

Jeff Stapleton
Information Assurance Consortium

ABSTRACT

This paper provides a description of biometric standards dealing with management and security controls and an overview of the standards organizations that developed such biometric standards. The paper concludes that security is a primary requirement for any reliable biometric authentication system and provides a possible integration approach of the biometric standards.

1. INTRODUCTION

The American National Standard X9.84-2003 was developed by the X9F4 Cryptographic Protocol and Application Security working group, which operates under the auspices of the Accredited Standards Committee X9 Inc.

2. ORGANIZATIONS

National bodies such as the United States will use their own domestic standards when an international (ISO) standard is either not available or it conflicts with national practices. In many cases, a national standard is developed for a specific industry, such as financial services, when an existing standard is either too broad or incomplete for use in such an industry. This section provides an overview of the related organizations that develop or accredit standards developers.

The decision to rely upon a standard or a proprietary solution is a challenge to many businesses. The reliability of proprietary solutions is based upon the vendor's credibility, experience and stability. Standards are developed and peer reviewed by experts from the industrial, technical and business sectors; and a standard will outlast any one vendor.

The decision to rely upon an ISO or a domestic standard is often another challenge. The scope of one's business, domestic only or international, a specific industry segment or cross-industry markets, are contributing decision factors. Further, the market acceptance, maturity, and applicability of any standard are other contributing decision factors.

Figure 1 - Standards Organizations shows the relationships between groups developing biometric standards.

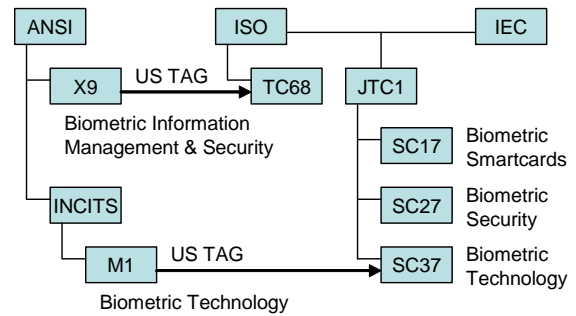


Figure 1 - Standards Organizations

2.1 ISO

ISO¹ is a non-governmental network of the national standards institutes of 157 countries, on the basis of one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. ISO is made up of its members who are divided into three categories:

- A *member body* of ISO is the national body "most representative of standardization in its country". Only one such body for each country is accepted for membership of ISO.
- A *correspondent member* is usually an organization in a country which does not yet have a fully-developed national standards activity.
- *Subscriber membership* has been established for countries with very small economies.

Many think "ISO" is an acronym, but it is not, rather ISO is its name. Because "International Organization for Standardization" would have different abbreviations in different languages ("IOS" in English, "OIN" in French for *Organisation internationale de normalisation*), it was decided at the outset to use a word derived from the Greek isos, meaning "equal". Therefore, whatever the country, whatever the language, the short form of the organization's name is always ISO.

Technical Committee 68 Financial Services develops standards and technical reports in the field of banking, securities and other financial services. Specifically, working group 10 in subcommittee 2 (TC68/2/10) is developing ISO 19092 Biometric Information Management and Security based on the US submission of the American National Standard X9.84 Biometric Information Management and Security.

¹ www.iso.org

2.2 JTC1

ISO and the International Electrotechnical Commission (IEC) established the Joint Technical Committee One (JTC1)² for developing information technology standards. ISO/IEC JTC1 develops generic standards that are agnostic to industry segments unlike the ISO technical committees. JTC1 operates under a slightly different set of rules than ISO, but similarly recognizes national standards bodies as members. The development of biometric standards has been segregated into three JTC1 subcommittees: SC17, SC27 and SC37.

- Subcommittee 17 Cards and Personal Identification is responsible for standardization in the area of identification and related documents, cards, and devices associated with their use in inter-industry applications and international interchange. Biometric standardization related to smart cards has also been assigned to SC17.
- Subcommittee 27 Information Technology (IT) Security Techniques is responsible for standardization of generic methods and techniques for IT security. This includes identification of generic requirements (including requirements methodology) for IT system security services; development of security techniques and mechanisms (including registration procedures and relationships of security components); development of security guidelines (e.g., interpretative documents, risk analysis); and development of management support documentation and standards (e.g. terminology and security evaluation criteria). Excluded is the embedding of mechanisms in applications. Biometric standardization for security techniques has also been assigned to SC27.
- Subcommittee 37 Biometrics is responsible for standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects. Excluded is the work in ISO/IEC JTC 1/SC 17 to apply biometric technologies to cards and personal identification; and the work in ISO/IEC JTC 1/SC 27 for biometric data protections techniques, biometric security testing, evaluations, and evaluations methodologies.

² www.jtc1.org

2.3 ANSI

The American National Standards Institute³ (ANSI) coordinates the development and use of voluntary consensus standards in the United States and represents the needs and views of U.S. stakeholders in standardization forums around the globe. ANSI is the official U.S. representative to ISO, the International Electrotechnical Commission (IEC), ISO/IEC JTC1 and a member of the International Accreditation Forum (IAF). ANSI itself does not develop standards; rather it accredits other US domestic organizations such as ASC X9 and INCITS as standards developers.

