NISTIR 6529

CBEFF

Common Biometric Exchange File Format

Fernando L. Podio
Jeffrey S. Dunn
Lawrence Reinert
Catherine J. Tilton
Lawrence O'Gorman
M. Paul Collier
Mark Jerde
Brigitte Wirtz

January 3, 2001

Partially sponsored by
U.S. National Security Agency

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

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
03-01-2001		xx-xx-2001 to xx-xx-2001

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
CBEFF Common Biometric Exchange File Format Unclassified	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Podio, Fernando L. ; Dunn, Jeffrey S. ; Reinert, Lawrence ; Tilton, Catherine J. ; O'Gorman, Lawrence ;	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME AND ADDRESS NIST/ITL 100 Bureau Drive, Stop 8951 Gaithersburg, MD20899-8951	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS U.S. National Security Agency Ft. Meade, MD20755	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See report.

15. SUBJECT TERMS
IATAC COLLECTION

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	38	email from Booz, Allen & Hamilton (IATAC), (blank) lfenster@dtic.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	1/3/2001	Report 1/3/2001

4. TITLE AND SUBTITLE
Common Biometric Exchange File Format (NISTIR 6529)

5. FUNDING NUMBERS

6. AUTHOR(S)
Podio, Fernando L.; Dunn, Jeffrey S.; Reinert, Lawrence; Tilton, Catherine J.; O'Gorman, Lawrence; Collier, M. Paul; Jerde, Mark; Wirtz, Brigitte

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

NIST

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

NSA/NIST
Ft. Meade, MD 20755/Gaithersburg MD 20899-8951

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

The Common Biometric Exchange File Format (CBEFF) describes a set of data elements necessary to support biometric technologies in a common way. These data 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. CBEEF'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 CBEFF, as described in this publication, in coordination with industrial organizations (I.e., the BioAPI Consortium, the X9.F4 Working Group, the International Biometric Industry Association, and the Interfaces Group of TeleTrust) and end users. CBEFF provides forward

14. SUBJECT TERMS
IATAC Collection, biometrics, biometric data format, biometric data elements, biometric data exchange, biometric technologies, data interchange, interoperability

15. NUMBER OF PAGES
37

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

NISTIR 6529

Fernando L. Podio[1]
Jeffrey S. Dunn[2]
Lawrence Reinert[2]
Catherine J. Tilton[3]
Lawrence O'Gorman[4]
M. Paul Collier[5]
Mark Jerde[6]
Brigitte Wirtz[7]

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

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

[3] *SAFLINK Corp.*
Redmond, WA 98052

[4] *Veridicom, Inc.*
Santa Clara, CA 95050

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

[6]*ANADAC*
Arlington, VA 22201

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

January 3, 2001

U.S. DEPARTMENT OF COMMERCE
Norman Y. Mineta, Secretary

TECHNOLOGY ADMINISTRATION
Dr. Cheryl L. Shavers, Under Secretary of Commerce for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Dr. Karen H. Brown, Acting Director

Foreword

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 in a common fingerprint template format. The participants identified the need for a "technology-blind" biometric file format that would facilitate the handling of different biometric types, versions, and biometric data structures in a common way. This common file format would facilitate exchange and interoperability of biometric data. (A "technology-blind biometric file 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 participants suggested that for the time being, the content of the biometric data structures (e.g., raw or processed biometric data) would not be defined in the common file 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 CBEFF as described in this publication. To ensure that the biometric data format would be in agreement with other biometric industrial efforts, the development was coordinated with industrial organizations such as the BioAPI Consortium, the X9.F4 Working Group, the International Biometric Industry Association, and the Interfaces Group of TeleTrusT.

The development included efforts focused on harmonizing the data formats among CBEFF, draft ANSI standard X9.84 and the specification developed by the BioAPI Consortium. Participation of the International Biometric Industry Association (IBIA) as the registration authority for the biometric data format was also addressed. This document reflects the result of these harmonization efforts. Further CBEFF development is proposed under the umbrella of the recently formed Biometrics Interoperability, Performance, and Assurance Working Group co-sponsored by NIST and the Biometric Consortium. A CBEFF smart card format is planned. This development will address harmonization of the CBEFF smart card data format with existing ISO standards and current ISO developments (e.g., ISO/IEC JTC1/SC17/WG4 Working Draft "Personal Verification Through Biometric Methods in Integrated Circuit(s) Cards").

Acknowledgements

The authors would like to express gratitude to the participants at the CBEFF Workshops that contributed to the CBEFF's initial conceptual definition and helped the technical development team to define CBEFF's scope of work. We would also like to thank the BioAPI Consortium members and the members of the X9.F4 Working Group. Their willingness to work with us contributed greatly to the biometric data format harmonization. We also want to thank the Interfaces Group of TeletrusT for their valuable editorial comments. Special thanks are due to the International Biometric Industry Association for their support to CBEFF and by acting as the Registration Authority for CBEFF Format Owners and Format Types.

Table of Contents

List of Figures

List of Tables

Common Biometric Exchange File Format (CBEFF)

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

Abstract

The Common Biometric Exchange File Format (CBEFF) describes a set of data elements necessary to support biometric technologies in a common way. These data 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. 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 CBEFF, as described in this publication, in coordination with industrial organizations (i.e., the BioAPI Consortium, the X9.F4 Working Group, the International Biometric Industry Association, and the Interfaces Group of TeleTrusT) and end users. 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. Further development (e.g., a CBEFF smart card format) is proposed under the umbrella of the recently formed Biometrics Interoperability, Performance, and Assurance Working Group co-sponsored by NIST and the Biometric Consortium.

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

[1]Convergent Information Systems Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8951
[2]Identification and Authentication Research Branch, National Security Agency, Ft. Meade, MD 20755
[3] SAFLINK Corp., Redmond, WA 98052
[4] Veridicom, Inc., Santa Clara, CA 95050
[5] Biometric Foundation, Washington, DC 20005
[6]ANADAC/Identix, Arlington, VA 22201
[7]Infineon Technologies AG, 81541 München, Germany

1. Introduction

The expected enormous growth in the use of biometric-based systems and applications highlights the need for exchange and interoperability of biometric data. It is conceivable that many biometric-based systems and applications are expected to support multiple biometric devices and biometric data. Products with that level of support for biometric-based authentication exist today. A Common Biometric Exchange File Format promotes interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange. CBEFF, as described in this publication, defines a common set of data elements necessary to support these biometric technologies. These data can be placed in a single file used to exchange biometric information between different system components or between systems.

The expected benefits of CBEFF are the ability to identify different biometric data structures (public or proprietary) supporting multiple biometric types within a system or application, the ability to reduce the need for additional software development and the ability to promote development cost savings.

CBEFF describes a set of "Required" and "Optional" fields, a "Domain of Use" to establish the applicability of a standard or specification that meets CBEFF requirements, and a process by which new technology or systems can create formats that meet these requirements. CBEFF allows for these standards or specifications to define a format and for these formats to define the data encoding. Adoption of CBEFF and compliance to those standards or specifications promotes interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange.

CBEFF's content reflects some current developments within the Biometric industry including the release of BioAPI Specification version 1.0 on March 30th, 2000 and the development of draft ANSI standard X9.84, "Biometric Information Management and Security".

By focusing on the description of the Biometric data elements, details such as data encoding, data and non-common elements can be left up to a standard or specification (see CBEFF Patrons in Section 8) that meets CBEFF requirements. By describing a process to establish new formats, the CBEFF can allow for biometrics data to be placed in new technologies and systems. Points of contact for CBEFF and liaisons to other organizations can be found in Appendix F.

