Published International Biometric Standards Developed by ISO/IEC JTC 1/SC 37 – *Biometrics and* Adopted by INCITS as INCITS/ISO/IEC Standards[1]

Revised September 5, 2012

F. Podio, INCITS M1 Chairman (fernando.podio@nist.gov)

INCITS M1 Public Website:
http://standards.incits.org/a/public/group/m1

INCITS M1 Program of Work:
http://www.incits.org/tc_projects/m1.pdf

[1] These standards may be obtained (for a fee) at ANSI's eStandards Store: http://webstore.ansi.org/. The INCITS adoption year of an ISO/IEC standard is indicated as [20xx] following the international standards designation and approval year.

TABLE OF CONTENTS

Biometric Technical Interface Standards		
Standard	**Title**	**Description**
INCITS/ISO/IEC 19784-1:2006 **[2007]**	Information technology - Biometric Application Programming Interface – Part 1: BioAPI Specification	Provides a defined interface that allows a software application to communicate with (utilize the services of) one or more biometric technologies. It includes a high-level generic biometric authentication model suited to a broad range of biometrically enabled applications and to most forms of biometric technology. An architectural model is described which enables components of a biometric system to be provided by different vendors, and to interwork through fully-defined Application Programming Interfaces (APIs), corresponding Service Provider Interfaces (SPIs), and associated data structures. The BioAPI specification covers the basic biometric functions of enrollment, verification, and identification and includes a database interface to allow an application to manage the storage of biometric records. Conformance requirements are identified and informative annexes, including sample code, is provided. This standard specifies a biometric data structure which is compatible with ISO/IEC 19785 and 19794.
INCITS/ISO/IEC 19784-1:2006/AM1:2007 **[2008]**	Information technology - BioAPI - Biometric Application Programming Interface - Part 1: BioAPI Specification - AMENDMENT 1: BioGUI specification	Specifies two versions of BioAPI: 2.0 and 2.1. All the provisions that apply only to one version of BioAPI (either 2.0 or 2.1) are labeled as such. The main difference of BioAPI 2.1 from BioAPI 2.0 is the support it provides for BioGUI. BioGUI stands for "BioAPI Graphical User Interface". The functionality specified in this amendment enables an application to control the display of graphics at enrollment, verification, and identification, as an alternative to using the graphical user interface provided by BSPs. It also aligns the values of the type definition BioAPI_BIR_BIOMETRIC_TYPE with those specified in ISO/IEC 19785-1:2006. It provides additional functions and parameters that are redundant in a purely local implementation of BIoAPI, but which enable other to modify the behaviour of a BioAPI framework to support interactions between an application and remote BSPs. Finally, it provides improvements to some of the functions and parameters defined for BioAPI 2.0, particularly in relation to support for tenprint capture, the electronic capture of ten human fingerprints.
INCITS/ISO/IEC 19784-1:2006/Amd 2:2009 **[2009]**	Biometric application programming interface – Part 1: BioAPI specification – Amendment 2: Framework-free BioAPI	Amends the text of the published BioAPI Part 1, with the published BioAPI Part 1 Amd. 1 applied, in order to provide a specification of Framework free BioAPI. This amendment adds support for biometric systems that use the BioAPI interface to BSPs without requiring the presence of a BioAPI Framework. Conformance is specified only for a BSP module. Applications access a conforming BSP module using system integration facilities provided by the operating system platform. This amendment also includes some minor editorial corrections to the base standard.

Biometric Technical Interface Standards		
Standard	**Title**	**Description**
INCITS/ISO/IEC 19784-1:2006/Amd 3:2010 **[2011]**	Biometric application programming interface – Part 1: BioAPI specification – Amendment 3: Support for interchange of certificates and security assertions, and other security aspects	This amendment to ISO/IEC 19784-1 defines a new version 2.2 of BioAPI which adds support for biometric fusion and security assertions to the Standard. It extends the API and the SPI of BioAPI by specifying new functions and new values for existing data types. ISO/IEC 19784-1:2006 provides no direct support for biometric fusion. In addition, the use of FARs in the representation of matching scores is not suitable, in general, for performing score-level fusion (although it does allow some limited forms of fusion). This amendment adds support of biometric fusion to the standard.
INCITS/ISO/IEC 19784-2:2007 **[2008]**	Information technology - BioAPI - Biometric Application Programming Interface - Part 2: Biometric Archive Function Provider Interface	Describes the interface between a BSP and a biometric archive function provider. A biometric archive function provider encapsulates all functionality for the storage, search and management of biometric reference data regardless of the kind of physical storage media. Using a biometric archive function provider a BSP does not have to take care for special handling of different storage media like database servers, smartcards, database web services etc. Whatever media is used, the BSP in all cases handles the same interface for a biometric archive function provider. The interface description contains management functions to attach and detach different archive BFPs, to query biometric data records and to store biometric data records.
INCITS/ISO/IEC 19784-4:2011 **[2011]**	Information technology -- Biometric application programming interface -- Part 4: Biometric sensor function provider interface	Specifies a biometric sensor interface for a Biometric Service Provider (BSP, see ISO/IEC 19784-1). The interface supports a BSP wishing to provide the BioAPI Service Provider Interface (SPI) functions, whilst removing device handling activity from the BSP. ISO/IEC 19784-4:2011 provides an interface that can be used by all types of biometric sensor, including inter alia image streaming sensors (infrared, face, iris, finger, etc.), voice streaming sensors and digital tablets providing dynamic signature data. It is not in the scope of ISO/IEC 19784-4:2011 to define security and privacy requirements for capturing and transferring of biometric data across the Sensor Function Provider Interface (SFPI).
INCITS/ISO/IEC 29141:2009 **[2010]**	Information technology – Biometrics - Tenprint capture using biometric application programming interface (BioAPI)	Specifies requirements for the use of ISO/IEC 19784-1, as amended by ISO/IEC 19784-1/Amd.1 (BioAPI) for the purpose of performing a tenprint capture operation. It specifies a biometric data block format that is used to interact with a BioAPI framework [and hence with biometric service providers (BSPs)] to support an application wishing to perform a tenprint capture. It specifies a capture control block and a capture output block that conforming BSPs are required to support if they conform to ISO/IEC 29141:2009.
INCITS/ISO/IEC 19785-1:2006	Information technology -	Defines a basic structure for standardized biometric information records (BIRs) that

