NISTIR 6529-A

# CBEFF

## Common Biometric Exchange Formats Framework

**Fernando L. Podio**
**Jeffrey S. Dunn**
**Lawrence Reinert**
**Catherine J. Tilton**
**Bruno Struif**
**Fred Herr**
**James Russell**
**M. Paul Collier**
**Mark Jerde**
**Lawrence O'Gorman**
**Brigitte Wirtz**

April 5, 2004

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

**Disclaimer:** Any mention of organizations, equipment, products, or technologies, is for information only: it does not imply NIST recommendation or endorsement, nor does it imply that the equipment, products or technologies mentioned are necessarily the best available for the purpose

NISTIR 6529-A

# Common Biometric Exchange Formats Framework (CBEFF)

**Fernando L. Podio**[1]
**Jeffrey S. Dunn**[2]
**Lawrence Reinert**[2]
**Catherine J. Tilton**[3]
**Bruno Struif**[4]
**Fred Herr**[5]
**Jim Russell**[6]
**M. Paul Collier**[5]
**Mark Jerde**[7]
**Lawrence O'Gorman**[8]
**Brigitte Wirtz**[9]

[1]*National Institute of Standards and Technology*
*Gaithersburg, MD 20899-8951*

[2]*National Security Agency*
*Ft. Meade, MD 20755*

[3] *SAFLINK Corp.*
*Bellevue, WA 98005*

[4] *Fraunhofer SIT,*

*64295 Darmstadt, Germany*

[5]*The Biometric Foundation*
*Washington, D.C. 20005*

[6]*Russell Technology*
*Stamford, CT 06902*

[7]*IDTechnology Partners*
*Gaithersburg, MD 20878*

[7] *Avaya, Inc.*
*Basking Ridge, NJ 07920*

[8]*Infineon Technologies AG*
*81541 München, Germany*

April 5 2004


**U.S. Department Of Commerce**
Donald L. Evans, Secretary

**Technology Administration**
Phillip J. Bond, Under Secretary of Commerce for Technology

**National Institute Of Standards And Technology**
Hratch Semerjian, Acting NIST Director

## Foreword

This specification, the Common Biometric Exchange Formats Framework, is an augmented and revised version of the original CBEFF, the Common Biometric Exchange File Format, published in January 2001 as NISTIR 6529. This version, NISTIR 6529-A, was developed by the CBEFF team based on the specification approved by the Biometrics Interoperability, Performance, and Assurance Working Group (NIST/BC WG) co-sponsored by NIST and the Biometric Consortium.

**Summary of Changes from the original CBEFF specification (NISTIR 6529)**

In addition to the name change, which reflects more accurately the scope of the specification, this revised version incorporates the following new features:

- **A CBEFF Nested Structure.** This structure consists of a Root Header followed by optional Sub-Headers, one or more CBEFF Basic Structures, and an optional Signature Block. A CBEFF nested structure can include: (a) standard or non-standard biometric data; (b) challenge data; and (c) payload. A nested structure has been specified in order to support multiple biometric data types (e.g., finger, face and voice) and/or multiple biometric data blocks of the same biometric type (e.g., finger biometric data blocks from more than one finger) within a CBEFF data structure. Nesting CBEFF structures accommodate such requirements and avoids having to utilize multiple consecutive CBEFF records for one specific operation.

- **A Subheader/Basic Structure Count**. The CBEFF nested structure has required defining this new field. This optional field specifies the number of nested levels below the current level in a CBEFF nested structure. This field has a value of zero in the lowest level of a nested structure.

- **The following additional and redefined fields**:

    - *A Patron Format Identifier* optional field that is used in nested structures to identify the CBEFF Patron Format of the next lower level in the structure.
    - *A Biometric Feature* optional field to further define the type of biometric data being placed in a CBEFF record.
    - *A Validity Period* optional field to denote the period (not before-not after) when the biometric data block is valid..
    - A modified definition of the *Creator field*. In this specification the Creator (optional field) specifies the organizational entity (e.g., issuer or application) responsible for the generation of the biometric data.
    - Addition of a *Product Identifier (PID) field*. This field identifies the entity (e.g., Biometric Service Provider (BSP) or transformation application) that created the biometric data object. This entity may or may not be the same as the entity which defined the format of the created data within the biometric data block.
    - *An Index field*. This optional field contains a unique value associated with a specific instance of biometric reference (enrollment) data. It may represent a database index. Uniqueness pertains only to a specific database. Use and management of this data is the responsibility of the application.
    - *A Challenge-Response field*. This optional field specifies the type of information used to present a challenge to the user or the system.
    - *A Payload field:* This optional field shall contain data (e.g. a person-identification-number) to be attached in a secure way to biometric reference data and used by a service system (e.g. access control system) in case the biometric verification is positive. Reference data is to be specified by the CBEFF Patron. Examples include a filename, database item, or URL**.**

- **Two new Formats have been added**:
    1. Biometric Information Data Objects for Use within Smart Cards or Other Tokens. This format has been defined with the collaboration of technical experts from ISO/IEC JTC 1 SC 17 WG4 and INCITS Technical Committee B10.

2. CBEFF Patron Format B, a simple root header for use in domains where more than one Patron Format, simple or nested, may be encountered.

In addition, more detailed information on the concept of CBEFF Patrons, the current list of Patrons and how to apply for a new CBEFF Patron have been added.

Other changes are:

- Several field names are changed to clarify that they describe attributes of the Biometric Data Block (BDB) rather than the CBEFF-conformant record header:
  - "Record Data Type" to "Biometric Data Type".
  - "Record Purpose" to "Biometric Purpose".
  - "Record Data Quality" to "Biometric Data Quality".
  - "Creation Date" to "Biometric Creation Date".
- Creator/PID field changed to two separate fields (as described above)
- In Biometric Type table, changed "Palm Geometry" to "Palm Print".
- In Biometric Type table, added "Foot Print".
- Discussion of OIDs has been removed.
- NIST BC/WG Patron Format A was re-specified to accommodate changes to some field definitions and to make it easier to use.
- Annex C, describing the BioAPI Biometric Identification Record, has been aligned with changes in clause 5.2 (Basic Data Structure).
- The Annex describing the X9.84 Biometric Object (based on the X9.84-2001 version) was removed. (X9.84-2001 is superceded by X9.84-2003. This version is being transposed to ISO through ISO TC68/SC2. Development of the ISO version is underway.)
- The Annex describing an example of embedding a CBEFF object has been removed. A report including examples of CBEFF utilizations is planned.

**Background**

On February 21st 1999, the Information Technology Laboratory of the National Institute of Standards and Technology (NIST) and the Biometric Consortium sponsored a Workshop to discuss the potential for reaching industry consensus on a common fingerprint template format. The participants identified the need for a "technology-blind" biometric format that would facilitate the handling of different biometric types, versions, and biometric data structures in a common way. This common format would facilitate exchange and interoperability of biometric data. (A "technology-blind biometric format would include all modalities of biometrics and would not bias, encourage, or discourage any particular vendor or biometric technology from another. It would not attempt to translate among different biometric technologies, but would identify them and facilitate their co-existence") The content of the biometric data structures (e.g., raw or processed biometric data) would not be defined in the common framework format.

The CBEFF's initial conceptual definition was achieved through a series of three Workshops co-sponsored by the National Institute of Standards and Technology and the Biometric Consortium on May 10, September 17, and December 1, 1999. A Technical Development Team, formed as a result of these Workshops, developed the original version of CBEFF (NISTIR 6529) To ensure that the biometric data structure would be in agreement with other biometric standards efforts, the development was coordinated with industrial organizations such as the BioAPI Consortium, the X9F4 Working Group, the International Biometric Industry Association, and the Interfaces Group of TeleTrusT. Harmonization of the data structures defined in the original version of CBEFF, ANSI standard X9.84 and the BioAPI specification (which was approved as an ANSI/INCITS standard in February 2002, ANSI/INCITS 358) was addressed. Participation of the International Biometric Industry Association (IBIA) as the Registration Authority for the biometric data format contained in the CBEFF structure was also addressed. The original CBEFF reflected the result of these harmonization efforts. Further CBEFF development was undertaken under the umbrella of the Biometrics Interoperability, Performance, and Assurance Working Group co-sponsored by NIST and the Biometric Consortium.

With the establishment of ISO/IEC JTC 1 SC 37, Biometrics, in 2002, there is now an international standards body focused on the field of biometrics. The United States National Body to JTC1 SC37, the InterNational Committee for Information Technology Standards (INCITS) M1 – Biometrics offered a draft version of NISTIR 6529-A as a contribution to JTC1 SC 37 for consideration as an international standard. A new project for the development of the international version of CBEFF was approved in March 2003. This international version is under development in the Technical Interfaces Working Group of JTC1 SC37. Through contributions of experts from many of the National Bodies represented in JTC1 SC37, the document under development (ISO/IEC 19785) reached Final Committee Draft (FCD) status in February 2004 and a 4-month ballot will be issued by SC37 to consider the document for the next stage as a Final Draft International Standard (FDIS).

Both biometric standards committees JTC1 SC37 and INCITS M1 are also developing a portfolio of biometric data interchange formats for a number of biometric technologies. These documents require that the biometric data record specified in these biometric data interchange standards be embedded in a CBEFF-compliant structure in the CBEFF Biometric Data Block. The international biometric data interchange standards include ISO/IEC 19785 as a normative reference and the US national standards include this specification (NISTIR 6529-A) as a normative reference.

