
**Information technology — Biometric
application programming interface —
Part 1:
BioAPI specification**

*Technologies de l'information — Interface de programmation
d'applications biométriques —
Partie 1: Spécifications BioAPI*

<https://standards.iteh.ai/catalog/standards/sist/6afc460b-0b7c-4eb9-b84e-1e0af4ba50ab/iso-iec-19784-1-2006>

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 19784-1:2006

<https://standards.iteh.ai/catalog/standards/sist/6afc460b-0b7c-4eb9-b84e-1e0af4ba50ab/iso-iec-19784-1-2006>

© ISO/IEC 2006

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword.....	vi
Introduction	vii
1 Scope	1
2 Conformance	2
3 Normative references	2
4 Terms and definitions.....	2
5 Symbols and abbreviated terms	7
6 The BioAPI architecture	8
6.1 The BioAPI API/SPI Architectural Model	8
6.2 The BioAPI BSP Architectural Model.....	9
6.3 The Component Registry	10
6.4 BSP and BFP Installation and De-installation	11
6.5 BSP Load and BioAPI Unit Attachment.....	12
6.6 Controlling BioAPI Units.....	13
6.7 BIR Structure and Handling.....	13
6.7.1 BIR Structure	13
6.7.2 BIR Data Handling.....	14
7 BioAPI types and macros	15
7.1 BioAPI	15
7.2 BioAPI_BFP_LIST_ELEMENT	15
7.3 BioAPI_BFP_SCHEMA	15
7.4 BioAPI_BIR	16
7.5 BioAPI_BIR_ARRAY_POPULATION	17
7.6 BioAPI_BIR_BIOMETRIC_DATA_FORMAT	17
7.7 BioAPI_BIR_BIOMETRIC_PRODUCT_ID	17
7.8 BioAPI_BIR_BIOMETRIC_TYPE	18
7.9 BioAPI_BIR_DATA_TYPE	18
7.10 BioAPI_BIR_HANDLE	19
7.11 BioAPI_BIR_HEADER.....	19
7.12 BioAPI_BIR_PURPOSE	20
7.13 BioAPI_BIR_SECURITY_BLOCK_FORMAT	21
7.14 BioAPI_BIR_SUBTYPE	21
7.15 BioAPI_BOOL.....	22
7.16 BioAPI_BSP_SCHEMA	22
7.17 BioAPI_CANDIDATE	23
7.18 BioAPI_CATEGORY	24
7.19 BioAPI_DATA	24
7.20 BioAPI_DATE	24
7.21 BioAPI_DB_ACCESS_TYPE	25
7.22 BioAPI_DB_MARKER_HANDLE	25
7.23 BioAPI_DB_HANDLE	25
7.24 BioAPI_DBBIR_ID	25
7.25 BioAPI_DTG.....	25
7.26 BioAPI_EVENT	26
7.27 BioAPI_EVENT_MASK.....	26
7.28 BioAPI_EventHandler	26
7.29 BioAPI_FMR	27
7.30 BioAPI_FRAMEWORK_SCHEMA	27
7.31 BioAPI_GUI_BITMAP	28

