BS ISO/IEC 30108-1:2015
Incorporating corrigendum June 2018

BSI Standards Publication

Information technology — Biometric Identity Assurance Services

Part 1: BIAS services

bsi.

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30108-1:2015

National foreword

This British Standard is the UK implementation of ISO/IEC 30108-1:2015.

The UK participation in its preparation was entrusted to Technical Committee IST/44, Biometrics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 539 01415 0

ICS 35.240.15

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 November 2015.

Amendments/corrigenda issued since publication

Date	Text affected
30 June 2018	Implementation of ISO corrected text 15 April 2016: See ISO Foreword for added Table A.1 rows

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30108-1:2015

INTERNATIONAL STANDARD

ISO/IEC 30108-1

First edition
2015-11-01

Corrected version
2016-04-15

Information technology — Biometric Identity Assurance Services —

Part 1: BIAS services

Technologies de l'information — Service d'assurance de l'identité biométrique (BIAS) —

Partie 1: Services BIAS

Reference number
ISO/IEC 30108-1:2015(E)

Documents
Document Sharing Hub

© ISO/IEC 2015

Full document details: BS ISO/IEC 30108-1:2015

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30108-1:2015

Contents

Page

Foreword ... **v**

Introduction ... **vii**

1 Scope ... **1**

2 Conformance ... **1**

3 Normative references ... **1**

4 Terms and definitions ... **1**

5 Symbols and abbreviated terms ... **3**

6 System context ... **3**
- 6.1 Service-oriented architectures ... 3
- 6.2 BIAS architecture ... 5
- 6.3 Identity models ... 6
- 6.4 Identity databases ... 8
- 6.5 BIAS implementation considerations (informative) ... 9

7 Biometric Identity Assurance Services ... **10**
- 7.1 BIAS interface XML schema ... 10
- 7.2 Primitive services ... 11
  - 7.2.1 Add Subject To Gallery ... 11
  - 7.2.2 Check Quality ... 12
  - 7.2.3 Classify Biometric Data ... 13
  - 7.2.4 Create Encounter ... 13
  - 7.2.5 Create Subject ... 14
  - 7.2.6 Delete Biographic Data ... 14
  - 7.2.7 Delete Biometric Data ... 15
  - 7.2.8 Delete Document Data ... 15
  - 7.2.9 Delete Encounter ... 16
  - 7.2.10 Delete Subject ... 16
  - 7.2.11 Delete Subject From Gallery ... 17
  - 7.2.12 Get Identify Subject Results ... 17
  - 7.2.13 Identify Subject ... 18
  - 7.2.14 List Biographic Data ... 19
  - 7.2.15 List Biometric Data ... 20
  - 7.2.16 List Document Data ... 21
  - 7.2.17 Perform Fusion ... 21
  - 7.2.18 Query Capabilities ... 22
  - 7.2.19 Retrieve Biographic Data ... 26
  - 7.2.20 Retrieve Biometric Data ... 27
  - 7.2.21 Retrieve Document Data ... 28
  - 7.2.22 Set Biographic Data ... 29
  - 7.2.23 Set Biometric Data ... 29
  - 7.2.24 Set Document Data ... 30
  - 7.2.25 Transform Biometric Data ... 31
  - 7.2.26 Update Biographic Data ... 31
  - 7.2.27 Update Biometric Data ... 32
  - 7.2.28 Update Document Data ... 32
  - 7.2.29 Verify subject ... 33
- 7.3 Aggregate Services ... 34
  - 7.3.1 Delete ... 34
  - 7.3.2 Enrol ... 35
  - 7.3.3 Get Deletion Results ... 36
  - 7.3.4 Get Enrol Results ... 36
  - 7.3.5 Get Identify Results ... 37
  - 7.3.6 Get Update Results ... 37

© ISO/IEC 2015 – All rights reserved

AVA Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30108-1:2015

7.3.7 Get Verify Results ... 38
7.3.8 Identify ... 38
7.3.9 Retrieve Data ... 40
7.3.10 Update ... 40
7.3.11 Verify ... 41

8 Data elements and data types ... 42
8.1 Biographic data ... 42
8.1.1 Biographic Data Type ... 42
8.1.2 Biographic Data Item Type ... 43
8.1.3 Biographic Data Set Type ... 43
8.1.4 Biographic Data List Type ... 44
8.2 Biometric Data ... 44
8.2.1 CBEFF BIR Type ... 44
8.2.2 CBEFF BIR List Type ... 45
8.2.3 Biometric Data Element Type ... 46
8.2.4 Biometric Data List Type ... 46
8.3 Document Data ... 46
8.3.1 Document Data Type ... 46
8.3.2 Document Data List Type ... 47
8.4 Candidate Lists ... 48
8.4.1 Candidate Type ... 48
8.4.2 Candidate List Type ... 48
8.5 Capabilities ... 49
8.5.1 Capability Type ... 49
8.5.2 Capability List Type ... 49
8.6 Fusion Information ... 50
8.6.1 Fusion Information Type ... 50
8.6.2 Fusion Information List Type ... 50
8.6.3 Fusion Identity List Type ... 51
8.7 Other Data Types ... 51
8.7.1 Encounter Category Type ... 51
8.7.2 Encounter List Type ... 51
8.7.3 Information Type ... 52
8.7.4 List Filter Type ... 52
8.7.5 Option Type ... 52
8.7.6 Processing Options Type ... 53
8.7.7 Token Type ... 53

9 Error handling and notification ... 54
9.1 Successful service calls ... 54
9.2 Error condition codes ... 54

10 Security ... 56

Annex A (normative) **Conformance requirements ... 57**

Annex B (informative) **Sample biographic data format references ... 66**

Annex C (informative) **Example usage scenarios ... 67**

Annex D (informative) **Example encounter scenarios ... 74**

Bibliography ... 78

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 37, *Biometrics*.

ISO/IEC 30108 consists of the following parts, under the general title *Information technology — Biometric Identity Assurance Services*:

— *Part 1: BIAS Services*

This corrected version of ISO/IEC 30108-1:2015 incorporates the following corrections plus other minor editorial modifications.