2.4 ASC X9

The Accredited Standards Committee X9⁴ (ASC X9), accredited by ANSI, has the mission to develop, establish, maintain, and promote standards for the Financial Services Industry in order to facilitate delivery of financial services and products. Under this mission ASC X9 fulfills the objectives of supporting existing standards, facilitates the development of new standards based upon consensus, and participates in and promotes the development of international (ISO) standards.

ASC X9 operates under its own procedures as well as those prescribed and approved by the American National Standards Institute. Presently, ASC X9 operates 5 technical subcommittees and 20-to-30 technical working groups that develop financial industry technical standards and guidelines. ASC X9 is the USA Technical Advisory Group (TAG) to the International Technical Committee on Financial Services (TC68) under the International Organization for Standardization (ISO), of Geneva, Switzerland. In this role, X9 holds the USA vote on all ISO standards of TC68 and its subcommittees.

- X9.84-2001 Biometric Information Management and Security was developed by the X9F4 Cryptographic Protocol and Application Security working group in cooperation with the BioAPI Consortium and the Biometric Consortium and published in January 2001 prior to the establishment of INCTIS M1 or JTC1 SC37.
- X9.84-2003 Biometric Information Management and Security was revised by X9F4 three years before its mandatory 5-year review to incorporate the OASIS XCBF standard, multiple biometric records based on public comments received from NIST after the original 2001 publication date, tightened up the False Non-Match error rates, Matching and Identification requirements.

X9.84-2001 was originally submitted to ISO TC68 in 2002 for its fast-track standardization process as a Draft International Standard (DIS) but was defeated

³ www.ansi.org

⁴ www.x9.org

by several European countries citing that the work was not specific to TC68 and belonged in JTC1 SC27. Later, X9.84-2003 was resubmitted to ISO TC68 in 2004 as an entry level Working Draft (WD) which was approved as new project ISO 19092 and assigned to working group 10 (WG10) under subcommittee 2 (SC2) in TC68 despite receiving similar comments.

2.5 INCITS

From 1961 - 1996, INCITS⁵ was known as Accredited Standards Committee X3 Information Technology. It was established within a year of ISO TC97 and ECMA as the U.S standards committee for information technology. X3 was accredited by ANSI and it was sponsored in 1961 by the Information Technology Industry (ITI) Council, a trade association then known as the Computer and Business Equipment Association (CBEMA). CBEMA was a forum for companies to identify and discuss areas of common concern, and its sponsorship of X3 provided a place for the providers of information technology and systems to receive feedback from users, government agencies, academia and other interested parties. The last accreditation was in April 2001 under the name INCITS, whose stated mission is to promote the effective use of Information and Communication Technology through standardization in a way that balances the interests of all stakeholders and increases the global competitiveness of the member organizations.

The Executive Board of INCITS established Technical Committee M1, Biometrics, in November 2001 to ensure a high priority, focused, and comprehensive approach in the United States for the rapid development and approval of formal national and international generic biometric standards. The M1 program of work includes biometric standards for data interchange formats, common file formats, application program interfaces, profiles, and performance testing and reporting. The goal of M1's work is to accelerate the deployment of significantly better, standards-based security solutions for purposes, such as, homeland defense and the prevention of identity theft as well as other government and commercial applications based on biometric personal authentication. M1 also serves as the USA Technical Advisory Group (TAG) to ISO/IEC JTC1/SC37 on Biometrics, which was established in June 2002. As the USA TAG to SC37, M1 is responsible for establishing USA positions and contributions to SC37, as well as representing the USA at SC37 meetings.

M1 has been rather prolific producing a myriad of biometric standards over a four year period, including:

- INCITS 358:2002 Information technology - BioAPI Specification

⁵ www.incits.org

- INCITS 377:2004 Information technology - Finger Pattern Based Interchange Format
- INCITS 378:2004 Information technology - Finger Minutiae Format for Data Interchange
- INCITS 379:2004 Information technology - Iris Image Interchange Format
- INCITS 381:2004 Information technology - Finger Image Based Interchange Format
- INCITS 383:2004 Information technology - Application Profile - Interoperability and Data Interchange - Biometric Based Verification and Identification of Transportation Workers
- INCITS 385:2004 Information technology - Face Recognition Format for Data Interchange
- INCITS 394:2004 Information technology - Application Profile for Interoperability - Data Interchange and Data Integrity of Biometric Based Personal Identification for Border Management
- INCITS 395:2005 Information technology - Biometric Data Interchange Formats - Signature/Sign Data
- INCITS 396:2005 Information technology - Hand Geometry Format for Data Interchange
- INCITS 398:2005 Information technology - Common Biometric Exchange Formats Framework (CBEFF)
- INCITS 409.1:2005 Information technology - Biometric Performance Testing and Reporting - Part 1: Principles and Framework
- INCITS 409.2:2005 Information technology - Biometric Performance Testing and Reporting - Part 2: Technology Testing and Reporting
- INCITS 409.3:2005 Information technology - Biometric Performance Testing and Reporting - Part 3: Scenario Testing and Reporting
- INCITS 409.4:2006 Information technology - Biometric Performance Testing and Reporting - Part 4: Operational Testing Methodologies

M1 is primarily focused on biometric technology as is ISO/IEC JTC1 SC37.

