Federal Office
for Information Security

Technical Guideline TR-03121-3

Biometrics for Public Sector Applications

Part 3: Application Profiles and Function Modules

Volume 5: General Identification Scenarios

Version 4.4

Federal Office for Information Security
P.O. Box 20 03 63, 53133 Bonn, Germany

E-Mail: TRBiometrics@bsi.bund.de

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

© Federal Office for Information Security 2013-2018

Index of Contents

1 Introduction ... 7

2 Application Profiles for General Identification Scenarios ... 9

2.1 Multimodal Identification with Watchlist Checks ... 9
2.1.1 Introduction ... 9
2.1.2 System Overview ... 9
2.1.3 Process Overview ... 11
2.1.4 Target Audience ... 12
2.1.5 Relevant Standards and Conditions ... 12
2.1.6 Information for Function Modules ... 12

3 Function Modules ... 15

3.1 Process ... 15
3.1.1 P-PH-APP ... 15
3.1.2 P-FP-PLAIN ... 19
3.1.3 P-IR-APP ... 35

3.2 Acquisition Hardware ... 37
3.2.1 AH-PH-DC ... 37
3.2.2 AH-FP-OPT ... 38
3.2.3 AH-IR-DC ... 40

3.3 Acquisition Software ... 41
3.3.1 AS-PH-DC ... 41
3.3.2 AS-FP-MF ... 41
3.3.3 AS-IR-DC ... 42

3.4 Presentation Attack Detection ... 42
3.4.1 PAD-FP-APP ... 42

3.5 Biometric Image Processing ... 44
3.5.1 BIP-PH-DC-HQ ... 44
3.5.2 BIP-FP-APP ... 45
3.5.3 BIP-IR-APP ... 46

3.6 Quality Assurance ... 46
3.6.1 QA-PH-SB ... 46
3.6.2 QA-PH-PG ... 49
3.6.3 QA-FP-APP ... 50
3.6.4 QA-IR-SB ... 54

3.7 Compression ... 56
3.7.1 COM-PH-JPG ... 56
3.7.2 COM-FP-WSQ ... 57
3.7.3 COM-IR-PNG ... 57

3.8 Operation ... 57
3.8.1 O-PH-ALL ... 58
3.8.2 O-PH-SPV ... 58
3.8.3 O-FP-ACQ ... 59
3.8.4 O-IR-ACQ ... 61

3.9 User Interface ... 62
3.9.1 UI-PH-APP ... 62
3.9.2 UI-FP-BSJ ... 62
3.9.3 UI-FP-OFF ... 63
3.9.4 UI-IR-APP ... 63

3.10 Reference Storage ... 64
3.11 Biometric Comparison ... 64
3.11.1 CMP-ALL-MMI ... 64
3.11.2 CMP-PH-GENERIC ... 65
3.11.3 CMP-FP-GENERIC ... 66
3.11.4 CMP-IR-GENERIC ... 67
3.12 Logging ... 68
3.12.1 LOG-PH-GENERIC ... 68
3.12.2 LOG-FP-GENERIC ... 69
3.12.3 LOG-IR-GENERIC ... 70
3.13 Coding ... 71
3.13.1 COD-ALL-GENERIC ... 71
3.13.2 COD-ALL-MMI ... 71
3.13.3 COD-PH-STANAG ... 72
3.13.4 COD-FP-STANAG ... 72
3.13.5 COD-IR-STANAG ... 72
3.14 Evaluation ... 72
4 List of Abbreviations ... 73
5 Bibliography ... 76

List of Tables

Table 2-1: Application Profile Multimodal Identification with Watchlist Checks....14
Table 3-1: Minimum and Maximum Modulation....39
Table 3-2: Usability Metrics PAD....43
Table 3-3: Requirements for the Size of Facial Images....45
Table 3-4: Requirements for the Size of Facial Images in GSAT Transactions....45
Table 3-5: Mapping of Relevant Quality Criteria....48
Table 3-6: Application Specific Thresholds for Facial Images....49
Table 3-7: Thresholds for Plain Fingerprints for Enrolment Purposes....52
Table 3-8: Thresholds for Plain Control /Identification Fingerprints....52
Table 3-9: Thresholds for Rolled Fingerprints....53
Table 3-10: Mapping of Relevant Quality Criteria to ISO Requirements....55
Table 3-11: Thresholds for Iris Images....56
Table 3-12: Requirements to Compression Using JPEG Format....57
Table 3-13: Multimodal Identification Performance Requirements....64
Table 3-14: Facial Image Identification Performance Requirements....65
Table 3-15: Fingerprint Identification Performance Requirements....66
Table 3-16: Iris Identification Performance Requirements....67

List of Figures

Figure 2-1: System Architecture Overview....10
Figure 2-2: Data Acquisition at the Registration Office....11
Figure 3-1: Relevant Function Blocks for the Facial Image Process....15
Figure 3-2: Image Provision Scan....17
Figure 3-3: Image Transmission via TR-03146....18
Figure 3-4: Image Provision from Live Enrolment Station....19
Figure 3-5: Relevant Function Blocks for Plain Fingerprint Acquisition Process....20
Figure 3-6: "Acquire Plain Slap" Task....22
Figure 3-7: "Capture Slap Unsupervised" Task....23
Figure 3-8: "Capture Plain Finger Unsupervised" Task....24
Figure 3-9: "Acquire Plain Finger" Task....26
Figure 3-10: Acquisition Workflow for 4-4-2 Identification....27
Figure 3-11: Acquisition Workflow for 4-4-2 Enrolment....28
Figure 3-12: Acquisition Workflow for 4-1-4-1 Enrolment....29
Figure 3-13: Acquisition Workflow for 4-1-4-1 Identification....30
Figure 3-14: Acquisition Workflow for Two Finger Enrolment Single Finger Hardware....32
Figure 3-15: Acquisition Workflow for Two Finger Enrolment Multi Finger Hardware....33
Figure 3-16: Unsupervised Acquisition Process for Two Plain Finger On Multi Finger Hardware for Enrolment....34
Figure 3-17: Unsupervised Acquisition Process for Two Plain Finger Single Finger Hardware for Enrolment....35
Figure 3-18: Relevant Function Blocks for Iris Image Process....36
Figure 3-19: Digital Provision of an Iris Image....37
Figure 3-20: Example for the Finger Position....60
Figure 3-21: Example for the Position of the Hand....61

1 Introduction

This document describes Application Profiles and Function Modules in the scope of the TR Biometrics. For an overview of this guideline, consult TR-03121-1.

2 Application Profiles for General Identification Scenarios

2.1 Multimodal Identification with Watchlist Checks

The following Application Profile describes the enrolment of biometric personal data for the purpose of performing watchlist checks and general deduplication. Therefore, it does not target a specific application but serves as a generic blueprint for scenarios with the need for identity management of larger populations.

2.1.1 Introduction

The current scenario targets population sizes in the range of 100.000 identities up to several millions. Where applicable, guidance is given for different gallery sizes.

2.1.2 System Overview

The main components in this context consist of one or more Central Identity Registers (CIR), the Biometric Evaluation Authority (BEA) and registration offices belonging to a specific Central Identity Register, as depicted in Figure 2-1.

Any request for biometric and biographic data retrieval or storage is performed via the CIR, which holds – directly or as proxy – all biographic and biometric data of the stored identities. The BEA represents the destination for log files documenting the process in detail.

The applicant appears in person at the local registration office, where an official operates the live enrolment equipment and guides the process.

This profile requires all three main biometric modalities (facial image, ten fingers, two iris images) to be enrolled for an identity. Depending on the expected gallery size, this requirement can be relaxed, but care should be taken, that the expected identification performance will not be reduced in an unacceptable manner.

In disconnected operations, there can be multiple instances of a CIR which have to be kept in sync asynchronously (see Figure 2-1). Details on the synchronisation protocol except for the specification of the biometric data exchange formats are out of scope of this profile.

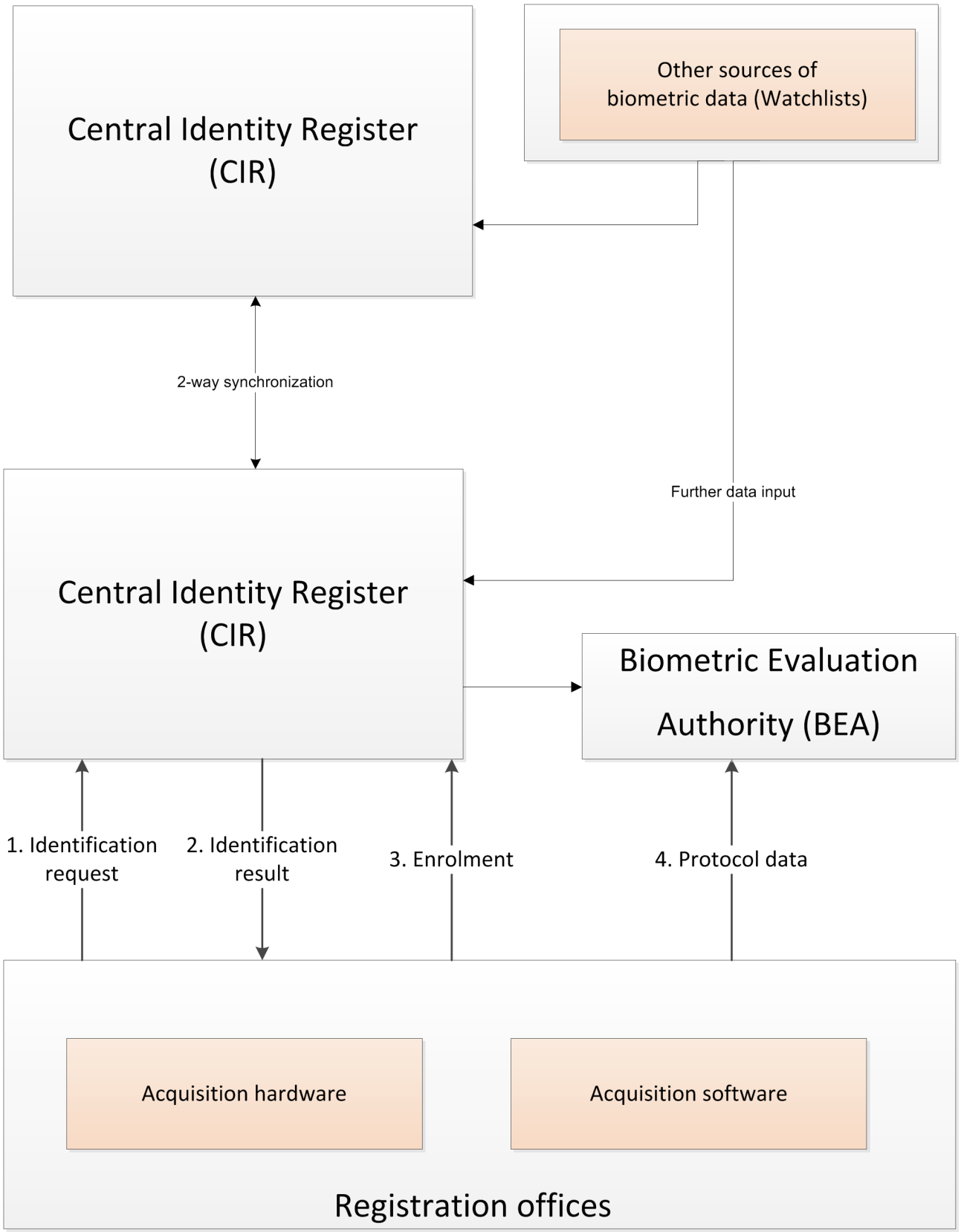

Figure 2-1: System Architecture Overview

2.1.3 Process Overview

Figure 2-2 depicts the acquisition process in the registration office. In general, the biometric data of the applicant is captured sequentially. Care shall be taken to ensure a high quality enrolment in a variations of its time and place of capture. Simultaneous capturing of the facial image and the iris image is possible by using combined equipment, nevertheless the distinct requirements apply to the multifunctional capture device.

When all biometric data are acquired according to the requirements laid out in this profile, an identification attempt is carried out to detect whether the person has already been enrolled. An officer has to handle the list of alleged duplicates and perform according actions depending on the usage scenario (e.g. linking identities together, issuing alerts or similar). Details on this are out of scope for this profile.

In case the identification fails, i.e. no record is returned from the CIR, a new data record for the applicant is created.

For each biometric capture, the set of quality requirements of this profile shall be adhered to, the policy how to deal with low quality and missing biometric features is application dependent and not further considered in this profile.

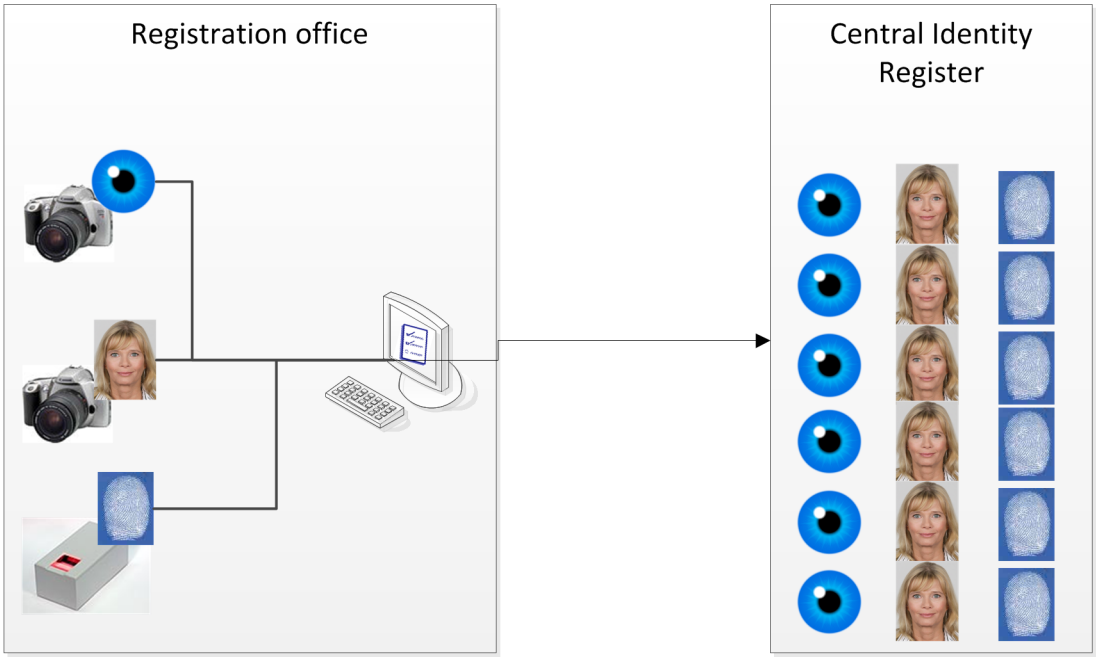

Figure 2-2: Data Acquisition at the Registration Office

The applicants biographic and biometric data including process and quality information are coded and passed to the CIR which performs the storage of the features and creates templates for biometric matching. It is strictly required that the CIR keeps the images to allow for re-enrolment in the biometric backend system and renewal of used algorithms.

After finishing the enrolment process of an applicant, logging data according to this profile shall be collected to allow for monitoring and evaluation of the process. The logging data shall be submitted to a dedicated organizational unit called “Biometric Evaluation Authority”. Depending on the usage scenario, this might happen online or offline in batch mode. In any case, regular evaluation of this data is highly recommended.

Watchlist Checks

In addition to the regular deduplication by searching the entire gallery in one-to-many mode, a dedicated matching against a watchlist may be performed. From a biometric point of view, biometric data originating

from a watchlist entry do not differ from data of regularly enrolled identities. Nevertheless, storage and referencing of the watchlist in the identification system might be different from the regular identification management.

Management and Export of Data

In the case of multiple disconnected Central Identity Registers and in the case of partial data exchange with other third parties, coding of the data for export shall be according to one of the allowed coding modules. The relevant coding module is typically determined by the usage scenario.

2.1.4 Target Audience

The Application Profile “Multimodal Identification with Watchlist Checks” is relevant for the following instances.

- owners of identification systems
- suppliers of hardware and software components

2.1.5 Relevant Standards and Conditions

In addition to the legal requirements, further basic directives and standards are applicable:

- ISO/IEC 19794-4
- ISO/IEC 19794-5
- ISO/IEC 19794-6 and ISO/IEC 29794-6

2.1.6 Information for Function Modules

All Function Modules necessary for the Application Profile “Multimodal Identification with Watchlist Checks” are presented in Table 2-1[1].