Biometric Technical Interface Standards		
Standard	**Title**	**Description**
[2008]	Common Biometric Exchange Framework Format (CBEFF) - Part 1: Data Element Specification	consists of three parts, the standard biometric header (SBH), the biometric data block (BDB), and the security block (SB). CBEFF also defines several data elements and their standardized abstract values that can be used in SBHs and SBs (CBEFF treats the BDB as opaque data). CBEFF also establishes mechanisms by which organizations, called "patrons" by CBEFF, can specify and publish BIR format specifications, which are in turn called "patron formats." CBEFF enables patrons to develop BIR specifications that are fully standardized and interoperable, yet are specifically adapted to the requirements of a particular application environment. CBEFF defines rules for BIRs that contain only one BDB (simple BIR) and that contain at least one BDB (complex BIR). CBEFF defines mandatory data elements that identify the format of a BDB and its security attributes (encryption and integrity). All the other CBEFF-defined data elements and abstract values are optional. CBEFF enables patrons to define additional data elements and abstract values as required by the application environment.
INCITS/ISO/IEC 19785-1:2006/Amd 1:2010 **[2010]**	Information technology - Common Biometric Exchange Framework Format (CBEFF) - Part 1: Data Element Specification – Amendment 1: Support for additional data elements	Amendment 1 of ISO/IEC 19785-1:2006 provides support for additional data elements (i.e., capture device owner, feature extraction algorithm owner, comparison algorithm owner, quality algorithm owner, and compression algorithm owner.)
INCITS/ISO/IEC 19785-2:2006 **[2008]**	Information technology - Common Biometric Exchange Framework Format (CBEFF) - Part 2: Procedures for the Operation of the Biometrics Registration Authority	Specifies procedures for a Registration Authority that is responsible for the assignment of ASN.1 object identifier components to identify biometric organizations, CBEFF patrons, security block formats, biometric data block formats, biometric information record formats and biometric products, to provide globally unambiguous identification in the context of the CBEFF ASN.1 object identifier.
INCITS/ISO/IEC 19785-2:2006/Amd 1:2010 **[2010]**	Information technology - Common Biometric Exchange Framework Format (CBEFF) - Part 2: Procedures for the Operation of the Biometrics Registration Authority – Amendment 1: Additional registrations	In addition to specifying the procedures to be followed by the Biometric Registration Authority (RA) in preparing, maintaining, and publishing registers of identifiers for biometric organizations, CBEFF patron formats, BDB formats, security block formats, and biometric products, this Amendment to ISO/IEC 19785-2:2006 adds to the above procedures to be followed by the Biometric Registration Authority in preparing, maintaining, and publishing registers of identifiers for specialized biometric products. With this amendment, ISO/IEC 19785-2 extends the procedures for a RA responsible for the assignment of ASN.1 object identifier components to identify biometric capture