2.6 IETF

The Internet Engineering Task Force⁶ (IETF) is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The IETF Mission Statement is documented in RFC 3935. The

⁶ www.ietf.org

IETF is not affiliated with ISO or ANSI, rather the IETF is a self-accredited standards body, although it is internationally well recognized. Individuals from any company and any country can be a member of the IETF.

- RFC 2630 Cryptographic Message Syntax (CMS) was originally published in June 1999.
- RFC 3211 Password-based Encryption for CMS was developed in December 2001.
- RFC 3369 Cryptographic Message Syntax (CMS) was published in August 2002 which obsoletes RFC 2630 and RFC 3211; and RFC 3370 Cryptographic Message Syntax (CMS) Algorithms was also published in August 2002.
- RFC 3852 Cryptographic Message Syntax (CMS) was published in July 2004 which obsoletes RFC 3369.

CMS describes an encapsulation syntax for data protection, supporting digital signatures and encryption with various key management schemes. The syntax allows multiple encapsulations; one encapsulation envelope can be nested inside another. Likewise, one party can digitally sign some previously encapsulated data. It also allows arbitrary attributes to be signed along with the message content, and provides for other attributes to be associated with a digital signature.

CMS employs object identifiers (OID) to identify cryptographic algorithms used for encryption, digital signatures, message authentication codes (MAC) and various key management schemes including key transport and key agreement. Algorithms include DES, Triple DES, AES, RSA, Diffie-Hellman (DH) and Elliptical Curve Cryptography (ECC).

ASC X9 standardized the RFC 3369 specification in X9.73 Cryptographic Message Syntax and in X9.96 XML Cryptographic Message Syntax. Further, the ISO TC68/2/14 working group is reviewing RFC 3852 and consolidating the US submissions X9.73 and X9.96 into ISO 22895 Financial Services – Security – Cryptographic Syntax Scheme.

2.7 OASIS

The Organization for the Advancement of Structured Information Standards (OASIS)⁷ is a not-for-profit, international consortium that develops XML and Web services standards. Founded in 1993, OASIS boasts more than 5,000 participants representing over 600 organizations and individual members in 100 countries with almost 100 technical committees.

The OASIS XML Common Biometric Format (XCBF) Technical Committee developed the XCBF 1.1 is an

⁷ www.oasis-open.org

OASIS Standard in 2003. XCBF 1.1 defines a common set of secure XML encodings for the patron formats specified in CBEFF (NISTIR 6529). These XML encodings are based on the ASN.1 schema defined in ANSI X9.84. They conform to the XML Encoding Rules (XER) for ASN.1 defined in ITU-T Recommendation X.693, and rely on the security and processing requirements specified in X9.96 XML Cryptographic Message Syntax (XCMS).

2.8 BIOAPI CONSORTIUM

The BioAPI Consortium⁸ was founded in 1998 to develop a biometric Application Programming Interface (API) that brings platform and device independence to application programmers and biometric service providers. The BioAPI Consortium developed a specification and reference implementation for a standardized API that is compatible with a wide range of biometric application programs and a broad spectrum of biometric technologies:

- BioAPI Specification Version 1.0 was released in March, 2000; and the Reference Implementation was released in September 2000.
- BioAPI Specification Version 1.1 and the Reference Implementation were released in March, 2001.
- BioAPI Specification Version 1.1 was submitted to INCITS M1 and approved as American National Standard ANSI/INCITS 358-2002.
- BioAPI Specification Version 2.0 was submitted to JTC1/SC37 and approved as ISO ISO/IEC 19784-1 in 2005.

2.9 BIOMETRIC CONSORTIUM

The Biometric Consortium⁹ serves as a focal point for research, development, testing, evaluation, and application of biometric-based personal identification and verification technology. It is jointly chaired by NIST and the NSA.

2.10 NIST

The National Institute of Standards and Technology¹⁰ (NIST) has had several names. Founded as the National Bureau of Standards in 1901, it was renamed Bureau of Standards in 1933 and in 1934, the word “national” was reattached to its name. For more than 50 years it remained the National Bureau of Standards (NBS), but became the National Institute of Standards and Technology (NIST) in 1988.

NIST carries out its mission in four cooperative programs: NIST Laboratories; the Baldrige National

⁸ www.bioapi.org

⁹ www.biometrics.org

¹⁰ www.nist.gov

Quality Program; the Manufacturing Extension Partnership and the Advanced Technology Program.

One of the NIST Laboratories areas is the Information Technology Laboratory (ITL). NIST ITL is organized into several research areas, including: Math, Networking, Computer Security, Information Access, Software Testing, and Statistics. The mission of the Computer Security Division (CSD) is to improve information systems security by:

- Raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies;
- Researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive Federal systems;
- Developing standards, metrics, tests and validation programs.
- Developing guidance to increase secure IT planning, implementation, management and operation

NIST ITL CSD¹¹ developed the Common Biometric Exchange File Format (CBEFF). 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 to promote interoperability of biometric-based application programs and systems developed by different vendors by allowing biometric data interchange.

