



DPC: 24/30464071 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 24 September 2024

Origin: International

Latest date for receipt of comments: 17 November 2024

Project No. 2022/02356

Responsible committee: IST/44/-/2 Biometric technical interfaces

Interested committees:

Title: Draft BS EN ISO/IEC 30108-1 BS EN ISO/IEC 30108-1 Biometrics – Identity attributes verification services. Part 1: IAVS services.

Please notify admin.start@bsigroup.com if you are aware of any keywords that might assist in clarifying or identifying the standard or of the content of this standard:

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 17 November 2024

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

E-mail: admin.start@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/ Figure/Table/Note	Type of comment	Comment (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



DRAFT International Standard

ISO/IEC DIS 30108-1

Biometrics – Identity attributes verification services —

Part 1: IAVS services

ICS: 35.240.15

ISO/IEC JTC 1/SC 37

Secretariat: **ANSI**

Voting begins on:
2024-09-24

Voting terminates on:
2024-12-17

This document is circulated as received from the committee secretariat.

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 30108-1:2024(en)

Full document details: 24/30464071 DC

© ISO/IEC 2024  **Documents**
Document Sharing Hub



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and Abbreviated Terms	2
5 Conformance	3
6 System Context	3
6.1 Service-Oriented Architectures	3
6.2 IAVS Architecture	4
6.3 Identity Models	5
6.4 Identity Databases	7
6.5 Use of encounter-based parameters	8
6.6 IAVS Implementation Considerations (Informative)	8
7 Identity Attributes Verification Services	9
7.1 General	9
7.2 IAVS Interface XML Schema	9
7.3 Primitive Services	10
7.3.1 Add Subject To Gallery	10
7.3.2 Check Quality	11
7.3.3 Classify Biometric Data	12
7.3.4 Create Encounter	13
7.3.5 Create Subject	13
7.3.6 Delete Biographic Data	14
7.3.7 Delete Biometric Data	14
7.3.8 Delete Document Data	15
7.3.9 Delete Encounter	16
7.3.10 Delete Subject	16
7.3.11 Delete Subject From Gallery	17
7.3.12 Get Identify Subject Results	17
7.3.13 Identify Subject	18
7.3.14 List Biographic Data	19
7.3.15 List Biometric Data	20
7.3.16 List Document Data	21
7.3.17 Perform Fusion	21
7.3.18 Query Capabilities	22
7.3.19 Retrieve Biographic Data	22
7.3.20 Retrieve Biometric Data	23
7.3.21 Retrieve Document Data	24
7.3.22 Set Biographic Data	25
7.3.23 Set Biometric Data	25
7.3.24 Set Document Data	26
7.3.25 Transform Biometric Data	27
7.3.26 Update Biographic Data	28
7.3.27 Update Biometric Data	28
7.3.28 Update Document Data	29
7.3.29 Verify Subject	29
7.4 Aggregated Services	30
7.4.1 Delete	30
7.4.2 Enrol	31
7.4.3 Get Deletion Results	32
7.4.4 Get Enrol Results	33

