FINAL WORKSHOP REPORT

BIOMETRIC STANDARDIZATION

A PUBLICATION OF THE
ANSI HOMELAND SECURITY STANDARDS PANEL

APRIL 2004

ANSI
American National Standards Institute

Table of Contents

Background on Biometric Standardization 3
List of Biometric Standards 8
ANSI Accredited Standards Committee X9 (Financial Services) 8
InterNational Committee for Information Technology Standards (INCITS) Technical Committee M1 - Biometrics 8
ISO/TC 68 – Banking, Securities, and other Financial Services 14
ISO/IEC JTC 1/SC 17 – Cards and Personal Identification 14
ISO/IEC JTC 1/SC 27 – IT Security Techniques 15
ISO/IEC JTC 1/SC 37 – Biometrics 15
National Institute of Standards and Technology (NIST) 25
Issues Identified at the ANSI-HSSP Biometrics Workshop and Subsequent Recommendations 27

Background on Biometric Standardization[1]

Introduction

Biometric technologies are becoming the foundation of an array of highly secure identification and verification solutions. Biometric technologies consist of automated methods of identifying a person or verifying the identity of a person based upon recognition of a physiological or a behavioral characteristic. Physiological characteristics include hand, finger, facial, iris, and speech. Behavioral characteristics are traits that are learned or acquired, such as dynamic signature verification and keystroke dynamics.

A biometric identification (or "1 to N matching") consists of matching a biometric sample against all records in a database of biometric identifiers. A biometric verification (or "1 to 1 matching") consists of matching the enrolled biometric sample against a single record. Biometric-based solutions can enable confidential financial transactions and personal data privacy. Enterprise-wide network security infrastructures, employee IDs, secure electronic banking and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from the application of biometric technologies.

Tying your biometric to your personal information can prevent identity theft, which occurs when someone appropriates your personal information without your knowledge to commit fraud or theft. As the incidences of security breaches and transaction fraud increase, the need for highly secure biometric identification and verification technologies becomes more apparent. A recent Federal Trade Commission report said identity theft complaints were the most common consumer fraud complaints last year with losses estimated at $343 million. Homeland security can also benefit from the utilization of biometric technologies. New Public Laws, such as the U.S.A. Patriot Act and the Enhanced Border Security Act, are relying on the deployment of biometric solutions.

To date, the many biometric standards activities underway have largely been successfully coordinated. Over the past eighteen months, the U.S has quickly worked to establish formal standards groups for accelerating and harmonizing the development of national and international biometric standards of high relevance to the U.S. The work of these new groups, the InterNational Committee for Information Technology Standards (INCITS) Technical Committee M1 and ISO/IEC JTC 1/SC 37, and others is described below.

Consortia Biometric Standards Activities

From 1999 to 2001, the BioAPI Consortium developed and approved the ***BioAPI Specification***. Subsequently, it was approved in February 2002, via INCITS fast track process, as **ANSI INCITS 358-2002**. It defines an open systems common application programming interface (API) between applications and biometric technology modules. The implementation of compliant solutions allow for the easy substitution of biometric

[1] A version of this text originally appeared in the Spring 2003 edition of the *ANSI Reporter*.

technologies, the utilization of biometric technologies across multiple applications, easy integration of multiple biometrics, and the rapid development of applications. The development of a single approach specified in this standard promotes interoperability among applications and biometric subsystems by defining a generic way of interfacing to a broad range of biometric technologies.

From 1999 to 2000, the Common Biometric Exchange File Format Development Team, sponsored by the National Institute of Standards and Technology (NIST) and the Biometric Consortium (BC), developed the ***Common Biometric Exchange File Format*** (CBEFF). CBEFF defines a biometric data structure, which assures that different biometric devices and applications can exchange biometric information efficiently. This common format facilitates exchange and interoperability of biometric data from all modalities of biometrics independent of the particular vendor that would generate the biometric data. CBEFF was published as NISTIR 6529 in January 2001. CBEFF is being incorporated in U.S. government and international requirements such as the technical specifications drafted by the International Civil Aviation Organization (ICAO).

The Biometric Interoperability, Performance, and Assurance Working Group, sponsored by NIST and the BC (NIST/BC Biometric WG) recently approved an augmented version of CBEFF, called the ***Common Biometric Exchange Formats Framework***. This revised version includes the specification of a nested structure that accommodates biometric data from multiple biometric types such as finger, facial and iris data in the same structure and also accommodates multiple samples of a specific biometric type. It also defines a Product Identifier that allows an application to determine the biometric data originator, and a CBEFF compatible smart card biometric data structure.

