Conformance Testing Methodologies for Biometric Data Interchange Formats, Standardization of

Dylan Yaga[1], John W. M. Campbell[2] and Gregory Zektser[3]

[1] National Institute of Standards and Technology, dylan.yaga@nist.gov
[2] Bion Biometrics Inc., Ottawa, Canada, john@bionbiometrics.com
[3] Booz Allen Hamilton, Inc., zektser_gregory@bah.com

Synonyms

Conformity, Compliance, Conformity Evaluation

Definition

The development of standardized methods and procedures for **conformance testing** (also known as conformity evaluation) of products or systems that claim to satisfy the requirements of one or more of the standardized biometric data interchange formats.

Main Body Text

Concepts in Conformance Testing

A national or international standard consists of a set of requirements and frequently a set of recommendations. The requirements specified in the standard are traditionally classified in three categories: mandatory requirements to be observed in all cases, optional requirements to be observed if so chosen by an implementer, and conditional requirements to be observed under specific conditions. A product, process or system that fully satisfies the requirements of the standard is described as being *conformant to that standard*. Conformance testing is the method that is used to determine if the product, process or system satisfies the requirements set forth in the standard to which they claim conformity to. The precise nature of these requirements differs substantially from one standard to another, but in all cases, there are certain important concepts.

The product, process or system being tested is known as an **implementation under test** (**IUT**). It does not always need to satisfy every requirement and recommendation of a standard, only those that that are defined as mandatory and those which the **IUT** claims conformity to. In certain cases, the mandatory requirements may be different for different applications or purposes. In the case of conformance testing for biometric data interchange format standards, for example, an **IUT** may be designed to produce biometric data interchange records or to use biometric data interchange records or both. In each case, the implemented requirements that are tested for conformance may be different.

No conformance test can be complete or perfect. Ultimately, it is only possible to prove that an **IUT** is non-conformant. The goal of conformance testing is therefore to identify enough of the requirements of the base standard and test their implementation under enough conditions, that any **IUT** that passes the conformance test is likely to be conformant. Frequently, there are inherent problems with the underlying standards that only become apparent during conformance testing. For instance some areas may be undefined (so that the specification of these areas is left to each vendor) or ill-defined/ambiguous (so that there may be a contradiction between parts of the base standard or an easy misinterpretation caused by the wording of the base standard). The latter problem may be resolved by an amendment to or revision of the standard, but the former problem may be difficult to resolve without making technically sound assumptions that need to be well documented by the testing organization.

Conformance testing does not guarantee interoperability; while it is a necessary prerequisite of interoperability, it can only provide a higher level of confidence that interoperability can be achieved. Although the ultimate goal of standards is to allow different products and systems to work together, even two products that are conformant to the same standard may have difficulty interoperating. This is because it is usually impossible for a standard to specify every aspect of the operation of a product or system under all possible conditions and circumstances. On the other hand, unless systems are conformant to a well written standard, it is very unlikely that they will be interoperable. Thus conformance testing is a critical element in assuring interoperability, even if it is not the only one.

Motivation for the Development of Conformance Testing Methodology Standards

As increasing numbers of biometric standards have been developed in recent years, more and more products have become available that claim to be conformant to the standards. This is particularly true in the area of standardized biometric data interchange formats which are standard methods of encoding biometric data for various technologies, including 2-dimensional face image, 3-dimensional face image, fingerprint image, finger pattern, finger minutiae, iris image, vein pattern, signature/sign, hand geometry, plantar image, DNA, etc. Theoretically, those products that support the relevant standard for a given technology should be able to work together, so that an end user of biometrics can mix products from a variety of vendors or support interoperability among different systems, thus ensuring interoperable biometric data interchange across products from different manufacturers.

Although vendors provide products and systems in good faith believing that they conform to a standard, if there is no corresponding **conformance testing methodology** (**CTM**) standard, then there is no clear standardized method for them to be able to verify their conformity claims. Similarly, end users of biometric products can not know with confidence if the products and systems they are using actually conform to the standards

unless a formal **CTM** standard exists and can be used to perform conformance testing of those products and systems in a reliable and repeatable manner.