Biometric Technical Interface Standards		
Standard	**Title**	**Description**
		devices, feature extraction algorithms, comparison algorithms, quality algorithms and compression algorithms to provide globally unambiguous identification in the context of the CBEFF ASN.1 object identifier.
INCITS/ISO/IEC 19785-3:2007 **[2008]**	Information technology - Common Biometric Exchange Formats Framework (CBEFF) - Part 3: Patron Format Specification	Specifies several patron formats that conform to the requirements of ISO/IEC 19785-1. ISO/IEC 19785-1 defines a basic structure for standardized biometric information records (BIRs) that consists of three parts, the standard biometric header (SBH), the biometric data block (BDB), and the security block (SB). CBEFF also defines several data elements and their standardized abstract values that can be used in SBHs and SBs (CBEFF treats the BDB as opaque data). CBEFF also establishes mechanisms by which organizations, called “patrons” by CBEFF, can specify and publish BIR format specifications, which are in turn called “patron formats”. CBEFF enables patrons to develop BIR specifications that are fully standardized and interoperable, yet are specifically adapted to the requirements of a particular application environment.
INCITS/ISO/IEC 19785-3:2007/Amd 1:2010 **[2010]**	Information technology - Common Biometric Exchange Formats Framework (CBEFF) - Part 3: Patron Format Specification – Amendment 1: Support for additional data elements	Provides support for additional data elements (i.e., capture device owner, feature extraction algorithm owner, comparison algorithm owner, quality algorithm owner, and compression algorithm owner.)
INCITS/ISO/IEC 19785-4:2010 **[2010]**	Information technology - Common Biometric Exchange Formats Framework (CBEFF) - Part 4: Security block format specifications	Specifies security block formats (see ISO/IEC 19785-1) registered in accordance with ISO/IEC 19785-2 as formats defined by the CBEFF biometric organization ISO/IEC JTC 1/SC 37, and specifies their registered security block format identifiers. [The security block format identifier is recorded in the standard biometric header (SBH) of a patron format (or defined by that patron format as the only available security block format).] The general-purpose security block format provides for specification of whether the biometric data block (BDB) is encrypted or the SBH and BDB have integrity applied (or both), and can include ACBio instances (see ISO/IEC 24761). This security block provides all necessary security parameters, including those used for encryption or integrity. It does not restrict the algorithms and parameters used for encryption or integrity, but provides for the recording of such algorithms and parameter values. It is a matter for profiling to determine, for a particular application area, what algorithms and parameter ranges can be used by the generator of a security block, and hence what algorithms and parameter ranges have to be supported by the user of a security block. This is out of the scope of ISO/IEC 19785-4:2010. The second security block is more

Biometric Technical Interface Standards		
Standard	**Title**	**Description**
		limited, but simpler (and in particular cannot contain ACBio instances, and does not support encryption of the BDB).
INCITS/ISO/IEC 24708:2008 **[2009]**	Information technology – BioAPI Interworking Protocol	ISO/IEC 24708:2008 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.

Conformance Testing Methodology Standards for the Biometric Technical Interfaces		
Standard	**Title**	**Description**
INCITS/ISO/IEC 24709.1:2007 **[2009]**	Information technology -- Conformance testing for the biometric application programming interface (BioAPI) -- Part 1: Methods and procedures	Part 1 of this multi-part standard specifies the concepts, framework, test methods, and criteria required to test conformity of biometric products claiming conformance to BioAPI(ISO/IEC 19784-1). Guidelines for specifying BioAPI conformance test suites, writing test assertions, and defining procedures to be followed during the conformance testing are provided. The conformance testing methodology is concerned with conformance testing of biometric products claiming conformance to BioAPI. Definitions of schemas of the assertion language are provided in normative annexes.
INCITS/ISO/IEC 24709.2:2007 **[2009]**	Information technology -- Conformance testing for the biometric application programming interface (BioAPI) -- Part 2: Test assertions for biometric service providers	Part 2 of this multi-part standard defines a number of test assertions written in the assertion language specified in Part 1 of ISO/IEC 24709. These assertions enable a user of this Part 2 of ISO/IEC 24709 (such as a testing laboratory) to test the conformance to ISO/IEC 19784-1 (BioAPI 2.0) of any biometric service provider (BSP) that claim to be a conforming implementation of that International Standard. Each test assertion specified in this Part 2 of ISO/IEC 24709 exercises one or more features of an implementation under test. Assertions are placed into packages (one or more assertions per package) as required by the assertion language. These assertions allow for testing conformance of BSP's of all conformance subclasses, and are further organized according to conformance subclasses and claimed support of optional features.
INCITS/ISO/IEC 24709.3:2011 **[2011]**	Information technology -- Conformance testing for the biometric application programming interface (BioAPI) -- Part 3: Test assertions for BioAPI frameworks	Part 3 of this multi-part standard defines a number of test assertions written in the assertion language specified in ISO/IEC 24709-1:2007. These assertions enable a user of ISO/IEC 24709-3:2011 (such as a testing laboratory) to test the conformance to ISO/IEC 19784-1 (BioAPI 2.0) of any BioAPI Framework that claims to be a conforming implementation of ISO/IEC 19784-1. Each test assertion specified in ISO/IEC 24709-3:2011 exercises one or more features of an implementation under test.