The NIST/BC Biometric WG has recently also approved two other biometric specifications, ***Template Protection and Usage*** and ***Biometric Application Programming (API) Interface for Java Card™***. Both specifications and the augmented version of CBEFF are candidates for further formal standardization.

The Open Group has developed an extension with a biometric component, ***Human Recognition Services Module*** (HRS***)***, to their ***Common Data Security Architecture*** (CDSA). CDSA is a set of layered security services and a cryptographic framework that provides the infrastructure for creating cross-platform, interoperable, security-enabled applications for client-server environments. The biometric component of the HRS is used in conjunction with other security modules (i.e., cryptographic, digital certificates, and data libraries) and is compatible with the BioAPI Specification and CBEFF.

Recently, the Organization for the Advancement of Structured Information Standards (OASIS) developed a specification, ***XML Common Biometric Format*** (XCBF) which intends to be CBEFF compliant to NISTIR 6529.

Formal National Biometric Standards Activities

Over the past two decades, biometric technology has been integrated with advances in information technology to provide new abilities for law enforcement. In September 2000, NIST published NIST Special Publication SP 500-245, ***ANSI/NIST-ITL 1-2000 Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information***. The standard specifies a common format to be used to exchange fingerprint, facial, scars, mark, and tattoo identification data effectively across jurisdictional lines or between dissimilar systems made by different manufacturers. All Federal, state and local law enforcement data are transmitted using this standard.

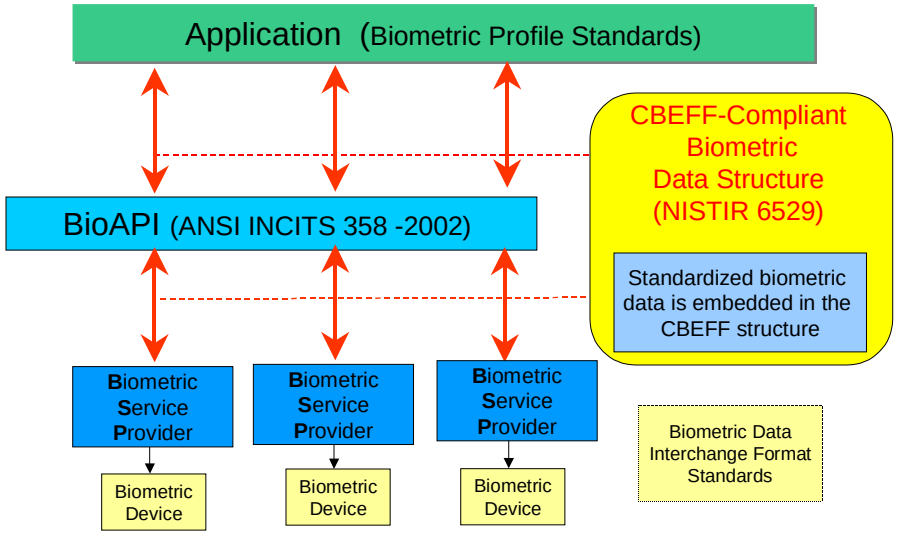
Accredited Standards Committee X9 (ASC X9) *Financial Services* is the only industry-wide forum that brings together bankers, securities professionals, manufacturers, regulators, associations, consultants, and others in the financial services industry to address technical issues, find the best solutions, and codify them as nationally accepted standards. ASC X9 has developed and published ***ANSI X9.84-2003, Biometrics Management and Security for the Financial Services Industry***. X9.84-2003 specifies the minimum-security requirements for effective management of biometrics data for the financial services industry and the security for the collection, distribution and processing of biometrics data. The recently published 2003 edition accommodates new areas, such as XML applications.

In November 2001, the INCITS Executive Board established Technical Committee M1 on Biometrics. M1 was established to ensure a high priority, focused and comprehensive approach in the United States for the rapid development and approval of formal national and international biometric standards for biometric data interchange and interoperability (see Figure 1). The M1 current program of work includes biometric standards for data interchange formats, exchange framework formats, APIs, profiles, and performance testing and reporting. M1 is now also serving as the U.S. Technical Advisory Group (TAG) to the new ISO/IEC Joint Technical Committee 1 (JTC 1) Subcommittee 37 on Biometrics.

