

InterNational Committee for Information Technology Standards
 INCITS Secretariat, Information Technology Industry Council (ITI)
 1250 Eye St. NW, Suite 200, Washington, DC 20005
 Telephone 202-737-8888; Fax 202-63-4922
 email: ncits@itic.org

Preliminary Application Profile Template for Project NCITS 1566 - D - Application Profile - Interoperability and Data Interchange - Biometrics-Based Verification and Identification for Border Crossing

ISO/IEC Technical Report TR 10000-1, Information Technology - Framework and Taxonomy of International Standardized Profiles

ISO/IEC Directives, Part 2, Rules for the Structure and Drafting of International Standards

Revision History

Revision	Date	M1 Doc	Comments
1	08/1/2002	020134	First Draft
2	09/10/2002	020209	Add definitions and Annexes A, B

Technical Editor: Fred Herr
fherr@idtechpartners.com
 Phone 215 527 6717

Foreword

INCITS (The International Committee for Information Technology Standards) is the ANSI recognized Standards Development Organization for information technology within the United States of America. Members of INCITS are drawn from Government, Corporations, Academia and other organizations with a material interest in the work of INCITS and its Technical Committees. INCITS does not restrict membership and attracts participants in its technical work from 13 different countries, and operates under the rules of the American National Standards Institute.

In the field of Biometrics, INCITS has established the Technical Committee M1. Standards developed by this Technical Committee have reached consensus throughout the development process and have been thoroughly reviewed through several Public Review processes. In addition, this American National Standard has been approved by the INCITS Executive Board and ANSI Board of Standards Review for Publication as an ANSI/INCITS Standard.

((Patent Statement to be inserted at this point))

Table of Contents

Foreword

Introduction

1. Scope

1.1 Functions overview

1.2 Requirements

1.3. Types of Users

1.4 Environments

2. Conformance

2.1 Required

2.2 Optional

2.3 Identification of options from related standards that are mandatory under this AP

3. Normative References

3.1 Existing Standards

3.2 Standards that need to be developed

4. Definitions

5. Symbols (and abbreviated terms)

6. Functions

6.1 Enrollment

6.2 Verification

6.3 Data formats for interchange

6.4 Data security and integrity

6.5 Message protocols, transaction specifications

6.6 Performance

6.7 Metrics

6.8 Testing

Annex A: Biometric Implementation Conformance Statement

Foreword

Introduction

1. Scope

This ANSI/INCITS Standard specifies the application profile to be used in support of biometrics-based identification and verification within border crossing applications and systems.

1.1 Functions overview

1.1.1 Verification and Border Crossing

Verification is the process of verifying that the bearer of the Biometric token is the same as the person for which the token was created during the enrollment process. Biometric information may take the form of, but not limited to, fingerprint minutia, fingerprint pattern, or facial image. Biometrics-based verification within border crossing systems increases the level of confidence that the bearer of the token, i.e., the person seeking to cross the border, is in fact the same person to whom the token was issued.

1.1.2 Biometric enrollment process

1.1.3 Multiple factor biometrics

1.1.4 Multiple enrollment locations

1.2 Requirements

1.2.1 Biometric identification of enrollees

One to many enrollment identification

1.2.2 Background check

1.2.3 Credential issuance

One to one verification of card owner

1.3. Types of Users

1.3.1 Card usage

1.3.2 Re-issuance

1.3.3 Administrator's authority biometrically verified

1.4 Environments

1.4.1 Data security and integrity

1.4.2 Data interchange

2. Conformance

5.1 Required

5.2 Optional

5.3 Identification of options from related standards that are mandatory under this AP

3. Normative References

3.1 Existing Standards

ANSI/INCITS 358-2002 - Information technology - BioAPI Specification

ANSI/INCITS xxx-200x – Information Technology - Finger Minutiae Format for Data Interchange

ANSI/INCITS yyy-200x – Information Technology - Face Recognition Format for Data Interchange

