GENERIC
Coding	FM COD-ALL-BCL, FM COD-FI-GENERIC, FM COD-FI-VER (for FI verification logging), FM COD-FI-EES (for FI data to Central System EES (CS EES))

Module Category	Required Function Modules
Evaluation	-

Table 2.7 Required Function Modules Application Profile Automated Border Control

2.5.3. Mandatory Partial Application Processes

All Partial Application Processes and Tasks which SHALL be applied for this Application Profile are listed in ▸Table 2.8. All listed Processes (separated by commas) are mandatory for this Application Profile unless specified otherwise. Processes separated by slash are alternatives to each other.

No.	Required Partial Application Process
1	▸PAP ACQ-FI-USV-1: Unsupervised Facial Image Acquisition with Prequalification
2	▸PAP VER-FI-ALL-1: Facial Image Verification
3	▸PAP EVA-VER-nCIR-1: Verification Evaluation Workflow for BMS without Identification Capability

Table 2.8 Required Partial Application Processes Application Profile Automated Border Control

2.6. Application Profile Self-Service System

This Application Profile specifies the requirements for self-service systems (SSSs) equipped with a facial image acquisition system, a fingerprint acquisition system and a document reader.

2.6.1. Mandatory Process

The following subsections specify the overall process of the biometric operations of the SSS and the biometric border control checks required per border control use case at the SSS.

2.6.1.1. Overview Process

▸Figure 2.5 depicts the general biometric process of the SSS.

A live facial image of the biometric subject is acquired. In some of the use cases the acquisition of the fingerprints is started in parallel. In case an applicable biometric modality could not be acquired from the biometric subject, the following process steps requiring this modality are skipped and the next border control step is the MBC.

Afterwards, the verification of the live facial image is carried out against the reference facial image on the Electronic Machine Readable Travel Document (eMRTD) and the evaluation workflow is started. In some use cases fingerprint verifications against CIRs (e.g. CS EES or Visa Information System (VIS)) are performed in parallel. If the verification against a CIR failed, an identification is performed within the same system which SHALL be multimodal if possible. The retrieval of the identification results SHALL never block the release message to the biometric subject to proceed to the next border control system.

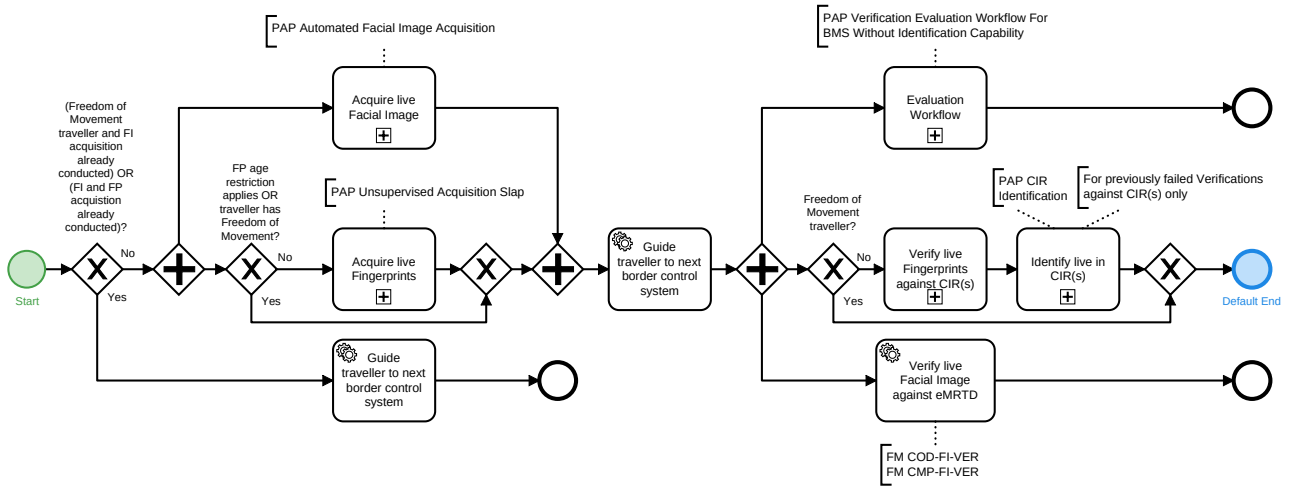

Figure 2.5. Overview Process Self-Service System Usage

2.6.2. Mandatory Function Modules

All Function Modules which SHALL be applied for this Application Profile are listed in ▸Table 2.9. All listed Function Modules (separated by commas) are mandatory for this Application Profile unless specified otherwise. Function Modules separated by slash are alternatives to each other. Function Modules in brackets are RECOMMENDED.

Module Category	Required Function Modules
Acquisition Hardware	▸FM AH-ALL-SSS, ▸FM AH-FI-ICS, ▸FM AH-FI-BCL, ▸FM AH-FI-SSS, ▸FM AH-FP-OPT, ▸FM AH-FP-SSS
Acquisition Software	▸FM AS-FI-ICS, ▸FM AS-FI-ICS3, ▸FM AS-FP-MF, ▸FM AS-FP-SLP
Biometric Image Processing	▸FM BIP-FI-APP, ▸FM BIP-FP-APP
Quality Assessment	▸FM QA-FI-GENERIC, ▸FM QA-FI-BCL, ▸FM QA-FP-APP
Presentation Attack Detection	▸FM PAD-FI-APP, ▸FM PAD-FP-APP1
Compression	▸FM COM-FI-GENERIC, ▸FM COM-FI-BCL, ▸FM COM-FP-WSQ, ▸FM COM-FP-BCL, ▸FM COM-CCTV-JPG
Operation	▸FM O-ALL-USV, ▸FM O-FI-ALL, ▸FM O-FI-DC, ▸FM O-FP-ALL
User Interface	▸FM UI-FI-BSJ, ▸FM UI-FP-BSJ
Reference Storage	-
Biometric Comparison	▸FM CMP-FI-VER, ▸FM CMP-FP-VER
Logging	▸FM LOG-ALL-GENERIC, ▸FM LOG-ALL-BCL, ▸FM LOG-FI-GENERIC, ▸FM LOG-FP-GENERIC
Coding	▸FM COD-ALL-BCL, ▸FM COD-FI-VER (for FI verification logging), ▸FM COD-FI-EES (for FI data to CS EES), ▸FM COD-FP-EES (for FP data to CS EES)
Evaluation	-

Table 2.9 Required Function Modules Application Profile Self-Service System

2.6.3. Mandatory Partial Application Processes

All Partial Application Processes and Tasks which SHALL be applied for this Application Profile are listed in ▸Table 2.10. All listed Processes (separated by commas) are mandatory for this Application Profile unless specified otherwise. Processes separated by slash are alternatives to each other.

No.	Required Partial Application Process
1	▸PAP ACQ-FPS-USV-1: Unsupervised Acquisition Slap
2	▸PAP ACQ-FI-AUTO-1: Automated Facial Image Acquisition
3	▸PAP ID-1: CIR Identification
4	▸PAP EVA-VER-nCIR-1: Verification Evaluation Workflow for BMS without Identification Capability

Table 2.10 Required Partial Application Processes Application Profile Self-Service System

2.7. Application Profile Biometric Matching Systems

This Application Profile specifies requirements for a Biometric Matching System (BMS).

2.7.1. Mandatory Process

The following subsections specify the overall process of the BMS as well as different evaluation workflows.

2.7.1.1. Overview Process

▸Figure 2.6 depicts the overall BMS process.

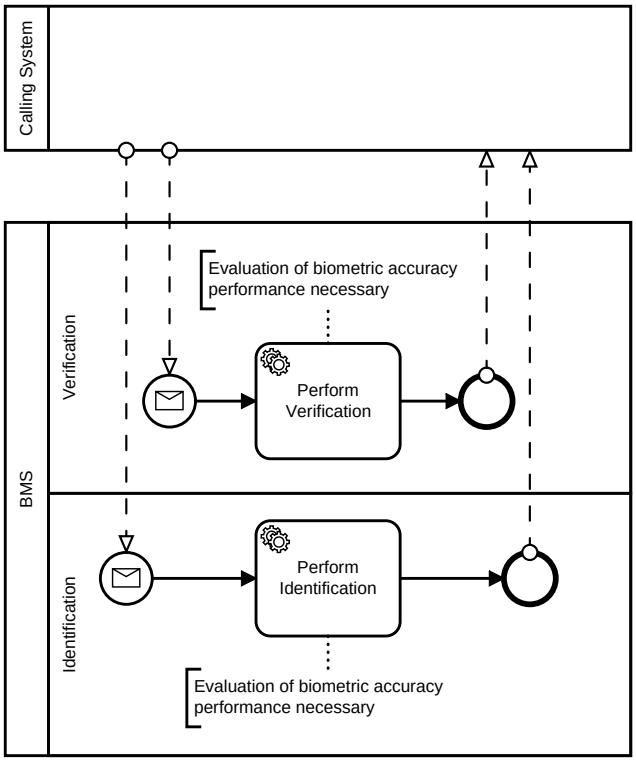

Figure 2.6. Overall BMS Process

2.7.1.2. Evaluation Worflows

The outcome of a biometric verification (match vs. non-match) [1] or identification (candidate list) is only reliable if the corresponding error rates are quantified and monitored. In order to enable a competent authority to evaluate false and true match rates and to configure the BMS comparison thresholds, the Application Profile specifies evaluation workflows which SHALL be executed in parallel for requests received by the BMS or made available to the BMS, unless the main working processes would be impaired in times of high load.

Note, the specifications of evaluation workflows do not distinguish between the type of biometric modality and are generic. Thus, they SHALL be applied to measure biometric performance of fingerprint, facial image and multimodal verification and identification depending on the used biometric modalities of the relevant system.

The evaluation workflows enable a competent authority...

- ... to continuously monitor biometric accuracy in terms of security and usability of the system.
- ... to precisely reconfigure comparison thresholds in order to meet defined security or usability targets.
- ... to assess the biometric performance of new comparison algorithms or updates of deployed comparison algorithms prior to deployment.
- ... to determine thresholds for deploying new or updated algorithms in order to meet defined security and usability targets.
- ... to evaluate and compare new quality algorithms or updates of deployed quality algorithms.
- ... to determine quality thresholds for biometric modalities to be included or excluded in a BMS to meet the defined accuracy targets.
- ... to evaluate and compare comparison algorithms to attribute type specific performance differences, e.g. sex or age.

The process specified by ▸PAP EVA-ID-wCIR-1: Identification Evaluation Workflow for BMS with Identification Capability and with Verification Capability SHALL be executed if an identification request is received.

The process specified by ▸PAP EVA-VER-wCIR-1: Verification Evaluation Workflow for BMS with Identification Capability and with Verification Capability SHALL be executed if a verification request is received and the BMS does not offer an identification capability.

The process specified by ▸PAP EVA-VER-nCIR-1: Verification Evaluation Workflow for BMS without Identification Capability SHALL be executed if a verification request is received and the BMS does offer an identification capability.

2.7.2. Mandatory Function Modules

All Function Modules which SHALL be applied for this Application Profile are listed in ▸Table 2.11. All listed Function Modules (separated by commas) are mandatory for this Application Profile unless specified otherwise. Function Modules separated by slash are alternatives to each other. Function Modules in brackets are RECOMMENDED.

Module Category	Required Function Modules
Acquisition Hardware	
Acquisition Software	
Biometric Image Processing	

[1] The term "biometric match" is ambiguous and could literally mean both "biometric recognition/comparison" or "biometric conformity/hit/equivalence". In the European Regulations and Implementing Acts, it appears being used for both meanings. For the sake of clarity, "match" will only correspond to a hit in the biometric recognition in the following, unless used within the fixed term "biometric matching system", where it is used in the sense of "recognition".

Module Category	Required Function Modules
Quality Assessment	▸FM QA-FI-GENERIC, ▸FM QA-FI-BCL, ▸FM QA-FP-APP
Presentation Attack Detection	
Compression	▸FM COM-FI-GENERIC
Operation	
User Interface	
Reference Storage	
Biometric Comparison	▸FM CMP-FI-VER, ▸FM CMP-FP-VER
Logging	Will be amended in a future version of this TR.
Coding	
Evaluation	Will be amended in a future version of this TR.

Table 2.11 Required Function Modules Application Profile Biometric Matching System Control

2.7.3. Mandatory Partial Application Processes

All Partial Application Processes and Tasks which SHALL be applied for this Application Profile are listed in ▸Table 2.12. All listed Processes (separated by commas) are mandatory for this Application Profile unless specified otherwise. Processes separated by slash are alternatives to each other.

No.	Required Partial Application Process
1	▸PAP EVA-ID-wCIR-1: Identification Evaluation Workflow for BMS with Identification Capability and with Verification Capability / ▸PAP EVA-VER-wCIR-1: Verification Evaluation Workflow for BMS with Identification Capability and with Verification Capability / ▸PAP EVA-VER-nCIR-1: Verification Evaluation Workflow for BMS without Identification Capability

Table 2.12 Required Partial Application Processes Application Profile Automated Border Control

3. Partial Application Processes

The Partial Application Processes (PAPs) specified by the following sections provide process specifications of basic biometric processes, e.g. the acquisition, identification or verification of biometrics or the evaluation processes for verification and identification. The PAPs are referenced by the relevant Application Profiles and are part of the overall processes specified therein.
A PAP MAY also be a task. A task is a process which functions as a generic reusable building block which is used by another PAP and is not referenced by an Application Profile directly.
The specific Function Modules that SHALL be implemented in the processes of this chapter are specified by the relevant Application Profiles.

3.1. PAP ACQ-FI-SV-5: Supervised Facial Image Acquisition System

This Partial Application Process specifies a facial image acquisition system to automatically acquire or manually capture facial images for enrolment, verification or identification purposes. Note, that the ▸PAP ACQ-FI-AUTO-1: Automated Facial Image Acquisition is used here.

3.1.1. Process

The facial image acquisition system consists of two main processes, whereby the automatied acquisition is mandatory in all application scenarios while the manual mode is

- OPTIONAL for devices that are subject to TR volume German Identity Documents (GID)
- MANDATORY for other devices, especially in the context of TR volume Border Control (BCL).

The overall process is depicted in ▸Figure 3.1:

1. The operator triggers the automatic acquisition of a facial image for enrolment or for verification/identification. The operator reviews the acquired facial image and the results of the software based Quality Assessment (QA). The operator SHALL have the option to manually crop and de-rotate the image. In case the manual review revealed bad quality of the facial image, the operator MAY discard the facial image in order to acquire a new facial image. The operator releases the image for further processing.
2. The operator triggers the manual acquisition of a facial image for enrolment or for verification/identification. The operator manually configures the camera system to the body height of the biometric subject (or triggers automatic height configuration). Next, the operator triggers the capture of a facial image of the biometric subject. The operator reviews the results of the software based QA. The operator SHALL have the option to manually crop and de-rotate the image. In case the manual review revealed bad quality of the facial image, the operator MAY discard the facial image in order to acquire a new facial image. The operator releases the image for further processing.

To support the two processes, the system provides the following two service modes via its interface, refer to ▸Section 3.1.1.1:

1. *automated mode*
   In this mode, the system obtains a request from the calling application to acquire an image by a certain quality level (enrolment, verification/identification quality). The system executes the required process autonomously and returns the final image to the calling application. Thereby, the system handles the process execution, e.g. configuration of the camera system to the height of the biometric subject, mandatory repetitions due to quality issues, QA, automatic capture of the facial image etc. The system SHALL imple-

ment the processes specified by the ▸PAP ACQ-FI-AUTO-1: Automated Facial Image Acquisition for the automated mode. This service mode is MANDATORY in all application scenrios.

2. *manual mode*
   In this mode, the system acts as a capture device for the calling application. The calling application sends atomic requests to the system, e.g. to adjust the system to the height of the biometric subject, to switch on the lighting or to capture a facial image. This service mode is OPTIONAL in the application context German Identity Documents (GID).

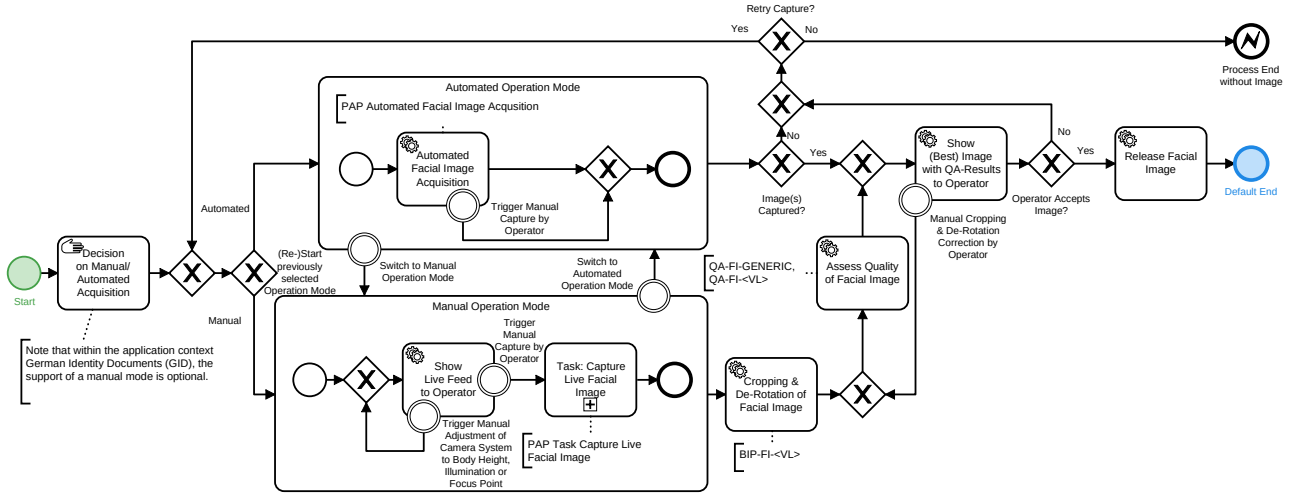

Figure 3.1. Supervised Facial Image Acquisition System: Overall Process

3.1.1.1. Interface Requirements

If High Level Biometric Services (HLBS) is used by the system, the "Service Definition Facial Image Acquisition System" of Part 2, Volume 2 of this Technical Guideline SHALL be implemented.

3.1.2. PAP Task ACQ-FI-1: Capture Live Facial Image

▸Figure 3.2 depicts the basic process of a live facial image capture. If the image acquisition is not supervised PAD SHALL be performed[1]. In case of supervised image acquisition PAD is OPTIONAL.

[1] Note that the requirement for PAD in supervised settings might be subject to transitional arrangements. The final obligation is regulated through the selection of mandatory Function Modules within the respective Application Profiles.

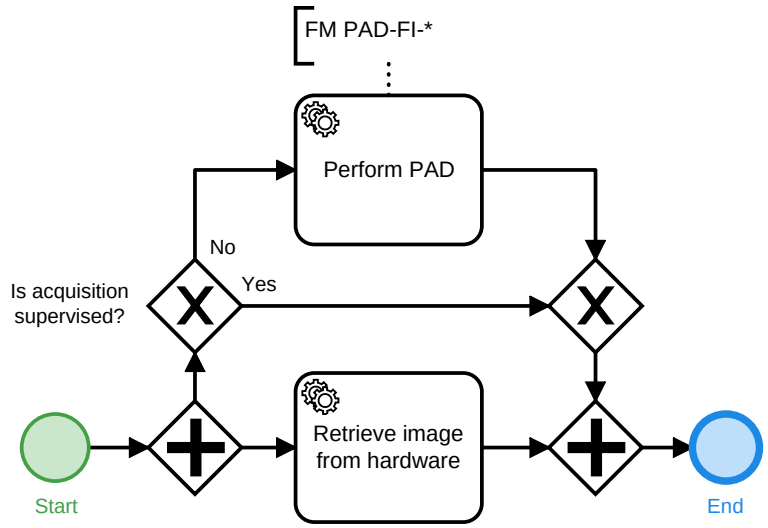

Figure 3.2. Partial Application Process Task "Capture Live Facial Image"

3.2. PAP ACQ-FI-SV-4: Supervised Facial Image Acquisition

3.2.1. Process

The facial image acquisition process, refer to ▸Figure 3.3, described by this section requires a supervised situation. Note, that the ▸PAP Task ACQ-FI-1: Capture Live Facial Image is used here. The biometric subject's facial image is captured using live enrolment equipment (including a digital camera within a photo studio setup) operated by an operator[2].

In case the acquisition system detects a face, the facial image capture SHALL be performed automatically. However, the operator SHALL also have the option to perform the capture manually. An immediately performed cropping and de-rotation of the face and software quality assessment for the captured facial image ensures its biometric usability. If the quality assessment succeeds positively, the image SHALL be shown to the operator. If the quality is assessed as insufficient and the timeout has not exceeded yet, the system SHALL recapture. If the operator has captured manually, the image SHALL be shown to the operator in any case. In case the timeout has exceeded, the system SHALL identify the best captured facial image and show this image to the operator. The operator SHALL have the option to correct the cropping and de-rotation on the shown image manually. The operator SHALL also have the option to accept the captured facial image. The image is then release to the calling application. This is also the case, if the quality has been assessed as insufficient by the system. In the negative case, the facial image SHALL be discarded, the timeout is reset and a recapture is performed.

If the timeout exceeds and no facial image has been captured (neither with sufficient nor with insufficient quality), the process terminates without releasing an image. It is the operator's decision to restart the acquisition process or to perform other actions.

The process SHALL be supervised by an operator.

[2] See ISO/IEC 19794-5, Annex B for "Best practices for Face Images"

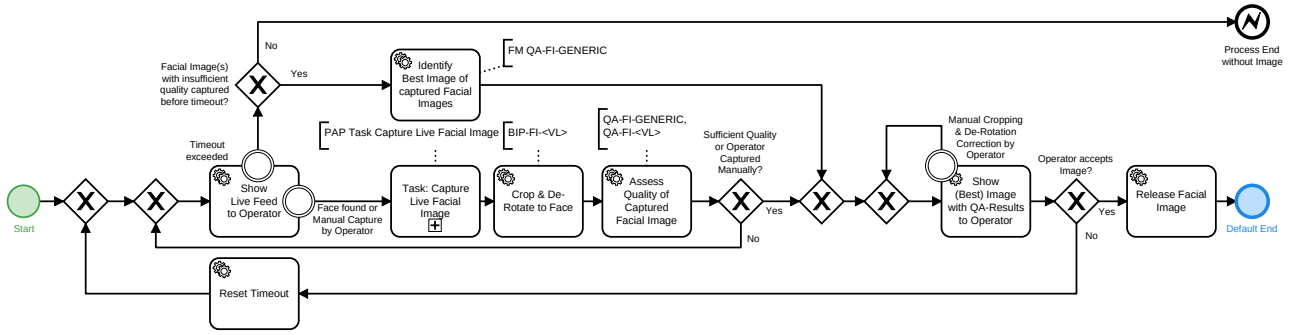

Figure 3.3. Partial Application Process "Supervised Facial Image Acquisition"

3.2.1.1. Interface Requirements

If HLBS is used by the system, the "Service Definition Basic Facial Image Acquisition System" of Part 2, Volume 2 of this Technical Guideline SHALL be implemented.

3.2.2. PAP Task ACQ-FI-1: Capture Live Facial Image

▸Figure 3.2 depicts the basic process of a live facial image capture. If the image acquisition is not supervised PAD SHALL be performed[3]. In case of supervised image acquisition PAD is OPTIONAL.

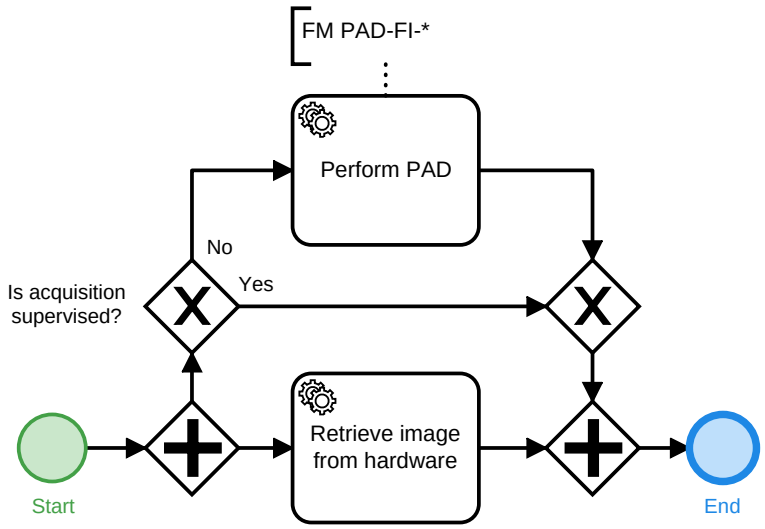

Figure 3.4. Partial Application Process Task "Capture Live Facial Image"

3.3. PAP ACQ-FI-USV-1: Unsupervised Facial Image Acquisition with Prequalification

The facial image acquisition process described by this section applies to unsupervised acquisition situations. The full process of image acquisition and the prequalification of the live facial image is presented in ▸Figure 3.5. Note, that the ▸PAP Task ACQ-FI-1: Capture Live Facial Image is used here.

The following steps SHALL be performed. Live image data is captured with respect to ▸FM Category Acquisition Hardware, ▸FM Category Acquisition Software, ▸FM Category Biometric Image Processing and ▸FM Category Quality Assessment. Prequalification (as defined by ▸FM QA-FI-PRE) ensures that only images of sufficient quality are taken. Live image data MAY be compressed according to ▸FM Category Compression.

