Federal Office
for Information Security

BSI Technical Guideline TR-03121-1

Biometrics for Public Sector Applications

Part 1: Framework

Version 7.0-draft2

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

Table of Contents

List of Figures

1 Changelog

The following tables present the changes introduced to this Technical Guideline since version 6.0. The changelog lists the changes grouped per part of this Technical Guideline, and per building block (Application Profile (AP), Partial Application Process (PAP), Task, Function Module (FM)) or element (section, table, figure):

- *Added* for new features
- *Changed* for changes in existing functionality
- *Deprecated* for soon-to-be removed features
- *Removed* for now removed features
- *Fixed* for any bug fixes
- *Security* in case of vulnerabilities

1.1 Changelog Version 7.0-draft1

This chapter includes all changes between Version 6.0 and Version 7.0-draft1.

1.1.1 Changelog BSI TR-03121, General

Element Name	Type of Change	Change Description
Schema	Changed	Replace XMLRecord with BinaryRecord in are5v2_overall_example.xml.

Table 1.1 Changelog BSI TR-03121, General

1.1.2 Changelog BSI TR-03121, Part 1

Element Name	Type of Change	Change Description
-	-	-

Table 1.2 Changelog BSI TR-03121, Part 1

1.1.3 Changelog BSI TR-03121, Part 2, Volume HLBS

Element Name	Type of Change	Change Description
Service Definition "Rolled Fingerprint Acquisition"	Changed	Changed unclear Service UUID to unique UUID

Table 1.3 Changelog BSI TR-03121, Part 2

1.1.4 Changelog BSI TR-03121, Part 3

TR Volume	Block / Section / Type	Name	Type of Change	Change Description
GID	FM	REF-FI-GID, LOG-ALL-GID	Changed	Changed "Behördenkennziffer (BHKZ)" to "Behördenkennzahl (BKZ)" to standardise the name.
BCL, GID, VIS, ARE, GIS, IMA	FM	AH-FI-DC, AH-FI-DC2	Changed	Added clarification for requirements of facial image cameras. Capture of full frontal facial image shall be possible and the camera shall allow cropping of captured facial image.
BCL, GID, VIS, ARE, GIS, IMA	FM	UI-FP-OP, UI-FI-OP	Changed	Added clarification for the case that no PAD result is available. This information shall be displayed to the operator.

TR Volume	Block / Section / Type	Name	Type of Change	Change Description
GID	FM	AS-FI-FBS	Changed	Removed the selection of the scanning mode for images in colour or in grey scale.
ARE	AP	Arrival Attestation Document	Changed	Replaced PAP ACQ-FI-SV-2 with PAP ACQ-FI-SV-4.
ARE	AP	Arrival Attestation Document in Special Situations	Changed	Replaced PAP ACQ-FI-SV-2 with PAP ACQ-FI-SV-4.
ARE	AP	Arrival Attestation Document	Changed	Marked PAP DEL-FI-SV-1 as optional.
ARE	AP	Arrival Attestation Document in Special Situations	Changed	Marked PAP DEL-FI-SV-1 as optional.
ARE	AP	Registration with Biometric Identification	Added	Added new Application Profile "Registration with Biometric Identification".
ARE	AP	Document Issuing with Biometric Verification	Added	Added new Application Profile "Document Issuing with Biometric Verification".
ARE	FM	COD-ALL-ARE	Changed	Removed the alternative option of using BinaryRecord elements.
BCL, GID, VIS, ARE, GIS, IMA	FM	LOG-FI-GENERIC, LOG-FP-GENERIC	Changed	Added the special case of canceled acquisition.
BCL, ARE, IMA	FM	AS-FP-SLP	Changed	Added the alternative of hardware-based detection.
GID	FM	COD-FI-CHIP	Changed	Added footnote to ISO reference BIB_ISO_FACE (transition to BIB_ISO_39794-5).
GID	FM	COD-FP-CHIP	Changed	Added footnote to ISO references BIB_ISO_FINGER (transition to BIB_ISO_39794-4).
GID	Basics for German Identity Documents	--	Changed	Added ISO/IEC 39794-4 and ISO/IEC 39794-5.
BCL	Volume Border Control	--	Changed	Added ISO/IEC 39794-4 and ISO/IEC 39794-5.
ARE	Volume Alien Register Enrolment	–	Changed	Added chapter for Application Profile combinations.

