Published Biometric American National Standards Developed by INCITS M1 – *Biometrics*[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/. For additional information and availability of withdrawn and superseded standards no available at the ANSI standards store, please contact Lynn Barra of INCITS at lbarra@itic.org

TABLE OF CONTENTS

Biometric Technical Interface Standards		
Standard	**Title**	**Description**
ANSI INCITS 358-2002 [R2007] (Initially developed by the BioAPI Consortium) Approved through INCITS Fast Track Process) **Reaffirmed 2007** **Will be Reaffirmed in 2012**	American National Standard for Information technology for Information Technology – The BioAPI Specification	Specifies 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. The BioAPI is intended to provide a high-level generic biometric authentication model; one suited for any form of biometric technology. 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.
INCITS 358:2002 AMENDMENT 1: 2007 **Will be Reaffirmed in 2012**	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.
ANSI INCITS 398-2008 **Revision of** **ANSI INCITS 398-2005**	American National Standard for Information Technology – Common Biometric Exchange Formats Framework (CBEFF)	Specifies a common set of data elements necessary to support multiple biometric technologies and to promote interoperability of biometric-based application programs and systems by allowing for biometric data exchange. This standard (revision of ANSI INCITS 398-2005) specifies a common set of data elements necessary to support multiple biometric technologies and to promote interoperability of biometric-based application programs and systems by allowing for biometric data exchange. These common data elements can be placed in a single file, record, or data object used to exchange biometric information between different system components and applications. This standard specifies the biometric data elements. These elements are assembled into data structures that are defined by CBEFF patron format specifications or standards. Each patron format specification that conforms to CBEFF defines which CBEFF data elements are present in its format and how the data elements are extracted and processed (details such as the data encoding scheme are the responsibility of the CBEFF patrons). The biometric data transported in a CBEFF structure can represent processed or unprocessed (raw) data. This standard itself specifies two Patron Formats (Patron Format A and B, see Annexes A and B). Annexes C through F document patron formats that have been specified external to this standard, as follows: C. The BioAPI BIR,

Biometric Technical Interface Standards		
Standard	**Title**	**Description**
		D. The NIST PIV CBEFF Patron Format specified in NIST SP 800-76, Feb 1, 2006, E. The ICAO Logical data Structure (LDS) , F. The Type 99 record specified in the revision of the ANSI/NIST-ITL 1-2000 standard (ANSI/NIST-ITL 1-2007, "Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information"). CBEFF does not specify the content or format of the actual biometric data contained within a CBEFF biometric data record. Protection of the privacy of individuals from inappropriate dissemination and use of biometric data is not in the Scope of this standard.
ANSI INCITS 434-2007 **Will be Reaffirmed in 2012**	American National Standard for Information Technology – Tenprint Capture using BioAPI	Specifies requirements for the use of ISO/IEC 19784-1, *BioAPI Specification* (also known as BioAPI 2.0), a software interface standard, for the purpose of performing a tenprint capture operation. This includes one or more of the following: (a) Identification of BioAPI functions to be utilized and the order (if any) in which they are to be called; (b) Specification of values for function parameters; (c) Definition of GUI (graphical user interface) events (for use with an application controlled GUI); (d) User interface specifications for use with a BSP (biometric service provider) controlled GUI; and (e) Sample calling sequences and example inputs/outputs.
ANSI INCITS 442-2010 **Revision of** **ANSI INCITS 442-2008**	American National Standard for Information Technology - Biometric Identity Assurance Services (BIAS)	Defines biometric services used for identity assurance that are invoked over a services-based framework. It is intended to provide a generic set of biometric and identity-related functions and associated data definitions to allow remote access to biometric services. The binding of these services to specific frameworks is not included in this project.