1 Slash separated entries denote alternative modules. Comma-separated entries denote requirements for all modules.

Module Category	Required Function Modules
Process	P-PH-APP P-FP-PLAIN P-IR-APP
Acquisition Hardware	AH-PH-DC AH-FP-OPT AH-IR-DC
Acquisition Software	AS-PH-DC AS-FP-MF AS-IR-DC
Presentation attack detection	PAD-FP-APP
Biometric Image Processing	BIP-PH-DC-HQ BIP-FP-APP BIP-IR-APP
Quality Assurance	QA-PH-SB, QA-PH-PG QA-FP-APP QA-IR-SB
Compression	COM-PH-JPG COM-FP-WSQ COM-IR-PNG
Coding	COD-ALL-MMI COD-PH-STANAG COD-FP-STANAG COD-IR-STANAG
Comparison	CMP-ALL-MMI CMP-PH-GENERIC CMP-FP-GENERIC CMP-IR-GENERIC
Operation	O-PH-ALL O-PH-SPV O-FP-ACQ O-IR-ACQ

Module Category	Required Function Modules
User Interface	UI-PH-APP UI-FP-BSJ UI-FP-OFF UI-IR-APP
Logging	LOG-PH-GENERIC LOG-FP-GENERIC LOG-IR-GENERIC
Evaluation	*Will be defined in a later version of the document*

Table 2-1: Application Profile Multimodal Identification with Watchlist Checks

3 Function Modules

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

3.1 Process

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

3.1.1 P-PH-APP

This function block describes the alternatives and the overall process requirements for the provisioning of facial images for enrolment purposes.

Requirements

All documents shall contain images of the type "full frontal image" according to the standard [ISO_FACE].

Multiple lossy compressions of face image data are not allowed within the overall process (with the exception of the initial capture by a digital camera whenever that camera does not support uncompressed image capture[2]).

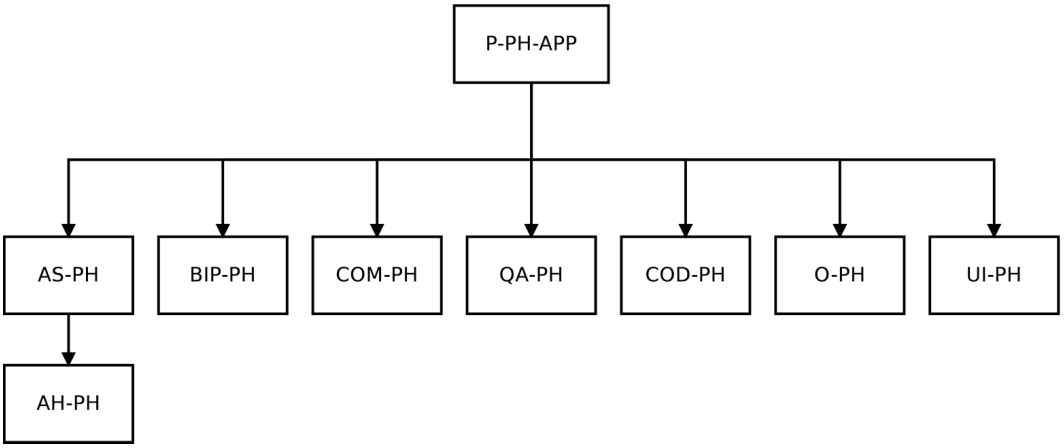

Figure 3-1: Relevant Function Blocks for the Facial Image Process

In order to obtain a facial image that complies with all specified requirements the following process has to be followed. In this context, several Function Modules and the according Function Blocks are involved and the respective requirements have to be fulfilled:

- FM Acquisition Hardware (FM AH)
- FM Acquisition Software (FM AS)
- FM Biometric Image Processing (FM BIP)
- FM Compression (FM COM)
- FM Quality Assurance (visual and software based) (FM QA)
- FM Coding (FM COD)
- FM Operation (FM O)

2 See detailed requirements on FM AH for further information

— FM User Interface (FM UI)

The respective detailed function modules from the corresponding application profile apply. Note: Not all profiles support all the options that are presented in the next sections.

The process of the acquisition of a facial image offers three options of how an image can be provided for the application (compare Figure 3-2).

— The applicant's photo which was taken and printed by a photographer is brought into the office and is scanned there (see AH-PH-FBS, AS-PH-FBS, and BIP-PH-FBS for further details).
— The photo is transmitted electronically into the application (according to [TR-03146]).
— The photo is taken by the responsible authority itself, either using a live enrolment station (see AH-PH-VID, AS-PH-DC, and BIP-PH-DC for further details) or a photographic studio setting (see AH-PH-DC, AS-PH-DC, and BIP-PH-DC for further details). When a live enrolment station is used, it shall contain a Quality Assurance module.

  Note: Not all profiles support all three options.

In the first case, see Figure 3-2, a photo taken and printed by a photographer is provided for the application. At first, a visual check shall be performed by the official at the application counter (see modules O and QA). Depending on the result of the visual inspection, the photo is rejected or accepted for further processing. In the successful case, the image shall be digitised at the application counter with a scanner (see modules AH, AS and BIP) and be compressed (see module COM). Afterwards, the scanned image shall be subject to Quality Assurance (see module QA). Finally, the operator shall have the option to give a veto in order to overrule the QA software decision.

In the second case, see Figure 3-3, a live capture is conducted detached from the counter office and electronically transferred to the official counter. The image shall be captured and compressed according to modules AH, AS, BIP and COM before transferring. The electronic transmission of the image shall comply to standard [TR03146]. In order to guarantee the connection between the facial image and the respective person, an identification check shall be conducted by the operator (see module O). In the successful case, the image shall be checked by the quality software (see module QA). Finally, the operator shall have the option to give a veto in order to overrule the QA software decision.

As a third option, see Figure 3-4, a live enrolment station can be used that works with an integrated Quality Assurance module (see module COD). The requirements of modules AH, AS and BI shall apply. The image quality shall be checked directly while the image is taken. If the quality is not suitable, the acquisition can be restarted. If the quality is sufficient, the image can be released for the application counter. For security reasons the official shall check whether the image was taken from the applicant (see module O). In the successful case, the image shall be checked by the quality software (see module QA). Finally, the operator shall have the option to give a veto in order to overrule the QA software decision.

In all cases the following shall apply: In addition to the check by QA software, the official shall verify the geometric features of the image using a photo template (one for adults and one for children) (see module QA). If the operator gives a veto (veto equals yes) a negative software decision of the quality assurance shall be overruled and the facial image shall be released. The operator shall in addition have the option to reject an image despite a positive software QA decision.

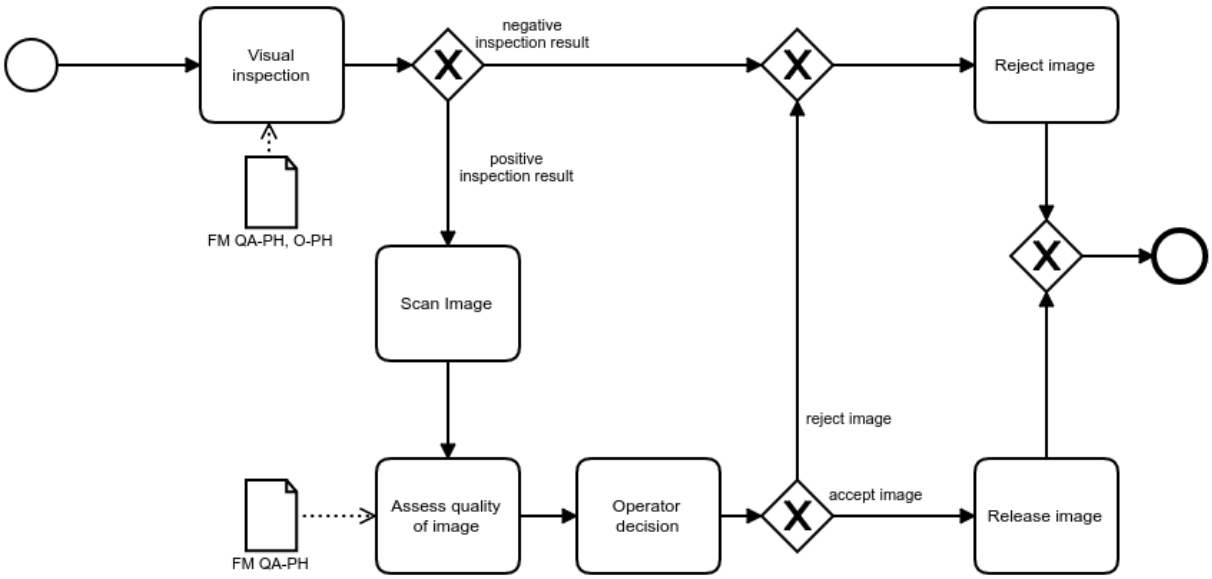

Figure 3-2: Image Provision Scan

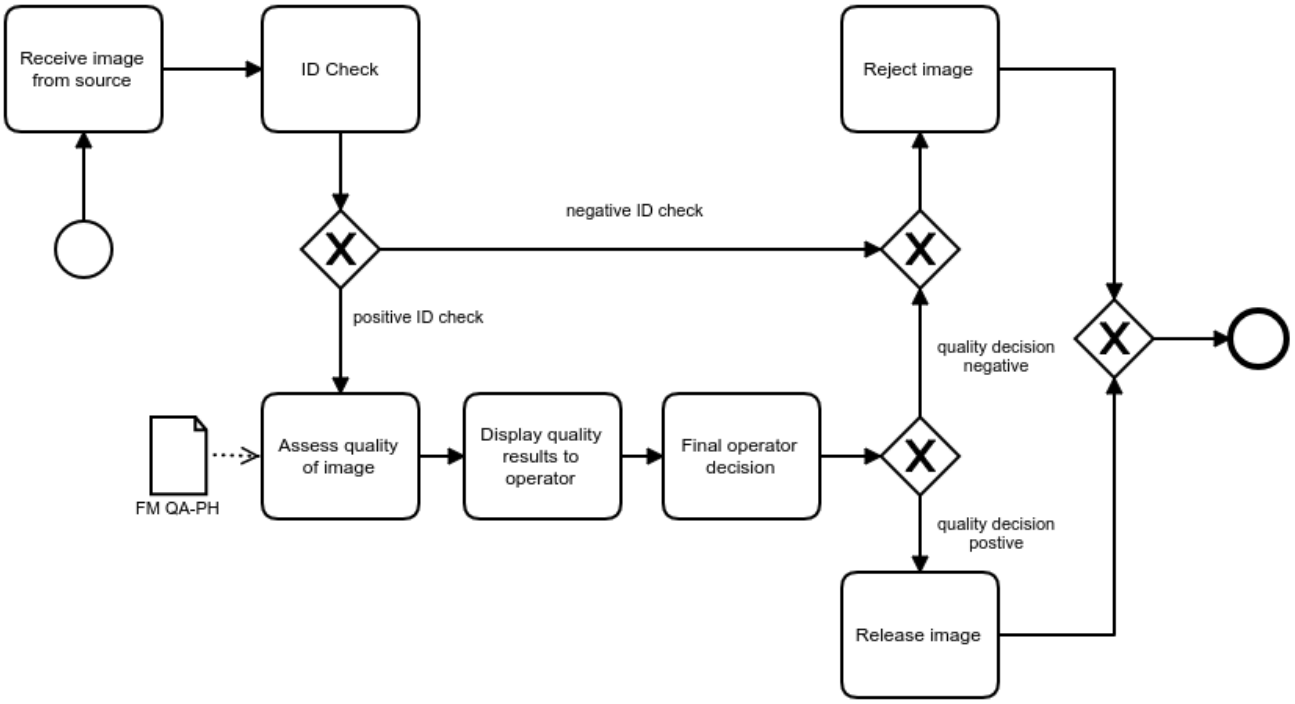

Figure 3-3: Image Transmission via TR-03146

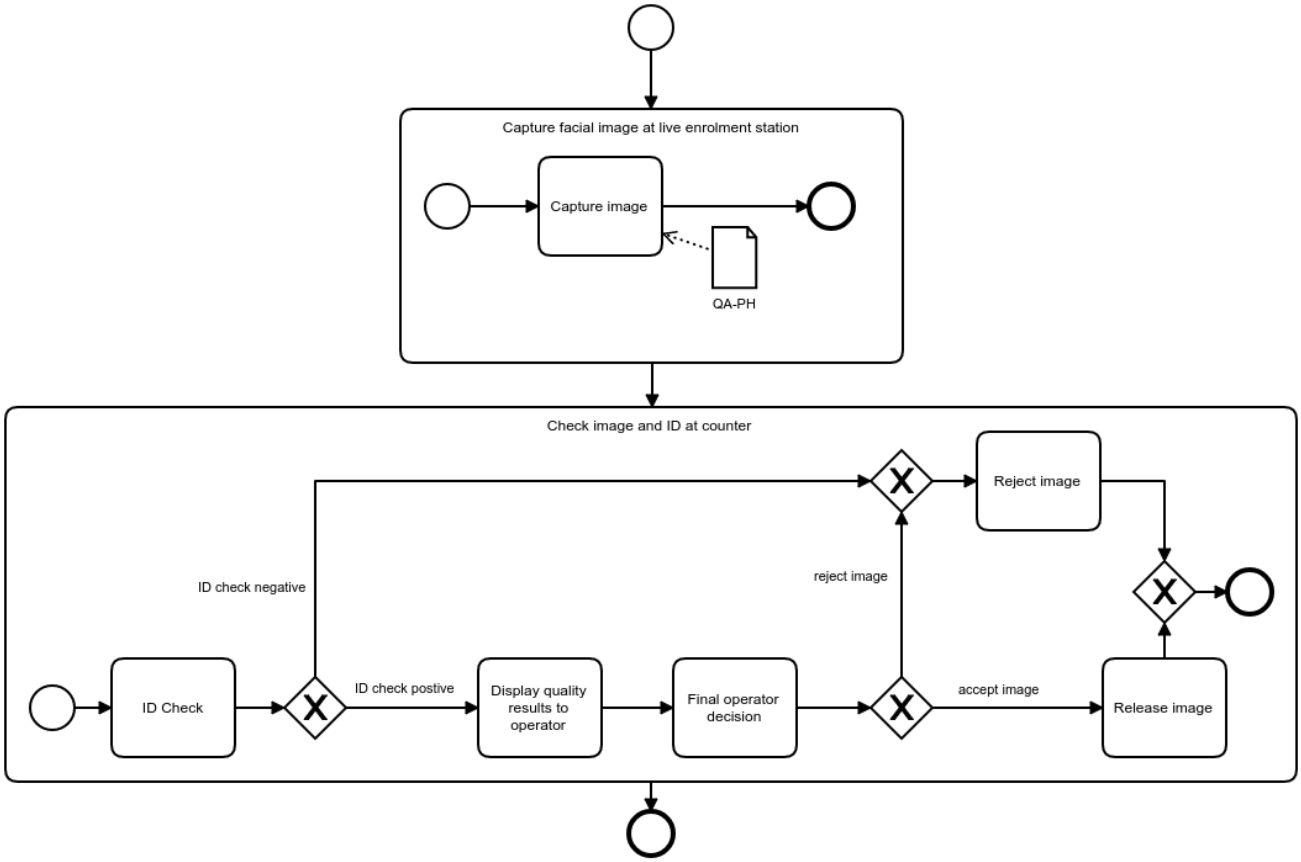

Figure 3-4: Image Provision from Live Enrolment Station

3.1.2 P-FP-PLAIN

This function block describes the overall process requirements for capturing up to ten plain fingerprints.

Requirements

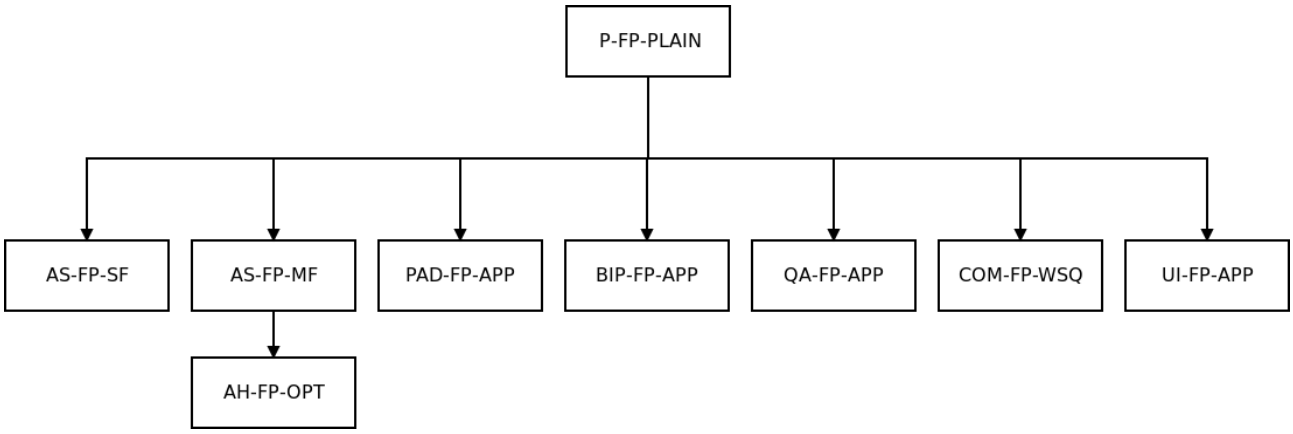

Figure 3-5: Relevant Function Blocks for Plain Fingerprint Acquisition Process

For fingerprint capture single-finger or multi-finger scanners can be used. Multiple lossy compressions on the fingerprint image data are not allowed during the process.