TR Volume	Block / Section / Type	Name	Type of Change	Change Description
ARE	FM	LOG-ALL-ARE	Changed	Added new Application Profiles.

Table 1.4 Changelog BSI TR-03121, Part 3

1.2 Changelog Version 7.0-draft2

This chapter includes all changes between Version 7.0-draft1 and Version 7.0-draft2.

1.2.1 Changelog BSI TR-03121, General

Element Name	Type of Change	Change Description
Schema	Changed	Add the attribute selected for bio:FaceCapture.
Schema	Changed	Add PNG and PNM data type to type.record.type.
Schema	Changed	Add result attribute to FingerDelivery and FaceDelivery.

Table 1.5 Changelog BSI TR-03121, General

1.2.2 Changelog BSI TR-03121, Part 1

Element Name	Type of Change	Change Description
-	-	-

Table 1.6 Changelog BSI TR-03121, Part 1

1.2.3 Changelog BSI TR-03121, Part 2, Volume HLBS

Element Name	Type of Change	Change Description
Service Definition "Rolled Fingerprint Acquisition"	Changed	Changed unclear Version value of ServiceInformation to acutal version of the current BSI TR-03121.
Service Definition "Facial Image Delivery Acquisition"	Changed	Changed unclear Version value of ServiceInformation to acutal version of the current BSI TR-03121.
Service Definition "Facial Image Delivery System"	Changed	Configuration Parameter FacialImages: hlbs:Image SHALL contain bio:Origin within xmlParameters; image format according to Application Profile.
Service Definition "Facial Image Delivery System"	Changed	User Command Parameter CropManually: added ImageListItem to specify the image to crop.
Service Definition "Facial Image Delivery System"	Changed	User Command Parameter RotateManually: added ImageListItem to specify the image to rotate manually.
Service Definition "Facial Image Delivery System"	Changed	User Command Parameter AcceptImage: added ImageListItem to specify the image to accept.
Service Definition "Facial Image Delivery System"	Changed	User Command Parameter RejectImage: renamed to RejectAllImages.
Service Definition "Facial Image Delivery System"	Changed	Feedback Parameter QAFeedback: renamed to QAFeedbackList, changed type to hlbs:StringList.
Service Definition "Facial Image Delivery System"	Changed	Feedback Parameter QAEntireFacialImage: renamed to QAEntireFacialImageList, changed type to hlbs:ImageList; image format according to Application Profile.
Service Definition "Facial Image Delivery System"	Changed	Feedback Parameter QACroppedFacialImage: renamed to QACroppedFacialImageList, changed type to hlbs:ImageList; image format according to Application Profile.

Element Name	Type of Change	Change Description
Service Definition "Facial Image Delivery System"	Changed	Feedback Parameter QACroppedFacialImageRotation: renamed to QACroppedFacialImageRotationList, changed type to hlbs:StringList.
Service Definition "Facial Image Delivery System"	Changed	Results Parameter FaceAcquisition: renamed to FaceDelivery.
Service Definition "Facial Image Acquisition System"	Changed	Changed unclear Version value of ServiceInformation to acutal version of the current BSI TR-03121.
Service Definition "Basic Facial Image Acquisition System"	Changed	Changed unclear Version value of ServiceInformation to acutal version of the current BSI TR-03121.
Service Definition "Fingerprint Acquisition"	Changed	Changed unclear Version value of ServiceInformation to acutal version of the current BSI TR-03121.
Service Definition "Self-Service System"	Changed	Changed unclear Version value of ServiceInformation to acutal version of the current BSI TR-03121 for both Automated Acquisition of Slap Fingerprints and Automated Acquisition of Facial Images .

Table 1.7 Changelog BSI TR-03121, Part 2

1.2.4 Changelog BSI TR-03121, Part 3

TR Volume	Block / Section / Type	Name	Type of Change	Change Description
GID	FM	LOG-FI-GID	Changed	Restricted the Exif data to printable ASCII characters.
GID	FM	AS-FI-DC2, AH-FI-DC2	Changed	Restricted the dispensing with a uniform background.
ARE	AP	Document Issuing with Biometric Verification, Arrival Attestation Document, Arrival Attestation Document in Special Situations	Changed	Changed order of printing and logging.
ARE	AP	Document Issuing with Biometric Verification, Arrival Attestation Document	Changed	Verification is included in PAP Task.
GID	AP	Biometric Data Selection	Changed	Added a clarification for the resolution of non-scanned facial images.
GID	FM	COD-FI-GID	Changed	Fixed the image resolution to 1244x1600 pixels.