Large organizations in the US planning to require conformance to or adopt in the near future the standard biometric data formats approved or under development in INCITS M1 also require conformance to CBEFF. Publication of NISTIR 6529-A meets these immediate needs. NISTIR 6529-A is based on the NIST/BC WG specification. Good concepts and clarifications on the content have also been adopted from the draft international version. The CBEFF team has received input from many biometrics technical experts and thanks to their contributions the specification has substantially improved. Special thanks to the National Biometric Security Project (NBSP) and The Biometric Foundation (TBF) for their editorial support and contributions during the development of this publication and to the International Biometric Industry Association (IBIA) for its role as the Registration Authority of CBEFF Format Owner identifiers. The structure of this document follows to the extent possible the format of the international version under development in JTC1 SC37.

# Contents

Page

# Common Biometric Exchange Formats Framework (CBEFF)

Fernando L. Podio[1], Jeffrey S. Dunn[2], Lawrence Reinert[2], Catherine Tilton[3], Bruno Struif[4], Fred Herr[5,] Jim Russell[6], M. Paul Collier[5], Mark Jerde[7], Lawrence O'Gorman[6], Brigitte Wirtz[9]

## Abstract

The Common Biometric Exchange Formats Framework (CBEFF) describes a set of data elements necessary to support biometric technologies in a common way. These data elements can be placed in a single file used to exchange biometric information between different system components or between systems. The result promotes interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange. This specification is a revised (and augmented) version of the original CBEFF, the Common Biometric Exchange File Format, published as NISTIR 6529. In addition to the name change, which reflects more accurately the scope of the specification, NISTIR 6529-A incorporates new features such as a CBEFF nested structure in order to support multiple biometric data types (e.g., finger, face and voice) and/or multiple biometric data blocks of the same biometric type (e.g., finger biometric data blocks from more than one finger) within a CBEFF data structure, a Biometric Feature to further define the type of biometric data being placed in the file, a Validity Period for that data, an expanded definition of the Creator field which now specifies a Product Identifier, and Index Field associated with a specific instance of biometric reference data, a Challenge-Response field and a Payload field. NISTIR 6529-A also defines two new CBEFF Formats, biometric data objects for use within smart cards and other tokens and a simple root header for use in domains where more than one Patron Format, simple or nested, may be encountered.

CBEFF provides forward compatibility accommodating for technology improvements and allows for new formats to be created. CBEFF implementations simplify integration of software and hardware provided by different vendors. CBEFF's initial conceptual definition was achieved through a series of three Workshops co-sponsored by the National Institute of Standards and Technology and the Biometric Consortium. A Technical Development Team, formed as a result of these Workshops, developed the original version of CBEFF. This version is based on the specification developed by the CBEFF team under the Biometrics Interoperability, Performance, and Assurance Working Group (NIST/BC WG) co-sponsored by NIST and the Biometric Consortium. It also embodies features recommended by many biometric experts to clarify CBEFF's purpose and functions, and to facilitate wider implementation of CBEFF compliant biometric solutions while maintaining attributes of the earlier version required by implementations that are already in conformance with CBEFF.

Key words: biometrics; biometric data format; biometric data elements; biometric data exchange; biometric technologies; data interchange; interoperability, nested structure.

1. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930
2. Identification and Authentication Research Branch, National Security Agency, Ft. Meade, MD 20755
3. SAFLINK Corp., Bellevue, WA 98005
4. Fraunhofer SIT, 64295 Darmstadt, Germany
5. The Biometric Foundation, Washington, DC 20005
6. Russel Technology, Stamford, CT 06902
7. ID Technology Partners, Gaithersburg, MD 20878
8. Avaya, Inc. Basking Ridge, NJ 07920
9. Infineon Technologies AG, 81541 München, Germany

# Introduction

The *Common Biometric Exchange Formats Framework* promotes interoperability of biometric-based application programs and systems. CBEFF defines a set of data elements for use in biometric record headers that supports the interchange of biometric data. CBEFF defines a publicly available process by which any public or private organization can formally register specified file formats using some or all of these data elements. This publication also specifies, in normative Annexes, several registered Patron formats for use where a more customized format is not required.

CBEFF defines **header fields** that can be assembled into a specific biometric data format structure and it defines the **logical content** of those fields. It defines the concept of a **"Domain of Use"** to establish the applicability of a standard or specification that meets CBEFF requirements, and a **process** by which organizations can create formats that meet these requirements. CBEFF requires these organizations to define a format and its data encoding. Adoption of CBEFF compliant Format Specifications promotes interoperability of biometric-based implementations developed by different vendors by allowing biometric data interchange via a standard mechanism.

CBEFF is not itself a specification of data format structures, although it does specify several structures in normative Annexes. By focusing on the definition of the Biometric header fields, domain-specific details such as data encoding, data and non-common elements are left to a standard or specification (see CBEFF Patrons in Clause 6) that meets CBEFF requirements. By describing a process to establish new formats, CBEFF enables biometric data to be supported in a standard manner in new technologies and systems. Clause 6 specifies instructions on how to add new CBEFF Patron formats and how to register Biometric Data Block Format Owners and Types. IBIA, the International Biometric Industry Association, is the Worldwide Registration Authority for these values. Points of contact for CBEFF and IBIA can be found in Annex F.

CBEFF does not specify the content or format of the actual biometric data contained within a CBEFF biometric data record. These biometric data structures are under development in the US through Technical Committee (INCITS M1 – Biometrics) and internationally as part of the program of work of JTC1 SC37 Biometrics Subcommittee. These draft standards require that the biometric data record specified in these standards be embedded in a CBEFF-compliant structure in the CBEFF Biometric Data Block. INCITS M1 data interchange standards include this specification (NISTIR 6529-A) as a normative reference. The international biometric data interchange standards under development in JTC 1 SC37 include ISO/IEC 19785 (the international version of CBEFF under development in JTC 1 SC37) as a normative reference.

CBEFF-compliant data structures facilitate the efficient use of the same biometric data in more than one Domain of Use. Annex E provides an example on how to utilize CBEFF across domains of use.

# Common Biometric Exchange Formats Framework

## 1 Scope

NISTIR 6529-A specifies a common set of data elements necessary to support multiple biometric technologies and to promote interoperability of biometric-based application programs and systems by allowing for biometric data exchange. These common data elements can be placed in a single file, record, or data object used to exchange biometric information between different system components and applications. This publication specifies the Biometric data elements. These elements are assembled into data structures that are defined by CBEFF Patron Format Specifications or standards. Each CBEFF-compliant Patron Format Specification defines which CBEFF data elements are present in its format and how the data elements are extracted and processed (details such as the data encoding scheme are the responsibility of the CBEFF Patrons). The Biometric data elements transported in a CBEFF structure can represent processed or unprocessed (raw) data.

CBEFF does not specify the content or format of the actual biometric data contained within a CBEFF biometric data record.

Protection of the privacy of individuals from inappropriate dissemination and use of biometric data is not in the Scope of this NISTIR.

## 2 Conformance

Conformance with this specification requires the following:

1) The use of a CBEFF-compliant Format Specification.

2) The use of the “Required” fields specified in Table 1.

3) If an “Optional” field is used, the CBEFF definition of that field is followed.

4) If nesting is used, the structure specified in *Clause 5.3 Nested CBEFF Structures* is used.

Note: Each registered CBEFF-compliant Format Specification defines a Domain of Use (the context in which a Format should be used). It is intended that there will be a limited number of Formats with a minimum of overlap in the areas (Domains) where the data is used. However, new technologies and applications may evolve that need new encoding rules and may require new Formats. This NISTIR describes a process to develop new Formats.

## 3 Normative references

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

1. ANSI/INCITS 358-2002, Information Technology – The BioAPI Specification, 13 February 2002

2. ISO/IEC 7816-4: “Organization, security and commands for interchange”

3. ISO/IEC 7816-11: “Personal verification through biometric methods”

## 4 Terms, acronyms, abbreviations and definitions

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

**4.1**
**BDB**
Biometric Data Block

**4.2**
**BER**
Basic Encoding Rules

**4.3**
**BHT**
Biometric Header Template

**4.4**
**BIT**
Biometric Information Template

**4.5**
**CBEFF**
Common Biometric Exchange Formats Framework

**4.6**
**CBEFF Basic Structure**
The basic CBEFF structure consists of a single Standard Biometric Header followed by a Biometric Data Block and an optional Signature Block

**4.7**
**CBEFF Client**
An entity that defines a biometric data block (BDB) structure (e.g., a BDB format owner) that is CBEFF compliant. This would include any vendor, standards body, working group, or industry consortium that has registered itself with IBIA and has defined one or more BDB format types.

**4.8**
**CBEFF Nested Structure**
A CBEFF Nested Structure consists of a Root Header followed by Sub-Headers, one or more CBEFF Basic Structures, and an optional Signature Block

**4.9**
**CBEFF Patron**
An organization that has defined a standard or specification incorporating biometric data objects that is CBEFF compliant

**4.10**
**CBEFF Root Header**
The CBEFF Standard Biometric Header that precedes all others in a CBEFF nested structure

**4.11**
**CBEFF Sub-Header**
Any CBEFF Standard Biometric Header in a CBEFF nested structure that follows the Root Header and precedes one or more Basic Data Structures. A CBEFF Sub-Header is not immediately followed by a Biometric Data Block.

**4.12**
**DO**
Data Object

**4.13**
**Domain of Use**
The intended usage of a format

**4.14**
**DOU**
Domain of Use

**4.15**
**MAC**
Message Authentication Code

**4.16**
**SB**
Signature Block

**4.17**
**SBH**
Standard Biometric Header

**4.18**
**TLV**
Tag-Length-Value

**4.19**
**Transforming Application**
An application that transforms a CBEFF Basic Data Structure from one Patron Format into another Patron Format. This can include processing of the content of the BDB, but need not. CBEFF defines rules for migrating the values in Standard Biometric Header fields.

# 5 CBEFF Data Structures

## 5.1 General

CBEFF provides the required information to uniquely identify the format and the originator of every biometric data substructure within a CBEFF-compliant structure. The combination of Format Owner, Format Type, Creator and the PID fields described in *Clause 5.2.1* meets this objective.

