Federal Office
for Information Security

Technical Guideline TR-03122-1

Conformance Test Specification for BSI-TR 03121 Biometrics for Public Sector Applications

Part 1: Framework

Version 4.3

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

Index of Contents

List of Tables

List of Figures

1 Introduction

1.1 Motivation and Objectives of the Conformance Test Specification

The Technical Guideline Biometrics for Public Sector Applications (TR-03121) specifies requirements and recommendations for the use of biometric data within the scope public sector applications. The requirements on specific Function Modules, as defined in TR-03121-3, can be implemented for different public sector applications through hardware and software components from various vendors.

The objective of this Technical Guideline is to offer a base for consistent and comparable quality assurance regarding the different components that will be applied in order to fulfil these requirements. This conformance test specification

- specifies tests for the Software Architecture (in particular in regard to conformance testing),
- defines all test cases being relevant to verify the conformance for the different requirements described in the Function Modules.

1.2 Target Audience

Audience for this guideline are institutions that are dealing with projects using biometrics in public sector applications that require certified modules, hardware, and/or software. These include:

- Vendors of hardware or software products that want to present their solutions for conformance test and acquire to be compliant to this Technical Guideline.
- Evaluation laboratories that check the conformance of hardware and/or software modules that are used within the scope of biometrics and electronic identity documents in public sector applications.

2 Structure of the Conformance Test Specification

The Conformance Test Specification consists of the following parts:

- Part 1: Framework (TR-03122-1)
  - TR-03122-1 is the framework document of the conformance test specification.
- Part 2: Software Architecture – BioAPI Conformance Testing (TR-03122-2)
  - The second part defines the architecture model for Software Architecture conformance testing. Essential topics are the description of the BioAPI Conformance Test Suite (CTS) as well as the Testing Methodology for BioAPI components.
- Part 3: Test Cases for Function Modules (TR-03122-3)
  - The third part defines test cases for hardware and software components according to their specification in TR-03121-3.

Figure 2-1 shows an structural overview of TR-03121 and TR-03122.