TR Volume	Block / Section / Type	Name	Type of Change	Change Description
GID	FM	COD-FI-ROD	Changed	Fixed the image resolution to 1244x1600 pixels.
GID	FM	COD-FP-CHIP	Changed	The ICAO-CBEFF container will be omitted in the future.
GID	AP	Biometric Data Selection	Changed	Added required FM LOG-ALL-BDS
GID	FM	LOG-ALL-GID	Changed	Moved parts to FM LOG-ALL-BDS
GID	FM	LOG-ALL-BDS	Added	Created new FM with parts of FM LOG-ALL-GID
GID	Basics for German Identity Documents	-	Changed	Changed ISO references and added footnotes to the ISO/IEC 39794 series.
BCL	Volume Border Control	-	Changed	Changed ISO references and added footnotes to the ISO/IEC 39794 series.

Table 1.8 Changelog BSI TR-03121, Part 3

2 Introduction

2.1 Motivation and Objectives of Technical Guideline Biometrics

Biometric methods are used in many different areas of applications. The solutions and systems available on the market are able to serve a broad range regarding performance, security, usability and standard conformance. For public sector applications, it is necessary to define precise requirements and general conditions. Furthermore, the systems have to be defined in a way which allows for extension in future developments.

The objective of this Technical Guideline (TR Biometrics) is to offer a basis for a consistent and comparable quality of public sector applications and for building a common architecture.

This guideline has the following objectives:

- *Modularity:* The complete guideline is built from several single guideline modules. For a single application area only the respective modules have to be taken into account. This is done in order to avoid side effects between different kinds of applications which would occur due to changes of special functions.
- *Clarity:* The concept of this guideline follows a well structured framework. With this framework it is easily understandable which kind of guideline modules are valid for the respective application scenario.
- *Expandability:* Modularity is the key component of expandability in the scope of this guideline. This is valid regarding new applications as well as new functional units.
- *Standard conformance:* The Technical Guideline takes national and international standards and guidelines into account and deploys them for governmental applications.
- *Conformance and certification:* The guideline modules are designed in such a way that requirements and conditions for single functional units are clearly separated from each other. Products for single functional units are clearly defined regarding the interfaces and the range of their functionality so that they can be tested for conformance with this guideline and certified.
- *Ability to reference:* The use of functional units allows to specify precise requirements for products that are used in according application scenarios. Therefore, this guideline can be used as a reference e.g. for tenders.
- *Market orientation:* The definition of functional units is related to the products that can be found on the market. Requirements of the guideline can be unambiguously assigned to the respective systems and components.

It should be noted that the content of this guideline is limited to the aspects of biometric characteristics. Interfaces to further technologies (e.g. connection of optical or electronic document readers) are out of scope of this document.

2.2 Target Audience and User

Audience for this guideline are institutions that are dealing with projects using biometric characteristics in public sector applications. These include:

- Agencies that are issuing identity documents or visas, e.g. passport agencies of the local authorities or missions abroad of the Federal Foreign Office.
- Public Authorities using biometric applications for identity verification of people, e.g. the German Federal Police (Polizeien des Bundes) or the Police of the Federal States (Polizeien der Länder), the German Customs Administration (Bundeszollverwaltung) or the Federal Administrative Office (Bundesverwaltungsamt).

Beside these users, this guideline also addresses vendors of biometric systems as well as integrators and application developers.

2.3 Terminology

The key words "MUST", MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this Technical Guideline are to be interpreted as described in [BIB_RFC2119].

2.4 Business Process Modelling Notation (BPMN)

The processes in this Technical Guideline are modelled using the Business Process Modelling Notation (BPMN). ▸Figure 2.1 gives an overview over the relevant icons herein.

