

White Paper:

Biometric Industry Standards

By Catherine J. Tilton
Chair, BioAPI committee

SAFLINK Corporation

Introduction

Is anything dryer than a talk (or paper) on standards? Although this topic is not as glamorous or exciting as the gee-whiz discussions about the technologies themselves, standards are one of the most critical elements to the long-term success of the biometrics market. Why? Because customers are slow to adopt a new technology for which their only choices are proprietary, point solutions – with their associated risks and lack of interoperability. Standards have become strategic business issues.

Since 1996, when the only biometric standards in existence were forensic fingerprint standards, the industry has made tremendous progress on the standards front. Not to say that there is not more work to do, but much has been accomplished in a relatively short amount of time. Several US national standards are now in place, others in progress, and new standards activities have sprung up this year.

Standards activities

Standards activities can be broken down into two categories – formal and informal. Formal standards organizations include ISO, the International Organization for Standardization, and national standards bodies, such as the American National Standards Institute (ANSI) in the US (as well as accredited organization thereof). Formal groups are well structured, with formal balloting rules and liaisons. Informal standards organizations are self-defined groups (such as consortia), which are generally technology driven. Although frequently legally chartered, they have a variety of membership and balloting rules, fees, and dues structures.

In June of 2002, ISO Joint Technical Committee 1 (JTC1), Information Technology, chartered a new sub-committee (SC) on biometrics, SC37. [1] This SC was formed to address generic biometric standards that cross application areas requiring identification and verification services. Specifically, the scope of work of SC37 includes the development of application programming interfaces, related application/implementation profiles, and data interchange formats, including biometric template standards.

The goal is to coalesce a wide range of interests in biometrics and make most efficient utilization of biometric experts. Rather than having biometric efforts scattered across various domain specific committees, with the possible effect of generating conflicting or duplicative standards, the biometric experts can cover a single committee and meeting schedule. SC37 plans to establish close liaison with other committees with an interest or work program related to biometrics – for example, SC17 (Cards and Personal Identification) and SC27 (IT Security Techniques).

The first meeting of SC37 is scheduled for December 02. As of 15 October, 16 countries have signed up for P-membership in SC37. A number of technical contributions have been submitted for consideration at this meeting.

In November of 2001, the International Committee for Information Technology Standards (INCITS) chartered a new technical committee (TC) on biometrics, M1, to ensure a high priority, focused, and comprehensive approach for the rapid development and approval of formal, generic biometric standards. [2] A goal of this new TC is to accelerate deployment of significantly better, open systems standards-based security solutions for purposes such as homeland defense and the prevention of identity theft.

INCITS serves as the secretariat of the US Technical Advisory Group (TAG) to ISO JTC1, and M1 was appointed the US TAG to ISO SC37.

Since it's first meeting in January of 2002, the M1 committee has chartered five ad-hoc working groups and approved eight new work item proposals (NPs) related to its core purpose. In addition to work items related to data interchange formats and application profiles, it is also working on others related to testing, quality, and vocabulary, and a study of the integration of biometrics within the (US) government smart card interoperability specification.

Standards summary

For purposes of discussion, the areas of biometric standards have been grouped into the following categories:

- Forensic and identification standards
- Data standards
- API standards
- Security standards
- Testing and certification standards and guidelines
- Other standards

Forensic and Identification Standards

Long before biometrics were being used for access control, fraud prevention, and other public and government applications, biometrics were used (sometimes in a more manual context) by law enforcement. In particular, fingerprints, facial photos (mug shots), signatures, and scars, marks, and tattoos (SMTs) were used in the identification of known criminals. As law enforcement agencies in the US and globally began to share this information, standards evolved for the format, quality, and transmission of this data. Other applications, such as national ID cards, generally reference the law enforcement standards since the requirements (i.e., large scale identification) are similar. Additionally, similar standards have evolved for drivers licensing and are evolving for border crossing/travel documents, such as passports.

Standards such as the following fall into this category:

ANSI/NIST ITL 1-2000, *Data Format for the Exchange of Fingerprint, Facial, and SMT Information*. This standard specifies record formats and quality requirements for fingerprint images, facial photos, and SMT data. [3]

CJIS/FBI IAFIS-IC-0110, FBI WSQ (Wavelet Scalar Quantization) standard for fingerprint image compression and decompression.