In the following, the process of capturing plain fingerprints for identification or enrolment purposes is described in detail. At the beginning of this section, an overview of the included Function Modules and the respective Function Blocks is given in advance.

The following FMs apply (see Figure 3-5).

— AH-FP-OPT
— AS-FP-MF
— AS-FP-SF
— PAD-FP-APP
— BIP-FP-APP
— QA-FP-APP
— COM-FP-WSQ
— UI-FP-APP

Furthermore, the official has to take the module O-FP-ACQ into account. Logging and coding of biometric data and quality data is conducted according to the given FM LOG and FM COD of the profile.

Acquire Plain Slap Task

Figure 3-6 depicts the basic capture sequence for a plain slap acquisition. A plain slap acquisition can be part of more complex acquisition processes, e.g. a ten finger acquisition by the 4-1-4-1 capture sequence for identification purposes. The plain slap capture acquisition is subsequently described in detail. The quality assessment is conducted according to the requirements of the applicable FM QA.

1. If the applicant is physically not capable to place all fingers of the slap on the acquisition hardware at the same time, the operator can decide to acquire each finger of the slap in single finger acquisition mode. Hereby, single finger acquisition mode refers to the “Acquire Plain Finger” task as described below.
2. The counter variable for the number of attempts for capturing the current slap is initialized as i = 1.
3. The slap image is acquired from hardware.
4. The fingerprints are segmented and each is assessed.
   a. In case the quality of the fingerprints meet 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) are temporarily stored.
   b. In case the quality requirements for one or more fingerprints of the slap are not met, the capture is repeated up to two times (i.e. the acquisition of a single slap consists of a maximum of three capture attempts).
5. A sequence check shall be conducted for the acquired slap image to detect the acquisition 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 sequence check as early as possible after a fingerprint image is available.
   a. In case the comparison of any finger of the current slap with any finger of a previous slap is successful, the sequence check shall throw an error.
   b. In case the comparisons of all fingers of the current slap with all fingers of previous slaps are not successful, the sequence check shall throw no error.

If the quality check of the third capture attempt fails, the best of the captured slaps is identified according to the corresponding QA Function Module and temporarily stored along with corresponding information. Note, that in verification scenarios no quality assessment is conducted by the QA module.

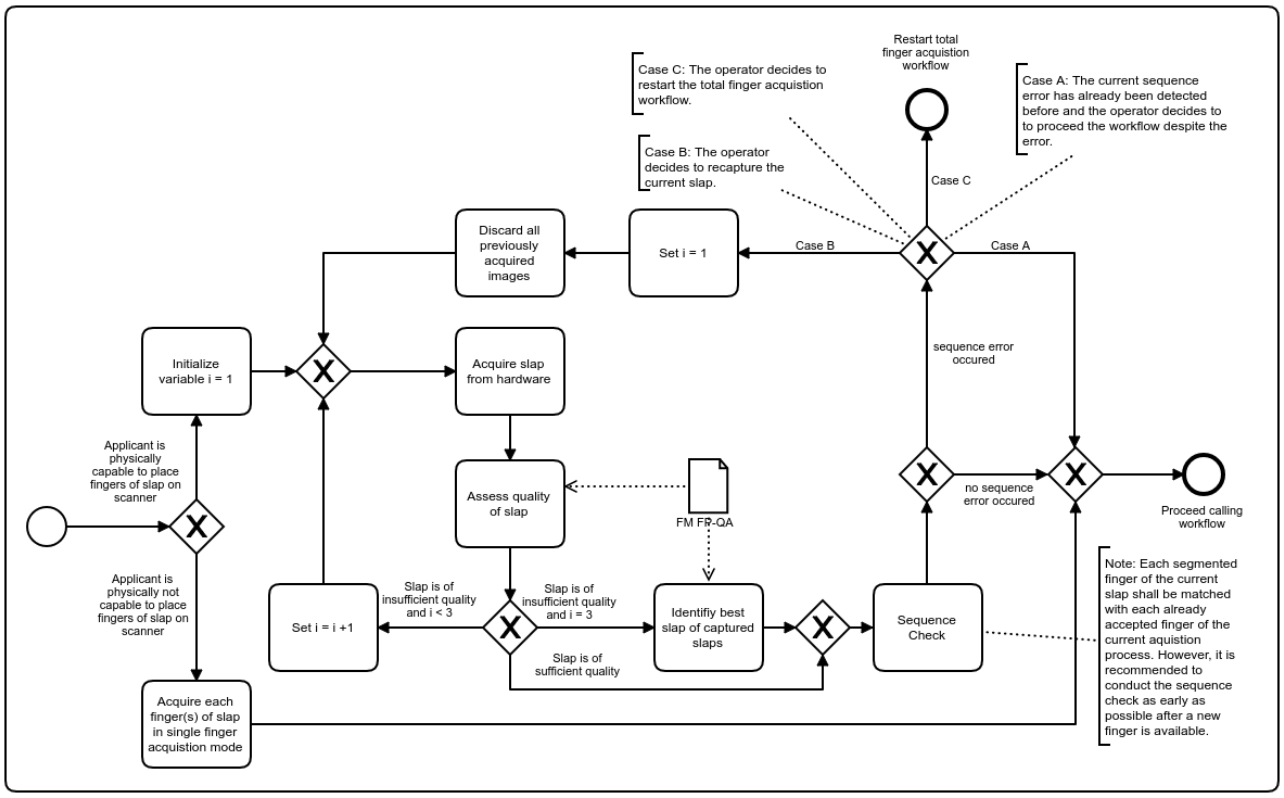

Figure 3-6: "Acquire Plain Slap" Task

“Capture Slap Unsupervised” Process

Figure 3-7 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 QA.

1. The slap image is retrieved from hardware.
2. The fingerprints are segmented and each is assessed.
   a. The PAD is carried out.
   b. The sequence check is conducted.
      i. If the sequence check fails, the captured image is discarded and the capture repeated.
      ii. If the sequence check fails for the second time for the same finger, the process continues with the quality assessment.
   c. In case the quality of the fingerprints meet the quality requirements defined in the corresponding Functional Module QA-FP, the captured slap and the set of segmented fingerprints and parameter data (e.g. quality values) are temporarily stored.
   d. The quality assessment shall be conducted within 300ms.
   e. 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 is stored with the set of segmented fingerprints and parameter data (e.g. quality values).
   f. In case the quality requirements for one or more fingerprints of the slap are not met, the capture is repeated if the timeout is not reached. The timeout starts with the start of retrieval of the first slap image from hardware and shall be configurable.

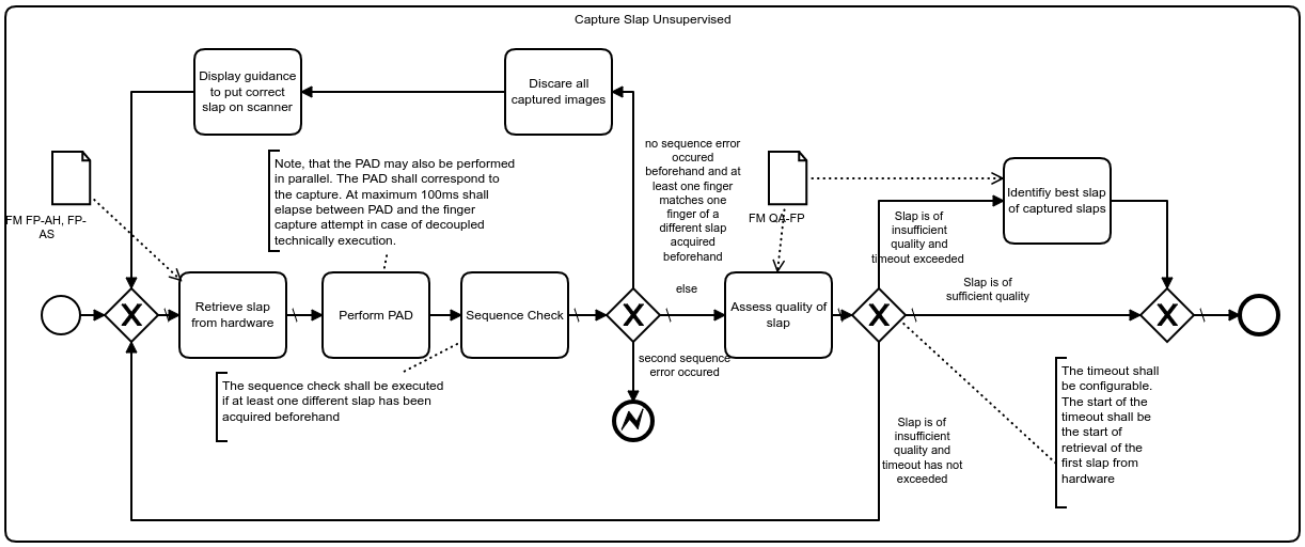

Figure 3-7: "Capture Slap Unsupervised" Task

“Capture Plain Finger Unsupervised” Process

Figure 3-8 depicts the basic process for a plain unsupervised finger capture. A plain finger capture can be part of more complex acquisition processes, e.g. a ten finger acquisition. The plain unsupervised finger capture is subsequently described in detail. The quality assessment is conducted according to the requirements of the applicable FM QA.

1. The finger image is retrieved from hardware.
2. The finger is assessed.
   a. The PAD is carried out.
   b. The sequence check is conducted.
      i. If the sequence check fails, the captured image is discarded and the capture repeated.
      ii. If the sequence check fails for the second time for the same finger, the process continues with the quality assessment.
   c. In case the quality of the fingerprint meets the quality requirements defined in the corresponding Functional Module QA-FP, the captured finger and parameter data (e.g. quality values) are temporarily stored.
   d. The quality assessment shall be conducted within 300ms.
   e. In case the timeout is reached and no finger image of sufficient quality was captured, the best finger image according to the corresponding QA Function Module is stored and parameter data (e.g. quality values).
   f. In case the quality requirements for the fingerprint is not met, the capture is repeated if the timeout is not reached. The timeout starts with the start of retrieval of the first finger image from hardware and shall be configurable.

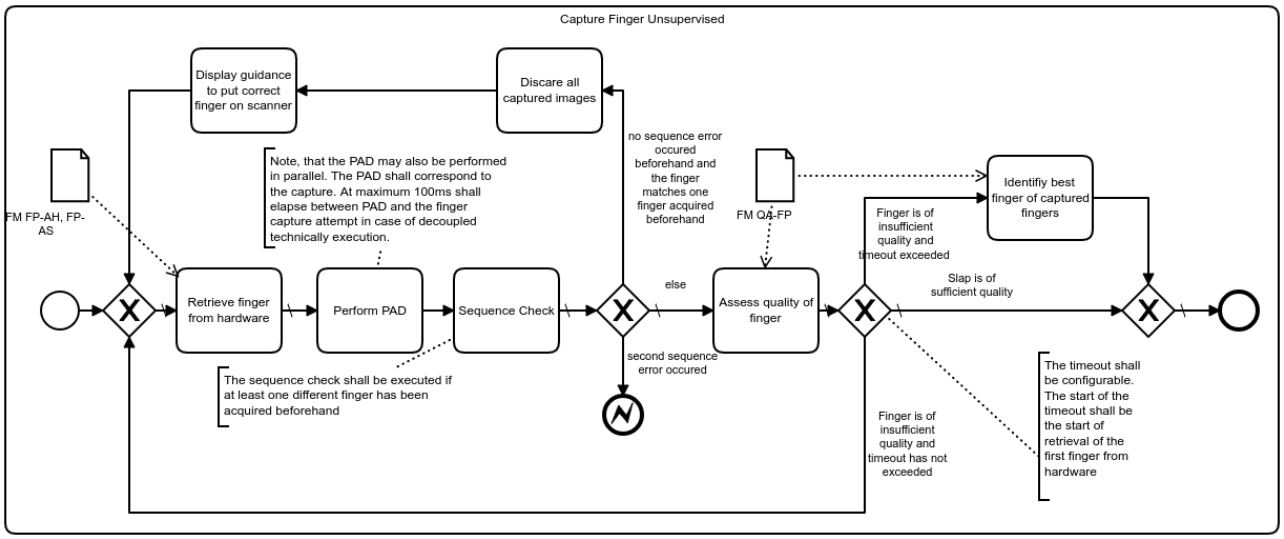

Figure 3-8: "Capture Plain Finger Unsupervised" Task

Acquire Plain Finger Task

Figure 3-9 depicts the basic capture sequence for a plain finger acquisition. A plain finger acquisition can be part of more complex acquisition processes e.g. a ten finger acquisition by the 4-1-4-1 capture sequence for identification purpose. The plain finger capture acquisition is described in detail subsequently. The quality assessment is conducted according to the requirements of the applicable FM QA.

1. The counter variable for the number of attempts for capturing the current slap is initialized as i = 1.
2. The finger image is acquired from hardware.
3. The fingerprint is assessed.
   a) In case the quality of the fingerprint meets the quality requirements defined in the corresponding QA Function Module, the captured fingerprint and parameter data (e.g. quality values) are temporarily stored.
   b) In case the quality requirements for the fingerprint is not met, the capture is repeated up to two times (i.e. the acquisition of a finger consists of a maximum of three capture attempts).
4. A sequence check shall be conducted for the acquired finger image to detect the acquisition 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 sequence check as early as possible after a fingerprint image is available.
   a) In case the comparison of the current finger with any previously captured finger is successful, the sequence check shall throw an error.
   b) In case the comparison of the current finger with any previously captured finger is not successful, the sequence check shall throw no error.

If the quality check of the third capture attempt fails, the best of the captured fingerprint images is identified according to the corresponding QA Function Module and temporarily stored along with corresponding information. Note, that in verification scenarios no quality assessment is conducted by the QA module.

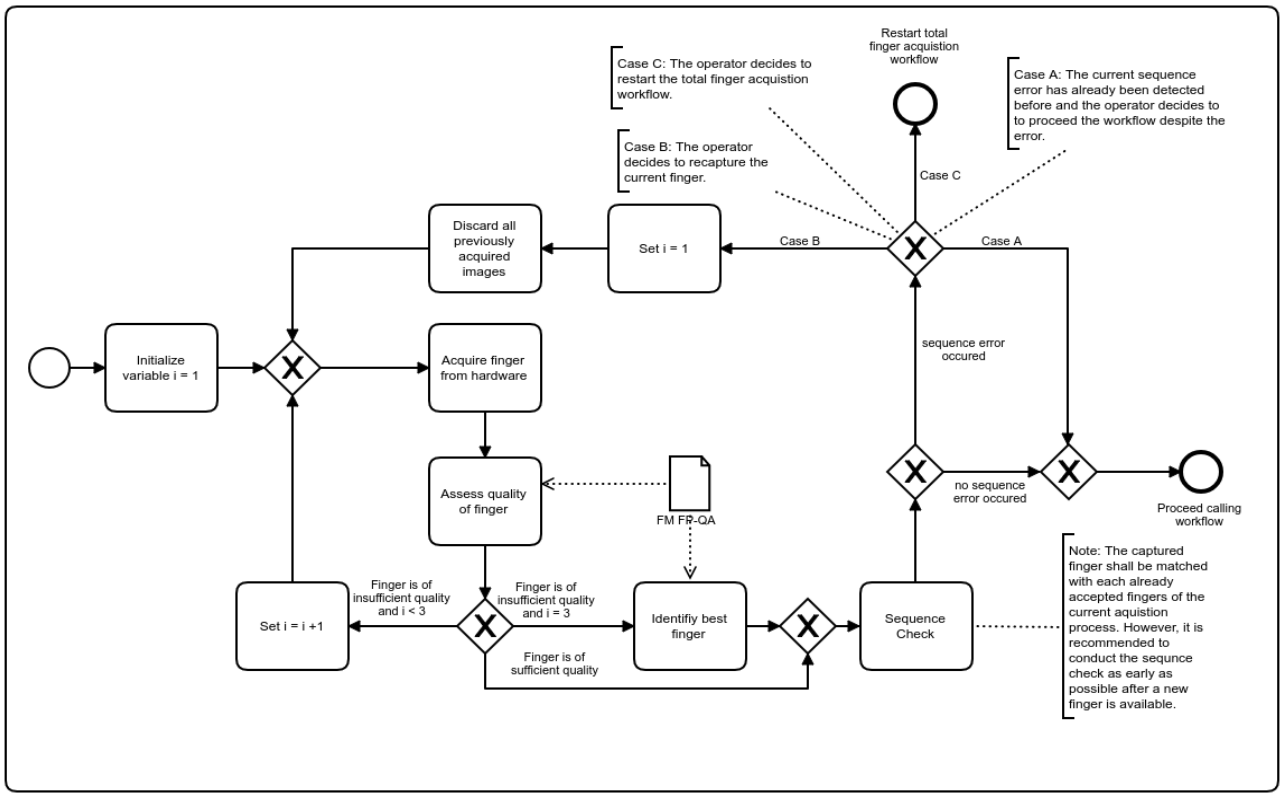

Figure 3-9: "Acquire Plain Finger" Task

Fingerprint Acquisition Processes

In the following fingerprint acquisition processes for enrolment, verification and identification processes are defined. Thereby, processes can be tailored to single-finger or multi-finger hardware. The processes use the acquisition process of plain slaps or fingers. The task “Acquire Plain Slap” refers to Figure 3-6 and the task “Acquire Plain Finger” refers to Figure 3-9. The remarks in brackets denote the fingers to capture by the individual capture process. It is recommended to select missing fingers for each slap right before the slap is captured. Selection of all missing fingers at the beginning of an acquisition process is also possible.