CBEFF provides the capability for CBEFF-compliant data structures to be either Basic or Nested. In order to achieve this, CBEFF describes a nested data structure that can be made as complex as the originator of the biometric data structure requires. An example of a nested structure is given in *Clause 5.3*. A nested structure could represent biometric data from the same biometric type (e.g., two finger templates) or different biometric data types (e.g., a finger template and a face template) while each substructure would uniquely identify the Format Owner/Format Type, the Creator and PID of each specific biometric data structure.

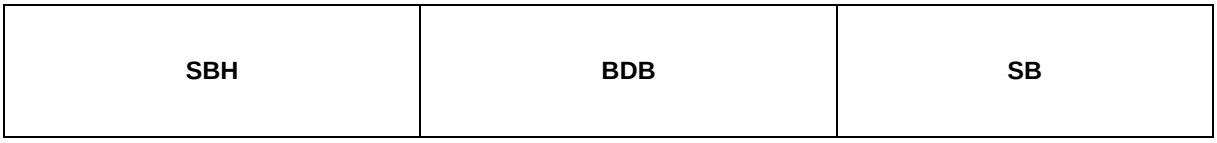
A standard biometric format that may be embedded in a CBEFF data structure is identified by the Format Owner. Upon request by this organization the CBEFF registration Authority, the International Biometric Industry Association (IBIA) in consultation with the CBEFF Technical Development Team, will assign a Format Owner value that will identify that biometric data format. IBIA provides these values to standards organizations free of charge. It is expected that the data conforming to the biometric data format specified in that standard will be used in the CBEFF Biometric Data Block (BDB).

Non-standard (proprietary) formats also need a Format Owner to be used within a CBEFF structure. This Format Owner can be directly requested from IBIA by the organization that defined that format to be used within the CBEFF BDB.

## 5.2 Basic Data Structure

In the CBEFF basic data structure, CBEFF data elements are placed in “fields” within a CBEFF record. The fields are grouped in three major sections (see Figure 1):

**Figure 1 – CBEFF Record Sections**




**SBH** – Standard Biometric Header, **BDB** – Biometric Data Block, **SB** – Signature Block.

Each section is defined in the following sub-clauses.

### 5.2.1 Standard Biometric Header (SBH)

This clause defines the required and optional fields to be used in CBEFF-compliant Formats. Definitions are specified for the fields to enable translation between Formats.

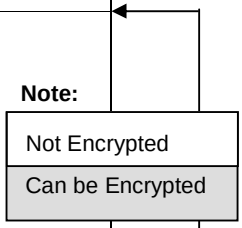
An SBH (Standard Biometric Header) specified in a CBEFF compliant Format Specification shall include the required fields illustrated in Table 1 and any necessary optional field(s). The Field name is the name given to the data element. The required or optional characteristic of the field is indicated.

Definitions and values for each of the fields in Table 1 are specified below. Values to be encoded in each field shall be specified by the CBEFF-compliant Format Specification. Format Specifications shall specify encoding for all CBEFF-defined values of any field used, even if the Format does not anticipate that a particular value will occur in its Domain of Use. Field lengths shall also be specified by the Format Specification.

The SBH shall not be encrypted, except that the Challenge/Response and Payload fields may be encrypted prior to their being encoded into the SBH. The BDB may be encrypted or not, as required by the Patron Format. If the CBEFF record has integrity applied to it, either via MAC (Message Authentication Code) or digital signature, then the SBH shall be included in the data covered by the MAC or signature.

**Table 1 - Standard Biometric Header Fields (Followed by the BDB and the SB)**

| Field Name | Required or Optional | Notes<br>**(Field lengths and encoding are to be specified by the Patron Format Specification.)**<br>**(Fields that CBEFF permits to be encrypted are indicated by shading and notes in this table.)** |
|---|---|---|
| SBH Security Options | Required | This field specifies the security applied to the record:<br>• No-Privacy: BDB is plaintext (not encrypted)<br>• Privacy-Only: BDB is encrypted<br>• Integrity-Only: (Record is Signed or MACed)<br>• Privacy-And-Integrity (BDB is encrypted and record is Signed or MACed)<br>Note: Encryption, signature and MAC algorithms are to be specified by the Patron Format Specification. |
| Integrity Options | Required if *SBH Security Options* = "Integrity-Only" or "Privacy-and-Integrity" | This field specifies which integrity attribute is applied to the record if Integrity is used:<br>• MACed<br>• Signed |
| CBEFF Header Version | Optional | CBEFF version to which the record conforms:<br>• Major = "01"<br>• Minor = "01" |
| Patron Header Version | Optional | Patron Format Specification or Standard version. |
| Biometric Type | Optional | Biometric type (e.g., fingerprint, voice, etc.). |
| Biometric Subtype | Optional | Additional specification within a biometric type. |
| Biometric Data Type | Optional | Level of processing applied to this data (e.g., raw, processed, etc.). |
| Biometric Purpose | Optional | Intended use of the data (e.g., enrolment, verification, etc.). |
| Biometric Data Quality | Optional | Quality of the biometric data. |
| Biometric Creation Date | Optional | Creation date and time of the biometric data. |
| Validity Period | Optional | Valid-From and Valid-Until Dates for this record. |
| Creator | Optional | Text identifier of the application's owner. |
| Index | Optional | Unique identifier for the biometric reference data within the record's application space. |
| Challenge/Response | Optional | Information used to present a challenge to a user or system within the record's application space. May be encrypted. |
| Payload | Optional | Arbitrary data stored in the SBH for convenient association with the biometric information. May be encrypted. |
| Subheader/Basic Structure Count | Optional | Number of CBEFF Structures in the level below this header's level in a CBEFF nested structure. |
| BDB Format Owner | Required | ID of the Group or Vendor which defined the BDB. |
| BDB Format Type | Required | BDB Format Type as specified by the Format Owner. |
| Product Identifier (PID) | Optional | Unique (registered) identifier of the entity that created the biometric data. |
| Patron Format Identifier | Optional | Unique (registered) identifier of the patron format of the next lower nested level. |
| Biometric Data Block (BDB) | Required | Defined by the Format Owner. May be encrypted. |
| Signature | Required if *SBH Security Options* = "Integrity-Only" or "Privacy-and-Integrity" | Signature or MAC. Only present if the SBH Security Options value is "Integrity-Only" or "Privacy-and-Integrity". |



#### 5.2.1.1 SBH Security Options

This field is required in all CBEFF compliant Format Specifications. This field specifies whether the BDB is encrypted (Privacy) and whether the entire CBEFF record is integrity-protected as shown in Table 2. If integrity is applied, either with or without Privacy, then the Integrity Options field (see next sub-clause) is required. Algorithms to be used for MAC, signature and encryption shall be specified by the Format Specification.

**Table 2 - SBH Security Options**

| **Field Value Names**: Definitions |
|---|
| **No-Privacy**: the BDB is not encrypted |
| **Privacy-Only**: the BDB is encrypted and the entire record does not have integrity applied to it |
| **Integrity-Only**: the BDB is not encrypted and the entire record has integrity applied to it (MAC or signature) |
| **Integrity-and-Privacy**: the BDB is encrypted and the entire record has integrity applied to it (MAC or signature) |

When transforming a CBEFF record from an initial Format to a target Format, the value of this field in the target record shall conform to the security options applied to the target CBEFF record, regardless of the security options of the initial CBEFF record.

#### 5.2.1.2 Integrity Options

This field is required in CBEFF records that use Integrity, as specified in the SBH Security Options field. This field specifies whether Integrity uses a Signature or Message Authentication Code (MAC). The Integrity options defined in this document are shown in Table 3.

**Table 3 - Integrity Options**

| **Field Value Names**: Definitions |
|---|
| **MACed**: the record's integrity is protected via Message Authentication Code |
| **Signed**: the record's integrity is protected via signature |

When transforming a CBEFF record from an initial Format to a target Format, the value of this field in the target CBEFF record shall conform to the security options applied to the target CBEFF record, regardless of the security options of the initial CBEFF record. If the target CBEFF record does not have the Integrity option, then this field shall not be present.

#### 5.2.1.3 CBEFF Header Version

Optional. A representation of the CBEFF Version. This specification has the following value:

- Major = "01"
- Minor = "01"

#### 5.2.1.4 Patron Header Version

Required. Format specifications or standards can define this field as having only a major component or a major and a minor component.

NOTE In order to decode CBEFF data, implementations shall have knowledge of all of the Patron Format Specifications within the Domain of Use and the data encoding schemes used.

When transforming a CBEFF record from an initial Format to a target Format, the value of this field in the target CBEFF record shall reflect the version of the target Format Specification.

#### 5.2.1.5 Biometric Type

Optional. This field defines the type of biometric technology. If used, the Format Specification shall specify this field as a matrix to allow for multiple types in a single record. Values available in the matrix shall include “Multiple-Biometrics-Used” and “No-Information-Given”.

Table 4 specifies a set of values for Biometric Type. This Table is not a normative requirement of this specification. Where it is a requirement of one or more Domains of Use (DOU) that *any* biometric mode be supported, this Table can be referenced by those DOUs to insure their Biometric Type values are compatible.

Where a DOU requires support of only a small number of biometric modes, if the Patron Format specifies the Biometric Type field by reference to Table 4, the resulting 24 bit field may cause inefficiency in implementation. Patron Formats have the option to specify a set of Biometric Type values that is optimally specified to their DOUs.

