INTERNATIONAL STANDARD

ISO/IEC 30108-2

First edition
2023-10

Biometrics — Identity attributes verification services —

Part 2: RESTful specification

Biométrique — Services de vérification des attributs d'identité —

Partie 2: Spécification RESTful

Reference number
ISO/IEC 30108-2:2023(E)

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

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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take 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 and IEC 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 and https://patents.iec.ch. ISO and IEC 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. In the IEC, see www.iec.ch/understanding-standards.

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

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

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 and www.iec.ch/national-committees.

Introduction

This document defines the architecture, operations, data elements and basic requirements for Identity Attributes Verification Services (IAVSs), thereby providing a framework for the implementation of generic identity services within a service-oriented environment. An identity in the context of IAVS comprises a subject, biographic data and biometric data. Other parts of the ISO/IEC 30108 series are intended to define specific IAVS implementations (or bindings) within specific environments, for example, Simple Object Access Protocol (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 the management, transformation and biometric comparison identity data. Services are invoked by an IAVS requester and implemented by an IAVS service provider (responder). IAVS does not prescribe the architecture or business logic of either the requester or service provider.

In IAVS 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 IAVS service provider.

In IAVS 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 person, whereas an encounter-based system retains data related to each interaction the person has with the system.

This document represents a version of IAVS defined in ISO/IEC 30108-1, but using a representational state transfer (RESTful) approach.

Biometrics — Identity attributes verification services —

Part 2: RESTful specification

1 Scope

The ISO/IEC 30108 series 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.

Although focused on biometrics, the ISO/IEC 30108 series includes support for other related identity assurance mechanisms such as biographic and document capabilities. Identity attributes verification services (IAVSs) are intended to be compatible with and used in conjunction with other biometric standards as described in ISO/IEC 30108-1.

This document implements the specification provided in ISO/IEC 30108-1 using representational state transfer (REST).

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 document.

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

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 30108-1:2015[1)], *Information technology — Biometric Identity Assurance Services — Part 1: BIAS services*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 30108-1 and ISO/IEC 2382-37 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/

1) Under revision.

4 Symbols and abbreviated terms

For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 30108-1 and the following apply.

BIR	biometric information record
BRA	ISO Biometric Registration Authority
CBEFF	Common Biometric Exchange Formats Framework (defined in ISO/IEC 19785 series)
EFTS	electronic fingerprint transmission specification
ID	identity / identification / identifier
IAVS	identity attributes verification services
JSON	JavaScript Object Notation
REST	representational state transfer
SOAP	Simple Object Access Protocol
UUID	universally unique identifier
YAML	Yet Another Markup Language[3]

5 Conformance

ISO/IEC 30108-1:2015, Annex A specifies the conformance requirements for systems/components claiming conformance to this document.

6 System context

This clause provides an overview of representational state transfer (REST), in the scope of IAVS.

The specification included in this document has been written in OpenAPI™,[2] using YAML™ (Yet Another Markup Language)[3] as the specification language. OpenAPI is an extended way to specify RESTful services, allowing a variety of tools to develop client and server applications, as well as using data in any of the data formats typically used in RESTful services, e.g. JSON (JavaScript Object Notation) or XML (eXtensible Markup Language).

A goal for this document is to be as open as possible. To that end, this specification is also available in an electronic OpenAPI file, available at https://standards.iso.org/iso-iec/30108/-2/ed-1.

The specification is written according to the following references:

— ECMA Standard ECMA-404 (2017 2nd Edition) The JSON Data Interchange Format ISO\IEC 21778

— Hyper Text Transfer Protocol (HTTP/1.1) RFC 7230 [https://httpwg.org/specs/rfc7230.html]

— Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content RFC 7231

— JSON Schema: A Media Type for Describing JSON Documents [http://json-schema.org/draft/2019-09/json-schema-core.html]

2) This trademark is provided for reasons of public interest or public safety. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC.

3) This trademark is provided for reasons of public interest or public safety. This information is given for the convenience of users of this document and does not constitute an endorsement by ISO or IEC.

— YAML Ain't Markup Language (YAML™) Version 1.2: 3rd Edition, Patched at 2009-10-01 [https://yaml.org/spec/1.2/spec.html]

All subclauses within Clause 7 entitled "REST method" (numbered 7.x.x.2) indicate the HTTP method used, among the various possibilities: GET, POST, DELETE, PUT and PATCH.