Biometric Data Interchange Format Standards		
Standard	**Title**	**Description**
INCITS/ISO/IEC 19794-1:2006 **[2007]**	Information technology -- Biometric data interchange format – Part 1: Framework	Part 1 of this multi-part standard describes the general aspects and requirements for defining biometric data interchange formats. The notation and transfer formats provide platform independence and separation of transfer syntax from content definition. This standard defines what is commonly applied for biometric data formats, i.e. the standardization of the common content, meaning, and representation of biometric data formats of biometric types considered in the specific parts of the multipart standard.
INCITS/ISO/IEC 19794-2:2005 **[2007]**	Information technology - Biometric data interchange format - Part 2: Finger minutiae data	Specifies a concept and data formats for representation of fingerprints using the fundamental notion of minutiae. The standard is generic, in that it may be applied and used in a wide range of application areas where automated fingerprint recognition is involved. The Standard contains definitions of relevant terms, a description of how minutiae shall be determined, data formats for containing the data for both general use and for use with cards, and conformance information. Guidelines and values for matching and decision parameters are provided in an informative Annex. ISO/IEC 19794-2 specifies: the fundamental data elements used for minutiae-based representation of a fingerprint,three data formats for interchange and storage of this data: a record-based format, and normal and compact formats for use on a smart card in a match-on-card application, optional extended data formats for including additional data such as ridge counts and core and delta location. ISO/IEC 19794-2 provides for interchange of finger minutiae data between sensing, storage and matching systems.
INCITS/ISO/IEC 19794-2: 2005/Cor 1: 2009 **[2010]**	Information technology - Biometric data interchange format - Part 2: Finger minutiae data – Corrigendum 1	ISO/IEC 19794-2:2005 Technical Corrigendum 1: 2010
INCITS/ISO/IEC 19794-2:2005/Amd 1:2010 **[2010]**	Information technology - Biometric data interchange format - Part 2: Finger minutiae data – Amendment 1: Detailed description of finger minutiae location, direction, and type	The scope of this informative annex of ISO/IEC 19794-2:2005 is to provide a more precise definition of location, direction, and type of minutiae in gray-scale finger images and a detailed description of the quality field. It enhances the readability of this part of ISO/IEC 19794 and decreases the possibility of misinterpretation. The standardization of algorithms is out of scope of this informative annex. This informative annex shall not supersede the existing Standard.
INCITS/ISO/IEC 19794-3:2006 **[2007]**	Information technology -- Biometric data interchange format -- Part 3: Finger pattern spectral data	Specifies requirements for the representation of local or global spectral data derived from a fingerprint image. The format is designed to provide flexibility in the choice of spectral representation in that spectral components may be based on quantized cosinusoidal triplets, Discrete Fourier Transformations or Gabor filters. The format also allows for a variable number of spectral components to be retained, which enables data

Biometric Data Interchange Format Standards		
Standard	**Title**	**Description**
		representations in a form that is more compact than storage of the entire fingerprint image. Example data records are provided for each of the spectral representations in informative annexes.
INCITS/ISO/IEC 19794-4:2005 **[2007]**	Information technology - Biometric data interchange format - Part 4: Finger image data	Specifies a data record interchange format for storing, recording, and transmitting the information from one or more finger or palm image areas within an ISO/IEC 19785-1 CBEFF data structure. This can 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 part of the ISO/IEC 19794 standard can be recorded on machine-readable media or may be transmitted by data communication facilities.
INCITS/ISO/IEC 19794-5:2005 **[2007]**	Information technology - Biometric data interchange format - Part 5: Face image data	Specifies scene, photographic, digitization and format requirements for images of faces to be used in the context of both human verification and computer automated recognition. The approach to specifying scene and photographic requirements in this format is to carefully describe constraints on how a photograph should appear rather than to dictate how the photograph should be taken. The format is designed to allow for the specification of visible information discernable by an observer pertaining to the face, such as gender, pose and eye color. The digital image format can be either ISO standard JPEG or JPEG2000. Finally, the “best practice” appendices provide guidance on photo capture for travel documents and face recognition performance verses digital compression.
INCITS/ISO/IEC 19794-5: 2005/Amd 1:2007 **[2009]**	Information technology - Biometric data interchange format - Part 5: Face image data / Amendment 1: Conditions for taking photographs for face image data	This Amendment is Annex B to ISO/IEC 19794-5 and is entitled “Conditions for Taking Photographs for Face Image Data.” It provides expert guidance for the design of photographic studios, photo booths and registration offices and, as such, it supplements the information provided in the standard and Annex A. It also provides guidance on printing quality and on scanning printed face photographs.
INCITS/ISO/IEC 19794-5:2005 Amd 2:2009 **[2010]**	Information technology -- Biometric data interchange formats -- Part 5: Face image	This amendment of ISO/IEC 19794-5:2005 is intended to establish a data interchange format for storing 3D human face images. To achieve this, several new image types are introduced that are a combination of 2D facial images and associated 3D shape