[3] Note that the requirement for PAD in supervised settings might be subject to transitional arrangements. The final obligation is regulated through the selection of mandatory Function Modules within the respective Application Profiles.

If the image quality is not sufficient and the specified timeout is not reached and no PAD alarm is triggered, the following SHALL be done: The captured image SHALL be added to a sorted list (sorted by image quality) and a new image SHALL be captured.

This process will finish in one of the following conditions:

- If the image quality is sufficient and the specified timeout is not reached and no PAD alarm is triggered, the acquired image SHALL be returned.
- If the timeout is reached and the sorted image list is not empty, the best quality image from the image list SHALL be returned. Otherwise if the list is empty no image SHALL be returned.
- If a PAD alarm is triggered, the PAD alarm message and the acquired image SHALL be returned to the calling application and displayed to the operator.

The timeout SHALL be configurable.

All gathered information is logged and coded according to ▸FM Category Coding and ▸FM Category Logging.

During the complete transaction of acquisition an operator SHOULD ensure that the biometric subject does not try to illegally bypass the system by using presentation attack instruments or other mechanisms. By means of ▸FM Category Presentation Attack Detection the operator SHALL receive a warning when the PAD subsystem detects a spoofing attack.

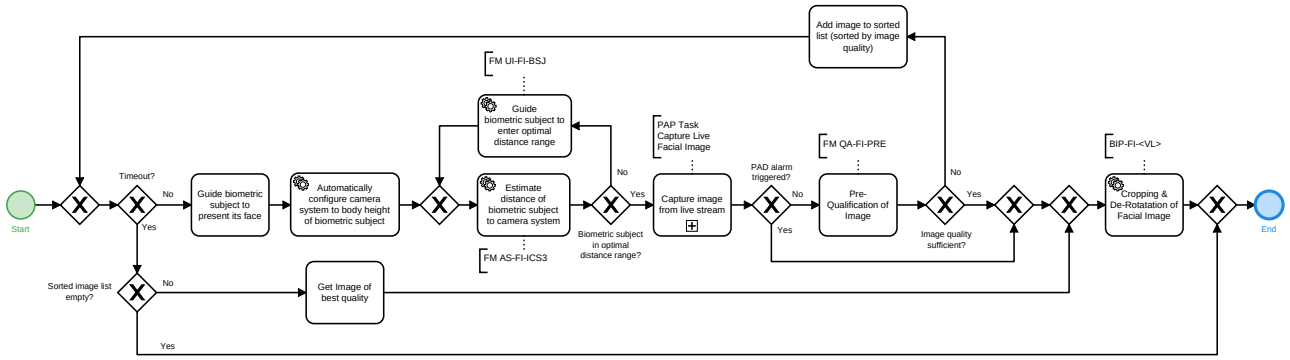

Figure 3.5. Partial Application Process "Unsupervised Facial Image Acquisition with Prequalification"

3.3.1. Interface Requirements

If HLBS is used by the system, the "Service Definition Facial Image Acquisition System" of Part 2, Volume 2 of this Technical Guideline SHALL be implemented.

3.3.2. PAP Task ACQ-FI-1: Capture Live Facial Image

▸Figure 3.2 depicts the basic process of a live facial image capture. If the image acquisition is not supervised PAD SHALL be performed[4]. In case of supervised image acquisition PAD is OPTIONAL.

[4] Note that the requirement for PAD in supervised settings might be subject to transitional arrangements. The final obligation is regulated through the selection of mandatory Function Modules within the respective Application Profiles.

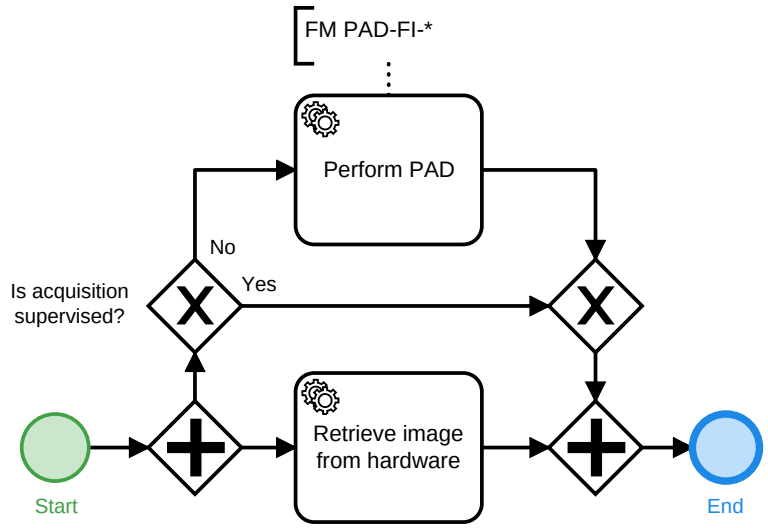

Figure 3.6. Partial Application Process Task "Capture Live Facial Image"

3.4. PAP VER-FI-ALL-1: Facial Image Verification

▸Figure 3.7 depicts the basic process of a facial image varification in an unsupervised scenario. The verification SHALL be performed according to ▸FM Category Biometric Comparison.

The facial image of the biometric subject is verified against the reference facial image on the eMRTD chip. If the biometric subject is a Third-Country National (TCN), verification against applicable CIRs is carried out additionally.

Also, the evaluation workflow is carried out in order to determine the biometric performance of the deployed comparison algorithm.

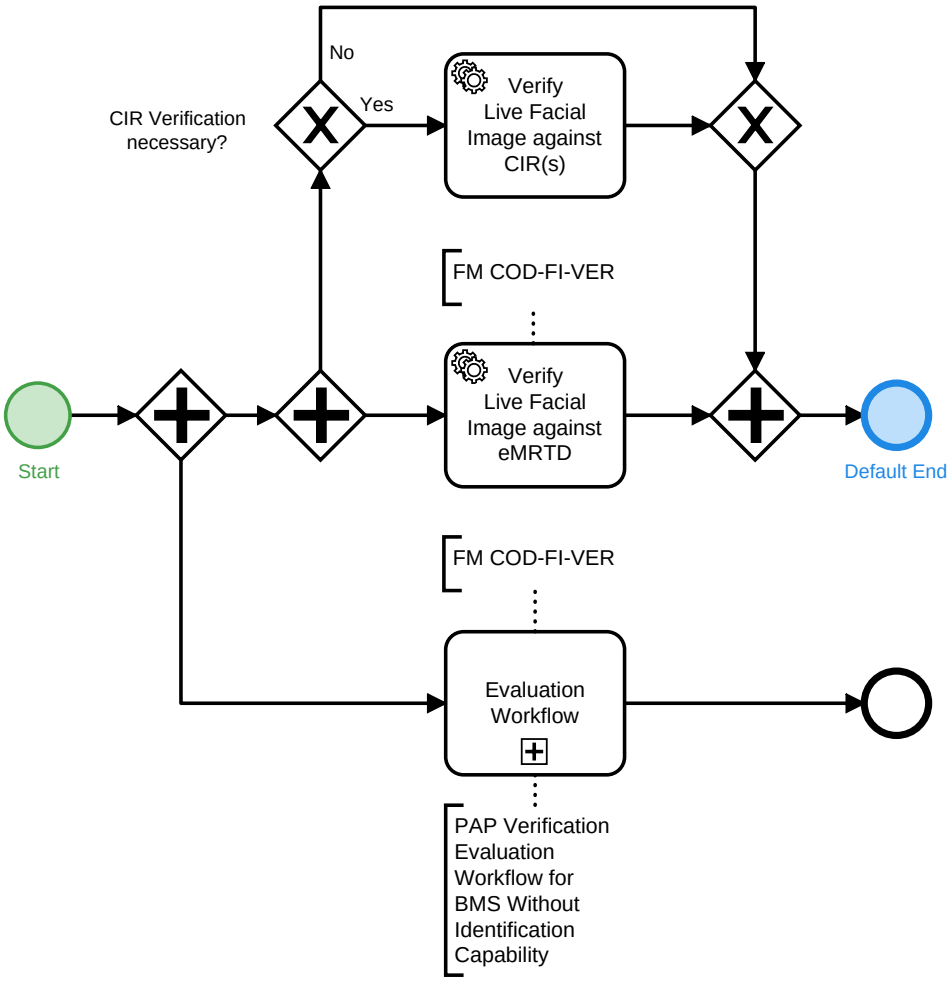

Figure 3.7. Partial Application Process "Facial Image Verification"

3.5. PAP ACQ-FI-AUTO-1: Automated Facial Image Acquisition

The facial image acquisition process described by this section applies to acquisition processes where the facial image is acquired automatically, refer to ▸Figure 3.8. Note, that the ▸PAP Task ACQ-FI-1: Capture Live Facial Image is used here.

An acquisition system SHALL be used that works with an integrated quality assessment Function Module (see ▸FM Category Quality Assessment). The requirements of ▸FM Category Acquisition Hardware, ▸FM Category Acquisition Software and ▸FM Category Biometric Image Processing SHALL apply. The process SHALL use the following steps:

1. The biometric subject SHALL be guided to present its face.
2. The camera system SHALL be automatically configured for the body height of the person.
3. Multiple faces in the acquisition image area SHALL be detected. Note, the detection SHALL be carried out all the time while the acquisition is ongoing until the facial image is captured.
4. If multiple faces are detected, a guidance SHALL advice the biometric subject to appear alone in front of the acquisition system.
5. The distance of the biometric subject to the camera system SHALL be determined.
6. If the biometric subject is not in the optimal capture range, a guidance SHALL advice the biometric subject to enter the optimal distance range.

7. If a facial image can not be captured within a configured timeout, e.g. the biometric subject does not look in the camera or disappears from the system, the acquisition processes ends. The timeout SHALL be configurable.
8. The facial image of the biometric subject SHALL be captured. The image SHALL then be cropped and de-rotated to the face.
9. The quality of the facial image SHALL be assessed according to the specific Function Module in ▸FM Category Quality Assessment.
10. If the quality is not sufficient and the timeout is not exceeded, a new facial image is captured. The timer for the timeout SHALL start with the retrieval of the first facial image from the capture system.
11. If the quality is sufficient, the facial image is released for the calling application.
12. If the timeout is exceeded and no image is of sufficient quality, the best facial image is selected among the captured images according to the specific Function Module in ▸FM Category Quality Assessment and the image SHALL be released for the calling application.
13. With optimal conditions (bona fide) the overall facial image acquisition process SHALL NOT exceed the following time limits:
    a. For devices that are subject to TR volume Border Control (BCL), the overall facial image acquisition process SHALL NOT exceed ten seconds. In case the system is not required to perform a PAD (e.g. supervised scenario) the overall facial image acquisition process SHALL NOT exceed seven seconds.
    b. For devices that are subject to TR volume German Identity Documents (GID), the overall facial image acquisition process SHALL NOT exceed thirty seconds (including PAD).

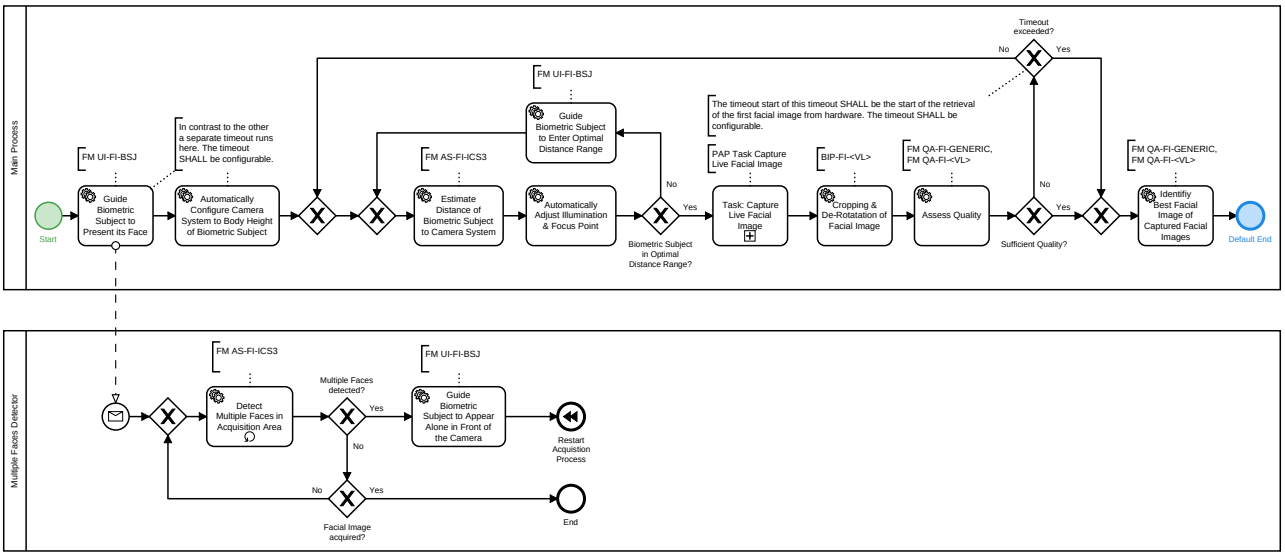

Figure 3.8. Partial Application Process "Automated Facial Image Acquisition"

3.5.1. Interface Requirements

If HLBS is used by the system, the "Service Definition Facial Image Acquisition System" of Part 2, Volume 2 of this Technical Guideline SHALL be implemented.

3.5.2. PAP Task ACQ-FI-1: Capture Live Facial Image

Figure 3.2 depicts the basic process of a live facial image capture. If the image acquisition is not supervised PAD SHALL be performed[5]. In case of supervised image acquisition PAD is OPTIONAL.

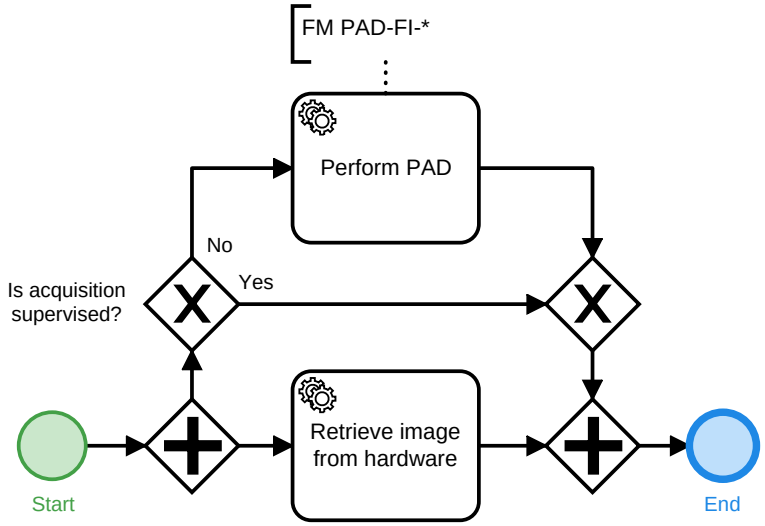

Figure 3.9. Partial Application Process Task "Capture Live Facial Image"

3.6. PAP ACQ-FPS-SV-1: Supervised Acquisition Single Slap

3.6.1. Process

Figure 3.10 depicts the supervised acquisition process of a slap.

At first the operator flags the missing fingers of the hand of the biometric subject. (Alternative: The operator flags the missing fingers of both hands of the biometric subject.)

The biometric subject SHALL be guided to place the hand correctly on the scanner and the slap SHALL be captured. Note, that the Section 3.6.2 is used here.

If already slaps of both hands were acquired, the process SHALL end here. Otherwise the operator SHALL decide if he likes to capture the slap of the other hand, too.

The process SHALL be supervised by an operator.

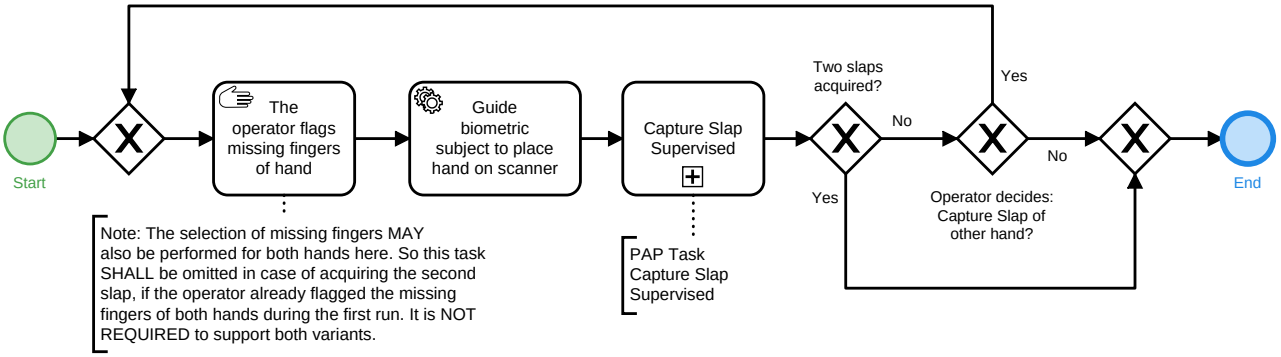

Figure 3.10. Partial Application Process "Supervised Acquisition Slap"

[5] Note that the requirement for PAD in supervised settings might be subject to transitional arrangements. The final obligation is regulated through the selection of mandatory Function Modules within the respective Application Profiles.

3.6.1.1. Interface Requirements

If HLBS is used by the system, the "Service Definition Fingerprint Acquisition" of Part 2, Volume 2 of this Technical Guideline SHALL be implemented.

3.6.2. PAP Task ACQ-FPS-SV-1: Capture Slap Supervised

▸Figure 3.11 depicts the basic process for a plain supervised slap capture. A plain slap capture can be part of more complex acquisition processes, e.g. a ten finger acquisition by the 4-1-4-1 capture sequence. The plain slap capture is subsequently described in detail. The quality assessment is conducted according to the requirements of the applicable ▸FM Category Quality Assessment. Note, that the ▸PAP Task ACQ-FPP-SV-2: Capture Plain Fingerprint Supervised is used here.

If the biometric subject is physically not capable to place all fingers of the slap on the capture hardware at the same time to achieve a slap image of good quality, the operator can decide to capture each finger of the slap in single finger capture mode. This SHALL be possible during the entire process. Hereby, single finger capture mode refers to the ▸PAP Task ACQ-FPP-SV-2: Capture Plain Fingerprint Supervised as described below.

1. The counter variable for the number of attempts for capturing the current slap SHALL be initialized as $i = 1$.
2. The slap image SHALL be retrieved from hardware. While the image is retrieved from hardware, PAD SHALL be performed. Note: The operator SHALL have the option to manually conduct the capture of slap(s).
3. The fingerprints SHALL be segmented and each fingerprint SHALL be quality assessed.
   a. In case the quality of the fingerprints meets the quality requirements defined in the corresponding QA Function Module, the captured slap and the set of segmented fingerprints and parameter data (e.g. quality values) SHALL be temporarily stored.
   b. In case the quality requirements for one or more fingerprints of the slap are not met, the capture SHALL be repeated up to two times (i.e. the acquisition of a single slap consists of a maximum of three capture attempts). The counter SHALL be set to $i = i + 1$.
4. A uniqueness check SHALL be conducted for the captured slap image to detect the capture of wrong fingers, e.g. due to interchanged hands or multiple acquisition of the same hand or finger. Note, that it is RECOMMENDED to conduct the uniqueness check as early as possible after a fingerprint image is available.
   a. In case
      - the comparison of any fingerprint of the current slap with any previously accepted fingerprint of a previous slap or
      - the comparison of any fingerprint of the current slap with another fingerprint of the current slap

      is successful, the uniqueness check SHALL raise a warning.
   b. In case the comparisons of all fingerprints of the current slap with all fingerprints of previous slaps are not successful, the uniqueness check SHALL NOT show a warning.
5. Generally, a slap classifier SHALL be used for the captured slap image to detect the capture of the wrong slap. It SHALL be configurable to switch the classifier off or in evaluation mode (logging of the result without showing the result/warning to the operator). Note, that the slap classifier is only required for 4 finger slaps. Other acquisitions currently do not require the corresponding FM.
   a. If the result of the classification concludes that the acquired slap mismatches the expected slap, a warning SHALL be reported.
   b. If the result of the classification concludes that the acquired slap matches the expected slap, no warning SHALL be reported.

If the quality check of the third capture attempt fails (counter i is set to 3), the best of the captured slaps SHALL be identified according to the corresponding QA Function Module and temporarily stored along with the corresponding information.

The process SHALL be supervised by an operator.

At the end of the process the operator decides on one of the three options:

1. Use the acquired slap.
2. Recapture the current slap. The counter SHALL be reset to $i = 1$.
3. Restart the total slap acquisition workflow.

The operator SHALL have the following veto options:

- Select none of the captured slaps despite sufficient quality.
- Select a slap of insufficient quality from the acquisition process.

At any point of the process the operator MAY decide to acquire any finger of the slap individually.

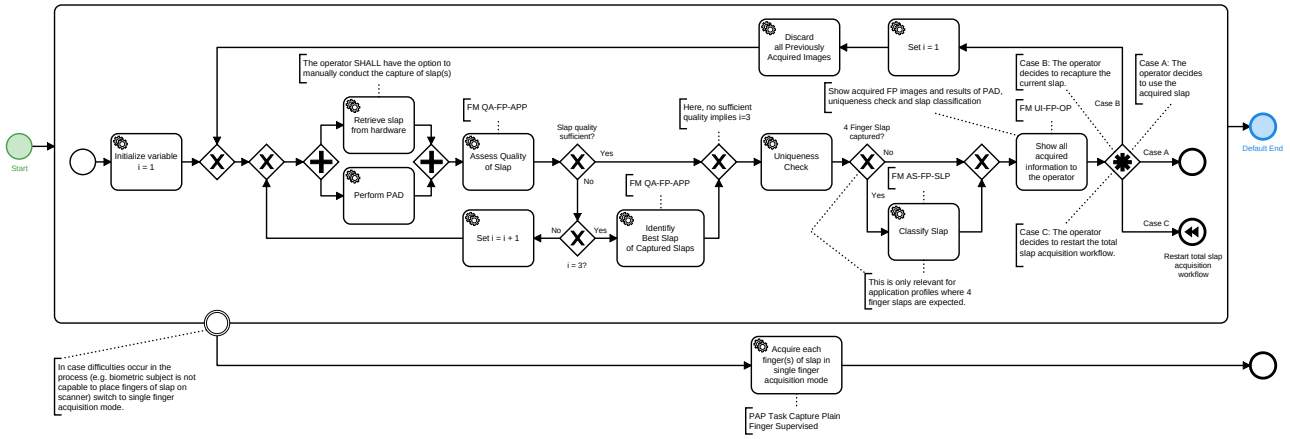

Figure 3.11. Partial Application Process Task "Capture Slap Supervised"

3.6.2.1. PAP Task ACQ-FPP-SV-2: Capture Plain Fingerprint Supervised

Figure 3.12 depicts the basic supervised capture process for a plain fingerprint capture. A plain fingerprint capture can be part of more complex acquisition processes, e.g. a ten finger acquisition by the 4-1-4-1 capture process. The plain fingerprint capture is described in detail subsequently. The quality assessment is conducted according to the requirements of the applicable FM Category Quality Assessment.

1. The counter variable for the number of attempts for capturing the current fingerprints SHALL be initialized as $i = 1$.
2. The fingerprint image SHALL be retrieved from hardware. While the image is retrieved from hardware, PAD SHALL be performed. Note: The operator SHALL have the option to manually conduct the capture of fingerprint(s).
3. The fingerprint SHALL be quality assessed and the captured fingerprint and parameter data (e.g. quality values) SHALL be temporarily stored.
4. In case the quality requirements for the fingerprint are not met, the capture SHALL be repeated up to two times (i.e. the acquisition of a finger consists of a maximum of three capture attempts). The counter SHALL be set to $i = i + 1$.
5. A uniqueness check SHALL be conducted for the captured fingerprint image to detect the capture of wrong fingers, e.g. due to interchanged hands or multiple acquisition of the same hand or finger. Note: It is RECOMMENDED to conduct the uniqueness check as early as possible after a fingerprint image is available.

a. In case the comparison of the current fingerprint with any previously captured fingerprint is successful, the uniqueness check SHALL report a warning.

b. In case the comparison of the current fingerprint with any previously captured fingerprint is not successful, the uniqueness check SHALL NOT report a warning.

6. The acquired finger prints and the results of PAD, QA and uniqueness check SHALL be displayed to the operator.

If the quality check of the third capture attempt fails (counter i is set to 3), the best of the captured fingerprint images SHALL be identified according to the corresponding QA Function Module and temporarily stored along with the corresponding information.

The process SHALL be supervised by an operator.

At the end of the process the operator decides on one of the three options:

1. Use the acquired fingerprint.
2. Recapture the current fingerprint. The counter SHALL be reset to $i = 1$.
3. Restart the ▸Figure 3.12 acquisition workflow.

The operator SHALL have the following veto options:

- Select none of the captured fingerprints despite sufficient quality.
- Select a fingerprint of insufficient quality from the acquisition process.