Conformance Testing Methodology Standards for the Biometric Technical Interfaces		
Standard	**Title**	**Description**
ANSI INCITS 429-2008	American National Standard for Information Technology - Conformance Testing Methodology for ANSI INCITS 358-2002, BioAPI Specification	Specifies the concepts, framework, test methods, and criteria to be achieved to claim conformity of Biometric Service Providers to the BioAPI specification ANSI INCITS 358-2002. It defines requirements and guidelines for specifying conformance test suites and related test methods for measuring conformity of Biometric Service Provider components to the BioAPI specification, and defines procedures to be followed before, during, and after conformance testing. The standard focuses only on the critical set of functions/features of the BioAPI specification and other requirements detailed in the conformance clause of the BioAPI specification.
ANSI INCITS 473-2011	American National Standard for Information Technology - Conformance Testing Methodology Standard for Patron Formats Conforming to INCITS 398-2008.	Specifies the concepts, test types and a conformance testing methodology to test conformance of CBEFF Biometric Information records (BIRs) claiming conformance to patron formats A, the BioAPI BIR or the NIST/ITL Type 99 data record specified in INCITS 398-2008 annexes as well as the LDS patron format for applications other than MRTD and other ICAO applications.
ANSI INCITS 474-2011	American National Standard for Information technology - Biometric Application Programming Interface - Java (BioAPI Java)	Specifies an interface of a BioAPI Java framework and BioAPI Java BSP which will mirror the corresponding components specified in ISO/IEC 19784-1. Therefore, the position occupied by the proposed standard within the general picture of biometrics standards will be the same position that ISO/IEC 19784-1 occupies, the only difference being the programming language of the interfaces. The concepts such as BioAPI unit, component registry, etc. are present in this standard and will have the same meaning as in ISO/IEC 19784-1. The semantic equivalence of this standard will be maintained with ISO/IEC 19784-1, but there are differences in actual parameters passed between functions and the sequence of function calls. These differences exist to take advantage of the object oriented benefits of Java.

Biometric Data Interchange Format Standards		
Standard	**Title**	**Description**
ANSI INCITS 377-2009 **Revision of ANSI INCITS 377-2004**	American National Standard for Information technology - Finger Pattern Based Interchange Format	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.
ANSI INCITS 378-2009 **Revision of ANSI INCITS 378-2004**	American National Standard for Information technology - Finger Minutiae Format for Data Interchange	This standard is a revision of ANSI INCITS 378-2004. It 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.
ANSI INCITS 378-2009/AM1-2010	American National Standard for Information technology - Finger Minutiae Format for Data Interchange – Amendment 1	This amendment of INCITS 378-2009 assigns a new version number to distinguish the INCITS version from the SC 37 version, provides additional choices for multiple-finger codes, resolves minor inconsistencies, clarifies ambiguities, and updates Annex B.
ANSI INCITS 379-2004 **Standard Withdrawn**	American National Standard for Information technology - Iris Interchange Format	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.
ANSI INCITS 381-2009 **Revision of ANSI INCITS 381-2004**	American National Standard for Information technology - Finger Image Based Interchange Format	This standard is a revision of ANSI INCITS 381-2004. It 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.
ANSI INCITS 381-2009/AM1-2011	American National Standard for Information technology - Finger Image Based Interchange Format – Amendment 1	This amendment to the INCITS 381-2009 assigns a new version number to distinguish the INCITS version from the SC 37 version, provides additional choices for multiple-finger codes, resolves minor inconsistencies, and clarifies ambiguities.
ANSI INCITS 385-2004 [R2009] **Reaffirmed in 2009**	American National Standard for Information technology - Face Recognition Format for Data Interchange	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.
ANSI INCITS 395-2005	American National Standard for Information technology -	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-