2. Purpose

The purpose of CBEFF is to define 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. It also provides forward compatibility for technology improvements, simplifies the software/hardware integration process, and describes how new formats can be created.

The common set of data elements described in CBEFF can be placed in a single file record or data object used to exchange biometric information between different system components (the Common Biometric Exchange File). Formatting the data (e.g. allowing individual components to be

referenced) will allow an application to easily recognize important processing information about the biometric data such as what type of biometric is available, what version number, vendor's name, etc.

Formatting the data will also provide pointers to the proper biometric data. These characteristics foster interoperability between different types of biometric systems, allow for the exchange of biometric related information between different systems, and allow systems with different requirements to translate between different formats.

3. Scope

CBEFF accommodates any biometric technology. It includes the definition of format and content for data elements such as:

- A biometric data header that contains such information as version number, length of data, whether the data is encrypted or not, etc., for each biometric type available to the application or system;
- Biometric data (content not specified);
- Any other required biometric data or data structures.

CBEFF also describes the means for obtaining a unique value for identifying the format (owner and type) of the biometric data (see Section 8).

The common biometric data format does not attempt to achieve compatibility among different biometric technologies, but merely identifies them and facilitates their co-existence in a system or application. Although it is conceivable that industrial or user groups may agree upon common standard template formats within the biometric data structures defined in CBEFF, a definition of the content of these biometric data structures is not included in this publication.

CBEFF focuses on the description of the Biometric data elements. In order to decode CBEFF data, the applications need to have previous knowledge of which Patron (see the definition of a CBEFF Patron in Section 5 and the discussion on CBEFF Patron Biometric File Formats in Section 8) and data encoding scheme was used. Therefore, a Patron identifier is not included within the CBEFF definition. Each CBEFF Patron is required to define which CBEFF Optional Fields are present in their format and how the data elements are extracted and processed (details such as the data encoding scheme are left up to the CBEFF Patrons).

4. References

- ANSI X9.57-1997, "Public Key Cryptography for the Financial Services Industry: Certificate Management".
- BioAPI Consortium: http://www.bioapi.org
- BioAPI Consortium BIOAPI Specification, Version 1.00 March 30, 2000.

- Biometric Interoperability, Performance, and Assurance Working Group, http://www.nist.gov/bcwg
- Draft ANSI standard X9.84, Biometric Information Management and Security – 2000 (in public review)
- International Biometric Industry Association: http://www.ibia.org
- ISO/IEC 8825-1:1988, "Information technology ASN.1 encoding rules: basic encoding rules (BER), canonical rules (CER) and distinguished encoding rules (DER)".
- ISO/IEC 9594-8: "Information technology – Open systems interconnection - The directory: Public-key and attribute certificate frameworks".

5. Definitions, Abbreviations, Notation, and Acronyms

AlgorithmIdentifier: An ASN.1 type that identifies an algorithm (by an object identifier) and any associated parameters. This type is defined in [ISO/IEC 8825].

ASN.1: Abstract Syntax Notation One, as defined in [ISO/IEC 8825].

Attribute: An ASN.1 type that identifies an attribute type (by an object identifier) and an associated attribute value. The ASN.1 type **Attribute** is defined in [ISO/IEC 8825].

BCD: Binary Code Decimal

BSMB – Biometric Specific Memory Block

CBEFF: Common Biometric Exchange File Format

CBEFF Patron: An organization that has defined a standard or specification incorporating a biometric data object that meets CBEFF requirements. Examples of CBEFF Patrons are the BioAPI Consortium and ANSI Subcommittee X9, Group F4.

CBEFF Client: An entity that defines a specific biometric data structure (e.g., a BSMB format owner) that meets 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 BSMB format types.

Certificate: A digitally signed data unit binding a public key to identity information. A specific format for certificates is defined in [ISO/IEC 9594-8].

DER: Distinguished Encoding Rules, as defined in [ISO/IEC 8825].

Domain Of Use (DOU): The intended market or usage for the format. It is intended that there be limited amount of overlap between the DOUs.

DNA: Deoxyribo-Nucleic Acid

GUID: A globally-unique identifier

IBIA: International Biometric Industry Association. The IBIA has agreed to be the registration authority for all Object Identifiers and Relative Object Identifiers related to CBEFF.

MAC: Message Authentication Code

Object Identifier: A sequence of integers that uniquely identifies an associated data object in a global name space administrated by a hierarchy of naming authorities. This is a primitive data type in ASN.1.

Protocol Data Unit (PDU): A sequence of bits in machine-independent format constituting a message in a protocol.

Relative Object Identifier: A proposed ASN.1 type which makes it possible to transmit an Object Identifier value in a more compact form by transmitting only their trailing arcs when the leading arcs can be determined based upon the context of use.

[…] – Used to denote a variable length, typically depending upon details of the implementation.

SB: Signature Block

SBH: Standard Biometric Header

6. CBEFF Requirements

There are three minimum CBEFF requirements. The requirements are:

- To use a defined Format* as described in this publication.
- To implement the required Fields defined in Section 7.
- If an optional field is used, use for the field the definition included in section 7.

(NOTE*) Each format described in this publication 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 (see Section 8). However, new technologies may evolve that need new encoding rules and may require a new formatting. CBEFF describes a process to develop new formats.

7. CBEFF Data Element Descriptions

CBEFF data elements are placed in "fields" within a CBEFF file. The fields are grouped in three major sections (see Figure 1 in the following page):

Figure 1 – CBEFF Data Elements

SBH – Standard Biometric Header.

BSMB – Biometric Specific Memory Block.

SB – Signature Block

Each data element above is defined in the following Subsections.

This section defines the required fields for CBEFF formats and several common optional fields. A common set of definitions is provided that allows for translation between formats. The fields do not need to be included if they are optional.

The Values defined in this section are suggestions. CBEFF requirements do not include utilizing the exact values defined in this publication, however the use of these values is strongly recommended.

Translation between different formats will be facilitated if these values are used. If the specification or standard that meets CBEFF requirements changes, these values then must be properly documented. (An attempt has been made to match the suggested field values to the current BioAPI v1.0 specification to simplify translation from CBEFF to BioAPI.)

7.1 Standard Biometric Header (SBH)

The Standard Biometric Header includes the fields illustrated in Table 1. The Field name is the name given to the data element. The required or optional characteristic of the field has been appropriately indicated.

Definitions and suggested values for each of the fields specified in Table 1 (following page) are described below. Length fields depend on the data encoding scheme (typical field sizes have been added for clarity). Values in Tables 1 to 6 are expressed in hexadecimal notation.

Table 1 - Standard Biometric Header Followed by the BSMB and the SB

Field Name	Required or Optional	Notes
SBH Security Options	Required	0x00 = plain Biometric 0x10 = with Privacy (Encryption) 0x20 = with Integrity (Signed or MACed) 0x30 = with Privacy and Integrity
Integrity Options	Optional	0x01 = MACed 0x02 = Signed This field only exists if Integrity is used (i.e. SBH Options=0x20 or 0x30).
CBEFF Header Version	Optional	Version of the CBEFF header. Currently set to: Major: 0x01, Minor: 0x00
Patron Header Version	Required	Version of header (of a patron format specification or standard)
Biometric Type	Optional	Indication of biometric type.
Record Data Type	Optional	Indication of record data type. Currently set to 0x02 (Processed, the default). This field doesn't exist if the default is used.
Record Purpose	Optional	Intended use of the data. Currently set to 0x04 (Enroll for Verification Only, the default). This field doesn't exist if the default is used.
Record Data Quality	Optional	Indication of the quality of the biometric data
Creation Date	Optional	Creation date and time of the biometric data
Creator	Optional	Unique identifier of the entity that created the biometric data
BSMB Format Owner	Required	ID of the Group or Vendor which defined the BSMB
BSMB Format Type	Required	Type as specified by the Format Owner
Biometric Specific Memory Block (BSMB)	Required	Defined by the Format Owner
Signature	Optional	Signature of MAC. Only present if the SBH value is 0x20 or 0x30

Biometric Object (Signed Data)

NOTE:

Not Encrypted
Can be Encrypted

SBH Security Options: This field (the field length is typically 1 byte) is used to determine if the file is to have data integrity, encryption, or both as shown in Table 2. If integrity or integrity and encryption are used, then the integrity field is required. If encryption or integrity and encryption are used, then the integrity field is required.