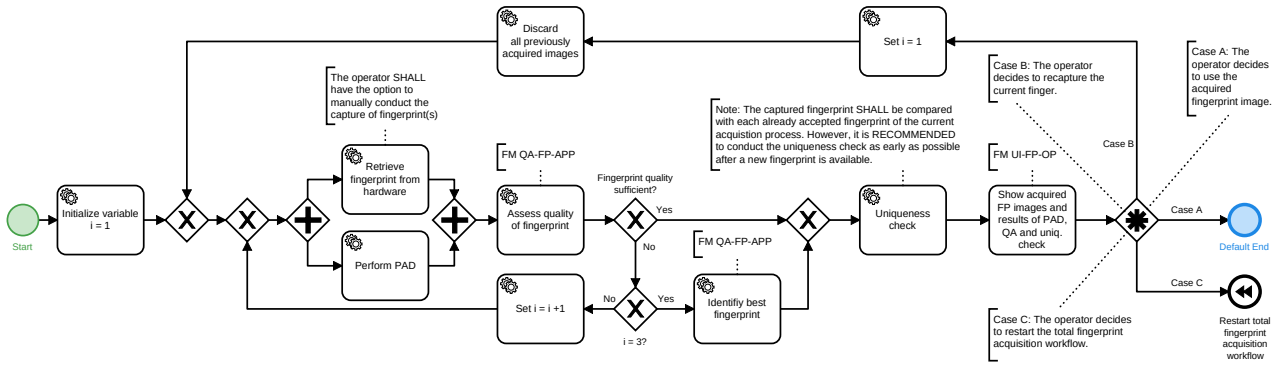

Figure 3.12. Partial Application Process Task "Capture Plain Fingerprint Supervised"

3.7. PAP ACQ-FPS-USV-1: Unsupervised Acquisition Slap

▸Figure 3.13 depicts the unsupervised acquisition process for slaps:

1. It SHALL be checked if all fingers of the desired slap are available, if not the process SHALL end.
2. The biometric subject SHALL be guided to place the hand on the scanner.
3. The slap SHALL be captured. Note, that the ▸PAP Task ACQ-FPS-USV-1: Capture Slap Unsupervised is used here. In parallel the surveillance images SHALL be captured, too.
4. If not four fingers were acquired: Acquired finger images and associated surveillance images SHALL be discarded.

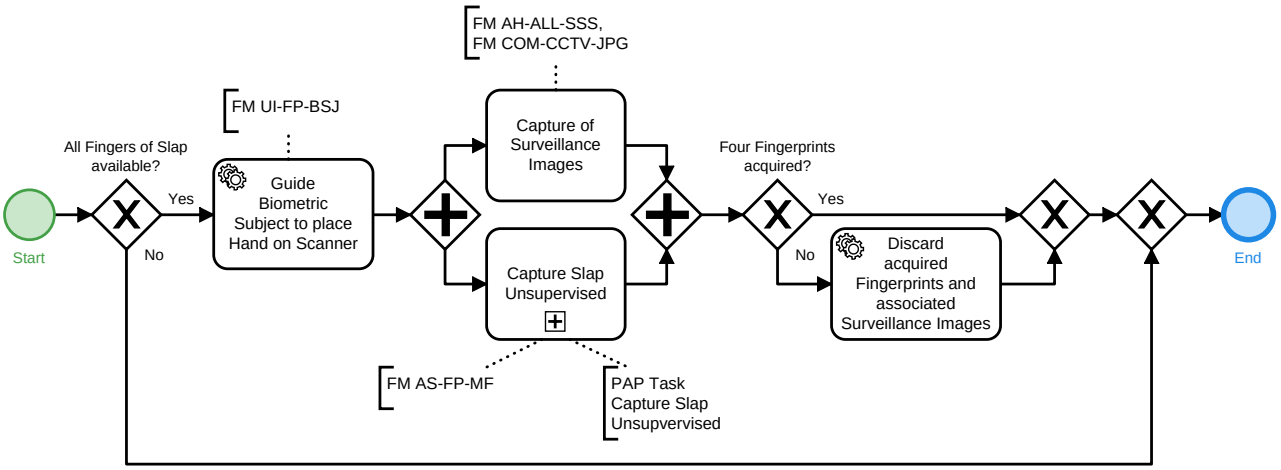

Figure 3.13. Partial Application Process "Unsupervised Acquisition Slap"

3.7.1. Interface Requirements

If HLBS is used by the system, the "Service Definition Fingerprint Acquisition System" of Part 2, Volume 2 of this Technical Guideline SHALL be implemented.

3.7.2. PAP Task ACQ-FPS-USV-1: Capture Slap Unsupervised

Figure 3.14 depicts the basic process for a plain unsupervised slap capture. A plain slap capture can be part of more complex acquisition processes, e.g. a ten finger acquisition by the 4-1-4-1 capture sequence. The plain unsupervised slap capture is subsequently described in detail. The quality assessment is conducted according to the requirements of the applicable FM Category Quality Assessment.

In a uniqueness check, each segmented fingerprint of the current slap SHALL be compared with each already accepted fingerprint of the current acquisition process. Note, this is only required in case more than one slap is captured within the acquisition process.

1. The slap image SHALL be retrieved from hardware. The timer for timeout SHALL be configurable and SHALL start right away with beginning of the whole process. Note, that this timeout can also occur before performing PAD respectively before retrieving slap from hardware.
   a. If the Pre-Qualification is insufficient and timeout has exceeded, the acquisition process, described in this chapter, SHALL continue as follows:
      i. In case no slap has been captured, it SHALL end without an acquired slap.
      ii. In case at least one slap has been captured, the best one SHALL be identified and the acquisition process SHALL end afterwards.
   b. If the Pre-Qualification is insufficient and timeout has not exceeded, the retrieval of an image SHALL be retried.
2. If the hardware returns a PAD alarm, the acquisition process SHALL end. Note, that the relevant information described in Section 4.5 SHALL be stored before ending the acquisition process.
3. QA SHALL be conducted. In case the quality of the fingerprints meet the quality requirements defined in the corresponding Section 4.4, the captured slap and the set of segmented fingerprints and parameter data (e.g. quality values) SHALL be temporarily stored.

a. In case the quality requirements for one or more fingerprints of the slap are not met, the capture SHALL be repeated if the timeout is not reached.

b. In case the timeout is reached and no slap image of sufficient quality was captured, the best slap image according to the corresponding QA Function Module SHALL be stored with the set of segmented fingerprints and parameter data (e.g. quality values).

4. The uniqueness check SHALL be conducted. If the uniqueness check fails, all captured images SHALL be discarded and the capture process SHALL be repeated from the beginning, but if the uniqueness check fails for the second time for the same slap, the acquisition process, described in this chapter, SHALL end without an acquired slap and a warning message SHALL be returned to the calling application, which SHALL be shown to the operator.

5. With optimal conditions (bona fide) the overall slap capture process SHALL NOT exceed ten seconds.

6. Generally, a slap classifier SHALL be used for the captured slap image to detect the capture of the wrong slap. It SHALL be configurable to switch the classifier off or in evaluation mode (logging of the result without showing the result/warning to the operator). Note, that the slap classifier is only required for 4 finger slaps. Other acquisitions currently do not require the corresponding FM.

a. If the result of the classification concludes that the acquired slap mismatches the expected slap, a warning SHALL be shown to the biometric subject, all captured images SHALL be discarded and the capture process SHALL be repeated from the beginning. The number of allowed retries SHALL be configurable.

b. If the result of the classification concludes that the acquired slap mismatches the expected slap and the image is transferred to the calling process, a warning SHALL be reported and shown to the operator. The operator decides whether the slap will be recaptured or the process continuous with the current slap.

c. If the result of the classification concludes that the acquired slap matches the expected slap, no warning SHALL be reported.

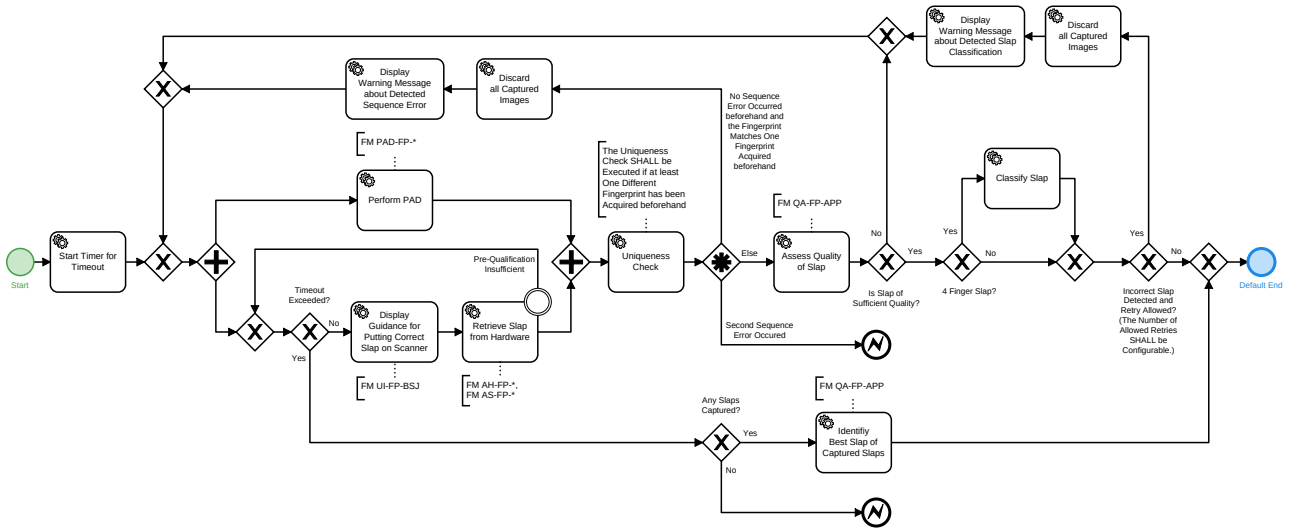

Figure 3.14. Partial Application Process Task "Capture Slap Unsupervised"

3.8. PAP ID-1: CIR Identification

Figure 3.15 depicts the process of a CIR identification.

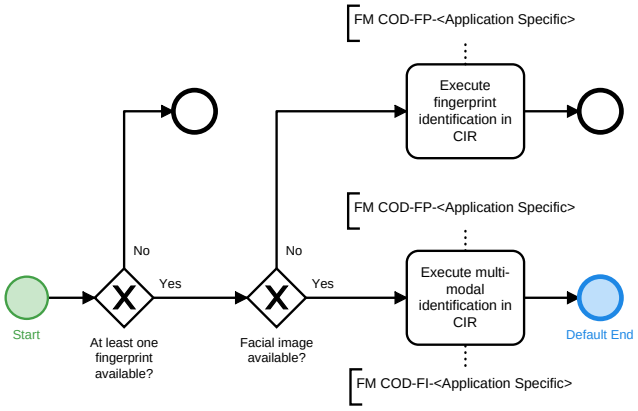

Figure 3.15. Partial Application Process "CIR Identification"

3.9. PAP ASS-B-USV-1: Assess Unsupervised Acquired Biometrics

Figure 3.16 depicts the process of assessment of unsupervised acquired biometrics by an operator.

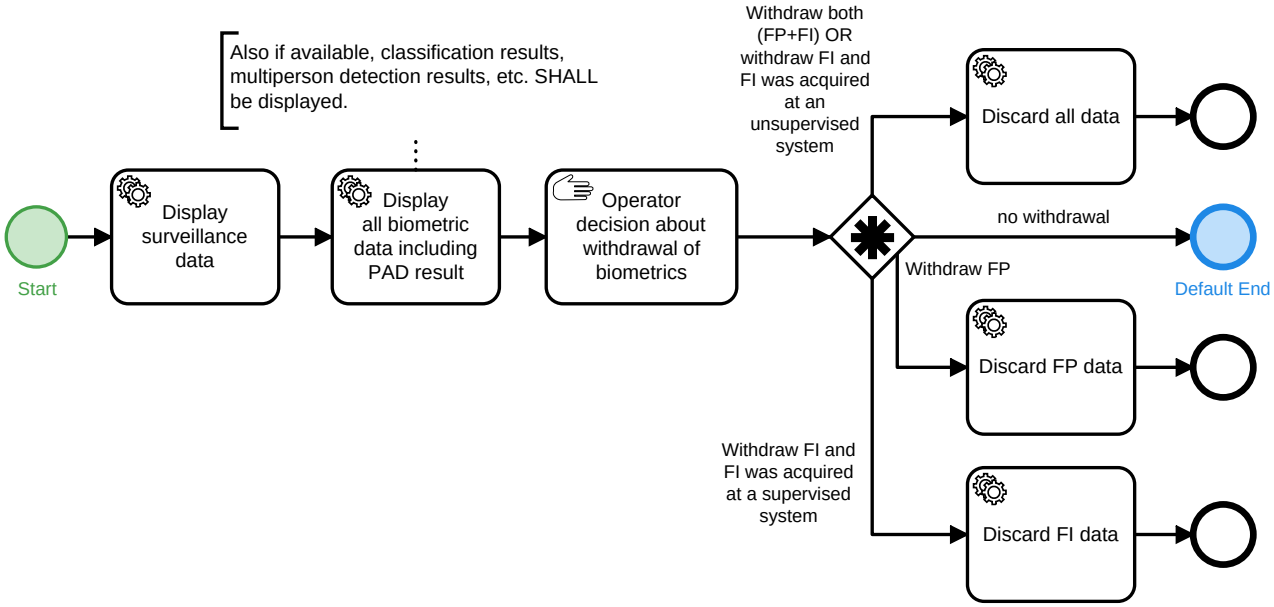

Figure 3.16. Partial Application Process "Assess Unsupervised Acquired Biometrics"

3.10. PAP EVA-ID-wCIR-1: Identification Evaluation Workflow for BMS with Identification Capability and with Verification Capability

This Partial Application Process specifies how the evaluation of biometric identification SHALL be carried out for biometric matching systems with identification and verification capability.

Our notation and exposition in this section closely follows the ISO-standard.

3.10.1. Identification Results and Identification Errors

The goal of *(algorithmic) identification* is to identify a subject by means of a given *(biometric) sample* (for instance, a facial image) inside a register that contains *(biometric) reference templates* of a set of individuals. In a typical algorithmic setting, the outcome of an identification process is based on the computation of numerical scores that are meant to quantify the resemblance between the given sample and the reference (templates) from the register. The algorithm then outputs a *candidate list* that contains all those subjects from the register

for which the corresponding numerical score exceeds a pre-defined threshold. In particular, the algorithm can return an empty list (no matching subject was found in the register), or a list which only contains a single subject.

An identification is also known as a (1:n comparison), since a single probe sample is compared to a set of n references, as opposed to the *verification setting* where we compare a single probe sample with a single reference sample. Accordingly, verification is also referred to as 1:1 comparison.

We now discuss the expected outcome of an identification process. First of all, if a subject P is enrolled in the register, then we expect that the identification system returns a candidate list CL which contains the subject P. We denote this expected *true-positive identification result* by $P \in CL$. If, on the other hand, the identification system returns a candidate list that lacks the subject P, although P is enrolled in the register, then this is considered to be an erroneous result, namely a *false-negative identification (FNI)* result.

Analogously, let us consider the case where the subject P is not enrolled in the register. Obviously, in this case P cannot be on the returned candidate list. In this case we would expect that the algorithm returns an empty candidate list, denote by $CL = \emptyset$. This is a *true-negative identification* result. If, on the other hand, the identification system returns a non-empty candidate list, then it wrongly claims that P is contained in the register. This erroneous event is referred to as a *false-positive identification (FPI)* result.

In order to analyse the quality of the identification system it is important to approximate the probabilities for these two types of erroneous results. Indeed, without any kind of knowledge about the range of these two probabilities, the results of the identification system are more or less meaningless. To this end, we introduce appropriate empirical rates to control the quality of the identification results. But before we do this, let us summarise our setting in the following table:

	P enrolled	**P not enrolled**
Expected Result	$P \in CL$	$CL = \emptyset$
Erroneous Result	$P \notin CL$	$CL \neq \emptyset$

Table 3.1 Identification Results

3.10.2. Introduction to the Error Rates

An identification (1:n comparison) consists of n successive comparisons between the current probe template and n references templates, where n usually denotes all reference templates enrolled in the identity register. Each match is added to a candidate list. Under the assumption that the BMS supports deduplication, i.e. at most one mated template is among the n reference templates, two different initial situations for each identification are possible:

- The identity register contains one *mated* (or *related*) reference to the current probe. This event is denoted as R in the context of identifications.
- The identity register contains only *non-mated* (or *unrelated*) references to the current probe. This event is denoted as $\bar{R}$ in the context of identifications.

In identifications with registers containing one mated reference, i.e. in case of event R, the following outcomes are possible:

- The mated reference is correctly returned in the candidate list. This event is denoted as I_R.
- The mated reference is not included in the returned candidate list. This event is denoted as $\bar{I}_R$. Since the mated reference was among the n references for identification, this is a *false-negative-identification* error (event $R \wedge \bar{I}_R$).

In identifications with registers containing only non-mated references, i.e. in case of event $\bar{R}$, the following outcomes are possible:

- The candidate list is empty. This event is denoted as $I_\emptyset$. Since the mated reference was not among the n references for identification, this is the correct outcome.

- The candidate list is not empty. This event is denoted as $I_{\bar{\emptyset}}$. Since the mated reference was not among the n references for identification, this is a *false-positive-identification* (event $\bar{R} \wedge I_{\bar{\emptyset}}$).

3.10.2.1. Calculation of the Error Rates for Identification

In the following context of identification evaluation, $|R|$ and $|\bar{R}|$ denote the counts of the events R and $\bar{R}$, respectively; i.e. $|R|$ is the number of identifications with a probe, where the identity register contains one mated reference, and $|\bar{R}|$ is the number of identifications, where the identity register does not contain a mated reference. The quantities $|\bar{I}_R|$, $|R \wedge \bar{I}_R|$, $|\bar{I}_{\bar{\emptyset}}|$ and $|\bar{R} \wedge \bar{I}_{\bar{\emptyset}}|$ are defined accordingly as counts of the corresponding events.

The following definitions of the error rates are in accordance to [BIB_ISO_19795-1:2021].

3.10.2.1.1. False-Negative Identification-Rate

The false-negative identification-rate (false-negative-identification-rate (FNIR)) is defined as the fraction of identifications not returning the mated reference as candidate among the conducted identifications with registers including a mated reference:

$$FNIR \quad = \frac{|R \wedge \bar{I}_R|}{|R|} \,. \tag{3.1}$$

This quantity can be measured under laboratory conditions, but the daily application may lack the certain information, whether the mated reference was contained among the n references for identification (i.e. whether the identification represents event $|R|$ or event $|\bar{R}|$) and whether the correct mated reference is returned in the candidate list (i.e. whether the identification result represent event I_R or $\bar{I}_R$). Therefore, the calculation of the FNIR SHOULD only use identifications, where the mated reference is assumed to be contained in the identity register and to be known, e.g. by comparison of associated identity information or by an operator decision as described in ▸Section 3.10.3.3. In this case, an estimate of the FNIR can be calculated using the following approximation and by estimating the count $|\bar{I}_R|$ by the number of cases, in which the assumed mated reference is not returned in the candidate list. [6]

$$FNIR \quad \approx \frac{|\bar{I}_R|}{N_{\mathrm{FNIR}}} \,, \tag{3.2}$$

where N_{FNIR} is the number of identifications performed to determine the FNIR.

3.10.2.1.2. False-Positive Identification-Rate

The false-positive identifications-rate (false-positive-identification-rate (FPIR)) is defined as the fraction of identifications returning a non-empty candidate list among the conducted identifications which did not include a comparison with the mated reference:[7]

$$FPIR \quad = \frac{|\bar{R} \wedge I_{\bar{\emptyset}}|}{|\bar{R}|} \,. \tag{3.3}$$

This quantity can be measured under laboratory conditions, but the daily application may lack the certain information, whether the mated reference is contained among the n references for identification (i.e. whether the identification represents event $|R|$ or event $|\bar{R}|$). Therefore, the calculation of the FPIR SHOULD use only identifications, where the mated reference is assumed to be not contained in the identity register. If the mated reference is assumed to be known, e.g. by comparison of associated identity information or by an operator

[6] Ideally, the addition of non-mated references in the register should have no influence on the occurrence of mated references in the candidate list. If this property can be assumed for an identification algorithm, a minimal register containing only the mated reference can be used to evaluate the FNIR.

[7] The FPIR is not affected by the results of comparisons between mated templates.

decision as described in ▸Section 3.10.3.3, it can be (temporarily) excluded from the identity register for evaluation purposes. [8]

Under the assumption that multiple references do not refer to the same biometric subject in the identity register and that the true mated reference is excluded in nearly all N_{FPIR} identifications ($|\bar{R}| \approx N_{\mathrm{FPIR}}$), the FPIR can be calculated as the fraction of identifications returning at least one candidate among the identifications with excluded mated reference:

$$FPIR \approx \frac{|I_{\bar{\emptyset}}|}{N_{\mathrm{FPIR}}}, \tag{3.4}$$

where N_{FPIR} is the number of identifications performed to determine the FPIR.

3.10.3. Identification Evaluation Workflow for BMS

The identification evaluation workflow can be triggered by both a verification request and an identification request and uses the biometric probe and, in case of a verification request, the reference from the request for evaluation. Depending on the biometric algorithm, the templates may be generated either explicitly prior to the comparison or implicitly during the comparison.

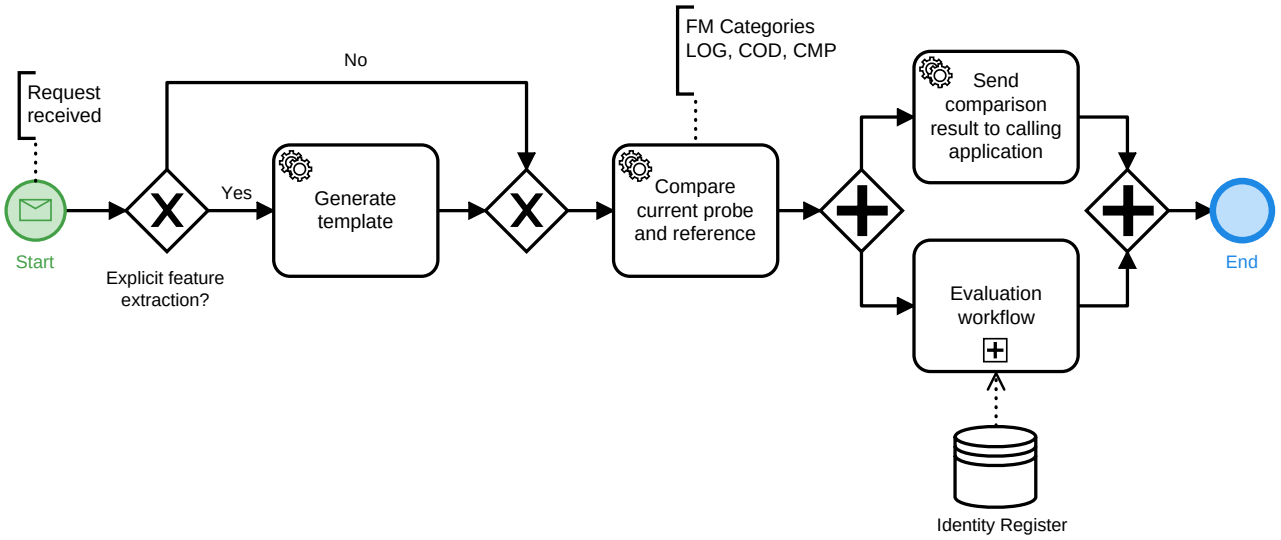

Figure 3.17. Overall Identification Workflow

This Partial Application Process allows to determine the error rates (FNIRs and FPIRs) of BMS for identification purpose.

3.10.3.1. Overall Process

The overall process is comprised of two workflows:

- Either a verification workflow, which compares the presented candidate (probe) and reference, or an identification workflow, which compares the presented candidate (probe) with all references from the identity register. After execution of the verification or identification workflow, respectively, the result is returned to the calling application. [9]

[8] Ideally, the inclusion of a mated reference in the register should have no influence on the occurrence of non-mated references in the candidate list. If this property can be assumed for an identification algorithm, the mated reference does not need to be excluded from the register; instead it can be simply ignored in the candidate list.

[9] The confidence in the assumed identity of the reference presented for verification is typically quite high, in particular, in case of a positive outcome. Therefore, these references from verification requests can be used to set up the identity registers used for the evaluation process.

- The evaluation workflow which conducts identifications with the presented probe by the algorithms deployed and under evaluation.

Figure 3.17 shows a general overview over the complete process within the BMS. Note, that the process "Evaluation workflow" is detailed in the following subsection. The probe data (and reference data in case of a verification request) are received or made available to the BMS. Templates are generated and the comparison is performed and logged according to FM Category Logging. Identification and evaluation logging data SHALL be linked by means of the provided transaction identifiers. Note, that the evaluation workflow MAY be scheduled to reduce system load at peak times. Templates MAY be cached to execute the evaluation workflow while low load is on the system.

3.10.3.2. Evaluation Workflow

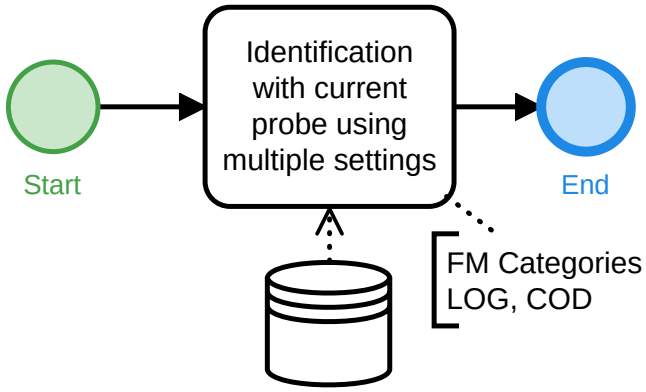

Figure 3.18. Evaluation Workflow for Identification

An overview of the evaluation workflow is given in Figure 3.18. The evaluation workflow executes an identification with the current probe from the current (verification or identification) request. The result of the identification is logged according to FM Category Coding and FM Category Logging. The identification and evaluation SHALL be conducted for each modality available separately and for the multimodal identification if multiple modalities are supplied in the initial (verification or identification) request. The evaluation workflow SHALL be an automatic process without manual processing.