7.4.5	Get Identify Results	33
7.4.6	Get Update Results	34
7.4.7	Get Verify Results	34
7.4.8	Identify	35
7.4.9	Retrieve Data	36
7.4.10	Update	37
7.4.11	Verify	38
8	Data Elements and Data Types	39
8.1	Biographic Data	39
8.1.1	Biographic Data Type	39
8.1.2	Biographic Data Item Type	40
8.1.3	Biographic Data Set Type	40
8.1.4	Biographic Data List Type	41
8.2	Biometric Data	41
8.2.1	CBEFF BIR Type	41
8.2.2	CBEFF BIR List Type	42
8.2.3	Biometric Data Element Type	43
8.2.4	Biometric Data List Type	43
8.2.5	Candidate Lists	44
8.2.6	Candidate List Type	44
8.3	Capabilities	45
8.3.1	Capability Type	45
8.3.2	Capability List Type	50
8.4	Document Data	50
8.4.1	Document Data Type	51
8.4.2	Document Data List Type	52
8.5	Fusion Information	52
8.5.1	Fusion Information Type	52
8.5.2	Fusion Information List Type	53
8.6	Other Data Types	53
8.6.1	Encounter Category Type	53
8.6.2	Encounter List Type	53
8.6.3	Information Type	54
8.6.4	List Filter Type	54
8.6.5	Option Type	55
8.6.6	Processing Options Type	55
8.6.7	Token Type	55
9	Error Handling and Notification	56
9.1	Overview	56
9.2	Successful Service Calls	56
9.3	Error Condition Codes	56
10	Security	59
Annex A (normative) Conformance Requirements		61
Annex B (informative) Sample Biographic Data Format References		70
Annex C (informative) Example Usage Scenarios		71
Annex D (informative) Example Encounter Scenarios		77
Bibliography		80

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO [had/had not] received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee [or Project Committee] ISO/IEC JTC [or ISO/PC] JTC1, *Information Technology*, Subcommittee SC 37, *Biometrics*.

This second edition cancels and replaces the first edition (ISO/IEC 30108-1:2015), which has been technically revised.

The main changes are as follows:

- The Biometric Identity Assurance Services (BIAS) were renamed to Identity Attributes Verification Services (IAVS). This has also been applied to the title of this International Standard.
- Debugged and ratified use of the concept of encounters
- Clarified the use of encounters, and debugging of the encounter-based parameters in the services.
- Removed Fusion Identity List Type
- Re-structure the information about Capabilities
- Solved lack of definition of namespaces, in particular, related to the use of ISO/IEC 19785-3.
- Major editorial changes to remove hanging paragraphs

A list of all parts in the ISO/IEC 30108 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

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

IAVS 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 IAVS requester and implemented by a IAVS 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 aggregated services tend to be higher level and enable more flexibility on the part of the IAVS 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 international standard represents a version of IAVS subsequent to that previously standardised by INCITS and OASIS, under the name "Biometric Identity Assurance Services (BIAS)"; therefore, as this is the revision, it is denoted as Version 3.0.

Biometrics – Identity attributes verification services —

Part 1: IAVS 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 document, but is the subject of other parts of the ISO/IEC 30108 series.

Although focused on biometrics, this standard includes support for other related identity assurance mechanisms such as biographic and document capabilities. IAVS 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 standard.

Integration of biometric services as part of an authentication service or protocol is not within the scope of this standard.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 2382-37, *Information technology — Vocabulary — Part 37: Biometrics*

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*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at <https://www.iso.org/obp>
- IEC Electropedia: available at <https://www.electropedia.org/>

3.1
encounter

individual interaction within the system related to a specific subject, either for enrolment or for recognition

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

3.2
encounter-centric system

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

3.3
gallery

group of subjects, related by a common purpose, designation, or status.

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

3.4
identity assurance

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

3.5
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 (e.g., sample or feature level fusion).

3.6
person-centric model

identity model in which a single master record is maintained on a subject, 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

3.7
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.

4 Symbols and Abbreviated Terms

ABIS	Automated Biometric Identification System
AFIS	Automated Fingerprint Identification System
IAVS	Identity Attributes Verification Services
BIR	Biometric Information Record
CBEFF	Common Biometric Exchange Formats Framework
ESB	Enterprise Service Bus
FBI	Federal Bureau of Investigation
ID	Identity/Identification/Identifier
IDMS	IDentity Management System

NGI	Next Generation Identification
OASIS	Organization for the Advancement of Structured Information Standards
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
TWIC	Transport Worker Identification Card

5 Conformance

[Annex A](#) specifies the conformance requirements for systems/components claiming conformance to this standard.