Table A.1: The following rows were missing and have been added to the end of the table:

Get Verify Results		C*			C*		C*
Identify		X					X
Retrieve Data		X			X		
Update		X			X		X
Verify		X			X		X
Capability Information Items							
AggregateInputDataOptional		X			X		X
AggregateInputDataRequired		X			X		X
AggregateProcessingOption		X			X		X
AggregateReturnData		X			X		X
AggregateServiceDescription		X			X		X
BiographicDataSet	X	X	X	X	X		
CBEFFPatronFormat	X	X	X	X	X	X	X

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

ClassificationAlgorithmType	X						
ConformanceClass	X	X	X	X	X	X	X
Gallery	X	X	X				
IdentityModel	X	X	X	X	X		
ComparisonAlgorithm	X	X	X	X	X	X	X
ComparisonScore	X	X	X	X	X	X	X
QualityAlgorithm	X						
SupportedBiometric	X	X	X	X	X	X	X
TransformOperation	X						

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

Introduction

This part of ISO/IEC 30108 defines the architecture, operations, data elements, and basic requirements for biometric identity assurance services – a framework for the implementation of generic, biometric-based identity services within a services-oriented environment. An identity in the context of BIAS comprises a subject, biographic data, and biometric data. Other parts are intended to define specific BIAS implementations (or bindings) within specific environments, for example, SOAP web services.

BIAS services are generic in nature, being modality neutral, and not targeted at any particular business application. These services include those related to identity data management, transformation, and biometric comparison. Services are invoked by a BIAS requester and implemented by a BIAS service provider (responder). It does not prescribe the architecture or business logic of either the requester or service provider.

Two categories of identity services are defined – primitive and aggregate. Primitive services are more atomic and well-defined, whereas the aggregate services tend to be higher level and enable more flexibility on the part of the BIAS service provider.

Two identity models are also defined – person-centric and encounter-based. Person-centric systems maintain a single up-to-date record (set of data) for a given subject, whereas an encounter-based system retains data related to each interaction the subject has with the system.

This part of ISO/IEC 30108 represents a version of BIAS subsequent to that previously standardized by INCITS and OASIS, therefore, it is denoted as version 2.0.

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

Information technology — Biometric Identity Assurance Services —

Part 1:
BIAS services

1 Scope

This part of ISO/IEC 30108 defines biometric services used for identity assurance that are invoked over a services-based framework. It provides a generic set of biometric and identity-related functions and associated data definitions to allow remote access to biometric services.

The binding of these services to specific frameworks is not included in this part of ISO/IEC 30108, but will be the subject of subsequent parts.

Although focused on biometrics, this part of ISO/IEC 30108 will necessarily include support for other related identity assurance mechanisms such as biographic and document capabilities. BIAS is intended to be compatible with and used in conjunction with other biometric standards as described in Clause 3.

Specification of biometric functionality is limited to remote (backend) services. Services between a client-side application and biometric capture devices are not within the scope of this part of ISO/IEC 30108.

Integration of biometric services as part of an authentication service or protocol is not within the scope of this part of ISO/IEC 30108.

2 Conformance

Annex A specifies the conformance requirements for systems/components claiming conformance to this part of ISO/IEC 30108.

3 Normative references

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

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

ISO/IEC 19785-3, *Information technology — Common Biometric Exchange Formats Framework — Part 3: Patron format specifications*

4 Terms and definitions

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

4.1
biometric sample
analogue or digital representation of biometric characteristics prior to biometric feature extraction

Note 1 to entry: As an example, a record containing the image of a finger is a biometric sample.

© ISO/IEC 2015 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

4.2
claim to identity
biometric claim
assertion that an individual is or is not the bodily source of a specified or unspecified biometric reference in an identity assurance system

4.3
encounter
event in which the BIAS requester interacts with a *subject* (4.11) resulting in data being collected during or about the encounter

Note 1 to entry: The event may involve collection of biographic, biometric, document, and/or contextual data during an enrolment or recognition interaction.

4.4
encounter-centric system
system that supports encounter processing maintaining a one-to-many relationship between *subjects* (4.11) and *encounters* (4.3) and which does not necessarily contain a single, unique set of information for each subject

4.5
gallery
group of *subjects* (4.11) related by a common purpose, designation, or status

EXAMPLE A watch list or a set of subjects entitled to a certain benefit.

4.6
identification
biometric identification
process of searching against a biometric enrolment database to find and return the biometric reference identifier(s) attributable to a single individual

4.7
identity assurance
process of establishing, determining, and/or confirming a subject identity

4.8
merge
combination of biometric data during the process of updating an enrolment record

Note 1 to entry: The "merge" operation is implementation specific, however, it may include either adding a new sample to a multi-sample record or performing some level of biometric fusion, for example, sample or feature level fusion.

4.9
merge
combination of two or more subject records into a single subject record

4.10
person-centric model
identity model in which a single master record is maintained on a *subject* (4.11) which is updated over time when additional, newer, or better biographic, biometric, and/or document information becomes available and which does not maintain separate historical data records for each system encounter with the subject

4.11
subject
person who is known to an identity assurance system

Note 1 to entry: The person may also be a biometric capture subject or biometric data subject, but this is not the case in all situations.

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

4.12
verification
biometric verification
process of confirming a *biometric claim* (4.2) through biometric comparison

Note 1 to entry: Verification is usually performed through a one-to-one comparison in which a *biometric sample* (4.1) from one individual (probe) is compared to a biometric reference(s) from one individual to produce a comparison decision (match/no-match) and optionally, a comparison score.

5 Symbols and abbreviated terms

AFIS	Automated Fingerprint Identification System
BIAS	Biometric Identity Assurance Services
BIR	Biometric Information Record
CBEFF	Common Biometric Exchange Formats Framework
ESB	Enterprise Service Bus
ID	Identity/Identification/Identifier
OASIS	Organization for the Advancement of Structured Information Standards
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol

6 System context

This clause provides an overview of Service-Oriented Architectures, the BIAS architecture, and BIAS implementation considerations.

6.1 Service-oriented architectures

Service-Oriented Architectures are software architectures in which reusable services are deployed onto application servers and then consumed by clients in different applications or business processes. They are intended to decouple the implementation of a software service from the interface that calls that service. This allows clients of a service to rely on a consistent interface regardless of the implementation technology of the service [JDJ] (see Annex C).

Biometric services are one of the types of services that can be provided over such a remote interface in a distributed information system across a collection of networks. This can occur in a 2-tier, 3-tier, or N-tier environment. A diagram of a simple N-tier architecture is shown in Figure 1.

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

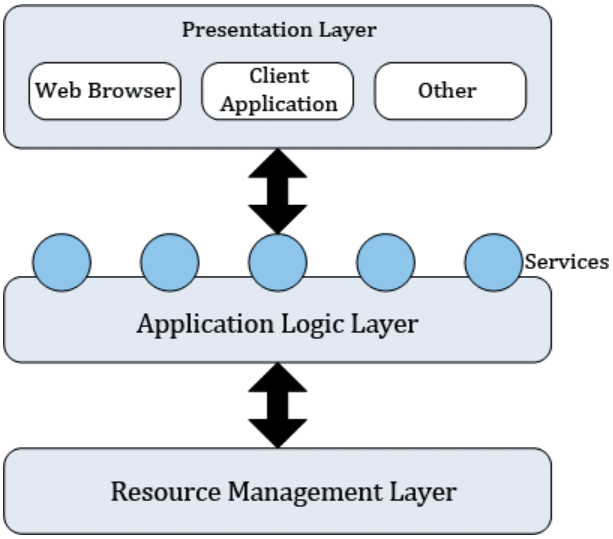

Figure 1 — Simple N-Tier architecture

In this diagram, BIAS services are defined between the application logic layer and the resource management layer.

