# Advances in Biometric Standardization – Addressing Global Market Requirements for Biometric Standards


## Name and Affiliation

Fernando L. Podio, National Institute of Standards and Technology (NIST), Gaithersburg, MD, USA



## Keywords

Biometric Data Interchange Formats; Biometric Technical Interfaces; Biometric Performance Measurements; Biometric Standards; Biometric Interoperability; Biometrics; Personal Identification; Personal Verification; Security Standards; Tele-Biometrics; Token-Based Standards.


## 1. Introduction

Biometric standards promote the availability of multiple sources of compatible products in the marketplace. They benefit end-users as well system developers, biometric vendors and the Information Technology industry. This paper addresses the status of published biometric standards, on-going biometric standards development activities and short-term standards development plans. Development of biometric standards often impacts related efforts such as token-based, security and telecommunication standards development. Examples are provided in sections 2.1.2, 2.1.3 and 2.2.2. A brief discussion on the global marketplace needs for these standards (reflected in the on-going development projects) and adoption examples are provided in section 2.3. The following clauses focus mainly on international standards, but other biometric standards considered to have a large international impact are also addressed.

## 2. Biometric Standard Activities

### *2.1 ISO/IEC Joint Technical Committee 1*

In the international arena the Joint Technical Committee 1 of the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) is the major standards body responsible for the development of "International standardization in the field of Information Technology". As stated in ISO/IEC JTC1 (2010) "JTC 1 is the standards development environment where experts come together to develop worldwide Information and Communication Technology (ICT) standards for business and consumer applications." Within JTC 1, Subcommittee 37 – *Biometrics,* SC 37 (2011) is responsible for the development of a large portfolio of international biometric standards to support interoperability and data interchange among applications and systems. Section 2.1.1 discusses this Subcommittee's work. Other JTC1 Subcommittees are involved in the development of biometric standards for certain aspects of standardization within their general scope of work. Section 2.1.2 addresses related work in JTC 1 Subcommittee 17 -*Cards and personal identification* SC 17 (2011) and Section 2.1.3 focuses on related work under JTC 1 Subcommittee 27 - *IT Security techniques* SC 27 (2011). A list of published standards and ongoing projects can be consulted through each Subcommittee's home page (under Work programme). ISO (2011) maintains a list of the published standards and provides a description of the content of each standard. Figure 1 depicts the international biometric standards activities within JTC 1 Subcommittees.

Other international organizations are currently involved in some aspects of biometric standardization or are addressing the use of biometric standards for their own standards, specifications or requirements. Examples of these efforts are mentioned section 2.2. Discussions provided in the section include related activities under ISO Technical Committee 68 – Financial Services – SC 2 – *Security* ISO/TC 68 (2011), the Telecommunications Union Telecommunication Standardization Sector Study Group 17 – *Security* ITU-T/SG17(2011), the International Civil Aviation Organization ICAO (2011), and the International Labour Organization from the United Nations ILO (2011). The paper also addresses the development of the ANSI/NIST-ITL standards NIST/ITL (2011) because of its impact and use by law enforcement, intelligence, military, and homeland security organizations throughout the world,.

These standards efforts outside of ISO/IEC JTC 1 are addressed in Section 2.2. Section 2.3 provides a few examples of biometric standards adoption of high impact within the global user community that needs these standards to support personal verification or identification applications. The section also provides examples on how standards bodies are responding to these users' needs.

### *2.1.1 ISO/IEC JTC 1 Subcommittee 37 – Biometrics*

JTC 1/SC 37 was established by JTC 1 in June 2002. This new effort within JTC 1 gave the IT community and end-users an international venue to accelerate and harmonize formal international biometric standards. SC 37 successfully brought together a wide range of interest among IT organizations, the biometric industry, security experts and customers of a large range of personal identification and verification applications and offered a well-structured approach to biometric standardization to meet the users' needs for homeland defense and other government and commercial applications.

The Subcommittee's scope of work, listed below, has not changed since it was established:

> "…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."

*2.1.1.1 Biometric data interchange formats and related standards.* JTC 1/SC 37 is dealing with the standardization of the content, meaning, and representation of biometric data interchange formats which are specific to a particular biometric technology or technologies. The ISO/IEC 19794 multi-part standard (ten parts already published), specifies biometric data interchange formats for a number of biometric modalities including fingerprint (i.e. minutiae, pattern spectral and skeletal) data, face, iris, and vascular image data, signature/sign time series data and hand silhouette data. JTC 1/SC 37 has begun development of the second edition of many of these standards to address technology innovations, the inclusion of richer metadata and new customers' needs. Development of data interchange format standards for three additional modalities (signature/sign processed dynamic data, voice and DNA data) is underway. In addition, a biometric sample quality multi-part standard (ISO/IEC 29794) is also under development. One part has been published as a standard (Part 1: *Framework*), and two additional parts (Part 4: *Finger Image Data* and Part 5: *Face Image Data*) have been published as Technical Reports. Development of conformance testing methodology standards for the biometric data interchange formats is also underway.