7.32	BioAPI_GUI_MESSAGE	28
7.33	BioAPI_GUI_PROGRESS	29
7.34	BioAPI_GUI_RESPONSE	29
7.35	BioAPI_GUI_STATE	29
7.36	BioAPI_GUI_STATE_CALLBACK	29
7.37	BioAPI_GUI_STREAMING_CALLBACK	30
7.38	BioAPI_HANDLE	30
7.39	BioAPI_IDENTIFY_POPULATION	31
7.40	BioAPI_IDENTIFY_POPULATION_TYPE	31
7.41	BioAPI_INDICATOR_STATUS	31
7.42	BioAPI_INPUT_BIR	31
7.43	BioAPI_INPUT_BIR_FORM	32
7.44	BioAPI_INSTALL_ACTION	32
7.45	BioAPI_INSTALL_ERROR	32
7.46	BioAPI_OPERATIONS_MASK	32
7.47	BioAPI_OPTIONS_MASK	33
7.48	BioAPI_POWER_MODE	34
7.49	BioAPI_QUALITY	34
7.50	BioAPI_RETURN	35
7.51	BioAPI_STRING	35
7.52	BioAPI_TIME	36
7.53	BioAPI_UNIT_ID	36
7.54	BioAPI_UNIT_LIST_ELEMENT	36
7.55	BioAPI_UNIT_SCHEMA	36
7.56	BioAPI_UUID	38
7.57	BioAPI_VERSION	38
8	BioAPI functions	39
8.1	Component Management Functions	39
8.1.1	BioAPI_Init	39
8.1.2	BioAPI_Terminate	40
8.1.3	BioAPI_GetFrameworkInfo	41
8.1.4	BioAPI_EnumBSPs	42
8.1.5	BioAPI_BSPLoad	43
8.1.6	BioAPI_BSPUnload	45
8.1.7	BioAPI_BSPAttach	46
8.1.8	BioAPI_BSPDetach	48
8.1.9	BioAPI_QueryUnits	49
8.1.10	BioAPI_EnumBFPs	51
8.1.11	BioAPI_QueryBFPs	52
8.1.12	BioAPI_ControlUnit	54
8.2	Data Handle Operations	55
8.2.1	BioAPI_FreeBIRHandle	55
8.2.2	BioAPI_GetBIRFromHandle	56
8.2.3	BioAPI_GetHeaderFromHandle	57
8.3	Callback and Event Operations	58
8.3.1	BioAPI_EnableEvents	58
8.3.2	BioAPI_SetGUICallbacks	59
8.4	Biometric Operations	60
8.4.1	BioAPI_Capture	60
8.4.2	BioAPI_CreateTemplate	62
8.4.3	BioAPI_Process	64
8.4.4	BioAPI_ProcessWithAuxBIR	65
8.4.5	BioAPI_VerifyMatch	67
8.4.6	BioAPI_IdentifyMatch	69
8.4.7	BioAPI_Enroll	72
8.4.8	BioAPI_Verify	74
8.4.9	BioAPI_Identify	76
8.4.10	BioAPI_Import	79
8.4.11	BioAPI_PresetIdentifyPopulation	80

ITeCh STANDARD PREVIEW

(standards.iteh.ai)

ISO/IEC 19784-1:2006

[https://standards.iteh.ai/catalog/standards/sist/6a1c400b-0b7c-4cb9-b84c-](https://standards.iteh.ai/catalog/standards/sist/6a1c400b-0b7c-4cb9-b84c-1c0a40a50ab/iso-iec-19784-1-2006)

[1c0a40a50ab/iso-iec-19784-1-2006](https://standards.iteh.ai/catalog/standards/sist/6a1c400b-0b7c-4cb9-b84c-1c0a40a50ab/iso-iec-19784-1-2006)