**Table 4 – Biometric Type**

| Field Value Name | Biometric Type Value (hex) |
|---|---|
| No Information Given | ‘000000’ |
| Multiple Biometrics Used | '000001' |
| Facial Features | '000002' |
| Voice | '000004' |
| Fingerprint | '000008' |
| Iris | '000010'' |
| Retina | '000020' |
| Hand Geometry | '000040' |
| Signature Dynamics | '000080' |
| Keystroke Dynamics | '000100' |
| Lip Movement | '000200' |
| Thermal Face Image | '000400' |
| Thermal Hand Image | '000800' |
| Gait | '001000' |
| Body Odor | '002000' |
| DNA | '004000' |
| Ear Shape | '008000' |
| Finger Geometry | '010000' |
| Palm Print | '020000' |
| Vein Pattern | '040000' |
| Foot Print | ‘080000’ |

Table 5 is an example of the binary representation of a biometric type value from Table 4 presented in a three byte data field:

**Table 5 – Example of Biometric Type**

| b8 b7 b6 b5 b4 b3 b2 b1 | b8 b7 b6 b5 b4 b3 b2 b1 | b8 b7 b6 b5 b4 b3 b2 b1 | Biometric Type |
|---|---|---|---|
| 0 0 0 0 0 0 0 0 | 0 0 0 0 0 0 0 0 | 0 1 0 0 0 0 0 0 | Hand Geometry |

When transforming a CBEFF record from an initial Format to a target Format, the value of this field in the target CBEFF record shall be the same as the value in the initial CBEFF record if the initial CBEFF record includes this field. If the initial CBEFF record does not include this field then the value of this field in the target CBEFF record shall be "No-Information-Given" if the field exists in the target CBEFF record. It is not a CBEFF requirement that the Biometric Type field in the target Format be the same length as that in the initial Format.

#### 5.2.1.6 Biometric Subtype

Optional. This field more specifically defines the type of biometric data in the CBEFF record. In a nested CBEFF structure this field shall only appear in the lowest level. If the Format Specification requires this field it shall define a value to represent "No-Information-Given" in addition to the other values.

Table 6 specifies a set of values for Biometric Subtype. This Table is not a normative part of this specification. Where it is a requirement of one or more Domains of Use that any of these biometric subtypes be supported, this Table can be referenced by those DOUs to insure their Biometric Subtype values are compatible.

Where a DOU requires support of only a small number of biometric subtypes, if the Patron Format specifies the Biometric Subtype field by reference to Table 6, the resulting 8 bit field may cause inefficiency in implementation. Patron Formats have the option to specify a set of Biometric Subtype values that is optimally tuned to their DOUs.

**Table 6 - Biometric Subtype**

| b8 b7 b6 b5 b4 b3 b2 b1 | Biometric Subtype |
|---|---|
| 0 0 0 0 0 0 0 0 | No information given |
| 0 1 | Right |
| 1 0 | Left |
| 0 0 0 | No meaning |
| 0 0 1 | Thumb |
| 0 1 0 | Pointer finger |
| 0 1 1 | Middle finger |
| 1 0 0 | Ring finger |
| 1 0 1 | Little finger |
| x x x | Reserved for future use |

When transforming a CBEFF record from an initial Format to a target Format, the value of this field in the target CBEFF record shall be the same as the value in the initial CBEFF record if the initial CBEFF record includes this field. If the initial CBEFF record does not include this field then the value of this field in the target CBEFF record shall be "No-Information-Given" if the field exists in the target CBEFF record. It is not a CBEFF requirement that the Biometric Subtype field in the target Format be the same length as that in the initial Format.

#### 5.2.1.7 Biometric Data Type

Optional. This field specifies the processed state of the data encoded in the BDB. The defined data types are shown in Table 7. The default value of this field is "Processed".

**Table 7 – Biometric Data Type**

| Field Value Names |
|---|
| **Raw**: the data in the BDB is in its raw form as delivered by the sensor |
| **Intermediate**: the data in the BDB has been processed from the form delivered by the sensor, but is not in a form usable for matching |
| **Processed**: the data in the BDB is in a form that can be used for matching |

When transforming a CBEFF record from an initial Format to a target Format, the value of this field in the target CBEFF record shall convey the type of the target BDB if the Transforming Application has processed the BDB into a different type. If the Transforming Application has not done such processing, the value in the target CBEFF record shall be the same as in the initial CBEFF record, unless the field does not exist in the initial CBEFF record, in which case the target value shall be “No-Information-Given”.

#### 5.2.1.8 Biometric Purpose

Optional. This field specifies the intended use of the data. The defined values are shown in Table 8. A Format Specification may specify one value as the default.

**Table 8 – Biometric Purpose**

| Field Value Names |
|---|
| **Verify** |
| **Identify** |
| **Enroll** |
| **Enroll for Verification Only** |
| **Enroll for Identification Only** |
| **Audit** |

When transforming a CBEFF record from an initial Format to a target Format, the value of this field in the target CBEFF record shall convey the purpose of the target BDB if the Transforming Application has processed the BDB into a different purpose. If the Transforming Application has not done such processing, the value in the target CBEFF record shall be the same as in the initial CBEFF record, unless the field does not exist in the initial CBEFF record, in which case the target value shall be “No-Information-Given”.

#### 5.2.1.9 Biometric Data Quality

Optional. This field specifies the quality of the data in the BDB.

**Table 9 – Record Data Quality**

| Field Value Names |
|---|
| **Quality not supported by SBH creator** |
| **Quality supported but not set** |
| **Quality value within range 0 through 100 where 100 is the highest quality (*see ANSI INCITS 358, the BioAPI specification*)** |

When transforming a CBEFF record from an initial Format to a target Format, the value of this field in the target CBEFF record shall be the same as the value in the initial CBEFF record if the initial CBEFF record includes this field. If the initial CBEFF record does not include this field then the value of this field in the target CBEFF record shall be “No-Information-Given” if the field exists in the target CBEFF record.

#### 5.2.1.10 Biometric Creation Date

Optional. This field specifies the date and time that the biometric data was taken. The Creation Date is expressed in the following format: YYYYMMDDhhmmssZ (Z denotes Coordinated Universal Time, which is abreviated UTC). For example, December 15, 2000 at 5 AM, 35 minutes and 30 seconds is expressed as 20001215053530Z.

When transforming a CBEFF record from an initial Format to a target Format, the value of this field in the target CBEFF record shall be the same as the value in the initial CBEFF record if the initial CBEFF record includes this field. If the initial CBEFF record does not include this field then the value of this field in the target CBEFF record shall be “No-Information-Given” if the field exists in the target CBEFF record.

#### 5.2.1.11 Validity Period

Optional. This field specifies the period (not-before through not-after) when the biometric data block is valid. The Validity Period is expressed in the following format: YYYYMMDDhhmmssZYYYYMMDDhhmmssZ. (See 5.2.1.10). When transforming a CBEFF record from an initial Format to a target Format, the value of this field in the target CBEFF record shall convey the Validity Period applicable to the target Domain of Use. The Validity Period of the initial CBEFF record may or may not be relevant to that of the target CBEFF record.

#### 5.2.1.12 Creator

Optional. This field is a text string that identifies the organization that is responsible for the application that created the CBEFF record. For example, biometric data in machine readable travel documents might be created by “US Dept of State” or “Passport Australia”.

#### 5.2.1.13 Index

Optional. This field contains a value associated with the BDB that is unique within this CBEFF record’s application space. It may represent a database index. Uniqueness pertains only to a specific database. Use and management of this data is the responsibility of the implementation. Use within a nested structure is addressed in *Clause 5.3 Nested CBEFF Structures*.

When transforming a CBEFF record from an initial Format to a target Format, the value of this field shall correspond to the situation of the target Domain of Use. The value of the Index field in the initial CBEFF record may or may not be relevant to that of the target CBEFF record.

#### 5.2.1.14 Challenge-Response

Optional. This field specifies the information used to present a challenge to the user or the system within this CBEFF record’s application space. Examples include user prompt text or a pointer to a database that contains challenge-response data.

When transforming a CBEFF record from an initial Format to a target Format, the value of this field shall correspond to the situation of the target Domain of Use. The Challenge-Response value in the initial CBEFF record may or may not be relevant to that of the target CBEFF record.

#### 5.2.1.15 Payload

Optional. This field contains arbitrary data stored in the SBH for convenient association with the biometric information. It could contain data (e.g. a person-identification-number) attached in a secure way to the BDB and used by a service system (e.g. access control system) in case that the biometric verification is positive.

When transforming a CBEFF record from an initial Format to a target Format, the value of this field in the target CBEFF record shall be the same as the value in the initial CBEFF record if the initial CBEFF record includes this field. If the initial CBEFF record does not include this field then the value of this field in the target CBEFF record shall be "No-Information-Given" if the field exists in the target CBEFF record. This is because the Payload is defined as data that is captured at Enrolment time.

#### 5.2.1.16 Subheader/Basic Structure Count

This field is used only in CBEFF nested structures (see *Clause 5.3 Nested CBEFF Structures; see also Annex B*). It specifies the number of Basic Data Structures in the next level below the current Sub-Header or Root Header. In the lowest level of a structure the value of this field shall be "zero".

#### 5.2.1.17 BDB Format Owner/Type

In a CBEFF structure the BDB Format Owner and Format Type, when used in combination, uniquely identify the specific format of the BDB content. The format and content of the BDB is "owned" by the CBEFF Client (see *Clause 6.1*). This BDB format definition may be published (public) or unpublished (non-public).

When transforming a CBEFF record from an initial Format to a target Format, the values of these fields shall identify the target BDB format.

**(1) Case where the format of the biometric data block is standard**

In this case, the Format Owner identifies the standards organization that developed the specific BDB format. IBIA will provide this value to the standards organization, free of charge. The Format Type then identifies the standard BDB format as specified by the Format Owner.

**(2) Case where the format of the biometric data block is proprietary**

In this case, the entity that defines the BDB format is not a standards body, but an independent company or organization, which must register itself as a Format Owner with IBIA. Registration of the Format Type(s) is recommended but not required.

