



Biometric Standards – An Overview

January 2006

By

Cathy Tilton, VP

TABLE OF CONTENTS

1. INTRODUCTION.....	3
2. STANDARDS ORGANIZATIONS.....	4
3. APPROVED STANDARDS.....	6
4. ONGOING STANDARDS ACTIVITIES & PROJECTS.....	8
5. ADOPTION	10
6. CONCLUSION	11

1. Introduction

Biometrics are coming of age. One indicator of this is the advancement and availability of technical standards for biometrics – generally a sign of industry maturity. Although standardization efforts began before 9/11, focus on the acceleration of biometric standards began soon thereafter.

Why are standards important? In general, technical standards support interchangeability and interoperability. This reduces risk to the integrator and end user, primarily because it simplifies integration, allows for substitution and upgrade of technologies, and reduces “vendor lock-in” effects. This can lead to a broader range and availability of products and movement towards commoditization.

The first biometric standards were in the area of law enforcement, where the need to exchange fingerprint data led the US National Bureau of Standards (now NIST) in 1986 to publish the first such standard (the precursor of the current fingerprint interchange standards used by law enforcement agencies around the world today). Since that time, commercial standards have emerged and continue to expand and evolve.

The following provides a survey of the organizations involved in biometric standardization and the standards that have resulted and are currently in progress.

Note that sometimes a company will create a technical specification that their business partners and 3rd party developers must follow that they then dub an “industry standard”. If the company has a large enough share of a big market, these can become “defacto” standards, however, in general, there is no such thing as a “proprietary standard”. This is an oxymoron.

2. Standards Organizations

There are two types of standards organizations – formal and informal. Formal standards bodies, also known as de jure organizations, comprise the official national standards bodies and internationally recognized bodies. Examples of national standards bodies are the American National Standards Institute (ANSI), the British Standards Institute (BSI), and the Japanese Industrial Standards Committee (JISC). These may or may not be government sponsored. International standards development organizations (SDOs) include the International Organization for Standardization (ISO), the International Electro-Technical Commission (IEC), and the International Telecommunications Union (ITU).

Informal standards bodies, also known as defacto standards organizations, generally comprise industry consortia. Organizational structures and rules vary more widely across informal bodies. Examples include the IETF, W3C, and OASIS. Some bodies that have specifically addressed biometrics include the BioAPI Consortium, the JavaCard Forum, and the Voice XML Forum.

Formal standards bodies

ISO and IEC have a joint technical committee for information technology standards called JTC1. In 2002, ISO/IEC JTC1 established a subcommittee to develop generic biometric standards, which was designated as SC37. This subcommittee is chaired by the US and is composed of six working groups, each addressing a specific area of work, as shown below:

- WG1 – Harmonized Biometric Vocabulary (Convener – Canada)
- WG2 – Biometric Technical Interfaces (Convener – Korea)
- WG3 – Biometric Data Interchange Formats (Convener – Germany)
- WG4 – Biometric Profiles (Convener – US)
- WG5 – Biometric Performance Testing and Reporting (Convener – UK)
- WG6 – Cross-Jurisdictional and Societal Aspects of Biometrics (Convener – Italy)

The website for SC37 is

<http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/customview.html?func=ll&objId=2262372&objAction=browse&sort=name>.

Within ISO, other technical committees and subcommittees have also addressed biometrics. This includes, for example, TC68 (Financial Services), JTC1 SC17 (Smart Cards and Personal Identification), and SC27 (IT Security). The SC37 biometrics group has a liaison relationship with each of these groups to coordinate efforts in this area.

In the US, the group responsible for biometric standards is the International Committee on Information Technology Standards (INCITS) technical committee M1. INCITS is accredited by ANSI and is the Technical Advisory Group (TAG) to ISO/IEC JTC1 SC37 international subcommittee on biometrics.

M1 is organized to mirror the activities of SC37. It develops American National Standards related to biometrics as well as actively participating in the development of standards at the international level. M1 was proposed immediately after 9/11 and its first meeting was held in January 2002. The website for M1 is http://www.incits.org/tc_home/m1.htm.