ANSI/INCITS zzz-200x – Information Technology - Finger Pattern-Based Format for Data Interchange

ANSI/NIST-ITL 1-2000, Standard Data Format for the Interchange of Fingerprint, Facial, & Scar mark & Tattoo (SMT) Information

ANSI/X9 X9.84-2001 - Biometric information management and security

ICAO Document 9303 – Machine Readable Travel Documents

ISO/IEC CD 7816-11.2 - Identification cards - Integrated circuit(s) cards with contacts - Part 11 Personal verification through biometric methods in integrated circuit cards

ISO/IEC FDIS 9594-8 Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

ISO/IEC 10918 - Information technology - Digital Compression and coding of continuous-tone still images (JPEG) (Parts 1-4)

ISO/IEC 15444 - Information technology - JPEG 2000 Image Coding System (Parts 1-10)

Federal Information Processing Standard (FIPS) - FIPS 197 Advanced Encryption Standard (AES) - November 2001

ISO/IEC WD 18033 - Information technology - Security techniques - Encryption algorithms (Parts 1-3)

3.2 Standards that need to be developed

NISTIR 6529-2001, Common Biometric Exchange File Format (CBEFF).

4. Terms and Definitions

Editor's note: The definitions in this draft section are those that I believe are relevant to the context of this and related Application Profiles. It is important that key terms have consistent meanings within and across the base standards and other, related Profiles, so I believe all the M1 Profiles being drafted should draw their definitions from the same source. Each profile should include only those definitions that it (and its base standards) actually uses, and it should also add any definitions that are unique to it. Contributors should feel free to offer additional terms and definitions, or to suggest changes.

I plan to follow Mike Hogan's recommendation that definitions should be based on a cited, hopefully stable, authority, with the text of the definition included in the Profile for the convenience of the reader.

The superscript on each term below identifies the source of its definition as follows:

1. AfB Glossary posted on AfB web site.
2. Paraphrased from Colin Soutar, "Biometric Functionality Definitions," M1 document M1/02-0196.
3. Original definition drafted by F. Herr in this Application Profile.
4. ISO/IEC TR 10000-1:1998(E) *Information Technology – Framework and taxonomy of International Standardized Profiles*

API (Application Program Interface)¹ – A set of services or instructions used to standardise an application. An API is computer code used by an application developer. Any biometric system that is compatible with the API can be added or interchanged by the application developer. APIs are often described by the degree to which they are high level or low level. High level means that the interface is close to the application and low level means that the interface is close to the device.

Application³ – A hardware/software system implemented to satisfy a [broad] set of requirements. In this context, an **application** incorporates a **biometric system** to satisfy a subset of requirements related to the **verification** or **identification** of an **end user's identity** so that the end user's **identifier** can be used to facilitate the end user's interaction with the system. For example, a