##### 5.2.1.17.1 BDB Format Owner

Required. This field denotes the Vendor, Standards Body, Working Group, or Industry Consortium that has defined the format of the Biometric Data (in the BDB). A CBEFF requirement, as described in this Standard, is that Format Owners register with IBIA for an assigned identifier of the Format Owner. The number is guaranteed to be unique. Refer to *Clause*

*6. CBEFF Patrons* and Clients for Registration information.

##### 5.2.1.17.2 BDB Format Type

Required. This field value is assigned by the Format Owner and represents the specific BDB Format as specified by the Format Owner. This may be a non-standard, unpublished data format or a data format that has been standardized by an industry group, consortium, or standards body. The registration of the Format Type value is recommended but not required. Refer to *Clause*

*6. CBEFF Patrons and* Clients for information about registration.

Note: It is the combined CBEFF Format Owner/Format Type value that uniquely identifies the BDB format.

#### 5.2.1.18 Product Identifier (PID)

Optional. This field identifies the product (e.g., the Biometric Service Provider (BSP) or Transforming Application) that created or transformed the biometric data object. This field uses the same format and registration method as the Format Owner/Type element.

The PID consists of two parts – the Product Owner and the Product Type, analogous to the Format Owner and the Format Type.

The Product Owner may or may not be the same entity as the Format Owner. If they are the same, the Product Owner and Format Owner are the same value and need not be registered separately, but a request must be made by the Product Owner that IBIA insert the PID value in the PID table. The Product Owner is permitted to assign the same value to the Product Type as has been assigned to a Format Type when, for example, the Product and BDB Format are tightly coupled.

If the Product Owner has not registered as a Format Owner, IBIA will assign a Product Owner value to be used within the PID field.

When an entity transforms a CBEFF record from an initial Format to a target Format, the value of this field in the target CBEFF record shall identify the Transforming Application if it has modified the data in the BDB in any way other than by decrypting it and/or re-encrypting it.

#### 5.2.1.19 Patron Format Identifier

Optional. This field identifies the patron format of the next lower level in a nested CBEFF data structure. This field uses the same format and registration method as the Format Owner/Type element.

The Patron Format Identifier consists of two parts – the Patron Format Owner and the Patron Format Type, analogous to the Format Owner and the Format Type.

Note It is possible to have more than one patron format in a single branch of a nested structure. In such a case, the patron format identifier shall apply to lower levels until a level is encountered where a different patron format identifier is encoded. This second identifier shall apply to lower levels until yet another identifier is encoded, and so forth.

### 5.2.2 The Biometric Data Block (BDB)

This block contains the biometric data. It is simply a block of memory that is specified by the owner of the type as specified in the **BDB Format Owner/Type** field of the SBH. Therefore, this can be a non-standard format or one data format developed or adopted by a Standards Body, Working Group, or Industry Consortium.

The Vendor, Standards Body, Working Group, or Industry Consortium can specify that this field contains only a biometric template, or it can specify a structure for the data with further parameters, information, and data**.**

The Patron Format Specification can require that the BDB be encrypted (using encryption techniques specified by the Patron Format Specification), that it not be encrypted, or that encryption of the BDB is optional under the Patron Format Specification.

### 5.2.3 Signature Block

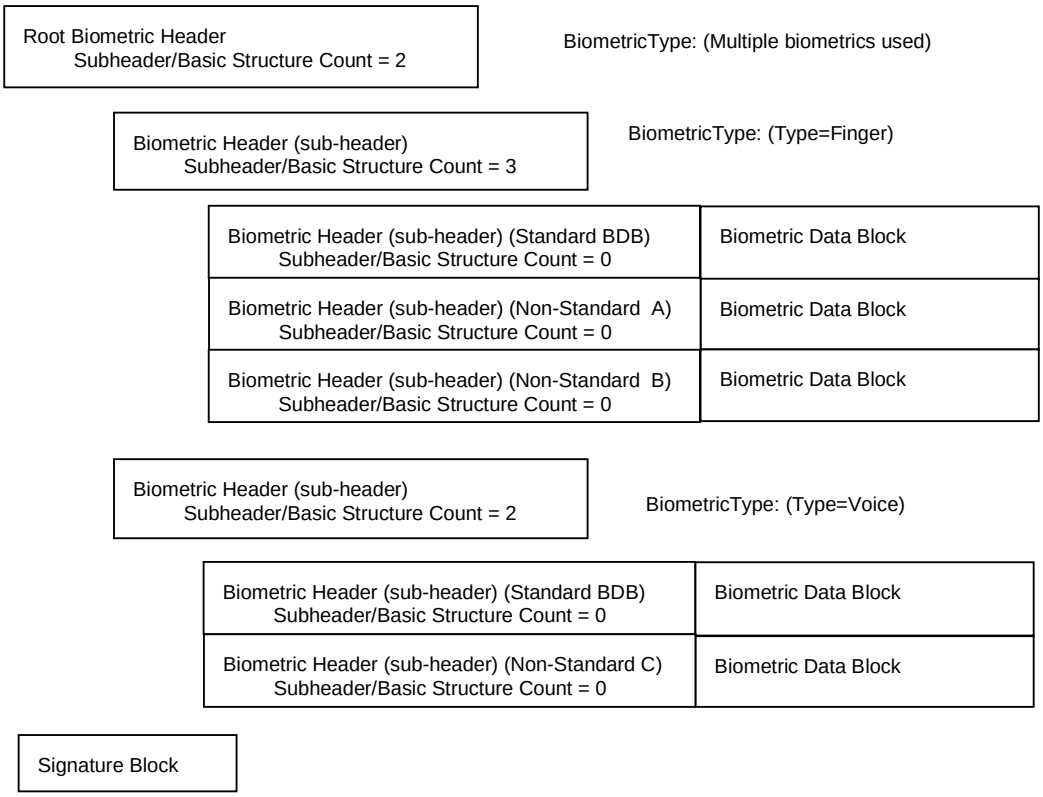
This field holds the Signature or MAC data. The content of this field shall be specified in the Patron Format Specification. This field can contain algorithm identifier information and/or any parameters needed to perform the Signature and/or the MAC function. This field exists only if the SBH Security Options field specifies Integrity-Only, or Integrity-And-Privacy.

## 5.3 Nested CBEFF Structures

A Patron Format Specification may need to support multiple biometric data types (e.g., finger, face and voice) and/or multiple biometric data blocks of the same biometric type (e.g., finger biometric data blocks from more than one finger) in a CBEFF data structure. An application may wish to combine within a CBEFF structure data records from the same or different biometric types. Nesting CBEFF structures accommodates such requirements and avoids having to utilize multiple consecutive CBEFF records for a specific operation.

Figure 2 is an example of a nested CBEFF structure that includes finger and voice data.

**Figure 2. – Example of a CBEFF compliant nested Format**




Required characteristics of a CBEFF nested structure:

1) If a field value pertains to all the sub headers, the field does not have to be included in all of them but only in the root header (see below) or the sub-header that precedes these sub-structures. For example, if three CBEFF substructures represent the same Biometric Type (e.g., finger), the Biometric Type field needs to be included only in the root header (or the sub-header that precedes these three sub-structures representing “finger”). The Patron Format Specification shall define if the Format is structured in this way.

2) In the event of a conflict between fields in the root header or higher level sub-header and lower level sub-header, the data within the lower level sub-header (i.e., that closest to the actual data) takes precedence.

3) If the Index data element is used, it may occur at one or more levels within the CBEFF nested structure (e.g., associated with an individual person or associated with each biometric type or sample for that person). In the case of multiple instances of Index values, the Format Specification shall specify how to use or not use each of these values.

4) If a nested structure needs to support more than one CBEFF-compliant Patron Format in its several branches, then the sub header at the root of each such branch shall contain a Patron Format Identifier field that identifies the CBEFF Patron Format.

# 6. CBEFF Patrons and Clients

## 6.1 General

A **CBEFF Patron** is an organization that has defined a Format Specification incorporating biometric data objects that comply with CBEFF requirements. Patron define **Domains of Use** (the context in which a format should be used). It is intended that there be a limited number of Format Specifications with a minimum of overlap in the areas (Domains) where the data is used. However, as new technologies and applications for biometrics emerge, new Patrons and requirements for new Formats will emerge. Each CBEFF Patron can define as many Patron Format Specifications as it requires for its Domains of Use.

A **CBEFF Client** is an entity that creates a specific biometric data structure (a CBEFF client is therefore a BDB format owner) that complies with CBEFF requirements. This would include any vendor, standards body, working group, or industry consortium that has registered itself with IBIA and has defined one or more BDB format types.

## 6.2 Adding New CBEFF Patron Formats

When an application emerges where current Patron Formats do not satisfy requirements, a new Patron Format may be proposed to the CBEFF Team.

Requests shall include the following information in the specified order:

1) The name of the Patron (this may be a new or existing Patron)

2) The intended Domain of Use.

3) An explanation of why a new Patron Format is needed, e.g. what unique features will be provided that are not already available in other formats.

4) CBEFF data elements and values to be used in the new format.

5) Descriptions of capabilities provided by the new format.

6) Encoding of the data elements

7) A description of the Biometric Header of the new format and which fields map to which fields of the CBEFF specification.

8) The full name and title of the document that describes the new format (this may be a document still in the creation process).

9) The date at which the new document is expected to be approved and published.

When the request for a new Patron format is accepted, the request document may be used as the basis for an Annex describing the new format. Such new annexes shall eventually be published as part of a revised version of this specification, but in the meantime they will be publicly available through the IBIA web site.

