Introduction (and a little history)

Biometric standards are one of the most important but least interesting topics in the biometrics field. Most practitioners see them as a necessary evil; however, they play a critical role in the adoption and successful implementation of biometrics in applications where interoperability and interchangeability are needed.

Prior to the events of 9/11, few biometric standards existed. The law enforcement community had developed the ANSI/NBS-ICST 1-1986 standard for the exchange of fingerprint data and its successors are used worldwide for the exchange of forensic biometric data today. By that time, a few “commercial” biometric standards had also emerged, most notably BioAPI. However, it was not uncommon to hear the refrain, “The trouble with biometrics is that there are no standards” as one of the reasons for the lack of large scale adoption of the technology. Those who understood the potential of biometrics in identity management and authentication were frustrated that sales had not lived up to that potential (or the hype).

At that time, the landscape was dominated by proprietary products and custom implementations. Outside of the criminal justice domain, Interoperability was nearly non-existent. For example, it was difficult if not impossible to enroll using Vendor A’s device/algorithms and later verify using Vendor B’s device/algorithms due primarily to data format incompatibilities. Vendors with an installed base tended to like it this as it created a “vendor lock-in” effect and a barrier to entry to new vendors. However, concurrently it increased risk for the end-user. Vendors did not always stay in business. System expansion and technology refresh were more difficult, sometimes requiring re-enrollment of users.

All of a sudden, biometrics were center-stage. Once an obscure technology, people were now talking about how they could be used to enhance national security. The US president actually used the “B-word” in a speech. But how could this technology be used effectively without associated standards?

Enter NIST (National Institute of Standards and Technology, formerly the National Bureau of Standards, NBS, who had authored the 1986 standard previously cited). NIST was tasked to accelerate the development of the needed biometric standards, a task they embraced and acted upon. By December of 2001, a new technical committee (TC) on biometrics (designated M1) was formed within the ANSI accredited INCITS (International Council on Information Technology Standards, formerly ANSI X3) and its first meeting was held in January of 2002. In parallel, the US proposed a new biometrics subcommittee within ISO (International Organization for Standardization) which was approved in June 2002 as SC37 and first met in December of that year, with 17 countries signed up to participate. By 2004, seven new American National Standards for biometrics had been approved and published, with more to follow. Internationally, by 2005 the first four international biometric data interchange format standards had hit the street.
Figure 1. A brief timeline of biometric standards development

**Why Standards?**

For biometrics to be used effectively, they must be exchanged. That exchange may only be between the capture device and a local resource or it could be between a collection system and a backend matching system or data interchange between systems, agencies, or governments. To support data exchange in a heterogeneous environment, standards are required to achieve interoperability.

IEEE estimates that $1.5B is invested globally each year in the creation and management of standards. [1] Does this surprise you? Perhaps it is because, as documented in a study by the German institute for standardization – DIN, standards contribute more to growth than patents and licenses and companies that participate actively in standards work have a head start on their competitors in adapting to market demands. [2] To integrators and end users, open standards are a way to reduce cost, schedule, and technical risks and to avoid “vendor lock-in” issues.

As stated in the Economist, “Without standards, a technology cannot become ubiquitous, particularly when it is part of a larger network.”[3]

However, like everything in life, there is a trade-off. To achieve the benefits of standards, you may have to compromise in other areas – for example, system performance – as sometimes there is additional overhead involved or loss of ability to fully optimize for a specific application.

**Standards Development**

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 – for example the British Standards Institute (BSI). These may or may not be government sponsored. International standards development organizations (SDOs) include the
International Organization for Standardization (ISO 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.

In addition, there are “defacto” or “industry standards”. These are usually developed by a single company or group of companies that create specifications that become widely adopted due to the market share represented.

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:

![SC37 work areas](image)

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.

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.
Standards development follows a process wherein a project is proposed and then moves through a series of steps towards publication. In ISO, these steps are:

- New work item proposal (NP)
- Working draft (WD)
- Committee draft (CD)
- Final committee draft (FCD)
- Draft international standard (DIS)
- International standard (IS)

**Current Status and Trends**

As of September 2010, ANSI/INCITS has published 28 biometric standards covering technical interfaces, data formats, application profiles, and performance testing. ISO has published 37 in these same areas plus vocabulary and societal related standards. In addition, other standards development organizations (SDOs) have also developed biometric related standards in the areas of finance, security, smartcards, telecommunications, and Web services.