CJIS-RS-0010(v)7 FBI *Electronic Fingerprint Transmission Standard* (EFTS). [4] This standard provides message transmission requirements for submission of fingerprint data for search/match, including (in Appendices F and G), detailed image quality specifications.

AAMVA DL/ID-2000 *National Standard for the Drivers License/Identification Card*, issued by the American Association of Motor Vehicle Administrators. [5] This specification defines physical characteristics, security mechanisms, data elements to be printed/stored on the card, and encoding mechanisms, including biometric information (fingerprint image and minutiae, facial, and signature capture, quality, formatting, and compression requirements).

ANSI/INCITS B10.8. This sub-committee has issued or has in draft a number of standards related to identification cards, several of which relate to biometrics.

ISO JTC1 SC17, Cards and Personal Identification. This international group has been working on a number of standards that incorporate biometrics. These include WG3, which is working on machine readable travel documents; WG4, which is working on smart card standards, including 7816-11 (draft), *Information technology – Integrated circuit(s) cards with contacts – Part 11, Personal verification through biometric methods*; WG10, which is working on drivers licenses; and WG11, a new working group formed this year to address biometrics across the SC17 functional areas which is currently working on a logical data structure for biometric data.

Data Standards

Although several of the above standards relate to data formats, there are others that are more generic in nature.

In February of 1999, the National Institute of Standards and Technology (NIST) hosted a meeting to look into the possibility of a common template standard. Although the participants failed to agree on this subject, they did agree on a standard method of packaging the biometric data. That agreement evolved into an effort and specification known as CBEFF – the Common Biometric Exchange File Format. [6] This specification was developed by a technical development team under the NIST/BC (Biometric Consortium) Biometric Interoperability,

Performance, and Assurance Working Group (BCWG) and was published as a NIST report, NISTIR 6529 in January of 2001.

CBEFF defines the basic structure of a biometric data record, consisting of a standard header, a biometric specific memory block (BSMB), and an optional digital signature. The header consists of a set of mandatory and optional data elements. Among the mandatory fields are the Format Owner and Format Type fields, which uniquely identify the specific format of the biometric data contained in the subsequent BSMB. To ensure uniqueness of values, the International Biometric Industry Association (IBIA) acts as the CBEFF registration authority [7]. Figure 1 portrays this structure.

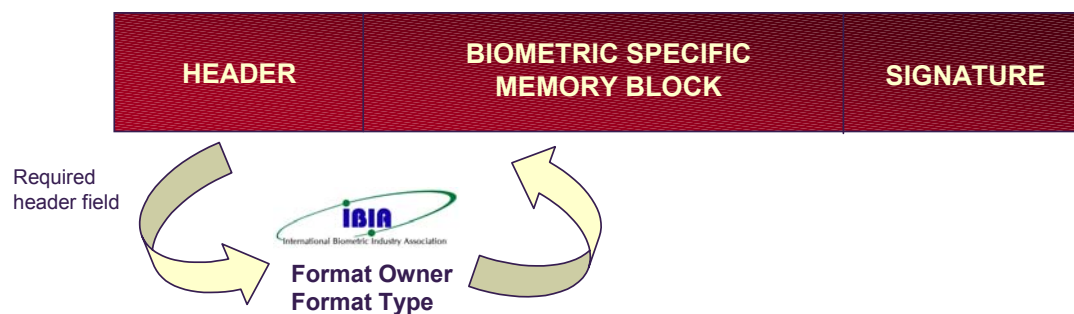


Figure 1. CBEFF Biometric Data Structure

CBEFF defines a Patron/Client model. In this model, *Patrons* are organizations that have developed a standard or specification that incorporates a biometric data object that conforms to the CBEFF requirements. Examples of CBEFF Patrons are the BioAPI and X9.84 (addressed below). CBEFF *Clients* are entities that define/implement a specific biometric data structure (e.g., a BSMB format owner) that meets CBEFF requirements. This would include any vendor, standards committee, working group, or industry consortium that has registered itself with IBIA and has defined one or more BSMB format types. Figure 2 depicts the relationship between CBEFF Patrons and Clients.