Examples of biometric resources that are of interest may include one or more of the following:

— A fingerprint verification server;

— A 1:N iris search engine;

— A facial biometric watch list;

— A criminal or civil automated fingerprint identification system (AFIS);

— A name-based biographic identity database;

— An archive of biometric identifiers;

— A population of subjects.

It is desired that a generic set of services be defined that allows clients to remotely access and manage these capabilities. To the extent possible, domain specific implementations are to be avoided.

NOTE This part of ISO/IEC 30108 is intended to support a wide variety of application domains which may include government (e.g. background checking, border management, and criminal justice), enterprise (e.g. logical access control), and commercial biometric identity management implementations (e.g. employee databases).

Services are well defined, self-contained modules that provide standard business functionality and are independent of the state or context of other services. Services can be easily assembled to form a collection of autonomous and loosely-coupled business processes.

It is not the intention that specific business logic be instantiated within the service definitions – this logic is more appropriate within the application logic layer – either in the higher level system initiating the series of requests, or within the middleware [e.g. an enterprise service bus (ESB), workflow manager, or biometric middleware] as appropriate. To do so would of necessity make the interface less generic, modular, and flexible and require that the interface be updated each time the logic changed, defeating one of the primary purposes of the services architecture.

The services to be defined are not targeted at a particular SOA implementation or framework. Instead, they are defined in such a manner as to be able to be utilised within any such architecture. This is accomplished by separately defining (in another standard) the bindings to that

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

architecture/implementation. For example, Web services bindings are defined in the OASIS BIAS Messaging Protocol.

6.2 BIAS architecture

The BIAS architecture consists of the following components:

— BIAS services (interface definition);

— BIAS data (schema definition);

— BIAS bindings (defined outside this standard).

The BIAS services expose a common set of operations to external requesters of these operations. These requesters may be an external system, a Web application, or an intermediary. The BIAS services themselves are platform and language independent. The BIAS services may be implemented with differing technologies on multiple platforms. For example, OASIS is defining Web services bindings for the BIAS services.

Figure 2 depicts the BIAS services within an application environment. BIAS services provide basic biometric functionality as modular and independent operations which can be assembled in many different ways to perform and/or support a variety of business processes. BIAS services can be publicly exposed directly and/or utilised indirectly in support of a service-provider's own public services.

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

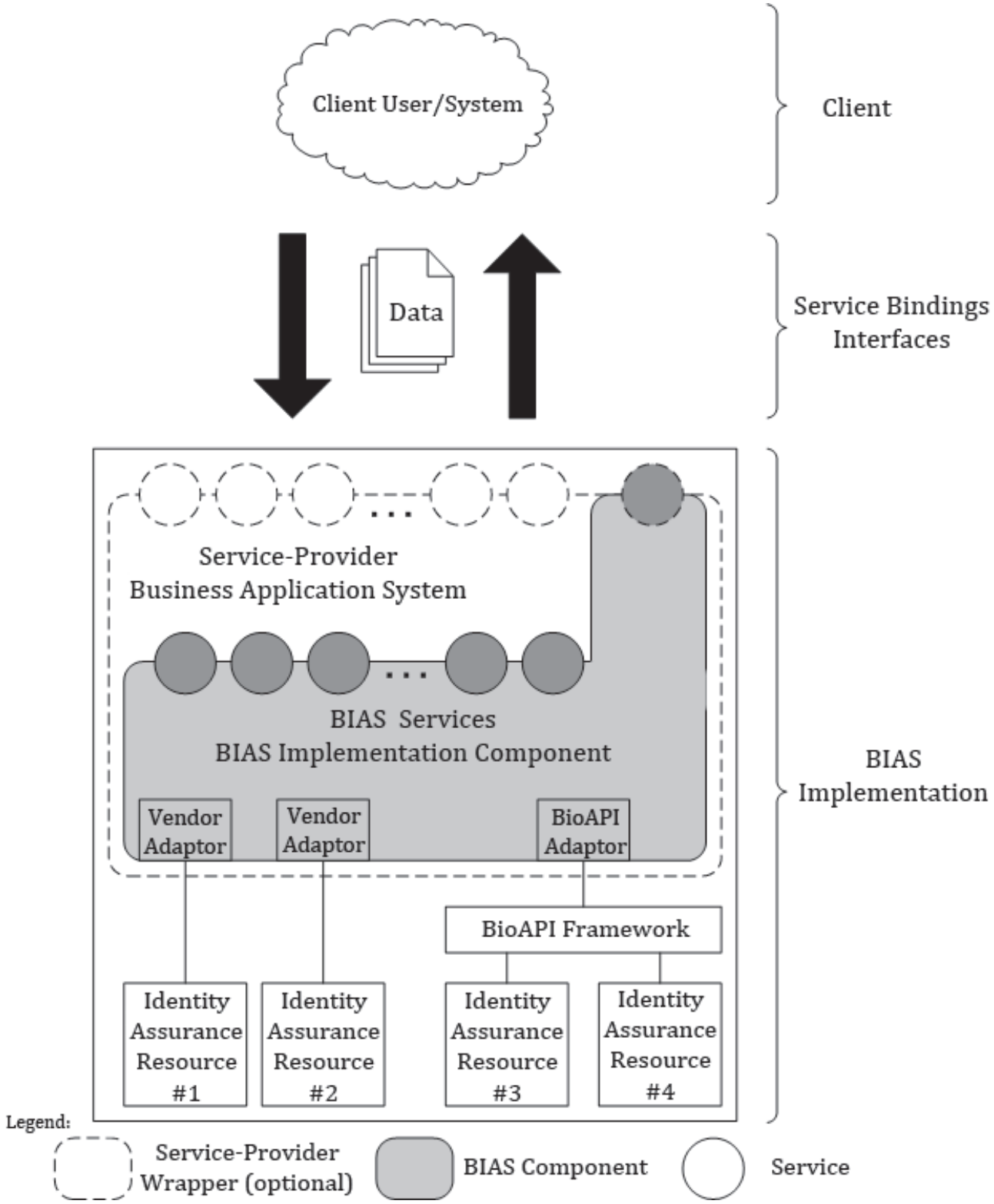

Figure 2 — BIAS application environment

6.3 Identity models

Some identity systems are person-centric and others are encounter-centric. That is, some base transactions on a unique identifier associated with an individual human being while others track

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

"biometric encounters" which may or may not be linked through such an identifier. Figure 3 provides context to further explain these concepts.