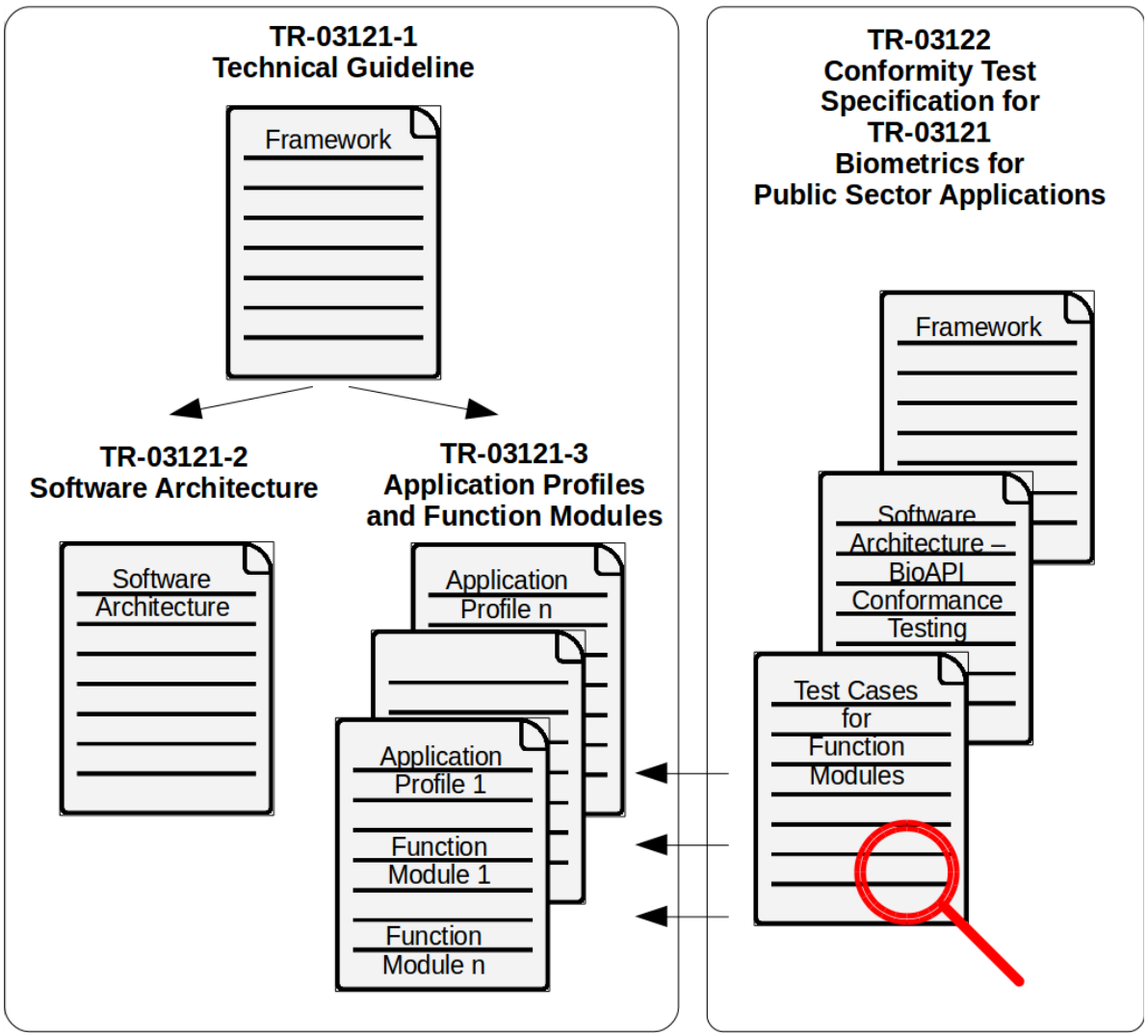

Figure 2-1: Overview of Technical Guidelines

2.1 Test Case Specification for Function Modules

The requirements for an electronic identity document and the connected public sector application are combined in several Function Modules within TR-03121-3. If the conformance to one or more specific Function Modules has to be checked the reader has to identify at first the relevant Function Modules with the according abbreviation e.g. P-FP-GID.
As a result the corresponding test cases can be selected in TR-03122-3 under the same identification while the prefix 'TC-' indicates the according test case. Depending on the number of defined test cases the abbreviation is followed by an ascending numbering e.g. TC-P-FP-GID-001.
In general, a test case in TR-03122-3 is structured in three parts as shown in Table 2-1.

Test Case ID: TC-P-FP-GID-001	
Scope	
— Short overview of the test case	
Precondition	
— Requirements that need to be fulfilled before the test case can be executed	
Description	
1. Listing of every single test step	
Expected Result	— Description of the expected result for the corresponding test step

Table 2-1: Example of the Structure of a Test Case

Conformance to the specification of a Function Module can be established if all test cases for that Function Module are completed successfully and the requirements of the test methodology are satisfied.
Several test cases can be assigned to one Function Module each containing one or multiple test steps.
Note that the Conformance Test Specification does not define requirements for the object to be tested except the interfaces for conformance testing.

3 Conformance Test Interfaces

Conformance testing in the context of TR-03121 is based on an interface compliant to Representational State Transfer (REST). This interface is described in the following sections.

The Implementation Under Test (IUT) must provide an external interface as REST service accessible to the Conformance Test Suite (CTS), through which conformance testing is performed. Using this interface, the IUT is able to output generated data to the CTS during the test execution of the regular process which is performed by the operator of the evaluation laboratory.

Additionally, the interface can be used to provide pre-defined input from the CTS to the IUT in order to be able to verify its output in a defined state.

In opposite to the standard workflow, this request is used as an alternative point of entry so that the standard steps for the acquisition of the biometric image (e.g. facial image or fingerprint image), further processing of the image and/or compression of the image can be skipped.

In case pre-defined input data is required for a test case, the IUT is provided with external test data through the interface by the CTS. The input data is provided as XML data with root element "`biocts-testsetup`" as defined in the XML schemata of TR-03121. The schema definition can be found in the file "`biocts4v2.xsd`". An example can be found in the file "`biocts-testsetup.xml`".

3.1 Interface description

In the conformance test scenario, a client-server architecture is at hand. The IUT represents the server providing a HTTP-based REST-interface to the CTS which acts as the client.

A test case is triggered by an HTTP request sent by the CTS to the IUT. The path as part of the request URI specifies the test case ID as defined in part 3 of this guideline:

```
/TR03122/{testcase-id}/{version}
```

The version indicates the revision of the specification for this test case and is typically incremented when the test case's interface requirements are changed.

The HTTP request method (relevant are GET and POST) depends on whether the test case requires input data. As described above, any input data for the IUT must be embedded in XML data (`biocts-testsetup`) within the request.