Elements Required in Conformance Testing Methodology Standards for Data Interchange Formats

In order to formally describe conformance testing for data interchange formats, it is necessary to identify a formal unambiguous language to define the context of conformance testing and conformance claims. Therefore a number of specialized terms have been developed. Many of the terms relate to the fact that there are numerous different types of testing that can be defined for different levels and types of conformance. In the standardization process that has taken place in the U.S. at the InterNational Committee for Information Technology Standards Technical Committee 1 (INCITS M1) – *Biometrics* [1] and at the National Institute of Standards and Technology (NIST), responsible for the development of ANSI/NIST-ITL standards [2] and internationally at the ISO/IEC Joint Technical Commission 1, Subcommittee 37 – *Biometrics* [3], several conformance testing –related elements have been defined including:

Test Assertion - The specification for testing a conformance requirement in an **IUT** in the forms defined in a conformance testing methodology standard. Test assertions are short specific statements that encapsulate a single requirement for a particular standard. A harmonized assertion description language has been developed for data interchange format conformance testing so that the assertions can be expressed in a simple form, regardless of the specific data interchange format being addressed.

Levels 1 to 3 Testing
The CTM standards developed by the Standards Development Organizations (SDOs) mentioned above used slightly different definitions for Level 1, 2, and 3 Testing. However, the different definitions do not contradict each other. The general concept of these levels of testing follows.

Level 1 Testing –A set of test methods within the conformance testing methodology that validates field by field and byte by byte conformance against the specification of the **Biometric Data Interchange Record** (**BDIR**) as specified in the base standard, both in terms of fields included and the ranges of the values in those fields.
(e.g., Testing for a value of a single field: “Does Field A have a value between 0 and 10?” Any value outside of 0 and 10 would not be conformant for Field A.)

Level 2 Testing –A set of test methods within the conformance testing methodology that tests the internal consistency of the **BDIR** under test, relating values from one part or field of the **BDIR** to values from other parts or fields of the **BDIR**.
(e.g., Testing for a relationship between two fields: “If Field A is 9, then Field B shall be 24.” In this case, any other value for Field B, besides 24, would be non-conformant if Field A was 9.)

Level 3 Testing –A set of test methods within the conformance testing methodology that tests that a **BDIR** produced by an **IUT** is a faithful reproduction of the input biometric data that was provided to the **IUT**.
(e.g., Are the fingerprint minutia points specified in the **IUT** actually the minutia points in the fingerprint they are said to derive from?)

Type A - Produce Conformant BDIR (Type A or PCB) – A conformance claim by an **IUT** that it is a conformant **BDIR**, or can create conformant **BDIR**s from appropriate input data.

Type B - Use Conformant BDIR (Type B or UCB) – A conformance claim by an **IUT** that it can read conformant **BDIR**s, interpret them correctly, and perform its desired function upon them.

Issues Related to Testing Levels

It is obvious from the carefully defined terminology listed above that there are issues that have led the standardization bodies to separate the different levels and types of testing. The main consideration is the need for a balance between the importance of delivering **CTM** standards that are meaningful and that can be used to support testing and the desire to thoroughly test all aspects of each data interchange format standard.

The first issue is the fact that data interchange format standards are mostly focused on the structure and content of the **BDIR**. This means that the test assertions for **Level 1** testing can be simply developed by analyzing the explicit requirements of the standard. Test assertions for **Level 2** testing may require consideration of the implicit requirements of the standard, but they can still be defined quite specifically. Some experts prefer to state that **Level 1** testing supports the syntactic requirements of the standard and **Level 2** testing supports the semantic requirements of the standard. Unfortunately, some semantic requirements can only be addressed through **Level 3** testing, and because of the inherently uncertain nature of biometric data, it is very difficult to establish a standardized method of determining whether a **BDIR** is or is not a faithful reproduction of the input biometric data used to produce it. Human biometric characteristics vary with every presentation to a biometric system and there is debate among experts on exactly how to define the relationship between the **BDIR** and the input characteristic, especially when it comes to acceptable levels of accuracy in the representation. For this reason, **Level 3** testing is still an area of research and has not been included in the conformance testing standards for most of the biometric modalities that are currently published or under development. Recently, however, research has progressed enough in ISO/IEC JTC 1/SC 37 to start drafting a **CTM** for finger minutiae data **Level 3** testing.