M1 has created four new Task Groups to handle increased activity in biometrics:

- M1.2 - Biometric Technical Interfaces
- M1.3 - Biometric Data Interchange Formats,
- M1.4 - Biometric Profiles
- M1.5 - Biometric Performance Testing and Reporting

Figure 1: The Role of Standards in
Biometric Interoperability and Data Interchange



Formal International Biometric Standards Activities

ISO/IEC Joint Technical Committee 1 (JTC 1) established Subcommittee 37 on Biometrics in June 2002. The formation of JTC 1/SC 37 was initiated and championed by the U.S. The establishment of JTC 1/SC 37 provides an international venue to accelerate and harmonize formal international biometric standardization. Such harmonization will help to ensure that future standards based systems and applications are more interoperable, scalable, reliable, usable, and secure.

The following working groups report to JTC 1/SC 37:

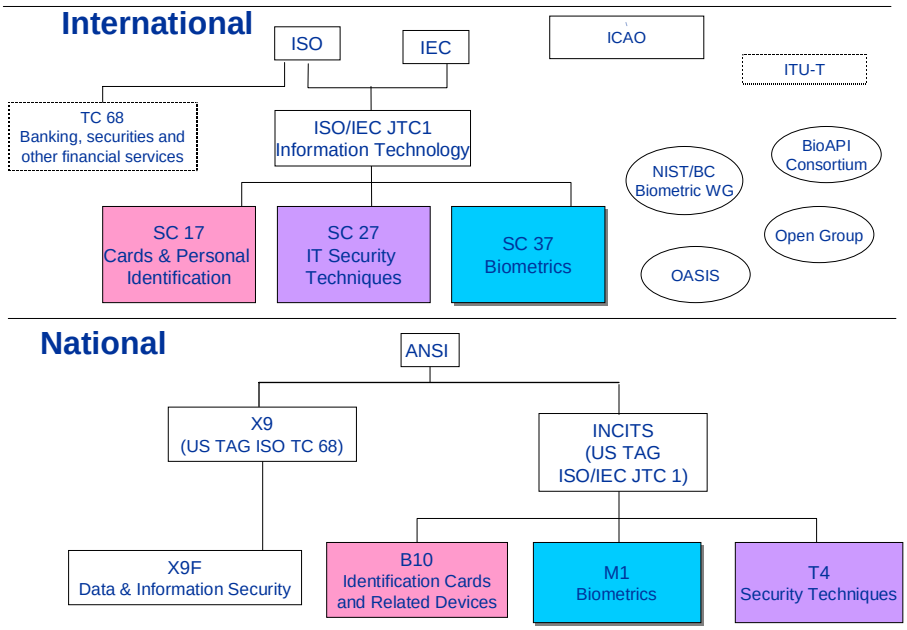
- WG 1 - Harmonized Biometric Vocabulary and Definitions
- WG 2 - Biometric Technical Interfaces
- WG 3 - Biometric Data Interchange Formats
- WG 4 - Biometric Functional Arcitecture and Related Profiles
- WG 5 - Biometric Testing and Reporting
- WG 6 - Cross-Jurisdictional and Societal Aspects

Other ongoing standards development includes a structure for biometric data on smart cards (**ISO/IEC FCD 7816-11**). This project is being done in ISO/IEC JTC 1/SC 17, Cards and Personal Identification. The recently approved NIST/BC Biometric WG biometric specification, ***Biometric Identifier Protection and Usage***, will be proposed to ISO/IEC JTC 1/SC 27, IT Security Techniques through the US TAG to SC 27, for processing as a formal international standard.

Summary

Post September 11th deployment of highly secure biometric security solutions will be challenging. A comprehensive infrastructure for biometric standardization has now been put into place to help answer this challenge (see Figure 2). INCITS Technical Committee M1, ISO/IEC JTC 1/SC 37 and others are now positioned to accomplish the timely development of harmonized formal national and international biometric standards - a key to a more secure world.

Figure 2: Biometrics Standards Activities



List of Biometric Standards

For more information on the development of American National Standards (ANS), please visit the ANSI website. Further information on the development of international ISO standards can be found on the ISO website.