Within this document, when a YAML specification is given (e.g. all subclauses numbered 7.x.x.5), it shall be placed within an OpenAPI file, in the section indicated, taking into account the template provided in Annex A.

7 Identity assurance 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. 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 they may provide (and requesters may use) a mixture of both primitive and aggregate types.

Aggregate services do not have to utilize primitive services.

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

7.2.1 Introduction

IAVS specifies the following set of primitive services.

7.2.2 Add Subject To Gallery

7.2.2.1 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.

7.2.2.2 REST method

POST

7.2.2.3 Parameters

— *Gallery ID* — the identifier of the gallery or population group to which the subject will be added.

— *Subject ID* — the identifier of the subject.

— *Identity Claim (optional)* — the identifier by which the subject is known to the gallery.

— *Encounter ID (conditional)* — the identifier of the encounter, required for encounter-centric models.

7.2.2.4 Responses

In addition to the generic HTTP responses defined in 9.2, the execution of this service shall provide one of the responses listed in Table 1 (see 9.3 for the definitions of each error condition code).

Table 1 — Particular responses for *Add Subject To Gallery* service

HTTP status code	HTTP status code meaning	Error condition code	Description
200	OK	SUCCESS	
400	Bad Request	INVALID_IDENTITY_CLAIM	
		INVALID_SUBJECT_ID	
		INVALID_ENCOUNTER_ID	
404	Not Found	UNKNOWN_GALLERY	
		UNKNOWN_SUBJECT	
		UNKNOWN_IDENTITY_CLAIM	
		UNKNOWN_ENCOUNTER	
500	Internal Server Error	CANNOT_STORE_DATA	
		INTERNAL_DATABASE_ERROR	

7.2.2.5 YAML specification

To be placed in section #/paths:

```
/addSubjectToGallery:
    post:
      summary: Add Subject To Gallery
      parameters:
        - name: galleryID
          in: query
          required: true
          schema:
            type: string
        - name: subjectID
          in: query
          required: true
          schema:
            type: string
        - name: identityClaim
          in: query
          required: false
          schema:
            type: string
        - name: encounterID
          in: query
          required: false #conditional
          schema:
            type: string
      responses:
        200:
          $ref: '#/components/responses/success'
```

```
400:
  description: Bad Request
  content:
    application/json:
      schema:
        oneOf:
          - $ref: '#/components/schemas/invalidIdentityClaim'
          - $ref: '#/components/schemas/invalidSubjectId'
          - $ref: '#/components/schemas/invalidEncounterId'
404:
  description: Not Found
  content:
    application/json:
      schema:
        oneOf:
          - $ref: '#/components/schemas/unknownGallery'
          - $ref: '#/components/schemas/unknownSubject'
          - $ref: '#/components/schemas/unknownIdentityClaim'
          - $ref: '#/components/schemas/unknownEncounter'
500:
  description: Internal Server Error
  content:
    application/json:
      schema:
        oneOf:
          - $ref: '#/components/schemas/cannotStoreData'
          - $ref: '#/components/schemas/internalDatabaseError'
          - $ref: '#/components/schemas/unknownError'
503:
  $ref: '#/components/responses/x503'
```


7.2.3 Check Quality

7.2.3.1 Description

The *Check Quality* service shall return a quality score for a given biometric sample or a specified subject. Either a biometric sample or a subject identifier (ID) shall be provided. The biometric input is provided in a Common Biometric Exchange Formats Framework (CBEFF, as defined in ISO/IEC 19785 series) basic structure or CBEFF record, which in this document is called a CBEFF-BIR (Biometric Information Record). 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 (BRA) and assigned unique identifiers as defined in ISO/IEC 19785-2. Algorithm Product IDs are assigned by the registered algorithm vendor.

7.2.3.2 REST method

GET

7.2.3.3 Parameters

— *BIR (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 (conditional)* — the identifier of the subject; required if no BIR is provided.

— *Algorithm Vendor (optional)* — the identifier of the vendor of the quality algorithm used to determine the quality.

— *Algorithm Vendor Product ID (conditional)* — the vendor-assigned ID for the algorithm used to determine the quality; required as input if algorithm vendor is provided.

7.2.3.4 Responses

In addition to the generic HTTP responses defined in 9.2, the execution of this service shall provide one of the responses listed in Table 2 (see 9.3 for the definitions of each error condition code).