The second issue relates to the fact that the **BDIR** itself is the focus of the biometric data interchange format standards. It is therefore easy to test claims of **Type A** conformance, since the output **BDIRs** can be tested at least for **Level 1** and **Level 2** conformance. An

IUT that claims **Type B** conformance, however, needs to interpret the **BDIRs** correctly and perform its appropriate function upon them. Since this function may be to use them for biometric matching, to display them for human examination, to convert them to another format or potentially a whole host of other things, it is very difficult to determine how best to test such claims of conformance. One option is to force **IUTs** to also support specific functions of usage that would only be used in **Type B** conformance testing, but so far this idea has not been popular among biometric vendors or standardization experts. It remains to be seen how **Type B** conformance testing will be addressed in the future.

Conformance Testing Standardization

The need for standardized and commonly accepted **CTM**s for Biometric data interchange formats has been recognized by the National and International Standards Bodies on Biometrics mentioned above. Several projects have been initiated over the years to develop **CTM**s. These projects are based on extensive analysis of the data format requirements specified in the base data interchange format standards, and are structured to take advantage of the commonalities found in the testable requirements as well as in the conformance test methods and procedures. The resulting structure of these standards varies from one standards development body to the next (as shown in the next two sections).

Conformance Testing Standardization – INCITS M1 and SC/37 Efforts

CTMs developed by INCITS M1 and ISO/IEC JTC 1/SC 37 were developed as multi-part standards.

- Part 1: Generalized **CTM**
- Part N: Modality-specific Testing Methodology (e.g., Part 2: **CTM** for Finger Minutiae Data Interchange Format)

The Generalized **CTM** contains the elements of the testing methodology that are common to all the data interchange formats (i.e. those elements that are modality independent). These elements include definitions of terms, descriptions of levels and types of testing, general requirements of test reports, specification of the assertion definition language, general test procedures, etc.

Each individual Part contains elements of the testing methodology specific to its respective modality. These elements include specific definitions of terms, specifications of test assertions, test criteria, modality-specific elements of test reports, test procedures, etc.

In February 2005, INCITS M1 initiated the development of a multi-part American National Standard on **CTM** for Biometric Data Interchange Formats. At the time of preparation of this paper, the various parts of this multi-part standard have been published

as ANSI INCITS 423.X. titles. Because the base standards of the ANSI INCITS Biometric Data Interchange formats are separate standards (and not just parts of a single, multi-part standard), the various parts of the multi-part ANSI INCITS 423.X standards reference different standards.

- ANSI INCITS 423.1: 2008 is a Generalized **CTM**
- ANSI INCITS 423.2: 2008 is a **CTM** for ANSI INCITS 378: 2004 – Finger Minutiae Format for Data Interchange
- ANSI INCITS 423.3: 2009 is a **CTM** for ANSI INCITS 377:2004 – Finger Pattern Data Interchange Format
- ANSI INCITS 423.4: 2009 is a **CTM** for ANSI INCITS 381-2004 – Finger Image Based Data Interchange Format

These standards can be found on the ANSI eStore [4].