## 6.3 Biometric Data Block Format Owner and Type Registration

CBEFF BDB Format Owner represents an entity that defines one or more Biometric Data Block formats. To become a recognized CBEFF BDB Format Owner (and thus obtain a guaranteed unique BDB Format Owner value), it is required that the format owner register with the Registration Authority. The International Biometric Industry Association (IBIA) has agreed to be the registration authority. The IBIA will manage the registration, issuance, and archiving of the Format Owner and Format Type values for Organizations and Vendors which require them. The IBIA has set up a web based support site, including the registration and retrieval of CBEFF

identifiers. Details of this process can be found by contacting the IBIA (www.ibia.org). See Annex F for IBIA contact information.

CBEFF BDB Format Type represents the specific Biometric Data Block format for a BDB, as defined by the BDB Format Owner. Registration of BDB Format Types is encouraged but not required. When the data format represented in the Format Type is not a standard or public specification, the BDB Format Owner is not required to publish information about registered BDB Format Types.

A standard biometric format shall be identified by the Format Owner of the standards body that specified that format. Upon request by the standards organization that developed or is developing the standard biometric format for data that is required to be used in the BDB within a CBEFF structure, the value will be assigned by the IBIA in consultation with the CBEFF Technical Development Team. This value is free of charge to the standards organization that developed (or is developing) that biometric data format standard.

A non-standard format (proprietary) also needs a Format Owner. This Format Owner can be directly requested from IBIA by the organization that defined that format to be used within the BDB of the CBEFF structure.

# Annex A
# (Normative)
# Patron Format A Description

## Patron

NIST/BC Biometric Interoperability, Performance, and Assurance Working Group
(www.nist.gov/bcwg; www.nist.gov/cbeff)

## Domain Of Use

Patron Format A is a convenience format for situations where a CBEFF structure needs to be used but it is not desired to establish a Patron and register a format.

## Requirements on users of this Patron Format

Application system specifications using this Patron Format are permitted to exclude optional CBEFF fields from the SBH used in that application system. If this is done, the application system specification shall

1. state that it is using the CBEFF Patron Format A specification for its Standard Biometric Headers, and
2. list the optional CBEFF fields that are to be included in the CBEFF headers within the application system, or
3. indicate if the Optional Fields Present Mask, which is a Patron Format A-specific field, is included in the SBH, and
4. require that the CBEFF fields in the CBEFF headers shall be in the same order as specified in Table A.1.

If the Biometric Type field is used, it shall be a three byte mask as defined in Table 4.

Note that by defining a Format more closely fitted to the requirements of a Domain of Use, rather than using CBEFF Patron Format A, the Patron can gain flexibility and efficiency regarding field order and, in some cases, field content. For example, if the DOU will use no more than 3 different biometric modalities, the Biometric Type field could be specified as a 3 bit mask rather than the 24 bits specified in Table 4.

The Standard Biometric Header of format A has the fields illustrated in the Table A.1. The length column is the number of bits or bytes used to represent each field. Refer to Clause 5.2.1 for definitions of the fields.

## Patron Format Specification

### Table A.1 – NIST BC/WG: Standard Biometric Header Patron Format A

| Field Name | Length | Bit Location | Mandatory/ Optional | Notes |
|---|---|---|---|---|
| BDB Format Owner | 2 bytes | | Mandatory | See 5.2.1.17.1 |
| BDB Format Type | 2 bytes | | Mandatory | See 5.2.1.17.2 |
| *Name not applicable to this byte (Provides for SBH Security Options and Integrity Options)* | 1 byte: | | Mandatory | The presence of this entire byte is Mandatory. |
| Optional Fields Present Mask | 1 bit | x'08' | Mandatory | Optional Fields Present Mask Used = 1<br>Optional Fields Present Mask Not Used = 0<br>(see note 1) |
| Signature/MAC | 1 bit | x'04' | Mandatory | Signature = 1; MAC = 0 |
| Privacy | 1 bit | x'02' | Mandatory | Privacy = 1; No-Privacy = 0 |
| Integrity | 1 bit | x'01' | Mandatory | Integrity = 1; No-Integrity = 0 |
| Reserved | 4 bits | x'F0' | Mandatory | These 4 bits shall have value 0 |
| Subheader/Basic Structure Count | 1 byte | | Optional | See 5.2.1.16. This field supports nesting to 255 levels. |
| PID | | | Optional | See 5.2.1.18 |
| Product Owner | 2 bytes | | | |
| Product Type | 2 bytes | | | |
| Patron Format Identifer | | | Optional | See 5.2.1.19 |
| Patron Format Owner | 2 bytes | | | |
| Patron Format Type | 2 bytes | | | |
| Index | 4 bytes | | Optional | See 5.2.1.13. This field supports indexes to 65,535. |
| Biometric Creation Date | 8 bytes | | Optional | See 5.2.1.10 |
| Validity Period | 16 bytes | | Optional | See 5.2.1.11 |
| Biometric Type | 3 bytes | | Optional | See 5.2.1.5 |
| Biometric Subtype | 1 byte | | Optional | See 5.2.1.6 |
| CBEFF Header Version | 1 byte | | Optional | See 5.2.1.3, value = b'0001 0001' (Major = 1, Minor = 1) |
| Patron Header Version | 1 byte | | Optional | See 5.2.1.4, value = b'0001 0001' (Major = 1, Minor = 1) |
| Biometric Purpose | 1 byte | | Optional | See 5.2.1.8:<br>Reserved = x'00'<br>"Verify" = x'01'<br>"Identify" = x'02'<br>"Enroll" = x'03'<br>"Enroll for Verification Only" = x'04'<br>"Enroll for Identification Only" = x'05'<br>"Audit" = x'06'<br>All other values are Reserved |
| Biometric Data Type | 1 byte | | Optional | See 5.2.1.7<br>"Raw" = b'001x xxxx'<br>"Intermediate" = b'010x xxxx'<br>"Processed" = b'100x xxxx'<br>All other values are Reserved |
| Biometric Data Quality | 1 byte | | Optional | See 5.2.1.9 |
| Creator | | | Optional | See 5.2.1.12 |
| Creator length | 4 bytes | | Mandatory | If the Creator field is present, then it shall be structured as a 4 byte length field and variable length content field. . The length value shall include the 4 byte length field. |
| Creator content | Variable | | Mandatory | |
| Challenge/Response | | | Optional | See 5.2.1.14 |
| Challenge/Response length | 4 bytes | | Mandatory | If the Challenge/Response field is present, then it shall be structured as a 4 byte length field and variable length content field. The length value shall include the 4 byte length field. |
| Challenge/Response content | Variable | | Mandatory | |
| Payload | | | Optional | See 5.2.1.15 |
| Payload length | 4 bytes | | Mandatory | If the Payload field is present, then it shall be structured as a 4 byte length field and variable length content field. . The length value shall include the 4 byte length field. |
| Payload content | Variable | | Mandatory | |

Note (1)

The Optional Fields Present Mask is a Patron Format A - specific field that may optionally be included in the SBH to indicate what specific CBEFF optional fields are present in the record/structure (see below). Use of this element facilitates the dynamic, automated interpretation or parsing of the information within the SBH.

| Patron Format A Specific Field | Field Source | Length | Bit Location | Mandatory/ Optional | Notes |
|---|---|---|---|---|---|
| Optional Fields Present Mask | Format A | 2 bytes | | Optional | Present only if "Optional Fields Present" = 1. |
| Subheader/Basic Structure Count | | | x'0001' | | The 16 bits in this mask each represent the indicated CBEFF-optional fields. Bit value = 1 indicates that field is present in the Header. |
| PID | | | x'0002' | | |
| Patron Format Identifier | | | x'0004' | | |
| Index | | | x'0008' | | |
| Biometric Creation Date | | | x'0010' | | |
| Validity Period | | | x'0020' | | |
| Biometric Type | | | x'0040' | | |
| Biometric Subtype | | | x'0080' | | |
| CBEFF Header Version | | | x'0100' | | |
| Patron Header Version | | | x'0200' | | |
| Biometric Purpose | | | x'0400' | | |
| Biometric Data Type | | | x'0800' | | |
| Biometric Data Quality | | | x'1000' | | |
| Creator | | | x'2000' | | |
| Challenge/Response | | | x'4000' | | |
| Payload | | | x'8000' | | |

Conformance with Patron Format A can be achieved with or without this specific field. If this field is used it must immediately follow the Subheader/Basic Structure Count field and all subsequent fields must strictly follow the order shown in Table A.1. If the field is not used, then the implementer of Patron Format A must define in their documentation which optional fields are present and what order they are in.

# Annex B
# (Normative)
# Patron Format B Description

**Patron:**

NIST/BC Biometric Interoperability, Performance, and Assurance Working Group
(www.nist.gov/bcwg; www.nist.gov/cbeff)

**Domain Of Use**:

Patron Format B provides a root header for CBEFF data structures in a domain where multiple Patron Formats may be encountered. In such a domain it is necessary for applications to be able to recognize the Patron Format of any CBEFF data structure before attempting to process it.

Patron Format B uses the CBEFF field Patron Format Identifier in a root header to identify the Patron Format of the SBH of the next level CBEFF data structure. Patron Format B is specified as having a zero-length BDB and a zero-length SB. Thus the CBEFF-required fields SBH Security Options, BDB Format Owner and BDB Format Type are, strictly speaking, encoded as zero length fields.

Patrons of Domains of Use where this Patron Format is used as a root header are required to specify CBEFF simple or nested-structure Patron Formats having non-zero length BDBs for use in their Domains. The level just below the root header in such Patron Formats may be a simple CBEFF structure, or it may be a nested CBEFF structure with two or more levels.

There can be up to 255 CBEFF structures in the next level below this root header. If the Domain of Use requires that every CBEFF structure in the next level below this root header shall be a simple CBEFF structure, then the SBH's of those simple CBEFF structures are not required to include the CBEFF Subheader/Basic Structure Count field. If, however, the Domain of Use permits *any* of the CBEFF structures in the next level below this root header to be a nested CBEFF structure, then *every* SBH of those structures is required to include the CBEFF Subheader/Basic Structure Count field.