Table 2 — Particular responses for *Check Quality* service

HTTP status code	HTTP status code meaning	Error condition code	Description
200	OK	SUCCESS	Adding also — *Quality Score* — *Algorithm Version* as seen below table.
400	Bad Request	INVALID_BIR	
		INVALID_SUBJECT_ID	
		INVALID_INPUT	
		BIOMETRIC_TYPE_NOT_SUPPORTED	
		UNKNOWN_FORMAT	
403	Forbidden	BIR_DECRYPTION_FAILURE	
		BIR_QUALITY_ERROR	
		BIR_SIGNATURE_FAILURE	
404	Not Found	UNKNOWN_SUBJECT	
500	Internal Server Error	CANNOT_CHECK_QUALITY	

A successful execution of this service will provide:

— *Quality Score* — the quality of the biometric, as defined by the Quality type in one of the JSON-coded patron formats ISO/IEC 19785-3.

— *Algorithm Version* — the version of the algorithm used to determine the quality

7.2.3.5 YAML specification

To be placed in section #/paths:

```
/checkQuality:
  get:
    summary: Check Quality
    parameters:
      - name: bir
        in: query
        required: false #conditional
        schema:
          $ref: '#/components/schemas/CBEFF_BIR_Type'
      - name: subjectID
        in: query
        required: false #conditional
        schema:
          type: string
      - name: algorithmVendor
        in: query #inout
        required: false
        schema:
          type: string
```

```
    - name: algorithmVendorProductID
      in: query #inout
      required: false #conditional
      schema:
        type: string
  responses:
    200:
      description: Success. Returns quality score and algorithm version
      content:
        application/json:
          schema:
            type: object
            properties:
              qualityScore:
                type: string #RAUL: CBEFF-3 JSON
                description: >
                  The quality of the biometric, as defined by the Quality
                  type in one of the JSON-coded patron formats ISO/IEC
                  19785-3
              algorithmVersion:
                type: string
                description: >
                  The version of the algorithm used to determine the
                  quality
    400:
      description: Bad Request
      content:
        application/json:
          schema:
            oneOf:
              - $ref: '#/components/schemas/invalidBir'
              - $ref: '#/components/schemas/invalidSubjectId'
              - $ref: '#/components/schemas/invalidInput'
              - $ref: '#/components/schemas/biometricTypeNotSupported'
              - $ref: '#/components/schemas/unknownFormat'
    403:
      description: Forbidden
      content:
        application/json:
          schema:
            oneOf:
              - $ref: '#/components/schemas/birDecryptionFailure'
              - $ref: '#/components/schemas/birQualityError'
              - $ref: '#/components/schemas/birSignatureFailure'
    404:
      description: Unknown Subject
      content:
        application/json:
          schema:
            $ref: '#/components/schemas/unknownSubject'
    500:
      description: Internal Server Error
      content:
        application/json:
          schema:
            oneOf:
              - $ref: '#/components/schemas/cannotCheckQuality'
              - $ref: '#/components/schemas/unknownError'
    503:
      $ref: '#/components/responses/x503'
```


7.2.4 Classify Biometric Data

7.2.4.1 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. Instead, they

are left for the implementing system to define. If no classification algorithm is input, then the IAVS service provider will make the selection.

7.2.4.2 REST method

GET

7.2.4.3 Parameters

— *BIR* — data structure containing a single biometric sample for which the classification is to be determined.

— *Classification Algorithm Type (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).

7.2.4.4 Responses

In addition to the generic HTTP responses defined in 9.2, the execution of this service shall provide one of the responses listed in Table 3 (see 9.3 for the definitions of each error condition code).

Table 3 — Particular responses for *Classify Biometric Data* service

HTTP status code	HTTP status code meaning	Error condition code	Description
200	OK	SUCCESS	Adding also *Classification*, as seen below table.
400	Bad Request	INVALID_BIR	
		INVALID_INPUT	
		BIOMETRIC_TYPE_NOT_SUPPORTED	
		UNKNOWN_FORMAT	
403	Forbidden	BIR_DECRYPTION_FAILURE	
		BIR_QUALITY_ERROR	
		BIR_SIGNATURE_FAILURE	
500	Internal Server Error	CANNOT_PROCESS_DATA	

A successful execution of this service will provide:

— *Classification* — the result of the classification.

7.2.4.5 YAML specification

To be placed in section #/paths:

```
/classifyBiometricData:
  get:
    summary: Classify Biometric Data
    parameters:
      - name: bir
        in: query
        required: true
        schema:
          $ref: '#/components/schemas/CBEFF_BIR_Type'
      - name: classificationAlgorithmType
        in: query
        required: false
        schema:
```