Figure 3-11 depicts the acquisition process for the 4-4-2 enrolment scenario and Figure 3-10 depicts the acquisition process for the 4-4-2 identification scenario. The 4-4-2 sequences are described in detail subsequently:

1. Acquire right hand: index finger, middle finger, ring finger, little finger
2. Acquire left hand: index finger, middle finger, ring finger, little finger
3. Thumbs of both hands (simultaneously)

In case of an enrolment scenario, additional single finger captures are possible for each slap capture after the slap capture itself. This variant is only recommended if a slap capture does not yield to sufficient quality.

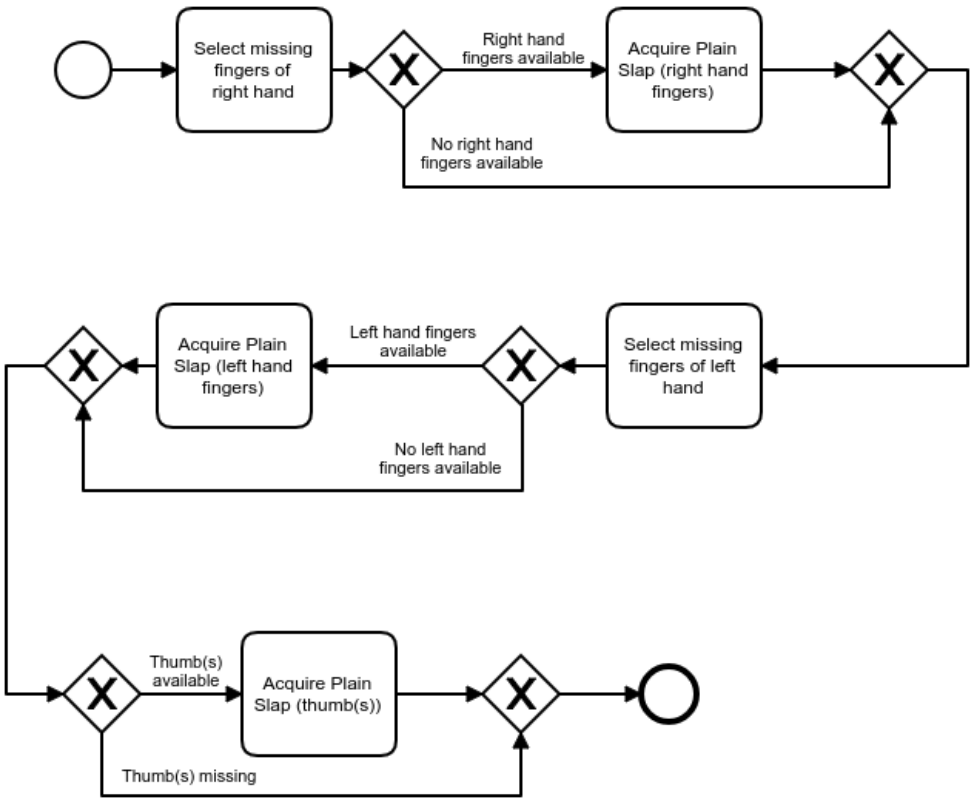

Figure 3-10: Acquisition Workflow for 4-4-2 Identification

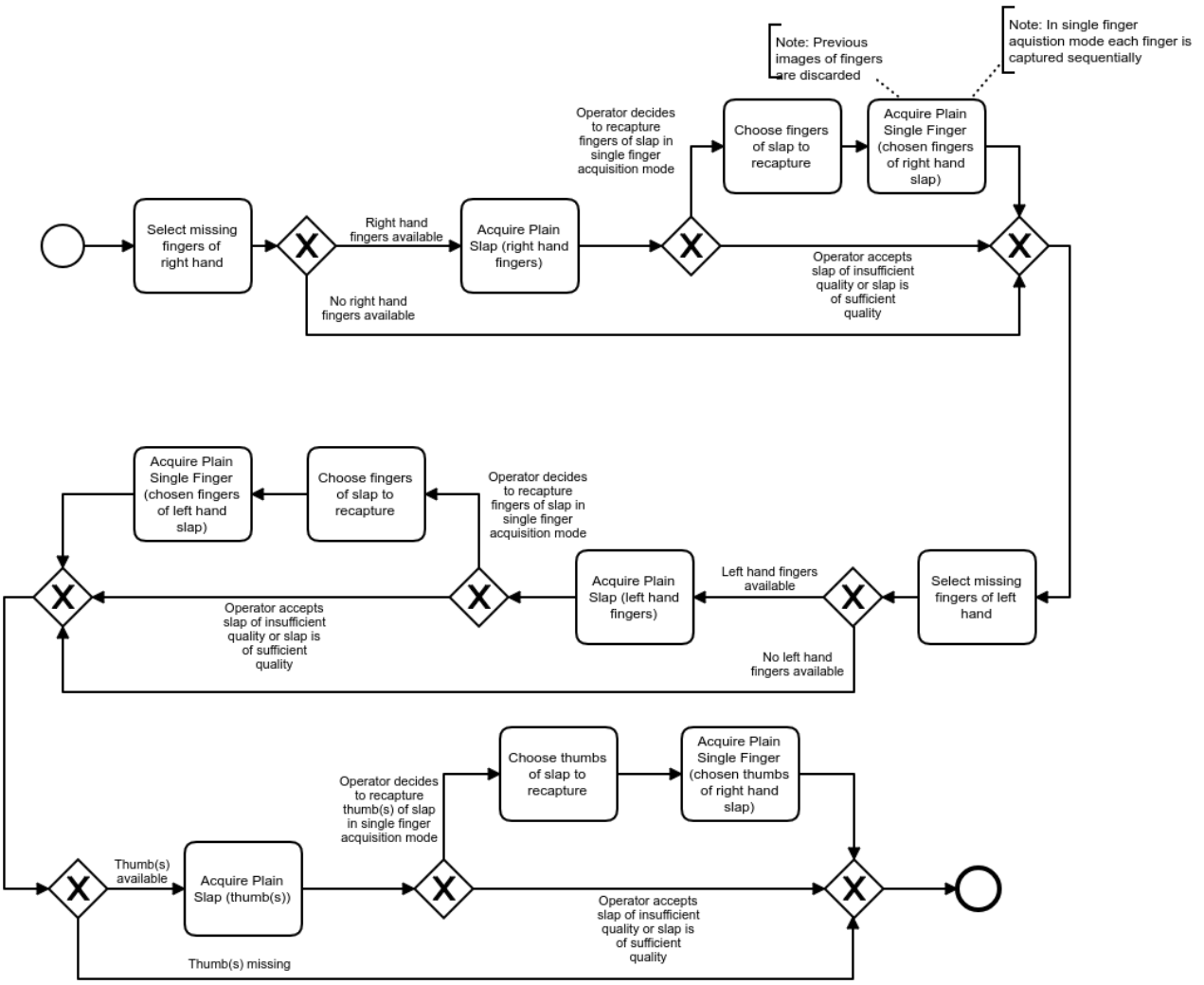

Figure 3-11: Acquisition Workflow for 4-4-2 Enrolment

Figure 3-12 depicts the acquisition process for 4-1-4-1 the enrolment scenarios and Figure 3-13 depicts the acquisition process for 4-1-4-1 the identification scenario. The 4-1-4-1 sequences are described in detail subsequently:

1. Acquire right hand: index finger, middle finger, ring finger, little finger
2. Acquire right hand: thumb
3. Acquire left hand: index finger, middle finger, ring finger, little finger
4. Acquire left hand: thumb

In case of a plain finger enrolment scenario, additional single finger captures are possible for the slaps. This variant is only recommended if a slap capture does not yield to sufficient quality.

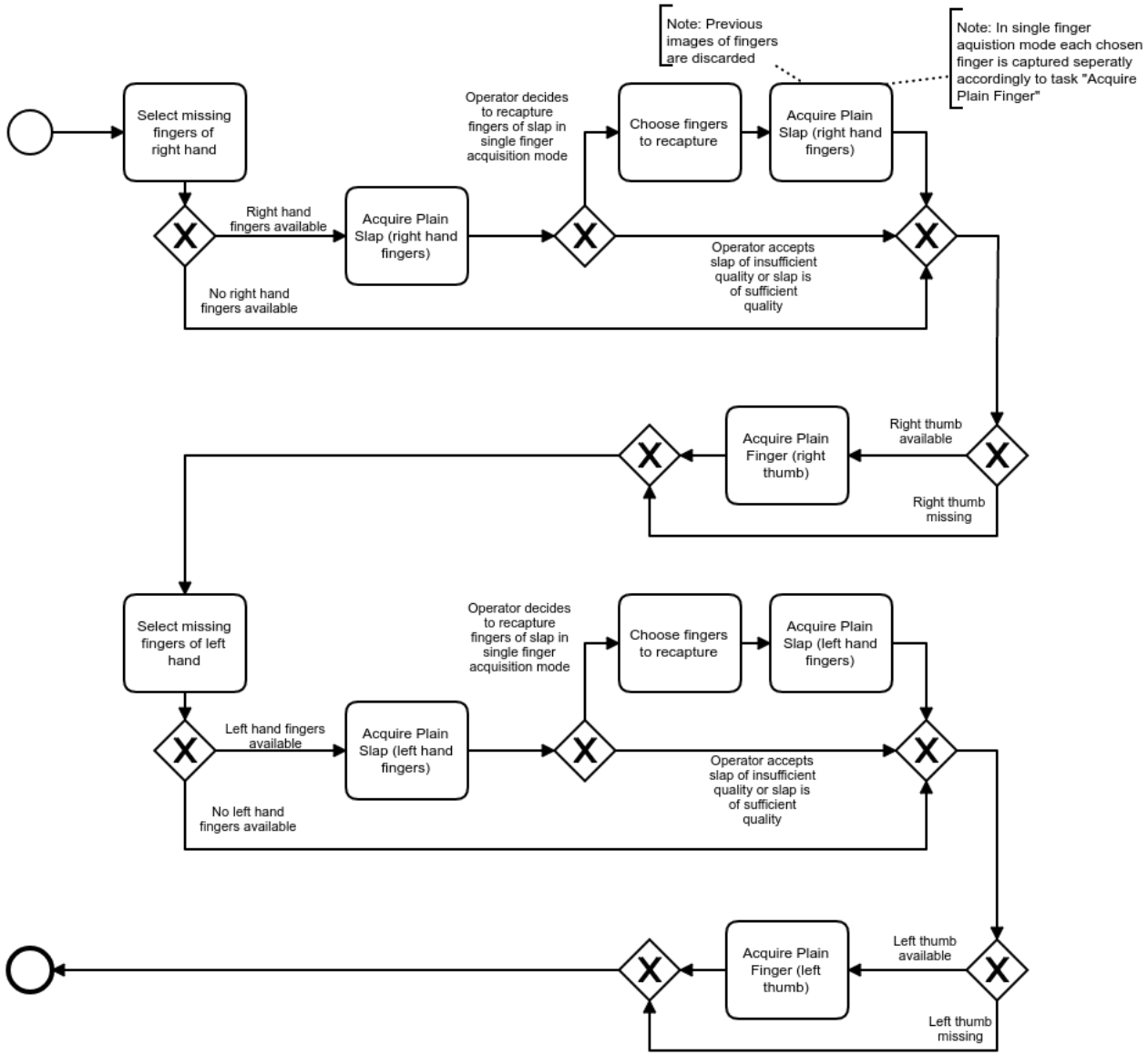

Figure 3-12: Acquisition Workflow for 4-1-4-1 Enrolment

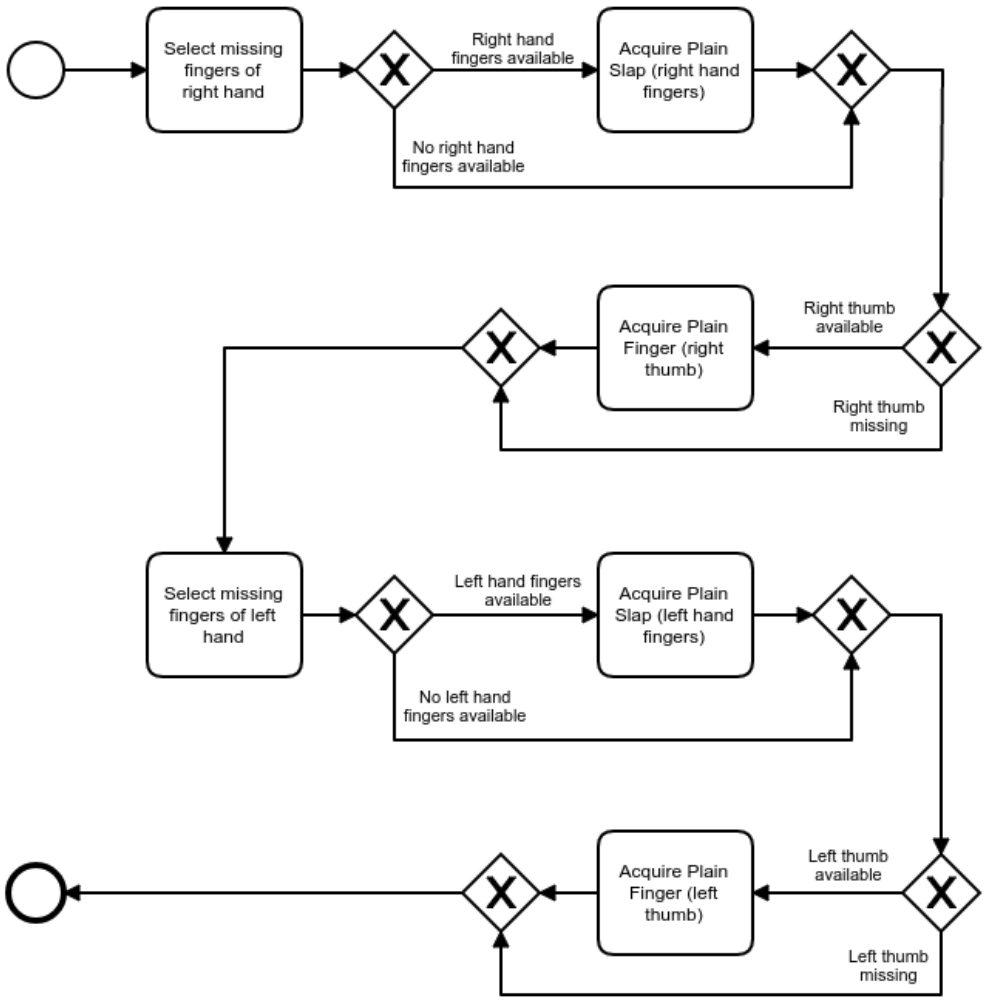

Figure 3-13: Acquisition Workflow for 4-1-4-1 Identification

Figure 3-14 depicts the acquisition process for two finger enrolment on single finger hardware, Figure 3-15 depicts the acquisition process for two finger enrolment on multi finger hardware. The two finger acquisition sequences are described in detail subsequently:

Sequence option for two finger enrolment capture with multi-finger acquisition hardware

1. Acquire right index finger, left index finger (as two-finger slap)
2. In case of insufficient index finger quality, alternative finger(s) should be acquire for each index finger of insufficient quality. First further fingers from the right hand are acquired in single-finger mode (if any available), then further fingers from the left hand. Further fingers are considered in the following order: thumb, middle finger, ring finger. The index fingers are not recaptured.
3. In any case, at least one further finger (if available) for each hand shall be acquired if the index finger does not fulfil the quality requirements.

