A Daon White Paper

Biometric Standards

Overview

Updated: March 2009

Catherine J. Tilton

Table of Contents

Biometric Standards – An Overview

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 (Cards and personal identification), and SC27 (IT security techniques). 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 and an ISO standard in 2006. The website for the BioAPI Consortium is http://www.bioapi.org.

Standards and specifications developed by informal standards organizations are identified in the following sections.

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, broken down by category. There has been a large increase in the number of published biometric standards over the last few years. In addition to quantity, many of the previously listed standards have undergone revision since then. A few US standards have been withdrawn in favor of the corresponding international standards.

ISO/IEC & INCITS

ISO/IEC	INCITS
Technical Interface Standards	
• ISO/IEC 19784-1:2006, Information technology – Biometric Application Programming Interface – Part 1: BioAPI Specification o ISO/IEC 19784-1 AMD1: 2007, "BioGUI specification" • ISO/IEC 19784-2:2007, Information technology – Biometric Application Programming Interface – Part 2: Biometric archive function provider interface • ISO/IEC 19785-1:2006, Information technology – Common Biometric Exchange Formats Framework – Part 1: Data element specification • ISO/IEC 19785-2:2006, Information technology – Common Biometric Exchange Formats Framework – Part 2: Procedures for the operation of the biometric registration authority • ISO/IEC 19785-3:2007, Information technology – Common Biometric Exchange Formats Framework – Part 3: Patron format specifications • ISO/IEC 24708:2008, Information technology – BioAPI Interworking Protocol (BIP) • ISO/IEC 24709-1:2007, Information technology – Conformance testing for the biometric application programming interface (BioAPI) – Part 1: Methods and procedures • ISO/IEC 24709-2:2007, Information technology – Conformance testing for the biometric application programming interface (BioAPI) – Part 2: Test assertions for biometric service providers	• ANSI INCITS 358-2002, "The BioAPI Specification", February 13, 2002 o ANSI INCITS 358-2002/AM1-2007, "Amendment 1: Support for Biometric Fusion", August 17, 2007 • ANSI INCITS 398-2008, "Common Biometric Exchange Formats Framework (CBEFF)", January 23, 2008, (Revision of INCITS 398-2005) • ANSI INCITS 434-2007, "Tenprint Capture Using BioAPI", December 10, 2007 • ANSI INCITS 442-2008, "Biometric Identity Assurance Services (BIAS)", May 21, 2008 • ANSI INCITS 429-2008, "Information technology - Conformance Testing Methodology for ANSI INCITS 358-2002, BioAPI Specification"
Data Formats	
• ISO/IEC 19794-1:2006, Information technology – Biometric Data Interchange Format – Part 1: Framework • ISO/IEC 19794-2:2005, Information technology – Biometric Data Interchange Format – Part 2: Finger minutiae data • ISO/IEC 19794-3:2006, Information technology – Biometric Data Interchange Format – Part 3: Finger pattern spectral data • ISO/IEC 19794-4:2005, Information technology – Biometric Data Interchange Format – Part 4: Finger image data • ISO/IEC 19794-5:2005, Information technology	• 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 • ANSI INCITS 379-2004, "Iris Image Interchange Format", May 13, 2004 - WITHDRAWN • ANSI INCITS 381-2004, "Finger Image Format for Data Interchange", May 13, 2004 • ANSI INCITS 385-2004, "Face Recognition

