

US Contribution to JTC 1 SC 37 on Suitability of ANSI/INCITS 358-2002 BioAPI Specification Ver. 1.1 for ISO/IEC JTC 1 Fast Track processing

History of the BioAPI Specification.

The BioAPI Specification is the result of several years of effort, beginning with the formation of the BioAPI Consortium in April of 1998. The founding members of the BioAPI Consortium were Compaq (now HP), Microsoft, IBM, Novell, Identicator (now Identix) and Miros (now eTrue). At that time, there were several competing biometric APIs in the marketplace, chief among them being the Human Authentication API (HA-API), sponsored by NSA and the Biometric Consortium (BC), and BAPI, sponsored by a private company, I/O Software. In March of 1999, the National Institute of Standards and Technology (NIST) sponsored a “unification meeting” among the various API groups, resulting in consolidation under a single organization, a revamped version of the BioAPI Consortium, which adhered to accepted practices among standards development bodies.

From April of 1999 through March of 2000, this group met at 4-6 week intervals at locations across the US and Canada for a series of 3 day meetings, ultimately resulting in Version 1.0 of the BioAPI Specification. Version 1.0 was released on 30 March 2000, with an official launch on 6 April in the form of a BioAPI Users and Developers Workshop hosted by the BC. This event drew an overflow audience.

Between March and September of 2000, efforts centered on developing a software reference implementation of the BioAPI framework (runtime). This was developed by 4 member companies – Intel, Bioscrypt, SAFLINK, and Iridian Technologies. Since (in parallel), Intel had developed the Human Recognition Services (HRS) extension to the Open Group’s Common Data Security Architecture (CDSA) which was wholly based on BioAPI, the existing HRS reference implementation code base was used as the starting point for the BioAPI code. A beta version of the reference implementation was released in September of 2000.

Based primarily on what was learned during software development, efforts then began to document necessary and suggested changes to the specification. As a result, Version 1.1 of the specification, along with a final version of the reference implementation, were released in March of 2001. Initial product announcements began soon thereafter.

As was intended from the start, the BioAPI specification and reference implementation were made publicly available for download from the BioAPI website at no charge. An open source license agreement was included with the software, which was provided as both source and executable (Win32).

It was also always intended for the BioAPI specification to ultimately transition to a formal standards body. The BioAPI Consortium had been investigating which path and organization would be the best choice for this work. In July of 2001, the chair of the

Consortium briefed the executive board of INCITS, who subsequently approved the BioAPI Specification to enter their Fast Track standardization process. Following this process, the BioAPI Specification, Version 1.1 was approved as ANSI/INCITS 358-2002 in February of 2002.

Since that time, more products have been announced and beta versions of a Unix (Sun Solaris) and Linux reference implementations have been developed (by the International Biometric Group (IBG) and NIST respectively). Although it is not possible to know of each product that exists or is in progress, the BioAPI Steering Committee is aware of at least 13 companies with BioAPI compliant products (some companies with multiple products) and at least 12 others in progress. The membership of the BioAPI Consortium is now at 114 members, including an international roster of biometric vendors, integrators, and end-users representing industry, government, and academia.

At its first meeting in January of 2001, the new INCITS Technical Committee M1 – Biometrics, passed a resolution of intent to move the BioAPI Specification into ISO.

Scope of the BioAPI Specification.

The BioAPI Specification, Version 1.1, defines a common method of communication between a software application and an underlying biometric technology module/service. It is composed of a set of C function calls, defined data structures, and related information such as error handling as well as conformance requirements. The intent of the specification was to provide an open system specification that would support a broad range of applications and be biometric technology/vendor neutral.

Function calls are defined at the API level (i.e., between the application and the framework) and at the SPI level (i.e., between the framework and the service provider, known as a BSP – Biometric Service Provider). A minimum set of calls are defined which cover module management, data management, and operations. Operational functions are defined to provide for all of the basic operations common across a variety of biometric technologies; that is, those generally provided in a vendor's SDK but avoiding any vendor/technology specific (unique) features to the extent possible. Examples of these include basic functions such as Enroll, Verify, Identify, and primitive functions such as Capture, Process, CreateTemplate, Verify_Match, and Identify_Match.