8.5	Database Operations	81
8.5.1	BioAPI_DbOpen	81
8.5.2	BioAPI_DbClose	83
8.5.3	BioAPI_DbCreate	84
8.5.4	BioAPI_DbDelete	85
8.5.5	BioAPI_DbSetMarker	86
8.5.6	BioAPI_DbFreeMarker	87
8.5.7	BioAPI_DbStoreBIR	88
8.5.8	BioAPI_DbGetBIR	89
8.5.9	BioAPI_DbGetNextBIR	90
8.5.10	BioAPI_DbDeleteBIR	91
8.6	BioAPI Unit operations	92
8.6.1	BioAPI_SetPowerMode	92
8.6.2	BioAPI_SetIndicatorStatus	93
8.6.3	BioAPI_GetIndicatorStatus	94
8.6.4	BioAPI_CalibrateSensor	95
8.7	Utility Functions	96
8.7.1	BioAPI_Cancel	96
8.7.2	BioAPI_Free	97
9	BioAPI Service Provider Interface	98
9.1	Summary	98
9.2	Type Definitions for Biometric Service Providers	98
9.2.1	BioSPI_EventHandler	98
9.2.2	BioSPI_BFP_ENUMERATION_HANDLER	99
9.2.3	BioSPI_MEMORY_FREE_HANDLER	100
9.3	Biometric Service Provider Operations	101
9.3.1	SPI Component Management Operations	101
9.3.2	SPI Data Handle Operations	107
9.3.3	SPI Callback and Event Operations	108
9.3.4	SPI Biometric Operations	109
9.3.5	SPI Database Operations	112
9.3.6	SPI BioAPI Unit operations	114
9.3.7	SPI Utility Functions	115
10	Component registry interface	116
10.1	BioAPI Registry Schema	116
10.1.1	Framework Schema	116
10.1.2	BSP Schema	117
10.1.3	BFP Schema	118
10.2	Component registry functions	119
10.2.1	BioAPI_Util_InstallBSP	119
10.2.2	BioAPI_Util_InstallBFP	120
11	BioAPI error handling	121
11.1	Error Values and Error Codes Scheme	121
11.2	Error Codes and Error Value Enumeration	121
11.2.1	BioAPI Error Value Constants	121
11.2.2	Implementation-Specific Error Codes	121
11.2.3	General Error Codes	121
11.2.4	Component Management Error Codes	123
11.2.5	Database Error Values	124
11.2.6	Location Error Values	125
11.2.7	Quality Error Codes	127
Annex A (normative)	Conformance	128
Annex B (normative)	CBEFF Patron Format Specification: BioAPI patron format	140
Annex C (informative)	Specification overview	145
Annex D (informative)	Calling sequence examples and sample code	154
Bibliography	167

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 19784-1 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

ISO/IEC 19784 consists of the following parts, under the general title *Information technology — Biometric application programming interface*:
(standards.iteh.ai)

- *Part 1: BioAPI specification* [ISO/IEC 19784-1:2006](https://standards.iteh.ai/catalog/standards/sist/6afc460b-0b7c-4eb9-b84e-1e0af3ba50ab/iso-iec-19784-1-2006)
- *Part 2: Biometric archive function provider interface*

This is the first ISO/IEC standard on BioAPI. Previous versions were published by ANSI and the BioAPI Consortium. As the last official non-ISO release was designated Version 1.1, this ISO/IEC 19784-1 version is designated Version 2.0. This is to distinguish the versions of BioAPI products in the marketplace.

Introduction

This part of ISO/IEC 19784, the BioAPI specification, provides a high-level generic biometric authentication model suited to most forms of biometric technology. No explicit support for multimodal biometrics is currently provided.

An architectural model is described which enables components of a biometric system to be provided by different vendors, and to interwork through fully-defined Application Programming Interfaces (APIs).

A key feature of the architecture is the BioAPI Framework, which supports calls by one or more application components (provided by different vendors, and potentially running concurrently) using the BioAPI API specification. The BioAPI Framework provides this support by invoking (through a Service Provider Interface, SPI) one or more biometric service provider (BSP) components (provided by different vendors, and potentially running concurrently) which can be dynamically loaded and invoked as required by an application component.

At the lowest level there is hardware or software that performs biometric functions such as capture, matching, or archiving. These parts of the architecture are called BioAPI Units, and can be integral to a BSP or can be supplied as part of a separate BioAPI Function Provider (BFP) component.

Interactions (through the BioAPI Framework) can occur between BSPs from different vendors provided data structures used to record information from the BioAPI Units they access conform to other International Standards, and in particular to ISO/IEC 19794 [5].