- CBEFF v1.0 was published by NIST in January 2001 as NISTIR 6529.
- CBEFF v1.1 was published by NIST three years later in 2005 as NISTIR 6529-A.
- CBEFF v1.1 was standardized and published by the INCITS M1 Committee later that same year as ANSI INCITS 398-2005.
- CBEFF v2.0 was internationalized and published by JTC1/SC37 as ISO/IEC 19785 Part 1 another year later in 2006.

NIST ITL CSD also developed the Federal Information Processing Standards Publication (FIPS PUB) 201 Personal Identification and Verification for Federal Employees and Contractors (PIV). This standard defines a government-wide PIV system for use in applications such as access to Federally controlled facilities and information systems. The standard contains two major sections. Part one describes the minimum requirements for a Federal

personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive 12, including personal identity proofing, registration, and issuance. Part two provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard.

- The interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in Special Publication 800-73 Interfaces for Personal Identity Verification.
- The interfaces and data formats of biometric information are specified in Special Publication 800-76 Biometric Data Specification for Personal Identity Verification.

Biometric data representation and protection rely on CBEFF and the digital signature representation relies on the IETF specification RFC 3258 Cryptographic Message Syntax (CMS).

3. BIOMETRIC APPLICATIONS

X9.84 provides a biometric framework and identifies three biometric applications using the framework: verification, identification and enrollment. Figure 2 - Biometric Framework shows the five components that interact either within a physically secure boundary or across an unsecured Transmission media:

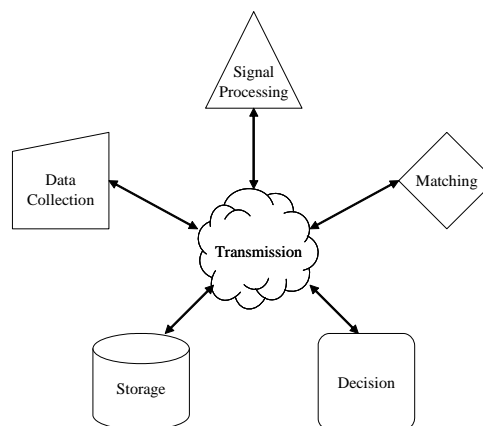


Figure 2 - Biometric Framework

- Data Collection is the component that contains the input device or sensor that reads the biometric information from the user and converts it to a form suitable for processing.
- Signal Processing is the component that receives the raw biometric data from the Data Collection

¹¹ <http://www.itl.nist.gov/div893/biometrics>

subsystem, and transforms that data into the form required by the Matching subsystem.

- Matching is the subsystem that receives the processed biometric data from the signal processing subsystem and compares it with the biometric template from the storage subsystem.
- Storage is the component that maintains the templates for the enrolled users. It provides for the addition, deletion and retrieval of an enrolled template (or templates) as needed by the matching subsystem
- Decision is the component that receives a score from the Matching subsystem, and using a confidence value based on business risks and risk policy, interprets the results of the score.

Figure 3 – Biometric Verification shows the five components interacting to create a biometric authentication system based on a claimed identity. Data Collection captures the raw unprocessed biometric sample and passes it to Signal Processing. Signal Processing transforms the raw biometric data into appropriate processed data and passes it to Matching. Matching retrieves the biometric template (previously created by Enrollment) from Storage based on the user's claimed identity, compares it against the live sample and passes the score to Decision. Decision evaluates the score based on a threshold parameter and passes the result (Yes or No) to an Application. Decision may also determine that the biometric template needs to be updated (represented by the dotted line) and adapts it based on the processed format.

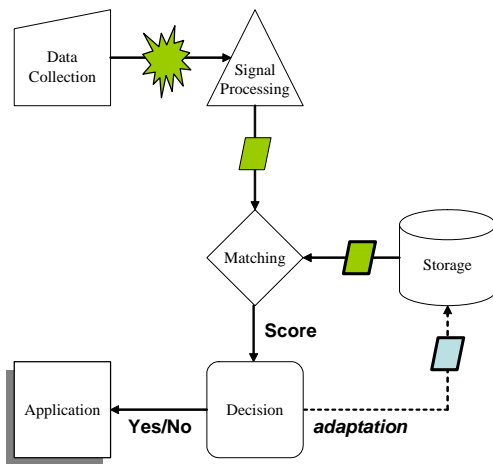


Figure 3 – Biometric Verification

Figure 4 - Biometric Identification shows the five components interacting to create a biometric authentication system without a claimed identity. Data Collection and Signal Processing operate the same as in Figure 3. Matching compares the live sample to every biometric template in Storage and

passes a candidate list to Decision based on a threshold parameter. Decision evaluates the candidate list based on a threshold parameter and passes a verified identity to an Application.

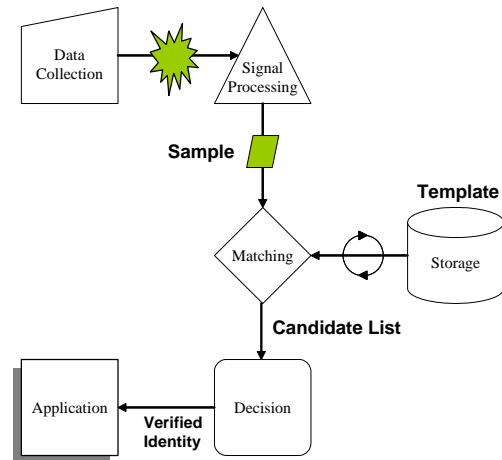


Figure 4 - Biometric Identification

Figure 5 - Biometric Enrollment shows four of the components interacting for the enrollment process. Data Collection and Signal Processing operate similarly as in Figure 3 and Figure 4 to produce the template that will be stored in Storage for subsequent Verification or Identification. For some enrollment processes the system will also perform Identification similar to Figure 4 to ensure that the enrollee has not been previously enrolled.