Biometric Data Interchange Format Standards		
Standard	**Title**	**Description**
	data / Amendment 2: Three-dimensional face image data interchange format	information. This document describes the necessary changes to the data interchange format regarding the capability to hold 3D information and the additional requirements for 3D Data.
INCITS/ISO/IEC 19794-5: 2005/Cor 1:2008 **[2009]**	Information technology - Biometric data interchange format - Part 5: Face image data/Corrigendum 1: 2008	ISO/IEC 19794-5:2005 Technical Corrigendum 1:2008
ISO/IEC 19794-5:2005/Cor 2: 2008 **[2009]**	Information technology - Biometric data interchange format - Part 5: Face image data/Corrigendum 2: 2008.	ISO/IEC 19794-5:2005 Technical Corrigendum 2:2008
INCITS/ISO/IEC 19794-6:2005 **[2007]**	Information technology - Biometric data interchange format - Part 6: Iris image data	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 by ISO/IEC 15444. 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.
INCITS/ISO/IEC 19794-7:2007 **[2007]**	Information technology - Biometric data interchange formats - Part 7: Signature/sign time series data	Specifies a concept and data interchange formats for dynamic signature/sign behavioural data captured in the form of a time series using devices such as digitizing tablets or advanced pen systems. The data interchange formats are generic in that they may be applied and used in a wide range of application areas where handwritten signs or signatures are involved. No application-specific requirements or features are addressed in this part of ISO/IEC 19794. This part of ISO/IEC 19794 contains definitions of relevant terms, a description of what data is captured, two data formats for containing the data — one for general use and one compact format for use with smart cards and other tokens — alongside examples of data block contents and best practice in capture.
INCITS/ISO/IEC 19794-7:2007/Cor 1:2009 **[2010]**	Information technology - Biometric data interchange formats - Part 7: Signature/sign time series data – Corrigendum 1	ISO/IEC 19794-7:2007 Technical Corrigendum 1:2010
INCITS/ISO/IEC 19794-8:2006	Information technology -	Describes all characteristics of a fingerprint in a small data record. Thus it allows for the

Biometric Data Interchange Format Standards		
Standard	**Title**	**Description**
[2009]	Biometric data interchange format -- Part 8: Finger pattern skeletal data	extraction of both spectral information (orientation, frequency, phase, etc.) and features (minutiae, core, ridge count, etc.). Transformations like translation and rotation can also be accommodated by the format defined herein. This standard for pattern-based skeletal representation of fingerprints supports the proliferation of low-cost commercial fingerprint sensors with limited coverage, dynamic range, or resolution. Thus the standard defines a data record that can be used to store biometric information on a variety a storage mediums (including, but not limited to, portable devices and smart cards).
INCITS/ISO/IEC 19794-9:2007 **[2007]**	Information technology -- Biometric data interchange format – Part 9: Vascular image data	Defines the exchange of human vascular biometric image information. It defines a specific definition of attributes, a data record format for storing and transmitting vascular biometric images and certain attributes, a sample record and conformance criteria. ISO/IEC 19794-9:2007 is intended for applications requiring the exchange of raw or processed vascular biometric images. It is intended for applications not limited by the amount of storage required. It is a compromise or a trade-off between the resources required for data storage or transmission and the potential for improved data quality/accuracy. Basically, it is to enable various algorithms to identify or verify the vascular biometric image data transferred from other image sources. Currently available vascular biometric technologies that may utilize ISO/IEC 19794-9:2007 for image exchange are technologies that use the back of the hand, palm and finger.
INCITS/ISO/IEC 19794-10:2007 **[2007]**	Information technology - Biometric data interchange formats - Part 10: Hand geometry silhouette data	Specifies a data interchange format (a CBEFF biometric data block – BDB) that can be used for storing, recording and transmitting the information obtained from a hand silhouette. This part of ISO/IEC 19794 defines the content, format and units of measurement for the exchange of hand silhouette data in a BDB. Information formatted in accordance with this part of ISO/IEC 19794 can be recorded on machine-readable media or transmitted by data communication between systems.
ISO/IEC 29159-1:2010 **[2011]**	Information technology -- Biometric calibration, augmentation and fusion data -- Part 1: Fusion information format	Specifies a biometric fusion information format that establishes machine readable data formats to describe the statistics of comparison score inputs to a fusion process. ISO/IEC 29159-1:2010 does not: ▪ standardize comparison-score normalization processes, nor ▪ standardize or define fusion processes.