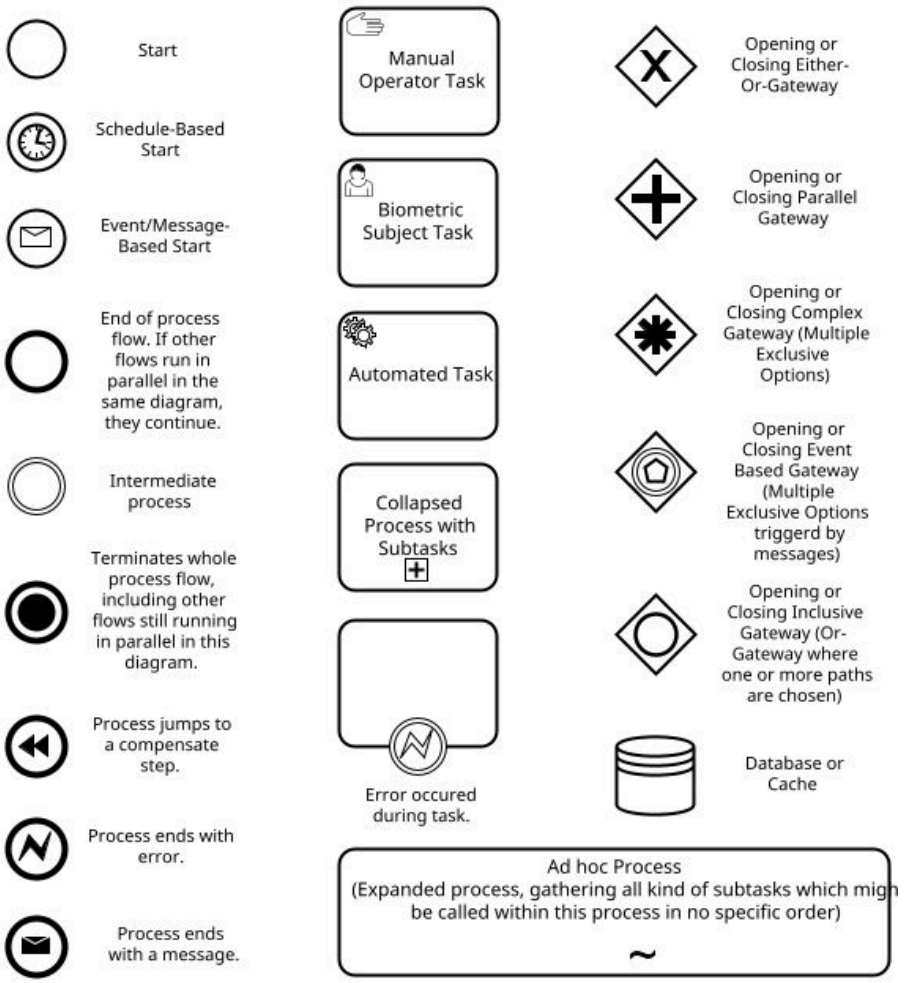

Figure 2.1. BPMN Symbols used for the Process Modelling

3 Structure of Technical Guideline Biometrics

This Technical Guideline consists of the following parts:

- Part 1: Framework (TR-03121-1)

  TR-03121-1 is the framework document of the guideline. It explains the concept and the relation between the different parts.

- Part 2: Software Architecture (TR-03121-2)

  The High Level Biometric Services (HLBS) as well as Service Definitions for specific use cases are specified here.

- Part 3: Application Profiles, Function Modules and Processes (TR-03121-3)
  - In the third part, the different Application Profiles with corresponding Partial Application Processes and Function Modules are defined. These contain the detailed technical requirements for each of the components.
    - Application Profiles may reference Function Modules, Partial Application Processes and Service Definitions (refer to Part 2).
    - Partial Application Processes may refer to Function Module Categories and may be comprised of *Tasks*. Tasks are processes which are part of more than one Partial Application Process.
  - For practical purposes, this part is split up in different volumes to serve different user groups.
    - Border Control (BCL)
    - German Identity Documents (GID)
    - Alien Register Enrolment (ARE)
    - Immigration Authorities (IMA)

Please refer to ▸Figure 3.1 for a class diagram of the structure described above.

