Conformance Test Suite Implementations for Common Biometric Exchange Formats Framework (CBEFF) Data Structures

Yooyoung Lee, Fernando L. Podio, Mark Jerde

National Institute of Standards and Technology, Information Technology Laboratory (NIST)
Gaithersburg, MD 20899-8930, USA
{yoo.lee, fernando.podio}@ nist.gov, mjerde@idtp.com

Abstract. Biometric technologies are able to establish or verify personal identity against previously enrolled individuals. Used alone, or together with other authentication technologies such as tokens and passwords, they can provide higher degrees of security than other technologies employed alone, and can also be used to overcome their weaknesses. Existing biometric interface standards define data structures called Biometric Information Records (BIRs) that contain biometric data and associated metadata that describes the biometric data. BIRs often are used for the protection, interchange, transmission and storage of biometric data. This paper describes a conformance testing methodology for BIRs that conform to instantiations of Common Biometric Exchange Formats Framework (CBEFF) and discusses the characteristics and functionality of Conformance Test Suite (CTS) implementations developed at NIST to support conformance testing of these data structures. Ongoing research and development work on testing architectures to support these CTS implementations is discussed.

Keywords: Biometrics; Biometric Information Records; Common Biometric Exchange Formats Framework; Standards, Biometrics; Testing, Conformance; Test Suites

1. Introduction

Biometrics is defined as automated methods of recognizing an individual based on measurable biological or behavioral characteristics. Biometric technologies are able to establish or verify personal identity against previously enrolled individuals. Used alone, or together with other authentication technologies, biometric technologies can provide higher degrees of security than other technologies employed alone, and can also be used to overcome their weaknesses.

For decades, biometric technologies were primarily used in law enforcement applications. In addition to these important applications, currently, they are also required in many public and private sector applications worldwide to authenticate a person’s identity, secure national borders and restrict access to secure sites including buildings and computer networks. Diverse environments such as amusement parks, banks, mobile devices, passport programs and driver’s licenses, colleges and school lunch programs are already using these technologies for personal verification or identification applications.

Standardization is a critical component in the advancement of all technology. Standards provide structure and a framework by which development, interoperability, interchange, and functionality are achieved. Currently published and ongoing biometric standards development efforts support the mass market adoption of biometric technologies by helping customers achieve higher levels of security and interoperability in personal verification and identification applications using biometric-based open systems solutions. A number of standards have been published or are under development to support interoperability and data interchange among biometrics applications and systems. Other standards have been developed to describe testing methodologies to assess biometric data formats and systems conformance, performance and interoperability. Metadata is usually required to facilitate the use and management of biometric data. The content, amount and detail conveyed in these metadata depend, in most instances, on the domain of use (application/system) of the biometric data. Standardized data structures designed to encapsulate biometric data support biometric data exchange by describing characteristics of the biometric data contained in these data structures such as the modality and format of the biometric. They can also convey information useful to support protection of the biometric data such as whether the data is encrypted or signed. The need for these data structures is addressed below. Also below we address conformance testing of these data structures called Biometric Information Records (BIRs).

Conformance testing captures the technical description of a standard and measures whether or not an implementation faithfully implements the standard. A precise notion of correctness of an implementation derived from using formal testing methods is needed [1]. Conformity assessment provides confidence to users through programs that demonstrate the conformity of products to specific standards. Ongoing research on conformance testing architectures to support testing of the components of BIRs is discussed below. Conformance Test Suite (CTS) implementations recently developed at the National Institute of Standards and Technology (NIST) for testing the conformance of instantiations of these BIRs to available standards are also discussed.

2. Biometric Information Records (BIRs)

Biometric data interchange format standards define a level of metadata on the biometric data described in these standards. Whether these metadata are sufficient to achieve system requirements is application-dependent (e.g., expected system functionality). Often, applications need additional metadata that is not specified in these records. The data structures used to contain the required additional metadata and encapsulate the biometric data are application-dependent (e.g., unsupervised local authentication or remote authentication applications). These data structures can be proprietary or standardized. They are sometimes required to provide means for self-describing biometric data records to reveal the format and other attributes of their biometric-specific data without exposing the data itself to applications. They are also used to provide means for applications to efficiently determine whether a particular biometric data record is of interest, and if so, which biometric services to call to process the biometric-specific data. Biometric standards development bodies [2 and 3] have developed technical interface standards that specify these data structures called BIRs.