6 System Context

6.1 Service-Oriented Architectures

This and the following subclauses provide an overview of Service-Oriented Architectures, the IAVS architecture, and IAVS implementation considerations.

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 (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. [Figure 1](#) shows a simple 3-tier architecture.

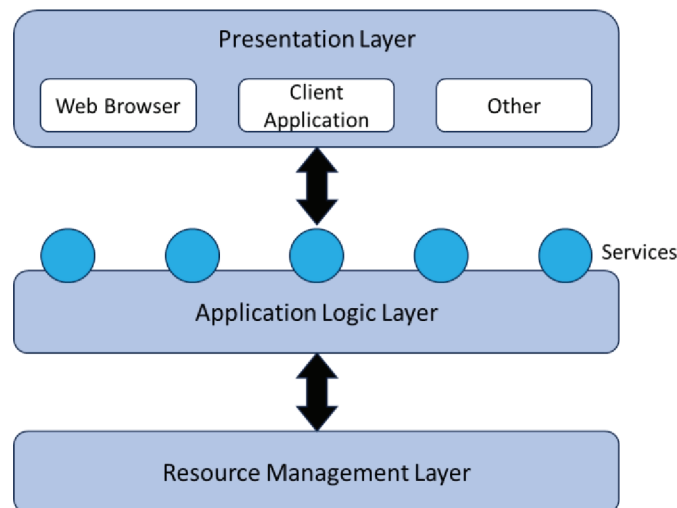


Figure 1 — Simple 3-Tier Architecture

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

Examples of - resources that are of interest include the following:

- A fingerprint verification server;

- A 1:N iris search engine;
- A facial biometric watch list;
- A criminal or civil automated biometric identification system (ABIS);
- 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 standard 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 architecture/implementation. For example, Web services bindings are defined in the OASIS BIAS Messaging Protocol, and RESTful implementation is defined in ISO/IEC 30108-2.

6.2 IAVS Architecture

The IAVS architecture consists of the following components:

- IAVS services (interface definition);
- IAVS data (schema definition);
- IAVS bindings (defined outside this standard).

The IAVS 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 IAVS services themselves are platform and language independent. The IAVS services may be implemented with differing technologies on multiple platforms.

[Figure 2](#) depicts the IAVS services within an application environment. IAVS 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. IAVS services can be publicly exposed directly and/or utilised indirectly in support of a service-provider's own public services.