During the development of INCITS 423, Working Group 3 of ISO/IEC JTC 1/SC 37 initiated the development of a similar multi-part international standard in 2006. This ISO/IEC Project 29109, named "Conformance Testing Methodology for Biometric Data Interchange Formats defined in ISO/IEC 19794." The ISO/IEC 29109 parts are **CTM**s for the "first generation" of ISO/IEC 19794 Biometric data interchange format standards. At the time of preparation of this paper the following parts of ISO/IEC 29109 are published, and can be found on the ISO store [5]:

- ISO/IEC 29109-1: 2009 Generalized **CTM**
- ISO/IEC 29109-2: 2010 **CTM** for Finger Minutiae data format
- ISO/IEC 29109-4: 2010 **CTM** for Finger Image data format
- ISO/IEC 29109-5: 2012 **CTM** for Face Image data format
- ISO/IEC 29109-6: 2011 **CTM** for Iris Image data format
- ISO/IEC 29109-7: 2011 **CTM** for Signature/Sign Time Series data format
- ISO/IEC 29109-8: 2011 **CTM** for Finger Pattern Skeletal data format
- ISO/IEC 29109-9: 2011 **CTM** for Vascular Image data format
- ISO/IEC 29109-10: 2010 **CTM** for Hand Geometry data format

A revision project was started internationally after the publication of the "first generation" of ISO/IEC 19794 standards. The parts of the "second generation" of ISO/IEC 19794 standards do not have corresponding ISO/IEC 29109 parts. The **CTM**s for the "second generation" of ISO/IEC 19794 standards are being specified for each part as an amendment of the base standard. At the time of preparation of this paper, many amendments to the parts of ISO/IEC 19794 are under development:

- ISO/IEC 19794-2: 2011/Amd 1 **CTM** for Finger minutia data format
- ISO/IEC 19794-5: 2011/Amd 1 **CTM** for Face image data format
- ISO/IEC 19794-6: 2011/Amd 1 **CTM** for Iris image data format
- ISO/IEC 19794-8: 2011/Amd 1 **CTM** for Finger pattern skeletal data format

- ISO/IEC 19794-11: 2013/Amd 1 **CTM** for Signature/sign processed dynamic data format
- ISO/IEC 19794-13 /Amd 1 **CTM** for Voice data format
- ISO/IEC 19794-14:2013/Amd 1 **CTM** for DNA data format

The following **CTM** amendments are published:

- ISO/IEC 19794-1:2011 / Amd 1: 2013 Generalized **CTM**
- ISO/IEC 19794-4:2011/Amd 1: 2013 **CTM** for Finger image data format
  ISO/IEC 19794-9:2011/Amd 1: 2013 **CTM** for Vascular image data format

Conformance Testing Standardization – For the ANSI/NIST-ITL Standard

The American National Standards Institute/National Institute of Standards and Technology-Information Technology Laboratory (ANSI/NIST-ITL) standard "Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information" is used by law enforcement, intelligence, military, and homeland security organizations throughout the world. The first version of the standard dates to 1986 and over the years it has been updated and expanded to cover more biometric modalities. ANSI/NIST-ITL 1-2011, NIST Special Publication 500-290 “Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information” (AN-2011) supersedes all previous versions and amendments to the standard [2].

The **CTM** developed to test the data formats specified in the ANSI/NIST-ITL 1-2011 standard was developed as a single document, with a section for assertions common to all record-types, and individual sections on a selected per-record-type (modality specific) basis. The **CTM** contains generic mathematic assertion syntax, the requirements from the base standard, and one or more assertions based on the requirement defined in the assertion syntax.

In August 2012, the National Institute of Standards and Technology released a **CTM** for the ANSI/NIST-ITL 1-2011 standard as NIST Special Publication (SP) 500-295 “Conformance Testing Methodology for ANSI/NIST-ITL 1-2011, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information”. NIST SP 500-295 was developed as a single-part document, which includes several tables of requirements, and test assertions for selected Record Types specified in the ANSI/NIST-ITL 1-2011 standard. This **CTM** includes the concepts and test types necessary to test transactions for conformance to the AN-2011 standard – including terms, test assertion syntax, requirements and test assertions.

Conformance Testing Activities

Approval and publishing of the **CTM** standards alone does not ensure conformance of the Biometric products to the base standards. It is imperative that the

published testing standards are adopted by the Biometric community, including technology vendors, system integrators, and end-users, and implemented in the form of conformance testing tools, processes and programs. Some of these efforts are already underway (e.g., National Voluntary Laboratory Accreditation Program (NVLAP) [6] has published a handbook [7], and accredits laboratories to perform conformance testing [8]), although at the time of publication of this paper there are very few large-scale conformance testing and conformity assessment/certification programs for Biometric data interchange formats.