Table 2 - SBH Security Options

Field Value Name	Type Value
None	0x00
With Privacy (Encryption)	0x10
With Integrity (signed or MACed)	0x20
With Integrity and Privacy (Encryption)	0x30

Integrity Options: This field (the field length is typically 1 byte) is used to determine if a Signature or Message Authentication Code (MAC) is used. A 0x01 indicates that MAC has been used. A 0x02 indicates that the data following this field is signed. This field is required only if the choice specified in the SBH security options is 0x20 or 0x30. The integrity options defined in this document are shown in Table 3.

Table 3 - Integrity Options

Field Value Name	Type Value
None	0x00
MACed	0x01
Signed	0x02

CBEFF Header Version: CBEFF Version (the field length is typically 2 bytes). It is defined as having a major and a minor component. Currently this field is set to:

Major: 0x01
Minor: 0x00

Patron Header Version: This field (the field length is typically 1 byte or 2 bytes) needs to be specified by implementations that conform to a format specification or standard (e.g., Format B in Section 8). Typically, it can be defined as having only a major component (typically 1 byte) or a major and a minor component (typically one byte-long each). In order to decode CBEFF data, the applications need to have previous knowledge of the Patron and the data encoding scheme that was used (see Scope). Therefore, a Patron identifier is not required within the CBEFF definition.

Biometric Type: This optional field (the field length is typically 1 to 3 bytes) defines the type of biometric technology. The currently defined types are shown in Table 4.

Table 4 – Biometric Type

Field Value Name	Biometric Type Value
Multiple Biometrics Used	0x01
Facial Features	0x02
Voice	0x04
Fingerprint	0x08
Iris	0x10
Retina	0x20
Hand Geometry	0x40
Signature Dynamics	0x80
Keystroke Dynamics	0x100
Lip Movement	0x200
Thermal Face Image	0x400
Thermal Hand Image	0x800
Gait	0x1000
Body Odor	0x2000
DNA	0x4000
Ear Shape	0x8000
Finger Geometry	0x010000
Palm Geometry	0x020000
Vein Pattern	0x040000

A binary representation example of Biometric Types Values follows:

b7 b6 b5 b4 b3 b2 b1 b0	b7 b6 b5 b4 b3 b2 b1 b0	b7 b6 b5 b4 b3 b2 b1 b0	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

The list of Biometric Type values may be expanded in future revisions of CBEFF. An optional field that represents the enrolled feature (e.g., left hand, ring finger or left ear) may be added in future revisions of CBEFF after the industry has the opportunity to address the need for (and content of) such optional field.

Record Data Type: This optional field (the field length is typically 1 byte) further defines the type of data being placed in the file. The defined data types are shown in Table 5. The default value of this field is "Processed" (0x02). This field doesn't exist if the default is used.

Table 5 – Record Data Type

Field Value Name	Type Value
Raw	0x00
Intermediate	0x01
Processed	0x02

Record Purpose: This optional field (the field length is typically 1 byte) denotes the intended use of the data. The defined values are shown in Table 6.

Table 6 – Record Purpose

Field Value Name	Type Value
Verify	0x01
Identify	0x02
Enroll	0x03
Enroll for Verification Only (default)	0x04
Enroll for Identification Only	0x05
Audit	0x06

The default value of this field is “Enroll for Verification Only” (0x04). This field doesn’t exist if the default is used.

Record Data Quality: This optional field (the field length is typically 1 byte) denotes the quality of the data. The values are in the range "0" through "100" (typically expressed in hexadecimal values 0x00 to 0x61), where "100" is the highest quality. A value of "–1" (typically 0xFF) indicates that quality was not set, and a value of "–2" (typically 0xFE) indicates that quality is not supported by the entity which created the SBH. The default value is "–2".

Creation Date: This optional field (the field length is typically 7 bytes) denotes the date and time that the biometric data was taken. The Creation Data is expressed in the following format: YYYY:MM:DD:HH:MM:SS. (Colons are not part of the field. December 15, 2000 at 5 AM, 35 minutes and 30 seconds, for example, is expressed as 20001215053520). Each letter in the “Creation Date” field represents a BCD (Binary Code Decimal) character (4 bits).

Creator: This optional field (16 bytes) contains a 128-bit length Unique Identifier of the entity that created the biometric data object according to the CBEFF requirements as described in this publication. It is recommended that this value be generated from a GUID.

BSMB Format Owner/Type: The BSMB Format Owner and Format Type, when used in combination, will uniquely identify the specific format of the BSMB content. The format and content of BSMB is “owned” by the CBEFF Client (see definition in Section 5). This BSMB format definition may be published (public) or unpublished (proprietary).

BSMB Format Owner: This field (the field length is typically 2 bytes) denotes the Vendor, Standards Body, Working Group, or Industry Consortium that has defined the format of the Biometric Data (in BSMB). A CBEFF requirement, as described in this publication, is that Format Owners register with IBIA for an assigned identifier of the Format Owner. The number is guaranteed to be unique. Refer to Section 8 for Registration information.

BSMB Format Type: This field value (the field length is typically 2 bytes) is assigned by the Format Owner and represents the specific BSMB Format as specified by the Format Owner.

Format Types can optionally be registered with IBIA. It is recommended that Format Owners register Format Types in use with the IBIA for archiving and publication purposes. Refer to Section 8 for information about registration.

7.2 The Biometric Specific Memory Block (BSMB)

This block contains the biometric data. It is simply a block of memory that can be specified in any way by the owner of the type as specified in the **Format Owner/Type** field of the SBH. Therefore, this can be a proprietary format or one agreed upon by a Standards Body, Working Group, or Industry Consortium.

The Vendor, Standards Body, Working Group, or Industry Consortium can place a biometric template directly into this field, or it can specify a format for the data with further parameters, information, and data.

The BSMB field format (e.g., a single bit map image) may not need any specification. There is likely to be a format analogous to the header/data format of most data storage structures. In this way, a vendor who "owns" this format can specify information in a header including version information, etc. Furthermore, it is conceivable, or likely, that Standards Bodies, Working Groups, or Industry Consortiums may agree upon common standard formats within BSMBs.

The BSMB may contain the following information:

- **BSMB Subheader** - may contain such information as version number, length of data, encryption info, etc.

- **BSMB data** - block of memory containing biometric data.

The BSMB may contain raw, intermediate, or processed biometric data collected for purposes of immediate matching or enrollment. The BSMB may include one or more samples of biometric data as well as non-biometric data.

7.3 Signature

This field holds the Signature or MAC data. 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 CBEFF Integrity Options field is 0x01 or 0x02.

8. Patron Biometric File Formats

CBEFF "Patrons" and "Clients" are defined in this Section. There can be several different derived Patron File Formats. All Patron Formats that meet the CBEFF requirements as described in this publication need to include the data elements identified in Section 7 as "required".