Conformance Testing Methodologies for the Biometric Data Interchange Formats		
Standard	**Title**	**Description**
INCITS/ISO/IEC 29109-1:2009 **[2010]**	Information Technology - Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 1: Generalized conformance testing methodology	This part of INCITS/ISO/IEC 29109 specifies the concepts, test types and conformance testing methodologies to test biometric data interchange records or computer algorithms that create biometric data interchange records. The biometric data interchange records are specified in the multi-part ISO/IEC 19794 biometric data interchange format standard. This standard defines two types (A and B) and three levels (1, 2 and 3) of conformance testing, but it only provides a detailed description and methodology for the three levels of Type A testing. In the case of the first two levels, there are many common test elements, and so the assertion language for specifying Level 1 and Level 2 test assertions is defined in this standard. ISO/IEC 29109 is not concerned with testing of other characteristics of biometric products or other types of testing of biometric products (i.e., acceptance, performance, robustness, security).
INCITS/ISO/IEC 29109-2:2010 **[2010]**	Information Technology - Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 2: Finger minutiae data	Specifies elements of conformance testing methodology, test assertions, and test procedures as applicable to the biometric data interchange format standard relating to finger minutiae data (i.e. ISO/IEC 19794-2). It establishes: ▪ tests of assertions of the structure of the finger minutiae data format as specified in ISO/IEC 19794-2:2005 (Type A Level 1 as defined in ISO/IEC 29109-1:2009), ▪ tests of assertions of internal consistency by checking the types of values that may be contained within each field (Type A Level 2 as defined in ISO/IEC 29109-1:2009), and ▪ tests of semantic assertions (Type A Level 3 as defined in ISO/IEC 29109-1:2009). ISO/IEC 29109-2:2010 does not establish: ▪ tests of conformance of CBEFF structures embedding ISO/IEC 19794-2:2005 biometric data blocks (BDBs), ▪ tests of other characteristics of biometric products or other types of testing of biometric products (e.g. acceptance, performance, robustness, security), ▪ tests of conformance of systems that do not produce ISO/IEC 19794-2:2005 records, or ▪ tests for level 3 conformance testing.
INCITS/ISO/IEC 29109-4:2010 **[2010]**	Information Technology - Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 4: Finger	Specifies elements of conformance testing methodology, test assertions, and test procedures as applicable to ISO/IEC 19794-4. It establishes: ▪ test assertions of the structure of the finger image data format as specified in ISO/IEC 19794-4:2005 (Type A Level 1 as defined in ISO/IEC 29109-1:2009), ▪ test asssertions of internal consistency by checking the types of values that may

Conformance Testing Methodologies for the Biometric Data Interchange Formats		
Standard	**Title**	**Description**
	image data	be contained within each field (Type A Level 2 as defined in ISO/IEC 29109-1:2009), ▪ tests of semantic assertions (Type A Level 3 as defined in ISO/IEC 29109-1:2009). ISO/IEC 29109-4:2010 does not establish: ▪ tests of conformance of CBEFF structures required by ISO/IEC 19794-4:2005, ▪ tests of other characteristics of biometric products or other types of testing of biometric products (e.g. acceptance, performance, robustness, security), ▪ tests of conformance of systems that do not produce ISO/IEC 19794-4:2005 records.
INCITS/ISO/IEC 29109-10:2010 **[2011]**	Information Technology - Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794 – Part 10: Hand geometry silhouette data	Specifies elements of conformance testing methodology, test assertions, and test procedures as applicable to ISO/IEC 19794-10. It establishes: ▪ test assertions of the structure of the hand geometry silhouette data format as specified in ISO/IEC 19794-10:2007 (Type A Level 1 as defined in ISO/IEC 29109-1:2009), ▪ test assertions of internal consistency by checking the types of values that may be contained within each field (Type A Level 2 as defined in ISO/IEC 29109-1:2009), ▪ informative guidance for testing the consistency of selected encoded data fields with the input biometric data (Type B Level 3 as defined in ISO/IEC 29109-1:2009). ISO/IEC 29109-10:2010 does not establish: ▪ test of conformance of CBEFF structures required by ISO/IEC 19794-10:2007, ▪ test of consistency with input biometric data record (Level 3 as defined in ISO/IEC 29109-1:2009), ▪ test of other characteristics of biometric products or other types of testing of biometric products (e.g. acceptance, performance, robustness, security), ▪ test of conformance of systems that do not produce ISO/IEC 19794-10:2007 records.

Sample Quality Standards		
Standard	**Standard**	**Standard**
INCITS/ISO/IEC 29794-1:2009 **[2010]**	Information technology – Biometric sample quality – Part 1: Framework	This part of ISO/IEC 29794, for any or all biometric sample types as necessary: ▪ establishes terms and definitions that are useful in the specification, and use of quality metrics, ▪ recommends the purpose and interpretation of biometric quality scores, ▪ defines the format and placement of quality data fields in biometric data interchange formats, ▪ suggests methods for developing biometric sample datasets for the purpose of quality score normalisation, and ▪ suggests format for exchange of quality algorithm results.
INCITS/ISO/IEC 29794-4:2010 **[2010]**	Information technology – Biometric sample quality – Part 4: Finger image data	For aspects of quality specific to the finger image modality, ISO/IEC TR 29794-4:2010: ▪ specifies terms and definitions that are useful in the specification, use, and test of finger image quality metrics; ▪ defines the interpretation of finger image quality scores; ▪ identifies or defines finger image corpora for the purpose of serving as information for algorithm developers and users; ▪ develops statistical methodologies specific to finger image corpora for characterizing quality metrics to facilitate interpretation of scores and their relation to matching performance. Performance assessment of quality algorithms and standardization of quality algorithms are outside the scope of ISO/IEC TR 29794-4:2010.
INCITS/ISO/IEC 29794-5:2010 **[2010]**	Information technology – Biometric sample quality – Part 5: Face image data	For aspects of quality specific to facial images, ISO/IEC TR 29794-5:2010: ▪ specifies terms and definitions that are useful in the specification, use and testing of face image quality metrics; ▪ defines the purpose, intent, and interpretation of face image quality scores. Performance assessment of quality algorithms and standardization of quality algorithms are outside the scope of ISO/IEC TR 29794-5:2010.