Sequence option for two finger enrolment capture with single-finger acquisition hardware

1. Right index finger (followed by optional capture of thumb, middle finger, ring finger of the right hand)
2. Left index finger (followed by optional capture of thumb, middle finger, ring finger of the left hand)
3. In any case, at least one further finger (if available) for each hand shall be acquired if the index finger does not fulfil the quality requirements.

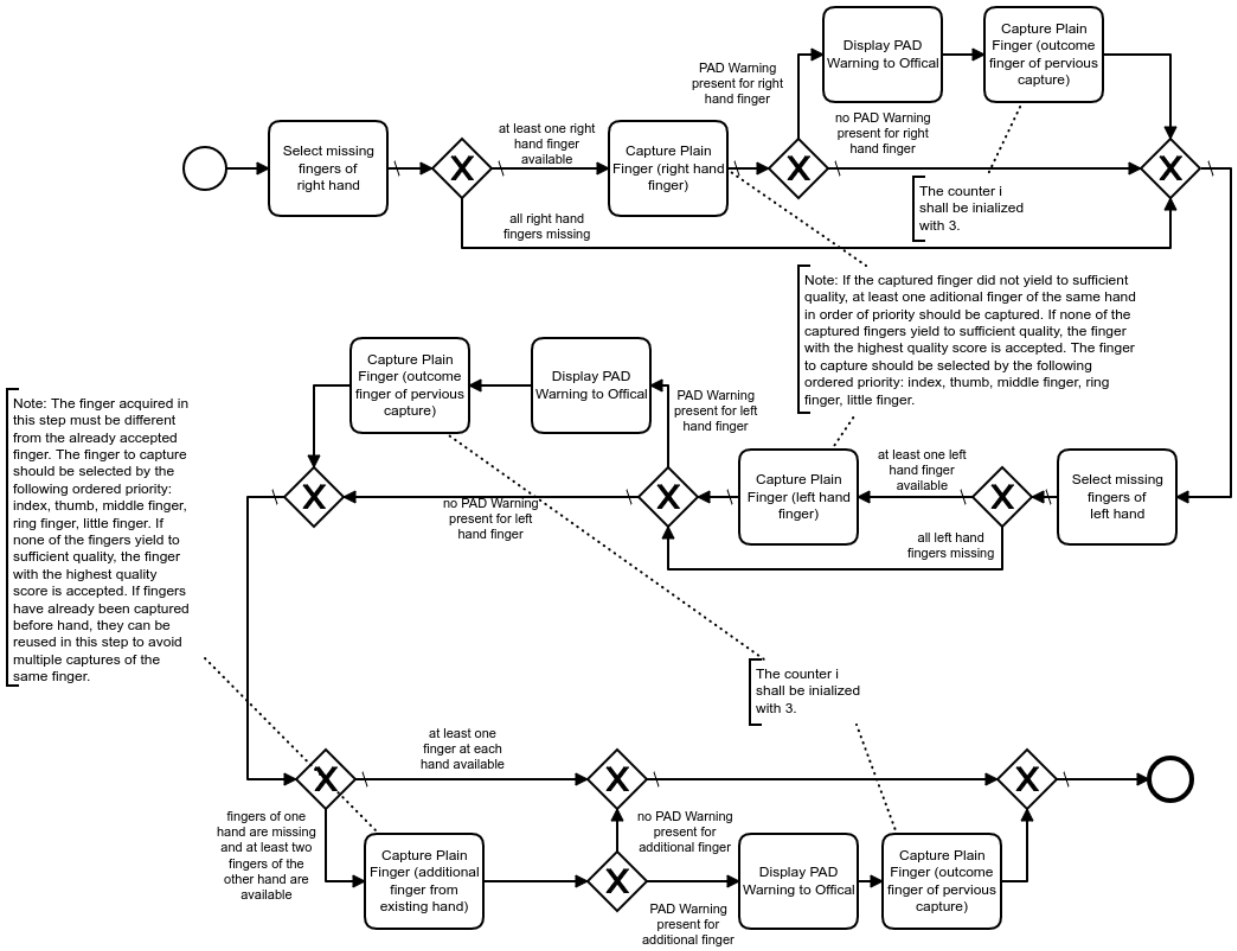

Figure 3-14: Acquisition Workflow for Two Finger Enrolment Single Finger Hardware

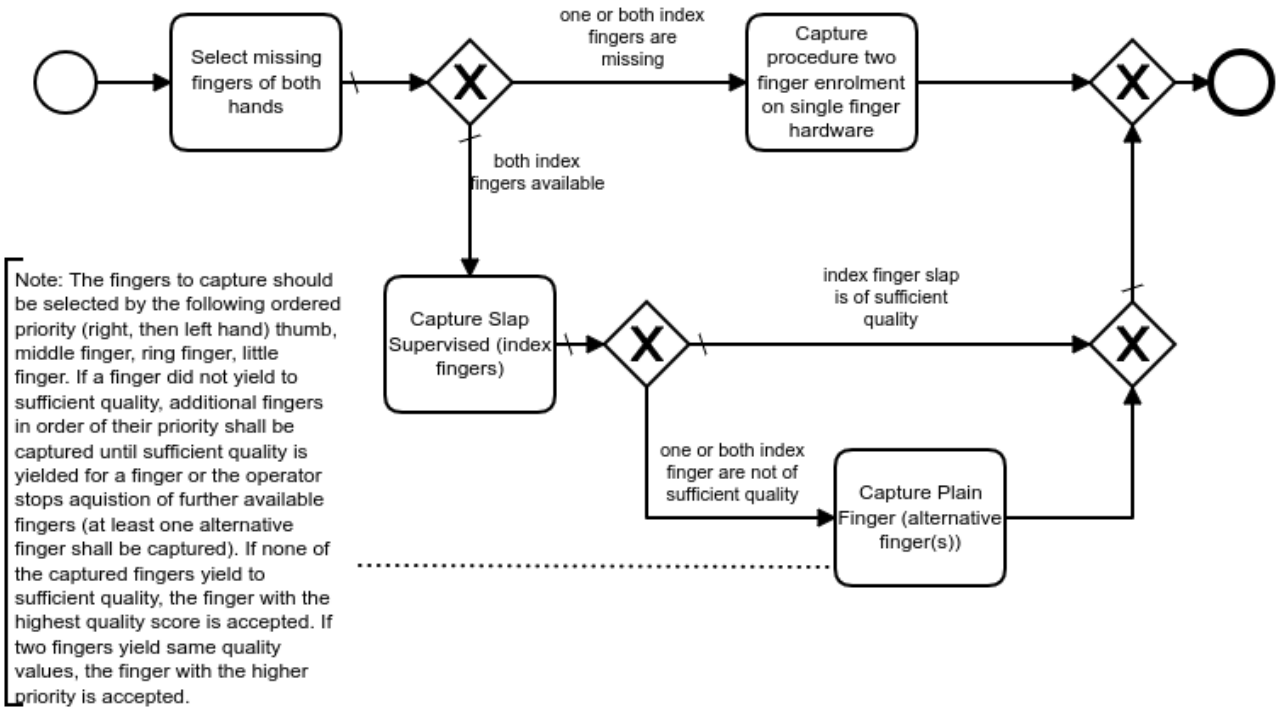

Figure 3-15: Acquisition Workflow for Two Finger Enrolment Multi Finger Hardware

Two Finger Plain Unsupervised Acquisition On Multi-Finger Hardware for Enrolment

Figure 3-16 depicts the unsupervised acquisition process for two finger enrolment on multi finger hardware. Note, that the “Capture Slap Supervised” process is used here. The sequence is described in detail subsequently:

1. Acquire right index finger, left index finger (as two-finger slap)
2. In case of insufficient index finger quality, alternative finger(s) should be acquire for each index finger of insufficient quality. First further fingers from the right hand are acquired in single-finger mode (if any available), then further fingers from the left hand. Further fingers are considered in the following order: thumb, middle finger, ring finger. The index fingers are not recaptured.
3. In any case, at least one further finger (if available) for each hand shall be acquired if the index finger does not fulfil the quality requirements.

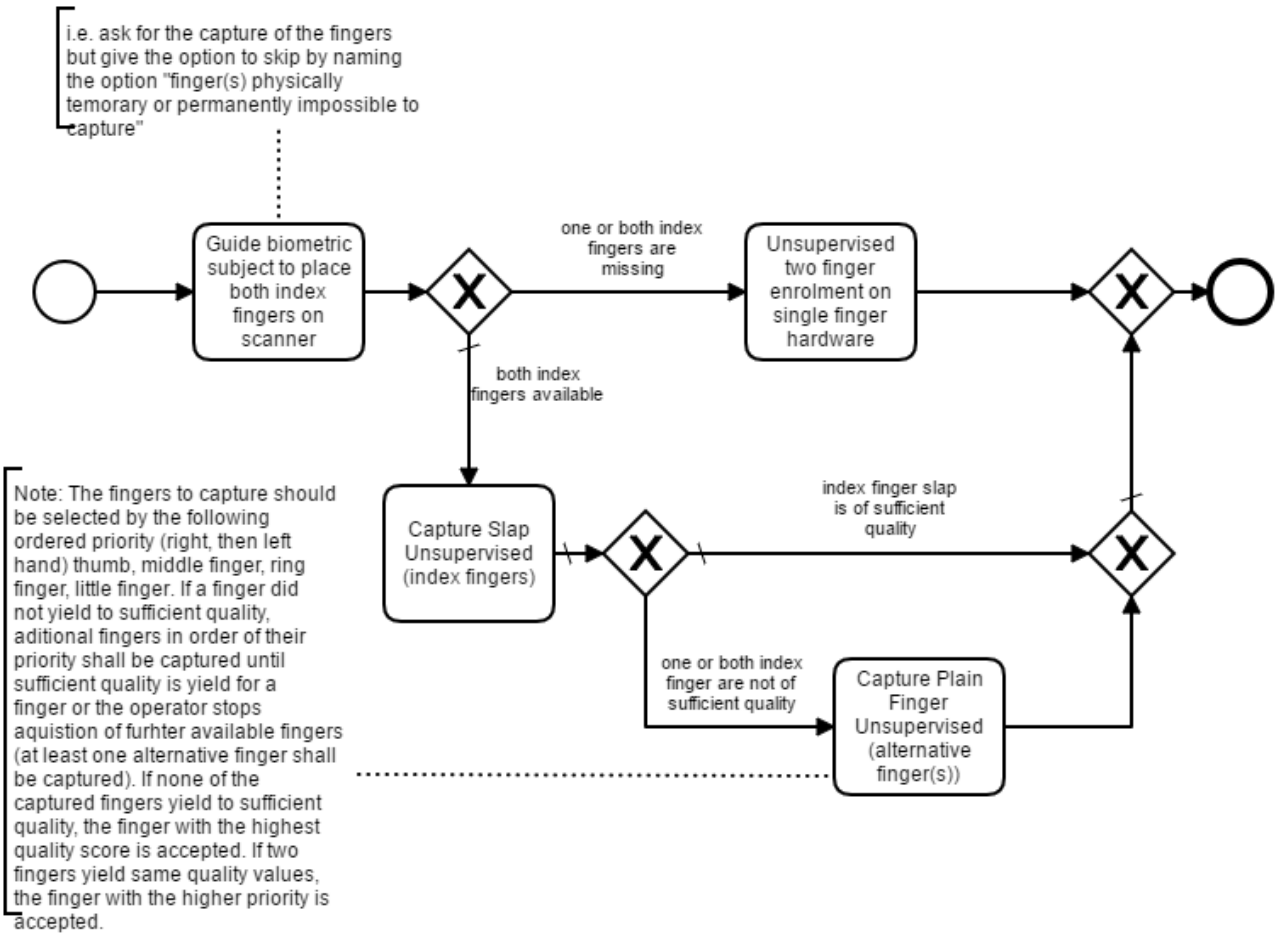

Figure 3-16: Unsupervised Acquisition Process for Two Plain Finger On Multi Finger Hardware for Enrolment

Two Finger Plain Unsupervised Acquisition On Single-Finger Hardware for Enrolment

Figure 3-17 depicts the unsupervised acquisition process for two finger enrolment on single finger hardware. Note, that the “Capture Plain Finger Unsupervised” process as defined is used here.

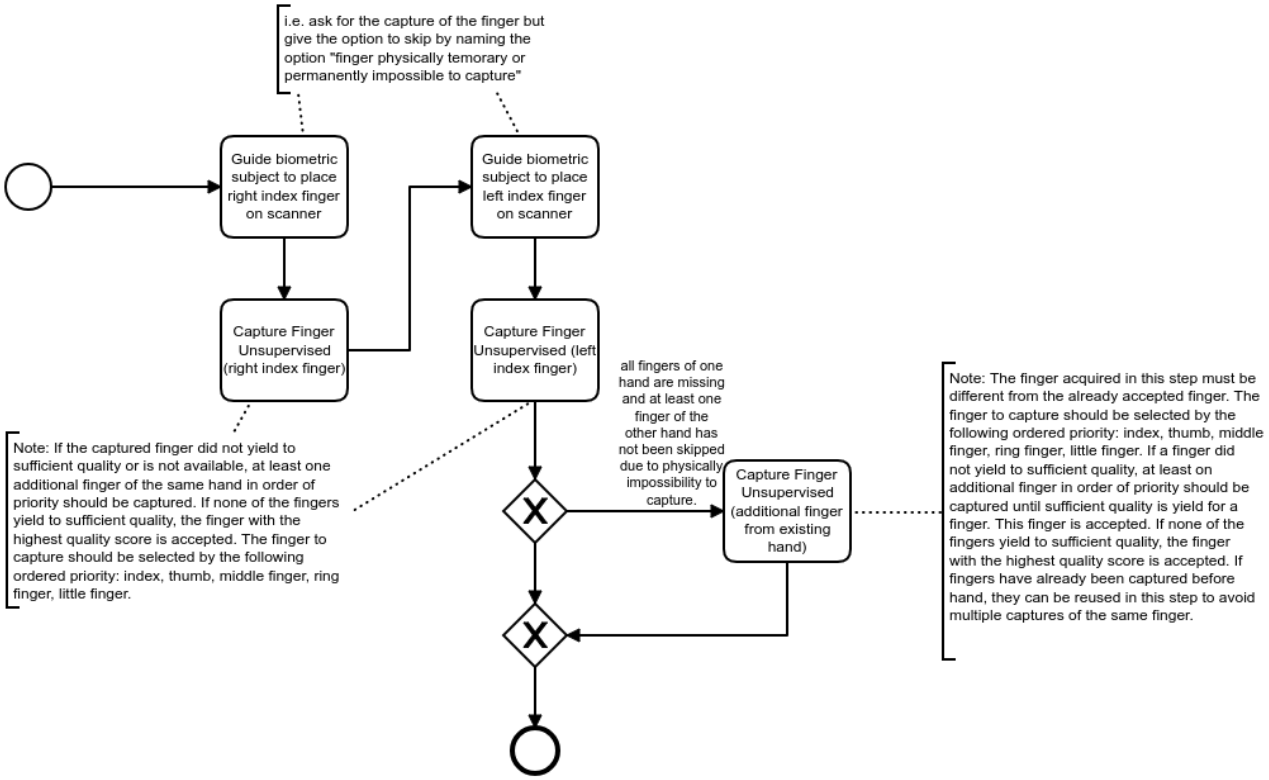

Figure 3-17: Unsupervised Acquisition Process for Two Plain Finger Single Finger Hardware for Enrolment

3.1.3 P-IR-APP

This function block describes the alternatives and the overall process requirements for the provisioning of iris images for enrolment purposes.

Requirements

All acquired iris images shall be of one of the following types according to the standard [ISO_IRIS].

- IMAGE_TYPE_VGA
- IMAGE_TYPE_CROPPED
- IMAGE_TYPE_CROPPED_AND_MASKED

Multiple lossy compressions of iris image data are not allowed within the overall process.

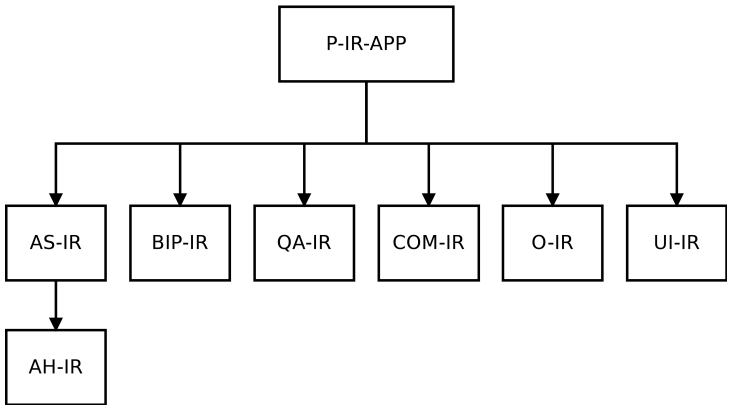

Figure 3-18: Relevant Function Blocks for Iris Image Process

In order to obtain an iris image that complies with all specified requirements the following process has to be followed. In this context, several Function Modules and the according Function Blocks are involved and the respective requirements have to be fulfilled.