– Biometric Data Interchange Format – Part 5: Face image data • ISO/IEC 19794-6:2005, Information technology – Biometric Data Interchange Format – Part 6: Iris Image Data o ISO/IEC 19794-5 AMD 1:2007, Information technology - Biometric Data Interchange Formats - Part 5: Face Image Data AMENDMENT 1: Face Image Data on Conditions for Taking Photographs • ISO/IEC 19794-7:2007, Information technology – Biometric Data Interchange Format – Part 7: Signature/sign time series data • ISO/IEC 19794-8:2006, Information technology – Biometric Data Interchange Format – Part 8: Finger pattern skeletal data • ISO/IEC 19794-9:2007, Information technology – Biometric Data Interchange Format – Part 9: Vascular image data • ISO/IEC 19794-10:2007, Information technology – Biometric Data Interchange Format – Part 10: Hand geometry silhouette data	Format for Data Interchange", May 13, 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 - WITHDRAWN • ANSI INCITS 423.1-2008, "Conformance Testing Methodology Standard for Biometric Data Interchange Format Standards – Part 1: Generalized Conformance Testing Methodology", January 23, 2008 • ANSI INCITS 423.2-2008, "Conformance Testing Methodology Standard for Biometric Data Interchange Format Standards – Part 2: Conformance Testing Methodology for INCITS 378-2004, Finger Minutiae Format for Data Interchange" • ANSI INCITS 439-2008, "Information technology - Fusion Information Format for Data Interchange", March 4, 2008
Profiles	
• ISO/IEC 24713-1:2008, Information technology - Biometric Profiles for Interoperability and Data Interchange - Part 1: Biometric Reference Architecture • ISO/IEC 24713-2:2008, Information technology - Biometric Profiles for Interoperability and Data Interchange - Part 2: Physical Access Control for Employees at Airports	• ANSI INCITS 383-2008, "Biometric Profile – Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Transportation Workers" , January 23, 2008 (Revision of INCITS 383-2004) • 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 421-2006, "Biometric Profile – Interoperability and Data Interchange – DoD Implementations, December 1, 2006 • ANSI INCITS 422-2007, "Application Profile for Commercial Biometric Physical Access Control", February 1, 2007
Testing	
• ISO/IEC 19795-1:2006, Information technology – Biometric performance testing and reporting – Part 1: Principles and framework • ISO/IEC 19795-2:2007, Information Technology – Biometric performance testing and reporting – Part 2: Testing methodologies for technology and scenario evaluation • ISO/IEC TR 19795-3:2007, Information Technology – Biometric performance testing	• ANSI INCITS 409.1-2005, "Biometric Performance Testing and Reporting – Part 1: Principles and Framework, October 25, 2005 • ANSI INCITS 409.2-2005, "Biometric Performance Testing and Reporting – Part 2: Technology Testing & Reporting, October 25, 2005 • ANSI INCITS 409.3-2005, "Biometric

and reporting – Part 3: Modality-specific testing • ISO/IEC 19795-4:2007, Information Technology – Biometric performance testing and reporting – Part 4: Interoperability performance testing	Performance Testing and Reporting – Part 3: Scenario Testing & Reporting, October 25, 2005 • ANSI INCITS 409.4-2006, "Biometric Performance Testing and Reporting – Part 4: Operational Testing Methodology, September 8, 2006

Technical Reports

- ISO/IEC TR 24722:2007, Information technology – Biometrics – Multimodal and other multibiometric fusion
- ISO/IEC TR 24741:2007, Information technology – Biometrics Tutorial
- ISO/IEC TR 24714-1:2008, Information technology – Biometrics – Jurisdictional and societal considerations for commercial applications – Part 1: General guidance

ICAO

- ICAO Doc 9303, "Machine Readable Travel Documents"
  - Part 1, "Machine Readable Passports", 6th Edition, 2006
    - Vol 1, "Passports with Machine Readable Data Stored in Optical Character Recognition Format"
    - Vol 2, "Specifications for Electronically Enabled Passports with Biometric Identification Capability"[1]
  - Part 2, "Machine Readable Visas", 3rd Edition, 2005
  - Part 3, "Machine Readable Official Travel Documents", 3rd Edition, 2008

[Note that ISO/IEC 7501 comprises the same content as ICAO 9303, though there is sometimes a time lag in publication.]

