Federal Office
for Information Security

Technical Guideline TR-03122-2

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

Part 2: Software Architecture - BioAPI Conformance Testing

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

1 Introduction ... 5
2 Overview of BioAPI Conformance Testing ... 7
2.1 Architecture Models for Conformance Testing ... 8
2.1.1 Conformance Testing of BioAPI Applications ... 8
2.1.2 Conformance Testing of BioAPI Frameworks ... 9
2.1.3 Conformance Testing of BioAPI BSPs ... 9
3 BioAPI Conformance Test Suite ... 11
3.1 Terminology ... 11
3.2 System Components ... 11
3.3 Scope and application area ... 11
3.4 Design of a CTS ... 11
4 Testing Methodology ... 13
4.1 Fundamentals ... 13
4.1.1 Provision of Relevant Conformance Test Components and Documentation ... 13
4.1.2 Test Preparation ... 13
4.1.3 Test Performance ... 13
4.1.4 Conformance Testing Documentation ... 13
4.2 Testing Methodology for BioAPI BSP ... 14
4.2.1 Basic Conditions ... 14
4.2.2 Conformance Testing Procedure ... 15
4.2.3 Conformance test components ... 15
4.2.4 Conformance Documentation ... 16
5 List of Abbreviations ... 17
6 Bibliography ... 20

List of Tables

List of Figures

Figure 2-1: Architecture Model According to BioAPI 2.0 7
Figure 2-2: Architecture Model for Conformance Testing of BioAPI Applications 8
Figure 2-3: Architecture Model for Conformance Testing of BioAPI Framework 9
Figure 2-4: Architecture Model for Conformance Testing of BioAPI BSPs 9
Figure 4-1: Architecture of the CTS for BSPs 15

1 Introduction

This document (BSI TR-03122-2) describes the conformance testing in the scope of the Software Architecture as defined in TR-03121-2. Within this document the BioAPI Conformance Test Suite is introduced and the testing methodology for BioAPI BSPs and frameworks is specified.

2 Overview of BioAPI Conformance Testing

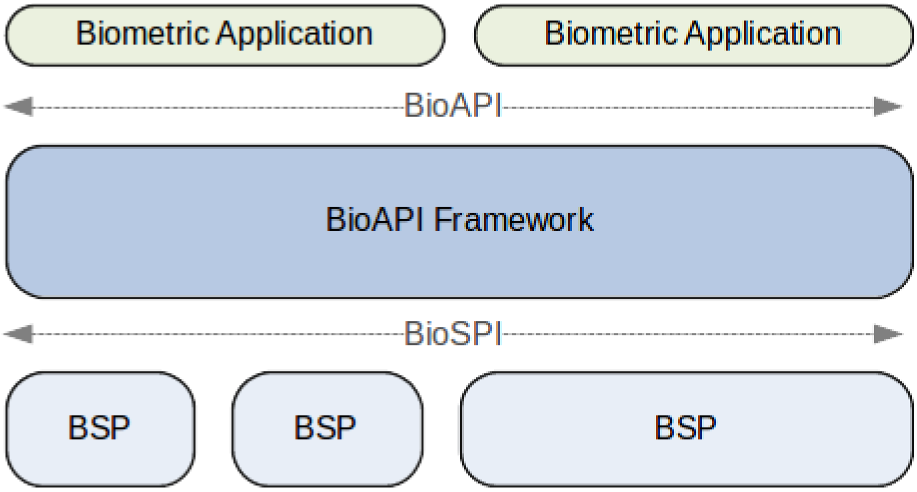

Figure 2-1: Architecture Model According to BioAPI 2.0

The ISO standard BioAPI 2.0 according to [ISO_19784-1] published in 2006 defines the architecture model for biometric systems as well as interfaces between the components of this architecture. The BioAPI architecture as shown in Figure 2-1 is structured in the following components:

- The **BioAPI application** uses biometric functions for a defined purpose. For example this can be the acquisition of biometric data within the scope of the application for electronic identity documents or the acquisition and verification of biometric data for access control.
- A **BioAPI framework** provides the required biometric functions to the application. The interface between the framework and the application is called Biometric Application Programming Interface (BioAPI) and is defined in [ISO_19784-1].
- A **Biometric Service Provider** (BSP) is a component that is loaded and administrated by the framework. It implements the main biometric functionality like enrolment of biometric data or the comparison of biometric data. The framework is able to load several BSPs and provide their functionality to the application. The interface between BSP and framework is called Biometric Service Provider Interface (BioSPI) and is defined in [ISO_19784-1].
- A **Biometric Function Provider** (BFP) is a component that is managed by the framework but is loaded by a BSP. The concept is to transfer basis functions like returning of image data of a sensor or the storage of data from this component. However this area has been standardised by ISO only partly until now and is excluded explicitly within the scope of the BioAPI conformance testing as defined later on.