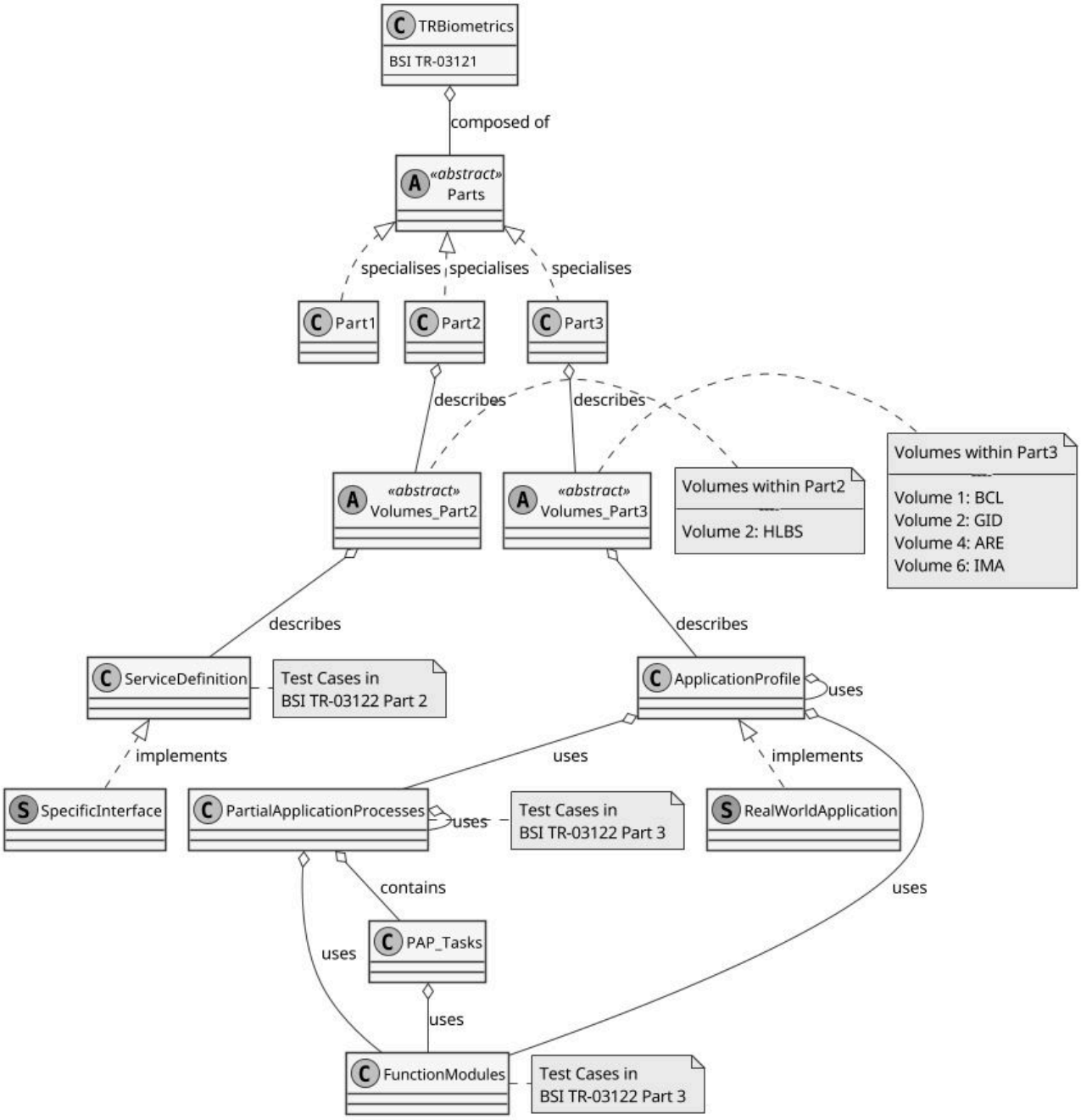

Figure 3.1. Class Diagram of the Technical Guidelines

Additionally, the Technical Guideline BSI-TR 03122 "Conformance Test Specification for Technical Guideline TR-03121 Biometrics for Public Sector Applications" describes the requirements that are essential to declare conformance or to declare the absence of conformance. It consists of the following parts:

- Part 1: Framework (TR-03122-1)
- Part 3: Test Cases for Function Modules and Processes (TR-03122-3)

4 How to use this Technical Guideline

This chapter gives a short overview how to read and apply this guideline step by step.