- FM Acquisition Hardware (FM AH)
- FM Acquisition Software (FM AS)
- FM Biometric Image Processing (FM BIP)
- FM Compression (FM COM)
- FM Quality Assurance (FM QA)
- FM Coding (FM COD)
- FM Operation (FM O)

The respective detailed function modules from the corresponding application profile apply. Note: Not all profiles support all the options that are presented in the next sections.

A live enrolment station is used that works with an integrated Quality Assurance module (see module COD). The requirements of modules AH, AS and BIP apply. The quality is checked directly while the image is taken. If the quality is not suitable, the acquisition can be started again. If the quality is sufficient, the image can be released for the application counter. For security reasons it has to be checked that applicant does not present printed contact lenses (see module O). If the presentation attack check within the application counter is successful and the official accepts the image for further use, the image is used for the further processing, otherwise the official gives a veto.

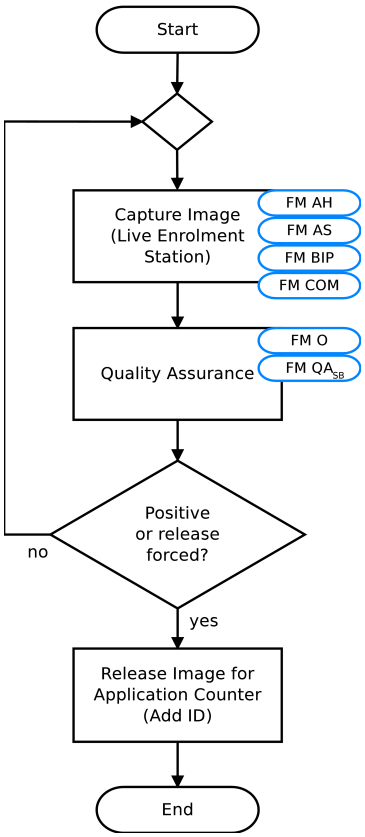

Figure 3-19: Digital Provision of an Iris Image

Note: If the operator gives a veto (veto equals yes) a negative software decision of the quality assurance can be overruled and the iris image is released. In case of a positive software decision of the quality assurance, the operator may reject the iris image (e.g. if the iris image is not from the person to enrol or a presentation attack is assumed).

3.2 Acquisition Hardware

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

3.2.1 AH-PH-DC

This function block describes the requirements and interfaces for digital cameras and physical setup that are used to obtain facial biometrics.

Requirements

For digital cameras the following requirements have to be met.

- physical resolution that allows a cropping of an image to 1600x1200 pixels without any upscaling
- adequate image quality to match requirements of [ISO_FACE]

— The physical and environmental conditions for capturing facial photos, such as the positioning of the camera, proper lighting of the face and a uniform background as described in Annex C of [ISO_FACE] have to be complied with.

3.2.2 AH-FP-OPT

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

Requirements

For the acquisition of the fingerprints, optical sensors using the principal of frustrated total reflection or direct contact (the imaging system is the sensor surface, typically separated by a transparent protection layer) according to setting level 31 or 41 in table 1 of [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 [EBTS/F]). Notwithstanding, a capturing area of at minimum 16 mm width and 20 mm height is required (deviating from table F 1 in [EBTS/F]) for single finger scanners.

Grayscale Linearity

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

Resolution and Geometrical Accuracy

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

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

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

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

Along-Bar geometric accuracy: When scanning a 1.0 cy/mm, multiple parallel bar target, in both vertical bar and horizontal bar orientations, the maximum difference in the horizontal or vertical direction,

respectively, between the locations of any two points within a 1.5 inch segment of a given bar image, shall be less than 0.016 inches for at least 99% of the tested cases in each print block measurement area and in each of the two orthogonal directions.

Contrast Transfer Function

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

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

Table 3-1: Minimum and Maximum Modulation

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

— 500 ppi scanner, for f = 1.0 to 10.0 cy/mm:
CTF = 3.04105 * 10^{-4} * f2 - 7.99095E-02 * f + 1.02774 [EQ 1]
— 1000 ppi scanner, for f = 1.0 to 20.0 cy/mm:
CTF = - 1.85487 * 10^{-5} *f3 +1.41666E-03*f2 - 5.73701E-02* f +1.01341 [EQ 2]

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

Signal-to-Noise Ratio and the Gray–Level Uniformity

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

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

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

Gray Scale Range of Fingerprint Images

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

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

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

3.2.3 AH-IR-DC

This function block describes the requirements and interfaces for digital cameras and physical setup that are used to obtain iris biometrics.

Requirements

For digital cameras the following requirements have to be met.

- The cameras must capture images with a physical resolution of at least 640x480 pixels that allows cropping of an iris image without any upscaling.
- Images of adequate quality must be captured conforming to requirements 6.2.2, 6.2.3, 6.2.5 and 6.2.10 of [ISO_IRIS_QA].
- Adequate physical setup and environmental conditions for capturing iris images should be provided such that they facilitate capturing iris images conforming to requirements 6.2.7 and 6.2.9 of [ISO_IRIS_QA].
- Adequate physical setup and environmental conditions for capturing iris images may be provided such that they facilitate capturing iris images conforming to requirements 6.3.1, 6.3.2 and 6.3.3 of [ISO_IRIS_QA].

3.3 Acquisition Software

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

3.3.1 AS-PH-DC

This function block describes the requirements and interfaces for Acquisition Software used for digital cameras in order to obtain digitised images.

Requirements

The image data should to be provided without any compression in one of the following image formats: Windows Bitmap Format Version 3, JPEG Lossless, DNG (in combination with JPEG Lossless).

If the acquisition device does not support a lossless mode, the image can alternatively be provided in JPEG mode with the minimal level of compression possible. In normal mode of operation, no compression artefacts shall be detectable in the image.

Recommendations

Acquisition Software that supports calibration procedures for the respective digital camera should be used (in particular colour management).

3.3.2 AS-FP-MF

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

Requirements

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

For the acquisition process, a pre-qualification of the fingerprints to prefer high quality has to be used. The activation of the acquisition has to occur automatically. The capture should prefer the highest quality image of all images within the sequence, that present a quality above a to be defined scanner-specific threshold. In the case of a time-out, at least the last captured image is returned.

If the Acquisition Software allows multiple thresholds for pre-qualification, the thresholds shall be documented by the vendor and be configurable by the system administrator.

It is possible that this functionality is part of the hardware firmware and may not be available as separate software component.

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

3.3.3 AS-IR-DC

This function block describes the requirements and interfaces for Acquisition Software used for digital cameras in order to obtain digitised iris images.

Requirements

The image data should be provided in PNG format without lossy compression.

Recommendations

Acquisition Software that supports calibration procedures for the respective digital camera should be used (in particular colour management).

3.4 Presentation Attack Detection

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

3.4.1 PAD-FP-APP

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

Requirements

General Requirements

The capture system shall contain a presentation attack detection subsystem according to [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 presentation attack detection subsystem may consist of hardware and software (e.g. the used fingerprint scanner may have additional sensors designed for this purpose).

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

The presentation attack detection shall be conducted both in supervised acquisition scenarios, e.g. in a counter scenario, and in unsupervised acquisition scenarios, e.g. in self-service scenarios. Thereby, the presentation attack detection shall be conducted for all acquisition purposes e.g. enrolment, identification and verification.

Neither the presentation attack detection result nor presentation attack score shall be displayed to the person who's fingerprints are acquired.

Performance

The presentation attack system's usability in the field in terms of bona fide presentation classification error rate (BPCER) and bona fide presentation non-response rate (BPNRR) as defined by [ISO_PAD_3] should be compliant with the thresholds in Table 3-2.

Usability Metric	Threshold
BPCER	< 2%
BPNRR	< 1%

Table 3-2: Usability Metrics PAD

Self-Service Scenarios Requirements

In self-service scenarios where the person who's fingerprints shall be acquired uses an unsupervised fingerprint scanner, the presentation attack detection results from the unsupervised acquisition shall be displayed to a responsible process operator in case of a presentation attack detection and should be displayed to a responsible process operator in case of no presentation attack detection.

Integration Requirements

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

If the module is used within a comparison scenario, it is allowed to only signal the detection result in conjunction with a positive matching decision. In any case, the omission of the detection result shall be signalled.

Certification Requirements

To ensure comparable performance of presentation attack detection subsystems, single finger devices shall be certified under the Common Criteria Agreement according to the Protection Profiles stated below. The certification of multi finger devices under the stated Protection Profiles is recommended[3].

- 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)

Maintenance Requirements

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

Transitional Rules

The requirements of this module only apply to devices and software put into operation after November 1, 2019.

After November 1, 2019, only software updates are allowed for non-certified PAD fingerprint scanners.

3.5 Biometric Image Processing

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

3.5.1 BIP-PH-DC-HQ

This function block describes requirements and interfaces for Biometric Image Processing with respect to the output of digital cameras to obtain a high quality facial image that fulfills the ISO requirements.

General Requirements

As a result of the image processing of this module, a facial image has to be generated that is compliant to the requirements of full frontal images specified in [ISO_FACE]. As a precondition, the person, a photograph is taken from, has to behave in a cooperative manner. The minimum distance between both eyes for capture positions of the applicant in the preferred area of the camera range shall be at last 120 pixel.

Basically, the image processing encloses cropping the facial image, resulting in images with a height/width ratio of 4:3. The general requirements for the image cropping in Table 3-3 apply to all images if no dedicate requirements are defined for a given use case in this Functional Module.

3 This is expected to be a mandatory requirement in a future version of this guideline.

Criterion	Value	Unit
Image height	1600	Pixel
Image width	1200	Pixel

Table 3-3: Requirements for the Size of Facial Images

Depending on the requirements of the COD modules, multiple differently cropped versions of the image might be created at this step of image processing.

Requirements GSAT Transactions

Requirements in Table 3-3 do not apply for GSAT transactions. The requirements in Table 3-4 apply to images used in GSAT transactions.

Criterion	Value	Unit
Image height	800	Pixel
Image width	600	Pixel

Table 3-4: Requirements for the Size of Facial Images in GSAT Transactions

Requirements on Printing

If the image is also used for printing to the target size of 45mm x 35mm, it shall be cropped equidistantly from the original 4:3 aspect ratio.[4]

3.5.2 BIP-FP-APP

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

Requirements

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

Depending on the call to capture one, two, three or four fingerprints, this number of individual fingerprints has to 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 have to be fulfilled.

- Ability to accept rotated fingerprints in the same direction up to 45°
- Rotated fingerprints in the same direction have to be corrected to be vertical
- Segment the first part of the finger (fingertip)

4 Note that for the purpose of biometric processing, the 45:35 image is not considered any further.

— Segmentation has to occur on uncompressed data

3.5.3 BIP-IR-APP

This function block describes requirements and interfaces for Biometric Image Processing with respect to the output of digital cameras to obtain a iris image that fulfills the ICAO requirements for travel documents.

Requirements

As a result of the image processing of this module, the Acquisition Software must generate iris images complying to at least one of the following image types defined by [ISO_IRIS].

— IMAGE_TYPE_VGA
— IMAGE_TYPE_CROPPED
— IMAGE_TYPE_CROPPED_AND_MASKED

3.6 Quality Assurance

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

3.6.1 QA-PH-SB

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

Requirements

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

The standard which is relevant for the quality of facial images [ISO_FACE] hierarchically describes requirements to the facial images. In the following, full frontal images are expected.

The QA module has to analyse and to evaluate all of the quality criteria listed in Table 3-5. For the criteria marked with "M", the quality values must be provided while quality values for the criteria marked with "O" may be provided in the defined format according to the respective criteria.

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

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

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

The QA module should operate on cropped images retrieved from the image processing according to FM BIP PH. Quality assurance must not happen on uncropped images.

ID	Criterion	ISO-Ref.[5]	M/O[6]	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 Compare [ISO_FACE]
6 Mandatory/Optional

ID	Criterion	ISO-Ref.	M/O	Unit/Range
5.7	Eye distance	8.4.1 A3.1.1	M	In pixel
Subject lighting				
6.1	Equally distributed lighting	7.2.7	O	Arbitrary units
6.2	No shadows over the face nor in the eye-sockets	7.2.8 7.2.9	O	Arbitrary units
6.3	No hot spots on skin	7.2.10	O	Arbitrary units
6.4	No effects on glasses	7.2.11	O	Arbitrary units
Image characteristics				
7.1	Proper exposure	7.3.2	M	Arbitrary units
7.2	Focus and depth of field	7.3.3	M	Arbitrary units
7.3	No unnatural colours	7.3.4	O	Arbitrary units
7.4	No red eyes	7.3.4	O	Arbitrary units
7.5	Colour space	7.4.2.3	M	RGB-24bit, YUV422, 8bit-grey scale
7.6	Grey scale density and colour saturation	7.4.2.1 7.4.2.2	M	Counted numbers of intensity values existing within the image

Table 3-5: Mapping of Relevant Quality Criteria

If defined, the thresholds for specific application profiles are detailed in Table 3-6.

ID	Criterion	Minimum	Maximum	Unit/Range
Image for passport chip (GID), ratio 45:35				
1.3	Roll, nose axis	-8	8	Degrees
5.1	Image height	403	423	In pixel
5.2	Image width	521	541	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
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

ID	Criterion	Minimum	Maximum	Unit/Range
5.7	Eye distance	90	-	In pixel
Image for Central Identity Register (AAD), ratio 4:3				
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
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 3-6: Application Specific Thresholds for Facial Images[7]

3.6.2 QA-PH-PG

This function block describes requirements for a photo guideline that is used for Quality Assurance.

Requirements

If the quality assurance is to be performed by a person, visual tools like a photo guideline [PhotoGuide] can be used for support.

The visual check with the photo guideline [PhotoGuide] must always be done even if the checks with the photo template and/or the QA software will be performed afterwards. A recent picture is required according to Annex A of [ISO_FACE].

If these basic criteria are not met, the image is rejected without any further checks by the software or the photo template.

In the case of the photo guideline, the following criteria have to be described, preferably using sample images for compliant and non compliant images (compare [ISO_FACE]):

— frontal pose

7 For quality criterion ID 5.5 “Vertical position of the face” the effective thresholds are [0,3; 0,5] according to the Technical Corrigenda of [ISO_FACE].

- neutral expression
- mouth closed
- eyes open
- no occlusion (glasses, hair, eye patch)
- eyes looking to the camera
- background uniformity (plainness, no textures, colour)
- no shadows
- no head coverings
- no further people / objects
- equally distributed lighting
- no shadows over the face
- no shadows in the eye-sockets
- no hot spots on skin
- no effects from glasses
- correct exposure
- correct contrast
- focus and depth of field
- no unnatural colours
- no red eyes

3.6.3 QA-FP-APP

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

Requirements

Quality Algorithm

As quality algorithm NFIQ 2.0 [NFIQ2.0] shall be used. As resulting quality value, the output value of NFIQ 2.0 in the integer range of $[0,100]$ shall be used. In the case of failure, the returned value 255 indicates that a computation was not successful, in this case, the value shall be returned as dedicated error code.

Quality Evaluation Process for a Slap or Single Fingerprint

In case a single captured fingerprint, respectively slap is passed, the quality assessment is performed as described in the following. Beforehand the fingerprints of the passed capture have to be segmented (considering missing fingers). Note, that in verification applications, a quality assessment is not conducted. Thus, every slap capture is considered sufficient and no thresholds are specified here.

1. For each segmented fingerprint $F_{A,j}$ of a passed capture A, a quality value $Q_{A,j}$ is calculated with $j \in \{1,\ldots,10\}$ (up to 4 fingers in one slap) representing the specific finger code according to [ISO_FINGER].
2. The resulting quality value is compared with the defined threshold for this finger. The application specific thresholds TH_j as defined in the following section apply.
3. In case all of the fingerprint qualities reach the specified threshold (i.e. $\forall\, j, Q_{A,j} \geqslant TH_j$), the boolean information $b=1$ indicates a successful capture.
4. In case one or more fingerprints do no 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 quality assurance process, the following values are returned to the calling process:
   a. The boolean information b
   b. The parameter set $P_A = \{Q_{A,j}, \ldots, Q_{A,l}\}$ with $j, l \in \{1, \ldots, 10\}$ representing the specific finger code

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 [ISO_FINGER] are passed, the best of the captures is 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 [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)
   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 an index finger slap is a set of the best captures of each index finger as indicated by the following two options.
      ii. 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.
      iii. 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.
   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 quality assurance process, the following values are returned:
   a. The identifier i representing the capture yielding the best quality
   b. The parameter set $P_A = \{Q_{A_i,j}, \ldots, Q_{A_i,l}\}$ with $j, l \in \{1, .., 10\}$

Thresholds for Plain Fingerprints for Enrolment Purposes

The following thresholds as indicated in Table 3-7 apply when fingerprints are captured plain for enrolment purposes. Note, the thresholds in Table 3-7 do not apply to plain captured fingerprint in enrolment

scenarios where the plain fingerprints are capture for control purpose of rolled fingerprints. In that case, thresholds as indicated in Table 3-8 apply for the plain fingerprints.

