

INCITS Biometric Standards

Revised October 25, 2007

Published Standards Developed by INCITS M1 - Biometrics

These standards can be obtained (for a fee) at ANSI's eStandards Store: <http://webstore.ansi.org/>

Biometric Technical Interface Standards			
Developer	Standard	Title	Description
INCITS/INCITS M1	ANSI INCITS 358-2002 (Approved through INCITS Fast Track Process)	American National Standard for Information Technology for Information Technology – The BioAPI Specification	<p>This specification defines the Application Programming Interface and Service Provider Interface for a standard biometric technology interface. It is beyond the scope of this specification to define security requirements for biometric applications and service providers, although some related information is included by way of explanation of how the API is intended to support good security practices.</p> <p>The BioAPI is intended to provide a high-level generic biometric authentication model; one suited for any form of biometric technology.</p> <p>The standard covers the basic functions of Enrollment, Verification, and Identification, and includes a database interface to allow a biometric service provider (BSP) to manage the Identification population for optimum performance. It also provides primitives that allow the application to manage the capture of samples on a client, and the Enrollment, Verification, and Identification on a server.</p> <p>The specification was originally developed and published in 2000 by the BioAPI Consortium. It was approved as an ANSI INCITS standard in 2002.</p>
INCITS/INCITS M1	ANSI INCITS 398-2005 (Approved through INCITS Fast Track Process)	American National Standard for Information Technology – Common Biometric Exchange Formats Framework (CBEFF)	<p>This specification, the Common Biometric Exchange Formats Framework, is an augmented and revised version of the original CBEFF, the Common Biometric Exchange File Format, published in January 2001 as NISTIR 6529. This version, ANSI INCITS 398-2005 (NISTIR 6529-A), was developed by the CBEFF team based on the specification approved by the Biometrics Interoperability, Performance, and Assurance Working Group (NIST/BC WG) co-sponsored by NIST and the Biometric Consortium.</p> <p>ANSI INCITS 398-2005 contains the same text as NISTIR 6529-A. NISTIR 6529-A was approved by NIST on April 5, 2004. It was approved as an ANSI INCITS standard in 2005.</p>

INCITS/INCITS M1	INCITS 358:2002 AMENDMENT 1: 2007	American National Standard for Information Technology - BioAPI Specification – Amendment 1: Support for Biometric Fusion	The current edition of INCITS 358 (BioAPI 1.1) provides no direct support for biometric fusion. In addition, the use of FARs in representation of matching scores is not suitable, in general, for performing score-level fusion (though it does allow some limited forms of fusion). This Amendment to INCITS 358 adds support for biometric fusion to the standard. This Amendment extends the API and the SPI of BioAPI by specifying new functions and new values for existing data types.
------------------	--------------------------------------	--	--

Biometric Data Interchange Format Standards

Developer	Standard	Title	Description
INCITS/INCITS M1	ANSI INCITS 377-2004	American National Standard for 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.
INCITS/INCITS M1	ANSI INCITS 378-2004	American National Standard for Information technology - Finger Minutiae Format for Data Interchange	This standard defines a method of representing fingerprint information using the concept of minutiae. It defines the placement of the minutiae on a fingerprint, a record format for containing the minutiae data, and optional extensions for ridge count and core/delta information.
INCITS/INCITS M1	ANSI INCITS 379-2004	American National Standard for Information technology - Iris Interchange Format	This standard describes a format for exchange of iris image information. It contains a definition of attributes, a data record format, sample records and conformance criteria. Two alternative formats for iris image data are described, one based on a cartesian coordinate system and the other on a polar coordinate system.
INCITS/INCITS M1	ANSI INCITS 381-2004	American National Standard for Information technology - Finger Image Based Interchange Format	This standard specifies an interchange format for the exchange of image-based fingerprint and palm print recognition data. It defines the content, format, and units of measurement for such information. This standard is intended for those identification and verification applications that require the use of raw or processed image data containing detailed pixel information.
INCITS/INCITS M1	ANSI INCITS 385-2004	American National Standard for Information technology - Face Recognition Format for Data Interchange	This standard specifies definitions of photographic (environment, subject pose, focus, etc.) properties, digital image attributes and a face interchange format for relevant applications, including human examination and computer automated face recognition.

INCITS/INCITS M1	ANSI INCITS 395-2005	American National Standard for Information technology - Biometric Data Interchange Format - Signature/Sign Data	This standard defines a data interchange format for Signature/Sign Data for the purposes of biometric enrolment, verification or identification. The standard contains definitions of raw, time-series based signature/sign sample data and signature/sign feature data as well as a data record format for transmitting these data including extended or proprietary data.
INCITS/INCITS M1	ANSI INCITS 396-2005	American National Standard for Information technology - Hand Geometry Interchange Format	This standard specifies an interchange format for the exchange of hand geometry data in a silhouette format. It defines the content, format, and units of measurement for such information. This standard is intended for those identification and verification applications that require the use of an interoperable hand geometry template.