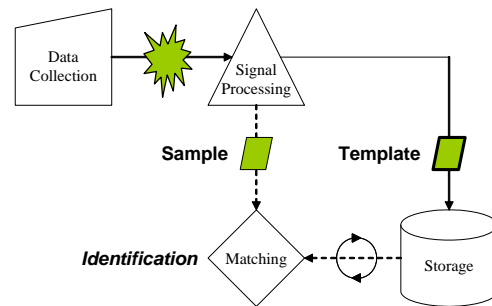


Figure 5 - Biometric Enrollment

In contrast, as shown in Figure 6 - BioAPI Specification (version 2.0) provides a multi-layered process stack that unlike the X9.84 framework is assumed to run as a single instance on a single platform without unsecured transmission in between any of its components.

- The BioAPI Application layer is equivalent to the X9.84 Application component.
- The BioAPI Matcher component is equivalent to the X9.84 Matcher component.
- The BioAPI Sensor components are equivalent to the X9.84 Data Collection components, and the

X9.84 Signal Processing would most likely be handled in the BioAPI BSP or BFP depending on the provider's hardware and software configuration.

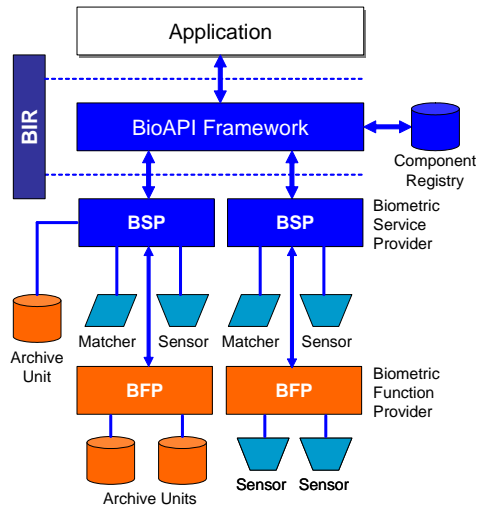


Figure 6 - BioAPI Specification

- The BioAPI Archive Units are equivalent to the X9.84 Storage component.
- The BioAPI Biometric Information Record (BIR) is equivalent to the X9.84 Biometric Object discussed in §5 Biometric Security.

The BioAPI Specification is primarily a biometric technology standard with a bit of security mentioned whereas X9.84 is primarily a biometric security standard with enough of a technology framework to provide sufficient context.

4. SECURITY REQUIREMENTS

X9.84 specifies three core requirements that apply to all applications and environments wherever biometric information is used, as follows:

1. Mechanisms shall be in place to maintain the integrity of biometric data and verification results between any two components.

The modification of biometric data or verification results could enable an inadvertent or adversarial false match or false non-match to occur within the biometric authentication system.

2. Mechanisms shall be in place to mutually authenticate the source and destination of the biometric data and verification results, between the sender and receiver component.

The substitution of biometric data or verification results could enable an inadvertent or adversarial

false match or false non-match to occur within the biometric authentication system.

3. If desired, mechanisms may be in place to ensure the confidentiality of the biometric data between any two components and within any component.

The unauthorized disclosure of biometric data or verification results could violate privacy rules. The confidentiality of biometric data is an unnecessary prerequisite because unlike PINs or passwords biometric data is not secret. Biometric data is easily captured, such as latent fingerprints, voice recordings, photographs and the like. Therefore a biometric authentication system cannot rely on the secrecy of such data when it is in fact not secret.

The mechanisms must be either cryptographic techniques such as digital signature, message authentication code, and encryption wherever transmission is involved; or physical protection where no transmission is involved and all components reside within the same tamper resistant unit.

X9.84 also requires authentication and authorization controls for enrollment and specifies false match and false non-match error rates for verification and identification. A false match occurs when a person is erroneously accepted. A false non-match occurs when a person is erroneously rejected. Further, X9.94 specifies the security levels required for the matching component based on the NIST FIPS 140-2 Security Requirements for Cryptographic Modules.

5. BIOMETRIC SECURITY

X9.84 specifies data encoding techniques with cryptographic mechanisms to achieve the integrity, authentication and privacy requirements to protect biometric information. Figure 7 - Biometric Object shows the basic building block used in the encoding techniques. The biometric object consists of a biometric header and the biometric data.