- biometrics-enabled time and attendance system has a [broad] requirement to record an employee's starting and leaving times so the employee can be paid the correct amount of wages. The system uses biometrics to verify the employee's [end user's] claim that his **identity** is the one that the system has associated with the employee's id-number [**identifier**] at the times when the employee interacts with the biometric device as he enters and leaves the work place.
- Application Developer**¹ – An individual entrusted with developing and implementing a biometric application.
- Application Profile**⁴ – conforming subsets or combinations of base standards used to provide specific functions. Application profiles identify the use of particular options available in base standards, and provide a basis for the interchange of data between applications and interoperability of systems.
- Authentication**¹ – [a term that should not be used] Alternative term for 'Verification'.
- Base Standard**⁴ – fundamental and generalized procedures. They provide an infrastructure that can be used by a variety of applications, each of which can make its own selection from the options offered by them.
- Biometric**¹ – A measurable, physical characteristic or personal behavioural trait used to recognise the identity, or verify the claimed identity, of an enrollee.
- Biometric Data**¹ – The information extracted from the biometric sample and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data).
- Biometric Sample**¹ – Raw data representing a biometric characteristic of an end-user as captured by a biometric system (for example the image of a fingerprint).
- Biometric System**¹ – An automated system capable of:
1. capturing a biometric sample from an end user;
 2. extracting biometric data from that sample;
 3. comparing the biometric data with that contained in one or more reference templates;
 4. deciding how well they match; and
 5. indicating whether or not an identification or verification of identity has been achieved.
- Capture**¹ – The method of taking a biometric sample from the end user.
- Certification**¹ – The process of testing a biometric system to ensure that it meets certain performance criteria. Systems that meet the testing criteria are said to have passed and are certified by the testing organisation.
- Comparison**¹ – The process of comparing a biometric sample with a previously stored reference template or templates. See also 'One-To-Many' and 'One-To-One'.
- Claimant**¹ – A person submitting a biometric sample for verification or identification whilst claiming a legitimate or false identity.
- Closed-Set Identification**¹ – When an unidentified end-user is known to be enrolled in the biometric system. Opposite of 'Open-Set Identification'.
- Database**¹ – Any storage of biometric templates and related end user information. Even if only one biometric template or record is stored, the database will simply be "a database of one". Generally speaking, however, a database will contain a number of biometric records.
- End User**¹ – [see User - different] A person who interacts with a biometric system to enrol or have his/her identity checked.
- End User Adaptation**¹ – The process of adjustment whereby a participant in a test becomes familiar with what is required and alters their responses accordingly.
- Encryption**¹ – The act of converting biometric data into a code so that people will be unable to read it. A key or a password is used to decrypt (decode) the encrypted biometric data.
- Enrollee**¹ – A person who has a biometric reference template on file.
- Enrolment**¹ – The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.
- Extraction**¹ – The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.
- False Acceptance**¹ – When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity.
- False Acceptance Rate/FAR**¹ – The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor

attempts. The False Accept Rate may be estimated as

$$FAR = NFA / NIIA$$

or

$$FAR = NFA / NIVA$$

where

FAR is the false acceptance rate

NFA is the number of false acceptances

NIIA is the number of impostor identification attempts

NIVA is the number of impostor verification attempts

False Match Rate¹ – Alternative to ‘False Acceptance Rate’. Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of ‘False Acceptance’ and ‘False Rejection’. See also ‘False Non-Match Rate’.

False Non-Match Rate¹ – Alternative to ‘False Rejection Rate’. Used to avoid confusion in applications that reject the claimant if their biometric data matches that of an enrollee. In such applications, the concepts of acceptance and rejection are reversed, thus reversing the meaning of ‘False Acceptance’ and ‘False Rejection’. See also ‘False Match Rate’.

False Rejection¹ – When a biometric system fails to identify an enrollee or fails to verify the legitimate claimed identity of an enrollee.

False Rejection Rate/FRR¹ – The probability that a biometric system will fail to identify an enrollee, or verify the legitimate claimed identity of an enrollee. The False Rejection Rate may be estimated as follows:

$$FRR = NFR / NEIA$$

or

$$FRR = NFR / NEVA$$

where

FRR is the false rejection rate

NFR is the number of false rejections

NEIA is the number of enrollee identification attempts

NEVA is the number of enrollee verification attempts

This estimate assumes that the enrollee identification/verification attempts are representative of those for the whole population of end-users. The False Rejection Rate normally excludes ‘Failure to Acquire’ errors

Identifier² – A unique data string used as a key in the biometric system to name a person’s *identity* and its associated attributes. An example of an *identifier* would be a passport number.

Identity² – The common sense notion of personal identity. A person’s name, personality, physical body, and history, including such attributes as nationality, educational achievements, employer, security clearances, financial and credit history, etc. In a biometric system, *identity* is typically established when the person is *registered* in the system through the use of so-called “breeder documents” such as birth certificate, passport, etc.

Identification/Identify¹ – The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the enrollee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with ‘Verification’.