Finger Position	Finger Code	NFIQ 2.0 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 3-7: Thresholds for Plain Fingerprints for Enrolment Purposes

Thresholds for Plain Control Fingerprints and Fingerprints used for Identification Searches

The following thresholds as indicated in Table 3-8 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 3-8 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	NFIQ 2.0 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 3-8: Thresholds for Plain Control /Identification Fingerprints

Thresholds for Rolled Fingerprints

The following thresholds as indicated in Table 3-9 apply when fingerprints are captured rolled for enrolment purposes.

Finger Position	Finger Code	NFIQ 2.0 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 3-9: Thresholds for Rolled Fingerprints

3.6.4 QA-IR-SB

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

Requirements

The Quality Assurance module defines the conformance criteria for automatic software-based checks of iris images after digitisation according to [ISO_IRIS_QA].

The QA module has to analyse and evaluate all of the quality criteria listed in Table 3-10. For the criteria marked with "M", the quality values must be provided while quality values for the criteria marked with "O" may be provided in the defined format according to the respective criteria. In addition, Table 3-10 maps the criteria to the corresponding [ISO_IRIS_QA] criteria if available.

A criterion is fulfilled if its calculated value is within the given threshold boundaries. Thresholds are defined in Table 3-11. For optional criteria no thresholds are provided as of today no sound studies discussing reasonable thresholds for those optional criteria are available.

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

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

ID	Criterion	ISO-Ref.[8]	M/O[9]	Unit/Range
Mandatory				
1.1	Usable iris area	6.2.1	M	Dimensionless between 0 and 100
1.2	Iris-sclera contrast	6.2.2	M	Dimensionless between 0 and 100
1.3	Iris-pupil contrast	6.2.3	M	Dimensionless between 0 and 100
1.4	Pupil boundary circularity	6.2.4	M	Dimensionless between 0-100
1.5	Grey scale utilisation	6.2.5	M	In bit
1.6	Iris radius	6.2.6	M	In pixel
1.7	Pupil dilation	6.2.7	M	Dimensionless between 0 and 100
1.8	Iris pupil concentricity	6.2.8	M	Dimensionless between 0 and 100
1.9	Margin adequacy	6.2.9	M	Dimensionless between 0 and 100
1.10	Sharpness	6.2.10	M	Dimensionless between 0 and 100
Optional				
2.1	Frontal gaze-elevation	6.3.1	O	Dimensionless between 0 and 100
2.2	Frontal gaze-azimuth	6.3.2	O	Dimensionless between 0 and 100
2.3	Motion blur	6.3.3	O	In pixels and degree

Table 3-10: Mapping of Relevant Quality Criteria to ISO Requirements

If defined, the thresholds for specific application profiles are detailed in Table 3-11.

8 Compare [ISO_IRIS]
9 Mandatory/Optional

ID	Criterion	Minimum	Maximum	Unit/Range
1.1	Usable iris area	70	100	Dimensionless between 0 and 100
1.2	Iris-sclera contrast	5	100	Dimensionless between 0 and 100
1.3	Iris-pupil contrast	30	100	Dimensionless between 0 and 100
1.4	Pupil boundary circularity	0	100	Dimensionless between 0-100
1.5	Grey scale utilisation	6	8	In bit
1.6	Iris radius	80	–	In pixel
1.7	Pupile dilation	20	70	Dimensionless between 0 and 100
1.8	Iris pupil concentricity	90	100	Dimensionless between 0 and 100
1.9	Margin adequacy	80	100	Dimensionless between 0 and 100
1.10	Sharpness	Application defined threshold	Application defined threshold	Dimensionless between 0 and 100

Table 3-11: Thresholds for Iris Images

3.7 Compression

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

3.7.1 COM-PH-JPG

This function block describes requirements and interfaces for the compression of photos using the JPEG format for reference storage.

Requirements

The compression method for facial images is JPEG (compare [ISO_10918-1]). The compression algorithm must parametrized that the application specific requirements as listed in Table 3-12 are met by the resulting compressed image. Within the Compression Module multiple lossy compressions are not allowed.

Minimum file size	Recommended compression ratio
Small size image (531x413 pixel)	

Minimum file size	Recommended compression ratio
25 KiB	20:1
Medium size image (800x600 pixel)	
35 KiB	20:1
Standard size image (1600x1200 pixel)	
100 KiB	20:1

Table 3-12: Requirements to Compression Using JPEG Format

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

3.7.2 COM-FP-WSQ

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

Requirements

As compression method for fingerprint images WSQ is used. A bit rate of 0.75 must be used as compression parameter. This is equivalent to a compression factor of approximately 1:15[10] (according to [ISO_FINGER]).

The implementation of the used WSQ algorithm has to be certified by the FBI and has to be referenced by the respective certificate number (coded in the WSQ header). The certified WSQ implementation shall be version 3.1.

Within the Compression Module multiple lossy compressions are not allowed.

3.7.3 COM-IR-PNG

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

Requirements

The encoding format for iris images shall be lossless PNG according to [ISO_15948].

3.8 Operation

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

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

3.8.1 O-PH-ALL

This function block describes requirements to be observed by the official who handles the facial image acquisition process. This includes the full working process.

Requirements

Veto

If the Quality Assurance module rejects the image, the official can give a veto in order to release the image despite a negative software decision. Reasons for this can exist due to software failures or because the biometric requirements cannot be fulfilled for this individual. If an image is provided by a life enrolment station, the operator is allowed to reject the image regardless of the Quality Assurance decision (e.g. failures by the life enrolment station). Optionally, the official can use the photo guideline (see module QA).

ID Check

In case of scenarios where the facial image is not taken supervised by the official at his counter, e.g. in case of self-service systems, the official shall check that the digital image belongs to the biometric subject.

3.8.2 O-PH-SPV

This function block describes requirements to be observed by the official who handles the facial image acquisition process. This includes the full working process.

Requirements

Operation of Devices

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

When a desired scanner is put into operation, it is the official who is responsible for a clean scanning surface so that adequate image results can be obtained in the following.

Visual Check

In case the biometric subject's facial image, which is going to be processed, was taken by a photographer, the official has to consider the photo guideline. Optionally, the official can use the photo template. The person on the photo has to be doubtlessly identified.

Scanning Facial Image

The official should place the picture carefully and with the correct orientation into the intended place.

Light Conditions

The following requirements for infrastructure and environment shall be met:

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

Veto

If the Quality Assurance module rejects the image, the official can give a veto in order to release the image despite a negative software decision. Reasons for this can exist due to software failures or because the biometric requirements cannot be fulfilled for this individual. If an image is provided by a life enrolment station, the operator is allowed to reject the image regardless of the Quality Assurance decision (e.g. failures by the life enrolment station). Optionally, the official can use the photo guideline (see module QA).

ID Check

In case of scenarios where the facial image is not taken supervised by the official at his counter, e.g. in case of self-service systems, the official shall check that the digital image belongs to the biometric subject.

3.8.3 O-FP-ACQ

This function block describes requirements to be observed by the official who handles the acquisition of fingerprints independent of the purpose of the acquisition.

Requirements

Operation of Devices

It is important to specify requirements that guarantee the correct working process. A calibration of the system may be necessary because of ageing aspects of the components used or through fluctuations of temperature and humidity as well as through transport of the components.

The operator is responsible for an adequate cleanliness of the sensor surface.

Quality Assurance

The quality assurance for the acquisition of the fingerprints is essentially based on technical functions. However, the official has to consider the following issues. Please note that all figures used within this Function Module are valid for any kind of sensor (single and multi finger devices) which are allowed to be used as specified in the according Function Module.

— The official has to ensure that there is no permutation between the hands or in the following the fingers requested for the image acquisition and the finger actually placed on the sensor.
— The official must assure that the person acquiring fingerprints does not use any finger dummies, fakes or something similar. Therefore, a direct view to the scanner is necessary. It is recommended that the person shows his fingers before starting the acquisition process.
— When capturing flat fingers, the palm shall not be lifted (as shown in Figure 3-20).

— Very dry fingers which only produce poor lines, have to be moisturised (e.g. by breathing upon) and the pressure can be increased. Very wet fingers which produce very strong lines with sweat traces have to be dried.
— For specific environment and especially dry fingers the usage of specialised tools is recommended. With this tools the contrast can be improved by swiping the fingers on it.

Figure 3-20: Example for the Finger Position

– The finger shall be positioned centrally and straight on the fingerprint scanner. An example is given in Figure 3-21.

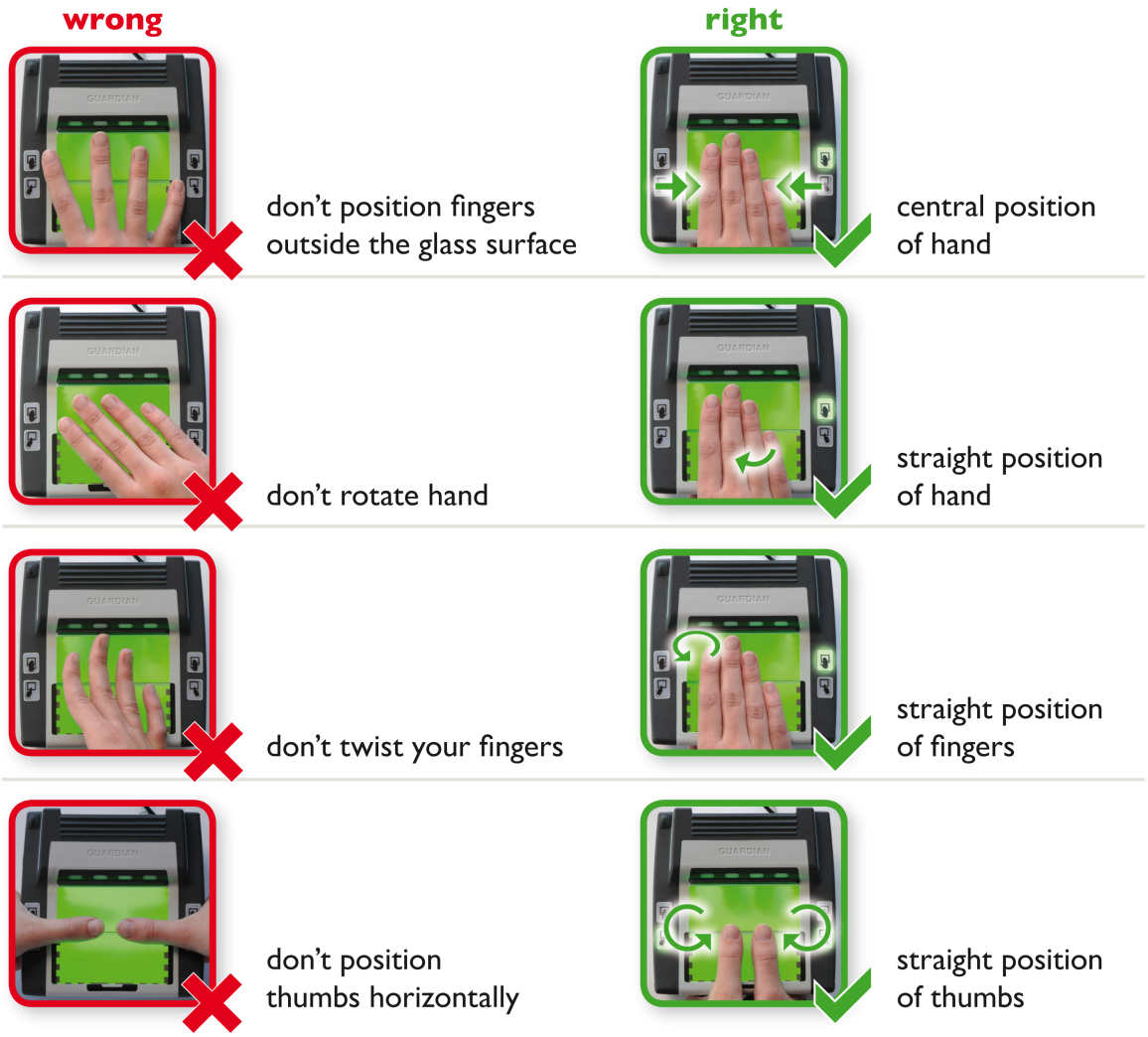

Figure 3-21: Example for the Position of the Hand

Process Requirements

The acquisition sequence for a fingerprint must be repeated completely, if operating errors have occurred by the official or the person acquiring fingerprints (e.g. if the wrong finger was placed on the sensor, incorrect identification by the official, or the finger was placed too late).

Process Requirements for Rolled Fingerprints

When rolling fingerprints, the conducting official has to ensure a steady rolling movement of each finger.

3.8.4 O-IR-ACQ

This function block describes requirements to be observed by the official who handles the applicants for iris image acquisition purposes. This includes the full working process.

Requirements

When a desired digital camera is put into operation, it is the operator who is responsible for a clean lens surface so that adequate image results can be obtained in the following.

The official ensures that the applicant presents no forged iris to the Acquisition Hardware e.g. by printed contact lenses. The process initiated if a presentation attack is detected by the official is out of scope of this document.

Veto

If the Quality Assurance module rejects the image, the official can give a veto in order to release the image despite a negative software decision. Reasons for this can exist due to software failures or because the biometric requirements cannot be fulfilled for this individual. The operator is allowed to reject the image regardless of the Quality Assurance decision (e.g. failures by the life enrolment station).

3.9 User Interface

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

3.9.1 UI-PH-APP

This function block describes requirements for the user interface of the software displaying the result of the Quality Assurance of facial images.

Requirements

The module calling the QA module and respectively the graphical user interface (GUI) has to provide the following functions:

- displaying of the current evaluated picture
- displaying of all criteria evaluated with the current value and threshold as well as their relation: OK/NOK for every criterion
- displaying of the summarised result OK/NOK for the current picture
- provision of the veto power for the official
  - enforcement of OK for obvious reasons (e.g. disability)
  - enforcement of OK without obvious reasons

3.9.2 UI-FP-BSJ

This function block describes requirements for the user interface of the biometric subject for fingerprint acquisitions.

Requirements

Visual feedback of the acquisition process shall be provided for the biometric subject.

Recommendations

The following recommendations should be met for the user interface:

- a visualization which fingerprint / hand to place on the sensor,
- an indicator showing the capture status should be displayed to the biometric subject,
- an indication when the capture process has finished,
- graphics should avoid multiple colours or harsh contrast.
- The acquisition process should be displayed as real time feedback to the biometric subject (e.g. with the help of a feedback monitor).

3.9.3 UI-FP-OFF

This function block describes requirements for the user interface of the software displaying the result of the Quality Assurance of fingerprint images to the official.

Requirements

Visual feedback of the fingerprint acquisition at least displaying of the final images shall be provided to the official.

If a control verification or sequence check error occurs, the fingers involved in the unexpected successful comparisons shall be displayed to the official.

In case no successful comparison occurred during the control verification, a warning shall be displayed to the official, that the control verification could not be carried out.

Recommendations

The segmented single fingerprints shall be visualised to the official to identify potential failures in segmentation. This can be realised by displaying the result containing up to ten segmented single fingerprints.

The indication of the quality level should be displayed to the official.

3.9.4 UI-IR-APP

This function block describes requirements for the user interface of the software displaying the result of the Quality Assurance of iris images.

Requirements

The module calling the QA module and respectively the graphical user interface (GUI) has to provide the following functions:

- displaying of image of left and right iris if available
- for each iris image available displaying of all criteria evaluated with their current value and threshold as well as their relation: OK/NOK for every criterion
- for each iris image available displaying of the summarised result OK/NOK

- in the case of summarised NOK: declaration of rejection arguments (as line of reasoning for the official in the case of rejection)
- provision of the veto power for the official
  - enforcement of OK for obvious reasons (e.g. disability)
  - enforcement of OK without obvious reasons

3.10 Reference Storage

The objective of this module is to store biometric data in a way that it can be used for reference purposes later on.

3.11 Biometric Comparison

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

3.11.1 CMP-ALL-MMI

This function block contains requirements on multimodal fusion of identification algorithms.

Requirements

General

When deploying a Central Identity Register (CIR) as a multimodal identification system, all biometric modalities available shall be used for identification purposes. The system shall return a single fusion-based score and candidate list with candidates above the configured threshold as indicated below.

The score shall express the aggregate performance in terms of False Positive Identification Rate and False Negative Identification Rate of the fusioned algorithms.