In 2007 the international standard ISO/IEC 24709:2007 for conformance testing of BioAPI components was published. Here, the necessary methods, procedures and test assertions are defined (for all different kinds of components of the architecture model that are used) to check conformance to the base BioAPI standard. In the following sections the different aspects of conformance testing are presented and a system architecture for a BioAPI Conformance Test Suite (CTS) is described.

The international standard ISO/IEC 24709 specifies the conformance testing of BioAPI components. So far[1] two parts of the standard have been published:

1 Last updated: June 2009

- Part 1 of the standard [ISO_24709-1] describes the general procedure for the conformance testing as well as modality how the different components of the BioAPI architecture are being tested individually. A main part of the standard defines a particular XML based language for the definition of single test assertions. Furthermore the XML syntax for the test protocols as well as the test reports.
- Part 2 of the standard [ISO_24709-2] contains the test assertions that have to be performed for conformance testing of the BSPs. The test cases are defined in an XML based language, which is specified in the first part of the standard.

Further parts of the standard will define test assertions for the conformance testing of a BioAPI framework (part 3) and furthermore test assertions for BioAPI applications (part 4).

Therefore, actual conformance testing based on this guideline is actually limited to BSP testing.

2.1 Architecture Models for Conformance Testing

Within the standard the BioAPI component that is to be tested is called "implementation under test" (IUT). Based on the BioAPI architecture model an IUT can be a BioAPI application, a BioAPI framework, or a BioAPI BSP. So far test assertions for BioAPI BFPs are not part of conformance testing due to the fact that the standardisation process has not been finished yet. Because the interfaces and the requirements for the different architecture components differ from each other, the standard defines different architecture models for conformance testing.

2.1.1 Conformance Testing of BioAPI Applications

Basically, the conformance testing of BioAPI applications checks if the application works in conformance with the BioAPI framework based on the standard. Thereby it has to be assumed that the functionality of the application can only be tested in connection with a real BioAPI framework and the corresponding BSPs that are required for a specific use case.

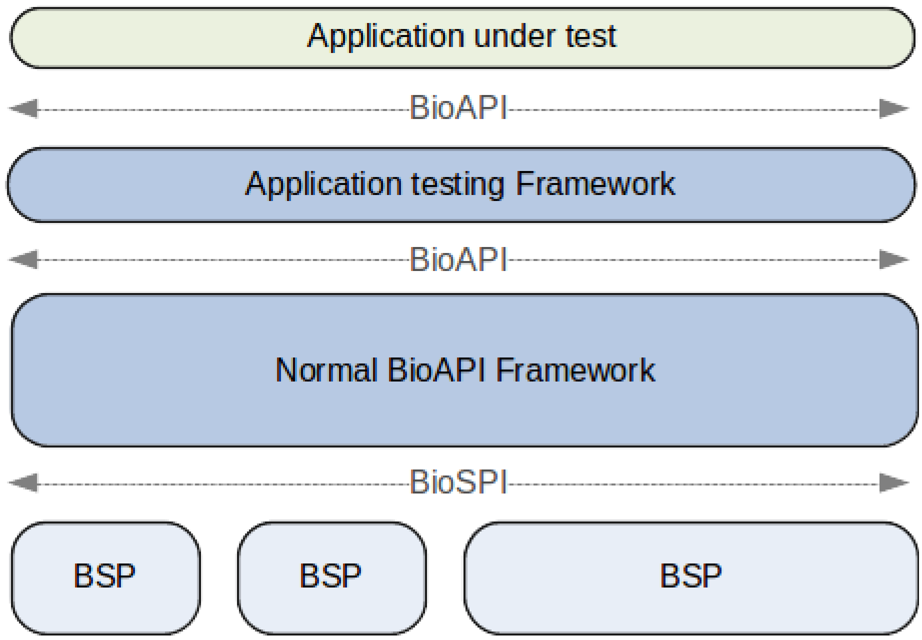

Figure 2-2: Architecture Model for Conformance Testing of BioAPI Applications

For conformance testing of BioAPI applications a test framework is integrated as an additional layer between the application to be tested and the regular BioAPI framework. The architecture model for conformance testing of BioAPI applications is shown in the Figure above.

The test framework provides the same interfaces as the BioAPI framework and forwards these according to the respective test cases.