Informal standards organizations

The most well known informal biometric standards organization is the BioAPI Consortium. This group was formed in 1998 to develop a common biometric application programming interface to allow software applications to communicate with biometric technologies in a platform and device independent manner. This group produced a specification in 2001 and it was later adopted as an ANSI standard in 2002. The website for the BioAPI Consortium is <http://www.bioapi.org>.

Standards and specifications developed by informal standards organizations are identified in Section 3, below.

Law enforcement and government

The earliest biometric standards were created by governments and law enforcement agencies to facilitate the exchange of fingerprint data. Additionally, government agencies frequently need to create “profiles” which tailor existing standards for use for particular application environments. These and other related standards are discussed below.

3. Approved Standards

Below is a listing of biometric standards that have been approved and published.

ISO/IEC

- ISO/IEC 19794-2, Information Technology – Biometric Data Interchange Format – Part 2: Finger Minutiae Data
- ISO/IEC 19794-4, Information Technology – Biometric Data Interchange Format – Part 4: Finger Image Data
- ISO/IEC 19794-5, Information Technology – Biometric Data Interchange Format – Part 5: Face Image Data
- ISO/IEC 19794-6, Information Technology – Biometric Data Interchange Format – Part 6: Iris Image Data
- ISO/IEC 7816-11:2004, Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods

ICAO

- ICAO Doc 9303, “Machine Readable Travel Documents”, 5th Edition, March 2003
 - “Biometrics Deployment of Machine Readable Travel Documents”, Technical Report, Version 2.0, May 21, 2004
 - “Machine Readable Travel Documents, Technical Report, Development of a Logical Data Structure – LDS – for Optional Capacity Expansion Technologies”, Technical Report, Version 1.7, May 18, 2004

INCITS

- ANSI/INCITS 358-2002, “The BioAPI Specification”, February 13, 2002
- ANSI/INCITS 377-2004, “Finger Pattern-Based Format for Data Interchange”, January 23, 2004
- ANSI/INCITS 378-2004, “Finger Minutiae Format for Data Interchange”, February 20, 2004
- INCITS 381-2004, “Finger Image Format for Data Interchange”, May 13, 2004
- ANSI/INCITS 385-2004, “Face Recognition Format for Data Interchange”, May 13, 2004
- ANSI/INCITS 394-2004, “Application Profile for Interoperability, Data Interchange and Data Integrity of Biometric-Based Personal Identification for Border Management”, October 5, 2004
- ANSI/INCITS 395-2005, “Signature/Sign Format (for Data Interchange)”, August 12, 2005
- ANSI/INCITS 396-2005, “Hand Geometry Format for Data Interchange”, May 12, 2005
- ANSI/INCITS 398-2005, “Common Biometric Exchange Formats Framework (CBEFF)”, February 7, 2005

ANSI

- ANSI X9.84-2003, “Biometric Information Management and Security for the Financial Services Industry”, June 2003
- ANSI/NIST-ITL 1-2000, “Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information”, July 27, 2000

OASIS

1. “XML Common Biometric Format (XCBF)”, Version 1.1, August 2003, Organization for the Advancement of Structured Information Standards

Other

- NISTIR 7151, “Fingerprint Image Quality”, August 19, 2004
- IAFIS-DOC-01078-7, “Electronic Fingerprint Transmission Specification (EFTS)”, Version 7.1, May 2, 2005, Federal Bureau of Investigation, Criminal Justice Information Services Division
- 2. IAFIS-IC-0010(V3), “Wavelet Scalar Quantization (WSQ) Grayscale Fingerprint Image Compression Specification”, December 19, 1997 (Federal Bureau of Investigation)

4. Ongoing Standards Activities & Projects

In addition to the published standards identified in section 3 above, many additional standards projects are in progress or have been proposed. Figures 1 and 2, below, provide an overview of projects that have been completed (**bold**) and that are in progress within SC37 and INCITS M1.