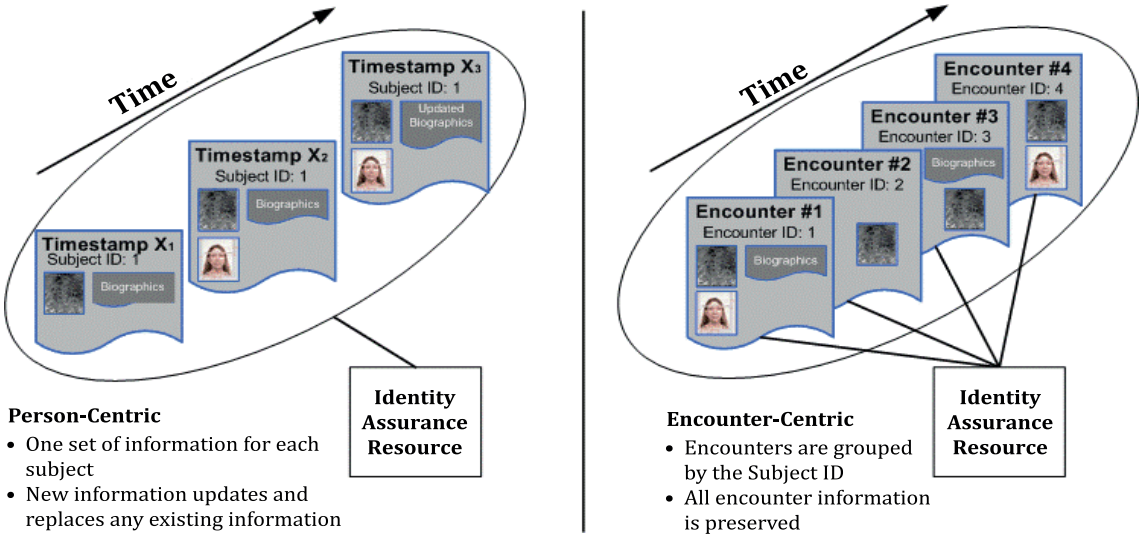

Figure 3 — Person-centric and encounter-centric views

In a person-centric model, as new data is received for a given subject, it is either added (if it does not already exist) or replaces previous data (if it already exists). For example, referring to Figure 3, if the initial enrolment contains biographic data and a set of fingerprints these are stored. If subsequently, a photo is received, it is added to the person-centric record. If later new biographic data is received (e.g. new address), it replaces the originally stored data. In this way, the "master" subject record is continuously updated to contain the most accurate, current information with (in general, but not exclusively) no need to retain historical data. This model is used, for example, in access control type systems.

An encounter-centric model, in comparison, retains all data received for every interaction with the subject. Initially, the subject record is created and populated with enrolment data (for example, fingerprint, facial photo, and biographic data as shown in Figure 3). Subsequently, if new fingerprint data is captured for that subject (during an interaction event, or encounter), a new encounter is created containing all data obtained during that encounter. The system now has two encounters for that subject. Later, in a third encounter, fingerprint and biographic data is captured and stored, in addition to the data previously stored in encounters one and two. Encounter IDs, unique to a subject, are assigned to each encounter. This model is used, for example, in case management type systems.

EXAMPLE In a border management system, a person is enroled in the system the first time they enter the country. A subject is created and biometric and biographic data are set, following any required identification operation(s). This represents the first encounter. Subsequently, when the person crosses the border in the future, their passport number is used as a claim of identity, a verification of that identity is performed, as well as any identification operations. Biometric and biographic data collected during this interaction is retained as another separately identified encounter (see Annex D for additional use cases).

Encounters can be classified as either enrolment or recognition encounters. Figure 4 depicts an example in which both biographic and biometric data are submitted during different types of encounters. Diagrams for additional scenarios are found in Annex D.

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

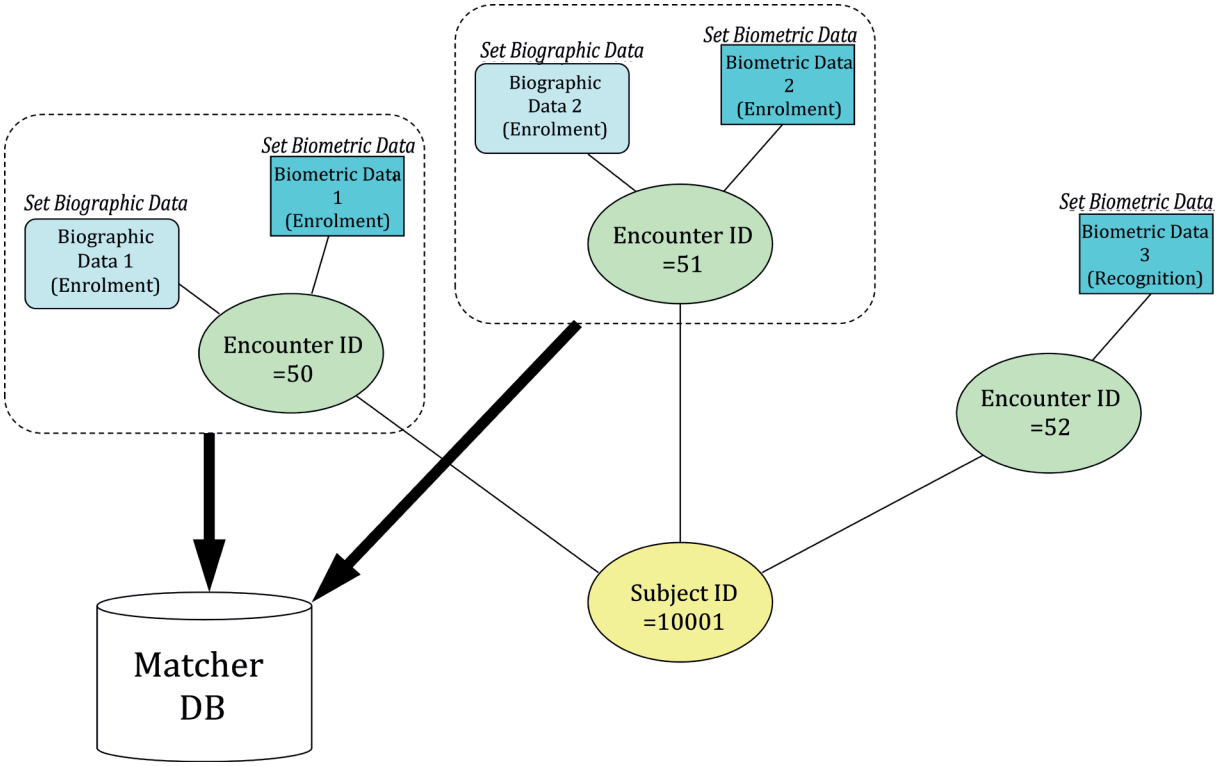

Figure 4 — Example of encounter types

NOTE Encounter type may be set using the ***Create Encounter*** operation. In addition, the Purpose field within the CBEFF header may be set to indicate this (see 8.2 for more information on biometric data).