Current ongoing activities and consideration of new projects include the development of XML encoding for the data formats as complementary standard formats, conformance testing methodologies for level 3 (semantic testing) for the data interchange formats and development of a new part for the biometric sample quality standard (i.e. iris image). An additional standard has been published that specifies a fusion information format. Recently, JTC1/SC 37 initiated the development of an additional standard: *Anti-Spoofing and Liveness Detection Techniques* (ISO/IEC 30107). The scope of this standard includes terms and definitions that are useful in the specification, characterization and evaluation of artifact and liveness detection methods; a common data format for conveying the type of approach used and the assessment of spoofing or liveness in data formats; conditions that allow for automated artifact or liveness detection to be used; principles and methods for performance assessment of artifact/liveness detection algorithms or mechanisms; and an informative list of a classification of known attacks types.

*2.1.1.2 Biometric technical interface standards.* JTC 1/SC 37 is also addressing the standardization of all necessary interfaces and interactions between biometric components and sub-systems, including the possible use of security mechanisms to protect stored data and data transferred between systems. Representative standards are the ISO/IEC 19784 multi-part standard which specifies a biometric Application Programming Interface, the BioAPI specification and related standards which include the specification of a biometric archive function provider interface and a biometric sensor function provider interface. Another technical interface multi-part standard is ISO/IEC 19785-1 *Common Biometric Exchange Formats Framework* (CBEFF). Part 1 defines a basic structure for standardized biometric information records (BIRs) within CBEFF. This structure consists of three parts: the standard biometric header (SBH), the biometric data block (BDB), and the security block (SB). Other parts of this multi-part standard specify procedures for the operation of the Biometrics Registration Authority for required identifies, patron format specifications (which are detailed specifications of the structure and content of a particular standardized BIR) and security block format specifications.

The Subcommittee is developing a conformance testing methodology multi-part standard for BioAPI (three parts were published: Part 1: *Methods and procedures*, Part 2: *Test assertions for biometric service providers* and Part 3: *Test assertions for biometric frameworks*). The Subcommittee is considering the development of advanced biometric interfaces that may be needed. Some examples include interfaces for enrolment by a remote station to a central database, authentication exchanges between a point of sale terminal and its related database, interfaces for building access and interfaces from border control stations to their underlying databases.

JTC 1/SC 37 started the development of two new related projects. The first multi-part standard is *Object-Oriented BioAPI* which currently consists of three parts: Part 1, *Architecture*, Part 2, *Java implementation* and Part 3, *C# implementation*. The other new project is *Biometric Identity Assurance Services* (BIAS) which defines biometric services used for identity assurance that are invoked over a services-based framework. It provides a generic set of biometric and identity-related functions and associated data definitions to allow remote access to biometric services.

*2.1.1.3 Biometric functional architectures and related profiles.* JTC 1/SC 37 is addressing the standardization of biometric functional architectures and related profiles that bind together the various biometric-related base standards in a manner consistent with functional blocks of operation of biometric systems. These profiles identify the pertinent biometric-related base standards and define which optional fields of the base standards shall be used, as well as how to set the configurable parameters, in order to achieve interoperability within a set of pre-defined constraints. Three parts of a multi-part standard (ISO/IEC 24713) are now published: Part 1: *Overview of biometric systems and biometric profiles*, Part 2: *Physical access control for employees at airports*, and Part 3: *Biometric-based verification and identification of seafarers*. The development of two Technical Reports was recently initiated. They will describe guidance for biometric enrolment and passenger processes for biometric recognition in automated border crossing systems. Potential areas of additional biometric profile development include physical access control for travelers; verification of customers at points-of-sale; and physical/logical access control for employees in manufacturing and service sectors such as healthcare, education, transportation, finance and government.

*2.1.1.4 Biometrics performance testing and reporting methodologies.* This area of standardization addresses the development of performance testing and reporting methodologies as well as metrics that cover biometric technologies, systems and components. Three parts of the biometric performance testing and reporting multi-part standard (ISO/IEC 19795) have been published: Part 1: *Principles and framework*, Part 2: *Testing methodologies for technology and scenario evaluation*, and Part 4: *Interoperability performance test*ing. Part 3, *Modality-specific testing*, has been published as a Technical Report, and additional parts of this standard are under development. Other representative projects include the development of a multi-part standard that specifies machine readable test

data for biometric testing and reporting and the development of two Technical Reports. The first report will provide guidance for specifying performance requirements to meet security and usability needs in applications using biometrics, and the second report will address the characterization and measurement of difficulty for fingerprint databases for technology evaluation. The development of an amendment to ISO/IEC 19795-2 was recently approved that will specify how to evaluate and report performance of multi-modal biometric systems. Another project is under development (ISO/IEC 29197)*: Evaluation Methodology for Environmental Influence in Biometric System Performance*.