2.1.2 Conformance Testing of BioAPI Frameworks

Within conformance testing of BioAPI frameworks both the interfaces to the application and the interfaces to the BSPs have to be considered by the test assertions. This is done by enclosing the BioAPI frameworks with two test components.

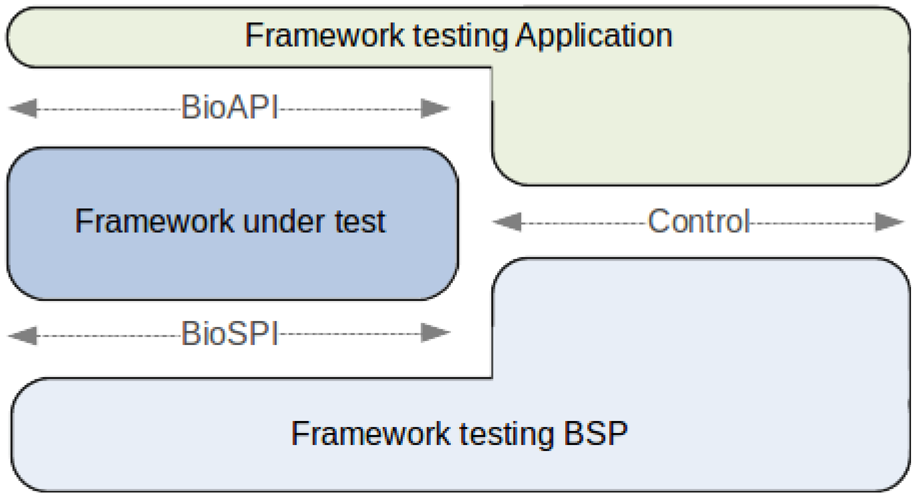

Figure 2-3: Architecture Model for Conformance Testing of BioAPI Framework

A test application calls functions from the framework under test and a framework testing BSP expects according requests from the framework. In order to handle the test assertions in a coordinated way, the test application and the test BSP have to communicate additionally over a direct control channel with each other.

2.1.3 Conformance Testing of BioAPI BSPs

Within the conformance testing of BioAPI BSPs the BSP to be tested is loaded from a BSP testing application instead of a BioAPI framework (compare Figure 2-3). This testing application calls the functions to be tested of the BSP.

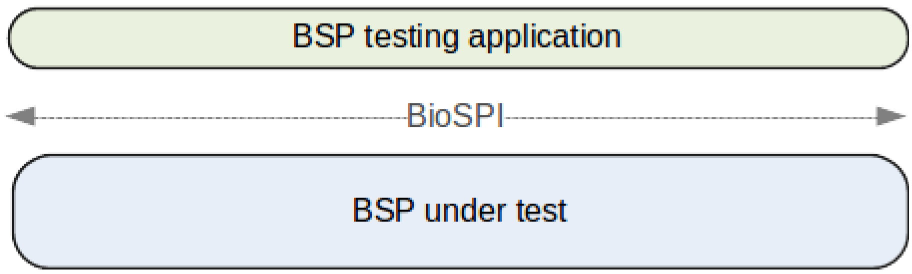

Figure 2-4: Architecture Model for Conformance Testing of BioAPI BSPs

Because, in general, a BSP implements besides the obligatory functions only a subset of the SPI interface (compare the different BSP classes in section A.4 in [ISO_19784-1]), a definition of the testing scope is mandatory.

3 BioAPI Conformance Test Suite

3.1 Terminology

BioAPI conformance testing is done through the use of a BioAPI Conformance Test Suite (CTS).

It is the task of the CTS to perform defined test assertions with connected test data in a defined test pass. The test pass has to be designed in a way that repetition of test cases is possible and provides the same results. The performance of the test cases should be automated as far as possible.

3.2 System Components

In order to cover all models of conformance testing a CTS has to provide the following system components:

- BSP testing application
- Framework testing application
- Framework testing BSP
- Application testing framework

Currently, only BSP testing is supported by this guideline.

For all components, the following properties are in place:

- The description of the test assertions is done on the basis of the XML language defined in [ISO_24709-1]. In all components it is necessary to provide the test assertions in an executable way. This can either be done by a native implementation or by an interpreter which loads the XML files dynamically and executes them.
- An XML based test protocol is generated for every test assertion. The syntax of the protocol is based on XML and is specified in [ISO_24709-1]. All system components of a CTS have to provide protocol data in the same way.

3.3 Scope and application area

The BioAPI standard [ISO_19784-1] defines only the architecture of the system as well as the interfaces between the components of this architecture. However, the physical architecture is not part of the standard. In general, the architecture components of the BioAPI standard are expected to be realised as dynamic libraries. On some platforms where this is not possible, they might be realised differently.