6.4 Identity databases

Biometric systems frequently include both a master database as well as a comparison engine database. The former is used to store all identity information (including encounter information). The latter, however, usually contains a single set of biometric reference data, even within an encounter-based system and minimal, if any, biographic data. Systems use various schemes to determine which data to include within the biometric engines and when that data is updated. Figure 5 provides an example of how these databases may exist within a BIAS implementation. This is not always the case; however, as in some systems the master and comparison engine databases may be one and the same.

Within this part of ISO/IEC 30108, all services (with the exception of comparison services, such as ***IdentifySubject***) operate upon the master database unless otherwise stated, with any associated updates to the comparison engine databases (when separate) left to the policies of the BIAS service provider.

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

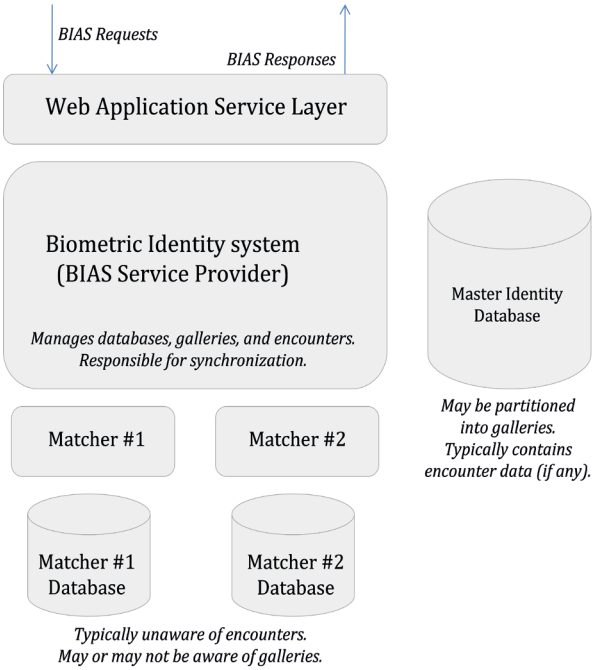

Figure 5 — Example master/engine database implementation

EXAMPLE In the previous border management example, fingerprint, face, and iris biometric data is collected on the first encounter. All information is stored in the master database. Additionally, selected fingerprint and iris data are processed into templates and stored within the appropriate comparison engine database. During the second encounter, only the data required for verification and identification is collected, and this data is stored in the master database. Templates are generated and used to perform the comparison operations. Based on service provider policy, following successful verification, it is found that the left index and ring fingerprints are of better quality than those collected during the first encounter and the engine database is updated with these fingerprints (replacing the original templates).

6.5 BIAS implementation considerations (informative)

Biometric services and the applications which use them, particularly in an identity assurance context, have unique characteristics which are summarised below:

— Some services can be performed very quickly while others (such as a 1:N identification within a large population) can take considerable time (on the order of hours) to complete. Therefore, the interface should support both synchronous and asynchronous operations;

— Biometric operations may be singular or multi-biometric.

Biometric data is in nearly all cases considered personal information and thus privacy protection is always a consideration.

— Before a biometric, biographic and/or document data transaction occurs between two different entities, the terms and conditions of the use of the data should be negotiated and made transparent. The following questions may be addressed:

  — Who will be the recipient of the data to be shared?

  — For what purpose(s) can the recipient use this data?

  — Who/what authorises this data to be shared with the recipient for this purpose?

  — How long may the recipient retain the data?

  — How must data be destroyed at the end of a retention period?

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

— May the recipient share this data with other entities? If so, with whom? For what purpose(s)? How long may the third party retain the data?

— A recipient would later have to understand what they are accepting and the terms and conditions of the agreement.

NOTE Implementers may consider implementation of a Biometric Policy (BP) and/or Biometric Practice Statement (BPS0 as defined in ISO 19092. A BP is a set of rules that specify the applicability of biometric information for use by a class of applications or community that share common security and privacy requirements. A BP may be used to control access to biometric information by an entity acting in some role or for some purpose (e.g. information sharing). A BPS describes the security and privacy practices that an organization follows during the biometric information life cycle, including business, legal, regulatory, and technical considerations for information sharing and exchange.

Security is important for any kind of SOA. As in the case of privacy protection, before a biometric, biographic and/or document data transaction occurs between two different entities, the security characteristics provided by the BIAS implementation should be known.

For the purposes of data integrity and quality assurance, a capability for creation of a chain of custody should be created to track events, changes, and transfers of data. For example, the deletion of data should be tracked and logged.

NOTE Organization management should require that formal mechanisms be used to document and report biometric system events, including system malfunctions and other security incidents, and additions, modifications, deletions, and transfers of data. Incident management results and metrics gathered from biometric systems event journals should be used in a periodic review process that causes security controls to be re-evaluated over time. An on-going, systematic approach to reviews should inform the continuous improvement of the biometric information management system over time.

Methods for service level monitoring and compliance with agreed-upon service level agreements may be critical to requesters and implementers. Terms and conditions for these capabilities may need to be negotiated.

7 Biometric Identity Assurance Services

This clause defines two categories of BIAS services, primitive and aggregate. Primitive services are lower-level operations that are used to request a specific capability. Aggregate services operate at a higher-level, performing a sequence of primitive operations in a single request. (An example of such a sequence would be a negative search where a 1:N identification which results in no matches being found is immediately followed by the addition of the biometric sample into that search population.) Implementers are not restricted to one or the other but may provide (and requesters use) a mixture of both primitive and aggregate types.

Aggregate services do not have to utilize primitive services.