ANSI Accredited Standards Committee X9 (Financial Services)

Designation	Title	Abstract	Status
ANSI X9.84 - 2003	Biometric Information Management and Security for the Financial Services Industry	X9.84 Biometric Information Management and Security defines requirements for managing and securing biometric information used in the financial services industry.	Published 2003 (replaces 2001 edition)

InterNational Committee for Information Technology Standards (INCITS) Technical Committee M1 - Biometrics

BSR INCITS PN-1566-D INCITS 383	Information Technology - Application Profile - Interoperability and Data Interchange - Biometrics Based Verification and Identification of Transportation Workers	This proposed standard is intended to support the development of biometric technologies in order to provide for significantly higher levels of interoperability and data interchange in biometric-based worker verification and identification within transportation systems (e.g., civil aviation systems)	Public Review concluded – awaiting submittal from SDO

BSR INCITS PN-1567D	Information Technology - Application Profile for Interoperability, Data Interchange and Data Integrity of Biometric Based Personal Identification for Border Management	This proposed Application Profile will define the functional requirements for biometric-based verification and identification of persons within border management applications and systems and will reference the use of specific requirements and/or options in relevant base standards in order to provide for biometric interoperability and data interchange in border management systems.	Project Initiation Notification System (PINS) announced
BSR INCITS PN-1575-D	Information Technology - Application Profile for Point-of-Sale Biometric Verification/Identification	This proposed standard will describe an application profile for use of biometrics in point-of-sale situations. Point-of-Sale (abbreviated POS) describes a wide range of applications where payment (in cash or other form) is exchanged for some good or service. In particular, points-of-sale may be attended or unattended. This standard is intended to describe the specific method of use of biometrics including: biometric enrollment methods for POS; media types for containing biometric information for POS; scenarios of use in POS; strategies for securing biometric data in POS applications; any other areas necessary to standardize for POS.	PINS announced
BSR INCITS PN-1602-D	Information technology - Biometric Performance Testing and Reporting	This proposed standard would establish common procedures for testing and reporting the performance of biometric systems. In addition, this proposed standard would specify the reporting requirements the compliant declarations must meet in association with such reports.	PINS announced

ANSI INCITS 377 - 2004	Information technology - Finger Pattern Based Interchange Format	This standard specifies an interchange format for the exchange of pattern-based fingerprint recognition data. It describes the conversion of a raw fingerprint image to a cropped and down- sampled finger pattern followed by the cellular representation of the finger pattern image to create the finger-pattern interchange data.	Published in 2004
ANSI INCITS 378-2004	Information technology - Finger Minutiae Format for Data Interchange	This Standard specifies a concept and data format for representation of fingerprints using the fundamental notion of minutiae. The data format is generic, in that it may be applied and used in a wide range of application areas where automated fingerprint recognition is involved. No application-specific requirements or features are addressed in this standard. This standard contains definitions of relevant terms, a description of where minutiae shall be defined, a data format for containing the data and conformance information.	Published in 2004

INCITS 379	Information technology - Iris Image Interchange Format	This Standard specifies two alternative image interchange formats for biometric authentication systems that utilize iris recognition. The first is based on a rectilinear image storage format that may be a raw, uncompressed array of intensity values or a compressed format such as that specified b the JPEG standard. Images may be monochrome or color with 256 or more intensity levels (grey or per-color), and vary in size depending on field of view and compression. Typical size is 25-30 Kbytes for JPEG format. The second format is based on a polar image specification that requires certain pre-processing and image segmentation steps, but produces a much more compact data structure that contains only iris information. the record size can be as small as 2 Kbytes. The polar image may be either raw or compressed format. Data that comply with either one of the iris image formats specified in this standard are intended to be embedded in a CBEFF-compliant structure in the CBEFF Biometric Data Block (BDB).	Second Public Review concluded

INCITS 381	Information technology - Finger Image Based Interchange Format	This standard specifies a data record interchange format for storing, recording, and transmitting the information from one or more finger or palm image areas within a CBEFF data structure. This proposed standard could be used for the exchange and comparison of finger image data. It defines the content, format, and units of measurement for the exchange of finger image data that may be used in the verification or identification process of a subject. The information consists of a variety of mandatory and optional items, including scanning parameters, compressed or uncompressed images and vendor-specific information. This information is intended for interchange among organizations that rely on automated devices and systems for identification or verification purposes based on the information from finger image areas. Information compiled and formatted in accordance with this standard can be recorded on machine-readable media or may be transmitted by data communication facilities.	Completed Public Review
INCITS PN- 1565-D	Information Technology - Face Recognition Format for Data Interchange	This proposed standard will define a data format for representing a face recognition record. The standard will contain a specific definition of attributes, A data record format for storing and transmitting the face image and attributes and a sample record and may include conformance criteria.	PINS announced