The experts developing these standards and Technical Reports recognize the need to identify developments, new requirements and technologies that may not be amenable to testing using the current test processes. Such areas may include testing of behavioural aspects of biometric technologies related to behavioural biometrics and behavioural elements of biological biometrics. There is also a perceived requirement for a standard, or minimally a Technical Report, specific to identification system testing. The current versions of the ISO/IEC 19795 multi-part standard address identification metrics and methodologies, but not the full range of considerations specific to identification systems (e.g., ingestion, queuing, and hardware optimization).

*2.1.1.5 Cross-jurisdictional and societal aspects of biometrics.* JTC 1/SC 37 is addressing the field of cross-jurisdictional and societal aspects in the application of international biometrics standards. The scope of work includes the support of design and implementation of biometric technologies with respect to accessibility, health and safety, support of legal requirements and acknowledgement of cross jurisdictional and societal considerations pertaining to personal information. A multi-part Technical Report (ISO/IEC TR 24714) addresses jurisdictional and societal considerations for commercial applications. Part 1: *General guidance* is published. The Subcommittee is also developing another multi-part Technical Report (ISO/IEC TR 24779) on pictograms, icons and symbols for use with biometric systems. Two additional representative projects include the development of a Technical Report on the use of biometric technology in commercial Identity Management applications and processes and a Technical Report that is aimed at providing guidance on the inclusive design and operation of biometric systems. Recently, a new project was approved for the development of a Technical Report on biometrics and children which will provide guidance on the implications of the use of biometric technologies by children. More specifically, this work will analyse the technical challenges and ethical implications of the use of different biometric technologies across different age groupings and in the context of specific applications (e.g. biometric in schools).

*2.1.1.6 Harmonized biometric vocabulary.* JTC1/SC 37 has advanced the development of part 37 of ISO/IEC 2382: *Information technology – Vocabulary*. The Subcommittee has already specified over one-hundred and twenty harmonized terms and definitions. They include general concept and biometric system terms, terms for data in biometric systems, and device, functioning, interacting, personnel, application and performance terms as well. The draft document (which reached Draft International Standard stage) is periodically sent to JTC 1/SC 37 Liaison Organizations.

JTC1/SC 37's work in conducted through six Working Groups addressing the different aspects of biometric standardization discussed above. At the time of this writing (October 2011), fifty-four International standards (including amendments and technical corrigendum) and six Technical Reports developed by the Subcommittee have been published. Including the revision of existing standards and new projects, the JTC1/SC 37 Programme of Work currently includes over one hundred and ten subprojects (published and ongoing projects included).

### *2.1.2 ISO/IEC JTC1 Subcommittee 17 – Cards and personal identification*

The technologies addressed by JTC 1/SC 17 and JTC 1/SC 37 are, for some applications, complementary in nature. JTC 1/SC 17's scope of work is the standardization in the areas of cards and devices and of personal identification and related documents. Many of the standards are associated with their use in inter-industry applications and International interchange. For the area of machine readable travel documents JTC 1/SC 17 maintains a number of specific standards related to machine readable passports (MRPs), and provides liaison between JTC1 and the International Civil Aviation Organization (ICAO) for ICAO Doc 9303, Part 1, the ICAO Standard defining technical specifications for MRPs. In recent years the Subcommittee has collaborated with ICAO on the development and publication of standards for a new generation of contactless chip and biometric-enabled travel documents (e.g. eMRP, eMRTD).

JTC 1/SC 17 has developed ISO/IEC 7816-11:2004 *Integrated circuit cards -- Part 11: Personal verification through biometric methods* in order to specify the usage of inter-industry commands and data objects related to personal verification through biometric methods in integrated circuit cards. The inter-industry commands used by Part 11 are defined in ISO/IEC 7816-4 *Integrated circuit cards -- Part 4: Organization, security and commands for interchange*. The data objects for Part 11 are partially defined in this International Standard, partially imported from ISO/IEC 19785-1:2006 *Common Biometric Exchange Formats Framework -- Part 1: Data element specification* developed by JTC 1/SC 37. ISO/IEC 7816-11 also presents examples for enrollment and verification and addresses security issues.