**Table B.1 – NIST BC/WG: Standard Biometric Header Patron Format B**

| Field Name | Field Source | Length | Bit Location | Mandatory/ Optional | Notes |
|---|---|---|---|---|---|
| BDB Format Owner | CBEFF | 0 bytes | | Mandatory | See 5.2.1.17.1 |
| BDB Format Type | CBEFF | 0 bytes | | Mandatory | See 5.2.1.17.2 |
| SBH Security Options | CBEFF | 0 bytes | | Mandatory | See 5.2.1.1 |
| Patron Format Identifier | CBEFF | 4 bytes | | Mandatory | See 5.2.1.19 |
| Subheader/Basic Structure Count | CBEFF | 1 byte | | Mandatory | See 5.2.1.16 |

# Annex C
(Normative)
# Format C – The BioAPI Biometric Identification Record (BIR)

**Patron:** BioAPI Consortium

**Domain of Use:** Applications and BSPs (Biometric Service Providers) requiring a BioAPI compliant Standard Biometric Header.

## C.1 Introduction

This Patron Format has been designed to be as flexible as possible, allowing the biometric vendor to store whatever information is needed, without unnecessary constraints. For example, the biometric data structures may contain a single biometric sample or may contain multiple samples. In order to support a wide range of process flow possibilities and biometric samples and templates (models), these structures can be used to store any combination of data necessary to facilitate subsequent matching. It is the responsibility of the Biometric Service Provider (BSP) to fill this data structure with the data needed and in the format needed, and to be able to extract this data when it is needed.

## C.2 Normative References

ANSI/INCITS 358-2002, Information Technology – The BioAPI Specification, 13 February 2002

## C.3 Biometric Record Header

This BioAPI Patron Format standardizes the header information preceding biometric data records to minimally and uniquely identify the content as well as to distinguish it from other, non-biometric data records.

```
typedef struct bioapi_bir {
    BioAPI_BIR_HEADER  Header;
    BioAPI_BIR_BIOMETRIC_DATA_PTR BiometricData; /* length indicated in header */
    BioAPI_DATA_PTR Signature; /* NULL if no signature; length is inherent in this type */
} BioAPI_BIR, *BioAPI_BIR_PTR;


typedef struct bioapi_bir_header {
    uint32 Length;   /* Length of Header + Opaque Data */
    BioAPI_BIR_VERSION HeaderVersion;
    BioAPI_BIR_DATA_TYPE Type;
    BioAPI_BIR_BIOMETRIC_DATA_FORMAT Format;
        BioAPI_QUALITY Quality;
        BioAPI_BIR_PURPOSE PurposeMask;
            BioAPI_BIR_AUTH_FACTORS FactorsMask;
    } BioAPI_BIR_HEADER, *BioAPI_BIR_HEADER_PTR;


    typedef struct bioapi_bir_biometric_data_format {
```

```
        uint16 FormatOwner;
        uint16 FormatID;
    } BioAPI_BIR_BIOMETRIC_DATA_FORMAT, *BioAPI_BIR_BIOMETRIC_DATA_FORMAT_PTR;

    typedef uint8 BioAPI_BIR_BIOMETRIC_DATA;
```

## C.4 BioAPI to CBEFF Translation

Table C.1 defines the mapping between CBEFF fields and BioAPI BIR header fields.

**Table C.1 – CBEFF to BioAPI BIR Header Field Mapping**

NEED TO GO BACK TO EARLIER VERSION REFLECTING THE ANSI VERSION OF BIOAPI

| CBEFF Field Name | BioAPI BIR Field Name | Notes |
|---|---|---|
| SBH Security Options | ANSI/INCITS 358-2002 Clause 2.1.7<br>BioAPI_BIR_DATA_TYPE<br>BioAPI DATA TYPE ENCRYPTED<br>BioAPI DATA TYPE SIGNED | BioAPI maps the CBEFF SBH Security Options and Biometric Data Type fields into the BioAPI_BIR_DATA_TYPE definition (mask). |
| Patron Header Version | ANSI/INCITS 358-2002 Clause 2.1.11<br>BioAPI_BIR_VERSION | |
| Biometric Type | ANSI/INCITS 358-2002 Clause 2.1.4<br>BioAPI_BIR_AUTH_FACTORS | BioAPI AUTH FACTORS is a mask.<br>If a BioAPI BIR contains multiple types, when translating to X9.84 or other format that only accommodates a single value, only the '01' (multiple) value shall be used. |
| Biometric Data Type | ANSI/INCITS 358-2002 Clause 2.1.7<br>BioAPI_BIR_DATA_TYPE<br>BioAPI_BIR_DATA_TYPE_RAW<br>BioAPI_BIR_DATA_TYPE_INTERMEDIATE<br>BioAPI_BIR_DATA_TYPE_PROCESSED | See note for SBH Security Options |
| Biometric Purpose | ANSI/INCITS 358-2002 Clause 2.1.10<br>BioAPI_BIR_PURPOSE | |
| Biometric Data Quality | ANSI/INCITS 358-2002 Clause 2.1.46<br>BioAPI_QUALITY | BioAPI further defines relative quality ranges |
| BDB Format Owner | ANSI/INCITS 358-2002 Clause 2.1.6<br>BioAPI_BIR_BIOMETRIC_DATA_FORMAT<br>FormatOwner | |
| BDB Format Type | ANSI/INCITS 358-2002 Clause 2.1.6<br>BioAPI_BIR_BIOMETRIC_DATA_FORMAT<br>FormatID | |
| Biometric Data Block (BDB) | ANSI/INCITS 358-2002 Clause 2.1.2 / 2.1.5<br>BioAPI_BIR_BIOMETRIC_DATA_PTR<br>Biometric Data | |
| Signature | ANSI/INCITS 358-2002 Clause 2.1.2<br>BioAPI_DATA_PTR<br>Signature | |

# Annex D: (Normative) Biometric Information Data Objects for Use within Smartcards or other Tokens

## D.1 Patron:

NIST/BC Biometric Interoperability, Performance, and Assurance Working Group (www.nist.gov/bcwg)

## D.2 Domain of Use

Applications using biometrics and tokens (such as smartcards conforming to ISO/IEC 7816). It is applicable for both on-card and off-card matching.

## D.3 Introduction

**D.3.1** In ISO/IEC 7816-11: "Personal verification through biometric methods" and in ISO/IEC 7816-4: "Organization, security and commands for interchange", the card related issues such as

- retrieval of information from the card prior to a verification process
- commands for performing a verification
- strategies for enrollment
- security mechanisms e.g. for establishing a trusted channel between the card and the service system

are specified.

**D.3.2** With respect to the data objects usable for on-card matching and off-card matching, ISO/IEC JTC 1/SC 17 has defined a "Biometric Information Template". A template is, in the ISO/IEC 7816 standards, the value field of a constructed data object encoded using ASN.1 BER-TLV. The Biometric Information Template relies on the import of data objects specified by ISO/IEC SC 37 in this CBEFF standard. To avoid any conflict in assigning tags for the respective data objects, the CBEFF data objects defined in this annex are nested in a constructed data object called "Biometric Header Template". All data objects are in compliance with ISO/IEC 7816 (Part 6 and Part 11). The usage of these data objects is described in ISO/IEC 7816-11.

NOTE The Biometric Header Template takes into account the data elements specified for the Standard Biometric Header as defined in clause 5, and is a conforming CBEFF patron format.

## D.4 Abbreviations and Notations

BER = Basic Encoding Rules
BHT = Biometric Header Template
BIT = Biometric Information Template
DO = Data Object
IC = Integrated Circuit(s)
L = Length
LSB = Least Significant Byte
MSB = Most Significant Byte
SE = Security Environment

NOTE For the representation of the data objects, BER coding with Tag-Length-Value (TLV structure) is used (see ISO/IEC 7816-4).

NOTE In this Annex the term “Template” is used in accordance with the ISO/IEC 7816 standard and denotes the value field of a constructed data object.

## D.5 Biometric information data objects used in case of on-card matching

Table D.1 shows the Biometric Information Template BIT (tag ‘7F60’ as defined in ISO/IEC 7816-11) relevant for on-card matching. The BIT has the following substructure:

DOs with tag ‘80’ and ‘83’ as defined in ISO/IEC 7816-11, containing values relevant for interindustry commands used for biometric verification as defined in ISO/IEC 7816-4

Biometric Header Template (BHT) with tag ‘A1’ as defined in ISO/IEC 7816-11. The tag allocation authority for the DOs nested in the BHT is ISO/IEC JTC1/SC37 (default tag allocation authority).

Biometric data objects based on data elements defined in the main part of this standard and relevant for on-card matching

Biometric data objects which are on-card matching specific and only defined in this annex.