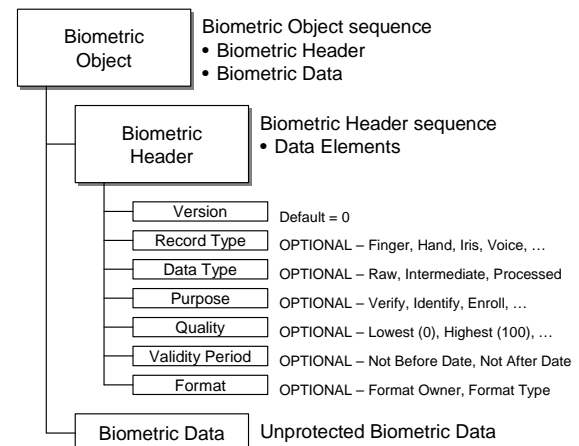


Figure 7 - Biometric Object

The biometric header is equivalent to the Biometric Information Record (BIR) specified in ANSI/INCITS 358 BioAPI Specification with several significant advantages:

- X9.84 defines data objects using Abstract Syntax Notation One (ASN.1) with self-defining variable length data elements. In contrast the BioAPI Specification uses fixed length fields.
- X9.84 supports an XML schema using the XML Encoding Rules (XER). In contrast the BioAPI Specification and CBEFF do not support XML.
- X9.84 allows optional data elements such that unnecessary fields can be eliminated from the biometric header. In contrast the BioAPI Specification requires that all fields be present in the header regardless of system redundancy.

Not that optional Standard Biometric Header (SBH) fields was added to CBEFF v1.1 in 2005, two years after the revised X9.84-2003 was published.

- Signature consists of the digital signature value and an algorithm identifier for the hash and signature algorithms used to generate the digital signature.
- Message Authentication Code (MAC) consists of the MAC value, an algorithm identifier for the MAC (or Keyed Hash MAC) algorithm used, and a key name to identify the symmetric key used to generate the MAC value.
- Signed Data is a more complicated structure providing a list of certificates; certificate revocation lists (CRL) and signer information allowing digital signatures for multiple receivers.
- Authenticated Data is also a more complicated structure providing the MAC value, an algorithm identifier, and recipient information to convey the symmetric key to one or more receivers.

Regardless of the integrity method chosen, the cryptographic integrity value is calculated over the entire Biometric Object providing integrity of the Biometric Header and the Biometric Data.

In contrast, BioAPI and CBEFF offer a single field labeled as a digital signature without the benefit of any key management material, basically making the digital signature ineffectual. The hash algorithm, the digital signature algorithm and key length are not conveyed in the Biometric Information Record (BIR) rendering the digital signature unverifiable by the relying party which negates the data integrity.

CBEFF v1.1 states if the CBEFF record has integrity applied to it, either via MAC (Message Authentication Code) or digital signature, then the SBH [Standard Biometric Header] shall be included in the data covered by the MAC or signature.

FIPS 201 states that the biometric data is prepended with a CBEFF header and appended with the CBEFF signature block, and redefines the CBEFF signature block as encoded as a CMS SignedData based on RFC 3852. Essentially, FIPS 201 published in 2005 ignores the American National Standard X9.84 and reinvents the X9.84 Integrity Object that was already published 5 years earlier in 2001.

5.1 INTEGRITY

Figure 8 - Integrity Object shows the X9.84 technique for providing a cryptographic based integrity control over the Biometric Object. The Integrity Object consists of two elements, the Biometric Object and the Integrity Block. The Biometric Object is composed of the Biometric Header and the Biometric Data. The Integrity Block is a CMS-based structure providing a choice of a digital signature, a Message Authentication Code (MAC), Signed Data or Authenticated Data.

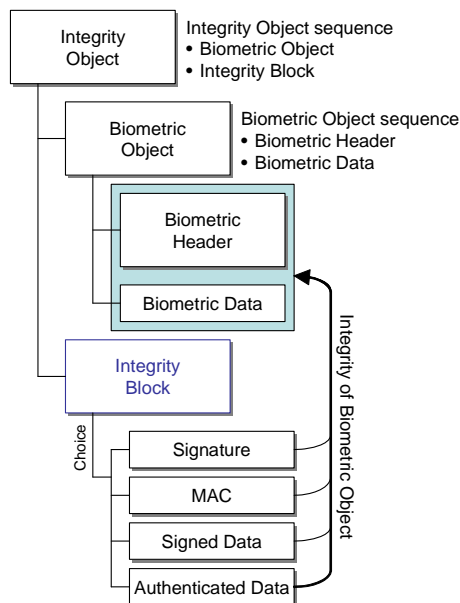


Figure 8 - Integrity Object

5.2 PRIVACY

Figure 9 - Privacy Object shows the X9.84 technique for providing a cryptographic based privacy control over the Biometric Object. The Privacy Object consists of the Privacy Block and an optional Biometric Header echoed from the Privacy Block. The Privacy Block is a CMS-based structure providing a choice of Fixed Key, Named Key, or Established Key encryption methods.

- Fixed Key consists only of the Encrypted Data with the presumption that an encryption has been previously established and is implicit to the biometric authentication system.
- Named Key consists of the Encrypted Data and a Key Name field that explicitly identified. The Named Key field allows a system to periodically change the encryption key but retain synchronization for each Privacy Object.
- Established Key is a CMS Enveloped Data object consisting of the Encrypted Data, a Version number for change control, Originator Info and the Recipient Info. The Originator Info and the Recipient Info allow public key certificates and other information to be exchanged for establishing the encryption key either by key transport (e.g. RSA) or key agreement (e.g. DH or ECC).