JTC 1/SC 17 is considering the scope of the revision to ISO/IEC 7816-8:2004 *Integrated circuit cards -- Part 8: Commands for security operations*, including the creation of a new Perform Biometrics Operation command. The Subcommittee has recently developed "ISO/IEC 24787:2010 *Identification cards -- On-card biometric comparison*, which establishes requirements and security policies for performing biometric comparisons returning decisions on an integrated circuit card. The standard also establishes commands and rules to permit pre-comparison computations to be executed off-card. ISO/IEC 24787:2010 does not establish requirements for off-card comparison implementations, requirements for system-on-card implementations, or modality-specific requirements for storage and comparison. The standard was developed on the basis of ISO/IEC 7816-11 and it uses the compact data interchange formats (e.g. finger-minutia and finger patterns data formats) specified in some of the JTC 1/SC 37 standards. JTC 1/SC 27 and SC 37 contributed to the development of these standards through established liaison relationships with JTC1 /SC 17.

A Technical Report *Guide to on-card biometric comparison standards and applications* is under development. This Technical Report will show how ISO/IEC 24787 interacts within published international standards, recommendations and technical reports covering Identification cards, biometrics and information security; this will include different implementation levels (e.g. application programming interfaces, security mechanisms).

### *2.1.3 ISO/IEC JTC1 Subcommittee 27 – IT Security techniques*

JTC 1/ SC 27 address a number of projects related to biometrics or to the use of biometric standards. Through an established liaison relationship, JTC 1/SC 37 experts worked with JTC 1/SC 27 experts in the development of several standards developed by this Subcommittee including three published standards, ISO/IEC 19792:2009 *Security techniques - Security evaluation of biometric*, ISO/IEC 24761:2009 *Security techniques -- Authentication context for biometrics* and ISO/IEC 24745:2011 *Security techniques -- Biometric information protection*.

ISO/IEC 19792:2009 specifies the subjects to be addressed during a security evaluation of a biometric system. It covers the biometric-specific aspects and principles to be considered during the security evaluation. It does not address the non-biometric aspects which might form part of the overall security evaluation of a system using biometric technology (e.g. requirements on databases or communication channels). ISO/IEC 19792:2009 does not aim to define any concrete methodology for the security evaluation of biometric systems but instead focuses on the

principal requirements. As such, the requirements in ISO/IEC 19792:2009 are independent of any evaluation or certification scheme and will need to be incorporated into and adapted before being used in the context of a concrete scheme. The standard is relevant to both evaluator and developer communities. It specifies requirements for evaluators and provides guidance on performing a security evaluation of a biometric system. It serves to inform developers of the requirements for biometric security evaluations to help them prepare for security evaluations. Although ISO/IEC 19792:2009 is independent of any specific evaluation scheme, it could serve as a framework for the development of concrete evaluation and testing methodologies to integrate the requirements for biometric evaluations into existing evaluation and certification schemes.

Two additional related standards are ISO/IEC 24761 and ISO/IEC 24745. Both standards have been published. ISO/IEC 24761:2009 specifies the structure and the data elements of Authentication Context for Biometrics (ACBio), which is used for checking the validity of the result of a biometric verification process executed at a remote site and specifies the cryptographic syntax of an ACBio instance. The standard allows any ACBio instance to accompany any data item that is involved in any biometric process related to verification and enrolment. The specification of ACBio is applicable not only to single modal biometric verification but also to multimodal fusion. The cryptographic syntax of an ACBio instance is based on an abstract Cryptographic Message Syntax (CMS) schema whose concrete values can be represented using either a compact binary encoding or a human-readable XML encoding. ISO/IEC 24761:2009 does not define protocols to be used between entities such as biometric processing units, claimant and validator. Its concern is entirely with the content and encoding of the ACBio instances for the various processing activities.

ISO/IEC 24745:2011 provides guidance for the protection of biometric information under various requirements for confidentiality, integrity and renewability/revocability during storage and transfer. Additionally, the standard provides requirements and guidelines for the secure and privacy-compliant management and processing of biometric information. This standard specifies the analysis of the threats to and countermeasures inherent in a biometric and biometric system application models; security requirements for secure binding between a biometric reference and an identity reference; biometric system application models with different scenarios for the storage of biometric references and comparison; and guidance on the protection of an individual's privacy during the processing of biometric information. The standard does not include general management issues related to physical security, environmental security and key management for cryptographic techniques.

Due to ongoing work on cross-jurisdictional issues related to the use of biometric technologies in commercial applications in JTC 1/SC 37, other standards under development in JTC 1/SC 27 are shared with JTC 1/SC 37 experts. Examples include A f*ramework for access management* (ISO/IEC 29146), *A Framework for Iidentity Management (*ISO/IEC 24760), *Privacy framework* (ISO/IEC 29100), *Privacy reference architecture* (ISO/IEC 29101) and *Entity authentication assurance* (ISO/IEC 29115).