Impostor¹ – A person who submits a biometric sample in either an intentional or inadvertent attempt to pass him/herself off as another person who is an enrollee.

Live Capture¹ – The process of capturing a biometric sample by an interaction between an end user and a biometric system.

Match/Matching¹ – The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. An accept or reject decision is then based upon whether this score exceeds the given threshold.

Multiple Biometric¹ – A biometric system that includes more than one biometric system or biometric technology.

- One-to-a-Few**¹ – A hybrid of one-to-many identification and one-to-one verification. Typically the one-to-a-few process involves comparing a submitted biometric sample against a small number of biometric reference templates on file.
- One-to-Many**¹ – Synonym for ‘Identification’.
- One-to-One**¹ – Synonym for ‘Verification’.
- Open-Set Identification**¹ – Identification, when it is possible that the individual is not enrolled in the biometric system. Opposite of ‘Closed-Set Identification’.
- Out of Set**¹ – In open-set identification, when the individual is not enrolled in the biometric system.
- PIN (Personal Identification Number)**¹ – A security method whereby a (usually) four digit number is entered by an individual to gain access to a particular system or area.
- Population**¹ – The set of end-users for the application.
- Recognition**¹ – The preferred term is ‘Identification’.
- Record**¹ – The template and other information about the end-user (e.g. access permissions)
- Registration**² – The process of making a person’s *identity* known to a biometric system, associating a unique *identifier* with that identity, and collecting and recording the person’s relevant attributes into the system.
- Template/Reference Template**¹ – Data, which represents the biometric measurement of an enrollee, used by a biometric system for comparison against subsequently submitted biometric samples.
- Template Ageing**¹ – The degree to which biometric data evolves and changes over time, and the process by which templates account for this change.
- Template Size**¹ – The amount of computer memory taken up by the biometric data.
- Type I Error**¹ – In statistics, the rejection of the null hypothesis (default assumption) when it is true. In a biometric system the usual default assumption is that the claimant is genuine, in which case this error corresponds to a ‘False Rejection’.
- Type II Error**¹ – In statistics, the acceptance of the null hypothesis (default assumption) when it is false. In a biometric system the usual default assumption is that the claimant is genuine, in which case this error corresponds to a ‘False Acceptance’.
- User**¹ – The client to any biometric vendor. The user must be differentiated from the end user and is responsible for managing and implementing the biometric application rather than actually interacting with the biometric system.
- Validation**¹ – The process of demonstrating that the system under consideration meets in all respects the specification of that system.
- Verification/Verify**¹ – The process of comparing a submitted biometric sample against the biometric reference template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee’s template. Contrast with ‘Identification’.
- WSQ (Wavelet Transform/Scalar Quantisation)**¹ – A compression algorithm used to reduce the size of reference templates.

5. Symbols (and abbreviated terms)
6. Functions
 - 6.1 Enrollment
 - 6.2 Verification
 - 6.3 Data formats for interchange
 - 6.4 Data security and integrity
 - 6.5 Message protocols, transaction specifications
 - 6.6 Performance
 - 6.7 Metrics
 - 6.8 Testing

Annex A

Requirements List (normative)

A.1 General

Use of this Standard imposes requirements on the implementation that go beyond those of the base standards referred to by this Standard. These result in modifications to the requirements expressed in the base standards. This annex specifies the modifications (the Requirements List - RL) that apply to the status of the items affected in each ICS proforma, with consequently modified requirements on the answers to be provided.

The status notation used in this annex is that defined in ISO/IEC 9646-7. In summary, the meaning of the notations is as follows:

- i Irrelevant or out-of-scope - this capability is outside the scope of this profile and is not subject to conformance testing in this context.
- m Mandatory - the capability is required to be supported.
- n/a Not Applicable - in the given context, it is impossible to use the capability.
- o Optional - the capability may be supported or not.
- o.i qualified optional - for mutually exclusive or selectable options from a set. "i" is an integer that identifies a unique group of related optional items and the logic of their selection, defined below the table.
- x eXcluded or prohibited - there is a requirement not to support this capability in this profile.