The fact that a number of Biometric industry vendors claim conformance of their products to national and international data interchange format standards suggests that at least some first-party conformance testing (vendor self-testing) is taking place. The extent to which standardized conformance testing methods and procedures are used for vendor self-testing is not known.

There are indications that governments are interested in establishing second- or third-party conformance testing programs. For example, the United States Department of Defense, Biometrics Identity Management Agency (BIMA) described their Biometric Conformity Assessment Initiative in [9]. Two additional examples of conformity assessment related programs were established ahead of the publication of the necessary standards, and the methods used in these programs have influenced the development of the standards. In the U.S., the certification for biometric algorithms to be approved for use with Personal Identity Verification (PIV) associated with Homeland Security Presidential Directive 12 (HSPD-12) requires that they be tested in a program called Minutia Exchange (MINEX) [10]. This testing ensures that biometric templates produced by the template generation algorithms are conformant to a profiled version of INCITS 378:2004 – Finger Minutiae Format defined specifically for PIV [11]. Similarly, template generation algorithms that are part of biometric products to be used with the Seafarers' Identity Documents programme associated with the International Labour Organization Convention No. 185 [12] were tested by a third party laboratory and were found to be conformant to a profiled version of ISO/IEC 19794-2:2005 – Finger Minutiae Data.

In addition, the National Institute of Standards and Technology’s Information Technology Laboratory, Computer Security Division (NIST/ITL CSD) is involved in another conformity assessment related effort. NIST/ITL CSD has developed and freely released two conformance testing tools under the name BioCTS (Biometric Conformance Test Software). The first tool, BioCTS for AN-2011, is designed to test implementations of the ANSI/NIST-ITL 1-2011 standard. The second tool, BioCTS for ISO/IEC, is designed to test implementations of the ISO/IEC 19794 standards. These test tools provide a common tool for implementers and testing laboratories to use. These tools implement the requirements, in software, specified in the **CTM**s for their respective standards. [13]

Current and Anticipated Needs

It is reasonably well understood that the major needs in implementations of the Biometric systems can be described as interoperability of the systems on all levels and ability to interchange the biometric data. These needs can be fulfilled, to a significant extent, by standardization of all aspects of biometric technology, including biometric formats for data interchange. Such standardization requires the following:

- Robust base standards must exist and be commonly accepted
- Biometric technology must be implemented in conformance with the base standards
- End-users must be able to verify conformance of the implementation to the standards

The last element by itself can be further decomposed in to the following:

- Standardized conformance testing methodologies must exist and be commonly accepted
- Conformance testing tools implementing the standardized methodologies must exist
- Laboratories performing the conformance testing must exist and be able to produce standardized test results
- A process of certification of test results by an independent authority must exist

As shown above, development of the conformance testing methodology standards is only the first necessary step in establishing the conformance testing programs that would be able to reliably test biometric products and provide reasonably conclusive determination of conformance (or non-conformance) of the products to the base standards. While publishing of the **CTM** standards, currently under development and expeditious development of conformance testing tools that implement these standards is recognized as an immediate need, establishing of such full-scale conformity assessment programs in the near future should be anticipated.

Gaps in Standards Development

The development of the **CTM** standards in national and international standards development bodies has been and continues to be successful. There are, however, certain gaps in the existing projects that will need to be addressed at some point in the future, for the testing methodologies to remain useful. These gaps can be divided into three categories:

a) Completeness of the standard. Currently, the conformance testing methodology standards don’t provide (and probably will never provide) full, absolute coverage of all requirements of the base standards. For example, **Type B** and **Level 3** testing are currently out of scope of most of the existing Parts of the conformance testing methodology standards. The motivation behind this is based on practical reasons, and on the fact that certain requirements can not be tested in a reasonable manner; nonetheless the conformance testing coverage is not 100% conclusive. It is expected that additional

test cases/assertions will be developed as the conformance testing methodologies mature, but it is unlikely that the desirable full coverage will ever be reached.