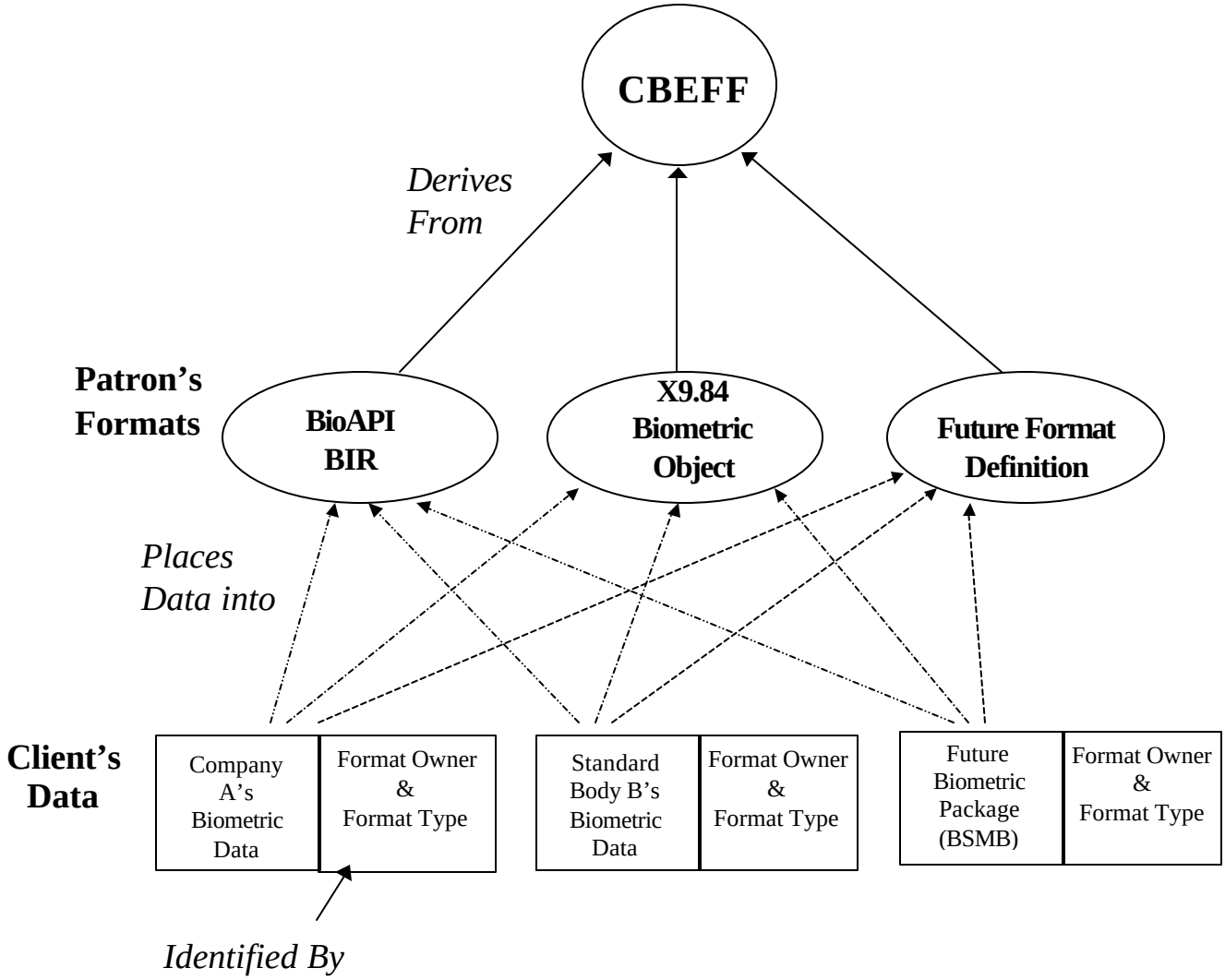
Each Patron Format specifies:

- Encoding of the data elements (i.e. packaging of the data with reference information)
- Additional (non-common) data elements
- Which Optional Fields are present and how the data elements are extracted and processed

Each Patron defines a **Domain of Use** (the context in which a format should be used). It is intended that there be a limited number of formats with a minimum of overlap in the areas (Domains) where the data is used. However, there may be new technologies that have adopted new encoding rules and require a new formatting.

This document describes the means for obtaining a unique value for identifying the format (owner and type) of the Biometric data (see Section 8.5). Figure 2 shows the relationship between CBEFF, CBEFF Patron Formats, and CBEFF Clients.

Figure 2. – Relationship Between CBEFF, CBEFF Patron Formats and CBEFF Clients



BIR: Biometric Identification Record

8.1 Patron Format A - The CBEFF Local Data Structure

Patron: CBEFF (www.nist.gov/cbeff)

Domain Of Use: Patron Format A is intended for small embedded or legacy systems that have limited data storage capabilities. This format assumes that the embedded system is not required to be BioAPI compliant.

This format implies that default mechanisms are used for the signature and/or encryption (There is not enough information to process a signature or encryption process without assuming default values which are generally passed with signed/encrypted data). Therefore this Format is NOT intended to be passed between systems, it is intended for the local system only.

8.2 Patron Format B - The BioAPI Specification v1.0 Biometric Identification Record Format

Patron: BioAPI Consortium (www.bioapi.org)

Domain Of Use: Patron Format B is intended for applications that are BIOAPI compliant. These systems are only required to store data and possibly exchange data between a client and a Server.

The BioAPI Consortium has published BioAPI Specification Version 1.0 and the BioAPI Reference Implementation. The BioAPI Biometric Identification Record (BIR) conforms to CBEFF.

8.3 Patron Format C – Draft ANSI Standard X9.84 Biometric Object

Patron: ANSI Subcommittee X9, Working Group F4.

Domain Of Use: Format C is intended for large systems that need to exchange biometric information in a secure, authenticate-able manor.

X9.F4 is the Standards Working Group that has developed draft ANSI standard X9.84, "Biometric Information Management and Security". X9.84 suggests the encoding of biometric data and defines the syntax via ASN.1 (refer to Appendix C for the description of biometric data that meets their security requirements). Refer to the X9.84 draft ANSI standard, when it becomes publicly available.

8.4 Adding New CBEFF Patron Formats

This publication describes how new CBEFF Patron Formats can be created when existing Patron Formats are determined to be insufficient to meet the requirements and constraints of the intended implementation.

The authors will propose to the recently established Biometric Interoperability, Performance, and Assurance Working Group (www.nist.gov/bcwg), a new initiative sponsored by NIST and the Biometric Consortium, to take on the responsibility to address these new requests and coordinate with the requestor of new Patron Formats development of the new format.

In the request for a new format the requestor needs to include:

- The intended Domain Of Use (where will it be used and how it differs from the currently supported domains). A description of why one of the existing Patron Formats cannot be used is suggested.
- Additional field descriptions that will be added (if known).
- The reference document that will be created which describes the entire format and its use.
- The timeframe in which the new format will be developed.

8.5 Format Owner and Format Type Registration

Since the BSMB contains biometric data whose content is not defined in this publication, a means must exist within the SBH to identify the format of that data. The 'Format Owner' and 'Format Type' header fields (objects) are the mechanism used for this purpose. By reading these values, an application or BSP can determine if the BSMB format is one that it is capable of interpreting and/or processing. To be used in this way, the Format Owner and Format Type values must be unique. This is accomplished through a registration process.

Format Owner is a 2-byte integer value. It represents an entity (an individual, vendor, or organization) that defines one or more biometric data formats. To become a recognized format owner (as described in this publication) and have a unique Format Owner value assigned, it is required that the format owner register with the registration authority.