### *2.2 Standards Activities Outside of ISO/IEC JTC 1*

As discussed above, other international organizations were or are currently involved in some aspects of biometric standardization or are referring to or using existing biometric standards for their own standards, specifications or requirements.

#### *2.2.1 ISO Technical Committee 68 – Financial Services – SC 2 – Security*

Technical Committee 68 (ISO/TC68) is the ISO standards development committee designated to develop standards and technical reports for the financial services industry. ISO/TC 68 standards cover a broad spectrum of financial services and transactions with specific focus on the securities market and related financial instruments, core banking, payments, and the information security to ensure the integrity and confidentiality of the financial infrastructure as a whole. ISO/TC68/SC2 focuses on the security requirements of the financial services industry.

In 2008, ISO/IEC published a standard developed by Subcommittee 2– *Security* of ISO Technical Committee 68 – *Financial Services.* ISO/IEC 19092:2008 *Financial services -- Biometrics -- Security framework* describes the security framework for using biometrics for authentication of individuals in financial services. It introduces the types of biometric technologies and addresses issues concerning their application. It also describes the architectures for implementation, specifies the minimum security requirements for effective management and provides control objectives and recommendations suitable for use by a professional practitioner. Its scope includes usage of biometrics for the authentication of employees and persons seeking financial services by verification of a claimed identity or identification of an individual; validation of credentials presented at enrolment to support authentication as required by risk management; management of biometric information across its life cycle; security of biometric information during its life cycle, encompassing data integrity, origin authentication and confidentiality; application of biometrics for logical and physical access control; surveillance to protect the financial institution and its customers; and security of the physical hardware used throughout the biometric information life cycle.

### *2.2.2 International Telecommunication Union - Study Group 17 (ITU-T/SG17)*

ITU-T Study Group 17 – *Security – ITU-T/SG 17 (2011)* is responsible for ITU-T's work on telecommunication security. It addresses challenges for more secure network infrastructure, services and applications. As of May 2011, over seventy standards (called "ITU-T Recommendations") were published. Within its scope of work, ITU-T/ SG 17 develops recommendations in the area of Telebiometrics (defined as "Biometrics in Telecommunication"). Within the well-established collaborative procedures between ITU-T and JTC 1 in areas such as security requirements, specifications and authentication, ITU-T SG 17 maintains close collaboration with JTC1/SC 37. This collaboration led to a joint development effort and publication of Recommendation X.1083 (ISO/IEC 24708:2008), *Biometric Interworking Protocol (BIP)*. This standard specifies the syntax, semantics, and encodings of a set of messages (BIP messages) that enable a BioAPI-conforming application (see ISO/IEC 19784-1) to request biometric operations in BioAPI-conforming biometric service providers (BSPs) across node or process boundaries and to be notified of events originating in those remote BSPs. It also specifies extensions to the architecture and behaviour of the BioAPI framework (specified in ISO/IEC 19784-1) that supports the creation, processing, sending and reception of BIP messages. It is applicable to all distributed applications of BioAPI.

ITU-T/SG 17 developed other Recommendations in the Telebiometrics area such as, Recommendation ITU-T X.1084:2008 *Telebiometrics System Mechanism* - Part1: *General biometric authentication protocol and profile for telecommunication systems*, Recommendation X.1086:2008 – *Telebiometrics Protection Procedures* - Part 1: *A guideline of technical and managerial countermeasures for biometric data security*, and Recommendation ITU-T X.1089:2008 *Telebiometrics Authentication Infrastructure*. Recommendation ITU-T X.1084 specifies biometric authentication protocols and profiles for telecommunication systems in open networks. It defines nine telebiometrics authentication models depending on the configuration of the client, the server and the trusted third party. It also defines the negotiation protocol for the policies and the device environments using the models. Furthermore, it specifies the requirements of biometric transportation data for each model.

Recommendation X.1086 defines the vulnerabilities and threats in operating telebiometric systems and proposes a general guideline for security countermeasures from both technical and managerial perspectives in order to establish a safe environment for the use of telebiometric systems and to protect individual privacy. Recommendation ITU-T X.1089 defines an authentication infrastructure, using a range of biometric certificates, for remote authentication of human beings. It extends Recommendation ITU-T X.509 Public-key and attribute certificate frameworks and ISO/IEC 24761 Authentication context for Biometrics developed by JTC 1/SC 27.