Biometric Data Interchange Format Standards		
Standard	**Title**	**Description**
Standard Withdrawn	Biometric Data Interchange Format - Signature/Sign Data	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.
ANSI INCITS 396-2005 **Standard Withdrawn**	American National Standard for Information technology - Hand Geometry Interchange Format	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.
ANSI INCITS 439-2008	American National Standard for Information technology – Fusion Information Format for Data Interchange	Specifies Fusion Information Formats (FIFs) for statistical information in support of interoperable, modular, score-level fusion of biometric systems. The standard does not define, describe nor otherwise standardize fusion processes.
ANSI INCITS 456-2010	American National Standard for Information technology – Speaker Recognition Format for Raw Data Interchange (SIVR-1)	Specifies a concept and data format for representation of the human voice at the raw-data level with optional inclusion of non-standardized extended data. It does not address handling of data that has been processed to the feature or voice model levels. The data format is generic in that it may be applied to and used in a wide range of application areas where automated and human-to-human SIV is performed. No application-specific requirements, equipment, or features are addressed in this standard. Through its XML orientation, this standard does, however, reflect recognition of the overwhelming dominance of the VoiceXML standard in speech processing and associated XML-based standards. This standard contains definitions of relevant terms, a description of the basic speaker-recognition Session, a data format for containing the data, and conformance information. SIV applications and engines utilize adaptation to automatically update the information in a reference model. Despite its value, representing adaptation lies outside of the bounds of this standard because it operates on voice model data and this standard focuses on raw data transmission.

Conformance Testing Methodologies for the Biometric Data Interchange Formats		
Standard	**Title**	**Description**
ANSI INCITS 423.1-2008	American National Standard for Information technology - Conformance Testing Methodology Standard for Biometric Data Interchange Format Standards – Part 1: Generalized Conformance Testing Methodology	Part 1 of the multi-part standard 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 INCITS biometric data interchange format standards. This part defines two types (A and B) and three levels (1, 2 and 3) of conformance testing, with a general description and methodology for each one. 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. This multi-part standard 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).
ANSI INCITS 423.2-2008	American National Standard for Information technology- Conformance Testing Methodology Standard for Biometric Data Interchange Format Standards – Part 2: Conformance Testing Methodology for ANSI INCITS 378-2004, Finger Minutiae Format for Data Interchange	Part 2 of ANSI INCITS 423 specifies the tests required to assure a vendor's application(s) or service(s) conforms to ANSI INCITS 378-2004. For the purposes of this part of ANSI INCITS 423, of the two types (A and B) and three levels (1,2 and 3) of conformance testing as defined in ANSI INCITS 423.1, only Type A and Levels 1 and 2 are within the scope of this part of ANSI INCITS 423.
ANSI INCITS 423.3-2009	American National Standard for Information technology- Conformance Testing Methodology Standard for Biometric Data Interchange Format Standards – Part 3: Conformance testing methodology for INCITS 377-4 Finger pattern data interchange format	This standard is concerned with conformance testing of implementations claiming conformance to the Finger Pattern Data Interchange Format specification defined in INCITS 377-2004. More specifically, it is concerned with testing only of the Biometric Data Interchange Records (BDIR) requirements as defined in INCITS 423.1. Conformance testing of the CBEFF requirements as set forth in INCITS 377-2004 is not within the scope of this standard. Furthermore, this standard 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). Any organization contemplating the use of test methods defined in this part, should carefully consider the constraints on their applicability. Two types (A and B) and three levels (1, 2, and 3) of conformance testing have been defined in INCITS 423.1. However, only Type A, and Levels 1 and 2 are within the scope of this standard.
ANSI INCITS 423.4-2009	American National Standard for Information technology-	This part of ANSI INCITS 423 is concerned with conformance testing of implementations claiming conformance to the Finger Image-Based Data Interchange

Conformance Testing Methodologies for the Biometric Data Interchange Formats		
Standard	**Title**	**Description**
	Conformance Testing Methodology Standard for Biometric Data Interchange Format Standards – Part 4: Conformance Testing Methodology for INCITS 381-2004, Finger Image-Based	Format specification as per ANSI INCITS 381-2004. Further, this part of ANSI INCITS 423 is concerned with testing only of the Biometric Data Interchange Records (BDIR) requirements as defined in ANSI INCITS 381-2004. For the purposes of this part of ANSI INCITS 423, and as also described in Part 1: Generalized Conformance Testing Methodology of ANSI INCITS 423, conformance testing of the CBEFF requirements as set forth in ANSI INCITS 381-2004 is not within the scope of this part of ANSI INCITS 423. This part of ANSI INCITS 423 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). Any organization contemplating the use of test methods defined in this part of ANSI INCITS 423 should carefully consider the constraints on their applicability. For the purposes of this part of ANSI INCITS 423, of the two types (A and B) and three levels (1, 2, and 3) of conformance testing as defined in ANSI INCITS 423.1, only Type A and Levels 1 and 2 are within the scope of this part of ANSI INCITS 423. Selected test cases and assertions that define Level 3 and Type B conformance test methods and procedures are included in this part of ANSI INCITS 423 as informative materials.