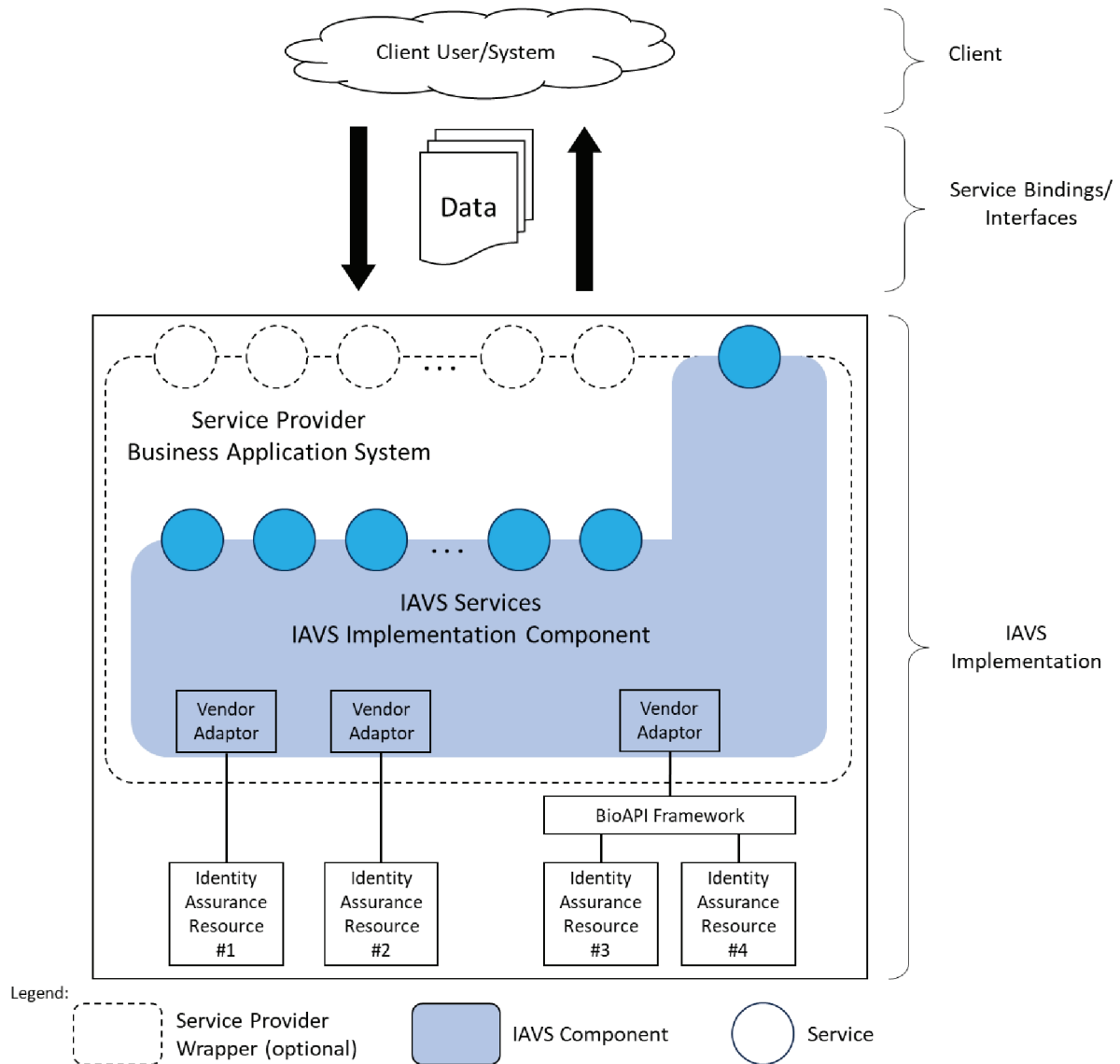


Figure 2 — IAVS Application Environment

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 “biometric encounters” which may or may not be linked through such an identifier. [Figure 3](#) provides context to further explain these concepts.