INCITS PN-1603-D	Information technology - Signature/Sign Image Based Interchange Format	This proposed standard will define a data record interchange format for storing, processing or transmitting the information from the sign or signature image data. There are currently numerous digitizers used for capturing signature data in this manner and there are also a numer of different methods of representing these data for the purpose of recording the electronic signatures.	PINS announced
INCITS PN- 1627-S	Information technology - Evaluating Multi-Modal Biometrics Systems: Concepts of Operation and Methods of Performance Evaluation (study project)	The proposed study project would define and specify methods of evaluating multi-modal biometric systems, in particular categorizing various terms and concepts of operation in multi-modal biometric systems. The proposed study project would also specify methods of evaluating performance in multi-modal biometric systems.	Study Project that is expected to result in a Project Report PINS announced
INCITS PN-1643-D	Information technology - Hand Geometry Format for Data Interchange	The purpose of this document is to define a standard for capturing signs/signatures for the purpose of biometric comparison. It is not intended to define a standard for electronic signature capture for other purposes, although it may be relevant to those applications.	PINS announced
INCITS PN-1676-D	Information technology - Biometric Profile - Interoperability and Data Interchange - DoD Implementations	The proposed standard is intended to support the deployment of biometric technologies in US Department of Defense (DoD) organizations and activities. The proposed standard's goals include facilitating an increase of interoperability and data interchange in DoD deployments of biometrics.	PINS announced

ISO/TC 68 – Banking, Securities, and other Financial Services

ISO/WD 19092	Biometric information management and security	This work item defines the components of a biometric authentication system and sets forth a framework of operational and technical practices and policy requirements for biometric authentication within the financial services industry. This work will result in a standard that provides techniques satisfying the privacy, integrity and authenticity of origin requirements for securely managing biometric information during the enrollment, verification and identification processes common to all biometric systems, and the secure storage and transmission of sensitive information that is increasingly bound to financial transactions. It further identifies the baseline operational and technical practices relative to broadly accepted information systems control objectives.	Working draft

ISO/IEC JTC 1/SC 17 – Cards and Personal Identification

ISO/IEC FDIS 7816-11	Identification cards -- Integrated circuit(s) cards with contacts -- Part 11: Personal verification through biometric methods		Currently under publication as International Standard
ISO/IEC AWI 18013-3	Information technology -- Motor Vehicle License -- Part 3: Biometrics, image processing and cryptography		Approved work item

ISO/IEC JTC 1/SC 27 – IT Security Techniques

ISO/IEC AWI 19792	Information technology -- Security techniques -- Framework for Security Evaluation and Testing of Biometric Technology		Approved work item

ISO/IEC JTC 1/SC 37 – Biometrics

Standing Document 2	Standing Document on Harmonized Biometric Vocabulary	This standing document will provide a systemic description of the concepts in the field of biometrics and will clarify the use of the terms in this field. The compilation of this vocabulary provided a forum for analyzing, discussing and coordinating key concepts found in ISO/IEC JTC1 SC 37 standards. This standing document is addressed to biometrics standardizers.	Document under review
ISO/IEC WD 19794-1	Information technology -- Biometric data interchange formats -- Part 1: Framework/Reference Model	This part will contain common requirements and approach of use of biometric data interchange formats. Exclusions from the data interchange formats will also be included here, such as an embedded link to the identity of the individual.	Working Draft

ISO/IEC FCD 19794-2	Information technology -- Biometric data interchange formats -- Part 2: Finger Minutiae Data Interchange Format	This part of the proposed standard will define an interchange format for representing one or more fingerprints in a "feature-based" manner, using the principle of minutiae points. The interchange format will contain a specific definition of minutiae points and other related attributes, a data record format for storing and transmitting the attributes, a sample record and may include conformance criteria.	Final Committee draft under ballot
ISO/IEC CD 19794-3	Information technology -- Biometric data interchange formats -- Part 3: Finger Pattern Spectral Data Interchange Format	In the interest of implementing interoperable personal biometric recognition systems, this ISO/IEC Standard establishes a data interchange format for fingerprint spectral data exchange. Goal of the standard: to allow the exchange of local or global spectral data derived from a fingerprint image without the exchange of the entire image. This will allow more compact data representations. Further, we wish the standard to be useful to many aspects of the fingerprint recognition process, possibly including flow field extraction, level 1 characterization, "core" location, quality assessment, comparison methods, and (possibly) "privacy" assurance. This standard would allow for representation of both Discrete Fourier Transform and (single-scale) Gabor Filter components extracted from global or stationary (not image dependent and not varying over the image) local overlapping or non-overlapping uniform-sized regions of the original intensity (non-color) image. Some or all of the extracted spectral components will be stored in the data format, depending upon the implementation.	Committe Draft under ballot