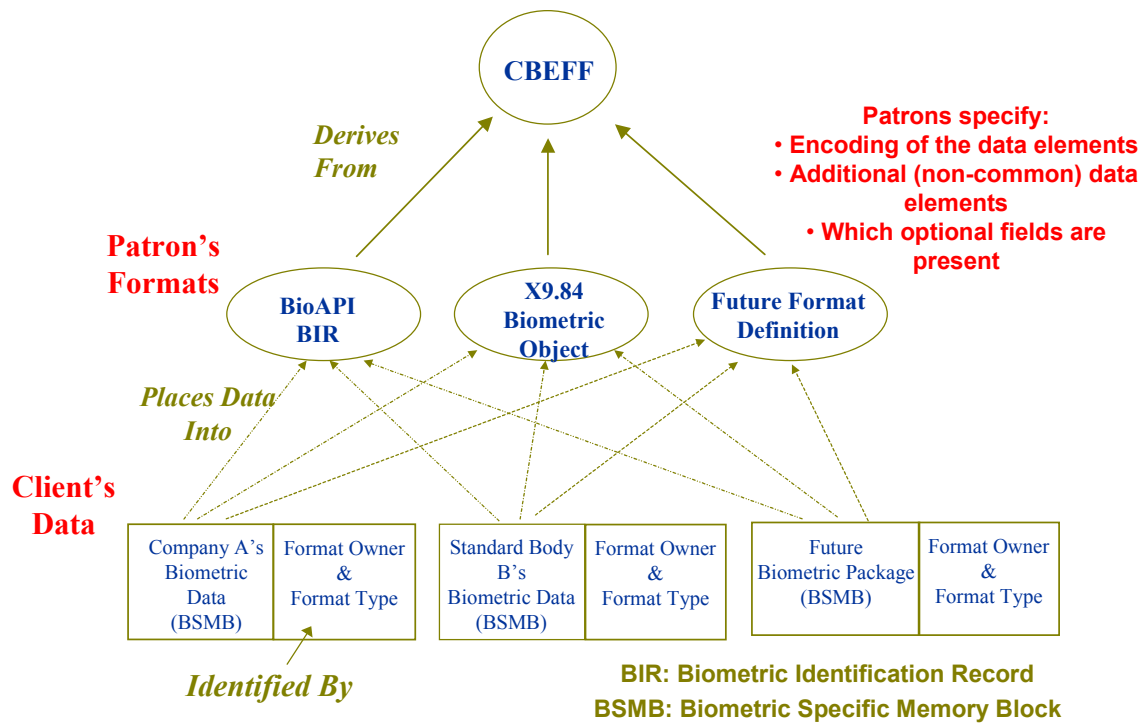


Figure 2. CBEFF Patron/Client Model.

CBEFF does not dictate how the biometric data is to be encoded – that is the responsibility of the Patron. The goal is to define standard elements that can be exchanged to facilitate interoperability; however, in some circumstances some encoding/decoding or value translation may be required.

Revision A of CBEFF is currently in progress and expected to be released soon. This version adds a smart card patron format and defines a nested structure for packaging multiple biometrics in a single object. Additionally, CBEFF is being considered by the INCITS M1 committee for its fast track process to become an ANSI standard.

The Organization for the Advancement of Structured Information Standards (OASIS) is currently working on an XML version of the CBEFF data structure called XCBF, which will be compatible with both the BioAPI and X9.84 instantiations of CBEFF. [8]

M1 has also approved five new work items for biometric data interchange formats:

- Finger Minutiae Interchange Format
- Finger Pattern Interchange Format
- Face Recognition Format for Data Interchange
- Iris Interchange Format
- Finger Image Based Interchange Format

Additionally, a proposal has been submitted for a Signature/Sign Image Based Interchange Format.

These interchange formats will define technology type specific standard formats for the interchange of data between systems/vendors. This would allow, for example, data to be collected (captured and full or partially processed) at one time/place by Vendor A and be matched (including any further processing, if necessary) at another time/place by Vendor B. These formats would comprise a standard BSMB format that will fit within the CBEFF data structure. Each format would thus be assigned a unique format owner/type such that receiving systems could determine how the data is to be routed/processed.