7.1 BIAS interface XML schema

A goal for this BIAS Standard is to be as language and protocol independent as possible. To that end, the services are specified using a simple XML schema as defined below.

```
<?xml version = "1.0" encoding="utf-8" ?>
<xs:schema id="BIAS_Interface" xmlns:xs="http://www.w3.org/2001/XMLSchema">
   <xs:complexType name="InterfaceType">
       <xs:sequence>
          <xs:element name="parameter" type="ParameterType"
             minOccurs="0" maxOccurs="unbounded" />
       </xs:sequence>
      <xs:attribute name="name" type="xs:string" use="required" />
   </xs:complexType>
   <xs:complexType name="ParameterType">
      <xs:attribute name="name" type="xs:string" use="required" />
      <xs:attribute name="type" type="xs:string" use="required" />
      <xs:attribute name="direction" type="DirectionType" use="required" />
```


© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

```
      <xs:attribute name="use" type="UseType" use="optional"
            default="required" />
   </xs:complexType>
   <xs:simpleType name="DirectionType">
      <xs:restriction base="xs:string">
         <xs:enumeration value="in" />
         <xs:enumeration value="out" />
         <xs:enumeration value="inout" />
      </xs:restriction>
   </xs:simpleType>
   <xs:simpleType name="UseType">
      <xs:restriction base="xs:string">
         <xs:enumeration value="required" />
         <xs:enumeration value="optional" />
         <xs:enumeration value="conditional" />
      </xs:restriction>
   </xs:simpleType>
   <xs:element name="interface" type="InterfaceType"></xs:element>
</xs:schema>
```

Each service is identified by an *<interface>* tag and must include a *name* attribute. Service parameters are identified by a *<parameter>* tag and must include a *name*, *type*, and *direction* attribute. The *direction* attribute specifies whether the parameter is an input parameter (*in*), an output parameter (*out*), or an input/output parameter (*inout*). Parameters may also include a *use* attribute to indicate if the parameter is required, optional, or conditional. If the parameter is conditional, the service description must identify the conditions.

7.2 Primitive services

BIAS specifies the following set of primitive services.

7.2.1 Add Subject To Gallery

```
<interface name="AddSubjectToGallery">
   <parameter name="GalleryID" type="xs:string" direction="in" />
   <parameter name="SubjectID" type="xs:string" direction="in" />
   <parameter name="IdentityClaim"
         type="xs:string" direction="in" use="optional" />
   <parameter name="EncounterID"
         type="xs:string" direction="in" use="conditional" />
   <parameter name="Return" type="xs:unsignedLong" direction="out" />
</interface>
```

7.2.1.1 Description

The ***Add Subject To Gallery*** service shall register a subject to a given gallery or population group. As an optional parameter, the value of the claim to identity by which the subject is known to the gallery may be specified. This claim to identity shall be unique across the gallery. If no claim to identity is specified, the subject ID (assigned with the ***Create Subject*** service) shall be used as the claim to identity. Additionally, in the encounter-centric model, the encounter ID associated with the subject's biometrics that will be added to the gallery shall be specified.

NOTE In the BIAS model, the creation and management of galleries are the responsibility of the service provider implementation. Services are not exposed to the requester for this purpose.

7.2.1.2 Parameters

Gallery ID (input) – the identifier of the gallery or population group to which the subject will be added

Subject ID (input) – the identifier of the subject

Identity Claim (input, optional) – the identifier by which the subject is known to the gallery

Encounter ID (input, conditional) – the identifier of the encounter, required for encounter-centric models

Return (output) – return value indicating success or specifying a particular error condition

© ISO/IEC 2015 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

7.2.1.3 Return codes

The ***Add Subject To Gallery*** service may return any of the return codes defined in Clause 9.

7.2.2 Check Quality

```
<interface name="CheckQuality">
   <parameter name="BIR"
         type="CBEFF_BIR_Type" direction="in" use="conditional" />
   <parameter name="SubjectID"
         type="xs:string" direction="in" use="conditional" />
   <parameter name="AlgorithmVendor"
         type="xs:string" direction="inout" use="optional" />
   <parameter name="AlgorithmVendorProductID"
         type="xs:string" direction="inout" use="conditional" />
   <parameter name="Return" type="xs:unsignedLong" direction="out" />
   <parameter name="QualityScore"
         type="iso-iec19785-3-7:Quality" direction="out" />
   <parameter name="AlgorithmVersion" type="xs:string" direction="out" />
</interface>
```

7.2.2.1 Description

The ***Check Quality*** service shall return a quality score for a given biometric or a specified subject. Either a biometric sample or a subject ID shall be provided. The biometric input is provided in a CBEFF basic structure or CBEFF record, which in this part of ISO/IEC 30108 is called a CBEFF-BIR. The algorithm vendor and algorithm vendor product ID may be optionally provided in order to request a particular algorithm's use in calculating the biometric quality. If an algorithm vendor is provided, then the algorithm vendor product ID is required. If no algorithm vendor is provided, the implementing system shall provide the algorithm vendor and algorithm vendor product ID that were used to calculate the biometric quality as output parameters.

NOTE Algorithm Vendors are registered with the ISO Biometric Registration Authority and assigned unique identifiers as defined in ISO/IEC 19785-2. Algorithm Product IDs are assigned by the registered algorithm vendor.

7.2.2.2 Parameters

BIR (input, conditional) – data structure containing a single biometric sample for which a quality score is to be determined; required if no Subject ID is provided

Subject ID (input, conditional) – the identifier of the subject; required if no BIR is provided

Algorithm Vendor (input, optional / output) – the identifier of the vendor of the quality algorithm used to determine the quality

Algorithm Vendor Product ID (input, conditional / output) – the vendor assigned ID for the algorithm used to determine the quality; required as input if algorithm vendor is provided

Return (output) – return value indicating success or specifying a particular error condition

Quality Score (output) – the quality of the biometric, as defined by the Quality type in the XML Patron Format specified in ISO/IEC 19785-3

Algorithm Version (output) – the version of the algorithm used to determine the quality

7.2.2.3 Return codes

The ***Check Quality*** service may return any of the return codes defined in Clause 9.

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

7.2.3 Classify Biometric Data

```
<interface name="ClassifyBiometricData">
   <parameter name="BIR" type="CBEFF_BIR_Type" direction="in" />
   <parameter name="ClassificationAlgorithmType"
         type="xs:string" direction="inout" />
   <parameter name="Return" type="xs:unsignedLong" direction="out" />
   <parameter name="Classification" type="xs:string" direction="out" />
</interface>
```

7.2.3.1 Description

The ***Classify Biometric Data*** service shall attempt to classify a biometric sample. For example, a fingerprint biometric sample may be classified as a whorl, loop, or arch (or other classification classes and sub-classes). The types of classification algorithms and classes are not specified here, rather they are left for the implementing system to define. If no classification algorithm is input, then the BIAS service provider will make the selection.

7.2.3.2 Parameters

BIR (input) – data structure containing a single biometric sample for which the classification is to be determined

Classification Algorithm Type (input, optional / output) – identifies the type of classification algorithm to be used (input) and that was used (output) to perform the classification (e.g. for fingerprints, Henry classification)

Return (output) – return value indicating success or specifying a particular error condition

Classification (output) – the result of the classification

7.2.3.3 Return codes

The ***Classify Biometric Data*** service may return any of the return codes defined in Clause 9.