ISO/IEC FCD 19794-4	Information technology -- Biometric data interchange formats -- Part 4: Finger Image Data Interchange Format	This part of the proposed standard will define a data record interchange format for storing and transmitting the information from a finger image area. The interchange format will contain detailed pixel information from the friction ridges and valleys of the image. It will define the content, format and units of measurement, and method of image compression for the exchange of fingerprint image information, and may consider quality metrics of the image.	Final Committee draft under ballot
ISO/IEC FCD 19794-5	Information technology -- Biometric data interchange formats -- Part 5: Face Image Data Interchange Format	This part of the proposed standard will develop an image-based interchange format for face recognition algorithms as well as human examination. The header of the format will contain generic geometric attributes of the image, the color characteristics of the image (when available), the eye positions and other significant landmarks of the face required for automatic recognition when available. The data will include the grayscale or color face image data. Both one-to-one and one-to-many applications will be supported.	Final Committee draft under ballot
ISO/IEC FCD 19794-6	Information technology -- Biometric data interchange formats -- Part 6: Iris Image Data Interchange Format	This part of the proposed standard will develop image-based interchange formats for iris recognition algorithms. The interchange format will comprise of a header and data. The header will contain the image coordinate system, the dimensions of the image, and other parameters to be defined. The data will include the grayscale image data.	Final Committee draft

ISO/IEC WD 19794-7	Information technology - Biometric data interchange formats - Part 7: Signature/Sign Behavioral Data Interchange Format	The proposed standard for signature/sign based biometric data interchange format will: •Allow interoperability across digitizers and to some extent across biometric technology vendors. •Encourage the adoption of biometrics in applications where interoperability is required. •Provision of this standard will provide improved visibility and marketing of SC37 standardization work.	Working Draft
ISO/IEC WD 19794-8	Information technology -- Biometric data interchange formats -- Part 8: Finger Pattern Skeletal Data Interchange Format	This Standard specifies the interchange format for the exchange of pattern-based fingerprint recognition data. The data format is generic, in that it may be applied and used in a wide range of application areas where automated fingerprint recognition is involved.	Committee Draft under ballot

ISO/IEC WD 19795-1	Information technology -- Biometrics performance testing and reporting - Part 1: Test Principles	The proposed standard would establish a framework for evaluating the technical performance of biometric systems. This framework would include: • definitions of performance measures of interest, • design of performance tests, • execution of tests, • data collection, • analyses, and • reporting. Such a framework would assure integrity of results and commonality of presentation, and will help obtain better estimates of real-world performance for single vendor biometric systems as well as those consisting of interoperable biometric components The scope would include technology, scenario and operational evaluations (as defined in Phillips et al. Computer, Feb 2000, 56-63), but exclude aspects of performance such as: • reliability, availability and maintainability, • security and vulnerability, and • user acceptance.	Working Draft
ISO/IEC WD 19795-2	Information technology -- Biometrics performance testing and reporting - Part 2: Testing methodologies	See 19795-1.	Working Draft
ISO/IEC AWI 19795-3	Information technology -- Biometrics performance testing and reporting - Part 3: Specific testing methodologies	See 19795-1.	Approved work item

ISO/IEC AWI 19795-4	Information technology -- Biometrics performance testing and reporting - Part 4: Specific test programmes	See 19795-1.	Approved work item
ISO/IEC FCD 19784	Information Technology -- Biometric Application Programme Interface (BioAPI)	The BioAPI Specification, Version 1.1, defines a common method of communication between a software application and an underlying biometric technology module/service. It is composed of a set of C function calls, defined data structures, and related information such as error handling as well as conformance requirements. The intent of the specification was to provide an open system specification that would support a broad range of applications and be biometric technology/vendor neutral. Function calls are defined at the API level (i.e., between the application and the framework) and at the SPI level (i.e., between the framework and the service provider, known as a BSP – Biometric Service Provider). A minimum set of calls are defined which cover module management, data management, and operations. Operational functions are defined to provide for all of the basic operations common across a variety of biometric technologies; that is, those generally provided in a vendor's SDK but avoiding any vendor/technology specific (unique) features to the extent possible. Examples of these include basic functions such as Enroll, Verify, Identify, and primitive functions such as Capture, Process, CreateTemplate, Verify_Match, and Identify_Match. In addition to standardizing functions, the BioAPI Specification also standardized on a biometric data structure (later abstracted within CBEFF) and a normalized method for performing scoring and thresholding. These were two areas of critical need within the biometrics industry and the source of much discussion during the development of the specification.	Second Final committee draft ballot to be issued in July 2004