In addition to standardizing functions, the BioAPI Specification also standardized on a biometric data structure (later abstracted within CBEFF) and a normalized method for performing scoring and thresholding. These were two areas of critical need within the biometrics industry and the source of much discussion during the development of the specification.

In addition to mandatory requirements, the BioAPI Specification also includes a set of optional features covering such things as model adaptation, application control of the GUI, client/server implementation, and data signing/encryption. Upon installation, the

BSP is required to post to the module registry what functions, options, authentication factors, and data formats it supports.

Relationship to other standards.

The BioAPI Consortium was proactive in establishing liaison relationships with other related organizations in order to ensure coordination of efforts and compatible end products. As a result, the following relationships exist:

- a) *Common Biometric Exchange File Format (CBEFF)*. The BioAPI is a Patron of CBEFF and its Biometric Identification Record (BIR) is a CBEFF compliant data structure, being documented as CBEFF Format B.
- b) *Human Recognition Services (HRS)*. The HRS specification, part of the Open Groups Common Data Security Architecture (CDSA) standard, is based entirely upon BioAPI, with identical function calls. HRS further extends BioAPI to work within the CDSA security framework and to add a number of security related capabilities available through this framework, such as mutual authentication of components.
- c) *ANSI X9.84-2000 Biometric Information Management and Security for the Financial Services Industry*. BioAPI was coordinated with this standard for data interchangeability and compatibility for use in conjunction with one another.
- d) *Future Data Interchange Standards*. The structure of the BioAPI data record was designed such that, in addition to proprietary formats, standard biometric templates could be immediately accommodated within its opaque data block and identified using an assigned Format ID.

Suitability for the JTC1 Fast Track process and US interest in submitting the standard to JTC 1 for fast track processing and placement in JTC 1 SC 37.

The US National Body considers ANSI/INCITS 358-2002, The BioAPI Specification Version 1.1 suitable for JTC 1 Fast Track Processing. The US believes that this specification meets the criteria set up for the JTC 1 Directives, Section 13 and is soliciting the opinion and comments of SC 37 members on the feasibility of submitting the BioAPI Specification for JTC 1 Fast Track processing and placement in JTC 1 SC 37.

The BioAPI Specification is the result of consensus development by an open consortium now numbering over 100 members, over 1/3 of which are non-US based.

Worldwide acceptance of BioAPI is growing. The biometric data structure specified in ANSI/INCITS 358 is fully compliant with CBEFF. Additionally, BioAPI is referenced in a number of other documents and specifications to include AAMVA's DL/ID-2000, the US drivers license standard published by the American Association of Motor Vehicle Administrators, and the draft US Biometric Protection Profile (BPP) developed by the US Department of Defense (DoD) Biometrics Management Office (BMO). It has recently

been translated into other languages. Government and commercial customers are beginning to include BioAPI compliance as a requirement within their solicitations.

Further, biometric vendors are now offering biometric products. Most of these products are technology modules (BSPs), but additionally, biometric applications and toolkits are also being marketed.

References:

[1] ANSI/INCITS 358-2002 American National Standard for Information Technology – The BioAPI Specification.

[2] NISTIR 6529, "Common Biometric Exchange File Format (CBEFF)", January 3, 2001. (<http://www.nist.gov/cbeff>)

[3] ANSI X9.84-2000, "Biometric Information Management and Security for the Financial Services Industry". (<http://www.x9.org>)

[4] National Institute of Standards and Technology (NIST) web site: <http://www.nist.gov>

[5] Biometric Consortium web site: <http://www.biometrics.org>

[6] InterNational Committee for Information Technology Standards (INCITS) On-Line web site: <http://www.techstreet.com/ncitsgate.html>

[7] BioAPI Consortium web site: <http://www.bioapi.org>

[8] American National Standards Institute web store
<http://webstore.ansi.org/ansidocstore/dept.asp>

[9] CDSA and CSSM Authentication: Human Recognition Service (HRS), V2
<http://www.opengroup.org/pubs/catalog/c013.htm>

[10] International Biometric Industry Association (IBIA) web site: <http://www.ibia.org/>

[11] Web Page for registration of Format Owner and Format Type Values under IBIA:
<http://www.ibia.org/formats.htm>