Representative ongoing work includes: (a) X.1086 (Amd. 1) – *Telebiometrics Protection Procedures* - Part1, Amd 1. – *Multibiometrics protection procedures*; (b) X.1091 – *Integrated framework for telebiometric data protection in e-health and word-wide medicines*; and (c) X.1098 – *A guideline for evaluating telebiometric template protection techniques.*

### 2.2.3 National Institute of Standards and Technology – Information Technology Laboratory (NIST/ITL)

The ANSI/NIST-ITL standard "Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information" is used by law enforcement, intelligence, military and homeland security organizations throughout the world. NIST/ITL (and its predecessor organizations) has been accredited by the American National Standards Institute as a standards developer since October 5, 1984. NIST/ITL is accredited to develop voluntary consensus standards as a sponsor using the ANSI Canvass Method for the following scope of activities: "*Standards and guidelines for information exchange relating to automatic data processing and related systems*". Under this responsibility, NIST/ITL has been developing a number of versions of the ANSI/NIST-ITL biometric standards. The first version of the standard dates to 1986. Over the years, it has been updated and expanded to cover more biometric modalities beyond the original record type of fingerprint minutiae. Revisions to the standard were made in 1993, 1997, 2000, and 2007. Updates to the standard are designed to be backward compatible, with new versions including additional biometric modalities and associated data. All of these versions used "Traditional" encoding. The latest published versions of the standard are ANSI/NIST-ITL 1-2007, Data Format for the Interchange of Fingerprint Facial, & Other Biometric Information - Part 1 and ANSI/NIST-ITL 1-2008, Part 2- XML Version.

ANSI/NIST-ITL 1-2007 Part 1 defines the content, format, and units of measurement for the exchange of fingerprint, palm print, facial/mug shot, scar mark & tattoo (SMT), iris, and other biometric sample information that may be used in the identification or verification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, related descriptive and record data, digitized fingerprint information and compressed or uncompressed images. This information is primarily intended for interchange among criminal justice administrations or organizations that rely on automated fingerprint and palm print identification systems, or use facial/mug shot, SMT, iris or other biometric data for identification purposes. The standard is specified using the conventional tagged-field format version.

ANSI/NIST-ITL 1-2008, Part 2 specifies the Extensible Markup Language (XML) version based upon the 2007 version. The 2007 and 2008 versions of the standard were designed to be the same except for the encoding. The XML encoding was developed using the naming conventions of the National Information Exchange Model (NIEM). Thus, this encoding is referred to as "NIEM-conformant XML." In 2009, a minor supplement to the 2007 and 2008 versions was approved that extended the codes for friction ridge images to include multiple finger capture.
The standard was currently updated to include new biometric modalities and associated data. This standard defines the content, format and units of measurement for the electronic exchange of fingerprint, palmprint, plantar, facial / mugshot, scar, mark & tattoo (SMT), iris, deoxyribonucleic acid (DNA) and other biometric sample and forensic information that may be used in the identification or verification process of a subject. The information consists of a variety of mandatory and optional items. This information is primarily intended for interchange among criminal justice administrations or organizations that rely on automated identification systems or use other biometric and image data for identification purposes. The updated version (2011) addresses both the Traditional and NIEM-conformant XML encodings in one standard version rather than two as found in the 2007/2008 versions. At the time of this writing, the draft standard which was recently completed is undergoing a ballot for final approval before publication NIST/ITL (2011).

A related conformance testing methodology standard for ANSI/NIST-ITL 1-2011 is under development at NIST/ITL with participation from NIST experts as well as experts from other government (federal, state and local)

institutions and industry. The first edition of this standard (planned as an Amendment to ANSI/NIST-ITL 1-2011) is expected to be completed in less than one year.

### 2.3 Standards Development Keeping Adoption in Mind

Although a detailed discussion on biometric standards adoption would be extensive and is beyond the scope of this paper, it is relevant to cite a few cases of biometric standards adoption of high impact within the user community that needs the standards in support of requirements for their personal verification or identification applications. One example of requirements that include biometric standards and data objects designed to contain biometric data is, as mentioned above, the ICAO. In addition to specifying data objects specified in a standard developed by JTC 1/SC 17, ICAO selected facial recognition as the globally interoperable biometric for machine-assisted identity confirmation for Machine Readable Travel Documents (MRTD) and requires conformance to the face recognition standard developed by JTC 1/SC 37. Other ICAO requirements for JTC 1/SC37 standards are the fingerprint data interchange formats and the iris recognition interchange format. ILO's requirements for the Seafarers' ID Card include the use of two fingerprint templates to be stored in a barcode placed in the area indicated by the ICAO's 9303 standard, and the requirements also specify the use of some of the standards approved by JTC 1/SC 37, specifically finger minutiae and finger image data interchange formats and an instantiation of the CBEFF data structure.

The European Union (EU) password specification working document EU (2006) describes solutions for chip enabled EU passports, based on EU's Council Regulation on standards for security features and biometrics in passports and travel documents issued by Member States EC (2004). The EU specification relies on international standards, especially ISO/IEC standards and ICAO recommendations on MRTDs, and includes specifications for biometric face and fingerprint identifiers; thus, the specifications are underpinned by ISO/IEC standards resulting from the work of JTC 1/SC 17 and JTC1/SC 37.

