INTERNATIONAL STANDARD

ISO/IEC 30108-1

First edition
2015-11-01

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)

COPYRIGHT PROTECTED DOCUMENT

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

Contents

Page

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*

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.

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.

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.

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.

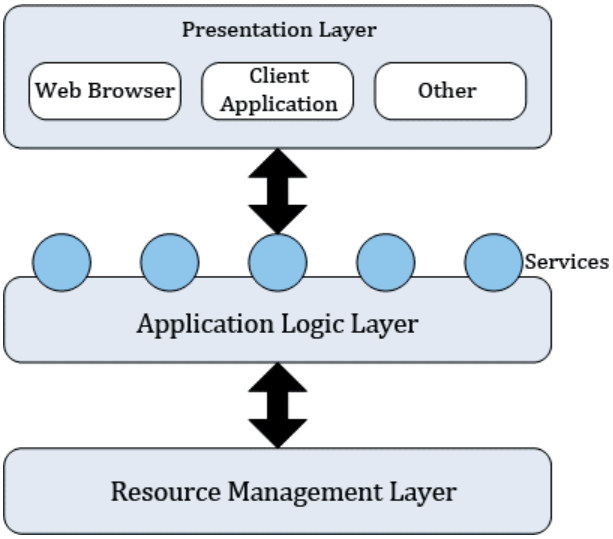

Figure 1 — Simple N-Tier architecture

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

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.

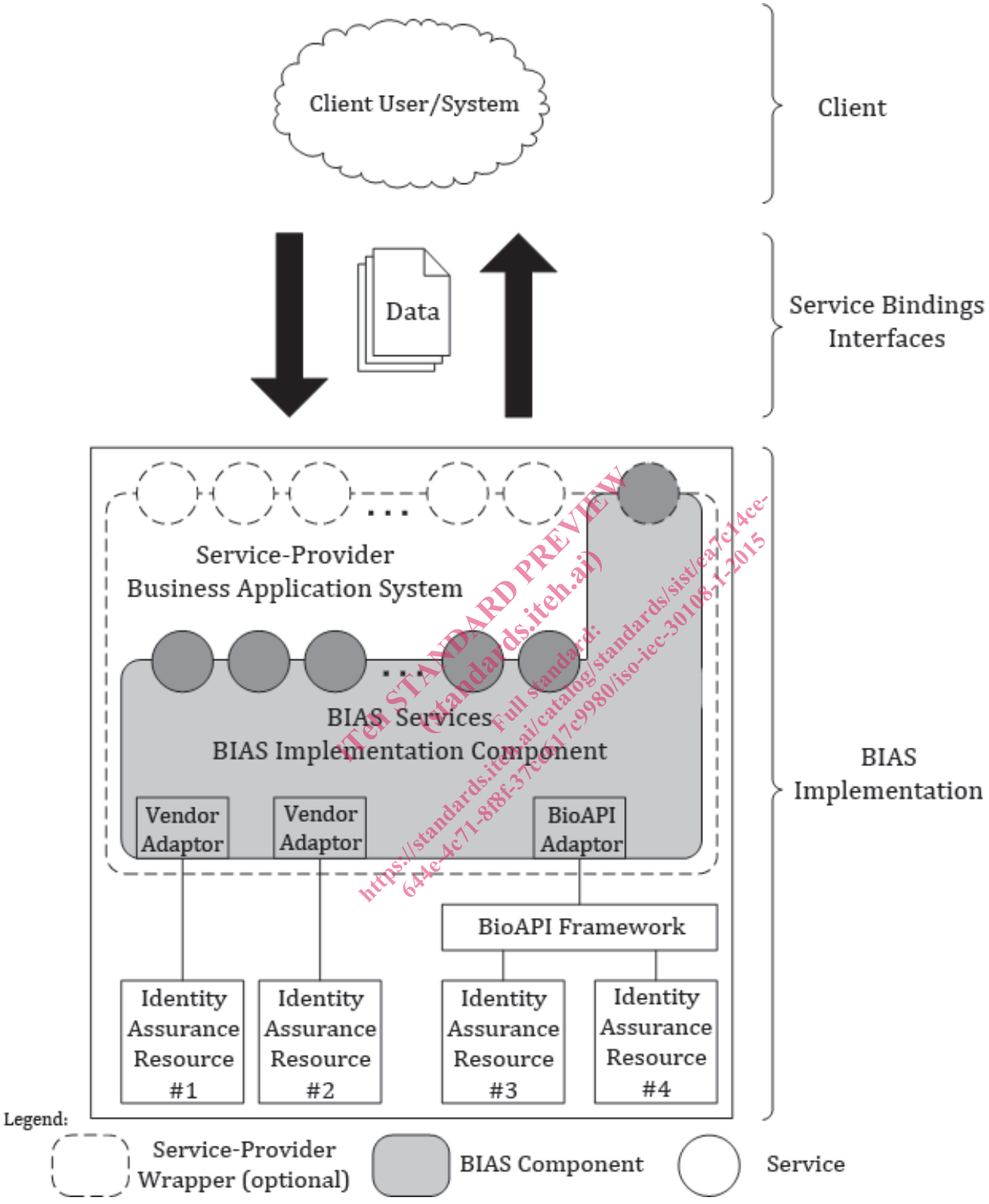

Figure 2 — BIAS application environment

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

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

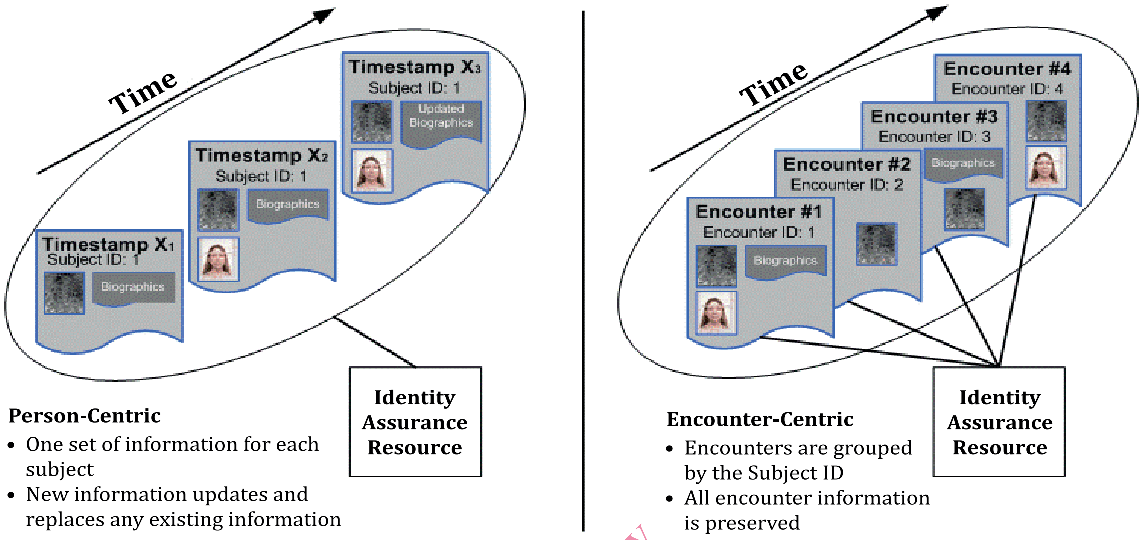

Figure 3 — Person-centric and encounter-centric views

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.