ANSI

- ANSI X9.84-2003, "Biometric Information Management and Security for the Financial Services Industry", June 2003
- ANSI/NIST-ITL 1-2007, "Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 1", April 20, 2007
  - ANSI/NIST-ITL 1-2000, "Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information", July 27, 2000 (Still in use.)
- ANSI/NIST-ITL 2-2008, ""Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 2: XML Version", August 12, 2008

OASIS

[1] Previous ICAO Technical Reports are now included in ICAO 9303, Part 1, Vol 2 as follows:
- Section II: THE DEPLOYMENT OF BIOMETRIC IDENTIFICATION AND THE ELECTRONIC STORAGE OF DATA IN MACHINE READABLE PASSPORTS
- Section III: A LOGICAL DATA STRUCTURE FOR CONTACTLESS INTEGRATED CIRCUIT DATA STORAGE TECHNOLOGY
- Section IV: PKI FOR MACHINE READABLE TRAVEL DOCUMENTS OFFERING ICC READ ONLY ACCESS

- **"**XML Common Biometric Format (XCBF)", Version 1.1, August 2003, Organization for the Advancement of Structured Information Standards

Other Standards & Specifications

- NISTIR 7151, "Fingerprint Image Quality", August 19, 2004
- IAFIS-DOC-01078-8.1, "Electronic Biometric Transmission Specification (EBTS)", Version 8.1, November 19, 2008, Federal Bureau of Investigation, Criminal Justice Information Services Division
    - IAFIS-DOC-01078-7, "Electronic Fingerprint Transmission Specification (EFTS)", Version 7.1, May 2, 2005, Federal Bureau of Investigation, Criminal Justice Information Services Division (Still in use.)
- INT-I, Interpol Implementation of ANSI/NIST ITL1-2000, Ver 4.22b, October 28, 2005, The Interpol AFIS Expert Group
- IAFIS-IC-0010(V3), "Wavelet Scalar Quantization (WSQ) Grayscale Fingerprint Image Compression Specification", December 19, 1997 (Federal Bureau of Investigation)
- FIPS 201-1, "Personal Identity Verification (PIV) of Federal Employees and Contractors", March 2006
    - NIST SP 800-76-1, "Biometric Data Specification for Personal Identity Verification", January 2007
- National Information Exchange Model (NIEM), Ver 2.0, June 2007, US DOJ/DHS

4. Ongoing Standards Activities and 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 (red), near completion (blue), and that are in progress within SC37 and INCITS M1.