In detail, the following process SHALL be executed in the evaluation workflow for identification:

1. A probe (sample or template) with one or more biometric modalities is received.
2. If not already conducted in a previous step, e.g. in a verification evaluation workflow, QA MAY be conducted according to FM Category Quality Assessment.
3. To enhance the quality of the calculation, measures SHOULD be taken to ensure that a mated reference is contained in the register for the following identifications; exemplary measures are listed in Section 3.10.3.3. The following steps are REQUIRED to calculate the FNIR:
    a. The score for the comparison of the current probe against the (assumed) mated reference from the identity register (genuine comparison) is obtained for the current identification setup under evaluation. If this score is already available, e.g. due to a previous comparison between both templates, this result MAY be reused if the algorithms coincided. In particular for the calculation of a Detection Error

Trade-Off (DET) curve, where the threshold profile is the only varying parameter, scores need to be obtained just once for each probe-reference-pair.

b. If the resulting score is below the threshold value for the identification under evaluation, the amount of false-negative-identifications $|\bar{I}_{\bar{R}}|$ is counted up.

c. The amount of identifications for FNIR evaluation, N_{FNIR}, is counted up.

d. In addition to the evaluation of the identification workflow in the current setup, steps 3(a) to 3(c) SHOULD be performed using other comparison algorithms and/or other threshold profiles. Note that for each algorithm (or deviating threshold profile), separate counts are REQUIRED.

e. The FNIRs for each setup under evaluation can be calculated by the fraction of both counts according to ▸Equation 3.1.

4. To enhance the quality of the calculation, measures SHOULD be taken to ensure that a mated reference is not contained in the register for the following identifications; exemplary measures are listed in ▸Section 3.10.3.3. The following steps are REQUIRED to calculate the FPIR:

   a. An identification is run, comparing the current probe template against all (assumed) non-mated reference templates from the identity register (imposter comparisons). If a comparison score exceeds the current threshold profile, the candidate is set on the candidate list.

   b. If at least one candidate is returned during an identification, the amount of false-positive-identifications, $|I_{\bar{R}}|$, is counted up.

   c. At the end of each identification, the amount of identifications for FPIR evaluation, N_{FPIR}, is counted up.

   d. In addition to the evaluation of the identification workflow in the current setup, steps 4(a) to 4(c) SHOULD be performed using other identification algorithms under evaluation or other threshold profiles. It should be noted that...

      - ... for each setup under evaluation (register, algorithm, threshold profile), separate counts are REQUIRED.
      - ... the FPIRs depends on the number n of references in the identity register and thus, the calculation of the FPIRs (for a given algorithm) SHOULD NOT combine identifications with considerably varying register sizes n (e.g. due to amendments to the register),
      - ... for the calculation of a DET curve, i.e. FPIRs for varying threshold values, the identification needs to be performed just on (using a low threshold profile) and the resulting scores can be checked against all required threshold values (greater or equal than the threshold used in the identification operation) without successive reproduction of the comparison scores.

   e. The FPIR for each setup under evaluation is calculated by the fraction of both corresponding counts according to ▸Equation 3.4.

5. The results SHALL be logged according to ▸FM Category Coding and ▸FM Category Logging.

3.10.3.3. Optional Measures to Enhance the Quality of the Evaluation

For the assumptions made above to calculate the error rates, it is essential to ensure, that the correct mated reference template is (or is not) contained in the pool of reference templates. Following implementations MAY be used to achieve this goal:

- For the accuracy evaluation of identifications or verifications using only one biometric modality, a preceding verification based on another biometric modality could give insight about the true nature (mated or non-mated) of the relation between probe and reference. As false-non-matches (or respectively false-matches) for different biometric modalities are independent, this does not introduce a bias. This is only possible if more biometric modalities are transmitted for the probe and are available for the references than

required for the evaluation. Additionally, it MUST be ensured that the accuracy provided by verification of another modality is sufficiently high to prevent from introducing errors.

- Further insight about the true nature (mated or non-mated) of the relation between probe and reference can be obtained by operator decisions from the main-workflow. Any non-match appearing during the border control process will require further inspection by an operator. The final decision entered by the operator can be used as additional information. If the operator ends this inspection by deciding on a true-non-match, the probe-reference pair SHOULD be excluded in evaluation workflows requiring mated pairs. Thus, the evaluation workflow itself will still be completely automatic, though its start SHALL be delayed until the main border control process is terminated, see ▸Figure 3.19.

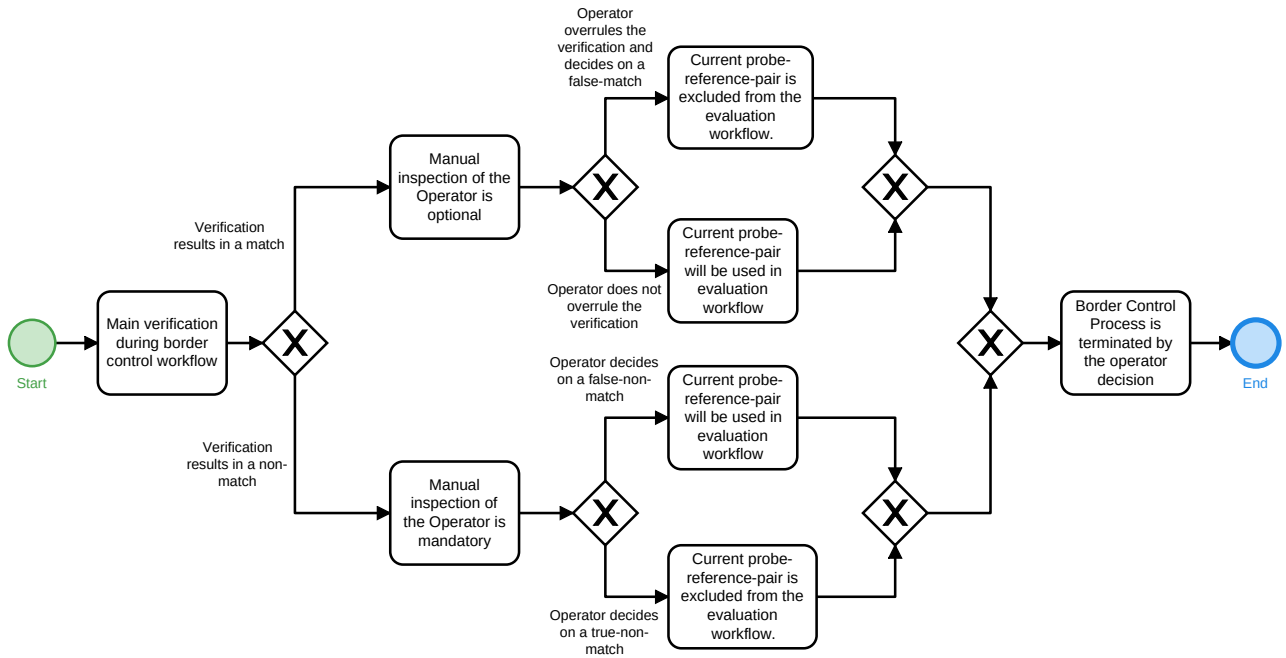

Figure 3.19. Use of Operator Decisions as a Background Filter

3.11. PAP EVA-VER-wCIR-1: Verification Evaluation Workflow for BMS with Identification Capability and with Verification Capability

This Partial Application Process specifies how the evaluation of biometric verification SHALL be carried out for biometric matching systems with identification and verification capability.

3.11.1. Introduction to the Error Rates

Biometric verifications and identifications are based on single algorithmic comparisons between a probe and a reference template, quantifying the resemblance between each pair of templates by a numerical score. The binary result of a comparison (match or non-match) depends on whether this numerical score exceeds a preset threshold value.

A verification consist of a single 1:1 comparison between one probe template and one reference template. Therefore, two scenarios are possible for the incoming probe and reference templates:

- Probe and reference are *mated* (or *related*), i.e. belong to the biometric characteristic of the same biometric subject. In the following context of verifications, this event is denoted as R.
- Probe and reference are *non-mated* (or *unrelated*), i.e. do not belong to the same biometric characteristic of the same biometric subject. In the following context of verifications, this event is denoted as $\bar{R}$.

A verification-threshold-value is set, so that two results for the biometric comparison are possible:

- If the score is above or equal to the threshold, the result of the comparison is a *match*. In the following context of verifications, this event is denoted as M.
- If the score is below the threshold, the result of the comparison is a *non-match*. In the following context of verifications, this event is denoted as $\bar{M}$.

As a consequence, four different scenarios between income and outcome are possible in a verification:

- Probe and reference are *mated* and the verification returns a *match*. This is a correct result (*true-match*) and denoted as $R \wedge M$.
- Probe and reference are *mated* and the verification returns a *non-match*. This is an error referred to as *false-non-match* and denoted as $R \wedge \bar{M}$.
- Probe and reference are *non-mated* and the verification returns a *match*. This is an error referred to as *false-match* and denoted as $\bar{R} \wedge M$.
- Probe and reference are *non-mated* and the verification returns a *non-match*. This is a correct result (*true-non-match*) and denoted as $\bar{R} \wedge \bar{M}$.

A false-match is usually security related, as access might be granted to an imposter. Therefore, an acceptable false-match-rate (FMR) needs to be predefined depending on the application and a strict obedience SHALL be monitored. A false-non-match can be related to a denial of access for a genuine user. This error is usually not security related, though a low false-non-match-rate (FNMR) is important to ensure a high performance, usability and acceptance by the users of the application.

3.11.1.1. Calculation of the Error Rates for Verification

In the following context of verification evaluation, $|R|$ denotes the amount of comparisons between mated templates for a set of N independent comparisons. The quantities $|\bar{R}|$, $|M|$, $|\bar{M}|$, $|R \wedge M|$, $|R \wedge \bar{M}|$, $|\bar{R} \wedge M|$, $|\bar{R} \wedge \bar{M}|$ are defined accordingly as counts of the corresponding events. This implies $N = |R| + |\bar{R}| = |M| + |\bar{M}|$.

The following definitions of the error rates are in accordance to [BIB_ISO_19795-1:2021].

3.11.1.1.1. False-Non-Match-Rate (FNMR)

The FNMR is defined as the fraction of comparisons returning a non-match among the comparisons between mated images:

$$\mathrm{FNMR} \quad = \frac{|R \wedge \bar{M}|}{|R|} \,. \tag{3.5}$$

Under laboratory conditions, R is known, i.e. whether two images are mated, thus $|R \wedge \bar{M}|$ can be measured and the FNMR exactly calculated. Though the evaluation within the daily application lacks information about whether or not two images are truly mated, thus R is unknown. Therefore, the FNMR needs to be approximated:

$$\begin{aligned} \mathrm{FNMR} \quad &= \frac{|R \wedge \bar{M}|}{|R|} \\ &= \frac{|\bar{M}|}{N_{\mathrm{FNMR}}} \left(1 + \frac{|\bar{R}|}{|R|}\right) - \frac{|\bar{R} \wedge \bar{M}|}{|R|} \\ &\approx \frac{|\bar{M}|}{N_{\mathrm{FNMR}}} \,, \end{aligned} \tag{3.6}$$

where N_{FNMR} is the number of verifications performed to determine the false-non-match-rate (FNMR).

Here, both quantities $|\bar{M}|$ and N_{FNMR} can be measured. The approximation in ▸Equation 3.6 holds if $|\bar{R}| \ll |R| \Rightarrow |R| \approx N_{\mathrm{FNMR}}$, thus the amount of true-non-matches is negligible to the amount of false-non-matches. Therefore, the calculation of the FNMR SHOULD only use verifications, where the reference and

probe can be assumed to be mated, e.g. by comparison of associated identity information or by an operator decision as described in ▸Section 3.10.3.3. [10]

3.11.1.1.2. False-Match-Rate (FMR)

The FMR is defined as the fraction of comparisons returning a match among the comparisons between non-mated images:

$$\mathrm{FMR} \quad = \frac{|\bar{R} \wedge M|}{|\bar{R}|} \,. \tag{3.7}$$

Under laboratory conditions, $\bar{R}$ is known, i.e. whether two images are non-mated, thus $|\bar{R} \wedge M|$ can be measured and the FMR exactly calculated. Though the evaluation within the daily application lacks information about whether or not two images are truely mated, thus $\bar{R}$ is unknown. Therefore, FMR needs to be approximated:

$$\begin{aligned} \mathrm{FMR} \quad &= \frac{|\bar{R} \wedge M|}{|\bar{R}|} \\ &= \frac{|M|}{N_{\mathrm{FMR}}} \left(1 + \frac{|R|}{|\bar{R}|}\right) - \frac{|R \wedge M|}{|\bar{R}|} \\ &\approx \frac{|M|}{N_{\mathrm{FMR}}} \,, \end{aligned} \tag{3.8}$$

where N_{FMR} is the number of identifications performed to determine the false-match-rate (FMR).

Here, both quantities $|M|$ and N_{FMR} can be measured. The approximation in ▸Equation 3.8 holds if $|R| \ll |\bar{R}| \Rightarrow |\bar{R}| \approx N_{\mathrm{FMR}}$, thus the amount of true-matches is negligible to the amount of false-matches. Therefore, the calculation of the FMR SHOULD only use verifications, where the reference and probe are assumed to be non-mated.

3.11.2. Verification Evaluation Workflow for BMS with Connected Identity Register

The verification evaluation workflow is triggered by a verification request and uses the biometric probe and reference from the request for evaluation. Depending on the biometric algorithm, the templates may be generated either explicitly prior to the comparison or implicitly during the comparison.

[10] Non-mated images could occur due to imposters or due to accidentally changed documents within travel groups.

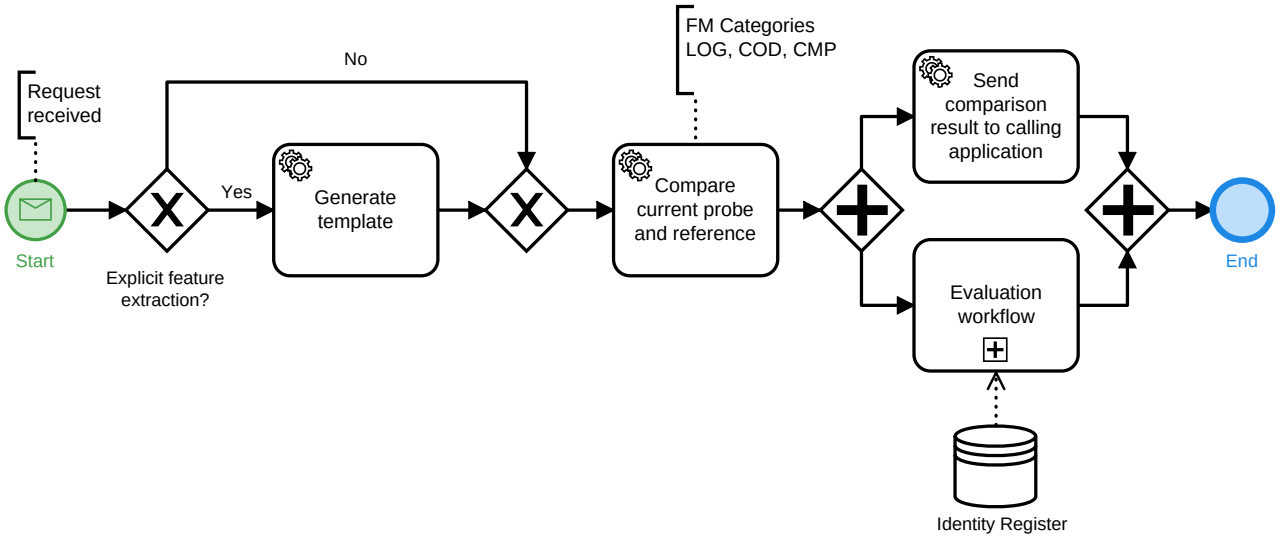

Figure 3.20. Overall Verification Workflow with CIR

Figure 3.20 shows a general overview over the complete verification workflow within the BMS. Note, that the process "Evaluation workflow" is detailed in the following subsection and Figure 3.21. The reference and probe data are received or made available to the BMS. Templates are generated and the comparison is performed and logged according to FM Category Logging. Verification and evaluation logging data SHALL be linked by means of the provided transaction identifiers.

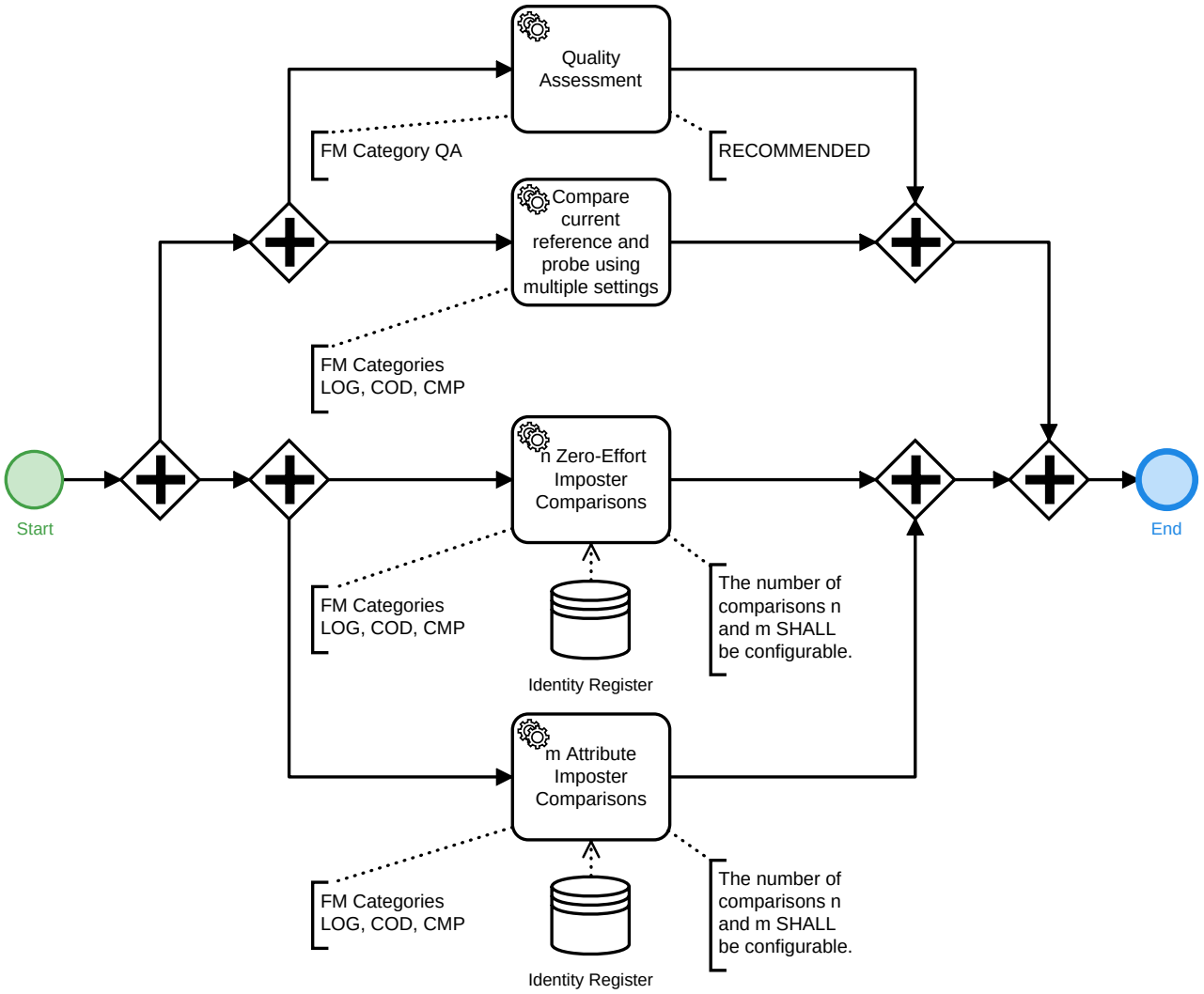

Figure 3.21. Verification Evaluation Workflow with Connected Identity Register

3.11.2.1. Evaluation Workflow

An overview over the evaluation workflow is given in ▸Figure 3.21. The evaluation workflow itself SHALL be comprised of three main tasks:

- recommended QA of the current probe and reference image
- comparison of the current probe with the current reference using an additional comparison algorithm, which was not used for the normal verification, or varying threshold profiles
- control-verifications of the current probe with non-mated reference templates

In detail, the following process SHALL be executed in the evaluation workflow for verification:

1. A probe template and the mated reference template are received.
2. QA for evaluation purposes MAY be conducted according to ▸FM Category Quality Assessment.
3. To enhance the quality of the calculation, measures SHOULD be taken to exclude non-mated comparisons in the following genuine comparisons. Exemplary measures are listed in ▸Section 3.10.3.3. The following steps are REQUIRED to calculate the FNMR:
   a. The current probe is compared against the current (assumed mated) reference (genuine comparison) to obtain a score. If this score is already available, e.g due to a previous comparison between both tem-

plates, this result MAY be reused if the algorithms coincided. In particular, for the calculation of a Detection-Error-Tradeoff curve, where the threshold profile is the only varying parameter, scores need to be obtained just once for each probe-template-pair.

b. If the score is below the threshold profile under evaluation, the amount of non-matches ($\bar{M}$) is counted up.

c. The amount of total comparisons (N_{FNMR}) is counted up.

d. In addition to the setup of the standard verification workflow, other comparison algorithms and/or other threshold profiles SHALL be evaluated here. Note that for each algorithm (or deviating threshold profile), the non-matches SHALL be counted separately.

e. The FNMR based on the yet evaluated data can be calculated for each setup according to ▸Equation 3.6.

4. To enhance the quality of the calculation, measures SHOULD be taken to exclude mated comparisons in the following impostor comparisons. Exemplary measures are listed in ▸Section 3.10.3.3. The following steps are REQUIRED to calculate FMR as follows:

a. Comparisons of the current probe with a sufficiently large amount of n templates in a pool of non-mated references from the identity register are conducted without respect to similiar attributes (zero effort). It SHALL be ensured that the pool neither contains the mated reference to the probe nor multiple references of the same biometric subject.

b. For each comparison, N_{FMR} is increased by 1.

c. For each comparison score exceeding the current threshold profile under evaluation, the (false) match counter $|M|$ is increased by 1. As all templates without restriction are used, these are the "zero-effort"-counts.

d. The FMRs for probe-reference-pairs coinciding in certain attributes SHALL be accessed by separated counts for matches and comparisons when one of the following attributes coincides:

i. Age groups

ii. Sex

iii. Nationality

iv. Document Issuer of Identity Document

Additional attributes MAY be evaluated.

e. The FMRs for the zero-effort and all attributes based on the yet evaluated data can be calculated according to ▸Equation 3.8.

5. The results are logged according to ▸FM Category Coding and ▸FM Category Logging.

3.11.2.2. Optional Measures to Enhance the Quality of the Evaluation

For the assumptions made above to calculate the error rates, it is essential to ensure, that the correct mated reference template is (or is not) contained in the pool of reference templates. Following implementations MAY be used to achieve this goal:

- For the accuracy evaluation of identifications or verifications using only one biometric modality, a preceding verification based on another biometric modality could give insight about the true nature (mated or non-mated) of the relation between probe and reference. As false-non-matches (or respectively false-matches) for different biometric modalities are independent, this does not introduce a bias. This is only possible if more biometric modalities are transmitted for the probe and are available for the references than required for the evaluation. Additionally, it MUST be ensured that the accuracy provided by verification of another modality is sufficiently high to prevent from introducing errors.

- Further insight about the true nature (mated or non-mated) of the relation between probe and reference can be obtained by operator decisions from the main-workflow. Any non-match appearing during the border control process will require further inspection by an operator. The final decision entered by the operator can be used as additional information. If the operator ends this inspection by deciding on a true-non-match, the probe-reference pair SHOULD be excluded in evaluation workflows requiring mated pairs. Thus, the evaluation workflow itself will still be completely automatic, though its start SHALL be delayed until the main border control process is terminated, see ▸Figure 3.19.