Format Type is a 2-byte integer value. It represents a specific biometric data format for the BSMB, as defined by the Format Owner. This may be a proprietary, unpublished data format or a data format that has been standardized by an industry group, consortia, or standards body. The registration of the Format Type value is optional.

It is the combined Format Owner/Format Type value that uniquely identifies the BSMB format.

Format Owners and Format Types need to be registered by a recognized authority to assure uniqueness. The International Biometric Industry Association (IBIA) has agreed to be the registration authority - the organization which 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 Appendix E for IBIA contact information.

The Format Owner and Format Type values can also be expressed as OBJECT IDENTIFIERS or OIDs. A base OID arch has been allocated by ANSI to the IBIA for this purpose, as follows:

```
x9-84 OBJECT IDENTIFIER ::= {
   iso(1) identified-organization(3) tc68(133) country(16) x9(840)
            x9Standards(9) x9-84(84) IBIA(4) }
```

IBIA has further extended this base OID with the following values, to accommodate the CBEFF Format Owner/Type assignment:

```
x9-84 OBJECT IDENTIFIER ::= {
   iso(1) identified-organization(3) tc68(133) country(16) x9(840)
            x9Standards(9) x9-84(84) IBIA(4)
                  CBEFF(1) Format Owner (xx) Format Type (xx)}
```

Where the Format Owner value is issued by the IBIA and the Format Type value is assigned by the Format Owner.

The root OID { 133 16 840 9 84 4 1 } is not used by BioAPI in the BIR header (since it is static and thus assumed); however, it is used within the ANSI X9.84 draft standard for the ASN.1 encoding of the SBH.

Registration of format owner is required to populate the BSMB format owner field of the CBEFF Header. Registration of any format type is optional but highly recommended. Both values need to be included in the CBEFF header.

8.6 Translating Between Formats that Meet CBEFF Requirements

When a Domain of Use must interact with another domain, there may be a need to translate between formats. The fields that meet CBEFF requirements have the best ability to be translated.

Methods for translating between formats are not described in this publication. It is envisioned that commercial applications will eventually provide this capability. This publication provides the commonality of data elements that facilitate the translation.

Note that data integrity (e.g. signatures) and/or privacy (encryption) may be lost during translation. Applications that require high security may need to consider this.

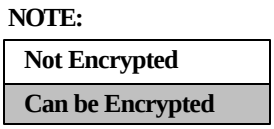
Appendix A: Patron Format A Description

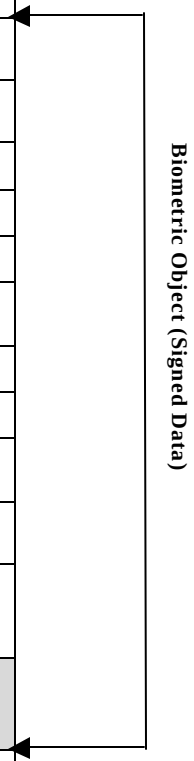
Patron: CBEFF (www.nist.gov/cbeff)

The Standard Biometric Header of format A has the fields illustrated in the following table. The length column is the number of bytes used to represent this field. Refer to Section 7 for the description of the fields.

Table A.1 – Format A Data Elements

Field Name	Length (Bytes)	Notes
SBH Security Options	1	Described in section 7
Integrity Options	1	Described in section 7
CBEFF Header	2	Described in section 7
Patron Header Version	2	Described in section 7
Biometric Type	3	Described in section 7
Record Data Type	1	Described in section 7
Record Purpose	1	Described in section 7
Record Data Quality	1	Described in section 7
Creation Date	7	Described in section 7
Creator	16	Described in section 7
BSMB Format Owner	2	Id of the Group or Vendor which defined the BSMB
BSMB Format Type	2	Type as specified by the Owner
Biometric Specific Memory Block (BSMB) Length	4	Length (in bytes) of the BSMB
Biometric Specific Memory Block Data (BSMB)	[…]	Defined by the Format Owner
Signature or MAC	0 or […]	Described in section 7





Most fields have a fixed length. The fields (with the exception of the BSMB length field) are described in section 7. The BSMB length field has been added to define the length of the BSMB. The Signature field immediately follows the last byte of the BSMB.

Appendix B: Patron Format B - The BioAPI Biometric Identification Record (BIR)

Patron: BioAPI Consortium (www.bioapi.org)

B.1. Introduction

The following is included for illustrative purposes only. Refer to the BioAPI documentation for a detailed description of the BioAPI specification or the BioAPI BIR.

This data structure is one that has been used in many fields involving data exchange; a single, technology-neutral header followed by a technology-specific data block. (It has been included in this proposal with the understanding that this is only an example of how the file format to be developed under this effort might look. It was included to encourage further discussions on the content of the required format.)

B.2. Data Structure Defined in the BioAPI Specification Version 1.0

The BioAPI Consortium has published the BioAPI v1.0 specification and the associated Reference Implementation. The data structure specified in BioAPI meets CBEFF's requirements.

The data structures herein defined have 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.

B.3. Biometric Record Header

This BioAPI data structure 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. Some of the data structures are currently defined as follows:

```
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;
```

Note: Other fields composing the BioAPI BIR header are defined in section 2.1 of the BioAPI specification (Version 1.0 of BioAPI is downloadable from the BioAPI website, www.bioapi.org)

B.4. BioAPI to CBEFF Translation

Table B.1 (following page) outlines the similarities between the CBEFF fields and the BioAPI BIR header information.

Table B.1 – CBEFF and BioAPI BIR Header Information

CBEFF Field Name	**Bio API BIR mapping**	**Notes**
Security Options	Section 2.1.7 BioAPI_BIR_DATA_TYPE BioAPI DATA TYPE ENCRYPTED BioAPI DATA TYPE SIGNED	BioAPI maps the SBH Security Options and Record Data Type fields into the BioAPI_BIR_DATA_TYPE definition (mask).
Integrity Options	N/A	
CBEFF Header Version	N/A	
Patron Header Version	Section 2.1.11 BioAPI_BIR_VERSION Header Version	
Biometric Type	Section 2.1.4 BioAPI_BIR_AUTH_FACTORS	BioAPI AUTH FACTORS is a mask. If a BioAPI BIR contains multiple types, when translating to X9.84 or other format that only accommodates a single value, only the 0x01 (multiple) value must be used.
Record Data Type	Section 2.1.7 BioAPI_BIR_DATA_TYPE BioAPI_BIR_DATA_TYPE_RAW BioAPI_BIR_DATA_TYPE_ INTERMEDIATE BioAPI_BIR_DATA_TYPE_PROCESSED	See note for Security Options
Record Purpose	Section 2.1.10 BioAPI_BIR_PURPOSE	Translates directly
Quality	Section 2.1.42 BioAPI_QUALITY	BioAPI further defines relative quality ranges
Creation Date	N/A	Not Used by the BioAPI
Creator	N/A	Not Used by the BioAPI
BSMB Format Owner	Section 2.1.6 BioAPI_BIR_BIOMETRIC_DATA_FORMAT FormatOwner	
BSMB Format Type	Section 2.1.6 BioAPI_BIR_BIOMETRIC_DATA_FORMAT FormatID	
Biometric Specific Memory Block (BSMB)	Section 2.1.2 / 2.1.5 BioAPI_BIR_BIOMETRIC_DATA_PTR Biometric Data	
Signature	Section 2.1.2 BioAPI_DATA_PTR Signature	

Appendix C: Format C - X9.84 Biometric Object

Patron: ANSI Subcommittee X9, Working Group F4

NOTE: At the time of the writing of this document, the X9.84 draft standard is about to initiate public review at which time it will be readily available. Please check with X9.84 for the status of the specification in terms of updates or changes.