b) Coverage of modalities. Currently, even if most of the existing modalities' conformance testing standardization is planned, many of the Parts have not been initiated even as preliminary drafts. For some relatively new modalities, it is not even clear how conformance testing should be performed. It is fully expected that eventually **CTM**s will be developed for all modalities, but at the present time this is a significant gap.

c) The testing methodologies are almost always "behind" the base standards. The base standards, however robust and mature, are always undergoing changes, amendments and revisions. These changes, sometimes significant, may not be immediately be reflected in the corresponding conformance testing standard, and the time gap between the base standard change and the conformance testing methodology standard corresponding change may be significant – from several months to several years.

Summary

The increased need for interoperability of biometric systems, especially their ability to interchange and share biometric data records has driven the demand for standardization of nearly every aspect of the biometric technology. One of the primary elements of this standardization effort has been development of the biometric data interchange format standards and corresponding conformance testing methodologies that ensure fulfillment by the biometric implementations of the requirements specified in the base standards.

Related Entries

Standardization

References

1. InterNational Committee for Information Technology Standards: M1. (2004). INCITS: M1 – Biometrics. Website URL: http://standards.incits.org/a/public/group/m1

2. NIST/ITL, Information Access Division. (2013). ANSI/NIST-ITL Standard Homepage. Website URL: http://www.nist.gov/itl/iad/ig/ansi_standard.cfm

3. International Organization for Standardization Joint Technical Committee 1/SubCommittee 37. (n.d.). JTC 1/SC 37– Biometrics Homepage. Website URL: http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/jtc1_home/jtc1_sc37_home.htm

4. American National Standards Institute. (2013). eStandards Store. Website URL: http://webstore.ansi.org/

5. International Organization for Standardization. (n.d.). ISO Store. Website URL: http://www.iso.org/iso/home/store.htm

6. NIST/National Voluntary Laboratory Accreditation Program. (2013). NVLAP. Website URL: http://www.nist.gov/nvlap/

7. Moore, Brad, Iorga, Michaela, "Biometrics Testing", NIST Handbook 150-25, 2009. Website URL: http://www.nist.gov/nvlap/upload/NIST-HB150-25-2009-1.pdf

8. NIST/National Voluntary Laboratory Accreditation Program. (2013). Directory of Accredited Laboratories, Biometrics Testing. Website URL: http://ts.nist.gov/standards/scopes/biometrics.htm

9. Biometrics Identity Management Agency (n.d.). Conformity Assessment. Website URL: http://www.biometrics.dod.mil/CurrentInitiatives/Standards/conformity.aspx

10. NIST/ITL, Information Access Division. (2011). MINEX Minutia Exchange. Website URL: http://www.nist.gov/itl/iad/ig/minex.cfm

11. Wilson, C., Grother, P., and Chandramouli, R., "Biometric Data Specification for Personal Identity Verification", NIST Special Publication 800-76-1, 2007

12. "Seafarers' Identity Documents Convention (Revised)", International Labour Organization Convention No. 185, International Labour Organization, 2003

13. NIST/ITL, Computer Security Division. (2013). Biometric Conformance Test Software for Biometric Data Interchange Formats. Website URL: http://www.nist.gov/itl/csd/biometrics/biocta_download.cfm

Definitional Entries

Conformance Testing

Conformance testing is the process of capturing the technical description of a specification and measuring whether an implementation faithfully implements the specification by achieving conformance to the technical description of the specification. Conformance is defined generally as the fulfillment by a product, process, or service of all relevant specified requirements.

Implementation Under Test (IUT)

The **IUT** is that which implements the base standard(s) being tested. Depending on the conformance requirements of the base standard, this may simply be a set of biometric data interchange records (**BDIR**s) or it may be a computer algorithm or other product that creates the **BDIR**s and/or uses the data contained in the **BDIR**s.

Biometric Data Interchange Record (BDIR)

A **BDIR** is a data package containing biometric data that claims to be in the form prescribed by a specific biometric data interchange format standard.