Many countries participating in the standards activities described above are also adopting standards developed by these standards bodies. In Spain, for example, the electronic national identity card (DNIe) includes personal information of the citizen, details of electronic certificates and the biometric information. The image of the face is stored following ISO/IEC 19794-5 and ICAO standards. Finger minutiae are stored using the ISO/IEC 19794-2 standard. In addition, the biometric data included in Spanish e-Passports is the image of the face based on ISO/IEC 19794-5 and ICAO standard compliant stored in JPEG2000 format (ISO 15444) Spain (2007). In the United States of America, several organizations require selected biometric data interchange standards developed by JTC1/SC 37, and some of the ongoing biometric testing programs use some of the performance testing methodology standards developed by the Subcommittee. The Registry of USA Government Recommended Biometric Standards developed by the Subcommittee of Biometrics and Identity Management of the Office of Science and Technology Policy, National Science and Technology Council recommends some of the standards developed by JTC 1/SC 37 NSTC Registry (2011).

As stated in SC 27 [2010]:

> "Standardized security techniques are becoming mandatory requirements for e- and m-commerce, health-care, telecoms, automotive and many other application areas in both the commercial and government sectors. The use of security techniques and in particular of identification, authentication and electronic signatures constitutes a core element in e-business, e-government and other on-line activities."

ITU-T Question 9/17 (Telebiometrics) ITU-T Q 9/17 (2011) prepared recently the environment for the usage of biometrics in telecommunication applications and provided necessary Recommendations. Tasks described include, but are not limited to, the enhancement of current Recommendations to accelerate their adoption to various telebiometric applications and populate the telebiometric database; study and develop security requirements and guidelines for any application of telebiometrics; study and develop requirements for evaluating security, conformance

and interoperability with privacy protection techniques for any application of telebiometrics; study and develop requirements for telebiometric applications in a high functionality network; study and develop requirements for telebiometric multi-factor authentication techniques based on biometric data protection and biometric encryption; and study and develop requirements for appropriate generic protocols providing safety, security, privacy protection and consent "for manipulating biometric data" in any application of telebiometrics (e.g. e-health, tele-medicine, tele-health).

The ANSI/NIST-ITL standards NIST/ITL (2011) have also been developed with adoption in mind, and they are widely adopted. As stated above, they have been used for many years by law enforcement, intelligence, military, and homeland security organizations throughout the world. One major use of the standard is for the Integrated Automated Fingerprint Identification System, more commonly known as IAFIS, by U.S. law enforcement (local, state, federal). INTERPOL has established a profile based on ANSI/NIST-ITL 1-2000 called INT-I and the Schengen Area's (EU except for UK & Ireland, plus Switzerland, Iceland and Norway) Visa Information System is also based on ANSI/NIST-ITL.

## 2.4 Conclusion

As discussed in the previous sessions a number of standards developers are addressing the development of biometric standards within their scope of work. These activities include three Subcommittees under the Joint Technical Committee of ISO/IEC as well as outside standards organizations. Examples have been provided on biometric standards adoption by large national and international organizations. Past and current activities show that the biometrics standards community is prepared to offer customers the standards needed to support biometric-based applications in open systems environments and that they can adapt their developments to technology innovations and current users' needs.

## References


ISO/IEC JTC 1 (2010), *ISO/IEC JTC 1 Value Proposition*, ISO/IEC JTC 1 N 10014, http://www.iso.org/iso/jtc_1_value_proposition.pdf

SC 37 (2011), JTC 1/SC 37 web page:http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=313770

SC 17 (2011), JTC 1 /SC 17 web page:http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45144

SC 27 (2011), JTC 1/SC 27 web page: http://www.iso.org/iso/standards_development/technical_committees/list_of_iso_technical_committees/iso_technical_committee.htm?commid=45306

ISO, 2011 List of Published Standards (per JTC 1 subcommittee): http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=45020

Technical Committee 68 (ISO/TC68) ISO/TC 68 Home page: http://isotc.iso.org/livelink/livelink/open/tc68

ITU-T/SG 17 (2011) ITU-T/SC 17 Home page: *http://www.itu.int/net/ITU-T/info/sg17.aspx*

ICAO (2011), ICAO web page: http://www2.icao.int/en/home/default.aspx

ILO (2011), ILO web page: http://www.ilo.org/global/lang--en/index.htm

NIST/ITL (2011), ANSI/NIST[ITL Standard home page: http://www.nist.gov/itl/iad/ig/ansi_standard.cfm

ITU-T Question 9/17 –Telebiometrics Home Page: http://www.itu.int/ITU-T/studygroups/com17/sg17-q9.html