The Requirements List in this annex shall be used to restrict the permitted support answers in the corresponding PICS.

A.2 Relationship between RL and corresponding PICS proformas

In the context of the profile specification contained in this Standard, ICS proformas of the base protocol standards contain tables in 3 categories. The 3 categories are:

- Those proforma tables where this profile does not restrict the permitted support answers;
- Those proforma tables where this profile restricts the permitted support answers;
- Those proforma tables that are not relevant to this profile.

The Requirements List consists of the tables falling into the second category, with an indication of the modified items in those tables.

Annex B

Implementation Conformance Statement (normative)

B.1 General

The layout and content of this annex is guided by ISO/IEC 9646-7.

The supplier of a profile implementation that is claimed to conform to this Standard shall complete the Profile specific Implementation Conformance Statement (ICS) proforma contained in this annex.

NOTE

The supplier is also required to complete a copy of the PICS proformas provided in each of the protocol standards referred to by this Standard.

A completed Profile specific ICS proforma is the ICS for the implementation in question. The ICS is a statement of which capabilities and options of the profile have been implemented. The ICS can have a number of uses, including use:

- By the profile implementer, as a check list to reduce the risk of failure to conform to the standard through oversight;
- By the supplier and acquirer (or potential acquirer) of the implementation, as a detailed indication of the capabilities of the implementation, stated relative to the common basis for understanding provided by the standard ICS proforma;
- By the user (or potential user) of the implementation, as a basis for initially checking the possibility of interworking with another implementation (note that, while interworking cannot be guaranteed, failure to interwork can often be predicted from incompatible ICS);
- By a protocol tester, as the basis for selecting appropriate test suites against which to assess the claim for conformance of the implementation.

B.2 Instruction for completing the ICS proforma

B.2.1 General structure of the ICS proforma

The ICS proforma is a fixed format questionnaire divided into subclauses each containing a group of individual items. Each item is identified by an item number, the name of the item (question to be answered), and the reference(s) to either the base standard, or a specific clause in a base standard, or specifying the item in the main body of this Standard (if no base standard is listed in the reference column).

The "Status" column indicates whether an item is applicable and if so whether support is mandatory or optional. The following terms are used:

- | | |
|----------|---|
| m | mandatory (the capability is required for conformance to the profile); |
| o | optional (the capability is not required for conformance to the profile but if the capability is implemented it is required to conform to the profile specification); |
| o.<n> | optional, but support of at least one of the group of options labelled by the same numeral <n> is required; |
| <item>:m | simple-conditional requirement, the capability being mandatory if item number <item> is supported, otherwise not applicable; |
| <item>:o | simple-conditional requirement, the capability being optional if item number <item> is supported, otherwise not applicable; |

- x prohibited;
- c.<cond> conditional requirement, depending on support for the item listed in condition <cond>.

Answers to the questionnaire items are to be provided in the "Support" column, by simply marking an answer to indicate a restricted choice (Yes or No), or in the "Not Applicable" column (N/A).

B.2.2 Additional Information

Items of Additional information allow a supplier to provide further information intended to assist the interpretation of the ICS. It is not intended or expected that a large quantity will be supplied, and an ICS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations.

References to items of Additional information may be entered next to any answer in the questionnaire, and may be included in items of Exception Information.

B.2.3 Exception Information

It may occasionally happen that a supplier will wish to answer an item with mandatory or prohibited status (after any conditions have been applied) in a way that conflicts with the indicated requirements. No pre-printed answer will be found in the Support column for this. Instead, the supplier is required to write into the support column an x.<i> reference to an item of Exception Information, and to provide the appropriate rationale in the Exception item itself.

An implementation for which a Exception item is required in this way does not conform to this Standard. A possible reason for the situation described above is that a defect in the standard has been reported, a correction for which is expected to change the requirement not met by the implementation.