It is expected that the first of these standard interchange formats will be published in mid-late 2003. Working drafts are available for review on the INCITS M1 document register website (see references).

API standards

Application Programming Interfaces (APIs) define a method for a software application to communicate with an underlying service or technology. Standard APIs provide a common interface method across a set of technologies. Standard biometric APIs do this generically across multiple types of biometric technologies. This allows a software application to be written once to accommodate any API-compliant technology. Benefits of implementing a standard biometric API within an application's software architecture include the ability:

- For rapid application development
- To substitute technologies
- To add technologies (perhaps as new products become available)
- To upgrade technologies (as a technology refresh path or to exploit price/performance improvements)
- For one application to utilize multiple technologies
- For multiple applications to leverage the same technology

The basic architecture of an API standard implementation is shown in Figure 3. In this diagram, the application communicates through the API to an API framework component. The biometric service provider (BSP) technology modules communicate through that same framework via a service provider interface (SPI). The framework handles module management and API/SPI translation.

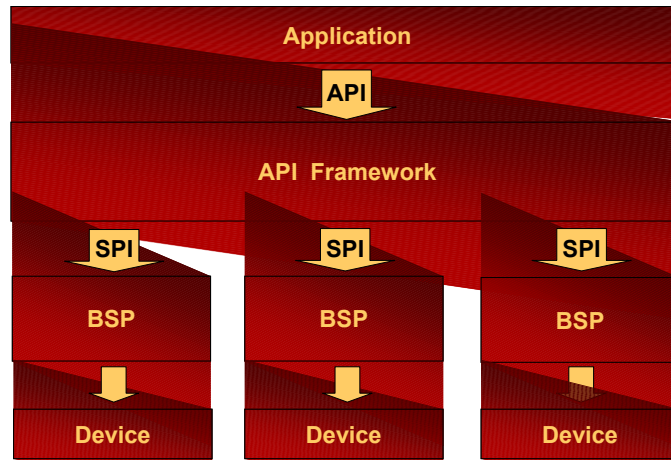


Figure 3. Standard API Architecture.

Prior to 1996, only product specific APIs provided with vendor software development kits (SDKs) were available. As a result, application developers and system integrators had to develop custom interfaces for each product they used. By the end of 1996, a biometric API standard known as the Speaker Verification API (SVAPI) was developed, which provided a common interface definition across voice technologies.

In early 1997, the National Security Agency (NSA) contracted for the development of a generic biometric API which would be usable across technology types. The Human Authentication API (HA-API), was released in late 1997. This API provided a simple set of functions in support of biometric authentication (i.e., 1:1 verification). It was eventually adopted by 20-30 vendors.

In April of 1998, a consortium of 6 companies (including Compaq, Microsoft, Novell, IBM, Identicator, and Miros) announced their intention of developing a multi-level biometric industry standard API. Although this was not initially well received, primarily due to the ongoing work of the then established HA-API working group, the two organizations merged in early 1999 to form a reconstituted BioAPI Consortium (less Microsoft). [9] Both IBM and I/O Software (who had published its own proprietary biometric API known as BAPI) had also agreed to merge their APIs into this effort. Intel, who assumed the technical editor role within BioAPI, likewise agreed to make their biometric service within their Common Data Security Architecture (CDSA) compatible with BioAPI.

For better or worse, immediately following the publication of the BioAPI Specification, Version 1.0, in March of 2000, Microsoft and I/O software subsequently announced in May of 2000 that Microsoft had licensed BAPI from I/O Software and planned to include it within some future version of the Windows operating system. As of today, Microsoft has not released such a product.

A brief overview of BioAPI and BAPI are provided in the following.

BioAPI is an open-system, consensus standard developed by a consortium of biometric vendors, integrators, and end-users over a period of several years. Membership now numbers over 100 companies and organizations from industry, government, and academia worldwide. In February of 2002, the BioAPI was approved as an ANSI standard, ANSI/INCITS 358-2002. [10] It has been submitted by the US as a technical contribution to ISO SC37 for consideration for fast track processing to become an ISO standard.

In addition to the specification, a Win32 reference implementation of the BioAPI framework software exists, with beta versions of both a Unix (Sun Solaris) and Linux ports ready for release.

BioAPI supports both basic and primitive functions, as shown in the table of Figure 4, below:

Basic Functions	Primitive Functions
<p><i>Module Management</i> BioAPI_ModuleLoad BioAPI_ModuleAttach</p>	<p><i>BioAPI_Capture</i> Captures raw/intermediate data from sensor</p>
<p><i>Data Handling</i> BioAPI_GetBIRFromHandle BioAPI_GetHeaderFromHandle</p>	<p><i>BioAPI_Process</i> Converts raw sample into processed template for matching</p>
<p><i>Callback & Event Operations</i> BioAPI_SetStreamCallback</p>	<p><i>BioAPI_CreateTemplate</i> Converts raw sample(s) into processed template for enrolment</p>
<p><i>Biometric Operations</i> <u><i>BioAPI_Enroll</i></u> – Captures biometric data and creates template <u><i>BioAPI_Verify</i></u> – Captures live biometric data and matches it against one enrolled template</p>	<p><i>BioAPI_VerifyMatch</i> Performs a 1:1 match <i>BioAPI_IdentifyMatch</i> Performs a 1:N match</p>
<p><u><i>BioAPI_Identify</i></u> – Captures live biometric data and matches it against a set of enrolled templates</p>	<p><i>BioAPI_Import</i> Imports non-realtime data for processing</p>

Figure 4. BioAPI Functions (not inclusive)

In addition to standardizing the function calls, BioAPI also standardizes the biometric data format (CBEFF compliant structure) and normalizes scoring and thresholding (the criteria and results of matching) values. It has a rich feature set which supports true client/server

implementations, model (template) adaptation, application control of the GUI, application or BSP controlled databases, data payloads, and support for self-contained devices.

It is important to note that BioAPI is an open system specification, written to be operating system independent. As a result, it can support biometric implementations in heterogeneous, cross-platform environments. An example would be access to a biometrically protected website (or within a web application) where the biometric data is captured through a browser on a Windows workstation and matched at a Unix or Linux web server.

BioAPI compliant products are now available – well over a dozen at last count – and customers, such as the US government, are beginning to include BioAPI compliance requirements in their solicitations. It is also being referenced in related standards and documents, such as DL/ID 2000, X9.84, and the draft biometric protection profile. In April of 2002, BioAPI received the Larry Linden Security Award at the CardTech/SecurTech conference in New Orleans.

BAPI is a “proprietary standard” developed and licensed by I/O Software (IOS), a privately held company based in Riverside, CA. [11] BAPI is a 3-level API specification, providing increasingly lower levels of sophistication, control, and technology dependence. The three BAPI levels are shown in Figure 5, below:

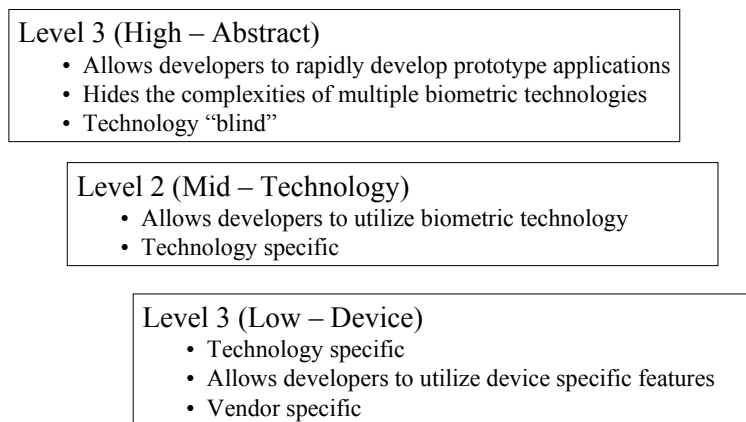


Figure 5. BAPI Levels.

BAPI supports several levels of device sophistication and modularity of components, with an event-driven architecture and direct user interaction.

Currently, the BAPI specification is not publicly available and the SDK must be licensed from I/O Software. However, a number of technology vendors have done so and are BAPI compliant.