The final component of the BioAPI architecture is the recognition that a BSP can provide its biometric services either:

- <http://standards.iteh.ai/catalog/standards/sist/6af5460b-0b7c-4eb9-b84e-1e0af4ba50ab/iso-iec-19784-1-2006>
- (standards.iteh.ai)
- a) by the use of BioAPI Units that are integral to (that is, directly managed by) the BSP, or
 - b) by invoking, through the BioAPI Function Provider Interface (FPI), one or more BFP components (provided by different vendors) that manage BioAPI Units that are integral to the BFP.

NOTE: A BioAPI Unit may consist of software only, or a combination of software and hardware (e.g., a biometric sensor, archive, or algorithm).

For each type of BioAPI Unit supported by a BSP (or BFP) there may be one or more BioAPI Units of that type which can be dynamically inserted and removed from the system. Insertion and removal generates events that can be signalled (through the BSP and the BioAPI Framework) to an application.

The BioAPI specification covers the basic biometric functions of Enrollment, Verification, and Identification (see Annex C), and includes a database interface to allow an application to manage the storage of biometric records through an archive BioAPI Unit managed by a BSP or BFP. This provides for optimum performance (e.g., when performing the biometric Identification function within a large population) of the archiving and biometric search processes.

The interface to the application provides primitives that allow it to manage the capture of biometric samples from a biometric sensor by accessing the corresponding BioAPI Unit, and the use of those biometric samples for Enrollment (storage in an application-controlled or BSP-controlled BIR database), and subsequent Verification or Identification against those stored records.

This part of ISO/IEC 19784 also specifies the content of a biometric component registry (information about the biometric components that have been installed on the biometric system). It also provides a component registry interface for the management and inspection of that registry.

This part of ISO/IEC 19784 uses the C programming language (see ISO/IEC 9899) to specify the data structures and function calls that form the BioAPI interfaces.

ISO/IEC 19784-1:2006(E)

Clause 6 describes the BioAPI architectural model and its components, and the interfaces that are specified between these components.

Clause 7 defines the data structures used in the BioAPI.

Clause 8 defines the function calls initiated by an application and supported by a conforming BioAPI Framework that are either handled internally by the BioAPI Framework (for example enumeration of installed BioAPI components) or mapped to a function provided by a BSP.

Clause 9 defines the function calls supported by a conforming BSP (and invoked by the BioAPI Framework in response to a call from a biometric application).

Clause 10 specifies the form of the biometric component registry and the component registry interface.

Clause 11 defines the handling of events and error returns.

Annex A is normative, and specifies details of conformance requirements and proformas that can be used by the vendor of a BioAPI Biometric Application, Framework, or BSP component to identify those functions and biometric record formats that must be supported.

NOTE: A future International Standard (ISO/IEC 24709) will address conformance testing for this BioAPI specification. [7]

Annex B is normative, and specifies the BioAPI biometric information record (BIR) as a CBEFF Patron Format in accordance with ISO/IEC 19785-1. It provides a description of the biometric record specified in this part of ISO/IEC 19784, together with the platform-independent bit-pattern representation of such a record for storage and transfer.

Annex C is informative, and provides a general tutorial on a number of aspects of the BioAPI specification.

Annex D is informative, and provides example code to illustrate calling sequences and to provide implementation guidance.

Information technology — Biometric application programming interface —

Part 1: BioAPI specification

1 Scope

This part of ISO/IEC 19784 defines the Application Programming Interface (API) and Service Provider Interface (SPI) for standard interfaces within a biometric system that support the provision of that biometric system using components from multiple vendors. It provides interworking between such components through adherence to this part of ISO/IEC 19784 and to other International Standards.

The BioAPI specification is applicable to a broad range of biometric technology types. It is also applicable to a wide variety of biometrically enabled applications, from personal devices, through network security applications, to large complex identification systems.

This part of ISO/IEC 19784 supports an architecture in which a BioAPI Framework supports multiple simultaneous biometric applications (provided by different vendors), using multiple dynamically installed and loaded (or unloaded) biometric service provider (BSP) components and BioAPI Units (provided by other different vendors), possibly using one of an alternative set of BioAPI Function Provider (BFP) components (provided by other vendors) or by direct management of BioAPI Units.