C.1. Introduction

X9.F4 is the standards committee Working Group chartered to develop biometric standards for the financial services industry. X9.84 is a draft standard developed for Biometric Information Management and Security. Section 8 of the X9.84 draft standard describes biometric objects. The description of the Biometric Objects in the current X9.84 draft meets CBEFF requirements. Since X9.84 has addressed many of the issues involved with the secure transmission of biometric data it includes additional fields added to object definition to handle a wide variety of transfer scenarios.

C.2. The X9.84 Data Structure

X9.84 has the requirement to use ASN.1 syntax to describe all information. According to Annex J of the X9.84 draft standard. The advantages of using ASN.1 over a fixed format (such as Format A or B) are:

- Optional Protocol Data Units (PDUs) can save on the number of bytes and make the overall data object smaller.
- Relative Object Identifiers (OIDs) can save on the number of bytes and make the overall data object smaller.
- OIDs are infinitely extensible and therefore the number of possible values can never end.
- OIDs managed by the IBIA are guaranteed to be unique.

The ANSI X9.84 draft standard also takes into account several factors not currently considered by either Format A or B.

- Management of the keys used for Integrity or Confidentiality process.
- Identification of the algorithms used for the Integrity or Confidentiality process.
- It is defined as an attribute and can be embedded into other objects, such as an X.509 certificate..
- It can also encapsulate other Formats, such as Format A or B, for transmission purposes.

These objects are to be encoded using Basic Encoding Rules (BER), Distinguished Encoding Rules (DER) or possibly Packed Encoding Rules (PER) for applications that are concerned about limiting data sizes.

C.3. X9.84 to CBEFF Translation

X9.84 describes 4 types of Biometric Objects that correspond to the security options in the CBEFF Security Options (the Biometric Syntax). Within these biometric objects are 4 subclasses as follows:

- Biometric Header - instantiation of SBH
- Biometric Data (BD) - equivalent to unprotected BSMB
- Integrity Block - equivalent to Signature
- Privacy Block - equivalent to encrypted BSMB

The following table outlines the similarities between the CBEFF fields and the X9.84 header information, as described within the X9.84 ANS.1 syntax:

Table C.1 – CBEFF and X9.84 Header Information

CBEFF Field Name	**X9.84 mapping**	**Notes**
Security Options	Section 8.2.1 BiometricSyntax	
Integrity Options	Section 8.2.7 IntegrityBlock	
CBEFF Header Version	N/A	
Patron Header Version	Section 8.2.2 BiomtricHeader, version	
Biometric Type	Section 8.2.2, RecordType ::= BIOMETRIC.&name Section 8.2.3 Biometric Types	OIDs are assigned to each Biometric Type value.
Data Type	Section 8.2.2 DataType	
Purpose	Section 8.2.2 Purpose	
Quality	Section 8.2.2 Quality	
Creation Date	Section 8.2.1 Validity period	Validity dates implies 2 dates: date it is valid from and the date is valid to. Creation date is equivalent to the valid from date.
Creator	N/A	
BSMB Format Owner	Section 8.2.2 Format Format Owner	
BSMB Format Type	Section 8.2.2 Format Format Type	
Biometric Specific Memory Block (BSMB)	Section 8.2.2 BiometricData	Encoded as octet string
Signature	Section 8.2.7 Integrity Object Signature MAC	

Appendix D: An Example of Embedding a CBEFF Object

D.1. The X.509 AuthenticationInfo Attribute Certificate

D.1.1 Certificate Background

This section has been appended as an example of how the CBEFF can be used to place biometric data within an Attribute certificate. It is widely believed that many systems will, in the future, use X.509 certificates to hold biometric templates, therefore this may be an appropriate example.

D.1.2 Attribute Certificates

Attribute certificates are used to convey a set of attributes along with a public key certificate identifier (i.e. a serial number and a public key certificate issuer name) or entity name. The attributes are placed in a separate structure to maintain conformance with existing international standards (X.509). An entity may have multiple attribute certificates associated with each of its public keys certificates. X9.57, developed by the American Bankers Association (ABA) and adopted by ANSI, also defines an attribute certificate which is complimentary to the X.509 certificate. There is no requirement that the same authority create both the public key certificate and the attribute certificate; in fact, role separation should frequently dictate otherwise. The generation of an attribute certificate may be requested by an entity other than the subject of the attribute certificate. The X9.57 standard does not define the messages between an entity and the attribute authority (AA) dealing with the generation of the attribute certificate.

X9.57 defines an attribute as information, excluding the public key, which is provided by an entity or an AA and certified by the AA in an attribute certificate. Attributes are bound to a public key certificate or entity name by the signature of the AA on the attribute certificate.

The AttributeCertificate matching rule was created to allow more complex matching than the certificateExactMatch (a matching rule defined in X.509). It allows comparison to the issuer's serialNumber, the owner, the issuerName, and the validity. Refer to X.509 for further information on the matching rules.

The information contained in the attribute certificate is shown in Table D.1.

Table D.1 - Information Contained in the Attribute Certificate

Field	Description
Version	This identifies the version of the attribute certificate.
serial Number	This field uniquely identifies this certificate among all those issued by the AA. (if the AA is also a CA, the serial number space is thus shared by the public key certificates and the attribute certificates.)
owner	An attribute certificate may be linked to either a particular entity, or one of that entity's public key certificates. The mechanism to be used is specified by the application or standard which uses the attribute certificate.
IssuerName	This field contains the name of the issuer of the attribute certificate (an AA).
Issuer Unique Identifier	This field uniquely identifies the issuer, in the case where the issuer name is not sufficient.
Validity	This specifies when a certificate is valid. The period is described by a start date and time and an end date and time as follows: notBefore: The start time that the certificate is valid. notAfter: The end time that the certificate is valid.
Attributes	The attributes are information concerning the entity, or the certification process. They may be supplied by either the entity, a third party entity or the AA depending upon the application.
Extension(s)	The extensions field allows addition of new fields to the attribute certificate without modification of the ASN.1 definition.
SignatureAlgorithm	This field identifies the algorithm used to sign the certificate.
Signature	The signature field consists of: The output of the signing function (i.e. the signed hash value of the data in this certificate). This data is used to verify the data in the certificate.

D.2 Attribute Certificate Advantages/Disadvantages

Attribute certificates are essentially X.509 certificates without public key information (alternatively one can perceive them as extended certificates without the X.509 certificate embedded into them.) They are intended to compliment the X.509 certificate with additional information about the user (subject). This would give the same advantages and disadvantages as the PKCS#6 certificate with the additional benefits and disadvantages listed below:

Advantages:

- Mutual verification, via a challenge response, can be performed between the holder of the attribute certificate and the user authenticator prior to sending the attribute information.
- The attribute information can be encrypted, providing access to the confidential information to verified authenticators only.

- Information can be separated into as many attribute certificates as needed by the system. This may be useful in meeting the "need to know" requirement of many systems.
- Anonymity can be accommodated if the Distinguished Name (DN) of the user's X.509 certificate is a reference, not an actual identity (i.e. a user number, database lookup, etc.). The DN can be used to match attribute certificates with X.509 certificates.
- Attribute certificates are becoming standardized (as with X.509).

Disadvantages:

- Introducing multiple attribute authorities into the system architecture makes the system more complex. Key management issues may be prevalent.
- User authentication processing time may be an issue if two signatures must be verified, and the attribute certificate needs to be decrypted.