1. The user chooses the desired Application Profile. With the help of the Application Profile the user can get a deeper insight into the application, the required software architecture components and the described functionality. TR-03121-2 offers further information about the software architecture component model.
2. Based on the Application Profile, the mandatory Partial Application Processes and Function Modules are identified. One profile can link to several Partial Application Processes and Function Modules due to different kinds of underlying biometric characteristics or the fact that different technologies (e.g. scanners or digital cameras for the digitisation of a photo) are used.

   Function Modules are referenced by an explicit identifier, e.g. AH-FP-GID. The first part identifies the requirement type (e.g. Hardware), the second part represents the biometric characteristic (e.g. fingerprint), and the last part denotes a further descriptor, typically the scope (e.g. German Identity Document).

   Function Modules for different biometric characteristics are divided by a comma while a choice between different technologies is denoted by a slash (e.g. AH-FP-FTR, AH-PH-FBS/AH-PH-DC).

   If a Function Module is denoted with a placeholder between a less-than and greater-than sign (< >) the actual referenced Function Module is dependant on the context in which the Function Module has been mentioned. For example the Function Module AH-FI-<VL> has been mentioned within a Partial Application Process used in the BCL volume, then the actual referenced Function Module is AH-FI-BCL. The same procedure holds for Application Profiles denoted as <AP> analogously. If no specific Function Module applies, then there are no further requirements defined for this context.

   Partial Application Processes are referenced by an explicit identifier, refer to Partial Application Profile section.
3. On the basis of the identifier the according Function Module and Partial Application Processes can be examined. Every Function Module and Partial Application Process provides detailed technical requirements and recommendations. Note, each reference to a Function Module or Partial Application Processes is a link within the document.

5 Logging scheme

5.1 Use cases

This chapter specifies a logging scheme, which allows to document all technical activities performed. The schema files contain additional and mandatory information on technical requirements. Such a logging scheme SHALL be used to measure the quality of the biometric processes across different systems, regardless of the used hard- or software. This enables the possibility of an operational monitoring for technical as well as functional processes and evaluations.

5.2 XML schemas

The logging scheme is based on a transactional logging format which collects performance and evaluation results from the different application domains. The schema file `trbio5v1.xsd` imports all other schema files and as such the main file used for validation.

A separate XML schema definition exists for each volume of TR-03121-3, which SHALL be used within the respective application area. ▸Table 5.1 gives an overview of the different XML schema files.

Application domain	Schemafile	Namespace
Alien register enrolment	are5v1.xsd	http://trbio.bsi.bund.de/are/5
Border control log	bcl5v1.xsd	http://trbio.bsi.bund.de/bcl/5
Type definitions	biotypes5v1.xsd	http://trbio.bsi.bund.de/base/5
German identity documents	gid5v1.xsd	http://trbio.bsi.bund.de/gid/5
High level biometric services	hlbs5v1.xsd	http://trbio.bsi.bund.de/hlbs/5
Immigration authorities	ima5v1.xsd	http://trbio.bsi.bund.de/ima/5
Conformance test specification	biocts5v1.xsd	http://trbio.bsi.bund.de/biocts/5

Table 5.1 Overview XML schema files

6 Application Profiles

Different areas in which this guideline can be used are defined in separate Application Profiles. Application Profiles can have mandatory status, e.g. through published regulations and laws or by requirements given in tenders. Besides, such Application Profiles can also be considered as Best Practices. Thus, the certification process SHALL use one or more seperate Application Profiles.

An Application Profile is described with the following items:

- Introduction (legal requirements)
- Process overview
  - Target audience
  - Users
- Relevant standards and conditions
- List of
  - required Function Modules
  - required Partial Application Processes

7 Organisation of the Function Modules

Specific technical requirements are structured in Function Modules. They contain detailed technical requirements for the respective component. Function Modules are aligned to the products on the market and to the targets of evaluation. Every Function Module is built of one or more subclauses which are assigned to unique identifiers. Within the subclauses requirements and recommendations are specified in detail.

Function Modules are referenced by their ID, which can contain up to three information items pointing to its contents. The basic structure of an ID is: "FM AAA-BBB-CCC".