It is not possible in a brief article to list all of the biometric standards that have been developed by these organizations; however, the Table 1 provides a summary level listing. Note that many standards are “multi-part.” That means they comprise a family of related standards, usually consisting of a general or base standard as part 1, followed by additional parts. The best example of this is the ISO/IEC 19794 family of data interchange format standards which includes a Part 1 Framework standard plus Parts 2-x for the modality specific (i.e., fingerprint, face, iris, etc.) data formats.
<table>
<thead>
<tr>
<th>Category</th>
<th>Published</th>
<th>In progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vocabulary</td>
<td>2382-37 Vocabulary - Biometrics</td>
<td></td>
</tr>
<tr>
<td>Interfaces</td>
<td>19784 BioAPI (with subparts) 19785 CBEFF (with subparts) 24709 BioAPI Conformance 24708 BioAPI Interworking Protocol 29141 Tenprint Capture using BioAPI OASIS XCBF (XML CBEFF) ITU-T 108x Telebiometrics</td>
<td>29164 Embedded BioAPI 19784-x BioAPI security &amp; sensor interface 30106 Object Oriented BioAPI 30108 Biometric Identity Assurance Services (BIAS)</td>
</tr>
<tr>
<td>Data Formats</td>
<td>19794-1 Framework -2 Finger Minutiae -3 Finger Pattern Spectral -4 Finger Image -5 Face -6 Iris -7 Signature (time series) -8 Finger skeletal -9 Vascular -10 Hand geometry 29109 Conformance testing (formats) (Parts 1,2,4) 29159 Fusion data ANSI/NIST-ITL 1-2007 Data Format for the Interchange of Fingerprint, Facial and other Biometric Data ANSI/NIST-ITL 2-2008 XML version</td>
<td>19794-11 Dynamic Signature -13 Voice -14 DNA 29109-x Conformance testing (formats), other parts 30107 Liveness detection</td>
</tr>
<tr>
<td>Quality</td>
<td>29794 Sample Quality (with subparts) NISTIR 7151 Fingerprint image quality FBI EFTS Appendix F – Fingerprint Image Quality</td>
<td>29794-x Sample quality for other modalities</td>
</tr>
<tr>
<td>Profiles</td>
<td>24713-1 Reference architecture 24713-2 Physical access control for airport employees 24713-3 Biometric identification and verification of seafarers FBI Electronic Biometric Transmission Specification (EBTS) INT-I Interpol Implementation of ANSI/NIST ITL1-2000 ICAO 9303 MRTDs</td>
<td></td>
</tr>
<tr>
<td>Testing</td>
<td>19795 Biometric Performance Testing -1 Principles -2 Technology &amp; scenario evaluation -3 (TR) Modality specific testing -4 Interoperability Performance testing</td>
<td>19795-x Additional parts 29120 Machine readable test data (with subparts) 29189 (TR) Examiner assisted applications 29197 Environmental influence 29198 (TR) Measurement of Difficulty for</td>
</tr>
<tr>
<td>Societal</td>
<td>FP DBs</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>24714-1 (TR): Guide to Accessibility, Privacy, Health and Safety Issues</td>
<td>24779 Pictograms, Icons, and Symbols (with subparts)</td>
<td></td>
</tr>
<tr>
<td>29144 Use of biometric technology in commercial identity management</td>
<td>29194 Guidance on Inclusive Design and Operation of Biometric Systems</td>
<td></td>
</tr>
<tr>
<td>29195 passenger processes for biometric recognition in automated border crossing systems</td>
<td>29156 Guidance on security and usability</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security</th>
<th>FP DBs</th>
</tr>
</thead>
<tbody>
<tr>
<td>19092-1 Biometric security framework (TC68)</td>
<td>24745 Biometric information protection</td>
</tr>
<tr>
<td>24761 Authentication Context for Biometrics</td>
<td></td>
</tr>
<tr>
<td>19792 Security evaluation of biometrics</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Smartcards</th>
<th>24787 On-card matching</th>
</tr>
</thead>
<tbody>
<tr>
<td>7816-11 Biometric verification</td>
<td></td>
</tr>
</tbody>
</table>

| Technical Reports                               | 29196 Guidance for Biometric Enrollment                               |
| (not specific to above)                         | 29195 Passenger Processes for Biometric Recognition in Automated Border Crossing Systems |
| 24722 Multimodal Fusion                         | 29156 Guidance on security and usability                             |
| 24741 Biometrics Tutorial                       |                                                                        |

*Notes:*

- a) Does not include national standards except for those used internationally.
- b) Full titles are not provided.
- c) Standard numbers are ISO/IEC unless otherwise indicated.
- d) Revision projects, amendments, and corrigenda omitted.
- e) Does not include data compression standards.

The first set of biometric standards developed are becoming known as the ‘Generation 1’ (G1) standards. Once published and in use, corrections and enhancements are frequently identified. Some of these are addressed through corrigenda and amendments; however, when the changes are extensive revision projects are initiated. This also happens when the original domain of use is broadened or the technology itself evolves.

An example of domain expansion relates to the ANSI/NIST standard. Originally used exclusively by the law enforcement community, its use has expanded to civil applications primarily related to background screening. For both this and its original purpose, the application of modalities beyond fingerprints has also led to the need to revise this standard.