D.3 X.509 Attributes

X.509 imports the attribute definition from X.501. The X.501 defined attribute (that is AttributeTypeandValue) is as follows:

```
AttributeTypeandValue ::= SEQUENCE
    type   ATTRIBUTE.&id ({SupportedAttributes});
    value ATTRIBUTE.&Type({SupportedAttributes}{@type})}
```

All attributes are assigned an identifier using an object type of id-at. Any registered attribute, assigned a unique identifier by an ISO recognized standards body, can be used. X.520 is a source for ISO defined attributes; however, many other standards bodies have registered attributes which may used.

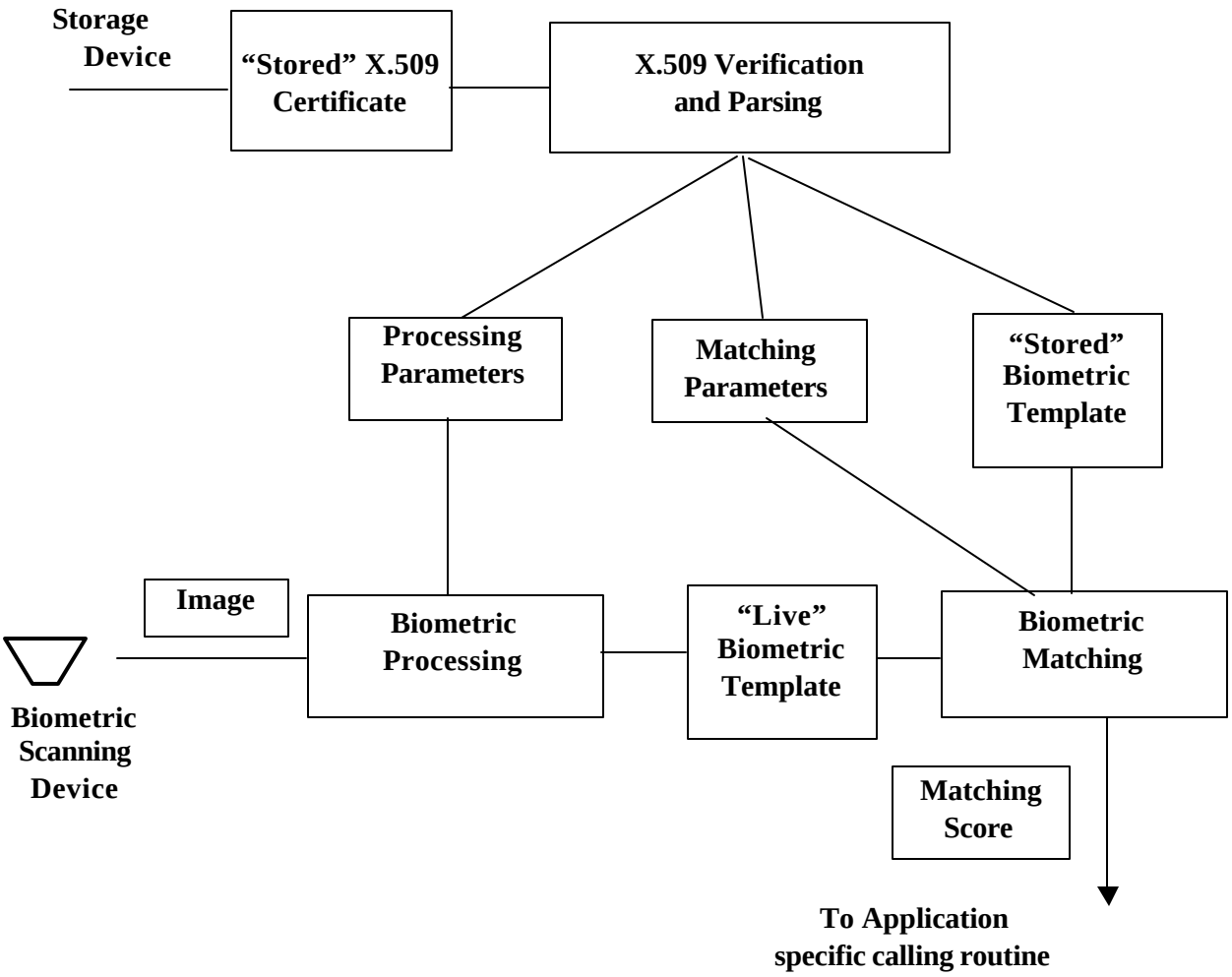
The CBEFF Object (the SBH) , as defined in this publication, can be used as an Attribute.The Biometric information can be placed in the CBEFF Object. The CBEFF Object can then be placed within the Attribute Certificate as detailed in the following sections. The X9.84 BSMB defintion will be used. The OID (From X9.84) is defined as follows:

```
X9-84-Biometrics {
      iso(1) identified-organization(3) tc68(133) country(16) x9(840)
            x9Standards(9) x9-84(84) module(0) biometrics(1) }
```

D.4. An Example Based Upon the X9.84's BSMB Definition

Figure D.1 illustrates how the biometric processing and matching parameters would be utilized during a biometric verification process.

Figure D.1 - Using an X.509 Certificate With Detailed Biometric Information



D.4.1 Optional Biometric Information

The need to identify this process is negligible from the Biometric Objects point of view, unless the process creating the livescan sample to compare against the certificate requires some customizing in regard to the individual who is being sampled.

The following X9.84 definition contains the information for such processing.

```
BiometricInfo ::= SEQUENCE SIZE(1..MAX) OF BioInformation

BioInformation ::= SEQUENCE {
                            processingInfo  [0] ProcessingInfo  OPTIONAL,
                            matchingInfo    [1] MatchingInfo
}
```

Biometric processing algorithms

The biometric processing information type specifies the processing algorithm used to create a given biometric template and any associated process specific parameters.

D.4.1.1 Processing Information

Biometric processing is the function which takes a biometric sample (typically a video image or an audio sample), extracts information from the sample (such as a location of the minutia in the fingerprint), and creates a output file (typically called a biometric template). The processing information field would be used to provide processing algorithm specific information which may be used to personalize the process for the individual. The algorithm used to create the biometric template is specified by the processingAlgorithmID. ProcessingAIDs is used to provide process specific parameters.

```
ProcessingInfo ::= SEQUENCE SIZE(1..MAX) OF ProcessingInformation

ProcessingInformation ::= SEQUENCE {
   id    BIOMETRIC.&name({ProcessingAIDs}),
   parms BIOMETRIC.&Type({ProcessingAIDs}{@id}) OPTIONAL
}
```

ProcessingAIDs BIOMETRIC ::= { ... }

The "processing" object identifier is the base identifier or root of a tree of biometric processing algorithms. It may also identify a default algorithm in contexts where interoperability is not required, or when it is necessary to identify biometric processing algorithms in general.

Processing OBJECT IDENTIFIER ::= { x9-84 algorithms(2) }

Examples of processing parameters may be:

Minimal Acceptable Quality: A minimum quality that the sample must have to be accepted for further processing (useful if the particular biometric can obtain preliminary quality ratings on a sample). This may relieve the need for users with poor biometric characteristics (such as a scarred finger) to reenter a biometric sample several times for verification.

Number of Samples: The number of samples that should be taken of the user which meet the MinimumAcceptableQuality threshold. This will also help users with poor biometric characteristics to avoid reentering a biometric sample several times.

D.4.1.2 Matching Information

Biometric matching is the function (algorithm) which takes two biometric templates and compares them for similarities. The output of the matching function is typically a matching score representing the amount of similarity found between the two templates.