Biometric Profiles		
Standard	**Standard**	**Standard**
INCITS/ISO/IEC 24713-1:2008 **[2009]**	Information technology -- Biometric profiles for interoperability and data interchange -- Part 1: Overview of biometric systems and biometric profiles	Part 1 of the multi-part standard provides common definitions used within the profile standards and references other standards applicable to the successful implementation of a generic biometric system. A harmonized (with the other part 1 standards in WG 3 and WG5) generic biometric system is described and a diagram is present. The description includes detail of the individual components present in a generic biometric system. ISO/IEC 24713-1:2008 furthermore describes the generic functions of the biometric system and the relationship between a biometric system and the application that uses that system. Lastly, it details the possible interfaces into a biometric system as well as the relationship that exists between the various base standards currently under development within SC37.
INCITS/ISO/IEC 24713-2:2008 **[2009]**	Information technology -- Biometric profiles for interoperability and data interchange -- Part 2: Physical access control for employees at airports	Part 2 of the multi-part standard specifies the application profile including necessary parameters and interfaces between function modules (i.e. BioAPI based modules and an external interface) in support of token-based biometric identification and verification of employees, at local access points (i.e. doors or other controlled entrances) and across local boundaries within the defined area of control in an airport. The token is expected to contain one or more reference biometrics, one or more operational biometrics, or both.
INCITS/ISO/IEC 24713-3:2009 **[2010]**	Information technology -- Biometric profiles for interoperability and data interchange -- Part 3: Biometrics based verification and identification of seafarers	In order to support a globally interoperable system of seafarers' identity documents, ISO/IEC 24713-3:2009 establishes a biometric profile to define how to use biometrics for verification and identification of seafarers at the various stages of document issuance and inspection. It defines a set of base standards and criteria for applying those standards in applications where identity documents are issued to seafarers and biometrics are used to link each document to the seafarer to whom it was issued. It attempts to provide information on the processes surrounding the enrolment and verification or identification of seafarers so that the biometric components of the system can be used in a proper context. It also addresses other system components such as the storage medium for the biometric data and the security of the system, since these will affect the use of the biometric technology.

Biometric Performance Testing and Reporting Standards		
Standard	**Standard**	**Standard**
INCITS/ISO/IEC 19795-1:2006 **[2007]**	Information technology – Biometric performance testing and reporting – Part 1: Principles and framework	Part 1 of the multi-part standard is concerned with the evaluation of biometric systems in terms of error rates and throughput rates. Metrics for the various error rates in biometric enrolment, verification and identification are unambiguously specified. Recommendations and requirements are given for the conduct of performance evaluations through the steps of planning the evaluation; collection of enrolment, verification or identification transaction data; analysis of error rates; and the reporting and presentation of results. The principles presented are generic to the range of biometric modalities, applications, and test purposes, and to both offline and online testing methodologies. These principles help avoid bias due to inappropriate data collection or analytic procedures; give better estimates of field performance for the expended effort; and clarify the limits of applicability of the test results.
INCITS/ISO/IEC 19795-2:2007 **[2009]**	Information technology – Biometric performance testing and reporting – Part 2: testing methodologies for technology and scenario evaluation	Addresses two specific biometric performance testing methodologies: technology and scenario evaluation. The large majority of biometric tests are of one of these two generic evaluation types. Technology evaluations evaluate enrolment and comparison algorithms by means of previously collected corpuses, while scenario evaluations evaluate sensors and algorithms by processing of samples collected from Test Subjects in real time. The former is intended for generation of large volumes of comparison scores and candidate lists indicative of the fundamental discriminating power of an algorithm. The latter is intended for measurement of performance in modeled environments, inclusive of Test Subject-system interactions.
INCITS/ISO/IEC TR 19795-3:2007 **[2009]**	Information technology – Biometric performance testing and reporting – Technical Report –Modality-specific Testing	In biometric performance testing and reporting, careful consideration needs to be given to the characteristic differences of each modality (fingerprint, face, iris, etc.). These differences naturally require variations within the general methodology defined in ISO/IEC 19795-1. Part 3 describes the methodologies relating to these modality-dependent variations. It presents and defines methods for determining, given a specific biometric modality, how to develop a technical performance test.
INCITS/ISO/IEC 19795-4:2008 **[2009]**	Information technology – Biometric performance testing and reporting – Performance and Interoperability Testing of Interchange Formats	Prescribes methods for technology and scenario evaluations of multi-supplier biometric systems that use biometric data conforming to biometric data interchange format standards. It specifies requirements needed to assess performance available from samples formatted according to a standard interchange format (SIF), performance available when samples formatted according to a SIF are exchanged, performance available from samples formatted according to a SIF, relative to proprietary data formats, SIF interoperability by quantifying cross-product performance relative to single-product performance, performance available from multi-sample and multimodal data