**Table D.1 — Biometric information data objects used in case of on-card matching**

| **Tag** | **L** | **Value** | | | | | **Presence** |
|---|---|---|---|---|---|---|---|
| ‘7F60’ | Var. | Biometric Information Template (BIT) | | | | | |
| | | **Tag** | **L** | **Value** | | | |
| | | ‘80’ | 1 | Algorithm reference for use in the VERIFY / EXT. AUTHENTICATE / MANAGE SE command as defined in ISO/IEC 7816-4 | | | Optional |
| | | ‘83’ | 1 | Reference data qualifier for use in the VERIFY / EXT. AUTHENTICATE / MANAGE SE command as defined in ISO/IEC 7816-4 | | | Optional |
| | | ‘A1’ | Var. | Biometric Header Template (BHT)<br>Tag allocation authority: ISO/IEC JTC 1/SC 37 | | | Mandatory |
| | | | | **Tag** | **L** | **Value** | |
| | | | | ’80’ | 2 | CBEFF_patron_header_version (default ‘0101’) | Mandatory<br>(if absent, the default value applies) |
| | | | | ‘90’ | Var. | CBEFF_BIR_index,<br>unique identifier used for referencing this biometric data set in an application context outside the card | Optional |
| | | | | ‘81’ | 1-3 | CBEFF_BDB_biometric_type,<br>see Table 4, Clause 5.2.1.5 | Optional |
| | | | | ‘82’ | 1 | CBEFF_BDB_biometric_subtype,<br>see Table 6, Clause 5.2.1.6 | Optional, use with biometric type only |
| | | | | ‘83’ | 7 | CBEFF_BDB_creation_date,<br>creation date and time of biometric data (CCYYMMDDhhmmss) as concatenation of binary coded digits (BCD) | Optional |
| | | | | ‘84’ | Var. | CBEFF_BIR_creator | Optional |
| | | | | ‘85’ | 8 | CBEFF_BDB_validity_period,<br>(from CCYYMMDD, to CCYYMMDD) as concatenation of binary coded digits (BCD) | Optional |
| | | | | ‘86’ | 4 | CBEFF_BDB_PID,<br>identifier of product (PID) that created the biometric reference data, value assigned by the biometrics registration authority | Optional |
| | | | | ‘87’ | 2 | CBEFF_BDB_format_owner, | Mandatory |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | format owner of the biometric verification data, value assigned by the biometrics registration authority | |
| | | | | ‘88’ | 2 | CBEFF_BDB_format_type,<br>format type of biometric verification data, specified by format owner | Mandatory |
| | | | | ‘91’ / ’B1’ | Var. | Biometric matching algorithm parameters (primitive / constructed), see note 4 | Optional |

NOTE 1 In Table D1 the biometric data block as defined in the main part of this standard is not present, since the biometric reference data are stored separately in the card and not in this BIT. The biometric verification data (format owner and format type indicated in the DOs with tag ‘87’ and ‘88’) have to be presented to the card using e.g. a VERIFY command.

NOTE 2 In Table D1 no payload is present, since usually access to a payload, if used by the application, is granted after successful completion of the biometric verification. The payload may be retrieved using interindustry access commands like GET DATA or READ BINARY.

NOTE 3 The outside world (i.e. the IFD) uses format owner / format type for identifying the required structure for the verification data. The matching algorithm in the card is addressed by the algorithm reference.

NOTE 4 This DO provides any special parameters of an on-card matching algorithm implementation, e.g. maximum number of minutiae expected in the biometric verification data. The content of this DO is defined by the format owner (see e.g. ISO/IEC 19794-2).

The use of the BIT according to table D.1, which is intended to be retrieved prior to a biometric user verification, and the verification process itself with the related interindustry commands and its security requirements are described in ISO/IEC 7816-11.

## D.6 Biometric information data objects used in case of off-card matching

Table D.2 shows the Biometric Information Template BIT (tag ‘7F60’ as defined in ISO/IEC 7816-11) relevant for off-card matching. The BIT has the following substructure:

Biometric Header Template (BHT) with tag ‘A1’ as defined in ISO/IEC 7816-11. The tag allocation authority for the DOs nested in the BHT is ISO/IEC JTC1/SC37 (default tag allocation authority).

Biometric data objects nested in the BHT are based on data elements defined for the Standard Biometric Header in the main part of this standard and relevant for off-card matching.

Biometric reference data objects (primitive or constructed) with tags as defined in ISO/IEC 7816-11, representing the Biometric Data Block (BDB).

Payload as content of a discretionary data DO with tag ‘53’ or ‘73’ as defined in ISO/IEC 7816-6.

Signature block for data security (see note 1 below table D.2).

The use of the data structure shown in table D.2 is not restricted to IC cards, i.e. the data structure may also be used in other types of cards, e.g. magnetic stripe cards, optical memory cards or cards with 2-dimensional barcode.

**Table D.2 — Biometric information data objects used in case of off-card matching**

| Tag | L | Value | | | | | Presence |
|---|---|---|---|---|---|---|---|
| '7F60' | var. | Biometric Information Template (BIT) | | | | | |
| | | Tag | L | Value | | | |
| | | 'A1' | var. | Biometric Header Template (BHT)<br>Tag allocation authority: ISO/IEC JTC 1/SC 37 | | | Mandatory |
| | | | | **Tag** | **L** | **Value** | |
| | | | | '92' | 2 | CBEFF_BDB_security_options and CBEFF_BIR_integrity_options,<br>(MSB: '00' No-Privacy, '01' Privacy only, '02' Integrity only, '03' Integrity and privacy;<br>LSB: '00' No-Integrity, '01' MACed,'03' Signed);<br>see note 1 | Optional |
| | | | | '80' | 2 | CBEFF_patron_header_version,<br>patron header version (default '0101') | Mandatory<br>(if absent, the default value applies) |
| | | | | '81' | 1-3 | CBEFF_BDB_biometric_type,<br>see Table 4, Clause 5.2.1.5 | Optional |
| | | | | '82' | 1 | CBEFF_BDB_biometric_subtype,<br>see Table 6, Clause 5.2.1.6 | Optional, used only together with biometric type |
| | | | | '83' | 7 | CBEFF_BDB_creation_date,<br>creation date and time of biometric reference data (CCYYMMDDhhmmss) as concatenation of binary coded digits (BCD) | Optional |
| | | | | '84' | var. | CBEFF_BDB_creator | Optional |
| | | | | '85' | 8 | CBEFF_BDB_validity_period,<br>validity period (from CCYYMMDD, to CCYYMMDD) as concatenation of binary coded digits (BCD) | Optional |
| | | | | '86' | 2 | CBEFF_BDB_PID,<br>identifier of product (PID) that created the biometric reference data, value assigned by the biometrics registration authority | Optional |
| | | | | '87' | 2 | CBEFF_BDB_format_owner,<br>format owner of the biometric reference data, value assigned by the biometrics registration authority | Mandatory |
| | | | | '88' | 2 | CBEFF_BDB_format_type,<br>format type of biometric reference data, specified by format owner | Mandatory |
| | | | | '90' | var. | CBEFF_BIR_index,<br>unique identifier used for referencing this biometric data set in an application context outside the card | Optional |
| | | '5F2E' / '7F2E' | var. | CBEFF_BDB,<br>biometric reference data (primitive / constructed); see note 3 | | | Mandatory |
| | | '53' / '73' | var. | CBEFF_BIR_payload,<br>discretionary data for payload (primitive / constructed) | | | Optional |
| | | '5F3D' / '7F3D' | var. | CBEFF_SB,<br>signature block for data security (primitive / constructed),<br>see note 1 and 2 | | | Conditional |

NOTE 1 The security features described in this specification with respect to indication of security and integrity options and provision of a field for a signature or MAC can be supported in a more flexible and enhanced way by using the Secure Messaging Template as described in ISO/IEC 7816-11.

NOTE 2 The signature or MAC covers all bytes starting with tag ‘A1’ of the BHT and ending with the last byte of the DO preceding the signature block DO.

NOTE 3 The structure of the biometric reference data in case of constructed allows the integration of a biometric challenge for user prompting (e.g. a phrase to be spoken) and a concatenation of biometric data with standardized and proprietary structure. The respective DOs are described in ISO/IEC 7816-11.

## D.7 Nested Structures

Several BITs may be nested in a group BIT (tag ‘7F61’ as defined in ISO/IEC 7816-11). The construction and use of nested structures both for on-card and off-card matching are described in ISO/IEC 7816-11.

# Annex E
# (Informative)
# Example of CBEFF Utilization Across Domains of Use

Described below is the utilization of CBEFF in a government or private organization that has different biometric enrollment applications for its employees and customers.

This application, uses BSPs (Biometric Service Providers, the biometric technology modules provided by biometrics vendors) that produce CBEFF-compliant biometric records that also comply with the BioAPI Patron Format. This organization provides its customers with biometric credentials to use in a public, CBEFF-compliant, national or world-wide applications that are also supported by many other organizations. The group of organizations that defined this application can specify and register its own CBEFF-compliant Patron Format that supports its particular Domain of Use.

The organization in this example must translate its customers' BioAPI-formatted data into the format of their Domain of Use. It does this through a **"Transforming Application"** The Transforming Application creates a new record that is compliant with the target Patron Format by mapping the values of the CBEFF fields that both Formats have in common, and by inserting appropriate values into fields that exist only in the target Format. (This could also mean that the Transforming Application must decrypt the **BDB** (Biometric Data Block -, the biometric data that is normally understood only within a BSP) from the initial record and re-encrypt it into the target record if the two Patron Formats specify different encryption techniques.

The organization must also translate its employees' BioAPI-formatted data into the organization's internal Domain of Use, where it has specified a CBEFF-compliant Format, but has elected not to register this Format for public use.

This example illustrates that the same BDB content can exist and be utilized in different CBEFF-compliant formats as required by different Domains of Use, so that applications within each Domain of Use can recognize and process that content regardless of the Domain of Use where it was created.

# Annex F
# (Informative)
# Contact Information for CBEFF as Specified in NISTIR 6529-A and IBIA

Inquiries about CBEFF or proposed CBEFF Patrons and requests for a standard Format Owner/Type value should be directed to the CBEFF Technical Development Team at cbeff@nist.gov

**International Biometric Industry Association**

Rebecca Dornbush, IBIA Deputy Director
601 Thirteenth Street, N.W., Suite 370 South
Washington, D.C. 20005
202-783-7272 voice
202-783-4345 fax
ibia@ibia.org
http://www.ibia.org

(For non-standard Format Owner/Type registrations: http://www.ibia.org/formats.htm)