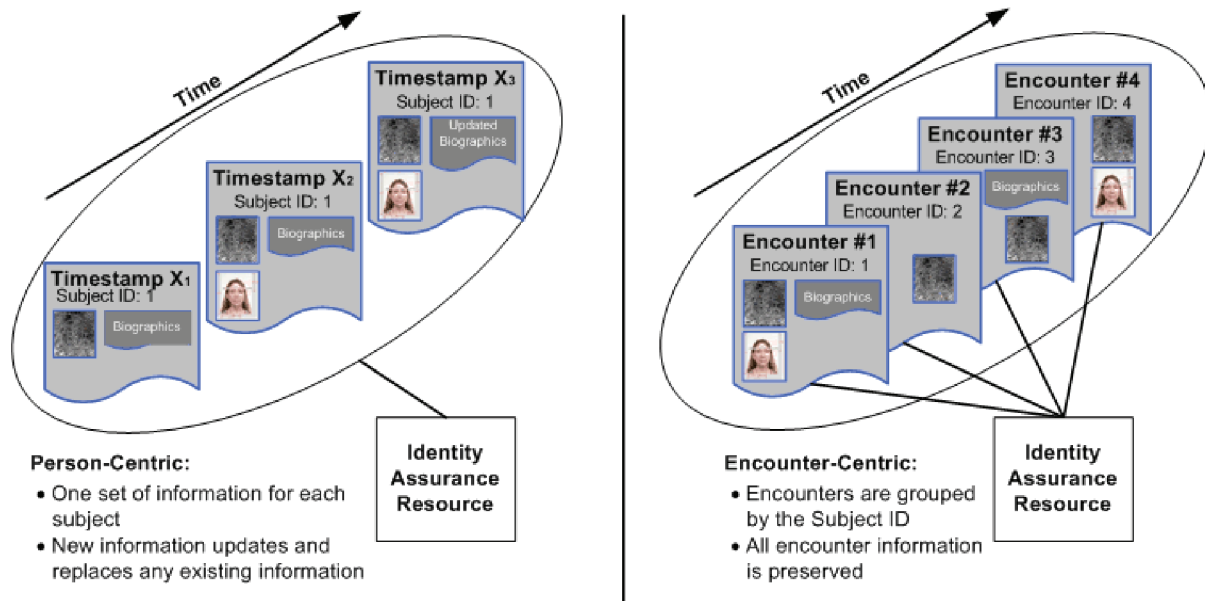


Figure 3 — Person-Centric and Encounter-Centric Views

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 entry/exit system, a person is enrolled 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](#).

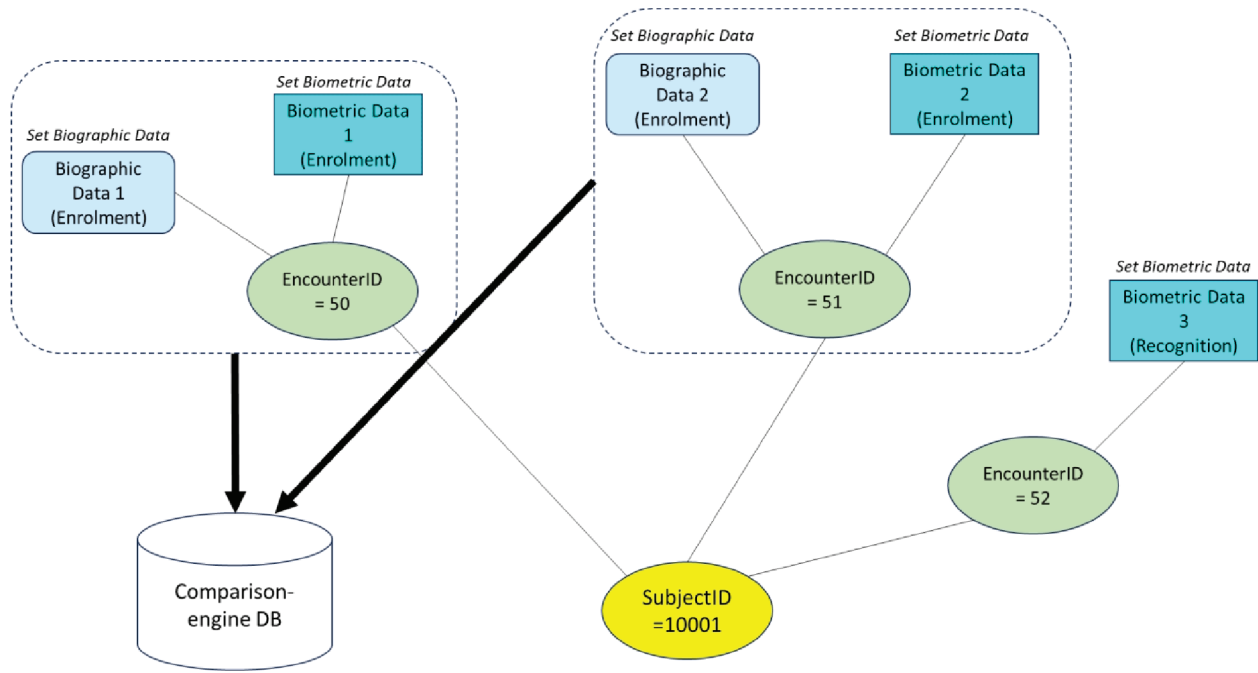


Figure 4 — Example of Encounter Types

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 IAVS 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 international standard, 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 IAVS service provider.