NOTE: Where BioAPI Units are provided by a different vendor from a BSP, a standardised BioAPI Function Provider Interface (FPI) may be needed. This is outside the scope of this part of ISO/IEC 19784, but is specified by later parts for the different categories of FPI.

This part of ISO/IEC 19784 is not required (and should normally not be referenced) when a complete biometric system is being procured from a single vendor, particularly if the addition or interchange of biometric hardware, services, or applications is not a feature of that biometric system. (Such systems are sometimes referred to as "embedded systems".) Standardisation of such systems is not in the scope of this part of ISO/IEC 19784.

It is not in the scope of this part of ISO/IEC 19784 to define security requirements for biometric applications and biometric service providers.

NOTE: ISO 19092 provides guidelines on security aspects of biometric systems. [3]

The performance of biometric systems (particularly in relation to searches of a large population to provide the biometric identification capability) is not in the scope of this part of ISO/IEC 19784. Trade-offs between interoperability and performance are not in the scope of this part of ISO/IEC 19784.

This part of ISO/IEC 19784 specifies a version of the BioAPI specification that is defined to have a version number described as Major 2, Minor 0, or version 2.0.

NOTE: Earlier versions of the BioAPI specification were not International Standards.

2 Conformance

2.1 Annex A specifies the conformance requirements for BioAPI components claiming conformance to this part of ISO/IEC 19784.

2.2 This part of ISO/IEC 19784 uses the C programming language (see ISO/IEC 9899) to specify the interfaces that it defines. A BioAPI component can conform to this part of ISO/IEC 19784 by the provision or use of that interface with languages other than the C programming language, provided that the component on the other side of such an interface can use the interface through the detailed C programming language specification given in this part of ISO/IEC 19784. (See also clause 7.1.)

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9834-8, *Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities: Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 Object Identifier components*

ISO/IEC 9899:1999, *Programming Languages — C*

ISO/IEC 10646:2003, *Information technology — Universal Multiple-Octet Coded Character Set (UCS)*

ISO/IEC 19785-1, *Information technology — Common Biometric Exchange Formats Framework — Part 1: Data element specification*

ISO/IEC 19785-2, *Information technology — Common Biometric Exchange Formats Framework — Part 2: Procedures for the operation of the Biometric Registration Authority*

4 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE: Function names and data element names are not included here, but are defined within the body of this part of ISO/IEC 19784.

4.1 adaptation
template adaptation
use of a BIR produced from a newly captured and verified biometric sample to automatically update or refresh a reference template

NOTE: This procedure is used to minimize the effects of template aging.

4.2 attach session
temporary association between an application, a single BSP, and a set of BioAPI Units that are managed either directly or indirectly by that BSP

4.3**BioAPI component**

component of the BioAPI architecture with a defined interface that can be supplied by a separate vendor and which is subject to conformance testing

NOTE: BioAPI components include BioAPI applications, the BioAPI Framework, BSPs, and BFPs.

4.4**BioAPI Function Provider****BFP**

component that manages one or more BioAPI Units of a specific category

NOTE 1: Interfaces to BioAPI Function Providers are standardized in subsequent parts of ISO/IEC 19784.

NOTE 2: BFPs are categorized according to the categories of BioAPI Units that they manage (see clause 6.2.4).

4.5**BioAPI Unit**

abstraction of a hardware or software resource that is directly managed by a BSP or BFP

NOTE: BioAPI Units are categorized (see clause 6.2.2) and include sensor units, archive units, matching algorithm units and processing algorithm units.

4.6**biometric** (adj.)

pertaining to the field of biometrics

4.7**biometric data block****BDB**

block of data with a defined format that contains one or more biometric samples or biometric templates

NOTE 1: ISO/IEC 19784 does not support BDB formats that are not an integral multiple of eight bits.

NOTE 2: There is no requirement that a BDB format be self-delimiting.