3.4 Design of a CTS

The CTS shall implement the following requirements:

- The testing is performed automatically.
- A repetition of testing is easily possible and given the same conditions the same results will be returned.
- The test assertions shall not be implemented statically, instead will be performed by dynamically loading and executing the respective XML test descriptions.

- The basic system components of the CTS are implemented independently from the underlying operating system.

4 Testing Methodology

This chapter describes the general procedure for conformance testing of biometric application programming interfaces (BioAPI). This includes the necessary preconditions and all test steps that have to be performed. It is assumed, that an adequate CTS as defined in section 3 is available to the evaluation laboratory.

4.1 Fundamentals

4.1.1 Provision of Relevant Conformance Test Components and Documentation

In order to perform the conformance testing for BioAPI BSPs, BioAPI frameworks, and BioAPI applications, it is necessary for the evaluation laboratory to be provided with all relevant components and documents. A main component is the IUT itself. [ISO_24709-1] does not specify the concrete characteristics of the IUT software, so different variants are possible (single files, an archive file, an installation package,...). Therefore, an installation manual is necessary in order to install the IUT in the test environment.

In case the IUT has to be run by the operator (i. e. user interaction is required) during test performance, an user manual is necessary. Here, in particular, information about the graphical user interface encapsulated in the BSP has to be provided.

The base document for the test procedure is the BioAPI Conformance Statement (BCS). It states formally which mandatory, optional, and conditional functions and requirements of the BioAPI standard are implemented by the IUT. As a result, the immediate scope of the tests to be performed on the IUT is deviated. The content of the BCS is based on the architecture model of the conformance test.

4.1.2 Test Preparation

After the evaluation laboratory has received all relevant components and documents for conformance testing, the according test preparations can be conducted. Basically, this means the following actions:

- Installation of the IUT in the test environment of the evaluation laboratory based on the provided installation manual.
- Preparation and configuration of the CTS for the conformance test in the IUT.
- Analysis of the BioAPI Conformance Statement (BCS) and creation of a Conformance Test Plan (CTP) that defines the scope of the conformance tests.

4.1.3 Test Performance

After the test preparation is finished, the test performance can be started based on the CTP. Therefore the CTS is executed by the operator of the evaluation operator and all relevant test protocols will be compiled within this process.

4.1.4 Conformance Testing Documentation

As described before, the test performance is connected with resulting test protocols that are used as the base for the documentation of conformance or the absence of conformance. After all test assertions have been finished, a test report is compiled based on all protocol files that have been generated during test performance. This report includes all performed test assertions in connection with all input and output parameters as well as the test results. Furthermore, the test reports encloses a detailed description of the test environment (in particular operating system, used hardware, etc.).

4.2 Testing Methodology for BioAPI BSP

In the following sections the testing methodology for conformance testing of BSPs is described.

4.2.1 Basic Conditions

The concept of the CTS shall be based on the following basic conditions:

- The BSP to be checked is available as dynamic library which is loaded during run time with the respective functions of the operating system (e.g. LoadLibrary under Microsoft Windows ©).
- The conformance test system requires no standard BioAPI framework for the performance of BSPs. A BSP to be tested has to be loaded and executed by the BSP testing application without a BioAPI framework.
- Generally, the BSP to be tested may not have further requirements regarding the BSP testing application of the CTS. If the BSP testing application has to call specific initialisation functions based on the architecture of the operating system, the vendor of the BSP has to provide adequate information regarding the BSP. For example, the initialisation functions of the graphical system can be referenced only once during application. Therefore, the BSP cannot call the initialisation functions again.