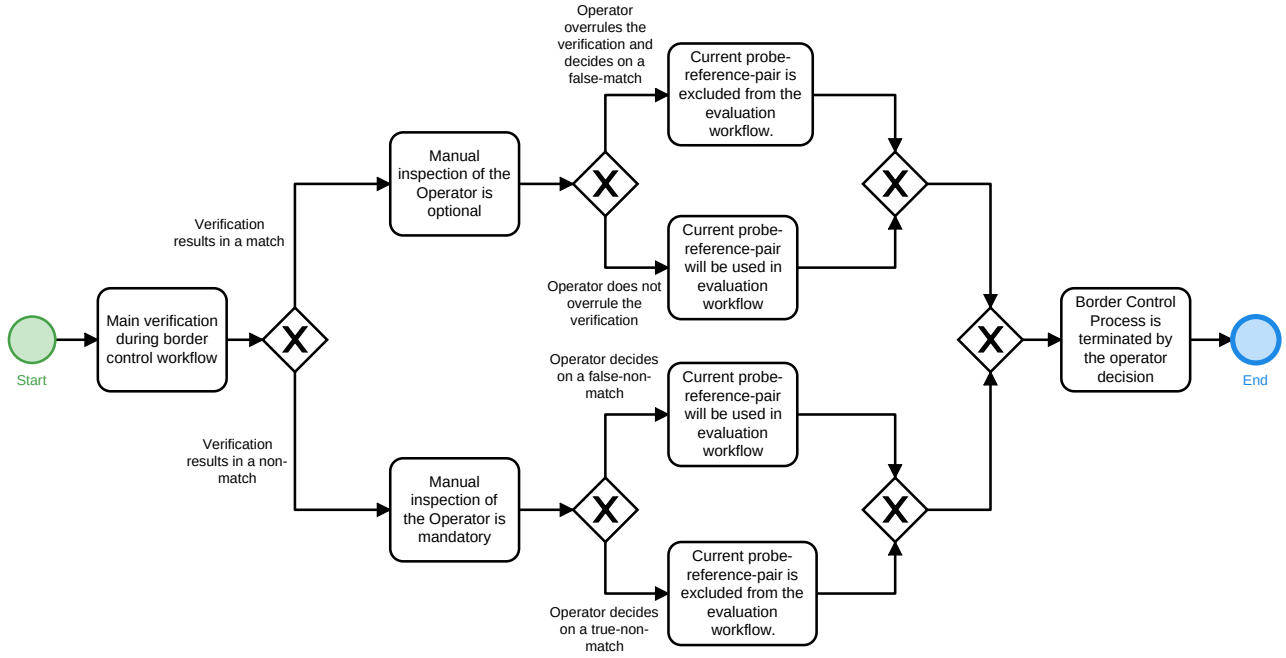

Figure 3.22. Use of Operator Decisions as a Background Filter

3.12. PAP EVA-VER-nCIR-1: Verification Evaluation Workflow for BMS without Identification Capability

This Partial Application Process specifies how the evaluation of biometric verification SHALL be carried out for biometric matching systems without identification capability.

3.12.1. Introduction to the Error Rates

Biometric verifications and identifications are based on single algorithmic comparisons between a probe and a reference template, quantifying the resemblance between each pair of templates by a numerical score. The binary result of a comparison (match or non-match) depends on whether this numerical score exceeds a preset threshold value.

A verification consist of a single 1:1 comparison between one probe template and one reference template. Therefore, two scenarios are possible for the incoming probe and reference templates:

- Probe and reference are *mated* (or *related*), i.e. belong to the biometric characteristic of the same biometric subject. In the following context of verifications, this event is denoted as R.
- Probe and reference are *non-mated* (or *unrelated*), i.e. do not belong to the same biometric characteristic of the same biometric subject. In the following context of verifications, this event is denoted as $\bar{R}$.

A verification-threshold-value is set, so that two results for the biometric comparison are possible:

- If the score is above or equal to the threshold, the result of the comparison is a *match*. In the following context of verifications, this event is denoted as M.

- If the score is below the threshold, the result of the comparison is a *non-match*. In the following context of verifications, this event is denoted as $\bar{M}$.

As a consequence, four different scenarios between income and outcome are possible in a verification:

- Probe and reference are *mated* and the verification returns a *match*. This is a correct result (*true-match*) and denoted as $R \wedge M$.
- Probe and reference are *mated* and the verification returns a *non-match*. This is an error referred to as *false-non-match* and denoted as $R \wedge \bar{M}$.
- Probe and reference are *non-mated* and the verification returns a *match*. This is an error referred to as *false-match* and denoted as $\bar{R} \wedge M$.
- Probe and reference are *non-mated* and the verification returns a *non-match*. This is a correct result (*true-non-match*) and denoted as $\bar{R} \wedge \bar{M}$.

A false-match is usually security related, as access might be granted to an imposter. Therefore, an acceptable false-match-rate (FMR) needs to be predefined depending on the application and a strict obedience SHALL be monitored. A false-non-match can be related to a denial of access for a genuine user. This error is usually not security related, though a low false-non-match-rate (FNMR) is important to ensure a high performance, usability and acceptance by the users of the application.

3.12.1.1. Calculation of the Error Rates for Verification

In the following context of verification evaluation, $|R|$ denotes the amount of comparisons between mated templates for a set of N independent comparisons. The quantities $|\bar{R}|$, $|M|$, $|\bar{M}|$, $|R \wedge M|$, $|R \wedge \bar{M}|$, $|\bar{R} \wedge M|$, $|\bar{R} \wedge \bar{M}|$ are defined accordingly as counts of the corresponding events. This implies $N = |R| + |\bar{R}| = |M| + |\bar{M}|$.

The following definitions of the error rates are in accordance to [BIB_ISO_19795-1:2021].

3.12.1.1.1. False-Non-Match-Rate (FNMR)

The FNMR is defined as the fraction of comparisons returning a non-match among the comparisons between mated images:

$$\mathrm{FNMR} \quad = \frac{|R \wedge \bar{M}|}{|R|} \,. \tag{3.9}$$

Under laboratory conditions, R is known, i.e. whether two images are mated, thus $|R \wedge \bar{M}|$ can be measured and the FNMR exactly calculated. Though the evaluation within the daily application lacks information about whether or not two images are truly mated, thus R is unknown. Therefore, the FNMR needs to be approximated:

$$\begin{aligned} \mathrm{FNMR} \quad &= \frac{|R \wedge \bar{M}|}{|R|} \\ &= \frac{|\bar{M}|}{N_{\mathrm{FNMR}}} \left(1 + \frac{|\bar{R}|}{|R|}\right) - \frac{|\bar{R} \wedge \bar{M}|}{|R|} \\ &\approx \frac{|\bar{M}|}{N_{\mathrm{FNMR}}} \,, \end{aligned} \tag{3.10}$$

where N_{FNMR} is the number of verifications performed to determine the FNMR.

Here, both quantities $|\bar{M}|$ and N_{FNMR} can be measured. The approximation in ▸Equation 3.6 holds if $|\bar{R}| \ll |R| \Rightarrow |R| \approx N_{\mathrm{FNMR}}$, thus the amount of true-non-matches is negligible to the amount of false-non-matches. Therefore, the calculation of the FNMR SHOULD only use verifications, where the reference and

probe can be assumed to be mated, e.g. by comparison of associated identity information or by an operator decision as described in ▸Section 3.10.3.3. [11]

3.12.1.1.2. False-Match-Rate (FMR)

The FMR is defined as the fraction of comparisons returning a match among the comparisons between non-mated images:

$$\mathrm{FMR} \quad = \frac{|\bar{R} \wedge M|}{|\bar{R}|} \,. \tag{3.11}$$

Under laboratory conditions, $\bar{R}$ is known, i.e. whether two images are non-mated, thus $|\bar{R} \wedge M|$ can be measured and the FMR exactly calculated. Though the evaluation within the daily application lacks information about whether or not two images are truely mated, thus $\bar{R}$ is unknown. Therefore, FMR needs to be approximated:

$$\begin{aligned} \mathrm{FMR} \quad &= \frac{|\bar{R} \wedge M|}{|\bar{R}|} \\ &= \frac{|M|}{N_{\mathrm{FMR}}} \left(1 + \frac{|R|}{|\bar{R}|}\right) - \frac{|R \wedge M|}{|\bar{R}|} \\ &\approx \frac{|M|}{N_{\mathrm{FMR}}} \,, \end{aligned} \tag{3.12}$$

where N_{FMR} is the number of identifications performed to determine the FMR.

Here, both quantities $|M|$ and N_{FMR} can be measured. The approximation in ▸Equation 3.8 holds if $|R| \ll |\bar{R}| \Rightarrow |\bar{R}| \approx N_{\mathrm{FMR}}$, thus the amount of true-matches is negligible to the amount of false-matches. Therefore, the calculation of the FMR SHOULD only use verifications, where the reference and probe are assumed to be non-mated.

3.12.2. Verification Evaluation Workflow for BMS without Connected Identity Register

The overall verification process is comprised of two workflows:

- the verification workflow which compares the presented candidate (probe) with a reference and returns the result to the calling application
- the evaluation workflow which conducts the comparisons with algorithms under evaluation, executes imposter control-verifications for accuracy evaluation and may evaluate the quality of biometric modalities by quality algorithms under evaluation

[11] Non-mated images could occur due to imposters or due to accidentally changed documents within travel groups.

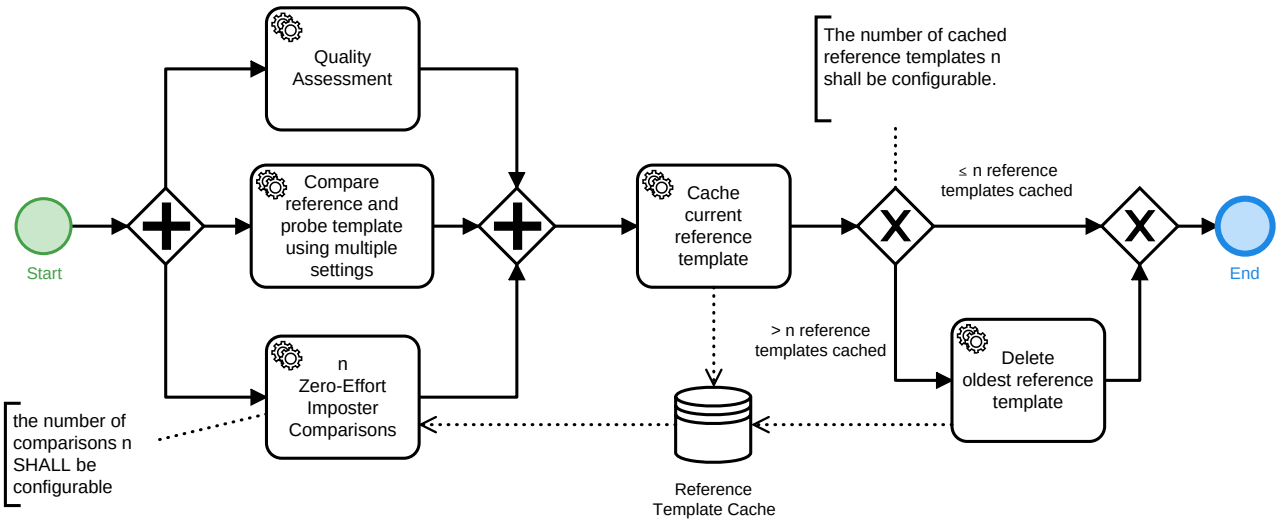

Figure 3.23. Overall Verification Workflow without CIR

Figure 3.23 shows a general overview over the complete verification workflow within the BMS. Note, that the process "Evaluation workflow" is detailed in the following subsection and Figure 3.24. The reference and probe data are received or made available to the BMS. Templates are generated and the comparison is performed and logged according to FM Category Logging. Verification and evaluation logging data SHALL be linked by means of the provided transaction identifiers.

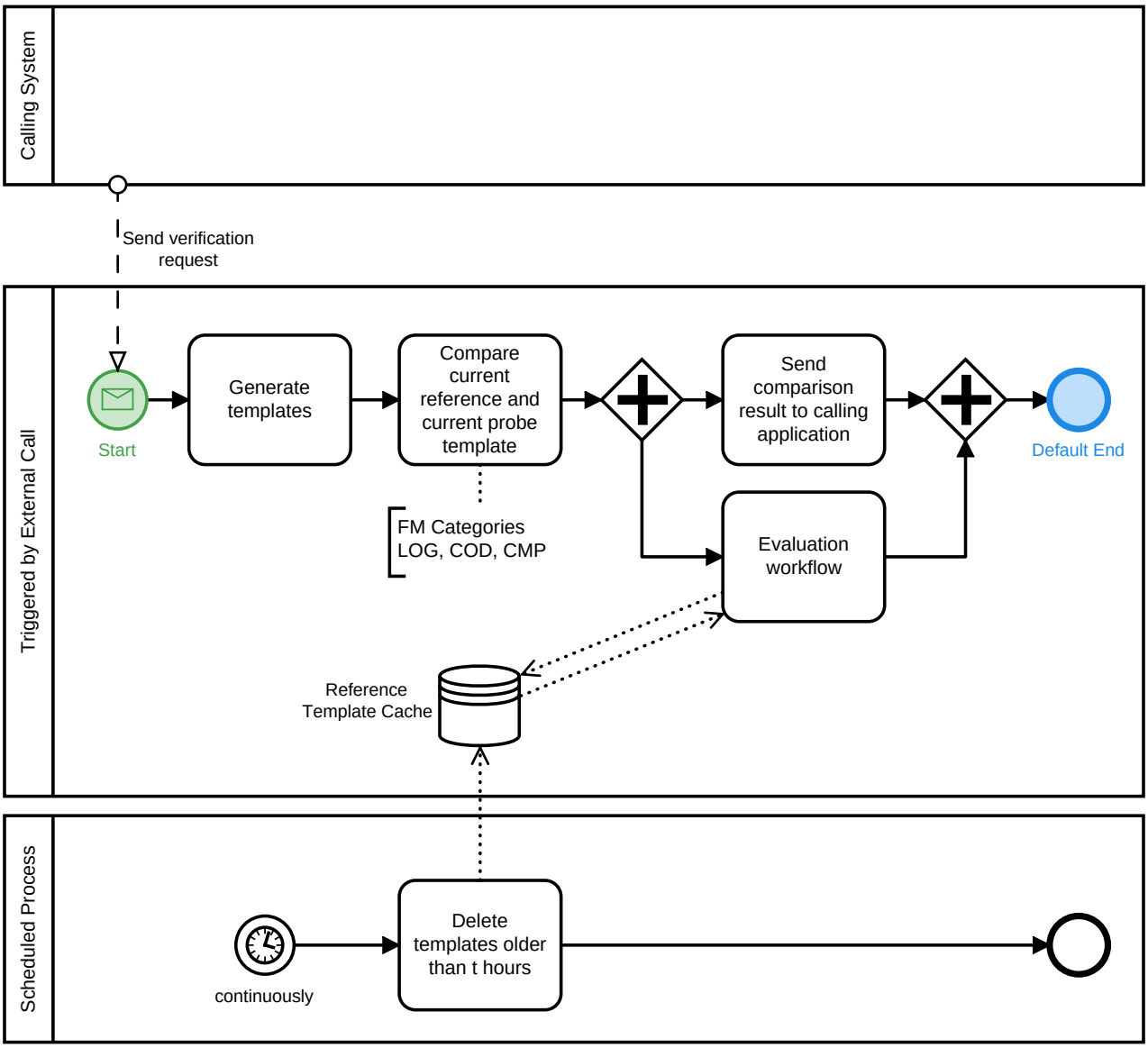

Figure 3.24. Verification Evaluation Workflow without Connected Identity Register

3.12.2.1. Evaluation Workflow

An overview over the evaluation workflow is given in ▸Figure 3.24. The evaluation workflow itself SHALL be comprised of three main tasks:

- recommended QA of the current probe and reference image
- comparison of the current probe with the current reference using an additional comparison algorithm, which was not used for the normal verification, or varying threshold profiles
- control-verifications of the current probe with non-mated reference templates

In detail, the following process SHALL be executed in the evaluation workflow for verification:

1. A probe template and the mated reference template are recieved.
2. QA for evaluation purposes MAY be conducted according to ▸FM Category Quality Assessment.

3. To enhance the quality of the calculation, measures SHOULD be taken to exclude non-mated comparisons in the evaluation. Exemplary measures are listed in ▸Section 3.10.3.3. The following steps are REQUIRED to calculate the FNMR:
   a. The current probe is compared against the current (assumed mated) reference (genuine comparison) to obtain a score. If this score is already available, e.g due to a previous comparison between both templates, this result MAY be reused if the algorithms coincided. In particular for the calculation of a Detection-Error-Tradeoff curve, where the threshold profile is the only varying parameter, scores need to be obtained just once for each probe-template-pair.
   b. If the score is below the threshold profile under evaluation, the amount of non-matches ($\bar{M}$) is counted up.
   c. The amount of total comparisons (N_{FNMR}) is counted up.
   d. In addition to the setup of the standard verification workflow, other comparison algorithms and/or other threshold profiles SHALL be evaluated here. Note that for each algorithm (or deviating threshold profile), the non-matches SHALL be counted separately.
   e. The FNMR based on the yet evaluated data can be calculated for each setup according to ▸Equation 3.6.
4. It is RECOMMENDED to take measures to exclude mated comparisons in the following evaluation steps (e.g. in analogy to ▸Section 3.10.3.3) as the current probe template from the verification process is assumed to be compared against non-mated reference templates (imposter comparisons) to calculate the FMR as follows:
   a. Comparisons of the current probe with a sufficiently large amount of n templates in a pool of cached non-mated references are conducted without respect to similiar attributes (zero effort). The pool SHALL NOT contain the mated reference to the probe or multiple references of the same biometric subject.
   b. For each comparison, N_{FMR} is increased by 1.
   c. For each comparison score exceeding the current threshold profile under evaluation, the (false) match counter $|M|$ is increased by 1. As all templates without restriction are used, these are the "zero-effort"-counts.
   d. The FMRs for probe-reference-pairs coinciding in certain attributes MAY be accessed by separated counts for matches and comparisons when one of the following attributes coincides:
      i. Age groups
      ii. Sex
      iii. Nationality
      iv. Document Issuer of Identity Document

      Additional attributes MAY be evaluated.
   e. The cache is updated:
      - The reference mated to the current probe SHALL be added to the cache after the imposter comparisons. It SHALL be ensured, that no reference of this biometric subject is already contained in the cache, e.g. by using the alphanumeric data from the identity document corresponding to the images.
      - The oldest reference in the cache SHALL be deleted, if more than n references are currently stored in the cache. This maximum amount n of references in the cache SHALL be configurable.
      - Additionally, cached references SHALL be deleted after a configurable time t in accordance with the applicable data protection regulations.
   f. The FMRs for the zero-effort and all attributes based on the yet evaluated data can be calculated according to ▸Equation 3.8.

5. The results are logged according to ▸FM Category Coding and ▸FM Category Logging.

3.12.2.2. Optional Measures to Enhance the Quality of the Evaluation

For the assumptions made above to calculate the error rates, it is essential to ensure, that the correct mated reference template is (or is not) contained in the pool of reference templates. Following implementations MAY be used to achieve this goal:

- For the accuracy evaluation of identifications or verifications using only one biometric modality, a preceding verification based on another biometric modality could give insight about the true nature (mated or non-mated) of the relation between probe and reference. As false-non-matches (or respectively false-matches) for different biometric modalities are independent, this does not introduce a bias. This is only possible if more biometric modalities are transmitted for the probe and are available for the references than required for the evaluation. Additionally, it MUST be ensured that the accuracy provided by verification of another modality is sufficiently high to prevent from introducing errors.
- Further insight about the true nature (mated or non-mated) of the relation between probe and reference can be obtained by operator decisions from the main-workflow. Any non-match appearing during the border control process will require further inspection by an operator. The final decision entered by the operator can be used as additional information. If the operator ends this inspection by deciding on a true-non-match, the probe-reference pair SHOULD be excluded in evaluation workflows requiring mated pairs. Thus, the evaluation workflow itself will still be completely automatic, though its start SHALL be delayed until the main border control process is terminated, see ▸Figure 3.19.

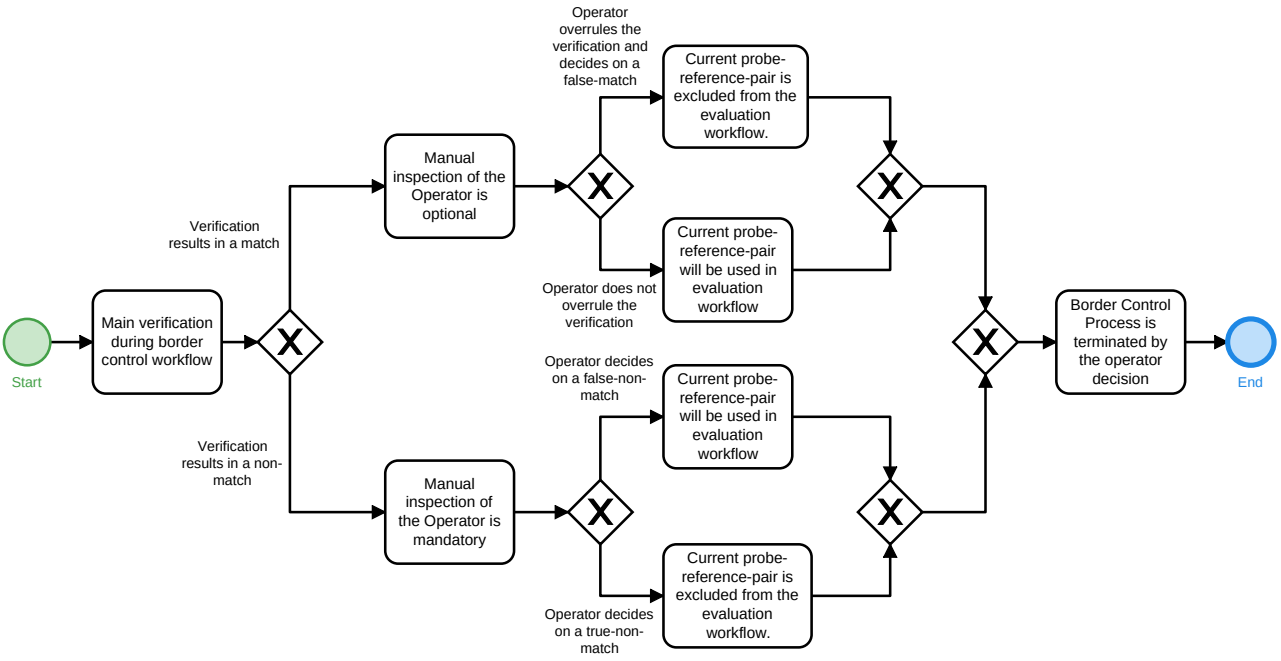

Figure 3.25. Use of Operator Decisions as a Background Filter

3.13. PAP UPD-B-EES-1: Update EES Reference Biometrics

This PAP it not used yet and is only part of this TR due to temporary reasons.

▸Figure 3.26 depicts the update process of reference biometrics in a CIR (here: CS EES) by live acquired images. Note, that the ▸PAP Task UPD-FP-EES-1: EES Biometric Update Fingerprints and ▸Section 3.13.1 are used here.

The process specified here SHALL only be executed if all prior verifications of the biometric subject were successful or, if a verification failed, an operator has qualified the prior verification result as false non-match.

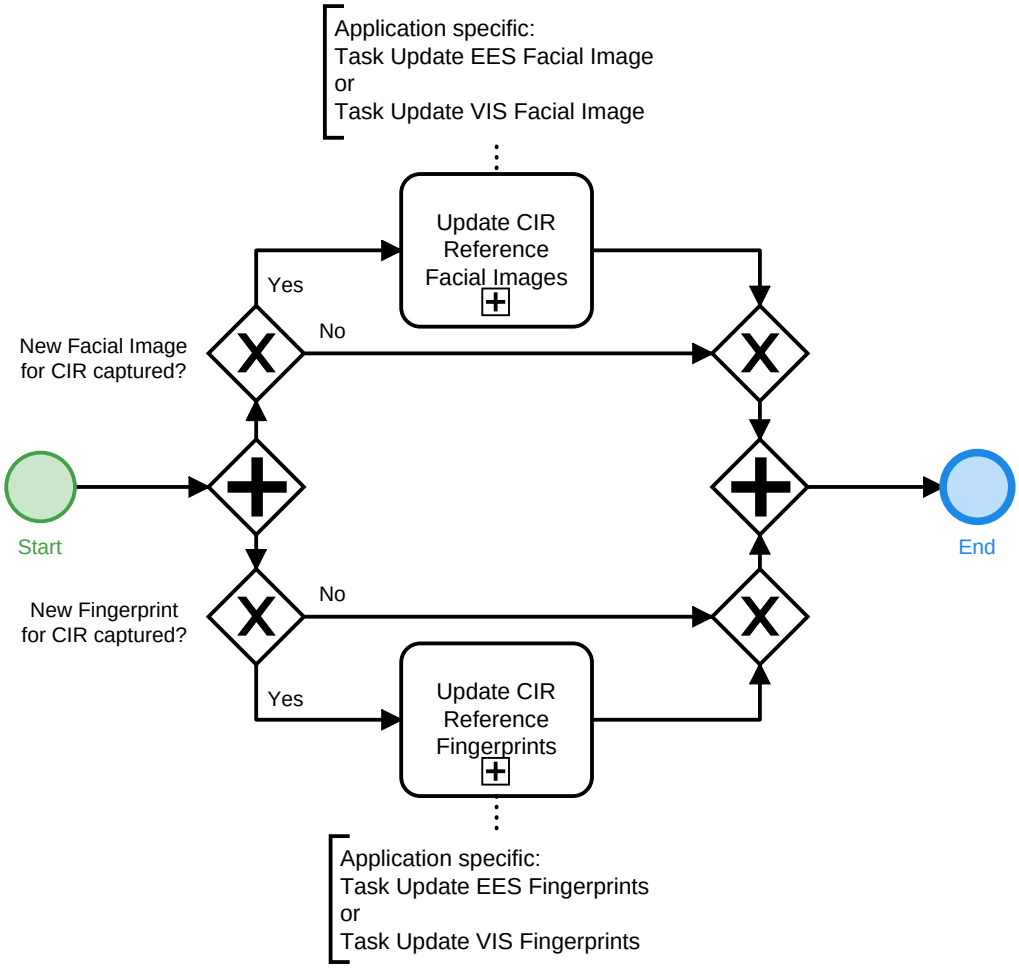

Figure 3.26. Partial Application Process "Update CIR Reference Biometrics"

3.13.1. PAP Task UPD-FI-EES-1: EES Biometric Update Facial Images

▸Figure 3.27 depicts the update process of reference facial images in the CS EES by live acquired facial images.