Biometric Profiles		
Standard	**Title**	**Description**
ANSI INCITS 383-2008 **Revision of** **ANSI INCITS 383-2004**	American National Standard for Information Technology – Biometric Profile – Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Transportation Workers	Specifies the application profile in support of identification and verification of transportation workers, through the use of Biometric data collected during enrollment, at local access points (i.e. doors or other controlled entrances) and across local boundaries within the defined area of control. 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.
ANSI INCITS 394-2004 **Standard Withdrawn**	American National Standard for Information technology - Application Profile for Interoperability, Data Interchange and Data Integrity of Biometric-Based Personal Identification for Border Management	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.
ANSI INCITS 421-2006 **Standard Withdrawn**	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.
ANSI INCITS 422-2007 **Standard Withdrawn**	American National Standard for Information Technology – Application Profile for Commercial Biometric Physical Access Control	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		
Standard	**Title**	**Description**
ANSI INCITS 409.1-2005 **Standard Withdrawn**	American National Standard for Information technology - Biometric Performance Testing and Reporting Part 1 - Principles Framework	Part 1 of the multi-part standard 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.
ANSI INCITS 409.2-2005 **Standard Withdrawn**	American National Standard for Information technology - Biometric Performance Testing and Reporting Part 2 - Technology Testing Methodology	Part 2 of the multi-part standard specifies procedures for conducting offline tests of the performance of biometric technologies.
ANSI INCITS 409.3-2005 **Standard Withdrawn**	American National Standard for Information technology - Biometric Performance Testing and Reporting Part 3 - Scenario Testing Methodologies	Part 3 of the multi-part standard specifies requirements for scenario-based biometric testing and reporting.
ANSI INCITS 409.4-2006 **Reaffirmed 2011**	American National Standard for Information Technology – Biometric Performance Testing and Reporting – Part 4: Operational Testing Methodologies	Part 4 of the multi-part 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.
ANSI INCITS 409.5-2011	American National Standard for Information technology - Biometric Performance Testing and Reporting - Part 5: Framework for Testing and Evaluation of Biometric System(s) for Access Control	Part 5 of the multi-part standard specifies test planning, execution, and reporting requirements. The standard establishes grade levels as functions of observed false reject rates at each of three separate false accept rates, failure to enroll rate and transaction time. The general purpose nature of the standard applies to most common access control application requirements, such that results are applicable to many but not all access control applications. The framework is not suitable for highly specialized access control applications (e.g. those requiring very high levels of protection or with specialized user populations such as the elderly). Highly specialized access control application warrant test processes beyond the scope of this standard.

Biometric Performance Testing and Reporting Standards		
Standard	**Title**	**Description**
		The following types of tests are not in the scope of this standard: • Active impostor testing; • Environmental; • Human factors, including user acceptance; • Identification performance metrics; • Reliability, availability and maintainability; • Safety; • Security, including vulnerability
ANSI INCITS TR-45-2009	INCITS Technical Report for Information Technology – Biometric Performance Testing and Reporting – Part 7: Framework for Testing Methodologies for Specific Modalities	The technical report documents modality-specific influencing factors that may impact biometric sub-system performance. These influencing factors may be categorized as environmental, biological, behavioral, usability-oriented, societal, and design-oriented. This technical report is arranged to: • Introduce influencing factor categories • Discuss factor categories that may influence performance for each modality • List testing protocols used in previous research.