2.1 Common Biometric Exchange Formats Framework (CBEFF)

BIRs defined in CBEFF standards [4-8] promote interoperability of biometric-based application programs and systems by specifying metadata that describes specific characteristics of the biometric data contained in these BIRs such as the modality and format of the biometric data, when it was captured, its expiry date, whether it is encrypted, etc. These BIRs can convey information useful to support security of the biometric data (e.g., security/integrity options, user-defined payload, challenge-response data). These standards specify a set of abstract data elements and values that can be used to create the header part of a BIR conforming to CBEFF. Clearly specified instantiations of these BIRs are called “Patron format specifications or standards”. These Patron Formats are fully-defined by a recognized standards development organization (which can be a standards body, working group, or industry consortium). ISO/IEC JTC 1 SC37 defines “CBEFF patrons” in [6] as organizations that have been accepted for registration with the Biometric Registration Authority in accordance with [7], and that can therefore specify one or more CBEFF patron formats. CBEFF standards specify the BIRs discussed above.

CBEFF BIRs define three major sections in a single structure:

- The SBH (Standard Biometric Header) includes the required data elements (e.g., format and modality of the biometric data, product identifier) and any necessary optional data element(s) such as security/integrity.
- The BDB (Biometric Data Block) contains the biometric data. It can contain processed or unprocessed biometric data.

- The SB (Security Block) contains information concerning the encryption of BDBs in a BIR and the integrity of the BIR.

Patron Formats specify details of these data structures. Two mandatory fields in the SBH are the BDB Format Owner and Type. The Format Owner denotes the vendor, standards body, working group or industry consortium that has defined the format of the biometric data (the data contained in the BDB). A CBEFF requirement is that format owners register with the International Biometric Industry Association (CBEFF Registration Authority) for an assigned identifier of the Format Owner. It is the combined CBEFF Format Owner/Format Type value that uniquely identifies the BDB format. Other metadata that can be found in the SBH is information on the modality of the biometric data contained in the BDB, identification of the product/device that generated the data, when the biometric data was captured, its expiry date, whether it is encrypted, etc. The SBH can also contain payload (public or secret) and challenge response metadata (both user-defined).

A number of standards and user's organizations have defined CBEFF Patron Formats or have adopted CBEFF Patron Formats developed by other organizations. In addition to the mandatory data elements specified in CBEFF standards, each Patron Format specification defines which CBEFF optional 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).

We have examined a number of these CBEFF Patron Formats specified in [5 and 8]. We discuss below an experimental conformance testing architecture developed with the purpose of supporting CTS implementations for the three components of CBEFF BIRs conforming to different patron formats. We discuss below a CTS implementation developed with the purpose of testing a number of BIRs claiming conformance to a specific existing patron format, Patron Format A (PF-A) specified in [5]. This patron format can be used for applications where other existing patron formats are not adequate for the application (or domain of use) and it is not desirable to establish a new patron format. Length and encoding of each data field is specified, therefore facilitating decoding of data structures conforming to this Patron Format. The required and optional CBEFF data elements present in the PF-A SBH follow a pre-determined sequence indicated in the standard further facilitating decoding of these structures. A field specified in the format (Optional Data Elements Present Mask) provides information to the decoder on what optional fields are present in the record header.

Applications and system specifications based on this format are permitted to exclude optional CBEFF data elements from the record header that are not required for the application. The format and length of each portion of the BIR is also specified.

3. CBEFF Conformance Testing

We discuss below elements of a conformance testing process and we describe a conformance testing architecture for the three components of a single CBEFF data structure. We also discuss the characteristics of a CTS developed by NIST to test data structures that conform to a specific CBEFF PF-A.

3.1 Elements of a Conformance Testing Process

A conformance testing process is the complete range of testing-related activities that ultimately lead to the assessment of conformity of an IUT (Implementation Under Test) to a specification or standard and therefore, it includes at a minimum:

a) Analysis of the specification or standard
  - Identification of data elements to be tested and other requirements (e.g., consistency of the data structure)

b) Development of a conformance testing methodology specification or standard including:
  - Scope of tests
  - Development of the test purposes and test cases
  - Development of a vendor implementation declaration format

c) CTS implementation including:
  - Development of the testing plan
  - Design of a detailed architecture
  - Generation of required test cases and binary data to test the CTS implementation
  - Execution of the tests
  - Generation of test logs and test reports

3.2 Conformance Testing Architecture and CTS Implementation

For the purpose of this paper IUTs are Biometric Information Records (BIRs) conforming to Patron Format A (PF-A) specified in [5]. The IUTs are expected to conform to all the requirements specified in the standard for this Patron Format. They include the mandatory requirements (including the required header fields), conditional fields specified in the CBEFF PF-A Header and the optional fields selected for a specific PF-A instantiation.