For the process decision of expired Entry-Exit System (EES) reference facial images, the following rule SHALL be applied. An EES reference facial image SHALL be considered as expired if one of the following statements hold true for the EES reference facial image:

- if the age of biometric subject was *less than or equal to 12 years* at the create timestamps of the EES reference facial image and the time range between the EES reference facial image create timestamps and the current date is *greater than 1 year*
- if the age of biometric subject was *greater than 12 years* at the create timestamps of the EES reference facial image and the time range between the EES reference image create timestamps and the current date is *greater than 3 years*

For the process decision of whether the EES reference facial images is superior in terms of quality to the live facial image, the ▸FM QA-FI-GENERIC and ▸FM QA-FI-BCL SHALL be applied.

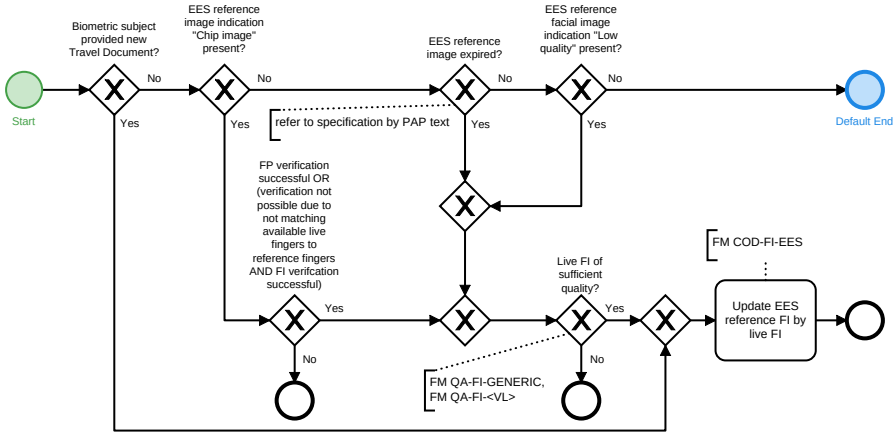

Figure 3.27. Partial Application Process Task "EES Biometric Update Facial Images"

3.13.2. PAP Task UPD-FP-EES-1: EES Biometric Update Fingerprints

Figure 3.28 depicts the update process of reference fingerprints in the CS EES by live acquired fingerprints.

For the decision on the conditions and fingerprint update actions, the process in Figure 3.28 SHALL be applied.

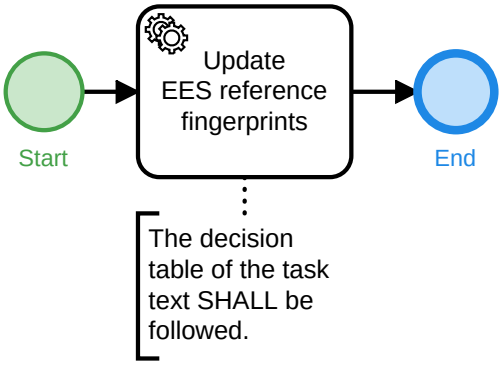

Figure 3.28. Partial Application Process Task "EES Biometric Update Fingerprints"

An update of EES reference fingerprint SHALL be conducted according to Table 3.2. In addition, a reasoning for the specified update rules will be amended in a next version of this Technical Guideline.

Note, that the following constraints have to be met by the update rules from a legislative point of view:

- Right and left hand fingerprint images SHALL never be stored simultaneously in the CS EES.
- If at least one finger of the right hand is available, the right hand slap SHALL be used, even if only one finger is available and four fingers of the left hand would be available.
- A "best of" slap SHALL NOT be created, i.e. a slap stored with single fingers acquired in different acquisition processes.

In addition, the following constraint is set:

- The quality of a fingerprint image is considered as sufficient if the quality score of the relevant finger excels a threshold. Update of fingerprints above the threshold SHALL NOT affect the update rules.
- As many fingerprint images as possible of suitable quality SHALL be enrolled in the EES.
- Information about the status of the missing fingers SHOULD be as accurate as possible.

For the decision whether the EES reference fingerprints are of better quality compared to the live fingerprint, the ▸FM QA-FP-APP SHALL be applied.

<table>
<tr><td></td><td></td><td></td><td colspan="4">Right Hand Fingerprints</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">no fingerprint stored in EES</td><td colspan="2">at least one fingerprint stored in EES</td></tr>
<tr><td></td><td></td><td></td><td>at least one live fingerprint available[12]</td><td>no live fingerprint available</td><td>at least one live fingerprint available[13]</td><td>no live fingerprint available</td></tr>
<tr><td rowspan="2">Left Hand Fingerprints</td><td rowspan="2">no fingerprint stored in EES</td><td>at least one live fingerprint available</td><td rowspan="2">1. add live right fingers to EES Traveller File</td><td>2.
• update EES reference right fingers' missing reason
• add live left fingers to EES Traveller File</td><td rowspan="2">3. if more live right fingers are available than EES Traveller File right fingers OR (the bad quality flag for any EES Traveller File right fingers is set AND the same live right finger as bad quality EES Traveller File fingers are available AND all live right fingers are of better or same quality than the EES Traveller File right fingers AND not less live right hand fingerprints are available than EES Traveller File right fingers): replace EES Traveller File right fingers by live right fingers</td><td>4.
• delete EES Traveller File right fingers and add live right fingers' missing reason
• add live left fingers to EES Traveller File</td></tr>
<tr><td>no live fingerprint available</td><td>5.
• update EES Traveller File right fingers' missing reason
• update EES Traveller File left fingers' missing reason</td><td>6. if all live right fingers marked as permanently missing: delete EES Traveller File right fingers and add live left fingers' missing reason.</td></tr>
</table>

[12] Note, if no EES reference fingerprint is stored and at least one right live fingerprint is available, the acquisition of a left hand fingerprint SHALL NOT happen as it is not required for any purpose. Thus, no distinction between the case of *at least one live fingerprint available* and *no live fingerprint available* for left hand fingerprints is required

[13] Note, if at least one right EES reference fingerprint is stored and at least one right live fingerprint is available, the acquisition of a left hand fingerprint SHALL NOT happen as it is not required for any purpose. Thus, no distinction between the case of *at least one live fingerprint available* and *no live fingerprint available* for left hand fingerprints is required

			Right Hand Fingerprints			
			no fingerprint stored in EES		**at least one fingerprint stored in EES**	
			at least one live fingerprint available[12]	**no live fingerprint available**	**at least one live fingerprint available[13]**	**no live fingerprint available**
	at least one fingerprint stored in EES	at least one live fingerprint available	7. • delete EES Traveller File left fingers • add live right fingers to EES Traveller File	8. • update EES Traveller File right fingers' missing reasons • do number 3 with live left hand fingerprints and left EES Traveller File fingers instead	By EU-regulation, CS EES never stores left and right hand fingerprints at the same time.	
		no live fingerprint available		9. • update EES Traveller File right fingers' missing reason • if all live left fingers marked as permanently missing: delete EES Traveller File left fingers and add live left fingers' missing reason		

Table 3.2 Decision Table EES Reference Fingerprint Update

3.13.2.1. Annotations to Decision ▸Table 3.2

The following annotations explain the reasoning behind the decision table. Each annotation refers to the cell of the decision table by its number.

1. If no fingerprints of the right hand are enrolled, though currently available, they SHALL be enrolled.
2. The reason for fingerprint images missing in the EES might change, e.g. from temporary missing fingers to permanently missing fingers. Therefore, an update is REQUIRED even if no fingerprint images can be acquired. If no fingerprint images of the right hand are available, the left hand SHALL be used for enrolment.

[12] Note, if no EES reference fingerprint is stored and at least one right live fingerprint is available, the acquisition of a left hand fingerprint SHALL NOT happen as it is not required for any purpose. Thus, no distinction between the case of *at least one live fingerprint available* and *no live fingerprint available* for left hand fingerprints is required

[13] Note, if at least one right EES reference fingerprint is stored and at least one right live fingerprint is available, the acquisition of a left hand fingerprint SHALL NOT happen as it is not required for any purpose. Thus, no distinction between the case of *at least one live fingerprint available* and *no live fingerprint available* for left hand fingerprints is required

3. Following the aim to store as many fingerprint images of sufficient quality of the right hand as possible in the EES.
4. -
5. If no fingerprint images of the right hand are available, the left hand SHALL be enrolment. As only fingerprints of one hand must be enrolled in the EES, the right hand fingerprints SHALL be deleted and the missing reasons saved.
6. If no fingerprints of any hand are currently available, an update SHALL NOT be done as it would delete the currently enrolled fingerprint images. The only exception is the case, where all fingers of the right hand are now permanently missing. In this case, the fingerprint images of the right hand SHALL be deleted in the EES, as they can no longer be used for traveller verification. In this case, at least the reasons for the missing left fingers SHALL be enrolled.
7. Following the legal requirements, that the fingers of the right hand SHALL always be enrolled if possible.
8. -
9. If no fingerprints of any hand are currently available, an update SHALL NOT be done as it would delete the currently enrolled fingerprint images. The only exception is the case, where all fingers of the left hand are now permanently missing. In this case, the fingerprint images of the left hand SHALL be deleted in the EES, as they can no longer be used for traveller verification. In this case, at least the reasons for the missing right fingers SHALL be enrolled.

4. Function Modules

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

4.1. FM Category Acquisition Hardware

Devices that are used for digitising physical, representable biometric characteristics are called Acquisition Hardware (AH). Digital cameras to capture images of the face, fingerprint sensors, or signature tablets can be named as examples.

4.1.1. FM AH-ALL-SSS

This Function Module describes the requirements for SSSs that are used to obtain digitised facial images and fingerprints.

4.1.1.1. Requirements

4.1.1.1.1. General Requirements

- An environment surveillance camera system SHALL supervise the area around the SSS.
  - The camera images SHALL allow to identify whether more than one person was in range of the SSS during the capture of the fingerprints.
  - The surveillance camera system SHALL capture an image of the surrounding area at the moment of each finger capture attempt. The face of the biometric subject using the fingerprint scanner SHALL be visible in the image of the surveillance camera.
  - The images SHALL be cached locally on the SSS.
  - A maximum of 100 ms SHALL be allowed to elapse between the fingerprint capture attempt image and the capture of the surveillance camera system.
  - For the fingerprint image selected in the acquisition process, the corresponding surveillance image SHALL be made available from the cache.
  - A colour camera SHALL be used for the environment surveillance.
  - The camera SHALL be capable to capture images with a resolution of at least 1280 x 720 pixels.
- A camera system SHALL closely supervise the fingerprint capture system.
  - The camera image is intended to identify whether presentation attack instruments are applied to the fingerprint capture system.
  - The camera system SHALL capture an image of the fingerprint acquisition area at the moment of each finger capture attempt.
  - The images SHALL be cached locally on the SSS.
  - A maximum of 100 ms SHALL be allowed to elapse between the fingerprint capture attempt image and the capture of the surveillance camera system.
  - A colour camera SHALL be used for the fingerprint capture surveillance.
  - The camera SHALL be capable to capture images with a resolution of at least 1280 x 720 pixels.

- In case the biometric subject leaves the corridor in front of the SSS system, the running SSS process SHALL be stopped. The corridor is defined by a distance of 100 cm in front of the SSS and the width of the SSS. Note, this requirement does not mandate a dedicate hardware sensor to enable the detection of leaving. The detection MAY also happen in software based on the surveillance images. In this case, the requirement does not affect any additional hardware.

4.1.1.2. Recommendations

In case the biometric subject is approaching close to the maximum allowed distance of the SSS the biometric subject SHOULD be warned.

4.1.2. FM AH-FI-BCL

This Function Module describes the requirements for systems where a digitised facial image is obtained. Note, the distance between camera system and biometric subject is defined as the geometrical optical-path length between the forehead of the biometric subject and the active camera system's optic. The optical-path MAY, for example, follow a straight line from forehead to optic, or be rerouted by using mirrors so that the biometric subject can stand closer to the device.

4.1.2.1. Requirements

- The system MAY measure the distance between the biometric subject and the camera system.
- The camera system SHALL capture images in colour.
- The system SHALL allow high quality acquisitions independently from the environmental light situation.
- The camera system SHALL at least allow to acquire facial images compliant to this Technical Guideline of biometric subject which have a body height in range of 140 cm to 200 cm if standing upright in front of the camera system.
- If the biometric subject is standing at 60 cm distance to the camera system, the minimum physical resolution of the camera system SHALL allow to crop the full frontal facial image of the biometric subject to 1600 x 1200 pixels with an allowed deviation of maximum negative 10 %.
- The camera system SHALL capture sharp full frontal images with minimized distortion of biometric subjects which
  - stand upright 40 cm to 100 cm[1] in front of the camera system and
  - look frontal.
- Biometric subjects with a distance of less than 40 cm or more than 100 cm SHALL NOT be captured.
- If the biometric subject is in the capture area of maximum 100 cm and minimum 40 cm distance to the camera system, the camera installation SHALL be able to capture an image according to the definition of "full frontal" (see [BIB_ISO_FACE]) on a hardware level. Especially an image capturing at "Frankfurt Horizon" SHALL be possible for all biometric subjects within the defined range of body height.

4.1.3. FM AH-FI-DC

This Function Module describes the requirements for facial image cameras and physical setups that are used to obtain facial images.

4.1.3.1. Requirements

- The minimum physical resolution of the camera SHALL allow a cropping of an image to 1200 x 1600 pixels without any upscaling. Note, this requirement is OPTIONAL for scenarios where only a facial verification is performed.

[1] Note, that the physical construction of the system may not allow the biometric subject to stand at the maximum distance.

- Adequate image quality to meet the requirements of [BIB_ISO_FACE] SHALL be provided.
- The physical and environmental conditions for capturing facial images, such as the positioning of the camera, proper lighting of the face and a uniform background as described in [BIB_ISO_FACE] and [BIB_ICAO_TR_Portrait_Quality] SHALL be complied with. It is RECOMMENDED to use a uniform background in grey (i.e. R=G=B) between #A1A1A1 and #E1E1E1.
- The camera system SHALL be able to capture images in colour (24 bit sRGB). Note, this requirement is OPTIONAL for scenarios where only a facial verification is performed.
- The requirements for focal length (depending on the size of the camera sensor) as described in [BIB_ICAO_TR_Portrait_Quality] (chapters 5.2.1 and 5.2.2) SHALL be complied with. Wide-angle settings MUST NOT be used.

4.1.4. FM AH-FI-EGT

This Function Module describes the requirements for e-gate scenarios where a digitised facial image is obtained.

4.1.4.1. Requirements

- The camera system SHALL cover at least a range of 140 cm to 200 cm of a person's body height (if standing in front of the camera system).
- The minimum physical resolution of the captured facial image SHALL be at least 600 x 800 pixels without any upscaling.
- The camera system SHALL be designed to be placed in the moving direction of the biometric subject (sideways attached camera units which require a rotation of the moving person SHALL NOT be used).
- Biometric subjects SHALL be captured within a typical range of at least 200 cm with sufficient sharpness and with minimized distortion of the captured face.

4.1.4.2. Recommendations

- The physical resolution of the captured facial image is RECOMMENDED to be 1200 x 1600 pixels without any upscaling.
- It is RECOMMENDED that at a distance of 70 cm before the end of the gate (typically the exit door), the necessary rotation of the person requires less than 15 degrees.

4.1.5. FM AH-FI-ICS

This Function Module describes the requirements for integrated camera systems that are used to obtain digitised facial images.

4.1.5.1. Requirements

- 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 diffuse lighting which SHALL adapt to the environmental light conditions for a uniform illumination of the biometric subject's face to ensure the capture of a well-exposed facial image; mirroring effects of glasses SHALL be avoided.
- The camera system SHALL provide a feedback screen for displaying the camera live acquisition image (digital mirror). If the biometric subject is looking straight to the feedback screen the viewing direction of the person SHALL be frontal. The feedback SHALL include guidance to help the biometric subject for correct positioning in front of the camera.
- The system SHALL allow high quality acquisitions independently from the environmental light situation that can usually be found in the environment in question.

- 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.
- The minimum physical resolution of the captured facial image SHALL be at least 1200 x 1600 pixels without any upscaling. Note, this requirement is OPTIONAL for scenarios where only a facial verification is performed.
- The camera system SHALL be able to capture images in colour (24 bit sRGB). Note, this requirement is OPTIONAL for scenarios where only a facial verification is performed.
- The requirements for focal length (depending on the size of the camera sensor) as described in [BIB_ICAO_TR_Portrait_Quality] (chapters 5.2.1 and 5.2.2) SHALL be complied with. Wide-angle settings MUST NOT be used.

4.1.6. FM AH-FI-SSS

This Function Module describes the requirements for SSS scenarios where a digitised facial image is obtained.

4.1.6.1. Requirements

The camera system SHALL NOT require the biometric subject to rotate its standing position while interacting with the graphical user interface in order to look straight to the camera system.

4.1.7. FM AH-FP-OPT

This Function Module describes the requirements for optical high quality fingerprint scanners (single finger and multi finger).

4.1.7.1. Requirements

- For the acquisition of the fingerprints, optical sensors using the principal of frustrated total reflection or direct contact (the imaging system is the sensor surface, typically separated by a transparent protection layer) according to the certification requirements of [BIB_ISO_FINGER] (especially this means a resolution of 500 ppi or 1000 ppi) SHALL be used exclusively.
- For the acquisition of the fingerprints, only devices are permitted which meet the following requirements (in analogy to [BIB_EBTS/F]). Notwithstanding, a capturing area of at minimum 16 mm width and 20 mm height is REQUIRED (deviating from table F 1 in [BIB_EBTS/F]) for single finger scanners.

4.1.7.1.1. Grey Scale Linearity

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

4.1.7.1.2. 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.

4.1.7.1.3. 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 ▸Equation 4.1 or equation ▸Equation 4.2, in both the detector's row and detector's column directions, and over any region of the scanner's field of view. CTF values computed from equations ▸Equation 4.1 and ▸Equation 4.2 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. It is NOT REQUIRED that the bar target contains the exact frequencies listed in ▸Table 4.1, 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 4.1:

- 500 ppi scanner, for f = 1.0 to 10.0 cy/mm:

$$CTF = 3.04105 \cdot 10^{-4} \cdot f^2 - 7.99095 \cdot 10^{-2} \cdot f + 1.02774 \tag{4.1}$$

- 1000 ppi scanner, for f = 1.0 to 20.0 cy/mm:

$$CTF = -1.85487 \cdot 10^{-5} \cdot f^3 + 1.41666 \cdot 10^{-3} \cdot f^2 - 5.73701 \cdot 10^{-2} \cdot f + 1.01341 \tag{4.2}$$

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).

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

Frequency [cy/mm]	Minimum Modulation for 500 ppi scanners	Minimum Modulation for 1000 ppi scanners	Maximum Modulation
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 4.1 Minimum and Maximum Modulation

4.1.7.1.4. Signal-to-Noise Ratio and the Grey–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 grey level uniformity is defined for the three following cases:

- Adjacent row, column uniformity: At least 99 % of the average grey 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 grey levels when scanning a uniform low reflectance target, and SHALL NOT differ by more than 2.0 grey 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, individual pixel's grey level SHALL NOT vary from the average by more than 22.0 grey levels, when scanning a uniform high reflectance target, and SHALL NOT vary from the average by more than 8.0 grey 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 grey levels of the two areas SHALL NOT differ by more than 12.0 grey levels when scanning a uniform high reflectance target, and SHALL NOT differ by more than 3.0 grey levels when scanning a uniform low reflectance target.

4.1.7.1.5. Grey Scale Range of Fingerprint Images

A fingerprint scanner operating at 500 ppi or 1000 ppi, SHALL 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 flat 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 grey values with at least 5 Pixels in this image are counted. The histogram SHALL show no break and no other artefact. At least 80 % of the captured individual fingerprint images SHALL have a grey scale dynamic range of at least 200 grey levels, and at least 99% SHALL have a dynamic range of at least 128 grey levels.

4.1.8. FM AH-FP-SSS

This Function Module describes the requirements for SSS scenarios where digitised fingerprints are obtained.

4.1.8.1. Requirements

- The spatial configuration of the fingerprint acquisition system SHALL be optimal for primary right hand acquisition.
- The spatial configuration of the fingerprint acquisition system SHALL allow the acquisition of left hands.

- During the fingerprint acquisition process multiple persons within the reach of the fingerprint acquisition system of the SSS SHALL be detected.
- The multiple person detection result SHALL be cached locally on the SSS.

4.1.8.2. Recommendation

Measures SHOULD be taken to make the fingerprint acquisition system apparent to the biometric subject as the active part of the SSS to interact with in the moment where an acquisition of fingerprints is foreseen.

4.2. FM Category Acquisition Software

The Function Module category Acquisition Software (AS) contains all functionality regarding image processing for biometric purposes. Therefore, these Function Modules 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.

4.2.1. FM AS-FI-DC

This Function Module describes the requirements and interfaces for acquisition software used for facial image cameras in order to obtain digitised images.

4.2.1.1. Requirements

- In regard to the application scenario an adequate resolution of the camera SHALL be chosen to acquire a facial image of at least 1200 x 1600 pixels with an inter eye distance of at least 120 pixels.
- The images SHALL be captured and stored in colour (24 bit sRGB). Note, this requirement is OPTIONAL for scenarios where only a facial verification is performed.
- In normal mode of operation, no compression artefacts SHALL be detectable in the image.

4.2.1.2. Recommendations

- The image data SHOULD be provided without any compression or with lossless compression. If the acquisition device does not support a lossless mode, the image MAY alternatively be provided with the minimal level of compression possible.
- Acquisition software that supports calibration procedures for the respective digital camera SHOULD be used (in particular colour management).

4.2.2. FM AS-FI-ICS

This Function Module describes the requirements and interfaces for acquisition software used for integrated camera systems in order to obtain digitised facial images.

4.2.2.1. Requirements

- The acquisition software of the camera system SHALL provide uncompressed image data for further processing.
- The selected resolution within the camera settings (e.g. configurable via camera firmware SHALL be at least 1200 x 1600 pixels. Note, this requirement is OPTIONAL for scenarios where only a facial verification is performed.
- The integrated camera system SHALL have the diffuse lighting activated within software.
- The capture of images in colour (24 bit sRGB) SHALL be selected. Note, this requirement is OPTIONAL for scenarios where only a facial verification is performed.

4.2.3. FM AS-FI-ICS3

This Function Module describes the requirements and interfaces for acquisition software used for integrated camera systems in order to obtain digitised facial images.

4.2.3.1. Requirements

- The acquisition software of the camera system SHALL detect whether multiple faces are presented to the camera system simultaneously in the capture area.
- The acquisition software of the camera system SHALL detect whether a face which is presented to the camera system completely leaves the capture area. The process SHALL then terminate after a configurable timeout.

4.2.4. FM AS-FP-MF

This Function Module describes the requirements and interfaces for acquisition software for multi finger scanners.

4.2.4.1. Requirements

- The image provided by acquisition software SHALL meet the criteria of fingerprints as described in [BIB_ISO_FINGER]. The requirements according to the certification requirements of [BIB_ISO_FINGER] SHALL be met.
- For the acquisition process, a pre-qualification of the fingerprints to prefer high quality SHALL be used. The activation of the acquisition SHALL occur automatically. The capture SHOULD prefer the highest quality image of a sequence.
- This functionality MAY be part of the hardware firmware and MAY NOT be available as separate software component.
- The thresholds of the pre-qualification for performing a capture SHALL be documented by the vendor.
- If the acquisition software allows multiple thresholds for pre-qualification, it SHALL be configurable by the system administrator.
- In case further requirements demand for an export of the uncompressed fingerprint image data BMP SHALL be used as image format.

4.2.4.2. Recommendations

In order to prevent unwanted duplicate acquisitions of the same fingers or slaps, the software SHOULD start the acquisition process not before the fingers from a previous acquisition have been removed from the sensor surface.

4.2.5. FM AS-FP-SF

This Function Module describes the requirements and interfaces for acquisition software for single finger scanners.

4.2.5.1. Requirements

- The image provided by acquisition software SHALL meet the criteria of fingerprints as described in [BIB_ISO_FINGER]. The requirements according to the certification requirements of [BIB_ISO_FINGER] SHALL be met.
- For the acquisition process, a pre-qualification of the fingerprints to prefer high quality SHALL be used. The activation of the acquisition SHALL occur automatically. The capture SHOULD prefer the highest quality image of a sequence. This functionality MAY be part of the hardware firmware and MAY NOT be available as separate software component.

- The thresholds of the pre-qualification for performing a capture SHALL be documented by the vendor.
- If the acquisition software allows multiple thresholds for pre-qualification, it SHALL be configurable by the system administrator.
- In case further requirements demand for an export of the uncompressed fingerprint image data BMP SHALL be used as image format.