The fusion shall be based on score level aggregation of the different scores from each single biometric identification and shall take into account the distinct performance capabilities of each modality-specific algorithm, see [ISO24722] for possible fusion schemes.

Performance

When combining facial image, fingerprint and iris identification, the performance requirements from Table 3-13 shall be met.

False Positive Identification Rate (FPIR)	False Negative Identification Rate (FNIR)
0,1% (10^{-3})	< 1%
0,01% (10^{-4})	< 2%

Table 3-13: Multimodal Identification Performance Requirements

Negative Identification Scenarios

When an algorithm is used in negative identification scenarios (e.g. watchlist checks), the penalty of a False Negative Identification is typically considered higher as the one of a False Positive Identification. Therefore, the fusion of the algorithms shall be tuned to a higher FPIR, typically at most 10^{-3} or higher. This is especially relevant when data in the CIR is not complete or of insufficient quality for all biometric features, i.e. only some of ten fingerprints available, iris images missing, etc.

The optimal value for a specific scenario depends on the gallery size and operator time available for search result inspection.

System Documentation

The vendor shall describe in its documentation:

- the fusion method used for combining the scores of the different modalities into a single result score,
- the calibration process used for combination of the different scores,
- weighting schemes used in combination of the different algorithms,
- the combination strategy for the case of incomplete records (e.g. where only a subset of required modalities is present).

3.11.2 CMP-PH-GENERIC

This function block contains requirements on the performance of facial image identification algorithms.

Requirements

Performance

The size `r` of the candidate list shall be configurable by the application. A typical initial value is `r=10`.

The used algorithm shall provide a search performance expressed in terms of False Positive Identification Rate (FPIR) and False Negative Identification Rate (FNIR) as indicated in Table 3-14.

Facial Image Identification Algorithm False Positive Identification Rate (FPIR)	**Facial Image Identification Algorithm False Negative Identification Rate (FNIR)**
1% (10^{-2})	< 2,5%
0,1% (10^{-3})	< 5%
0,01% (10^{-4})	< 10%

Table 3-14: Facial Image Identification Performance Requirements

It is allowed to configure a threshold which allows stronger settings (lower FPIR and/or FNIR).

The algorithm vendor shall provide evidence to these performance requirements in terms of test results that are similar in relation to gallery size and capture characteristics to the application scenario.

Negative Identification Scenarios

When an algorithm is used in negative identification scenarios (e.g. watchlist checks), the penalty of a False Negative Identification is typically considered higher as the one of a False Positive Identification. Therefore, the algorithm shall be tuned to a higher FPIR, typically at most 10^{-2} or higher.

The optimal value for a specific scenario depends on the gallery size and operator time available for search result inspection.

System Documentation

The vendor shall document which data was used for calibration of the algorithm, especially concerning

- the size and image characteristics of the databases the algorithm was trained on,
- the conversion routine between raw scores and threshold defined by False Positive Identification Rate.

3.11.3 CMP-FP-GENERIC

This function block contains requirements on the performance of fingerprint identification algorithms.

Requirements

Performance

A fingerprint identification algorithm shall be used for searching in a Central Identity Register (CIR). The algorithm shall take images from up to ten available fingers into account and a list of candidates with the score above the threshold as indicated below for the combined search.

The size `r` of the candidate list shall be configurable by the application. A typical initial value is `r=10`.

The used algorithm shall provide a search performance expressed in terms of False Positive Identification Rate (FPIR) and False Negative Identification Rate (FNIR) as indicated in Table 3-15.

Fingerprint Identification Algorithm False Positive Identification Rate (FPIR)	**Fingerprint Identification Algorithm False Negative Identification Rate (FNIR)**
0,1% (10^{-3})	< 1,5%
0,01% (10^{-4})	< 3%

Table 3-15: Fingerprint Identification Performance Requirements

It is allowed to configure a threshold which allows stronger settings (lower FPIR and/or FNIR).

The algorithm vendor shall provide evidence to these performance requirements in terms of test results that are similar in relation to gallery size and capture characteristics to the application scenario.

Negative Identification Scenarios

When an algorithm is used in negative identification scenarios (e.g. watchlist checks), the penalty of a False Negative Identification is typically considered higher as the one of a False Positive Identification. Therefore, the algorithm shall be tuned to a higher FPIR, typically at most 10^{-3} or higher.

The optimal value for a specific scenario depends on the gallery size and operator time available for search result inspection.

System Documentation

The vendor shall document which data was used for calibration of the algorithm, especially concerning

- the size and image characteristics of the databases the algorithm was trained on,
- the conversion routine between raw scores and threshold defined by False Positive Identification Rate.

3.11.4 CMP-IR-GENERIC

This function block contains requirements on the performance of iris identification algorithms.

Requirements

Performance Requirements

An iris identification algorithm shall be used for searching in a Central Identity Register (CIR). The algorithm shall take images from both eyes into account and deliver a single score and a list of candidates with the score above the threshold as indicated below for the combined search.

The size `r` of the candidate list shall be configurable by the application. A typical initial value is `r=10`.

The used algorithm shall provide a search performance expressed in terms of False Positive Identification Rate (FPIR) and False Negative Identification Rate (FNIR) as indicated in Table 3-16.

Iris Identification Algorithm False Positive Identification Rate (FPIR)	**Iris Identification Algorithm False Negative Identification Rate (FNIR)**
0,1% (10^{-3})	< 1,5%
0,01% (10^{-4})	< 3%

Table 3-16: Iris Identification Performance Requirements

It is allowed to configure a threshold which allows stronger settings (lower FPIR and/or FNIR).

The algorithm vendor shall provide evidence to these performance requirements in terms of test results that are similar in relation to gallery size and capture characteristics to the application scenario.

Negative Identification Scenarios

When an algorithm is used in negative identification scenarios (e.g. watchlist checks), the penalty of a False Negative Identification is typically considered higher as the one of a False Positive Identification. Therefore, the algorithm shall be tuned to a higher FPIR, typically at most 10^{-3} or higher.

The optimal value for a specific scenario depends on the gallery size and operator time available for search result inspection.

System Documentation

The vendor shall document which data was used for calibration of the algorithm, especially concerning

- the size and image characteristics of the databases the algorithm was trained on,
- the conversion routine between raw scores and threshold defined by False Positive Identification Rate.

3.12 Logging

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

3.12.1 LOG-PH-GENERIC

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

Requirements

Within a transaction for each facial image used for enrolment / verification / identification, the following data items shall be collected:

- the purpose of the acquisition (enrolment, identification, verification)
- start time of the facial acquisition process
- end time of the facial acquisition process
- software components used in this facial acquisition process
- hardware components used in this facial acquisition process
- the source of the facial image under consideration
- the count of face captures performed
- for the best capture, detailed quality information about the result, detailing
  - information about the quality assessment software
  - duration of quality assessment
  - detailed quality values accompanied by
    - identifiers
    - upper and lower value bounds
    - upper and lower threshold bounds
  - any error code in case of abnormal termination of the quality assessment
- information about presentation attack detection (PAD) data during the capture
  - information about the PAD subsystem
  - the overall PAD assessment result
  - for each probe
    - the PAD result
  - detailed PAD quality values accompanied by
  - identifiers
  - upper and lower value bounds
  - upper and lower threshold bounds
- an error code in case of abnormal termination of the facial acquisition process.

The vendor shall provide a detailed list of error codes used with complete semantic descriptions.

3.12.2 LOG-FP-GENERIC

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

Requirements

Within a transaction for each set of fingerprints used for enrolment / verification / identification, the following data items shall be collected:

- the purpose of the acquisition (enrolment, identification, verification)
- start time of the fingerprint acquisition process
- end time of the fingerprint acquisition process
- software components used in this fingerprint acquisition process
- hardware components used in this fingerprint acquisition process
- the finger capture mode (flat, rolled, contactless)
- information about missing fingers (in relation to the requirement of the profile)
- information for each capture process for a dedicated fingerprint of slap, detailing
  - fingerprint or slap code
  - duration of the capture
  - information whether this capture satisfies the quality requirements of the profile
  - count of single capture attempts performed for this fingerprint of slap
  - the capture number of the selected fingerprint or slap in case of multiple acquisitions
  - results from the control verification process for each finger (e.g. when comparing a rolled image against a finger extracted from a control slap)
  - for each capture attempt, detailing
    - whether this was an acceptable capture attempt (from the application software perspective, independent of the quality assessment)
    - the duration of the capture attempt
    - in case of an unacceptable capture attempt
      - the reason for rejection this capture attempt
      - an error code detailing the reason of rejection
- For the best capture attempt, detailed quality information about the result shall be logged. For all other capture attempts detailed quality information, if calculated during the process, should be logged:
  - information about the quality assessment software
  - duration of quality assessment
  - detailed quality values in the range 0-100
  - fingerprint or slap code
  - any error code in case of abnormal termination of the quality assessment
- uniqueness check information, detailing
  - information about the uniqueness check algorithm
  - the configured security level
  - information about potential duplicates including finger codes and detailed scoring information
  - any error code in case of abnormal termination of the uniqueness check
- information about presentation attack detection (PAD) data during the capture
  - information about the PAD subsystem

- the overall PAD assessment result
- for each probe
  - the PAD result
  - detailed PAD quality values accompanied by
  - identifiers
  - upper and lower value bounds
  - upper and lower threshold bounds
- an error code in case of abnormal termination of the fingerprint acquisition process.

The vendor shall provide a detailed list of error codes used with complete semantic descriptions.

Within a transaction for each capture attempt acquired for enrolment / verification / identification, detailed information about the quality, if calculated during the process, should be logged:

- information about the quality assessment software
- duration of quality assessment
- detailed quality values in the range 0-100
- fingerprint or slap code
- any error code in case of abnormal termination of the quality assessment

3.12.3 LOG-IR-GENERIC

This function block describes requirements and interfaces for the logging of information regarding iris images for all profiles.

Requirements

Within a transaction for each iris image used for enrolment / verification / identification, the following data items shall be collected.

- the purpose of the acquisition (enrolment, identification, verification)
- start time of the iris acquisition process
- end time of the iris acquisition process
- software components used in the iris acquisition process
- hardware components used in the iris acquisition process
- information about missing irises
  - label of missing iris (both, left, right, undefined)
  - reason why iris is missing (temporary, permanent, no reason given)
- information about capturing process of the iris image
  - label of captured iris (both, left, right, undefined)
  - duration of the capture of the iris (encompasses multiple tries if performed)
- quality assurance information about captured iris images
  - information about the quality assessment software
  - duration of quality assessment
  - results of iris image quality criteria accompanied by
    - identifiers
    - upper and lower value bounds
    - upper and lower threshold bounds

  - any error code in case of abnormal termination of the quality assessment
- information about presentation attack detection (PAD) data during the capture
  - information about the PAD subsystem
  - the overall PAD assessment result
  - for each probe
    - the PAD result
  - detailed PAD quality values accompanied by
  - identifiers
  - upper and lower value bounds
  - upper and lower threshold bounds
- an error code in case of abnormal termination of the iris acquisition process

3.13 Coding

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

3.13.1 COD-ALL-GENERIC

This function block describes requirements and interfaces for the overall coding of biometric and biographic data used for all application profiles.

Requirements

The logging data as defined by the FM LOG is encoded in XML according to the schema definitions published alongside to this Technical Guideline.

3.13.2 COD-ALL-MMI

This function block describes requirements and interfaces for the overall coding of biometric and biographic data used within the context of the multimodal identification with watchlist checks.

Requirements

The biographic and biometric data shall be encoded for import and export from CIR according to [STANAG4715].

All biographic data fields in Type-2 shall be supported by the application for import and export.

Requirements on Encoding Logging Data

The logging data as defined by the FM LOG is encoded is XML according to the schema definition as `mmi` element. The XML encoding is defined by the XML schema definition in the file „mmi4v3.xsd“ and referenced schema files.

All log data has to 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).

The biometric data transaction container (e.g. according to [STANAG4715]) shall be embedded in the log (`Record` element) for conformance testing of the encoding.

3.13.3 COD-PH-STANAG

This function block describes requirements and interfaces for the coding of facial images according to [STANAG4715] transactions in binary format.

Requirements

The facial images shall be encoded as a Type-10 record according to [STANAG4715]. The application profile shall encode all mandatory fields of the standard.

3.13.4 COD-FP-STANAG

This function block describes requirements and interfaces for the coding of fingerprint images according to [STANAG4715] transactions in binary format.

Requirements

The fingerprint images shall be encoded as a Type-14 record according to [STANAG4715]. The application profile shall encode all mandatory fields of the standard.

3.13.5 COD-IR-STANAG

This function block describes requirements and interfaces for the coding of iris images according to [STANAG4715] transactions in binary format.

Requirements

The iris images shall be encoded as a Type-17 record according to [STANAG4715]. The application profile shall encode all mandatory fields of the standard.

3.14 Evaluation

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

4 List of Abbreviations

Abbreviation	Description
AAD	Arrival Attestation Document
ACQ	Acquisition
AD	Acquisition Device
AFIS	Automated Fingerprint Identification System
AH	Acquisition Hardware
ANSI	American National Standards Institute
AP	Application Profile
APP	Application
AS	Acquisition Software
BEA	Biometric Evaluation Authority
BioAPI	Biometric Application Programming Interface
BioSFPI	Biometric Sensor Function Provider Interface
BioSPI	BioAPI Service Provider Interface
BIP	Biometric Image Processing
BMS	Biometric Matching System
BMP	Windows Bitmap version 3
BPCER	Bona fide presentation classification error rate
BFNRR	Bona fide presentation non-response rate
BSI	Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security)
BFP	Biometric Function Provider
BSFP	Biometric Sensor Function Provider
BSP	Biometric Service Provider
CDF	Cumulative Distribution Function
CMP	Biometric Comparison
COD	Coding

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

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

5 Bibliography

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

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

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

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

[EC_767_2008] Regulation (EC) No. 767|2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas (VIS Regulation)

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

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

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

[GSAT3] German Standard for AFIS transactions. XML schema files version 3.01_4.

[ICAO_9303] ICAO Document 9303, Machine Readable Travel Documents, 7th edition, 2016

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

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

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

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

[ISO_IRIS] ISO/IEC 19794-6:2011 “Information technology” - Biometric data interchange formats - Part 6: Iris image data

[ISO_IRIS_QA] ISO/IEC 29794-6:2015 “Information technology” - Biometric sample quality - Part 6: Iris image data

[ISO_PAD_1] ISO/IEC 30107-1: Information technology – Biometric presentation attack detection – Part 1: Framework

[ISO_PAD_3] ISO/IEC 30107-3: Information technology – Biometric presentation attack detection – Part 3: Testing and reporting

[ISO_10918-1] ISO/IEC 10918-1:1994: “Information technology – Digital compression and coding of continuous-tone still images: Requirements and guidelines”

[ISO_15444] ISO/IEC 15444-1:2004 “Information technology – JPEG 2000 image coding system: Core coding system”

[ISO_15948] ISO/IEC 15948:2004 “Information technology – Computer graphics and image processing – Portable Network Graphics (PNG): Functional specification”

[ISO_19785-3] ISO/IEC 19785-3:2007 “Information technology – Common Biometric Exchange Formats Framework – Part 3: Patron format specification”

[ISO_24709-1] ISO/IEC 24709-1: 2007 “Information technology – Conformance testing for the biometric application programming interface (BioAPI) – Part 1: Methods and procedures”

[ISO_24709-2] ISO/IEC 24709-2: 2007 “Information technology – Conformance testing for the biometric application programming interface (BioAPI) – Part 2: Test assertions for biometric service providers”

[ISO_24722] ISO/IEC TR 24722:2015: “Information technology – Biometrics – Multimodal and other multibiometric fusion”

[NBIS] http://fingerprint.nist.gov/NBIS/index.html

[NFIS] http://fingerprint.nist.gov/NFIS/index.html

[NFIQ2.0] http://www.nist.gov/itl/iad/ig/development_nfiq_2.cfm, Source code from Apr 28, 2016.

[PhotoGuide] Photo guideline ("Fotomustertafel")

[RFC2119] RFC 2119: Key words for use in RFCs to Indicate Requirement Levels.

[STANAG4715] NATO STANAG 4715: “Biometric Data, Interchange, Watchlist and Reporting”, 2013

[TR03146] BSI TR-03146 Elektronische Bildübermittlung zur Beantragung hoheitlicher Dokumente (E-Bild hD) ,Version 1.0

[Template] Photo template ("Lichtbildschablone")

[UN REGIO] Standard Country or Area Codes for statistical Use, United Nations Department Of Economic and Social Affairs Statistics Division, 1999

[VIS-ANSI_NIST] VIS-ANSI/NIST, European Commission Directorate-General Justice, Freedom and Security – Visa Information System – NIST Description, Version 1.23, 2009