Biometric Profiles

Developer	Standard	Title	Description
INCITS/INCITS M1	ANSI INCITS 383-2004	American National Standard for Information technology - Biometric Profile – Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Transportation Workers	This standard specifies a biometric profile for transportation workers. It defines a set of base standards and criteria for applying those standards in applications where tokens are used for access control and identification of employees. This standard is intended for use in the transportation industry and other industries where identification and verification of employees is necessary to ensure safety and integrity within the work environment.
INCITS/INCITS M1	ANSI INCITS 394-2004	American National Standard for Information technology - Application Profile for Interoperability, Data Interchange and Data Integrity of Biometric-Based Personal Identification for Border Management	This standard specifies a biometric profile for border management applications. It defines a set of base standards and criteria for applying those standards in applications that use biometrics to authenticate the identity of non-citizens as they enter, stay in, and leave the United States.
INCITS/INCITS M1	ANSI INCITS 421-2006	American National Standard for Information Technology – Biometric Profile – Interoperability and Data Interchange – DoD Implementations.	This profile standard selects subsets of existing base standards that are used in the implementation of biometrically enabled systems. Base standards referenced in this document include BioAPI, ANSI/NIST ITL 1-2000, and the FBI's EFTS. It describes military biometric application profile settings for Red Force applications, which process and store biometric data on Enemy Prisoners of War (EPW), detainees, internees, and persons of interest with respect to national security.

INCITS/INCITS M1	ANSI INCITS 422-2006	American National Standard for Information Technology – Application Profile for Commercial Biometric Physical Access Control	This standard specifies a biometric profile for access control applications. It defines a set of base standards and criteria for applying those standards in applications that use biometrics to authenticate the identity of users requesting access to a facility. It establishes minimum conformity requirements for the biometric parts of such systems. It does so without presupposing the use of any particular biometric technology, data storage medium, operating system or card/document media.
------------------	----------------------	--	--

Biometric Performance Testing and Reporting Standards

Developer	Standard	Title	Description
INCITS/INCITS M1	ANSI INCITS 409.1-2005	American National Standard for Information technology - Biometric Performance Testing and Reporting Part 1 - Principles Framework	This standard is Part 1 of a multipart standard that specifies a common set of methodologies and procedures to be followed for conducting technical performance testing and evaluations. Included are guidelines that address issues regarding required test sizes, performance statistics, error reporting, and presentation of performance results. These procedures can be incorporated in an "end-to-end" system approach or from an individual technical component perspective.
INCITS/INCITS M1	ANSI INCITS 409.2-2005	American National Standard for Information technology - Biometric Performance Testing and Reporting Part 2 - Technology Testing Methodology	This part of the multipart standard specifies procedures for conducting offline tests of the performance of biometric technologies.
INCITS/INCITS M1	ANSI INCITS 409.3-2005	American National Standard for Information technology - Biometric Performance Testing and Reporting Part 3 - Scenario Testing Methodologies	This part of the multipart standard specifies requirements for scenario-based biometric testing and reporting.
INCITS/INCITS M1	ANSI INCITS 409.4-2006	American National Standard for Information Technology – Biometric Performance Testing and Reporting – Part 4: Operational Testing Methodologies	This part of the multipart standard specifies requirements for operational based biometric testing and reporting. It provides the test planning, test execution and test reporting requirements that must be followed during biometric system's operational tests.

Standards Developed by ISO/IEC JTC 1/SC 37 - Biometrics Recently Adopted by INCITS

Adoption year: [2007]

Not yet available at ANSI's eStandards Store:

Biometric Technical Interface Standards			
Developer	Standard	Title	Description
ISO/IEC JTC 1/SC 37	INCITS/ISO/IEC 19784-1:2006 [2007]	Information technology - Biometric Application Programming Interface – Part 1: BioAPI Specification	This standard 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.
Biometric Data Interchange Format Standards			
Developer	Standard	Title	Description
ISO/IEC JTC 1/SC 37	INCITS/ISO/IEC 19794-1: 2006 [2007]	Information technology -- Biometric data interchange format – Part 1: Framework	ISO/IEC 19794 - Information technology -- Biometric data interchange formats is multi-part standard. This part of the 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.

ISO/IEC JTC 1/SC 37	INCITS/ISO/IEC 19794-2: 2005 [2007]	Information technology - Biometric data interchange format - Part 2: Finger minutiae data	This part of the standard 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.
ISO/IEC JTC 1/SC 37	INCITS/ISO/IEC 19794-3: 2006 [2007]	Information technology -- Biometric data interchange format -- Part 3: Finger pattern spectral data	This part of the standard 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 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.
ISO/IEC JTC 1/SC 37	INCITS/ISO/IEC 19794-4: 2005 [2007]	Information technology - Biometric data interchange format - Part 4: Finger image data	This part of the standard 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.
ISO/IEC JTC 1/SC 37	INCITS/ISO/IEC 19794-5: 2005 [2007]	Information technology - Biometric data interchange format - Part 5: Face image data	This part of the standard 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.

ISO/IEC JTC 1/SC 37	INCITS/ISO/IEC 19794-6: 2005 [2007]	Information technology - Biometric data interchange format - Part 6: Iris image data	This part of the 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 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.
ISO/IEC JTC 1/SC 37	INCITS/ISO/IEC 19794-7:2007 [2007]	Information technology - Biometric data interchange formats - Part 7: Signature/sign time series data	This part of ISO/IEC 19794 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.
ISO/IEC JTC 1/SC 37	INCITS/ISO/IEC 19794-9:2007 [2007]	Information technology -- Biometric data interchange format – Part 9: Vascular image data	This part of the standard 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.
ISO/IEC JTC 1/SC 37	INCITS/ISO/IEC 19794-10-2007	Information technology - Biometric data interchange formats - Part 10: Hand geometry silhouette data	This part of ISO/IEC 19794 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

Biometric Performance Testing and Reporting Standards

Developer	Standard	Title	Description
ISO/IEC JTC 1/SC 37	INCITS/ISO/IEC 19795-1:2006 [2007]	Information technology – Biometric performance testing and reporting – Part 1: Principles and framework	This part of this 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.