Federal Office
for Information Security

BSI Technical Guideline TR-03121-2

Biometrics for Public Sector Applications

Part 1: Framework

Version 5.0

Federal Office for Information Security
P.O. Box 20 03 63
53133 Bonn, Germany
E-mail: TRBiometrics@bsi.bund.de
Web: https://bsi.bund.de

List of Figures

List of Tables

1. Changelog

The following tables present the changes introduced between the latest versions of this Technical Guideline. The changelog lists the changes grouped per part of this Technical Guideline, per building block (Application Profile (AP), Partial Application Process (PAP), Task, Function Module (FM)) or element (section, table, figure) and type of change, refer to [KeepAChangelog]:

- *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-5.0

1.1.1. Changelog BSI TR-03121, Part 1

Element Name	Type of Change	Change Description
Building Blocks Mapping	Add	Added Building Blocks for AP Second Line.
Building Blocks Mapping	Fix	Added missing FM O-FI-DC and corresponding crosses.
Building Blocks Mapping	Fix	Added missing PAP UPD-B-EES-1 and PAP-ACQ-FPS-SV-1 for AP MBC. Added missing FM QA-FP-APP for GID APs. Corrected used REF FMs for GID-APs. Shifted order of the columns according to the order in the volume.

Table 1.1. Changelog BSI TR-03121, Part 1

1.1.2. Changelog BSI TR-03121, Part 2, Volume HLBS

Element Name	Type of Change	Change Description

Table 1.2. Changelog BSI TR-03121, Part 2

1.1.3. Changelog BSI TR-03121, Part 3

TR Building Block/Section		Type of Change	Change Description
Type	Name		
AP	Second Line, Volume BCL	Add	Preliminary version of this AP was added
AP	Manual Border Control, Volume BCL	Fix	Fingerprint acquisition was correctly implemented in the detailed processes, but it was missing in the ad-hoc-process for illustration.

TR Building Block/Section		Type of Change	Change Description
Type	Name		
AP	Manual Border Control, Volume BCL	Fix	The PAPs "Update EES Reference Biometrics" and "Supervised Acquisition Single Slap for Verification" were missing in the table of the required PAPs although they were correctly shown in the figures.
AP	Manual Border Control, Volume BCL	Fix	In figure "Visa Exempt First-Time Registered Border Crossing by Manual Border Control", the description of the arrows ("yes"/"no") following "FI data available?" was interchanged.
PAP	ACQ-FI-AUTO-1	Added	FI acquisitions without PAD shall perform within sevens seconds and with PAD within ten seconds.
FM	AH-FI-ICS	Changed	Lighting shall now be dynamic (dependent on the lighting conditions of the environment).
FM	AH-ALL-SSS, COM-CCTV-JPG	Changed	Changed minimum resolution for surveillance images from 1600 x 1200 to 1280 x 720.
FM	PAD-FP-APP	Removed	Removed requirement to signal omission of PAD alert as this is a logging requirement stated in LOG-FP-GENERIC, prolonged transition phase for non-certified PAD single finger scanners
PAP	Task ACQ-FPR-1	Added	Added Case A Option 2
FM	O-ALL-USV	Removed	Removed FM as it is not relevant for this volume.
FM	O-FI-ALL	Changed	Moved digital camera requirements to new FM O-FI-DC and flat bat scanner requirements to new FM O-FI-FBS
PAP	Introduction	Fix	FM Coding was missing in the list of Function Modules that may be applied in a PAP.

Table 1.3. 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 biometrics. 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 biometrics 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 [RFC2119].

3. Structure of TR 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)
  - In first volume of part 2, the Software Architecture based on the BioAPI standard (ISO/IEC 19784-1) is defined. Note, this part is deprecated.
  - In the second volume, the High Level Biometric Services (HLBS) are specified as well as Service Definitions for specific use cases.
- Part 3: Application Profiles, Function Modules and Processes (TR-03121-3)
  - In the third part, the different Applications 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.