Here, *AAA* is the primary information item, pointing to the main contents. *BBB* and *CCC* are optional information items, which can further specify the Function Module. These information items may be two to seven alphanumeric digits. ▸Table 7.1 gives an overview of the different primary information items used for Function Module categories. ▸Table 7.2 gives an overview of the different optional information items *BBB* used for Function Module categories.

Primary Information Item	Function Module Category	Description
AH	Acquisition Hardware	Devices that are used for digitising physical representable biometric characteristics are called Acquisition Hardware. Scanners for capturing photographs, digital cameras to capture facial images, fingerprint sensors, or signature tablets can be named as examples.
AS	Acquisition Software	Acquisition Software encapsulates 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. Furthermore, colour management and image enhancement mechanisms are often part of this software layer.
BIP	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 biometric characteristics is addressed here e.g. provision of full frontal images or segmentation of fingerprints.
CMP	Biometric Comparison	The module Biometric Comparison encloses the mechanisms and algorithms to verify or identify an identity based on a one-to-one or one-to-many biometric comparison between reference data and a current biometric sample (usually a live presented image) no matter where the reference is stored.
COD	Coding	This module contains the procedures to code logging data as well as biometric data in defined formats. Interoperability is provided by means of standard compliant coding.

Primary Information Item	Function Module Category	Description
COM	Compression	The objective of the module Compression is to keep the biometric data below a feasible size without losing too much quality for biometric verification or identification.
EVA	Evaluation	Methods and interfaces which are used in the scope of evaluation are the content of this module.
LOG	Logging	The module Logging contains requirements how and in which modality data has to be logged.
O	Operation	Within the module Operation, the working process is specified for the respective operator.
PAD	Presentation Attack Detection	The Presentation Attack Detection modules give requirements on fake detection. This encloses, among other things, functionality and certification requirements.
QA	Quality Assessment	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. Quality Assessment is typically used in evaluation of an application's performance over time.
REF	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.
UI	User Interface	The User Interface modules give requirements on visualization and user interaction. This encloses, among other things, functionality, quality assurance information, and veto messages.

Table 7.1 Overview FM Categories Primary Information Items

Optional Information Item	Function Module Category
ALL	Overall
CCTV	Closed Circuit Television (Surveillance Camera)
FI	Facial Image
FP	Fingerprint

Table 7.2 Overview FM Categories Optional Information Items

8 Organisation of the Partial Application Processes

Partial Application Processes are referenced by their ID, which can contain up to three information items pointing to its contents. The basic structure of an ID is: "PAP (Task) AAA-BBB-CCC-#".

Here, "Task" is optional and is only used if the *PAP* is a task. *AAA* is the primary information item, pointing to the main contents. *BBB* and *CCC* are optional information items, which can further specify the PAP. These information items may be one to six alphanumeric digits. The abbreviations used for the PAP IDs are listed in ▸Table 8.1 and ▸Table 8.2. All PAP IDs end with a number #. This number is usually 1, unless multiple IDs with similar preceding information items exist. In this case, they are enumerated increasingly.

Primary Information Item	Description
ACQ	Acquisition
ASS	Assessment
DEL	Delivery
EVA	Evaluation
ID	Identification
UPD	Update
VER	Verification

Table 8.1 Overview PAP ID Primary Information Items

Optional Information Item	Description
ALL	Overall
AUTO	Automated
B	Biometrics (fingerprints and facial images)
EES	Entry-Exit-System
FI	Facial Image
FP10R	Fingerprint 10 Finger Rolled
FP2P	2 Plain Fingerprints
FP4141	Fingerprint 4-1-4-1
FP442	Fingerprint 4-4-2
FPS	Single Slap Fingerprint Image
ID	Identification
nCIR	no Connected Identity Register
SV	Supervised
USV	Unsupervised
VER	Verification
wCIR	with Connected Identity Register

Table 8.2 Overview PAP ID Optional Information Items

List of Abbreviations

Abbreviation	Description
AP	Application Profile
ARE	Alien Register Enrolment
BCL	Border Control
FM	Function Module
GID	German Identity Documents
HLBS	High Level Biometric Services
IMA	Immigration Authorities
PAP	Partial Application Process

Bibliography

[BIB_RFC2119] *RFC 2119: Key words for use in RFCs to Indicate Requirement Levels.*