4.2.5.2. Recommendations

In order to prevent unwanted duplicate acquisitions of the same finger, the software SHOULD start the acquisition process not before the finger from a previous acquisition has been removed from the sensor surface.

4.2.6. FM AS-FP-SLP

This Function Module describes the requirements and interfaces for acquisition software for four finger slap scanners running in slap acquisition mode.

4.2.6.1. Requirements

- It SHALL be classified by software whether the left or right hand slap has been acquired. Thumb slap classification is NOT REQUIRED. This MAY be achieved by using the acquired fingerprint images or with the help of further sensors or images (e.g. surveillance) if available.
- The classification SHALL have a performance of at least 99% i.e. 99% of all left hand slaps SHALL be correctly classified as left hand slaps and 99% of all right hand slaps SHALL be correctly classified as right hand slaps.
- In case the classification can return more than two possible results, e.g. "left", "right", or "unknown", a classification threshold SHALL be configurable.
- It SHALL be configurable to switch the classification off or to only use the classification result information for evaluation purposes.

4.3. FM Category Biometric Image Processing

The Function Module Biometric Image Processing (BIP) 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 biometric characteristics is addressed here.

4.3.1. FM BIP-FI-APP

This Function Module 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.

4.3.1.1. Requirements

- The colour depth SHALL be 24 bit sRGB. Note, this requirement is OPTIONAL for scenarios where only a facial verification is performed.
- The face SHALL be fully visible in the foreground of the provided image.
- The minimum distance between both eyes for capture positions of the biometric subject in the preferred area of the camera range SHALL be 120 pixels.
- The face SHALL be cropped and de-rotated from the overall scene in the captured image. Post processing of the image orientation in regard to pitch and jaw (see [BIB_ISO_FACE]) SHALL NOT be done.
- The size of the face within the image SHALL be according to the geometric requirements of [BIB_ISO_FACE] and QA category of this TR.

4.3.2. FM BIP-FP-APP

This Function Module 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.

4.3.2.1. Requirements

- The resolution of the fingerprint image has to be 500 ppi or 1000 ppi corresponding to the certification requirements of [BIB_ISO_FINGER] and, therefore, MAY differ from the scan resolution.
- Depending on the call, as many individual fingerprints as requested SHALL be extracted from the input image and provided as single fingerprints.

  Note: Segmentation for single finger scanners is OPTIONAL.

  For this segmentation process, the following requirements SHALL be fulfilled:

  - ability to accept fingerprints which are rotated in the same direction up to 45 degrees
  - in the same direction rotated fingerprints have to be corrected to be vertical
  - segment the first part over the finger (fingertip)
  - segmentation has to occur on uncompressed data
- Fingerprint images SHALL NOT be upscaled. If the targeted system or database requires fingerprint images of higher size than captured the fingerprint image SHALL be evenly surrounded with white pixels to reach the desired size.

4.4. FM Category Quality Assessment

The Function Module Quality Assessment 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.

4.4.1. FM QA-FI-GENERIC

This Function Module describes requirements and interfaces for software that is used for quality assessment of digital images to ensure compliance with [BIB_ISO_FACE].

4.4.1.1. Requirements

4.4.1.1.1. General Requirements

The QA module is used for the software-based automatic check of the conformance of the picture to [BIB_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 [BIB_ISO_FACE] hierarchically describes requirements for the facial images. In the following, full frontal images are expected.

The QA module SHALL analyse and evaluate all of the quality criteria listed in ▸Table 4.2. For the criteria marked with "M", the quality values SHALL 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 SHALL reject or approve the picture. The total result is true if every single quality criteria is fulfilled.

The 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. The image type to process depends on the image type requirements of the application profile to implement.

The QA module SHOULD operate on cropped images retrieved from the image processing according to ▸FM Category Biometric Image Processing.

ID	Criterion	ISO-Ref., compare [BIB_ISO_FACE]	Mandatory / Optional	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
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

ID	Criterion	ISO-Ref., compare [BIB_ISO_FACE]	Mandatory / Optional	Unit/Range
Photographic requirements				
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	According to [BIB_ISO_FACE] using Decimal notation (e.g. "1" for RGB-24bit, "2" for YUV422 or "3" for 8bit-grey scale and "0" for *unknown* or errors)
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

Table 4.2 Mapping of Relevant Quality Criteria

4.4.1.1.2. Identification of the Best Capture

When multiple facial images and their corresponding set of quality metrics are present, the best capture of the list SHALL be identified in an automated manner as described in the following[2]:

1. If exactly one facial image conforms to more mandatory criteria than all other images, this image is chosen.
2. If more than one facial image is conform to more mandatory criteria than all other facial images, the facial image fulfilling the most optional criteria SHALL be chosen.
3. If more than one facial image is conform to more mandatory and optional criteria than all other facial images, the most recent facial image within this selection SHALL be chosen. If no timestamp is available, a random selection MAY be applied among the facial images fulfilling the most criteria.

4.4.2. FM QA-FI-BCL

This Function Module describes requirements and interfaces for software that is used for quality assessment of digital images within the context of border control to ensure compliance with [BIB_ISO_FACE].

4.4.2.1. Requirements

The threshold requirements of ▸Table 4.3 SHALL be in place within the context of border control. These thresholds relate to the generic quality criteria of ▸FM QA-FI-GENERIC.

ID	Criterion	Minimum	Maximum	Unit/Range
1.1	Yaw, neck axis	-5	5	Degrees
1.2	Pitch, ear axis	-5	5	Degrees
1.3	Roll, nose axis	-8	8	Degrees
5.1	Image height	800	1600	In pixel
5.2	Image width	600	1200	In pixel
5.3	Ratio: Head width / image width	0,5	0,75	As ratio between 0 and 1
5.4	Ratio: Head height / image height	0,6	0,9	As ratio between 0 and 1

[2] Note that this is a description of the automated selection of the best capture among a list of facial images. Operators may always decide otherwise during the process (veto).

ID	Criterion	Minimum	Maximum	Unit/Range
5.5	Vertical position of the face	0,3	0,5	As ratio between 0 and 1
5.6	Horizontally centred face	0,45	0,55	As ratio between 0 and 1
5.7	Eye distance	120	-	In pixel

Table 4.3 Quality Threshold Requirements for Facial Images for Border Control

4.4.3. FM QA-FI-PRE

This Function Module describes quality requirements for a digital live facial image that is used for automated face recognition (pre-qualification).

4.4.3.1. Requirements

- Pre-qualification of captured live facial images from the acquisition stream SHALL be used. Images SHALL be ranked according to the conducted pre-qualification and passed to the subsequent stage as indicated by the rank.
- Pre-qualification SHALL be conducted at least according to the following criteria, refer to [BIB_ISO_FACE]:
  - pose of the head
  - illumination of the face
  - position of the eyes
- The pre-qualification result SHALL depend only on the provided live-captured facial image. In particular, the pre-qualification SHALL be independet of any other biometric sample that might be extracted from other sources, e.g. eMRTD, etc.

4.4.4. FM QA-FP-APP

This Function Module describes requirements for the quality assessment of plain or rolled fingerprints including quality assessment of single fingerprint, respectively slap and selection of the best quality image out of multiple instances.

4.4.4.1. Requirements

4.4.4.1.1. Quality Algorithm

As quality algorithm, the latest version of NIST Fingerprint Image Quality 2.2 (NFIQ2.2) [BIB_NFIQ2.2] SHALL be used, and therefore, images with 1000 ppi SHALL be resampled to 500 ppi before application of NFIQ2.2. Note, that the resampled image SHALL be used for NFIQ2.2 only. As resulting quality value, the output value of NFIQ2.2 in the integer range of [0,100] SHALL be used. In the case of failure, the returned error code 255 indicates that a computation was not successful and the resulting quality value SHALL be returned as the result, as described in ▸Section 4.11.1.

4.4.4.1.2. Quality Evaluation Process for a Slap or Single Fingerprint

In case a single captured fingerprint, respectively slap is passed, the QA SHALL be performed as described in the following. Beforehand, the fingerprints of the passed capture SHALL be segmented (considering missing fingers). Note, that in verification applications, a QA is not conducted. Thus, every slap capture is considered sufficient and no thresholds are specified here. Skipping the QA is expected to accelerate the overall process. OPTIONALLY, a QA can be performed.

1. For each segmented fingerprint $F_{A,j}$ of a passed capture A, a quality value $Q_{A,j}$ is calculated with $j \in 1, ..., 10$ (up to 4 fingers in one slap) representing the specific finger code according to [BIB_ISO_FINGER].

2. The resulting quality value is compared with the defined threshold TH_j for this finger. The application specific thresholds as defined in the following section apply.
3. In case all of the fingerprint qualities reach the specified threshold (i.e. $\forall j, Q_{A,j} \geq TH_j$), the boolean information $b = 1$ indicates a successful capture.
4. In case one or more fingerprints do not reach the threshold (i.e. $\exists j, Q_{A,j} < TH_j$), the boolean information $b = 0$ indicates insufficient quality of the capture.
5. For the segmented fingerprint $F_{A,j}$ the corresponding parameter set $P_{A,j}$ is compiled and returned.
6. As a result of the QA process, the following values are returned to the calling process:
   a. the boolean information b
   b. the parameter set $P_A = Q_{A,j}, ..., Q_{A,l}$ with $j, l \in 1, ..., 10$ representing the specific finger code

4.4.4.1.3. Identification of the Best Capture out of Multiple Captures

When multiple captures $A_i, i \in 1, ..., n$ and their corresponding set of segmented fingerprints $F_{A_i,j}$ with $j \in 1, ..., 10$ representing the specific finger code according to [BIB_ISO_FINGER] are passed, the best of the captures SHALL be identified as described in the following section:

1. For each segmented fingerprint $F_{A_i,j}$ of a passed capture A_i, the quality value $Q_{A_i,j}$ is calculated with representing the specific finger code according to [BIB_ISO_FINGER].
2. The captures are ranked according to the quality values of the fingerprints according to the following (lexicographical) order. The highest ranked capture is considered as the capture yielding the best quality.
   a. for left/right four-finger slaps, the order is as follows:
      i. index finger (highest priority)
      ii. middle finger
      iii. ring finger
      iv. little finger (lowest priority)

      Example 1: Two Slaps of a right hand. Middle finger, ring finger and little finger of the first slap have a better quality than the middle finger, ring finger and little finger of the second slap, but the quality of the index finger is better in the second slap. Consequently, the second slap SHALL be taken.

      Example 2: Three Slaps of a left hand. The quality of the index finger and the middle finger is the same in all three slaps, but the quality of the ring finger is better in the first slap. So the first slap SHALL be taken, no matter how high or low the quality of the little finger is in any slap.
   b. for thumb slaps, the order is as follows:
      i. right thumb (highest priority)
      ii. left thumb (lowest priority)
   c. for index finger slaps:
      i. In contrast to the other two slap types, the best capture of index finger slaps is a set of the best captures of each index finger as indicated by the following two options.

         If each index finger yields sufficient quality in at least one of the already conducted captures, the index fingers of sufficient quality are accepted and the total index finger slap capture is considered as of sufficient quality.

If not both index fingers yield at least once sufficient quality in a capture, the best image for each index finger is returned as the best capture and the slap captured is considered as of insufficient quality.

ii. If for a single slap both index fingers yield to sufficient quality, those two index fingers SHALL be selected even if an index finger of another slap yield to better quality.

d. for rolled single finger captures:

i. Of the set of captured images obtained in the process beforehand, which are not annotated by a hardware reported issue, the capture with the highest quality value is considered as the best image.

ii. If the set of captured images obtained in the process beforehand on does only contain images which are annotated by hardware reported issues, the capture with the highest quality value of the entire set is considered as the best image.

iii. In case several captures yield to the same highest quality value, the last (temporal) of highest quality captures is considered as the best image.

3. As a result of the QA process, the following values are returned:

a. the identifier i representing the capture yielding the best quality

b. the parameter set $P_A = Q_{A_{i,j}}, Q_{A_{i,l}}$ with $j, l \in 1, ...10$.

4.4.4.1.4. Thresholds for Plain Fingerprints for Enrolment Purposes

The following thresholds as indicated in ▸Table 4.4 apply when fingerprints are captured plain for enrolment purposes. Note, the thresholds in ▸Table 4.4 do not apply to plain captured fingerprint in enrolment scenarios where the plain fingerprints are captured for control purpose of rolled fingerprints. In that case, thresholds as indicated in ▸Table 4.5 apply for the plain fingerprints.

Finger Position	Finger Code	NFIQ2.2 Threshold
Right thumb	1	30
Right index finger	2	30
Right middle finger	3	20
Right ring finger	4	10
Right little finger	5	10
Left thumb	6	30
Left index finger	7	30
Left middle finger	8	20
Left ring finger	9	10
Left little finger	10	10

Table 4.4 Thresholds for Plain Fingerprints for Enrolment Purposes

4.4.4.1.5. Thresholds for Plain Control Fingerprints and Fingerprints used for Identification Searches

The following thresholds as indicated in ▸Table 4.5 apply when fingerprints are captured plain for the purpose of control slaps (used for comparison with rolled prints) or for use in identification searches. Note, the thresholds in ▸Table 4.5 do apply to plain captured fingerprint in enrolment scenarios where the plain fingerprints are captured for control purpose of rolled fingerprints.

Finger Position	Finger Code	NFIQ2.2 Threshold
Right thumb	1	20
Right index finger	2	20
Right middle finger	3	20
Right ring finger	4	10
Right little finger	5	10
Left thumb	6	20
Left index finger	7	20
Left middle finger	8	20
Left ring finger	9	10
Left little finger	10	10

Table 4.5 Thresholds for Plain Control /Identification Fingerprints

4.4.4.1.6. Thresholds for Rolled Fingerprints

The following thresholds as indicated in ▸Table 4.6 apply when fingerprints are captured rolled for enrolment purposes.

Finger Position	Finger Code	NFIQ2.2 Threshold
Right thumb	1	20
Right index finger	2	15
Right middle finger	3	15
Right ring finger	4	10
Right little finger	5	5
Left thumb	6	20
Left index finger	7	15
Left middle finger	8	15
Left ring finger	9	10
Left little finger	10	5

Table 4.6 Thresholds for Rolled Fingerprints

4.5. FM Category Presentation Attack Detection

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

4.5.1. FM PAD-FI-APP

This Function Module describes requirements for PAD in the context of the acquisition of facial images. This Function Module is especially relevant for use cases where no direct observation of the acquisition process by an operator is possible (e.g. in SSS scenarios).

4.5.1.1. Requirements

4.5.1.1.1. General Requirements

The capture subsystem SHALL contain a PAD 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 PAD subsystem MAY consist of hardware and software (e.g. the used camera system MAY have additional sensors designed for this purpose).

The PAD subsystem SHALL be able to detect different artefact classes listed in the following:

- Complete artefacts (covering the whole or nearly the whole face of the attacker), either built from one piece or from multiple pieces.
- Partial artefacts (covering only parts of the attacker's face, such as artefacts covering the chin only), either built from one piece or from multiple pieces.

The PAD subsystem SHALL be able to detect all well-known artefact material types listed in the following:

- Photographs printed on paper with different thicknesses and structures of paper and different structures of printing (colouring, etc.).
- Photographs displayed on electronic devices (e.g. phones, tablets, laptops, etc.) where different methods of displaying might be used.
- Videos displayed on electronic devices, especially showing motion of the biometric subject.
- Photographs printed on fabrics with different thicknesses and structures of the fabrics and different methods of printing (flock print, silk screening, etc.).
- 3D masks in big (size of a face) and small (smaller than a normal face) sizes and different thicknesses based on,
  - Paper
  - Casted silicon
  - 3D-printer
  - Latex

On top of the listed attack classes and materials, additional attack classes MAY be detected by the PAD subsystem:

- Makeup (normal or professional)
- Additional artefacts beyond the imitation of faces, such as glasses etc.

Under optimal testing conditions, the PAD subsystem SHALL feature a false-alarm-rate of 2% maximum when tested with bona fide biometric subjects. This rate is monitored via logfiles analysis within the operational environment. If this rate is significantly exceeded, any certification that may have been issued might be re-evaluated (depending on application context)[3].

Also, the detection subsystem SHALL be adequate to the usage setting in correspondence with the security requirements in question. The performance MAY be described by a risk analysis for every considered attack type. The current version of [BIB_ISO_PAD_3] SHALL be taken into account.

4.5.1.1.2. Integration Requirements

The PAD 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 PAD score to

[3] Note that during certification a relaxed false-alarm-rate is tested. The requirement of the rate specified in this Function Module is tested on operational collected data only.

the calling application. The score SHALL be a normalized `double` in the range [0,1] using at least ten uniformly distributed interim values, where 0 indicates bona fide and 1 presentation attack. A binary score SHALL NOT be used (e.g. True or False, 1 or 0). Detailed information about the PAD (results) SHALL be logged as described in ▸Section 4.12. The technical information including the result value and description of the mapping between technical result and interpretation SHALL be stored additionally, if they are provided.

Even if the Function Module is used within a comparison scenario, the detection result SHALL be signalled in any case, independent from any biometric comparison score. Also, the omission of the detection result SHALL be signalled in any case.

The PAD result SHALL correspond to the chosen facial image.

Note that a facial image SHALL be taken independently of a possible PAD alarm.

4.5.1.1.3. Maintenance Requirements

As new technologies and new attack mechanisms are developed over time, the PAD subsystem SHALL be regularly updated and re-evaluated.

4.5.1.1.4. Certification Requirements

To ensure comparable performance of presentation attack detection subsystems, the system SHALL be certified

- either under the Common Criteria Agreement according to the Protection Profile "BSI-CC-PP-0118-2022: Common Criteria Protection Profile - Biometric Mechanisms Protection Profile (BMPP), Version 2.0, base PP and at least the functional package PAD"
- or according to BSI TR-03122: Conformance Test Specification for Technical Guideline TR-03121 - Biometrics for Public Sector Applications, respectively this technical guideline.

4.5.2. FM PAD-FP-APP1

This Function Module describes requirements for PAD in the context of the acquisition of biometric characteristics of fingerprints.

4.5.2.1. Requirements

4.5.2.1.1. General Requirements

The capture system SHALL contain a PAD subsystem according to [BIB_ISO_PAD_1] 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 PAD subsystem MAY consist of hardware and software (e.g. the used fingerprint scanner MAY have additional sensors designed for this purpose).

According to the used fingerprint scanner, PAD subsystem SHALL be able to detect artefact classes listed in the following:

- Fingertips, created in different thicknesses
- Single fingers (massive)

The PAD subsystem SHALL be able to detect all typical artefact material types listed in the following:

- Artefacts created from different kinds of silicon
- Artefacts created from different kinds of latex
- Artefacts created from different kinds of gelatine
- Artefacts created from different kinds of wood glue
- Artefacts created from different kinds of window painting

- Artefacts created from different kinds of paper

each in different colourings.

Under optimal testing conditions, the PAD subsystem SHALL feature a false-alarm-rate of 2% maximum when tested with bona fide biometric subjects with generally good quality fingerprints. This rate is monitored via logfiles analysis within the operational environment. If this rate is significantly exceeded, any certification that may have been issued might be re-evaluated (depending on application context) [4].

Also, the detection subsystem SHALL be adequate to the usage setting in correspondence with the security requirements in question. The performance MAY be described by a risk analysis for every considered attack type. The current version of [BIB_ISO_PAD_3] SHALL be taken into account.

The PAD SHALL be conducted both in supervised acquisition scenarios, e.g. in a counter scenario, and in unsupervised acquisition scenarios, e.g. in SSS scenarios. Thereby, the PAD SHALL be conducted for all acquisition purposes, e.g. enrolment, identification and verification.

4.5.2.1.2. Integration Requirements

The PAD subsystem SHALL be independent of the regular capture subsystem.

It SHALL signal its detection results in the form of a PAD score for each finger individually. Additionally, an overall result SHALL be returned to the calling application.

The score for each finger SHALL be a normalized as `double` in the range [0,1] using at least ten uniformly distributed interim values, where 0 indicates bona fide and 1 presentation attack. A binary score SHALL NOT be used (e.g. True or False, 1 or 0). The PAD subsystem SHALL additionally provide detailed information about the scores of the PAD.

The overall result SHALL be a boolean value (e.g. True or False). The value SHALL be true, if any of the fingers individual result triggers a PAD alarm.

Even if the Function Module is used within a comparison scenario, the detection result SHALL be signalled in any case, independent from any biometric comparison score. Also, the omission of the detection result SHALL be signalled in any case.

The PAD result SHALL correspond to the respective finger capture attempt.

Note, that an image of the fingerprint or slap in question SHALL be acquired independently of a possible PAD alarm.

4.5.2.1.3. Maintenance Requirements

As new technologies and new attack mechanisms are developed over time, the PAD subsystem SHALL be updated and checked whenever necessary, so it stays capable against old and new attacks and attack types.

4.5.2.1.4. Certification Requirements

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

- BSI-CC-PP-0063-2010: Fingerprint Spoof Detection Protection Profile (FSDPP)
- BSI-CC-PP-0062-2010: Fingerprint Spoof Detection Protection Profile based on Organisational Security Policies (FSDPP_OSP)
- BSI-CC-PP-0118-2022: Common Criteria Protection Profile - Biometric Mechanisms Protection Profile (BMPP), Version 2.0, base PP and at least the functional package PAD

or according to BSI TR-03122: Conformance Test Specification for Technical Guideline TR-03121 - Biometrics for Public Sector Applications, respectively this technical guideline. Note that the PAD certification according

[4] Note that during certification a relaxed false-alarm-rate is tested. The requirement of the rate specified in this Function Module is tested on operational collected data only.

to BSI TR-03122 is preliminary and still subject to amendments. Anticipating certification under this Function Modul MAY only be realised with the permission of the Federal Ministry of the Interior and Community and upon consultation with the Federal Office for Information Security.

4.5.2.1.5. Transitional Rules

The following transition rules are defined for the requirements of this Function Module.

- The requirements of this Function Module only apply to devices and software put into operation after November 1, 2020.
- However, this transition rule ends by May 1, 2025: By May 1, 2025, all devices and software SHALL apply to the requirements of this Function Module.
- For non-certified PAD devices that are already in use and meet the PAD requirements, only software updates are allowed. This applies to the period from November 1, 2020 to May 1, 2025.

4.6. FM Category Compression

The objective of the Function Module Compression (COM) is to keep the biometric data within a feasible size without losing too much quality for a biometric verification or identification.

4.6.1. FM COM-CCTV-JPG

This Function Module describes requirements and interfaces for the compression of surveillance images.

4.6.1.1. Requirements

- The compression method for surveillance images SHALL be JPEG (compare [BIB_ISO_10918-1]). Multiple lossy compressions SHALL NOT take place.
- The compression ratio SHALL be configurable.
- The image resolution SHALL be at least 1280 x 720 pixels.

4.6.2. FM COM-FI-GENERIC

The following requirements are generic and apply to all Function Modules (FMs) regarding compression of facial images.

4.6.2.1. Requirements

Multiple lossy compressions of the facial image data SHALL NOT take place with the exception of the initial capture by a digital camera whenever that camera does not support uncompressed image capture.

4.6.3. FM COM-FI-BCL

This Function Module describes requirements and interfaces for the compression of live images used within the context of border control.

4.6.3.1. Requirements

4.6.3.1.1. General Requirements

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

4.6.3.2. Compression Requirements

Property	Value
Compression method (Image format)	JPEG 2000 (compare [BIB_ISO_15444]) or JPEG (compare [BIB_ISO_10918-1])

Property	Value
Multiple lossy compressions	not allowed
Maximum compression ratio	20:1
Minimum file size	-
Maximum file size	375 kB

Table 4.7 Compression Requirements for Facial Images for Border Control

4.6.4. FM COM-FP-BCL

This Function Module describes requirements and interfaces for the compression of fingerprint images contained in [BIB_ANSI_NIST_2011:2015] files within the context of border control.

4.6.4.1. Requirements

The NIST file size after compression SHALL have a maximum file size of 5332 kB for EES purposes.

The NIST file size after compression SHALL have a maximum file size of 3000 kB for Schengen Information System (SIS) purposes.

4.6.5. FM COM-FP-WSQ

This Function Module describes requirements and interfaces for the compression of fingerprint images by Wavelet Scalar Quantisation (WSQ) method.

4.6.5.1. Requirements

WSQ SHALL be used as compression method for fingerprint images. A bit rate of 0.75 SHALL be used as compression parameter. This is equivalent to a compression factor of approximately 15:1[5] (according to [BIB_ISO_FINGER]). The implementation of the used WSQ algorithm SHALL be certified by the FBI and SHALL be referenced by the respective certificate number (coded in the WSQ header). The certified WSQ implementation SHALL be version 3.1 and SHALL base on NBIS Version 5.0. Multiple lossy compressions SHALL NOT take place.

4.7. FM Category Operation

Within the Function Module Operation (O), 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.

4.7.1. FM O-ALL-LNK

This Function Module describes requirements to be observed by the operator who handles the identification process.

4.7.1.1. Requirements

4.7.1.1.1. Organisational Requirements

- The operator SHALL determine whether the identification was positive by means of manually assessing the returned candidate list.
- If multiple identities of the biometric subject are revealed by the identification, the operator SHALL assure the identities are linked in the Automated Biometric Identification System (ABIS) for deduplication purpose.

[5] For estimation of compression factor it is allowed to crop to the minimum size containing the fingerprint defined if a sensor is used with a larger capturing area than this minimum.

4.7.2. FM O-ALL-USV

This Function Module describes requirements to be observed by the responsible operator of the unsupervised acquisition process of biometric characteristics.