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

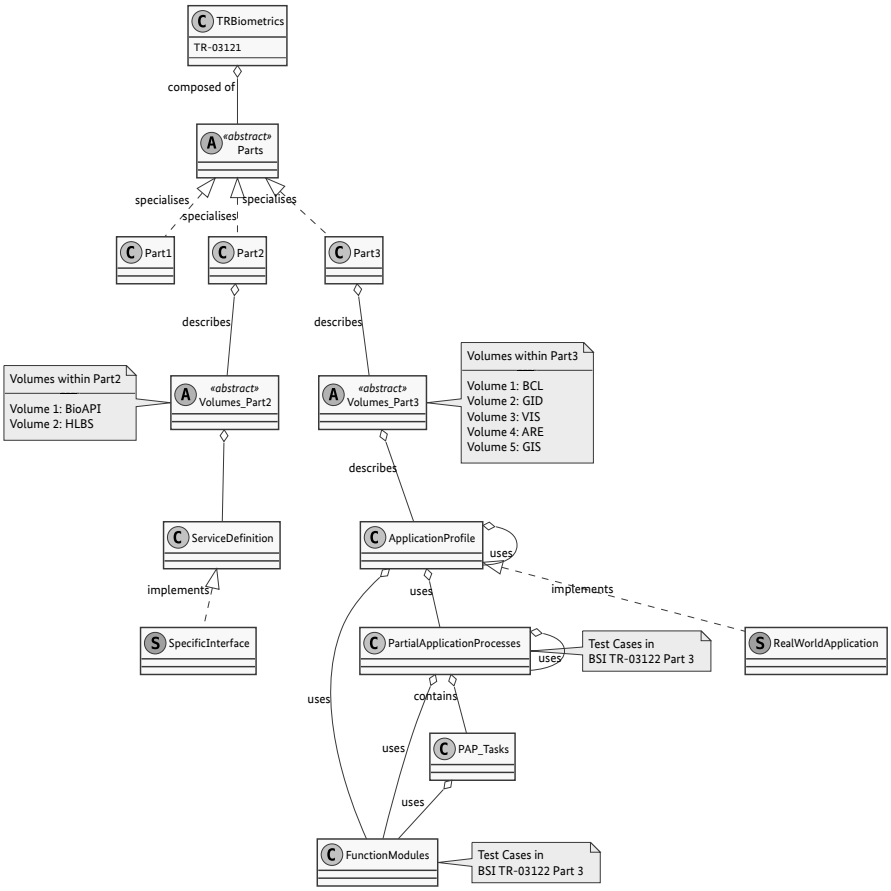

Figure 3.1. Class Diagram of the Technical Guidelines

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 2: Software Architecture – BioAPI Conformance Testing (TR-03122-2)
- 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 Border Control (BCL) volume, then the actual referenced Function Module is AH-FI-BCL. The same procedure holds for Application Profiles denoted as <AP> analogue. If no specific Function Module matches, 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 an Function Module or Partial Application Processes is a link within the document.

5. 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.

An Application Profile is described with the following items:

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

6. Function Modules

6.1. 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 sub-clauses which are assigned to unique identifiers. Within the sub-clauses requirements and recommendations are specified in detail.

6.2. Function Module Classes

Table 6.1 gives an overview of the different Function Module categories.

Function Module Category	Description
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.
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.
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 e.g. provision of full frontal images or segmentation of fingerprints.
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. Quality assurance is typically used in evaluation of an application's performance over time.
Presentation Attack Detection	The Presentation Attack Detection modules give requirements on the fake detection. This encloses, among other things, functionality and certification requirements.
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.
Operation	Within the module Operation, the working process is specified for the respective operator.
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.
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.
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

Function Module Category	Description
	reference data and a current biometric sample (usually a live presented image) no matter where the reference is stored.
Logging	The module Logging contains requirements how and in which modality data has to be logged.
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.
Evaluation	Methods and interfaces which are used in the scope of evaluation are the content of this module.

Table 6.1. Overview Function Module Categories

7. Partial Application Processes

7.1. 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 main 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 1-6 alphanumeric digits. The abbreviations used for the PAP ID are listed in Table 7.1 and Table 7.2. 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
EVA	Evaluation
ID	Identification
LNK	Linking
REQ	Request
UPD	Update
VER	Verification

Table 7.1. Overview PAP ID Primary Information Items

Optional Information Item	Description
CL	Candidate List
FI	Facial Image
FP	Fingerprint
FP1P	1 Plain Fingerprint
FP2P	2 Plain Fingerprints
FP4141	Fingerprint 4-1-4-1
FP442	Fingerprint 4-4-2
FPP	Plain Fingerprint
FPR	Rolled Fingerprint
FPS	Single Slap Fingerprint Image
ID	Identification
nCIR	no Connected Identity Register

Optional Information Item	Description
SV	Supervised
USV	Unsupervised
TF	Traveller File
VER	Verification
wCIR	with Connected Identity Register
B	Biometrics (fingerprints and facial images)

Table 7.2. Overview PAP ID Optional Information Items

List of Abbreviations

Abbreviation	Description
AP	Application Profile
FM	Function Module
HLBS	High Level Biometric Services
PAP	Partial Application Process

Bibliography

[KeepAChangelog] *Keep a Changelog – https://keepachangelog.com/en/1.0.0/*.

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