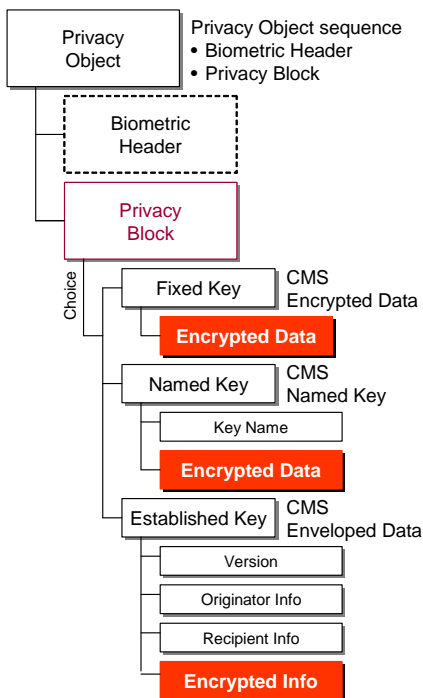


Figure 9 - Privacy Object

Figure 10 - Encrypted Data shows that the Encrypted Data object contains the Biometric Object consisting of the Biometric Header and the Biometric Data. The Biometric Header is encrypted along with the Biometric Data to prevent substitution attacks. As noted above the Biometric Header can optionally be echoed in the Privacy Object for easier processing, however the unencrypted header should always be verified against the decrypted header.

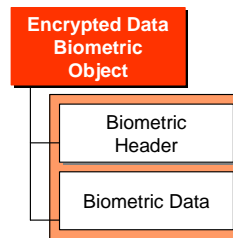


Figure 10 - Encrypted Data

In contrast, BioAPI does not support encryption. CBEFF v1.1 added Integrity only, Privacy only, and Privacy and Integrity options in 2005, two years after the revised X9.84-2003 was published. However, CBEFF v1.1 states that the SBH [Standard Biometric Header] 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 [Biometric Data Block] may be encrypted or not, as required by the Patron Format.

5.3 INTEGRITY AND PRIVACY

Figure 11 - Integrity and Privacy Object shows the X9.84 technique for combining the Integrity Object and the Privacy object. The Integrity and Privacy object consists of the Integrity Block, the Privacy Block and the optional Biometric Header.

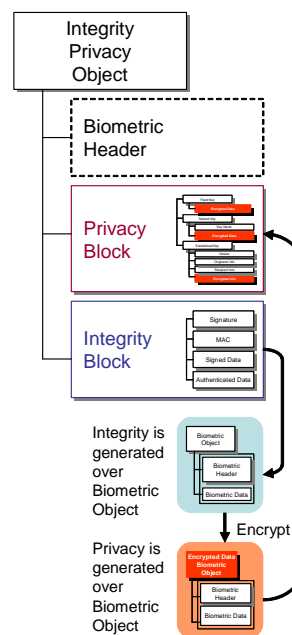


Figure 11 - Integrity and Privacy Object

The Integrity Block is first generated from the Biometric Object and then the Biometric Object is encrypted to create the Privacy Block. To process the Integrity and Privacy Object, the Biometric Object is first recovered from the Privacy Block, and then the Integrity Block is used to verify the recovered Biometric Object.

5.4 SYNTAX SETS

X9.84 also supports multiple sets of biometric data, named Biometric Syntax Set. Figure 12 - Biometric Syntax Set shows a set as one or more instances of a Biometric Syntax object where each syntax object is a choice of a Biometric Objects, Integrity Objects or Privacy Objects.

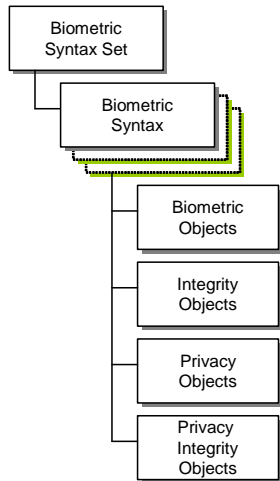


Figure 12 - Biometric Syntax Set

Figure 13 - Biometric Objects shows the structure is simply one or more instances of a Biometric Object such that each Biometric Data object has its own Biometric Header.

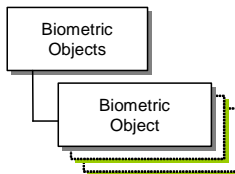


Figure 13 - Biometric Objects

Figure 14 - Integrity Objects shows the structure consists of a Biometric Objects and a single instance of an Integrity Block such that the one or more instances of a Biometric Object within the Biometric Objects are protected by the Integrity Block.

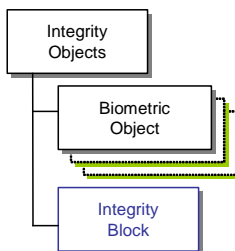


Figure 14 - Integrity Objects

Figure 15 - Privacy Objects shows the structure consists of optional Biometric Headers and a single

instance of a Privacy Block such the one or more instances of encrypted Biometric Objects are contained in the Privacy Block.