At this point, it is not clear to what extent Microsoft will modify the code it received from IOS in 2000, what “level” of the API it will expose to third party applications, or when it will be released, possibly as “MS-BAPI”. It is also not clear if the biometric data will be available for

export outside of the Windows environment or if so, if this data will be CBEFF compliant. That said, it is exciting to see Microsoft embrace biometrics and embedded OS support can be nothing but good for the biometrics market. A third, newer specification on its way to standardization is the JavaCard Forum's Biometric API. This API defines a standard way for a Java Applet (running on a smart/chip card to communicate with a biometric applet, such as a match-on-card (MOC) applet. This specification has been approved by the BCWG and is being considered by INCITS M1 for further standardization.

Security standards

Biometrics and security go hand-in-hand, right? So how do you ensure that by adding biometrics to your system that you have actually improved security, rather than reduced it by adding new vulnerabilities? That is the subject of several standards and activities.

In 2000, ANSI X9.84-2002, *Biometric Information Management and Security for the Financial Services Industry* was published. [12] This standard provides guidelines for the secure implementation of biometric systems, applicable not only to financial environments and transactions, but far beyond. The scope of X9.84 covers security and management of biometric data across its life cycle, usage of biometric technology for *verification* and *identification* banking customers and employees, application of biometric technology for physical and logical access controls, encapsulation of biometric data, techniques for securely transmitting and storing biometric data, and security of the physical hardware.

X9.84 begins by defining a biometric data processing framework, as shown in Figure 6. This framework defines common processing components and transmission paths within a biometrically enabled system which must be secured.

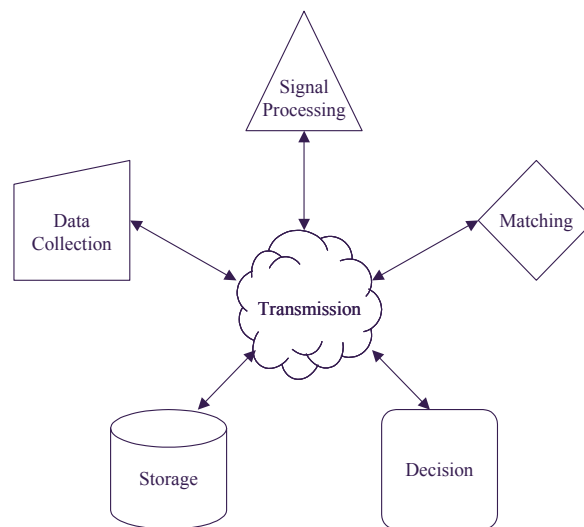


Figure 6. X9.84 Biometric Framework.

A basic tenet of X9.84 is that biometric data should be handles similarly to a public key – where integrity of the data is paramount and unauthorized disclosure of the biometric data should not compromise either the system or the individual. Encryption of the data may be provided for reasons of privacy.

The basic requirements of X9.84 are:

1. Mechanisms ... to maintain the data integrity of biometric data and verification results

between any two components:

- Cryptographic mechanisms such as a MAC or digital signature,
- Physical protection where no transmission is involved and all components reside within the same tamper resistant unit

2. Mechanisms ... to authenticate the source of the biometric data and verification results,

between the sender and receiver component:

- Cryptographic mechanisms such as a MAC or digital signature
- Using physical protection where no transmission is involved and all components reside within the same tamper resistant unit

3. If desired, mechanisms ... to ensure the confidentiality of the biometric data during transmission

The X9.84 specification was developed in coordination with BioAPI. The two specifications are compatible, with X9.84 providing additional security features to augment those supported, but not required by BioAPI. It is also CBEFF compliant. X9.84 is currently in revision and is anticipated to be considered for ISO standardization in the future.

Another security related standard is The Open Group's (TOG's) Common Data Security Architecture (CDSA), which provides a security services framework for a variety of platforms. [13] The Human Recognition Services (HRS) extension to CDSA provides strong authentication services, including biometrics. HRS is based on and compatible with BioAPI, thus it can also be classified as an API standard. Figure 7 is a diagram of the CDSA architecture and how HRS fits in with other security services such as cryptologic, trust policy, certificate library, secure data storage, and key management services.