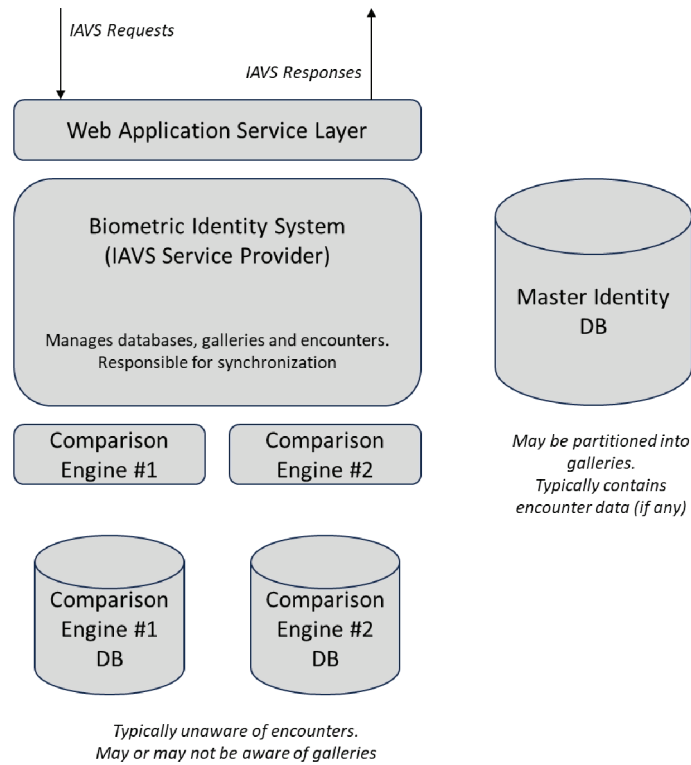


Figure 5 — Example Master/Engine Database Implementation

EXAMPLE In the previous example for a border entry/exit system, 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 Use of encounter-based parameters

6.6 IAVS 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?
- 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 can consider implementation of a Biometric Policy (BP) and/or Biometric Practice Statement (BPS) 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 can 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 IAVS 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 can 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 can be used in a periodic review process that causes security controls to be re-evaluated over time. An on-going, systematic approach to reviews can 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 Identity Attributes Verification Services

7.1 General

This clause defines two categories of IAVS services, primitive and aggregate. Primitive services are lower-level operations that are used to request a specific capability. Aggregated 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.

The intent of IAVS is to standardise the service request. System requirements and organizational business rules will determine how the service is implemented. While the description for an aggregated service may provide examples of how each one may be implemented using the primitive services defined in [clause 7.3](#), service providers are not required to utilise any of the primitive services when implementing the aggregated services.

Primitive services are specified in [clause 7.3](#), while aggregated services are specified in [clause 7.4](#).

7.2 IAVS Interface XML Schema

A goal for this IAVS 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="IAVS_Interface" xmlns:xs="https://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" />
    <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.

Whenever biometric data is used, it shall use the patron format defined in ISO/IEC 19785-3, and the namespace for that datatype is defined as:

```

<CBEFF_BIR xmlns="https://standards.iso.org/iso-iec/19785/-3/ed-3/en">
</CBEFF_BIR>

```

Within the definition of the following services, when CBEFF_BIR is used, it is expected that the declaration of the namespace is included where relevant.

7.3 Primitive Services

7.3.1 Add Subject To Gallery

7.3.1.1 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 biometric sample that will be added to the gallery shall be specified.

NOTE In the IAVS 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.

7.3.1.2 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 (see [6.5](#))
- *Return (output)* – return value indicating success or specifying a particular error condition

7.3.1.3 Return Codes

The **Add Subject To Gallery** service may return any of the return codes defined in [Section 9](#).