NOTE 3: Each part of ISO/IEC 19794 standardises one or more BDB formats. Vendor specific formats can also be specified and identified.

NOTE 4: Within BioAPI, the BDB is "opaque" to the application and is therefore sometimes referred to as an opaque biometric data block.

4.8**biometric information record****BIR**

data structure containing one or more BDBs, together with information identifying the BDB formats, and possibly further information such as whether a BDB is signed or encrypted (see ISO/IEC 19785-1)

NOTE: This part of ISO/IEC 19784 defines a BIR format (see clause 7.4) that supports only a single BDB. ISO/IEC 19785-1 defines a more general BIR format that supports multiple BDBs within the BIR, and the above definition is used in common by the two International Standards. When the term BIR is used in this part of ISO/IEC 19784, it normally refers to the specific BIR format defined by BioAPI (see Annex B), not to an arbitrary BIR. The term BioAPI BIR is used where clarity is needed.

4.8.1**reference BIR**

BIR whose BDB(s) contain one or more biometric templates

4.8.2**sample BIR**

BIR whose BDB(s) contain only biometric samples that are not templates

4.9

biometric sample

information obtained from a biometric sensor, either directly or after further processing

NOTE: See also raw biometric sample, intermediate biometric sample, and processed biometric sample.

4.9.1

biometric template

biometric sample or combination of biometric samples that is suitable for storage as a reference for future comparison

4.9.2

intermediate biometric sample

biometric sample obtained by processing a raw biometric sample, intended for further processing

4.9.3

processed biometric sample

biometric sample suitable for comparison

4.9.4

raw biometric sample

biometric sample obtained directly from a biometric sensor

NOTE: The formats for raw biometric samples are not currently standardised, and depend on the nature of the biometric device and the vendor of that device. They may in the future be standardised as part of the standardisation of specific biometric devices.

ITeH STANDARD PREVIEW
(standards.iteh.ai)

4.9.5

reference template

biometric template that has been stored

[ISO/IEC 19784-1:2006](https://standards.iteh.ai/catalog/standards/sist/6afc460b-0b7c-4eb9-b84e-1e0af4ba50ab/iso-iec-19784-1-2006)

4.10

biometric sensor

biometric hardware used to capture raw biometric samples from a subject

<https://standards.iteh.ai/catalog/standards/sist/6afc460b-0b7c-4eb9-b84e-1e0af4ba50ab/iso-iec-19784-1-2006>

NOTE: The term 'biometric device' is used interchangeably with this term.

4.11

biometric service provider

BSP

component that provides biometric services to an application through a defined interface by managing one or more BioAPI Units directly, or through interfaces to BioAPI Function Providers

4.12

biometrics (noun)

automated recognition of individuals based on their behavioural and biological characteristics

4.13

callback

mechanism by which a component that exposes an API invokes a function within a component that uses that API, where the address of that function has been previously passed as an input parameter of an API function call

NOTE: This mechanism enables a BioAPI component to communicate with another BioAPI component other than by invoking an API function, usually in response to an event or interrupt.

4.14

component registry

information maintained by the BioAPI Framework concerning the BioAPI components that are available on a biometric system

4.15 encrypt encryption

(reversible) transformation of data by a cryptographic algorithm to produce ciphertext; that is, to hide the information content (protect the confidentiality) of the data

NOTE 1: Encryption algorithms consist of two processes: encryption (or encipherment) which transforms plaintext into ciphertext, and decryption (or decipherment) which transforms ciphertext to plaintext.

NOTE 2: Encryption may be used for either security or privacy reasons.

4.16 enrollment

process of collecting one or more biometric samples from an individual, and the subsequent construction of a biometric reference template which can then be used to verify or determine the individual's identity

NOTE: The reference template would normally be stored by a biometric application, a BSP supporting an archive BioAPI Unit, or both.