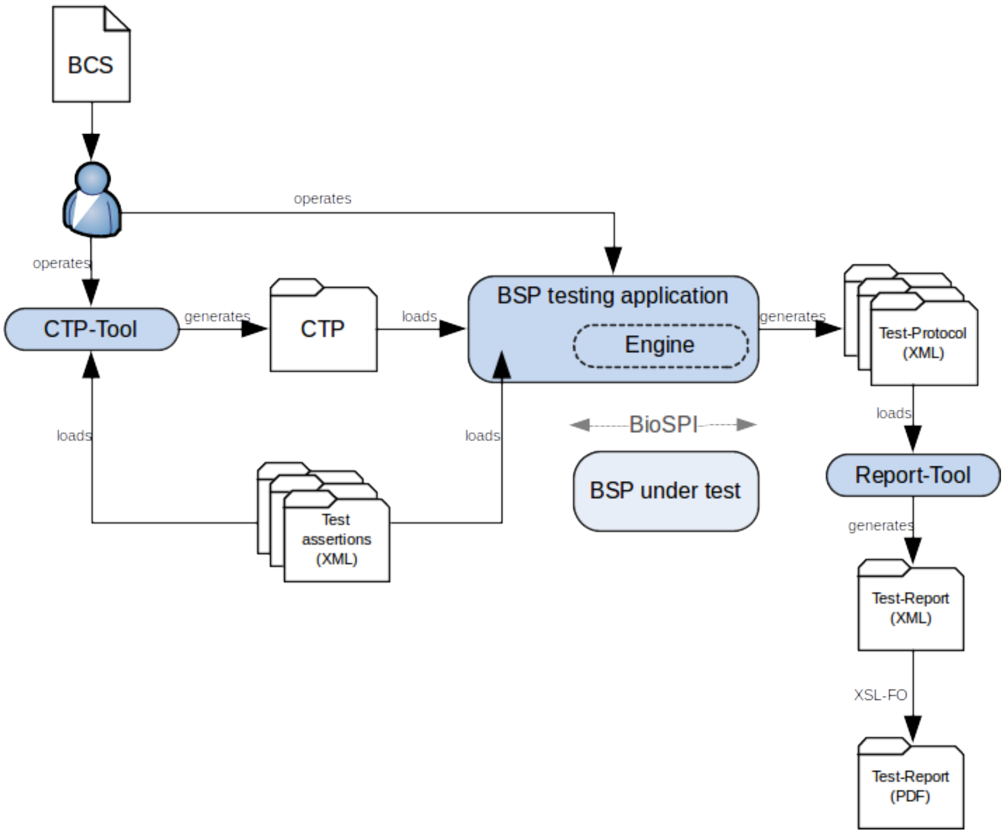

Figure 4-1: Architecture of the CTS for BSPs

4.2.2 Conformance Testing Procedure

Figure 4-1 illustrates the architecture of the CTS for BSPs. The respective components will be explained individually in the following.

In general the following sequence is intended:

1. At first, all standard installation and configuration steps are performed in order to integrate the BSP to be checked in the infrastructure of the evaluation laboratory.
2. The operator starts the CTP tool and loads all test assertions that are available. With the aid of the information given in the BCS, all test assertions to be executed are compiled and are saved within a CTP file.
3. Afterwards, the BSP test application is started by the operator and the CTS file as well as the necessary test assertions are loaded. The application offers the possibility to the operator to choose the execution of a single or all test assertions. The respective test protocols are compiled accordingly.
4. Once the operator has finished the tests, the test report is generated with the aid of the report tool based on the XML syntax based on the ISO standard. A human readable report document is created.

4.2.3 Conformance test components

- Test assertions (XML)
  The description of the test assertions follows the same notation as specified in [ISO_24709-2]. They are

distributed over different files, each file contains exactly one <package> element. The test assertion files are loaded by the CTS tool and the BSP testing application and are executed in the following.

- CTP tool
  The CTP tool supports the operator to arrange the concrete tests to be performed for a BSP. As a base, the test assertions files and as well as the BCS which is provided by the vendor are made available. The content of the BCS depends on the architecture model of the conformance tests. Section 7 in [ISO_24709-2] specifies all relevant information that has to be provided in the BCS for the conformance test of BSPs.
- CTP file
  The CTP file is generated by the CTP tool and contains the test assertions to be performed for the specific conformance test. The format of this file is not specified by ISO 24709. It seems to be reasonable to follow the format of the other files of the CTS by providing a XML based structure. In general a CTP file should be generated only once during conformance test of a BSP during test preparation. The availability of a CTP file has the advantage that it is permanently defined and saved during the scope of the conformance test. Therefore repetition of all or only individual test assertions is possible at any time.
- BSP testing application
  The BSP testing application loads the CTP file as well as all necessary test assertions. Afterwards the operator executes the test assertions.

During execution of a test assertion the BSP testing application generates a test protocol for this test.

4.2.4 Conformance Documentation

- Test protocols
  During execution the BSP test application generates a test protocol for every test assertion. The syntax of the protocol is defined in [ISO_24709-1].
- Report tool
  The report tool generates a test report based on all test protocols containing all documented and accumulated results.
- Test report (XML)
  The test report contains all results of the conformance tests. Although the XML syntax of the test report is described in [ISO_24709-1] informally, it is not defined in a XML schema in opposite to the XML test protocols.
- Test report (final documentation)
  As last step, a transformation is applied to the XML test report to generate a human readable report.

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