7.3.1.4 XML interface

```
<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>
```

7.3.2 Check Quality

7.3.2.1 Description

The **Check Quality** service shall return a quality score for a given biometric sample or for 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 standard 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.

7.3.2.2 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

7.3.2.3 Return Codes

The **Check Quality** service may return any of the return codes defined in [Section 9](#).

7.3.2.4 XML interface

```
<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="CBEFF_BIR:QualityScoreType" direction="out" />
  <parameter name="AlgorithmVersion" type="xs:string" direction="out" />
</interface>
```

7.3.3 Classify Biometric Data

7.3.3.1 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 IAVS service provider will make the selection.

7.3.3.2 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

7.3.3.3 Return Codes

The **Classify Biometric Data** service may return any of the return codes defined in [Section 9](#).

7.3.3.4 XML interface

```
<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>
```

7.3.4 Create Encounter

7.3.4.1 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 IAVS 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 IAVS service provider will create the encounter and will set the encounter type to "recognition".

7.3.4.2 Parameters

- *Subject ID (input)* – the identifier of the subject
- *Encounter Type (input)* – the category of encounter (see [6.5](#))
- *Encounter ID (input, optional / output)* – the identifier of the encounter (see [6.5](#))
- *Return (output)* – return value indicating success or specifying a particular error condition

7.3.4.3 Return Codes

The **Create Encounter** service may return any of the return codes defined in [Section 9](#).

7.3.4.4 XML interface

```
<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>
```

7.3.5 Create Subject

7.3.5.1 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.

7.3.5.2 Parameters

- *Return (output)* – return value indicating success or specifying a particular error condition
- *Subject ID (output)* – the identifier of the subject

7.3.5.3 Return Codes

The **Create Subject** service may return any of the return codes defined in [Section 9](#).

7.3.5.4 XML interface

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

7.3.6 Delete Biographic Data

7.3.6.1 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, IAVS 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.

7.3.6.2 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 (see [6.5](#))
- *Return (output)* – return value indicating success or specifying a particular error condition

7.3.6.3 Return Codes

The **Delete Biographic Data** service may return any of the return codes defined in [Section 9](#).

7.3.6.4 XML interface

```
<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>
```

7.3.7 Delete Biometric Data

7.3.7.1 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, IAVS 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.

7.3.7.2 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 (see [6.5](#))
- *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

7.3.7.3 Return Codes

The **Delete Biometric Data** service may return any of the return codes defined in [Section 9](#).

7.3.7.4 XML interface

```
<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="CBEFF_BIR:MultipleTypesType" direction="in" use="optional" />
  <parameter name="Return" type="xs:unsignedLong" direction="out" />
</interface>
```

7.3.8 Delete Document Data

7.3.8.1 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 no categories are specified, then all categories (for the specified encounters) shall be deleted. When deleting data, IAVS 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.

7.3.8.2 Parameters

- *Subject ID (input)* – the identifier of the subject
- *Encounter ID (input, conditional)* – the identifier of the encounter, required for encounter-centric models (see [6.5](#))
- *Return (output)* – return value indicating success or specifying a particular error condition

7.3.8.3 Return Codes

The **Delete Document Data** service may return any of the return codes defined in [Section 9](#).

7.3.8.4 XML interface

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

7.3.9 Delete Encounter

7.3.9.1 Description

The **Delete Encounter** service shall delete an existing encounter record from the system. When deleting an encounter, IAVS 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.

7.3.9.2 Parameters

- *Subject ID (input)* – the identifier of the subject
- *Encounter ID (input)* – the identifier of the encounter (see [6.5](#))
- *Return (output)* – return value indicating success or specifying a particular error condition

7.3.9.3 Return Codes

The **Delete Encounter** service may return any of the return codes defined in [Section 9](#).

7.3.9.4 XML interface

```
<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>
```

7.3.10 Delete Subject

7.3.10.1 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, IAVS 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.