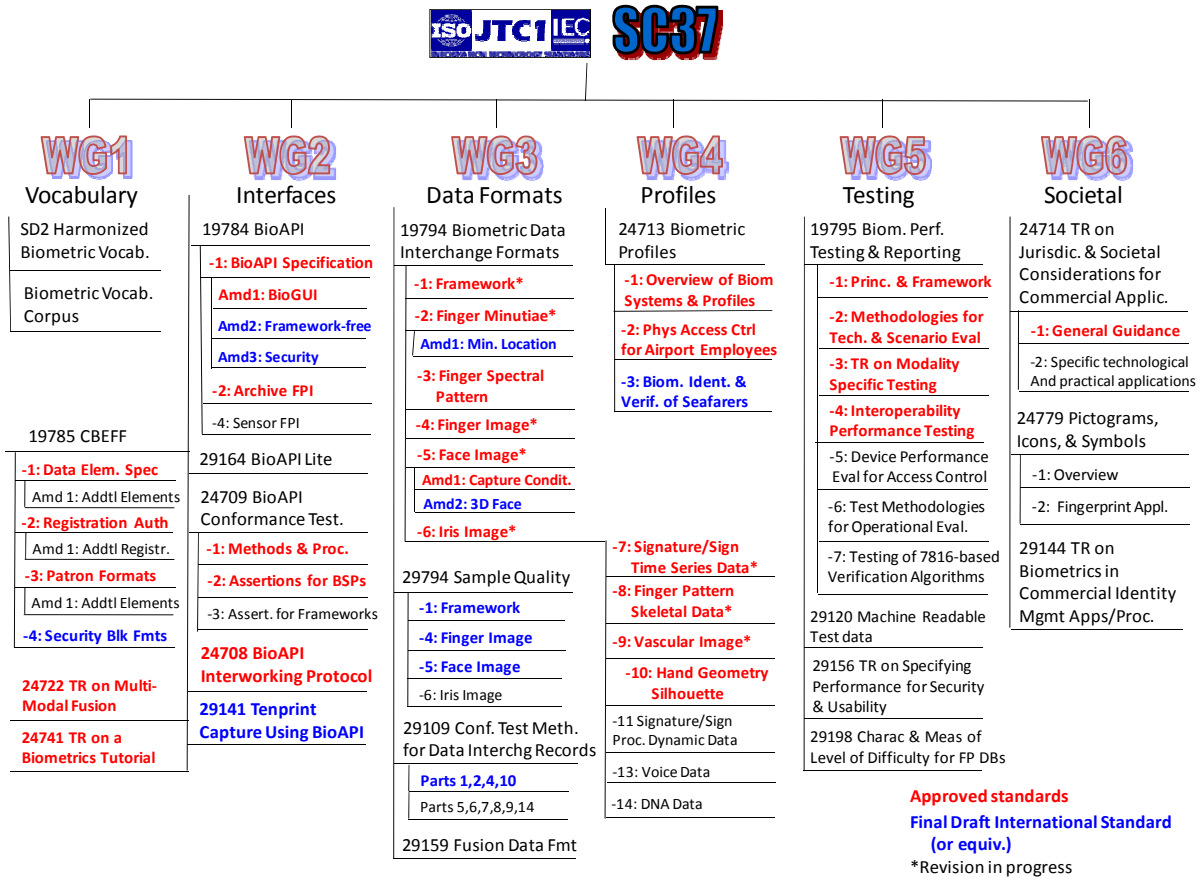

Figure 1. ISO/IEC JTC1 SC37 Standards Activities

Figure 2. INCITS M1 Standards Activities

Notable among the projects above are the following observations:

- *Conformance*. Now that a critical mass of standards exists, there is a movement to develop associated conformance testing methodologies to provide a means of assessing conformity to those standards.
- *Modalities*. In addition to the initial set of commonly used biometric types, we see vascular now having an approved data interchange format, and voice and DNA projects coming along.
- *Quality*. The industry is working to get its arms around how to measure and represent data quality in a standard way across modalities.
- *Revisions*. Now that the standards exist and are being used, feedback has been coming in from the field with corrections and enhancements. This has resulted in many standards moving into a revision phase.

Other work either completed (year given) or in progress (stage indicated) includes the following:

ISO/IEC JTC1 SC17

- ISO/IEC 7816-11:2004, Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods
- ISO/IEC 24787 – Information technology – Identification cards – On-Card biometric comparison (CD2)

ISO/IEC JTC1 SC27

- ISO/IEC 19792, Information technology – Security techniques - Security evaluation of biometrics (FCD)
- ISO/IEC 24745 - Information technology – Security techniques – Biometric template protection (WD4)
- ISO/IEC 24761, Information technology – Security techniques – Authentication context for biometrics (ACBio) (FDIS)
- ISO/IEC 24760, Information technology – Security techniques – A Framework for Identity Management (WD6)

ISO TC68

- ISO 19092-1:2006, Financial Services – Biometrics – Part 1: Security Framework

ITU-T

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

OASIS

- Biometric Identity Assurance Services (BIAS) SOAP Profile (WD7)

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 conformance. 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 (See FIPS 201, above).

US Government. In 2007, the Subcommittee on Biometrics and Identity Management of the National Science and Technology Council (NSTC) of the Office of Science and Technology Policy of the Executive Office of the President, issued the "NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards" which set goals for biometric standards adoption citing that "The success of Federal biometric applications is particularly dependent on the interoperability of biometric systems." Subsequently, in 2008, a companion "Registry of USG Recommended Biometric Standards" was issued identifying specific standards to enable that interoperability, including many of those cited above.

Product availability is in progress, particularly since most of the standards are relatively recent, but a good example is the availability of BioAPI 1.1 compliant products. BioAPI 1.1 was released in 2001 and became an official ANSI standard in 2002. Soon thereafter, approximately 40 products had been announced. Part of this success was due to the availability of an open source reference implementation – a good lesson learned.

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.