The biometric templates are generally designed to work with a specific biometric matching algorithm. The application can reference the ID of the MatchingInfo in this field to determine compatibility.

```
MatchingInfo ::= SEQUENCE SIZE(1..MAX) OF MatchingInformation

MatchingInformation ::= SEQUENCE {
   id     BIOMETRIC.&name({MatchingAIDs}),
   parms  BIOMETRIC.&Type({MatchingAIDs}{@id}) OPTIONAL
}
```

MatchingAIDs BIOMETRIC ::= { ... }

The matching method object identifier is the base identifier or root of a tree of biometric matching functions (algorithms). It may also identify a default algorithm in contexts where interoperability is not required, or when it is necessary to identify matching functions (algorithms) in general.

Matching OBJECT IDENTIFIER ::= { x9-84 methods(3) }

Examples of Matching parameters may be:

Matching Algorithm: A Relative OID which specifies the Algorothm to be used for matching the processed image against a template.

Individual threshold: The minimum matching score required for the user. This may be a useful parameter for those users in which the particular biometric technology has a problem with verification.

D.4.2 Registering Biometric Processes

If this is the case, then the individual process creating the template needs to be registered by a recognized organization. The International Biometric Industry Association (IBIA) has agreed to be the organization which will manage the registration, issuance, and archiving of the OBJECT IDENTIFIERs and relative OBJECT IDENTIFIERs for Organizations and Vendors which require them.

D.4.2.1 Registering Biometric Processing or Matching Parameters

As stated above, biometric processes only need to be registered if there are associated parameters that need to be set. The individual processing parameters do not have to be registered as long as they are defined and maintained by the organization which registered the process. The processing parameters are associated with that particular OBJECT IDENTIFIER.

The application would be responsible for determining compatible versions. If the versions are incompatible, then the processing information may have to be rejected, and therefore the authentication process would have to fail.

Such parameters should and could be standardized to reduce the overhead for systems that want to incorporate multiple biometric devices. This is likely to happen in the future as biometric

technology matures, and could lead to accepted standard processing algorithms and matching methods being registered under X9.84 object identifiers for the industry by the IBIA.

D.4.3 User Verification

The certificate used to store the biometric information would be transferred to the entity performing the verification (from a database, smartcard, disk, etc.). The entity would verify the signature on the X.509 certificate to detect alteration and to prove the validity of the biometric template. The CBEFF object (the SBH) is a certificate and can be extracted from the certificate. The SBH is DER decoded using a commercial encode/decode engine. The Biomtric template and each of the processing/matching parameters can be extracted from the data returned from the engine.

The processing parameters are fed to the biometric processing function which converts the livescan image to a livescan biometric template. The livescan biometric template, the biometric template from the X.509 certificate and the matching algorithm parameters from the X.509 certificate are fed into the matching algorithm for verification of the user. The result of that operation should indicate the authenticity of the claimed identity of the user.

D.4.4 ASN.1 Authentication Attribute Certificate Definition

The attribute certificate that holds the authentication information attribute is described in ASN.1 as follows (see ISO/IEC 9594-8:1997):

```
AttributeCertificate ::= SIGNED {AttributeCertificateInfo}

AttributeCertificateInfo ::= SEQUENCE {
        version  Version DEFAULT v1,
        subject  CHOICE {
                 baseCertificateID[0]     IssuerSerial, -- associated with a
Public Key Certificate
                 subjectName[1]GeneralNames },  -- associated with a name
        issuer                            GeneralNames, -- CA issuing the
attribute certificate
        signature                         AlgorithmIdentifier,
        serialNumber             CertificateSerialNumber,
        attrCertValidityPeriod   AttCertValidityPeriod,
standardBiometic         SBH,
        issuerUniqueID           UniqueIdentifier OPTIONAL,
        extensions                        Extensions OPTIONAL}

IssuerSerial  ::= SEQUENCE {
        issuer           GeneralNames,
        serial                   CertificateSerialNumber,
        issuerUID                UniqueIdentifier OPTIONAL}

AttCertValidityPeriod ::= SEQUENCE {
        notBeforeTime    GeneralizedTime,
        notAfterTime     GeneralizedTime }
```

D.4.5. Approximate Certificate Data Size

An approximation of data sizes can be made on the following assumptions.

- The size of the signature and public key info is set at 512 bits (64 octets where 1octet = 1 byte).
- No extensions are used.
- Distinguished Encoding Rules (DER) are utilized by the CA signature certificates and user certificate.

Table D.2 shows the content of the Attribute Certificate.

Table D.2 – Contents of the Attribute Certificate - Identification & Authentication Certif.

Item	Item Size	Number of Items	Total Size
Version	5 octets	1	5 octets
Owner (baseCertificateID)	8 octets	1	8 octets
Issuer (AA)	183 octets	1	183 octets
Signature	9 octets	1	9 octets
SerialNumber	6 octets	1	6 octets
Validity	32 octets	1	32 octets
AuthenticationInfo - biometricInfo	500 octets	1	500 octets
IssuerUniqueID (Token Serial #)	16 octets	1	16 octets
AlgorithmIdentifier	9 octets	1	9 octets
SignatureValue	70 octets	1	70 octets
		Total	838 octets

If additional fields are added (such as extensions) the new field length needs to be added to the total.

Appendix E: Contacts and Liaisons

The CBEFF Technical Development Team includes the authors of this NIST IR. Contact information follows:

Fernando Podio, Information Technology Laboratory, National Institute of Standards and Technology
Co-Chair, Biometric Consortium
(301) 975-2947
fernando.podio@nist.gov

Jeffrey S. Dunn, Identification and Authentication Research Branch, National Security Agency
Co-Chair, Biometric Consortium
(301) 688-0276
Dunn@biometrics.org

Lawrence Reinert, Identification and Authentication Research Branch, National Security Agency
(301) 688-0278
lareine@alpha.ncsc.mil

Catherine J. Tilton, SAFLink Corporation
(703)-708-9280
ctilton@saflink.com

Lawrence O'Gorman, Veridicom
(973) 701-8700
log@veridicom.com

M. Paul Collier, The Biometric Foundation
301-990-9404
paulcollier@biometricfoundation.org

Mark Jerde, Biometric Solutions Division, ANADAC
703-741-7199 x 7143
jerdem@anadac.com

Brigitte Wirtz, Infineon Technologies
+49 89 2 34 - 4 16 34
Brigitte.Wirtz@infineon.com

Liaisons:

BioAPI Consortium:

Larry O'Gorman, Veridicom, Inc., 973-701-8700, log@veridicom.com

International Biometric Industry Association (IBIA):

M. Paul Collier, The Biometric Foundation, 301-990-9404, paulcollier@biometricfoundation.org

X9F4 Working Group:

Catherine J. Tilton, SAFLink Corporation, (703)-708-9280, ctilton@saflink.com

TeleTrusT:

Brigitte Wirtz, Infineon Technologies, +49 89 2 34 - 4 16 34, Brigitte.Wirtz@infineon.com

Biometric Consortium:

Fernando L. Podio	Jeffrey S. Dunn
NIST/ITL	NSA
(301) 975-2947	(301) 688-0276
Podio@biometrics.org	Dunn@biometrics.org

Other contacts

International Biometric Industry Association

Richard E. Norton, IBIA Executive 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 Format Owner/Type registrations: http://www.ibia.org/formats.htm)

Information about CBEFF and the Biometrics Interoperability, Performance, and Assurance Working Group:

Fernando L. Podio, NIST/ITL, Co-Chair Biometric Consortium, 100 Bureau Drive, Stop 8951, Gaithersburg, MD 20899-8951, (301) 975-2947, (301) 869-7429 (fax), Podio@biometrics.org
http://www.nist.gov/cbeff and http://www.nist.gov/bcwg