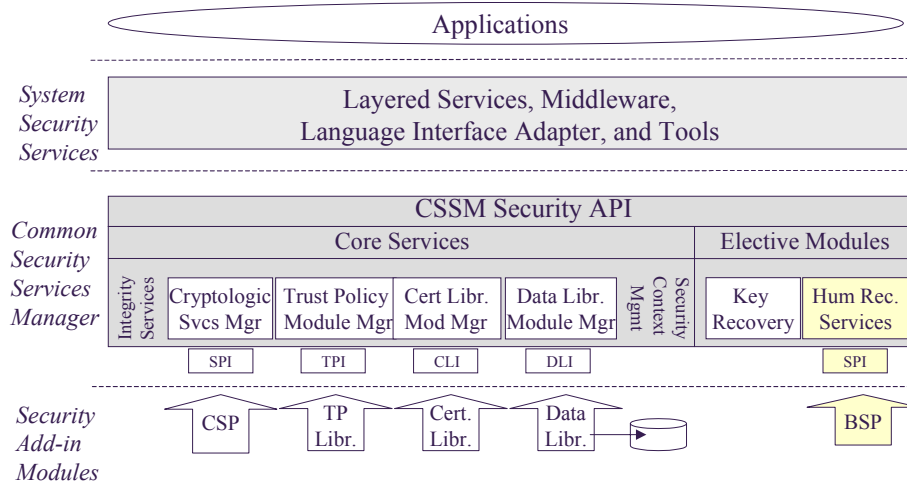


Figure 7. CDSA Architecture

Within the Common Criteria (ISO 15408) scheme of information assurance evaluation and certification, protection profiles serve to define a common set of security requirements for a particular type of products, e.g., firewalls. Biometric Protection Profiles define the security requirements and level of assurance required for biometric devices/systems. Two such biometric protection profiles are currently under development – an evaluated assurance level (EAL) 4 (medium) by the US Department of Defense (DoD) and and EAL level 2 (low) by the UK CESG. [14] [15] These BPPs define the target environment, potential attacks, and security functions.

A companion document, developed by the UK Biometric Working Group (BWG) is the *Biometric Evaluation Methodology* supplement, which provides guidelines for the application of the Common Criteria (CC) to the assurance requirements and evaluation of biometric systems. [16] Similar to X9.84, it defines a simplified biometric system, comprised of components (data and processes) and transmission paths, as the framework for discussing security requirements. The two main areas of consideration within this document are analysis of vulnerabilities and performance testing. BioAPI, CBEFF, and X9.84 are referenced by this document.

Both of the above documents, while security focused, could also perhaps be classified within the next category of standards.

Testing and certification standards and guidelines

There are unique considerations when conducting any sort of test of a biometric system. In particular, performance testing, which seeks to determine the accuracy and other performance features of a biometric component or subsystem, requires guidelines to ensure that the data

collected and analysed is unbiased and statistically sound. The conditions under which the data are collected greatly affect the results.

The pre-eminent guideline in this regard is *Best Practices for Testing and Reporting Performance of Biometric Devices*, authored by Dr. Tony Mansfield of the National Physical Laboratory, UK, and Dr. Jim Wayman, San Jose State University, US. [17] It provides guidance in the areas of test planning, data collection, analysis, uncertainty estimates, and reporting, including practical advice and lessons learned, as well as solid scientific grounding. It discusses the different types of biometric testing – technology, scenario, and operational evaluations as well as the various performance measurements of interest.

In addition, INCITS M1 has recently approved a new work item entitled *Biometric Performance Testing and Reporting*. The scope of this work item is to develop common procedures for measuring and reporting the performance of biometric algorithms. Additionally, it will delineate minimal sets of data that compliant declarations must disclose in association with such reports. No working draft is yet available for review.

Other Standards

In addition to those highlighted above, INCITS M1 is currently working on three application profile standards:

- Application Profile for Biometric-Based Verification and Identification of Transportation Workers
- Application Profile for Biometric-Based Verification and Identification for Border Crossing
- Application Profile for Point of Sale Biometric-Based Verification and Identification

These application profiles will provide guidance on standards requirements for the use of biometrics within these application environments, identifying base standards and the classes, subsets, options, and parameters within the standards needed to accomplish a particular function.