ISO/IEC FCD 19785-1	Information technology -- Common Biometric Exchange Formats Framework (CBEFF) - Part 1: Data Element Specification	CBEFF includes the definition of format and content for data elements such as: • A biometric data header that contains such information as version number, length of data, whether the data is encrypted or not, etc., for each biometric type available to the application or system; • Biometric data (content not specified); • A Basic Biometric Data Structure (Data Header plus processed or raw Biometric Data); • Any other required biometric data or data structures. CBEFF also describes a nested Biometric Data Structure; and the means for obtaining a unique value for identifying the format (owner and type) of the biometric data. CBEFF focuses on the description of the Biometric data elements. In order to decode CBEFF data, the applications need to have previous knowledge of the organization that has defined a standard or specification incorporating biometric data objects that meet CBEFF requirements and the data encoding scheme that was used. These organizations are defined as CBEFF Patrons. A Patron identifier is not included within the CBEFF definition. Each CBEFF Patron is required to define which CBEFF optional fields are present in their format and how the data elements are extracted and processed (details such as the data encoding scheme are left up to the CBEFF Patrons).	Final committee draft
ISO/IEC FCD 19785-2	Information technology -- Common Biometric Exchange Formats Framework (CBEFF) - Part 2: Procedures for the Operation of the Biometrics Registration Authority	See 19785-1	Final Committee Draft

ISO/IEC WD 24708	Information technology -- Biometric Interworking Protocol	This International Standard specifies the messages/exchange formats (down to the bit-level) for messages that are to be transferred (over some carrier such as TCP/IP) between a system supporting a (single) biometric device and a central repository of biometric data. This International Standard provides messages to support all the main functions defined in the BioAPI interface, such as BioAPI_Enroll, BioAPI_VerifyMatch, BioAPI-Identify_Match, etc, and is fully aligned with the BioAPI Standard (see the supporting document for further detail).	Working Draft
ISO/IEC WD 24709	Information technology -- Conformance Testing Method and Procedure for BioAPI of ISO 19784 Part 1	This proposed work item will describe the conformance test suite for BioAPI specification ver.1.1 based on Windows systems. The conformance test suite will test if the both verification and identification BSPs are compliant to BioAPI specification ver1.1 for various items such as valid input/output and SPI functions including mandatory and optional functions.	Working draft
ISO/IEC WD 24713-1	Biometric Profiles for Interoperability and Data Interchange - Part 1: Biometric Reference Architecture	This is Part 1 of the proposed multi-part standard for biometric profiles which will define biometric functions and will reference the use of specific requirements and/or options in relevant base standards in order to provide for interoperability and data interchange of biometric information. This part of the standard will define the functional blocks of biometric systems. It will also define a biometric reference architecture incorporating the relevant biometric-related base standards to support interoperability and data interchange.	Working Draft

ISO/IEC WD 24713-2	Biometric Profiles for Interoperability and Data Interchange - Part 2: Biometric Profile for Employees	This is Part 2 of the proposed multi-part standard for biometric profiles which will define biometric functions and will reference the use of specific requirements and/or options in relevant base standards in order to provide for interoperability and data interchange of biometric information. This part of the standard will define the specific profile for use by employers for employees. It will define the functions necessary to use a set of base standards; it will list the optional fields and parameters of the base standards and identify the elements of the base standard used to perform the functions; and will provide an implementation conformance statement proforma for use in determining conformance, interoperability, and data interchange.	Working Draft

ISO/IEC AWI 24714	Multi-part Technical Report on Cross Jurisdictional and Societal Aspects of Implementations of Biometric Technologies	This proposed multi-part technical report will provide a base for further development of standards in the context of cross-jurisdictional and societal aspects of the application of ISO/IEC biometric standards, including both existing technologies considered for standardization, and prospective technologies. Cross-jurisdictional and societal aspects include the support of design and implementation of biometric technolgies with respect to: -accessibility -health and safety -support of legal requirements and acknowledgement of cross-jurisdictional and societal considerations pertaining to personal information. Specficiation and assessment of government policy are excluded. Part 1 will focus on generic aspects of the implementation of all biometric technologies. Part 2 will focus on particular issues in the implementation of biometric technologies in different contexts. Further, the Technical Report shall identify the issues and technologies appropriate for SC 37 to address within its technical standards and programme of work. Remaining issues shall be examined by identifiying the bodies/forums (inside and outside ISO/IEC) in which they are currently being addressed or by recommending alternative bodies/forums best suited to address these issues.	Approved work item