As discussed above, consistency of the BIR structure (e.g., length of each main element) is also tested. The CTS tests the extent to which an IUT satisfies both Level 1 and 2 testing requirements. Level 1 testing addresses the testing methodology that verifies field by field and byte by byte conformance of the CBEFF BIR header with respect to what is specified in the standard, the patron format and the vendor implementation declaration that describes the characteristics of the IUT (called “Manifest” in this paper) both in terms of field values and the ranges of values for those fields. Level 2 testing is testing of the internal consistency of the BIR header relating values from one field to other(s) in the header and the rest of the BIR structure [9]. CTS implementations use the “Manifest” to test the IUT only against the characteristics implemented in the IUT and not against the entire range of features and possible values specified in the standard.

As shown in Fig. 1 the CTS architecture consists of a controller/Graphical User Interface (GUI) and CTS module implementations developed to test for conformance to different CBEFF Patron Formats. The architecture supports SBH, BDB and SB testing modules.

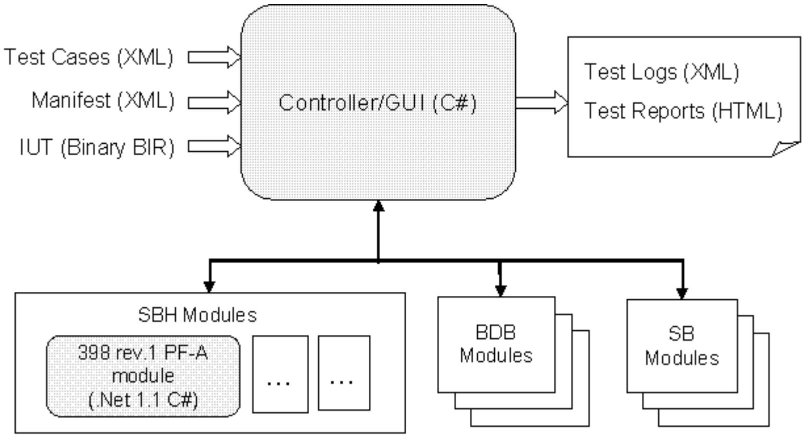


Fig.1. Conformance Testing Architecture

3.2.1 Controller/GUI and Interfaces

The Controller is responsible for handling the tests, logging test results, test suite parameterization, selection and handling of the GUI and the interface with the appropriate testing module. The architecture is extensible to other CTS modules developed to test for conformance to other CBEFF Patron Formats or Biometric Data Blocks (BDBs) containing biometric data of any modality. Support for CTS implementations testing conformance to Security Blocks (SBs) is also provided. The controller is designed to communicate with a number of CTS module implementations. The interface supported by the controller is shown below:

C# interface between the Controller and the modules:

```
public bool Is_CBEFF(byte[] byteArray,
             CBEFF_FIELDS[] fieldsArray,
             out CBEFF_ERRORS[] ErrRay,
             out int errByteRayPos,
             out int errField,
             out int errNum )
```

3.2.2 CTS Modules and CTS PF-A Implementation

As shown in Fig. 2 the current CTS implementation allows the user to perform the following tasks/tests:

- Generation/editing of Manifests representing the characteristics of specific binary files (BIRs under test).
- Generation/editing/testing of single test cases and binary files.
- Simultaneous testing of a large number of test cases or binary files.