The result generated by the IUT must also be returned as XML data to the CTS. Depending on the test case at hand, the result consists of XML data conforming to TR-03121, which further may include an embedded, application specific format (e.g. GSAT XML). The specific data format and URI for test case initiation is described further in each test case definition of TR-03122 Part 3.

Since performing a test case may comprise manual interaction within the IUT and hence can take accordingly long, the communication timeout has to be considered and set adequately high.

3.1.1 Test cases *not* requiring pre-defined input data

In case a test case does not require any input data a priori, the CTS sends a GET request to the IUT. The IUT is triggered upon receiving the request and performs the test case (e.g. facial image capture and encoding).

Subsequently, the result data is returned to the CTS within the response body. The response header must be set to "`Content-Type: application/xml; charset=utf-8`" and include the message length of the response body.

Example:

Request (CTS → IUT):

```
GET /TR03122/TC-COD-PH-GSAT3-001/1 HTTP/1.1
Content-Type: application/xml; charset=utf-8
```

Response (IUT → CTS):

```
HTTP/1.1 200 OK
Content-Type: application/xml; charset=utf-8
Content-Length: 12345

<aad:aad-app [...]
      <bio:Records>
      <bio:XMLRecord type="gsat-xml" purpose="enrolment"  id="id_1234"
size="5687">
      [...]
</aad:aad-app>
```

3.1.2 Test cases requiring pre-defined input data

Should a test case require initial provision of data, the CTS sends a POST request to the IUT including this data. The request header must be set to "`Content-Type: application/xml; charset=utf-8`" and include the content length. Any input data is provided within the message body as XML (UTF-8 encoded).

The result data is returned to the CTS within the response body including a response header set to "`Content-Type: application/xml; charset=utf-8`" and respective content length.

Example:

Request (CTS → IUT):

```
POST /TR03122/TC-QA-PH-SB-001/1 HTTP/1.1
Content-Type: application/xml; charset=utf-8
Content-Length: 12345

<?xml version="1.0" encoding="UTF-8"?>
[...]
<biocts:Parameter type="face" format="bmp">
VghpcyBmaWVQLg==</biocts:Parameter>
</biocts:biocts-testsetup>
```

Response (IUT → CTS):

```
HTTP/1.1 200 OK
Content-Type: application/xml; charset=utf-8
Content-Length: 67890

<?xml version="1.0" encoding="UTF-8"?>
<FaceQuality [...]
```

3.1.3 Response Codes

Table 3-1 lists the possible HTTP status codes which must be returned by the IUT to indicate the status to the CTS.

Status Code	Status message	Description
200	*OK*	The request was successfully processed. Test case result data is included in the response body.
400	*Bad Request*	The IUT could not process the request due to defective input data.
404	*Not Found*	The IUT cannot perform the test case, e.g. due to missing implementation.
500	*Internal Server Error*	An internal, technical error occurred in the IUT during processing the request.

Table 3-1: Possible status codes used by the IUT

4 Conformance Instruments

Besides the interfaces and the subject which is to be tested, the conformance instruments build an important part for conformance testing. All necessary components for conformance testing are included.

The certification authority approves all conformance instruments. Part of this are the following components:

- Conformance test tools
  The software components that are used to check the compliance of the BSP compare the expected result with the actually received result. Furthermore, for the validation of the coding, a validating parser shall be used.
- Appropriate conformance test databases
  The conformance test databases contain specific test data that are used by the evaluation laboratory to perform certain test cases. Furthermore, tolerance thresholds and domain parameters (e.g. ground truth values) are provided. Default processing, exceptions, and error behaviour can be verified.

Besides the afore described components further test resources are necessary for specific test cases:

- Images
  In order to check the regular process of scanning, a photo in order to acquire a facial image needs to be available.
- Application Form
  Facial images can be processed directly in digital form or by scanning photos that were taken by a photographer. In the second case, an application form is used to adjust the photo on a document with a special pattern.
- Finger
  In order to check the regular process of capturing fingerprint images, several fingers need to be available.
- Image decoding algorithm
  For the further image decoding respective algorithms such as a FBI certified WSQ algorithm and a JPEG2000 Decoder according to ISO need to be available.

5 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
CMP	Biometric Comparison
COD	Coding
COM	Compression

Abbreviation	Description
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
NCA	National Central Authority

Abbreviation	Description
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

6 Bibliography

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

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

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

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

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

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

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

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

[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