4.17 False Match Rate FMR

measure of the probability that a biometric matching process will incorrectly identify an individual or will fail to reject an impostor

NOTE 1: Within BioAPI, FMR is used as a means of specifying scores and thresholds (see clause C.4).

NOTE 2: Historically, False Acceptance Rate (FAR) has also been used with a similar definition, but FMR is the preferred term in International Standards. Similarly for False Rejection Rate (FRR), as opposed to the preferred False Non-Match Rate (FNMR).

4.18 handle

parameter returned by a BioAPI function (A say) that can be used by the BioAPI application in a subsequent function call to identify a BioAPI component or data element within the component A

NOTE: Types of handles include:

BIR_Handle, generated by a BSP to select or access a BIR within that BSP.

BSP Attach Session Handle, for an attach session.

DB_Handle, generated by a BSP to select or access a BIR database controlled by that BSP.

4.19 identify identification

one-to-many process of comparing a submitted biometric sample against a reference population to determine whether the submitted biometric sample matches any of the reference templates in that reference population in order to determine the identity of the enrollee whose template was matched

NOTE: This is often called an "identification match" or "identifymatch".

4.20 match matching

one-to-one process of comparing a submitted biometric sample against a single biometric reference template and scoring the level of similarity.

NOTE 1: An accept or reject decision would then normally be based upon whether this score exceeds a given threshold.

NOTE 2: Matching algorithms and their effect on False Match Rate and False Non-Match Rate scores are currently not standardised.

NOTE 3: See also identify (4.19) and verify (4.28).

4.21

payload

data, provided at the time of enrollment and associated with a reference template, which can be released upon a successful biometric verification.

NOTE: Examples of payloads include user names, accounts, passwords, cryptographic keys, or digital certificates (see clause C.5).

4.22

score

scoring

value indicating the degree of similarity or correlation between a biometric sample and a biometric reference template

4.23

security block

SB

block of data with a defined format that contains security information (for example, related to encryption or integrity) related to a BIR (see ISO/IEC 19785-1)

4.24

self-contained device

combination device which includes a biometric sensor and all or part of the BSP functionality

iTeh STANDARD PREVIEW
(standards.iteh.ai)

NOTE: A self-contained device may include the ability to not only capture a biometric, but also to process, match, and/or store it. This functionality is typically implemented in hardware/firmware.

<https://standards.iteh.ai/catalog/standards/sist/6afc460b-0b7c-4eb9-b84e-1e0af4ba50ab/iso-iec-19784-1-2006>

4.25

signature

digital signature

data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the origin and integrity of the data unit and protect against forgery, e.g. by the recipient

NOTE: Digital signatures may be used for purposes of authentication, data integrity, and non-repudiation

4.26

threshold

predefined value which establishes the degree of similarity or correlation (that is, a score) necessary for a biometric sample to be deemed a match with a biometric reference template

4.27

universally unique identifier

UUID

128-bit value generated in accordance with ISO/IEC 9834-8 and providing unique values between systems and over time

4.28

verify

verification

one-to-one process of comparing a single submitted biometric sample against a biometric reference template to determine whether the submitted biometric sample matches the reference template

NOTE: This is often called a "verification match" or "verifymatch".

5 Symbols and abbreviated terms

API – Application Programming Interface

BDB – Biometric Data Block

BFP – BioAPI Function Provider

BIR – Biometric Information Record

BSP – Biometric Service Provider

CBEFF – Common Biometric Exchange Formats Framework

FMR – False Match Rate

FPI – Function Provider Interface

GUI – Graphical User Interface

ID – Identity/Identification/Identifier

MOC – Match on Card

PID – Product ID

SB – Security Block

SBH – Standard Biometric Header

NOTE: This term and abbreviation is imported from ISO/IEC 19785-1

SPI – Service Provider Interface

UUID – Universally Unique Identifier

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC 19784-1:2006](#)

[and abbreviation is imported from ISO/IEC 19785-1](#)
[1e0af4ba50ab/iso-iec-19784-1-2006](#)