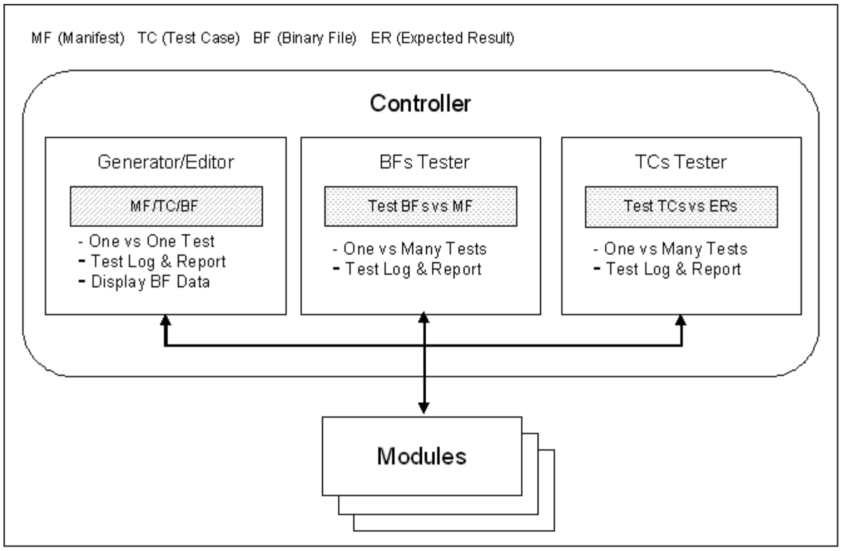


Fig. 2. Controller

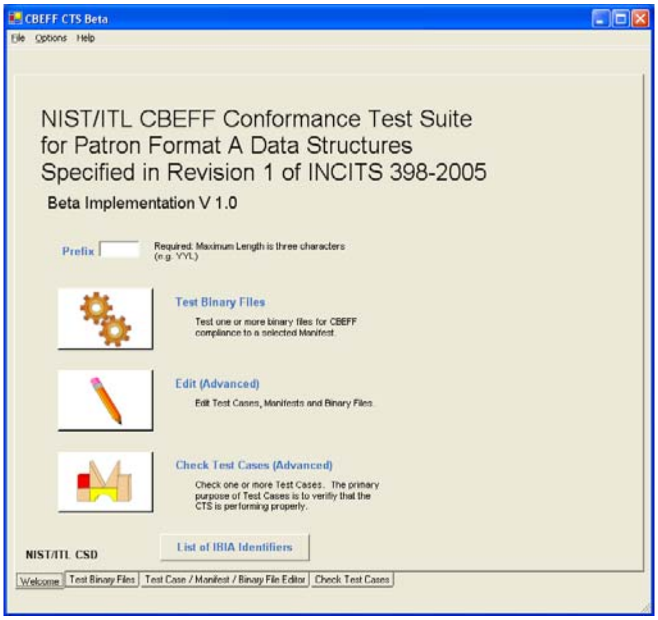
A number of test cases ("Valid" and "Invalid") were developed. They describe the detailed steps that must be followed in order to achieve the stated purpose of each test. At the end of each test case, a verdict to the test case is included. These criteria are expressed as "Pass" or "Fail". Test case generation is determined by the specification and the conformance requirements. The CTS implementation is evaluated by checking whether all generated test cases have been performed successfully. "Fail" verdicts may be caused by a fault or unexpected behavior in the CTS. Associated error messages help to determine what circumstance produced the fault. A test case is performed successfully when the test result is the same as the expected result. An additional benefit of these test cases is verifying the correctness of the standard [10]. If errors are found, one can correctly deduce that the implementation does not conform to the specification; however, the absence of errors does not necessarily imply the converse [11]. Over 400 files were developed for the current PF-A CTS implementation. For instance, the test case shown below in Fig. 3 is a "Valid" test case. The test purpose is to test the relationship between the Biometric Type and Biometric Subtype fields.

```
<?xml version="1.0" encoding="UTF-8" ?>
<TestSuite Type="TestCases" DLL="INCITS 398 Rev.1 – Patron Format
A" DateTime="4/26/2007 7:18:58 PM UTC" NumTestCases="1"
NumPass="1" NumFail="0">
<TestCase xsi:noNamespaceSchemaLocation="Schema_03.xsd"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<Name>Valid_Test_Case_Example</Name>
<Description>The relationship between the Biometric Type and
Biometric Subtype is pass</Description>
<ExpectedResult>Pass</ExpectedResult>
<NumberOfFields>16</NumberOfFields>
<Field Sequence="1" Name="SBH_patron_format_owner"
DefinedLength="2" ActualLength="2" BytesBase64="ABs=" Hex="001B"
/>
                              :

<Field Sequence="16" Name="Biometric_data_block"
DefinedLength="1" ActualLength="1" BytesBase64="AA==" Hex="00" />
<TestResult>Pass</TestResult>
</TestCase>
</TestSuite>
```

Fig. 3. “Valid” Test Case Example

The CTS module implemented by NIST tests binary files claiming conformance to PF- A specified in [5]. This CTS implementation can be used to test data structures to determine whether the requirements specified in the CBEFF standard for implementations of this Patron Format are met. Fig. 4, is a screen shot of the CTS implementation’s main page.



NIST/ITL CBEFF Conformance Test Suite
for Patron Format A Data Structures
Specified in Revision 1 of INCITS 398-2005

Beta Implementation V 1.0

Prefix ▭ Required: Maximum Length is three characters (e.g. YYL)

Test one or more binary files for CBEFF compliance to a selected Manifest.

Edit Test Cases, Manifests and Binary Files.

Check one or more Test Cases. The primary purpose of Test Cases is to verify that the CTS is performing properly.

Fig. 4. CBEFF Patron Format A CTS Implementation

The CBEFF PF-A CTS tests whether IUTs satisfy both Level 1 and 2 testing requirements. These BIRs are expected to conform to all the requirements specified in the standard for this Patron Format and the description of a particular instantiation of PF-A as described in the Manifest.