Additionally, a work item pertaining to Template Protection and Use is underway, a harmonized biometric vocabulary has been proposed, and an ad hoc study group is looking at how to extend the Government Smart Card Interoperability Specification (itself being considered for formal standardization) to include biometric functionality. [18]

Lastly, in the area of non-technical standards, the IBIA has established standards for its members, namely:

- Use of biometrics only for legal, ethical, and non-discriminatory purposes
- Highest standards of system integrity and database security to deter identity theft, protect personal privacy, and ensure equal rights

- Professional courtesy among competitors
- Truth in marketing (including accuracy claims)
- Demonstration that products are safe, accurate, and effective
- Commitment to principles of free trade
- Privacy principles

Conclusion

Biometric standards are in place to support the widespread adoption of biometrics. The industry is aware of the need and importance of standards and was very early to develop and promote them. Standards activities are expanding and the standards development efforts are accelerating. This paper has attempted to provide awareness and status of current standards and ongoing standards efforts.

References:

- [1] ISO Joint Technical Committee 1 – Information Technology, Sub-Committee on Biometrics (SC37), website: <http://www.jtc1.org> (select SC37).
- [2] International Committee on Information Technology Standards, Technical Committee on Biometrics (M1), website: <http://www.incits.org> (select Technical Committees, then M1).
- [3] ANSI/NIST ITL 1-2000, *Data Format for the Exchange of Fingerprint, Facial, and SMT Information*. See ftp://sequoyah.nist.gov/pub/nist_internal_reports/sp500-245-a16.pdf.
- [4] CJIS-RS-0010(v)7 FBI *Electronic Fingerprint Transmission Standard*. Available from <http://www.fbi.gov/hq/cjisd/iafis/efts70/cover.htm>
- [5] AAMVA DL/ID-2000 *National Standard for the Drivers License/Identification Card*. Available from <http://www.aamva.org/standards/stdAAMVADLIdStandard2000.asp>
- [6] NISTIR 6529, *Common Biometric Exchange File Format*, January 2001. Available from <http://www.nist.gov/cbeff>.
- [7] International Biometric Industry Association, CBEFF format registry. Website: <http://www.ibia.org/formats.htm>
- [8] Organization for the Advancement of Structured Information Standards (OASIS), XCBF, website: <http://www.oasis-open.org/committees/xcbf>.
- [9] BioAPI Consortium, website: <http://www.bioapi.org>
- [10] ANSI/INCITS 358-2002, BioAPI Specification, Version 1.1. Available through the INCITS on-line standards store, <http://www.techstreet.com/ncitsgate.html>.
- [11] *BAPI*, I/O Software, website: <http://www.iosoftware.com/pages/Products/SecureTec%20SDK/BAPI/index.asp>
- [12] ANSI X9.84-2002, *Biometric Information Management and Security for the Financial Services Industry*. <http://www.x9.org>
- [13] Common Data Security Architecture, The Open Group. See website: <http://www.opengroup.org/pubs/catalog/c013.htm>
- [14] US DoD Draft Biometric Protection Profile. Downloadable from: <http://www.c3i.osd.mil/biometrics/> (click on Initiatives, then Biometrics Protection Profiles).

[15] Draft *Biometric Device Protection Profile (BDPP)*, UK Government Biometric Working Group (BWG), sponsored by CESG. Downloadable from:

<http://www.cesg.gov.uk/technology/biometrics/media/bdpp082.pdf>

[16] *Biometric Evaluation Methodology*. Downloadable from:

http://www.cesg.gov.uk/technology/biometrics/media/BEM_10.pdf

[17] *Best Practices for Testing and Reporting Performance of Biometric Devices, Ver 2.01*, A.J. Mansfield and J.L. Wayman, August 2002. Published by the National Physical Laboratory, UK. Downloadable from:

<http://www.cesg.gov.uk/technology/biometrics/media/Best%20Practice.pdf>

[18] NISTIR 6887: *Government Smart Card Interoperability Specification, Ver 2.0*, available from <http://smartcard.nist.gov>