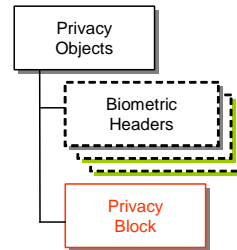


Figure 15 - Privacy Objects

Figure 16 - Integrity and Privacy Objects shows the structure consists of optional Biometric Headers, a single instance of an Integrity Block and a single instance of a Privacy Block. The one or more instances of encrypted Biometric Objects contained in the Privacy Block are protected by the Integrity Block.

To generate the Integrity and Privacy Objects, the Biometric Objects are first used to generate the Integrity Block and then the Biometric Objects are encrypted to create the Privacy Block. To process the Integrity and Privacy Objects, the Biometric Objects is first recovered from the Privacy Block, and then the Integrity Block is used to verify the recovered Biometric Objects.

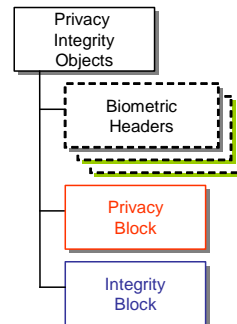


Figure 16 - Integrity and Privacy Objects

In contrast to X9.84, nested structures 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) was added to CBEFF v1.1 published in 2005 (two years after the X9.84-2003 revision).

Further, FIPS 201 mandates that all ten fingerprint records and a facial image record be pre-pended with a single CBEFF header and appended with the CBEFF signature block.

6. VALIDATION CONTROL OBJECTIVES

The goal of any organizations should be to meet or exceed industry standard practices when using

technology in a responsible manner by imposing proper controls. Compliance to policies, standards, and procedures can only be assured by verification of the controls via an *audit*. There are two primary types of security review audits: internal audits performed by an internal audit group or out-sourced to an external audit firm; and external audits performed by an independent third party, such as an accounting or audit firm. The control objectives provided in X9.84 represent recommended practices for business, operational, and technical use against which a time stamp entity may be evaluated or audited.

The control objectives and evaluation criteria in X9.84 are organized by IT environmental controls, key management controls, and time management controls. The evaluation criteria are organized into three broad categories: IT Environmental control objectives, Key Management control objectives, and Biometric Management control objectives. The control objectives and criteria are written in audit approved language and adapted from similar standards with comparable objectives and evaluation criteria:

- ANS X9.79-2001 PKI Policy and Practices Framework
- AICPA/CICA Webtrust for Certification Authority

Altogether there are eleven IT Environmental control objectives with 141 specific evaluation criteria statements; six Key Management control objectives with 61 evaluation criteria statements; and five Biometric Management control objectives with 128 evaluation criteria statements.

In contrast neither BioAPI, CBEFF or FIPS 201 provide any control objectives or evaluation criteria.

7. CONCLUSION

X9.84 and its planned successor ISO 19092 squarely address the management and security of biometric information, while other standards such as BioAPI and CBEFF focus primarily on biometric technology and interoperability with security as an afterthought. Security controls using cryptographic techniques need well defined requirements, techniques and validation control objectives to ensure a proper implementation using sound business practices. The INCITS M1 and JTC1 SC37 standards are important for the biometric industry at large to be interoperable, and should be developed with X9.84 and ISO 19092 security controls included in their scope.

X9.84 developed in ASC X9 and ISO 19092 being developed in TC68 originated in the financial services industry as many cryptographic based security standards are today, because the financial services industry is risk adverse and tends to be a leader in cryptographic security controls. There has been push back from several non-US standard developers who

have taken the position that biometric security is an IT issue not specific to the financial services industry and therefore should be developed in other standards organizations. However, to date no other standards organization has addressed security as a primary requirement except for the financial services industry.

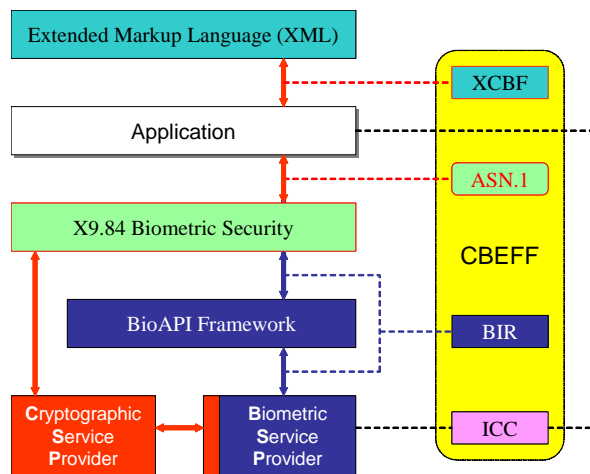


Figure 17 - Biometric Architecture

The question often is raised as to how the various standards might fit together. Figure 17 - Biometric Architecture provides a possible approach. The BioAPI framework platform implementation uses a Biometric Service Provider (BSP) to provide the specific biometric technology solution (e.g. fingerprint). The X9.84 framework could be a layer on top providing security and enabling biometric authentication components (e.g. Matching) on disparate platforms across unsecured transmission. Since X9.84 requires a Cryptographic Service Provider (CSP) and the BioAPI does not support a CPS, either the CSP would communicate directly with the X9.84 layer, or perhaps the BSP might provide a CSP interface. Regardless, the Application could then take advantage of the X9.84 security and the BioAPI for biometric authentication. Web based application might then use XML to use or provide biometric authentication services in a Services Oriented Architecture (SOA).