Biometric Performance Testing and Reporting Standards		
Standard	**Standard**	**Standard**
		formatted according to one or more SIFs, and performance interoperability of biometric capture devices. In addition, it includes procedures for establishing an interoperable set of implementations, defines procedures for testing interoperability with previously established sets of implementations, and gives testing procedures for the measurement of interoperable performance. It does not establish a conformance test for biometric data interchange formats, or provide test procedures for online data collection.
INCITS/ISO/IEC 19795-5:2011 **[2011]**	Information technology -- Biometric performance testing and reporting -- Part 5: Access control scenario and grading scheme	Specifies a framework for testing and a grading scheme for reporting the performance of a biometric system suitable for use in access control applications. It also allows for specifying application performance requirements in terms of the required performance of the biometric component of the access control system. It specifies the environment in which and the means by which testing will be performed and how the results will be reported. The grading scheme takes a conservative approach, using statistical analysis and confidence intervals to support the claim that the device performance is at least as good as the graded performance indicates. ISO/IEC 19795-5:2011 addresses conventional access control circumstances, and unusual or extreme circumstances are not within its scope.
INCITS/ISO/IEC 19795-7:2011 **[2011]**	Information technology – Biometric performance testing and reporting – Part 7: Testing of on-card biometric comparison algorithms	Establishes a mechanism for measuring the core algorithmic capabilities of biometric comparison algorithms running on ISO/IEC 7816 integrated circuit cards. Specifically, ISO/IEC 19795-7:2011 ▪ instantiates a mechanism for on-card biometric comparison testing; ▪ standardizes procedures for the measurement of the accuracy of on-card biometric comparison implementations running on object-based, test-specific sample cards; ▪ standardizes procedures for the measurement of durations of the various operations; ▪ gives examples for matching ISO/IEC 19794-2:2005 compact card minutiae templates. The following are specifically not within the scope of ISO/IEC 19795-7:2011: ▪ procedures for securing the communications channel, including cryptographic protection of the biometric templates; ▪ procedures for protection of sample or template integrity using digital signatures; ▪ authentication of the card and reader; ▪ selection or use of transmission protocols (e.g. contactless); ▪ profiles of specific data interchange standards; ▪ procedures for evaluation of readers, including performance, conformance and interoperability;

Biometric Performance Testing and Reporting Standards		
Standard	**Standard**	**Standard**
		▪ procedures for evaluation of ruggedness or durability of the card; ▪ on-card template generation (e.g. extraction of minutiae from images); ▪ template update or adaptation; ▪ formal conformance tests of ISO/IEC 7816-4 and ISO/IEC 7816-11; ▪ testing of devices not conforming to ISO/IEC 7816, including all system-on-card devices.

Other Technical Reports Not Included Above		
Technical Report	**Title**	**Description**
INCITS/ISO/IEC TR 24722: 2007 **[2009]**	Information technology -- Biometrics—Technical Report on Multi-modal and Other Multi-biometric fusion	Provides a description of and analysis of current practice on multimodal and other multibiometric fusion, including (as appropriate) reference to a more detailed description. It also discusses the need for, and possible routes to, standardization to support multibiometric systems.
INCITS/ISO/IEC TR 24741: 2007 **[2009]**	Information technology -- Biometrics—Technical Report for a Biometrics Tutorial	Describes the main biometric technologies, with some historical information. An annex describes the work of creating International Standards for biometrics and provides a layered model for the placement of the various International Standards being produced, with a short description of each. A second annex contains some of the terms and definitions currently used in these International Standards or the drafts of these International Standards.
ISO/IEC TR 24714-1:2008 **[2009]**	Information technology – Biometrics – Jurisdictional and societal considerations for commercial applications – Part 1: General guidance	Gives guidelines for the stages in the life cycle of a system's biometric and associated elements. This covers the following: ▪ the capture and design of initial requirements, including legal frameworks; ▪ development and deployment; ▪ operations, including enrolment and subsequent usage; ▪ interrelationships with other systems; ▪ related data storage and security of data; ▪ data updates and maintenance; ▪ training and awareness; ▪ system evaluation and audit; ▪ controlled system expiration. The areas addressed are limited to the design and implementation of biometric technologies with respect to the following: ▪ legal and societal constraints on the use of biometric data; ▪ accessibility for the widest population; ▪ health and safety, addressing the concerns of users regarding direct potential hazards as well as the possibility of the misuse of inferred data from biometric information. The intended audiences for ISO/IEC TR 24714-1:2008 are planners, implementers and system operators of biometric systems.