7.2.4 Create Encounter

```
<interface name="CreateEncounter">
   <parameter name="SubjectID" type="xs:string" direction="in" />
   <parameter name="EncounterType" type="EncounterCategoryType" direction="in" />
   <parameter name="EncounterID"
         type="xs:string" direction="inout" use="optional" />
   <parameter name="Return" type="xs:unsignedLong" direction="out" />
</interface>
```

7.2.4.1 Description

The ***Create Encounter*** service shall, for the specified subject, create a new encounter record and associate an encounter ID to that record. If not provided by the requester, the ***Create Encounter*** service shall generate an encounter ID that uniquely identifies the encounter within the subject record in the system.

NOTE Typically the BIAS service provider will assign the encounter ID. In the event that the requester assigns the encounter ID, it shall be used unless it duplicates an existing encounter ID in which case an error shall be returned.

The ***Create Encounter*** service is performed prior to a ***Set Biographic Data***, ***Set Biometric Data***, or ***Set Document Data*** operation.

NOTE When in encounter mode, for comparison operations, it is not necessary to explicitly create an encounter. The BIAS service provider will create the encounter and will set the encounter type to “recognition”.

7.2.4.2 Parameters

Subject ID (input) – the identifier of the subject

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

Encounter Type (input) – the category of encounter

Encounter ID (input, optional / output) – the identifier of the encounter

Return (output) – return value indicating success or specifying a particular error condition

7.2.4.3 Return Codes

The ***Create Encounter*** service may return any of the return codes defined in Clause 9.

7.2.5 Create Subject

```
<interface name="CreateSubject">
   <parameter name="Return" type="xs:unsignedLong" direction="out" />
   <parameter name="SubjectID" type="xs:string" direction="out" />
</interface>
```

7.2.5.1 Description

The ***Create Subject*** service shall create a new subject record and associate a subject ID to that record. The ***Create Subject*** service shall generate a subject ID that uniquely identifies the subject in the system.

NOTE When cross-system uniqueness is required, UUIDs should be used for Subject IDs.

7.2.5.2 Parameters

Return (output) – return value indicating success or specifying a particular error condition

Subject ID (output) – the identifier of the subject

7.2.5.3 Return codes

The ***Create Subject*** service may return any of the return codes defined in Clause 9.

7.2.6 Delete Biographic Data

```
<interface name="DeleteBiographicData">
   <parameter name="SubjectID" type="xs:string" direction="in" />
   <parameter name="GalleryID" type="xs:string" direction="in" use="optional" />
   <parameter name="EncounterID"
           type="xs:string" direction="in" use="conditional" />
   <parameter name="Return" type="xs:unsignedLong" direction="out" />
</interface>
```

7.2.6.1 Description

The ***Delete Biographic Data*** service shall erase all of the biographic data associated with a given subject record. In the encounter-centric model the service shall erase all of the biographic data associated with a given encounter, and therefore the encounter ID shall be specified. If no encounter ID is specified, or it is null, biographic data will be removed from all encounters. If a gallery is specified, biographic data will be deleted from that gallery only. When deleting data, BIAS implementations may completely erase the information in order to prevent the ability to reconstruct a record in whole or in part, or they may track and record the deleted information for auditing and/or quality control purposes.

7.2.6.2 Parameters

Subject ID (input) – the identifier of the subject

Gallery ID (input, optional) – the identifier of the gallery or population group from which the biographic information will be deleted

Encounter ID (input, conditional) – the identifier of the encounter, required for encounter-centric models

© ISO/IEC 2015 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

Return (output) – return value indicating success or specifying a particular error condition

7.2.6.3 Return codes

The ***Delete Biographic Data*** service may return any of the return codes defined in Clause 9.

7.2.7 Delete Biometric Data

```
<interface name="DeleteBiometricData">
   <parameter name="SubjectID" type="xs:string" direction="in" />
   <parameter name="GalleryID" type="xs:string" direction="in" use="optional" />
   <parameter name="EncounterID"
         type="xs:string" direction="in" use="conditional" />
   <parameter name="BiometricType"
         type="iso-iec19785-3-7:Multiple-types" direction="in" use="optional" />
   <parameter name="Return" type="xs:unsignedLong" direction="out" />
</interface>
```

7.2.7.1 Description

The ***Delete Biometric Data*** service shall remove biometric data from a given subject record. In the encounter-centric model, the encounter ID shall be specified. If no encounter ID is specified, or it is null, biometric data will be removed from all encounters. If a gallery is specified, biometric data will be deleted from that gallery only. If a biometric type(s) is specified, then only biometric data of that type shall be deleted. When deleting data, BIAS implementations may completely erase the information in order to prevent the ability to reconstruct a record in whole or in part, or they may track and record the deleted information for auditing and/or quality control purposes.

7.2.7.2 Parameters

Subject ID (input) – the identifier of the subject

Gallery ID (input, optional) – the identifier of the gallery or population group from which the biometric information will be deleted

Encounter ID (input, conditional) – the identifier of the encounter, required for encounter-centric models

Biometric Type (input, optional) – the type of biological or behavioural data to delete, as defined by the Multiple-types type in the XML Patron Format specified in ISO/IEC 19785-3

Return (output) – return value indicating success or specifying a particular error condition

7.2.7.3 Return Codes

The ***Delete Biometric Data*** service may return any of the return codes defined in Clause 9.

7.2.8 Delete Document Data

```
<interface name="DeleteDocumentData">
   <parameter name="SubjectID" type="xs:string" direction="in" />
   <parameter name="EncounterID"
         type="xs:string" direction="in" use="conditional" />
   <parameter name="DocumentCategory"
         type="xs:string" direction="in" use="optional" />
   <parameter name="Return" type="xs:unsignedLong" direction="out" />
</interface>
```

7.2.8.1 Description

The ***Delete Document Data*** service shall erase all of the document data of the specified category(ies) associated with a given subject record. In the encounter-centric model the service shall erase all of the document data associated with a given encounter, and therefore the encounter ID shall be specified. If no encounter ID is specified, or it is null, document data will be removed from all encounters. If

© ISO/IEC 2015 – All rights reserved

AVA Documents Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

no categories are specified, then all categories (for the specified encounters) shall be deleted. When deleting data, BIAS implementations may completely erase the information in order to prevent the ability to reconstruct a record in whole or in part, or they may track and record the deleted information for auditing and/or quality control purposes.