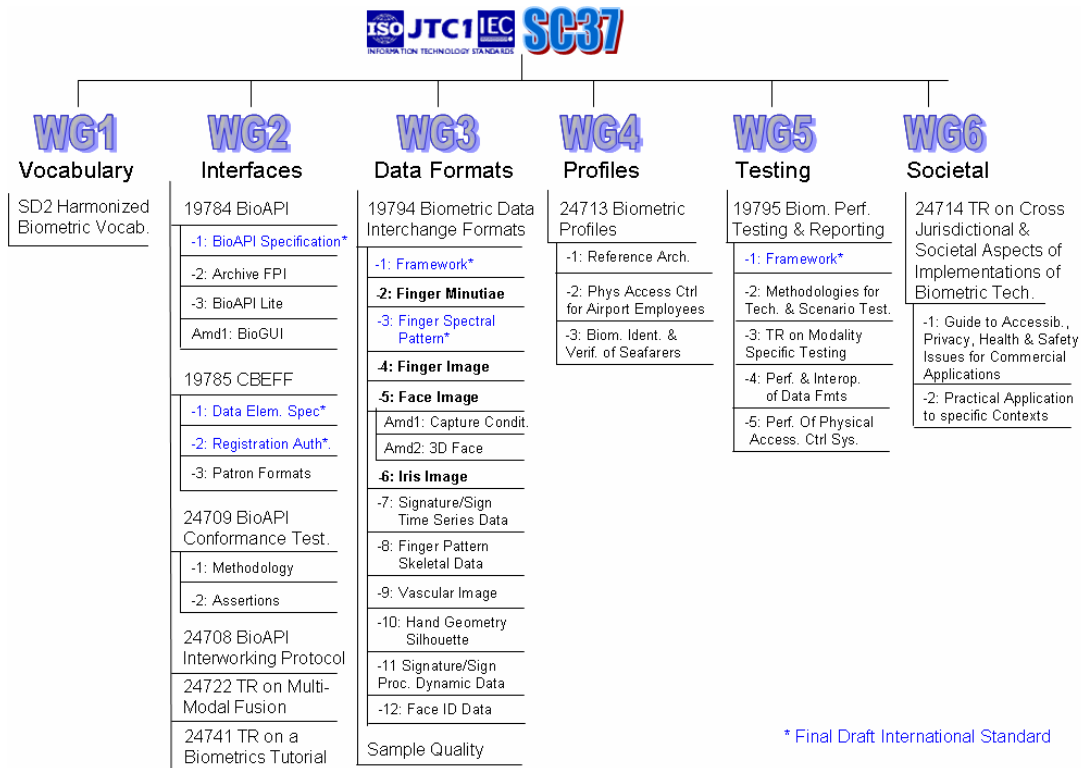


Figure 1. ISO/IEC JTC1 SC37 Standards Activities

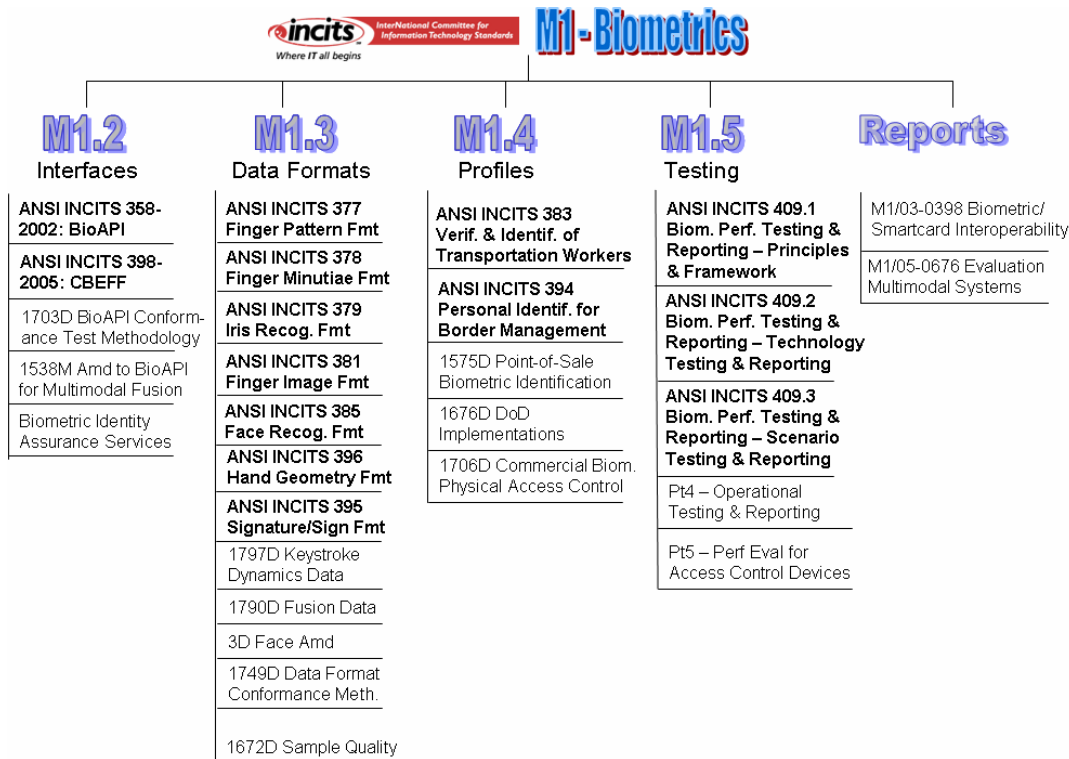


Figure 2. INCITS M1 Standards Activities

Other work in progress includes the following:

ISO/IEC JTC1 SC27

- ISO/IEC 19792, Information technology – Security techniques - A framework for security evaluation and testing of biometric technology (4th WD)
- ISO/IEC 1st WD 24745 - Information technology – Security techniques – Biometric template protection
- ISO/IEC 24761, Information technology – Security techniques – Biometric authentication context (BAC) (1st WD)

ISO TC68

- ISO DIS 19092, *Financial Services – Biometrics*

ITU-T

- ITU-T X.1081, *Telebiometric Multimodal Model Framework (TMMF)*, Q.8/17

5. Adoption

Standards are useful only if they are adopted – that is, required by customers/users and used by vendors to build standards compliant products. There is generally a lag time between the availability of standards and the availability of compliant products. Further, many times vendors delay implementing the standards until they see customer demand for compliance. Below are some examples of end-user adoption of standards.

E-Passports. The International Civil Aviation Organization (ICAO) of the UN sets the requirements for machine readable travel documents (MRTDs), including e-passports and visas. ICAO has required that the biometrics stored within the e-passport conform to the requirements of the SC37 biometric data interchange format for face, fingerprint, and iris data.

Seafarer Identification. The International Labour Organization (ILO) of the UN has a program for issuing a common identification credential for seafarers. This program has required that the fingerprint minutiae templates stored on the seafarer ID card conform to ISO/IEC 19794-2.

US Department of Homeland Security. DHS has required the use of INCITS biometric standards in several of its large biometric projects to include:

- US Visitor and Immigration Status Indicator Technology (US VISIT) border management program
- Transportation Worker Identification Credential (TWIC)
- TSA Registered Traveler program

US Department of Defense. A number of INCITS standards have been adopted within the DoD Joint Technical Architecture and the Defense Information Standards Registry.

US Federal Employee Personal Identity Verification. To comply with Homeland Security Presidential Directive (HSPD) 12, NIST developed technical specifications for the associated biometric-based credentialing system. Included in these specifications are requirements for compliance with the INCITS biometric data format specifications for finger images, minutiae templates, and facial images.

Product availability is in progress, particularly since most of the standards are so recent, but a good example is the availability of BioAPI compliant products. BioAPI was released in 2001 and became an official ANSI standard in 2002. At this point, approximately 40 products have been announced.

6. Conclusion

Biometric standards have come a long way from their humble beginnings in 1986 with the first law enforcement fingerprint standard. Today, many standards are available and many more are on their way. It is no longer acceptable to make excuses that “there are no standards for biometrics” or “it is too hard to implement the standards”. The standards are there and there are many benefits to using them. This is critical to the expansion of the biometrics market.

Cathy Tilton is VP of Standards and Technology at Daon. Since October 1999 she has been the elected chair of the BioAPI Consortium and for the last three years she has been the head of the U.S. delegation to ISO. Cathy has a deep understanding of biometric technologies and has a very strong reputation in the industry, presenting on a regular basis at industry conferences and events.