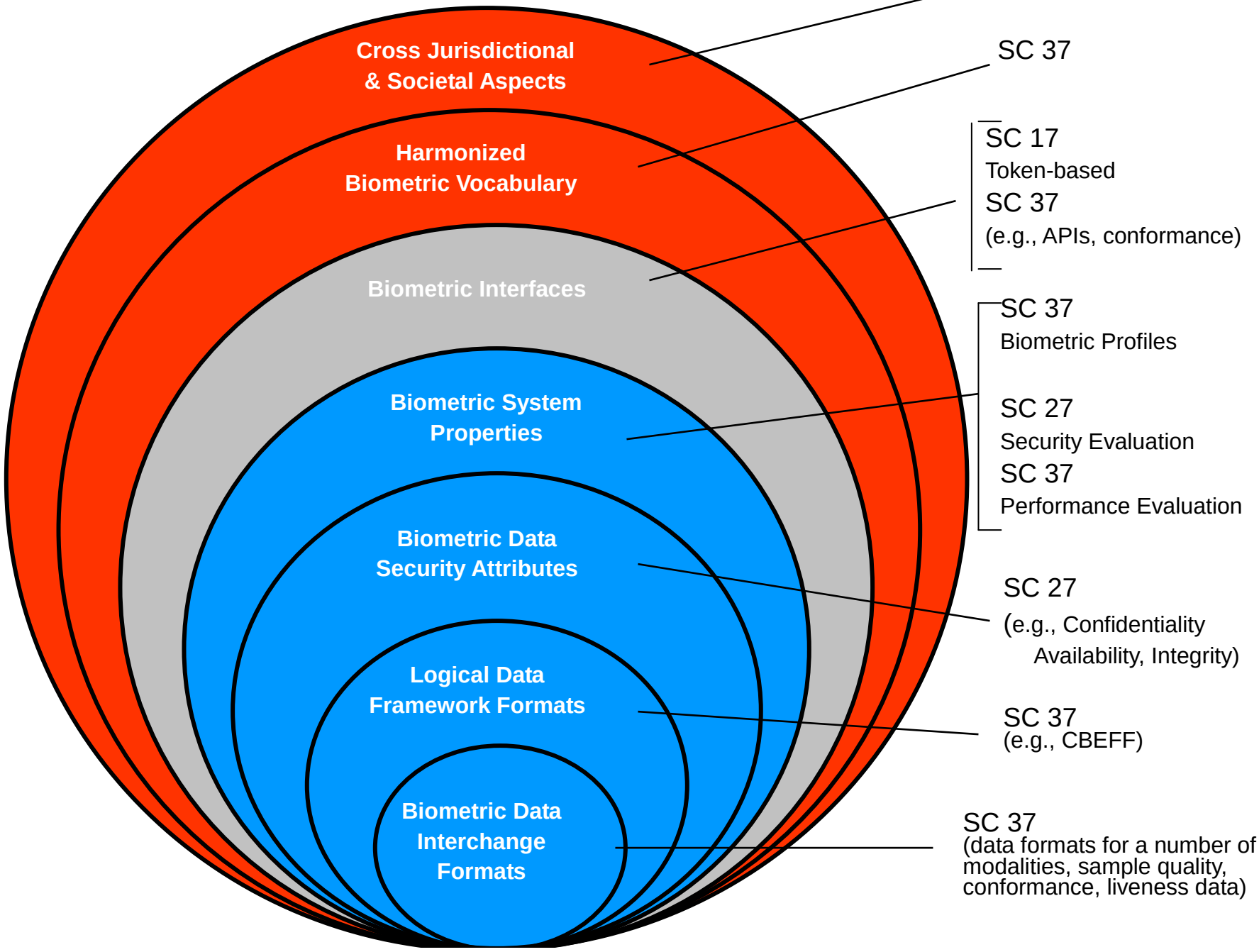
EU (2006) "Biometrics Deployment of EU-Passports", The European Union password specification working document (EN) – 28 June, 2006.

EC (2004) EC Council Regulation No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. Official Journal of the European Union, L 385/1.

Spain (2007) Communication from Dr. Angel L. Puebla, president of AEN CTN71/SC37 (Spanish Subcommittee of Biometric Identification), Economic and Technical Coordination Division of the Spanish Main Directorate of the Police and the Civil Guard, July 2007.

NSTC Registry (2011) "Registry of USG Recommended Biometric Standards, Version 1.0, June 2008, Version 2.0, August 2009 and Version 3.0, February 8, 2011, Subcommittee of Biometrics and Identity Management, Office of Science and Technology Policy, National Science and Technology Council, http://www.biometrics.gov/Standards/Default.aspx

Figure 1 - ISO/IEC JTC1 Biometric Standards Activities*




The “onion” representation of biometric standards activities was derived from a similar representation developed by Dr. Colin Soutar.