7.2.8.2 Parameters

Subject ID (input) – the identifier of the subject

Encounter ID (input, conditional) – the identifier of the encounter, required for encounter-centric models

Document Category (input, optional) – the category(ies) of the identity documents to be retrieved

Return (output) – return value indicating success or specifying a particular error condition

7.2.8.3 Return Codes

The ***Delete Document Data*** service may return any of the return codes defined in Clause 9.

7.2.9 Delete Encounter

```
<interface name="DeleteEncounter">
   <parameter name="SubjectID" type="xs:string" direction="in" />
   <parameter name="EncounterID" type="xs:string" direction="in" />
   <parameter name="Return" type="xs:unsignedLong" direction="out" />
</interface>
```

7.2.9.1 Description

The ***Delete Encounter*** service shall delete an existing encounter record from the system. When deleting an encounter, BIAS implementations may completely erase the encounter information in order to prevent the ability to reconstruct a record or records in whole or in part, or they may track and record the deleted information for auditing and/or quality control purposes.

7.2.9.2 Parameters

Subject ID (input) – the identifier of the subject

Encounter ID (input) – the identifier of the encounter

Return (output) – return value indicating success or specifying a particular error condition

7.2.9.3 Return Codes

The ***Delete Encounter*** service may return any of the return codes defined in Clause 9.

7.2.10 Delete Subject

```
<interface name="DeleteSubject">
   <parameter name="SubjectID" type="xs:string" direction="in" />
   <parameter name="Return" type="xs:unsignedLong" direction="out" />
</interface>
```

7.2.10.1 Description

The ***Delete Subject*** service shall delete an existing subject record and, in an encounter-centric model, any associated encounter information from the system. This service shall also remove the subject from any registered galleries. When deleting a subject, BIAS implementations may completely erase the subject information in order to prevent the ability to reconstruct a record or records in whole or in part, or they may track and record the deleted information for auditing and/or quality control purposes.

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

7.2.10.2 Parameters

Subject ID (input) – the identifier of the subject

Return (output) – return value indicating success or specifying a particular error condition

7.2.10.3 Return Codes

The ***Delete Subject*** service may return any of the return codes defined in Clause 9.

7.2.11 Delete Subject From Gallery

```
<interface name="DeleteSubjectFromGallery">
   <parameter name="GalleryID" type="xs:string" direction="in" />
   <parameter name="SubjectID"
         type="xs:string" direction="in" use="conditional" />
   <parameter name="IdentityClaim"
         type="xs:string" direction="in" use="conditional" />
<parameter name="Return" type="xs:unsignedLong" direction="out" />
</interface>
```

7.2.11.1 Description

The ***Delete Subject From Gallery*** service shall remove the registration of a subject from a gallery or population group. The subject shall be identified by either the subject ID or the claim to identity that was specified in the ***Add Subject To Gallery*** service.

7.2.11.2 Parameters

Gallery ID (input) – the identifier of the gallery or population group from which the subject will be deleted

Subject ID (input, conditional) – the identifier of the subject; required if an identity claim is not provided

Identity Claim (input, conditional) – the identifier by which the subject is known to the gallery; required if a subject ID is not provided

Return (output) – return value indicating success or specifying a particular error condition

7.2.11.3 Return Codes

The ***Delete Subject From Gallery*** service may return any of the return codes defined in Clause 9.

7.2.12 Get Identify Subject Results

```
<interface name="GetIdentifySubjectResults">
   <parameter name="Token" type="TokenType" direction="in" />
   <parameter name="Return" type="xs:unsignedLong" direction="out" />
   <parameter name="CandidateList" type="CandidateListType" direction="out" />
</interface>
```

7.2.12.1 Description

The ***Get Identify Subject Results*** service shall retrieve the identification results for the specified token. This service is used in conjunction with the ***Identify Subject*** service. If the ***Identify Subject*** service is implemented as an asynchronous service, the implementing system returns a token, and the ***Get Identify Subject Results*** service is used to poll for the results of the original ***Identify Subject*** request.

7.2.12.2 Parameters

Token (input) – a value used to retrieve the results of the ***Identify Subject*** request

Return (output) – return value indicating success or specifying a particular error condition

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015

Candidate List (output) – a rank-ordered list of candidates that have a likelihood of matching the input biometric sample

7.2.12.3 Return Codes

The ***Get Identify Subject Results*** service may return any of the return codes defined in Clause 9.

7.2.13 Identify Subject

```
<interface name="IdentifySubject">
   <parameter name="GalleryID" type="xs:string" direction="in" use="optional" />
   <parameter name="Gallery "
         type="CandidateListType" direction="in" use="optional" />
   <parameter name="BIR" type="CBEFF_BIR_Type" direction="in" />
   <parameter name="MaxListSize" type="xs:positiveInteger" direction="in" />
   <parameter name="Return" type="xs:unsignedLong" direction="out" />
   <parameter name="CandidateList"
         type="CandidateListType" direction="out" use="conditional" />
   <parameter name="Token"
         type="TokenType" direction="out" use="conditional" />
</interface>
```

7.2.13.1 Description

The ***Identify Subject*** service shall perform an identification search against a given gallery for a given biometric type, returning a rank-ordered candidate list of a given maximum size.

If the ***Identify Subject*** service is implemented as a synchronous service, the implementing system shall immediately process the request and return the results in the candidate list. If the ***Identify Subject*** service is implemented as an asynchronous service, the implementing system shall return a token, which is an indication that the request is being handled asynchronously. In this case, the ***Get Identify Subject Results*** service shall be used to poll for the results of the ***Identify Subject*** request.

The candidate list shall include only those candidates whose comparison score exceeds a system-defined threshold, thus indicating a likely match with the subject. In the event that there are more candidates than the requested Max List Size, the system shall determine which candidate is included in the last position in the candidate list.

NOTE When in encounter mode, for comparison operations, it is not necessary to explicitly create an encounter. The BIAS service provider will create the encounter and will set the encounter type to “recognition”.

7.2.13.2 Parameters

Gallery ID (input, optional) – the identifier of the gallery or population group which will be searched; this parameter may also be used to identify an external system where the identification request should be forwarded, if this capability is supported by the implementing system. This parameter shall not be used in conjunction with *Gallery*

Gallery (input, optional) – a list of BIRs that shall be used instead of a stored gallery. This parameter shall not be used in conjunction with *Gallery ID*

BIR (input) – data structure containing the biometric sample for the search

NOTE: When multiple samples are included as input (e.g. in a multimodal operation), a complex BIR is used.

Max List Size (input) – the maximum size of the candidate list that should be returned

Return (output) – return value indicating success or specifying a particular error condition

Candidate List (output, conditional) – a rank-ordered list of candidates that have a likelihood of matching the input biometric sample; returned with successful, synchronous request processing

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30108-1:2015