7.3.10.2 Parameters

- *Subject ID (input)* – the identifier of the subject
- *Return (output)* – return value indicating success or specifying a particular error condition

7.3.10.3 Return Codes

The **Delete Subject** service may return any of the return codes defined in [Section 9](#).

7.3.10.4 XML interface

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

7.3.11 Delete Subject From Gallery

7.3.11.1 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.

7.3.11.2 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

7.3.11.3 Return Codes

The **Delete Subject From Gallery** service may return any of the return codes defined in [Section 9](#).

7.3.11.4 XML interface

```
<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>
```

7.3.12 Get Identify Subject Results

7.3.12.1 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.

7.3.12.2 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
- *Candidate List (output)* – a rank-ordered list of candidates that have a likelihood of matching the input biometric sample

7.3.12.3 Return Codes

The **Get Identify Subject Results** service may return any of the return codes defined in [Section 9](#).

7.3.12.4 XML interface

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

```
<parameter name="CandidateList" type="CandidateListType" direction="out" />
</interface>
```

7.3.13 Identify Subject

7.3.13.1 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 IAVS service provider will create the encounter and will set the encounter type to "recognition".

7.3.13.2 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
- *Token (output)* – a token used to retrieve the results of the **Identify Subject** request; returned with asynchronous request processing. If set to zero, operation is processed synchronously and candidate list is returned. If set to a non-zero value, operation is processed asynchronously and **Get Identify Results** must be used to retrieve the results.

7.3.13.3 Return Codes

The **Identify Subject** service may return any of the return codes defined in [Section 9](#).

NOTE Multiple scores/candidates is already built in as a score comes with a CandidateType which is a member of Candidate List.

7.3.13.4 XML interface

```
<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>

```

7.3.14 List Biographic Data

7.3.14.1 Description

The **List Biographic Data** service shall list the biographic data elements stored for a subject using the Biographic Data Elements output parameter. Note that no actual biographic data is returned by this service (see the **Retrieve Biographic Data** service to obtain the biographic data). In the encounter-centric model, an encounter ID may be specified to indicate that only the biographic data elements stored for that encounter should be returned. If an encounter ID is not specified and encounter data exists for the subject, the service shall return the list of encounter IDs which contain biographic data using the Encounter List output parameter, and the Biographic Data Elements output parameter shall be empty.

7.3.14.2 Parameters

- *Subject ID (input)* – the identifier of the subject
- *Encounter ID (input, optional)* – the identifier of the encounter (see [6.5](#))
- *Encounter Type (input, optional)* – the category of encounter (see [6.5](#))
- *Return (output)* – return value indicating success or specifying a particular error condition
- *Biographic Data Elements (output, conditional)* – a list of biographic data elements associated with a subject or encounter; non-empty if the service was successful, biographic data exists, and either (a) the person-centric model is being used or (b) the encounter-centric model is being used and an encounter identifier was specified
- *Encounter List (output, conditional)* – a list of encounter ID's associated with a subject and which contain biographic data; non-empty if the service was successful, biographic data exists, the encounter-centric model is being used, and an encounter identifier was not specified (see [6.5](#))

7.3.14.3 Return Codes

The **List Biographic Data** service may return any of the return codes defined in [Section 9](#).

7.3.14.4 XML interface

```

<interface name="ListBiographicData">
  <parameter name="SubjectID" type="xs:string" direction="in" />
  <parameter name="EncounterID"
    type="xs:string" direction="in" use="optional" />
  <parameter name="EncounterType"
    type="EncounterCategoryType" direction="in" use="optional" />
  <parameter name="Return" type="xs:unsignedLong" direction="out" />
  <parameter name="BiographicDataElements"
    type="BiographicDataType" direction="out" use="conditional" />
  <parameter name="EncounterList"
    type="EncounterListType" direction="out" use="conditional" />
</interface>

```