ISO/IEC AWI 24722	Multi-Modal Biometric Fusion	This proposed technical report will analyze existing methods and practices for fusion in multi-modal biometric systems, for the purpose of identifying areas requiring future standardization. The technical report will focus on methods of using match results from separate comparisons of different biometric characteristics (result fusion). Thus, it will not deal with methods of combining biometric samples obtained from devices for capturing different biometric characteristics (source fusion).	Approved work item

National Institute of Standards and Technology (NIST)

ANSI/NIST-ITL 1-2000	Information Systems- Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information	This standard specifies formats to be used for exchanging fingerprint and other image data. It defines the content, format and units of measurement for the exchange of fingerprint, palmprint, facial/mugshot, and SMT image information that may be used in the identification 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 intended for interchange among criminal justice administrations or organizations that rely on automated fingerprint and palmprint identification systems or use facial/mugshot or SMT data for identification purposes.	Approved standard in use by the FBI and other federal, state, and local agencies. It is also a de facto standard used by the UK's Home Office and Interpol.

Issues Identified at the ANSI-HSSP Biometrics Workshop and Subsequent Recommendations

Issue #1

Need for a single certification body for biometrics products that are expected to be utilized in the Department of Homeland Security (DHS)/Transportation Security Administration (TSA) applications to make the process more efficient and to prevent situations such as airports having to decide which biometric products to buy on their own.

Recommendation/Current Work Underway

INCITS/M1 has formed the Ad Hoc Group "Issues for Harmonizing Conformity Assessment to Biometric Standards" with the following terms of reference:

- Develop a taxonomy, which identifies and defines the possible types of activities that may occur under Conformity Assessment schemes (e.g., supplier's declaration, laboratory accreditation, conformance testing and reporting, test tool(s) development and maintenance, conformance test results and certification/validation).
- Map the ISO/CASCO, Committee on conformity assessment, developed guides and standards to the above activities.
- Identify the various kinds of biometric standards, which M1 could develop for use in biometric standards based conformance testing programs.
- Identify issues and solutions for harmonizing biometric standards-based conformance testing programs.
- Develop recommendations to M1 on US national body comments on document JTC 1/SC 37 N 395 and subsequent editions.

The Ad Hoc Group will work between M1 Meeting #9 (January 2004) and Meeting #11 (May 2004). The output of this work will be a report to M1 for consideration by M1 as: an M1 standing document, possible subsequent publication as a NISTIR, and possible submission as a US national body contribution to the international committee ISO/IEC JTC 1/SC 37 (Biometrics).

Issue #2

Need for speaker recognition interoperability standards

Recommendation/Current Work Underway

The workshop recommends that INCITS and INCITS/M1 approach the speaker recognition industry and interested users to explore the initiation of a project(s) for data interchange and interoperability for this technology under INCITS/M1. The workshop further recommends to M1 that this work also be proposed to JTC 1/SC 37 after a national project is underway in M1.

Issue #3
Is there an entity(s) planning to run a performance testing program for biometric standards? If not, this issue needs to be addressed.

Recommendation/Current Work Underway
NIST is responding to legislative requirements by conducting performance evaluations for biometric technologies (fingerprint and face). It is expected that other key government users (i.e., DoD Biometric Management Office will undertake other aspects of biometric testing.

Issue #4
Conformance testing methodologies should be developed for the biometric interoperability standards under development. Test tools can then be developed based on these testing methodology standards. Once testing takes place, expedited approaches to re-testing need to be found

Recommendation/Current Work Underway
The M1 Ad Hoc Group on "Issues for Harmonizing Conformity Assessment (CA) to Biometric Standards" is developing a taxonomy that identifies and defines the possible types of activities that may occur under Conformity Assessment Schemes and identifies the various kinds of biometric standards which M1 could develop for use in biometric standards-based conformance testing programs. Additionally, NIST, under its program on accelerating the development of national and international biometric standards, is taking a leadership role in working with industry and users in identifying issues and solutions for harmonizing biometric standards-based conformance testing programs. NIST is supporting initial biometrics CA efforts by contributing experts in CA. Some M1 members are considering proposing CA testing methodology projects.

Issue #5
The users need, in the shortest timeframe possible, the performance evaluation standards that are being developed under INCITS/M1 and JTC 1/SC 37.

Recommendation/Current Work Underway
Users of these standards and industry technical experts not currently involved in these efforts should consider participation in the development of these standards.