4.7.2.1. Requirements

4.7.2.1.1. General Organisational Requirements

During operating hours the device SHALL be (potentially) visible to an authority employee. Curtains, doors or similar SHALL NOT be used during operating hours. The installation in the visible area is intended to prevent manipulation of the device, as well as vandalism. Note that this requirement does not necessitate that an authority employee watches the device permanently.

4.7.2.1.2. Additional Organisational Requirements within the application context German Identity Documents (GID)

For devices which are subject to the TR volume German Identity Documents the following requirements apply additionally:

The device SHALL be set up in such a way that the capture process can be permanently observed by an official during opening hours. The installation in the observable area is intended to prevent counterfeits and misuse of the device. Note, the usage of monitoring technology (exclusively) is not sufficient to fulfil this requirement.

4.7.2.2. Recommendations

4.7.2.2.1. Organisational Recommendations within the application context Border Control (BCL)

For devices which are subject to the TR volume Border Control the following requirement is recommended additionally:

The operator SHOULD assure that only one person was in near distance of the biometric capture devices. The operator MAY be assisted in this requirement, e.g. by corresponding sensors. This is typically used in conjunction with additional video surveillance.

4.7.3. FM O-FI-ALL

This Function Module describes requirements to be observed by the operator who handles the facial image acquisition process. This includes the full working process.

4.7.3.1. Requirements

- If the software based QA rejects the image, the operator SHALL have the option to give a veto in order to release the image despite a negative software decision and vice versa.
- The operator SHALL be responsible for an adequate cleanliness of all capture hardware components.

4.7.3.2. Recommendations

OPTIONALLY, the operator can use the photo guideline.

4.7.4. FM O-FI-DC

This Function Module describes requirements to be observed by the operator who handles the facial image acquisition process with a digital camera.

4.7.4.1. Requirements

- 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 facial image.

- Direct and cross irradiation of lighting SHALL be avoided by the operator.

4.7.5. FM O-FP-ALL

This Function Module describes requirements to be observed by the operator who handles the acquisition process of fingerprint images.

4.7.5.1. Requirements

4.7.5.1.1. Operation of Devices

- The operator SHALL be responsible for an adequate cleanliness of all capture hardware components. Fingerprint scanners SHALL be cleaned regularly to provide good probe images.
- The fingerprint scanner SHALL be regularly calibrated (e.g. once a day), if the used fingerprint scanner technology requires such a calibration. The operator SHALL ensure that the sensor platen is clean before calibration to reduce the risk of ghost images.

4.7.5.1.2. Environmental Requirements

- 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.

4.8. FM Category User Interface

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

4.8.1. FM UI-FI-BSJ

This Function Module describes requirements for the user interface of facial image acquisition shown to the biometric subject.

4.8.1.1. Requirements

If PAD was conducted: Neither the PAD result nor PAD score SHALL be displayed to the person whose facial image is acquired. In a supervised acquisition scenario the process operator MAY be responsible for screen positioning, so that the PAD result or the PAD score is not displayed to the person whose facial image is acquired.

If the acquisition system is required to have a feedback screen for the facial image acquisition within a specific application context, or if the vendor decided to implement a feedback screen although it is not mandatory in the respective application context, the following requirements SHALL be fulfilled:

- The acquisition system SHALL show a digital mirror or physical mirror image to the biometric subject to guide it for the correct positioning in front of the camera.
- The acquisition system SHALL show user guidance information to help the biometric subject with the correct positioning in front of the camera when one of the following conditions is met:

- The biometric subject is too close to or too far away from the camera.
- The biometric subject is too far left or right to the camera.
- The biometric subject is too high or low and the camera is not able to compensate this with a vertical adjustment.
- The biometric subject is in too much movement.
- The biometric subject is not facing frontally to the camera.
- The eyes of the biometric subject are closed.
- The mouth of the biometric subject is opened.
- Multiple faces were detected in front of the camera.

4.8.1.2. Recommendations

- An indicator showing the capture status SHOULD be displayed to the biometric subject.
- Graphics (e.g. buttons or pictograms) SHOULD use a uniform colour palette without utilizing clashing colours.

4.8.2. FM UI-FI-OP

This Function Module describes requirements for the user interface of the software displaying the result of the quality assessment and verification (if performed) of facial images to the operator.

4.8.2.1. Requirements

- The current evaluated picture SHALL be displayed to the operator for the enrolment.
- All criteria evaluated with the current value and threshold as well as their relation: OK/NOK for every criterion SHALL be displayed to the operator for the enrolment.
- The summarised result OK/NOK for the current picture SHALL be displayed to the operator for the enrolment.
- The provision of the veto power for the operator SHALL be shown to the operator for the enrolment:
  - enforcement of OK for obvious reasons (e.g. disability)
  - enforcement of OK without obvious reasons
  - enforcement of NOK to overrule software based quality assessment
- If PAD was performed and a presentation attack was detected, a warning with the overall result SHALL be displayed to the operator. All facial images that have caused a PAD alarm SHALL be displayed to the operator as well. In addition, all facial images within an acquisition where at least one facial image caused a PAD alarm SHALL be displayed to the operator.

If verifications are performed[6]:

- 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 SHALL be displayed to the operator.
- If the verification fails, then the operator SHALL get access to at least one complete and coherent set of biometric samples and verification results corresponding to a single verification attempt. For instance, in case of verification of a live-captured facial image against a facial image from chip (Data Group 2) and CIR, such a complete set would consist of the live-captured facial image, the facial image extracted from chip, the facial image stored in the CIR, and both corresponding verification results of the live-captured facial image against the facial image from chip and the CIR image.

[6] This is only the case if the application profile defines verification processes explicitly.

4.8.3. FM UI-FP-BSJ

This Function Module describes requirements for the user interface of the biometric subject for fingerprint acquisitions. The user interface MAY be e.g. monitors, buttons, pictograms or status lights.

4.8.3.1. Requirements

The following requirements SHALL be met for the user interface:

- An indicator showing the capture status and an indication when the capture process has finished SHALL be displayed to the biometric subject. The capture status SHALL include: Where to place the fingers, an indication of the scanning process and the feedback in case of mispositioning of fingers.
- In an unsupervised scenario a visualisation which fingerprint or hand to place on the sensor SHALL be given, whereby in the case of a supervised scenario the visualisation MAY be given.

If PAD was conducted: Neither the PAD result nor PAD score SHALL be displayed to the person whose fingerprints are acquired. In a supervised acquisition scenario the process operator MAY be responsible for screen positioning, so that the PAD result or the PAD score is not displayed to the person whose fingerprints are acquired.

4.8.3.2. Recommendations

The following recommendations SHOULD be met for the user interface:

- Graphics (e.g. buttons or pictograms) SHOULD use a uniform colour palette without utilizing clashing colours.
- The acquisition process SHOULD be displayed as real time feedback to the biometric subject (e.g. with the help of a feedback monitor).

4.8.4. FM UI-FP-OP

This Function Module describes requirements for the user interface of the software displaying the live feedback and results of the fingerprint acquisition, QA and control verification of fingerprint images to the operator.

4.8.4.1. Requirements

- The user interface SHALL signal which fingerprints are expected for the current slap or fingerprint acquisition such that the operator can guide the biometric subject to place the correct fingers on the fingerprint scanner.
- Visual feedback of the fingerprint acquisition at least displaying of the final images SHALL be provided to the operator.
- If a uniqueness check error occurs, the fingers involved in the unexpected successful comparisons SHALL be pictorially displayed to the operator and in case of a slap image, only the affected finger(s) SHALL be marked in the displayed image. In case a control verification was attempted and no successful comparison occurred during the control verification, a warning SHALL be displayed to the operator that the control verification was not successful.
- The segmented single fingerprints SHALL be visualised to the operator to identify potential failures in segmentation. This can be realised by displaying the result containing up to ten segmented single fingerprints. In case the amount of captured fingerprints mismatches with the amount of expected fingers a warning SHALL be displayed to the operator.
- If a slap acquisition is in place and a slap classifier is in use (and activated not only for evaluation purpose), a warning SHALL be displayed to the operator when the classification result mismatches with the expected slap of the current acquisition.

- If PAD was performed and a presentation attack was detected, a warning SHALL be displayed to the operator and displayed for each finger individually. An overall result SHALL also be displayed additionally.
- The indication of the quality level SHALL be displayed to the operator.
- The provision of the veto power for the operator SHALL be shown to the operator for the enrolment:
  - enforcement of OK for obvious reasons (e.g. disability)
  - enforcement of OK without obvious reasons
  - enforcement of NOK to overrule software based quality assessment

4.8.4.2. Recommendations

A live view from the fingerprint scanner SHOULD be displayed to the operator during the fingerprint acquisition. This also includes live information, e.g. about the correct positioning of fingers on the fingerprint scanner or about the current quality level, that supports the operator guiding the biometric subject.

The user interface SHOULD show a graphical representation of the fingerprints that are expected for the current slap or fingerprint acquisition.

4.8.5. FM UI-FP-VER

This Function Module describes requirements for the user interface of the operator for verification of fingerprint images.

4.8.5.1. Requirements

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

4.8.5.2. Recommendations

- A visualization which fingerprint / hand to place on the sensor SHOULD be displayed.
- An indicator showing the capture status SHOULD be displayed to the biometric subject.
- An indication when the capture process has finished or the capture process is to be retried.
- Information about the successful or failed verification process SHOULD be displayed.
- Graphics SHOULD avoid multiple colours or harsh contrast.

4.9. FM Category Reference Storage

The objective of the Function Module Reference Storage (REF) is to store biometric data in a way that it can be used for reference purposes later on.

4.9.1. FM REF-FI-EES

This Function Module describes requirements how facial images are stored as reference data in the EES.

4.9.1.1. Requirements

The acquired facial image data SHALL be stored in the CS EES if enrolment or update of facial images is required by the relevant use case.

4.9.2. FM REF-FP-EES

This Function Module describes requirements how fingerprint images are stored as reference data in the EES.

4.9.2.1. Requirements

The acquired fingerprint data SHALL be stored in the CS EES if enrolment or update of fingerprints is required by the relevant use case.

4.10. FM Category Biometric Comparison

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

It is RECOMMENDED that the verifications conducted during uniqueness checks comply with this FM.

4.10.1. FM CMP-FI-VER

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

4.10.1.1. Requirements

4.10.1.1.1. Requirements on the Algorithm Performance

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

- The face verification algorithm SHALL be configured at a security level (threshold) guaranteeing an FMR of at most 0.1 % (1:1000) (0.01 %, 1:10,000 is RECOMMENDED) in conjunction with an FNMR less than 2 %.
- The threshold SHALL be configurable by the system administrator 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[7] 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 the 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 Electronic Passport deployment).

4.10.1.1.2. Requirements on the System Performance

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

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

4.10.2. FM CMP-FP-VER

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

[7] Typically a vendor-specific uncalibrated raw score

4.10.2.1. Requirements

4.10.2.1.1. 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 an FMR of 0.1 % (1:1000) in conjunction with an FNMR less than 2 %.
- The threshold SHALL be configurable by the system administrator 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[8] 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 the 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 Electronic Passport deployment).

4.10.2.1.2. Requirements on the System Performance

The following requirements SHALL be met for the system performance (including FTE) and FTA rates):

The FRR SHALL be less than 4 % at an FAR of 0.1 %.

4.11. FM Category Logging

The Function Module Logging (LOG) contains logging requirements. The requirements of this chapter and the requirements of the schema of information to log apply both.

4.11.1. FM LOG-ALL-GENERIC

The Function Module Logging contains requirements as to which data has to be logged for a specific application.

4.11.1.1. Requirements

- A transaction SHALL cover all information concerning one single biometric subject. Created IDs SHALL be unique globally. During the biometric process all data SHALL be gathered or created by the application.
- Each transaction SHALL contain the generic process information about the system that are defined in `type.transaction`. The exact semantic for the location of station is profile-dependent. See the specific profile for a refined definition. If the transaction is dependent or derived from another transaction the ID of the reference SHALL be set.
- In case of abnormal termination of the transaction or any of its sub-processes, the error code SHALL be logged. The vendor SHALL provide a detailed list of all error codes used with complete semantic descriptions.
- During the transaction performed enrolment processes SHALL be logged as `Enrolment`. In cases where the central system replies directly with enrolment status information the submit time SHALL be recorded. If any control verification is performed during enrolment the result SHALL be contained.

[8] Typically a vendor-specific uncalibrated raw score

- For identification processes the data defined in `Identification` SHALL be recorded. The list of candidates SHALL be contained if detailed scoring information is provided by the central system.
- A verification processes SHALL be recorded based on the `Verification` element. Per verification all performed comparisons SHALL be included. For each comparison the vendor specific score as well as the threshold SHALL be contained.

4.11.2. FM LOG-ALL-BCL

The Function Module Logging contains requirements as to which data has to be logged for the application of border control.

4.11.2.1. Requirements

In case a record is stored externally, the external reference SHALL be defined giving information about the actual location of the data. For this purpose the `externalReference` attribute of the `bio:BinaryRecord` element SHALL be used.There SHALL NOT be data within the respective record of the log when the external reference is used.

In order to allocate border control logs to their respective application profile the element `ApplicationProfile` SHALL be filled as described in ▸Table 4.8.

Application Profile within TR	ApplicationProfile-Element
▸Application Profile Manual Border Control	`BCL_ManualBorderControl`
▸Application Profile Semi-Mobile Manual Border Control	`BCL_SemiMobileManualBorderControl`
▸Application Profile Automated Border Control (Face-Verification Only)	`BCL_AutomatedBorderControlFaceVerfication`
▸Application Profile Self-Service System	`BCL_SelfServiceSystem`

Table 4.8 Mapping Logs to Application Profiles

4.11.2.2. Recommendations

It is RECOMMENDED to store the images of the fingerprints and the facial image not only in the application specific container (e.g. EES-ANSI-NIST) record within the log, but also as separated records (e.g. in JPEG, BMP, WSQ). Thereby, the log-reading applications are able to parse the images easier, as they only need knowledge about the syntax of the BSI TR-03121 log schema.

4.11.3. FM LOG-FI-GENERIC

This Function Module describes requirements and interfaces for the logging of information regarding facial images for all profiles.

4.11.3.1. Requirements

- Within a transaction for each facial image acquisition or delivery performed for enrolment, verification or identification, all data defined in `FaceAcquisition` (of which some MAY be contained within a `MultiModalAcquisition`) or `FaceDelivery` SHALL be collected, if available.
- During an acquisition process, the available details for all captures SHALL be logged.
- If a veto was put by the operator the type of veto (OK/NOK) SHALL be set.
- Detailed quality information SHALL be logged at least for the selected facial image. The overall result MAY be omitted if it is undefined. For each criterion the identifier, upper and lower value bound as well as the upper and lower threshold bound SHALL be included if available. When more than one facial image is present, all face quality elements SHALL reference to the corresponding record element.

- For each performed PAD the detailed PAD quality values accompanied by identifiers, upper and lower value bounds and upper and lower threshold bounds SHALL be collected.
- If a user interface is available during the acquisition process, the displayed information, e.g. an indication of a PAD alert or live feedback screen SHALL be logged.
- In case of abnormal termination of the facial image acquisition process or any of its sub-processes, the error code SHALL be logged. The vendor SHALL provide a detailed list of all error codes used with complete semantic descriptions.

4.11.4. FM LOG-FP-GENERIC

This Function Module describes requirements and interfaces for the logging of information regarding fingerprint images for all profiles.

4.11.4.1. Requirements

- Within a transaction for each fingerprint acquisition or delivery performed for enrolment, verification, control verification or identification, all data defined in `FingerAcquisition` (of which some MAY be contained within a `MultiModalAcquisition`) or `FingerDelivery` SHALL be collected, if available. If a fingerprint could not be acquired, the reason for each missing finger SHALL be logged.
- For each capture process of a dedicated fingerprint or slap, all available information SHALL be logged. In case of multiple captures for a finger or slap the number of the capture details for which slap was selected as the best capture SHALL be specified. Within the finger capture the reference to the corresponding record of the probe SHALL be set. Further the details of each during the capture performed attempt SHALL be provided, including the reference to the corresponding record if available. In case of an unacceptable capture attempt the reason for rejection of this capture attempt SHALL be selected. If the rejection reason is `other` an error code detailing the reason of rejection SHALL be set.
- If a veto was put by the operator the type of veto (OK/NOK) SHALL be set.
- For the best capture attempt, detailed quality information about the result SHALL be logged. For all other capture attempts quality information, if calculated during the process, SHOULD be logged. For each finger or slap within a capture the quality result value and the threshold SHALL be presented within a range from 0 to 100 when available. If an overall quality value can be estimated by the quality assessment algorithm it SHALL be specified.
- If a slap classification is performed during the acquisition process, the details SHALL be logged as `FingerClassifierInformation`. This includes the classification results, information about the configured threshold of the algorithm and whether the classifier has been used in evaluation mode.
- When a uniqueness check is performed, the results SHALL be collected. If the FMR is known, the security level for the uniqueness check SHALL be contained. The log SHALL specify all detected duplicate fingers.
- For each performed PAD the detailed PAD quality values accompanied by identifiers, upper and lower value bounds and upper and lower threshold bounds SHALL be collected. In case the probe is a slap and a PAD result is expected for each individual finger of the slap, the finger code SHALL be defined and PAD information SHALL be present for each finger.
- If a user interface is available during the acquisition process, the displayed information, e.g. an indication of a PAD alert or live feedback screen SHALL be logged.
- In unsupervised acquisition scenarios all available surveillance information SHALL be stored for each corresponding capture attempt. The surveillance image contained within a record SHALL be linked to the fingerprint capture attempt.
- It SHALL be logged if multiple persons have been detected or not during the fingerprint acquisition process or single capture attempts.

- When the acquisition process is performed with the presence of a configured timeout the corresponding value SHALL be specified in milliseconds. The logging of the configured value SHALL be independent from the occurrence of a timeout.
- If a control verification is performed (e.g. for rolled vs flat fingerprints or for fingerprints acquired at a SSS vs fingerprints acquired at the counter) all available information SHALL be logged within a `Verification` element.
- In case of abnormal termination of the fingerprint acquisition process or any of its sub-processes, the error code SHALL be logged. Errors during the fingerprint segmentation or uniqueness check SHALL be specified additionally by their corresponding error element. The vendor SHALL provide a detailed list of all error codes used with complete semantic descriptions.
- Information about the configured pixel density in dpi (dots-per-inch) of the fingerprint scanner SHALL be contained in `FingerAcquisition/Hardware/ConfigurationInformation` using *PixelDensity* as type.

4.12. FM Category Coding

This Function Module Coding (COD) contains the procedures to encode quality data as well as biometric data in defined formats. Interoperability is provided by means of standard compliant coding.

4.12.1. FM COD-ALL-BCL

This Function Module describes requirements and interfaces for the overall coding of biometric and biographic data used within the context of border control.

4.12.1.1. Requirements

- The logging data as defined by the FM of the ▸FM Category Logging SHALL be encoded as XML according to the schema definition as `bcl-log` element. The XML encoding is defined by the XML schema definition in the file „bcl5v1.xsd“ and referenced schema files.
- Optional attributes and elements of the schema SHALL be considered as far as possible (e.g. error codes only need to be logged, in case an error occurred; an acquisition element is only required, in case an acquisition process has at least been started).
- All log data SHALL be encoded as far as it is available throughout the acquisition process (e.g. fingerprint quality data is encoded if and only if fingerprint capture was performed).

4.12.2. FM COD-ALL-EES

This Function Module describes requirements and interfaces for the coding of general information according to EES-ANSI-NIST transactions.

4.12.2.1. Requirements

The general coding SHALL be conformant to the current version of the [BIB_EES_ICD] in the binary format. Some required EES-ANSI-NIST data fields (e.g. biographic information) may not be available for the acquisition system (see ▸Table 4.9) . In order to keep the schema conformance during the entire process, these fields SHALL be filled with conformant placeholders. These placeholders SHALL be replaced as soon as possible with the actual values by the calling application.

Record Type	Mnemonic	Field Name
1	PRY	Priority
1	ORI	Originating Agency Identifier
10	SRC	Source Agency

Record Type	Mnemonic	Field Name
14	SRC	Source Agency

Table 4.9 Potential EES-ANSI-NIST Fields for Placeholders

4.12.3. FM COD-FI-GENERIC

This Function Module describes requirements for the coding used during the acquisition process of facial images.

4.12.3.1. Requirements

All results of the acquisition or delivery process SHALL be encoded in XML as `FaceAcquisition` or `FaceDelivery`.

The XML encoding is defined by the XML schema definition in `biotypes5v1.xsd` for all volumes.

4.12.4. FM COD-FI-EES

This Function Module describes requirements for the coding used within the context of border control.

4.12.4.1. Requirements

- The coding for facial images SHALL be conformant to the current version of the [BIB_EES_ICD] in the binary format.
- The minimum image resolution SHALL be 600 x 800 pixels.
- The maximum image resolution SHALL be 1200 x 1600 pixels.

4.12.5. FM COD-FI-VER

This Function Module describes requirements for the coding used during the verification process of facial images.

4.12.5.1. 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 SHALL be encoded in XML according to the schema definition as `Verification` within bcl-log element.
- All results of the evaluation work flow SHALL be encoded in XML according to the schema definition as fi-bcl-eval element.

The XML encoding is defined by the XML schema definition in "bcl5v1.xsd". Examples can be found in "bcl-log.xml" and "fi-bcl-eval.xml".

4.12.6. FM COD-FP-EES

This Function Module describes requirements for the coding used to send fingerprint images to the CS EES.

4.12.6.1. Requirements

The coding for fingerprint images SHALL be conformant to the current version of the [BIB_EES_ICD] in the binary format.

4.12.7. FM COD-FP-VER

This Function Module describes requirements for the coding used during the verification process of fingerprint images.

4.12.7.1. 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 SHALL be encoded in XML as `Verification` within "bcl-log".
- All results of the evaluation work flow SHALL be encoded in XML as "fp-bcl-eval".

The XML encoding is defined by the XML schema definition in "bcl5v1.xsd". Examples can be found in "bcl-log.xml" and "fp-bcl-eval.xml".

4.13. FM Category Evaluation

Will be amended in a future version of this TR.

List of Abbreviations

Abbreviation	Description
ABC	Automated Border Control
ABIS	Automated Biometric Identification System
AH	Acquisition Hardware
AS	Acquisition Software
BCL	Border Control
BIP	Biometric Image Processing
BMS	Biometric Matching System
CIR	Central Identity Register
CMP	Biometric Comparison
COD	Coding
COM	Compression
CS EES	Central System EES
CTF	contrast transfer function
DET	Detection Error Trade-Off
EES	Entry-Exit System
eMRTD	Electronic Machine Readable Travel Document
FAR	false accept rate
FI	facial image
FM	Function Module
FMR	false-match-rate
FNIR	false-negative-identification-rate
FNMR	false-non-match-rate
FP	fingerprint
FPIR	false-positive-identification-rate
FRR	false reject rate
FTA	failure to aquire
FTE	failure to enrol
HLBS	High Level Biometric Services
LOG	Logging
MBC	Manual Border Control
NFIQ2.2	NIST Fingerprint Image Quality 2.2
O	Operation
PAD	Presentation Attack Detection

Abbreviation	Description
PAP	Partial Application Process
QA	Quality Assessment
REF	Reference Storage
SIS	Schengen Information System
SNR	signal-to-noise ratio
SSS	self-service system
TCN	Third-Country National
TR	Technical Guideline
UI	User Interface
VIS	Visa Information System
WSQ	Wavelet Scalar Quantisation

Bibliography

[BIB_ANSI_NIST_2011:2015] *ANSI/NIST-ITL 1-2011: Update 2015, American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information ANSI/NIST-ITL 1-2011 NIST Special Publication 500-290 Edition 3, available at: http://dx.doi.org/10.6028/NIST.SP.500-290e3.*

[BIB_EBTS/F] *FBI Electronic Biometric Transmission Specification Version 11, Appendix F, April 2021.*

[BIB_EES_ICD] *euLISA EES Interface Control Document, Annex 5 - NIST Fields, Version 0.7.2, 2023, 05.07.2023.*

[BIB_ICAO_TR_Portrait_Quality] *ICAO Technical Report: Portrait Quality (Reference Facial Images for MRTD), version 1.0, April 2018.*

[BIB_ISO_10918-1] *ISO/IEC 10918-1:1994 "Information technology – Digital compression and coding of continuous-tone still images: Requirements and guidelines".*

[BIB_ISO_15444] *ISO/IEC 15444-1:2004 "Information technology – JPEG 2000 image coding system: Core coding system".*

[BIB_ISO_19795-1:2021] *ISO/IEC 19795-1:2021 "Information technology — Biometric performance testing and reporting — Part 1: Principles and framework".*

[BIB_ISO_FACE] *ISO/IEC 19794-5:2005 "Information technology - Biometric data interchange formats – Part 5: Face image data".*

[BIB_ISO_FINGER] *ISO/IEC 19794-4:2005 "Information technology - Biometric data interchange formats – Part 4: Finger image data".*

[BIB_ISO_PAD_1] *ISO/IEC 30107-1:2016 "Information technology – Biometric presentation attack detection – Part 1: Framework".*

[BIB_ISO_PAD_3] *ISO/IEC 30107-3:2017 "Information technology – Biometric presentation attack detection – Part 3: Testing and reporting".*

[BIB_NFIQ2.2] *NIST Fingerprint Image Quality 2.2.*