The PF-A CTS implementation tests the following:

- All CBEFF BIR header mandatory fields and the conditional and optional header fields (specified in the Manifest)
- All required interrelationships between the header fields

- The required sequence of header fields
- Length of the full BIR (Standard Biometric Header, Biometric Data Block and Security Block)
- Consistency of the full BIR

Test results generated by the CTS implementation are evaluated using “Pass”/”Fail” criteria.

As shown in Fig. 1, the CTS architecture supports testing modules for the three sections of the CBEFF BIRs. As described above, the current CTS beta implementation tests the BIR headers (PF-A SBHs), the length of the three BIR sections and the consistency of the BIRs. Plans for a modified CTS version (under development) include incorporating testing modules for the other CBEFF BIR sections (i.e., BDBs, SBs) as well as for other CBEFF Patron Formats.

4. Results

The Conformance Test Suite (CTS) implementation developed by NIST has been successfully tested using a large set of “Valid” and “Invalid” test cases. Over 400 test cases were developed and used in the tests to evaluate the CTS performance. A large number of binary files representing similar combinations of characteristics specified in Manifests have been successfully tested. The testing architecture is extensible to other CTS modules developed to test the three elements of CBEFF Biometric Information Records (BIRs) including modules to test Standard Biometric Headers (SBHs) conforming to other Patron Formats as well as CTS modules to test Biometric Data Blocks (BDBs) and Security Blocks (SBs).

5. Conclusion, ongoing and future work

We have discussed a conformance testing architecture that was developed to support CTS implementations for testing the three elements of CBEFF data structures. We have discussed a conformance testing module developed to test binary files (BIRs) conforming to a Patron Format specified in a standard (PF-A defined in [5]). The CTS design allows for efficient processing of a large number of test cases or binary files in a very short amount of time. Test results are expressed in two formats. For easy human verification of single test results, test reports in HTML are generated. To facilitate automated verification and statistics generation over a large number of binary files tested, test logs encoded in XML are also generated. The controller/module interface allows easy integration of other testing modules for BIRs conforming to other Patron Formats as well as modules to test conformance of the content of BDBs and SBs. Tests are currently performed on a modified testing architecture. Research and development on advanced conformance testing architectures is ongoing.

References

1. Belinfante, J. Feenstra, R. d. Vries, J. Tretmans, N. Goga, L. Feijs, S. Mauw, and L. Heerink, “Formal test automation: A simple experiment”, In G. Csopaki, S. Dibuz, and K. Tarnay, editors, 12th Int. Workshop on Testing of Communicating Systems, pages 179--196. Kluwer Academic Publishers, 1999.
2. International Standards Organization/ International Electrotechnical Commission (ISO/IEC) Joint technical Committee 1 (JTC 1) Subcommittee 37 (SC 37) – Biometrics.
3. InterNational Committee for Information Technology Standards (INCITS) Technical Committee M1 – Biometrics.
4. Fernando L. Podio, Jeffrey S. Dunn, Lawrence Reinert, Catherine Tilton, Bruno Struif, Fred Herr, Jim Russell, M. Paul Collier, Mark Jerde, Lawrence O. Gorman, Brigitte Wirtz, “Common Biometric Exchange Formats Framework (CBEFF 1.1)”, NISTIR 6529-A, 2002.
5. Common Biometric Exchange Formats Framework (CBEFF), Revision of ANSI/INCITS 398-2005.
6. Information technology - Common Biometric Exchange Formats Framework (CBEFF) - Part 1: Data Element Specification, ISO/IEC 19785-1 Information Technology, 1 May 2006.
7. Information technology - Common Biometric Exchange Formats Framework (CBEFF) - Part 2: Procedures for the Operation of the Biometric Registration Authority, ISO/IEC 19785-2: 2006.
8. Information technology - Common Biometric Exchange Formats Framework (CBEFF) - Part 3, FDIS ISO/IEC 19785-3 Patron Format Specifications.
9. Conformance Testing Methodology Standard for Biometric Data Interchange Formats – Part 1: Generalized Conformance Testing Methodology, M1/06-0768, http://m1.incits.org/m1htm/2006docs/m1docreg_2006.htm.
10. P. Jalote, “Testing the completeness of specifications” IEEE Transactions on Software Engineering, 15(5):526-531, May 1989.
11. Martha Gray, Alan Goldfine, Lynne Rosenthal, Lisa Carnahan, National Institute of Standards and Technology, http://xml.coverpages.org/conform20000112.html

Comment [FKH1]: Citations 11 and 12 are not referenced in the text.

Comment [FKH2]: Does this citation have a title?