Technology evolution is exemplified by the advent of 3D facial recognition and compact iris formats. The original face format addressed the traditional 2D facial image; however, as the 3D facial technology matured and multiple providers entered the field, the need to define an interchange format emerged as well. In the case of the iris format, the original (2005) standard included both a rectilinear image and a polar image, the latter intended for use as a compact format – when space or bandwidth constraints limited the record size, when stored on a smartcard for example. However, since the original publication, NIST conducted a large scale iris test called IREX which tested the interoperability
performance of different interchange formats and compression. This showed that a cropped, masked, and compressed rectilinear iris image performed better than a compressed polar image in this environment. In both of these cases, resulting changes are being reflected in revisions to these standards (known as ‘Generation 2’ or G2) which are expected to be published in early-mid 2011.

Another trend being reflected in newer biometric standards and in amendments to older standards is the inclusion of XML encoding. As biometrics are more often used within service oriented architectures, this is a natural evolution. Some examples of XML-based standards in development are:

- The new DNA and voice data formats are being developed natively in XML
- The existing binary data formats are being amended to include an XML encoding option
- In 2008, an XML format was added as part 2 of the ANSI/NIST standard (ANSI/NIST-ITL 2-2008) and specifications based on this standard (e.g., the FBI and Interpol) are also being updated to take advantage of this option
- OASIS and INCITS are jointly developing standards for Biometric Identity Assurance Services (BIAS) which are XML based and include a SOAP Profile (WSDL implementation)
- The current CBEFF (Common Biometric Exchange Formats Framework, ISO/IEC 19785) standard contains an XML patron format to encode metadata and security information

What other recent trends and activities may be of interest? Besides revisions and XML, work has begun in a number of other areas. Now that the basic set of standards is in place, experts are looking into more specific topics. For example, standards related to sample quality, fusion, and conformance methodologies have recently been developed. New projects have begun on usability, environmental influence, characterizing difficulty levels, icons and symbols, and the role of biometrics in identity management. Others have been proposed for object oriented APIs and liveness detection.

Little known is the fact that besides standards, many SDOs including ISO also develop technical reports. This is done when either the subject is not yet mature enough for standardization or the topic is informative in nature or more suitable as guidance. SC37 has published a number of such reports (e.g., related to multimodal fusion, cross-jurisdictional and societal considerations, and modality specific quality and testing). New projects on enrollment guidance and automated biometric border clearance are also targeted as technical reports.

Two important biometric standards events have recently occurred. The first was the SC37 meeting held in January 2011 in Stockholm at which many of the recent developments above occurred. The second was the ANSI/NIST update workshop held in July 2010 at which the content of the 2011 version of this important standard were decided. This includes the addition of new modalities, geolocation data, and security features as well as extension of existing fields/values and deprecation of old record types.

So who says standards work is not exciting? Keep watch as the biometric standards saga continues and interoperability benefits are realized.
Adoption

What about adoption of these standards? If you build them, will they come??? Three examples are offered for your consideration.

On August 27, 2004, the US President signed HSPD-12 “Policy for a Common Identification Standard for Federal Employees and Contractors” which required the development and agency implementation of a mandatory, government-wide standard for secure and reliable forms of identification (credentialing) of Federal employees and contractors. NIST was tasked with creating the technical specifications for this credentialing program, which had to be interoperable across government agencies which may independently implement it (i.e., use different vendors). Biometrics were key to this Personal Identity Verification (PIV) as it became known and NIST relied on the recently developed INCITS data format standards, as well as the ANSI/NIST standard, for this purpose.

On the international front, work had been ongoing since 1996 by ICAO (International Civil Aviation Organization, a UN agency) on machine readable travel documents (MRTDs) such as ePassports and eVisas. By 2003, ICAO had “adopted a global, harmonized blueprint for the integration of biometric identification information into passports and other MRTDs”, selecting facial recognition as the globally interoperable biometric and high-capacity, contactless integrated circuit (IC) chips to store identification information within these MRTDs. Following this announcement, ICAO (in conjunction with ISO) began work on the technical specifications, including the logical data structure (LDS), eventually selecting the SC37 data structure/format standards for the biometric data to be stored therein (the need for interoperability of passport data between countries being fairly obvious).

More recently, India has initiated the world’s largest biometric project. The Unique Identity Authority of India (UIDAI) Aadhaar project will enroll 1.2B residents with the goal of financial inclusion. In order to ensure uniqueness of the identities it registers, it uses multi-modal biometric 1:many matching to identify duplicates. Residents will be able to assert and prove their identities as well through biometric verification. The UIDAI chose the SC37 suite of biometric data packaging and format standards to ensure interoperability across its many enrollment agencies, authentication locations, and backend systems.

Conclusion
In the past few years, the adoption of biometrics and the maturity of its standards have both increased. Although we now have an extensive suite of standards to work with, efforts continue to make them more complete and usable. What is most needed now is their adoption and participation in their development from a broader cross-section of users.

References:

