

INCTTS M1/02-0208
Project NCITS 1566 - D

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

Title: 2nd Working Draft - Application Profile - Interoperability and Data Interchange - Biometrics-Based Verification and Identification of Transportation Workers

Source: Project Editor

Date: 09 September 2002

Revision History

Revision	Date	M1 Doc	Comments
1	08/1/2002	020134	First Draft
2	09/9/2002	020208	Added Annexes and additional text

Editor Contact Information:

John Neumann

Email: openstrat@aol.com

Ph: 703 729 4858

Fax: 703 729 0304

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

Purpose

1. Scope
2. Conformance
3. Normative references
4. Definitions
5. Functions
- 5.1 Enrollment process
- 5.2 Submission process

Annex A: Requirements List

Annex B: Biometric Implementation Conformance Statement

Annex C: Biometrics Phasing

Annex D: Performance

Purpose

In the interest of implementing a more secure personal verification system, this ANSI/INCITS Standard establishes a transportation system-wide application profile to meet current and future physical and logical access requirements for all personnel of all modes of responsibility. This ANSI/INCITS Standard is a uniform transportation-wide effort to defend against and/or prevent against unauthorized access through the improvement of identity verification capabilities using biometrics for individuals seeking physical and logical access to secure areas.

1. Scope

This ANSI/INCITS Standard 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.

Identification 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. Verification is the process of confirming that the bearer of the token who has been identified by the token has been previously enrolled and that the token is a valid token. Access control is the process of confirming that the bearer identified by the token has the right to enter the location based on the role or position that the bearer has in the operation within the location being accessed. Access control may consist of, but not limited to, a mechanism for Role Based authentication or employee identification.

Biometric enrollment is the process by which biometric data is collected from a perspective token bearer by means of collection devices such as digital cameras and fingerprint readers. The biometric data is verified within local, regional, and national databases to insure that the applicant enrollee has not previously enrolled using a different identity. Once verified, the biometric data is stored within a token and on local and regional databases for use during identification, verification and access control functions. Different access needs may dictate that multiple forms of biometric data be used during the identification and access control function. As such, all forms of biometric data for use within a token will be collected and stored within the token and the local/regional database.

2. Conformance

A system conforms to this standard if it correctly performs all the mandatory capabilities defined in the requirements list (annex A) and the profile specific Implementation Conformance Statement (ICS) in annex B. Note that more capabilities may be required than in the base standards.

3. Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this standard. All standards are subject to revisions, and parties to agreements based there upon, are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

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

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

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
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)
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
NISTIR 6529-2001 - Common Biometric Exchange File Format (CBEFF),
ANSI/INCITS 359-2002 – Information Technology – Roll Based access Control

4. Definitions

4.1 API (Application Program Interface) – 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.

4.1 Application – 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.

4.3 Application Developer – An individual entrusted with developing and implementing a biometric application.

4.4 Application Profile – 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.

4.5 Authentication – [a term that should not be used] Alternative term for 'Verification'.

4.6 Base Standard – 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.

4.7 Biometric – A measurable, physical characteristic or personal behavioural trait used to recognise the identity, or verify the claimed identity, of an enrollee.

4.8 Biometric Data – 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).

4.9 Biometric Sample – Raw data representing a biometric characteristic of an end-user as captured by a biometric system (for example the image of a fingerprint).

4.10 Biometric System – 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.

4.11 Capture – The method of taking a biometric sample from the end user.

4.12 Certification – 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.

4.13 Comparison – The process of comparing a biometric sample with a previously stored reference template or templates. See also ‘One-To-Many’ and ‘One-To-One’.

4.14 Claimant – A person submitting a biometric sample for verification or identification whilst claiming a legitimate or false identity.

4.15 Closed-Set Identification – When an unidentified end-user is known to be enrolled in the biometric system. Opposite of ‘Open-Set Identification’.

4.16 Database – 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.

4.17 End User – [see User - different] A person who interacts with a biometric system to enrol or have his/her identity checked.

4.18 End User Adaptation – The process of adjustment whereby a participant in a test becomes familiar with what is required and alters their responses accordingly.

4.19 Encryption – 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.

4.20 Enrollee – A person who has a biometric reference template on file.

4.21 Enrolment – The process of collecting biometric samples from a person and the subsequent preparation and storage of biometric reference templates representing that person's identity.

4.22 Extraction – The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.

4.23 False Acceptance – When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity.

4.24 False Acceptance Rate/FAR – 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

4.25 False Match Rate – 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’.

4.26 False Non-Match Rate – 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’.

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

4.28 False Rejection Rate/FRR – 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

4.29 Identifier – 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.

4.30 Identity – 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.

4.31 Identification/Identify – 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’.

4.32 Impostor – 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.

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

4.34 Match/Matching – 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.

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

4.36 One-to-a-Few – 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.

4.37 One-to-Many – Synonym for ‘Identification’.

4.38 One-to-One – Synonym for ‘Verification’.

4.39 Open-Set Identification – Identification, when it is possible that the individual is not enrolled in the biometric system. Opposite of ‘Closed-Set Identification’.

4.40 Out of Set – In open-set identification, when the individual is not enrolled in the biometric system.

4.41 PIN (Personal Identification Number) – A security method whereby a (usually) four digit number is entered by an individual to gain access to a particular system or area.

4.42 Population – The set of end-users for the application.

4.43 Recognition – The preferred term is ‘Identification’.

4.44 Record – The template and other information about the end-user (e.g. access permissions)

4.45 Registration – 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.

4.46 Template/Reference Template – Data, which represents the biometric measurement of an enrollee, used by a biometric system for comparison against subsequently submitted biometric samples.

4.47 Template Ageing – The degree to which biometric data evolves and changes over time, and the process by which templates account for this change.

4.48 Template Size – The amount of computer memory taken up by the biometric data.

4.49 Type I Error – 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’.

4.50 Type II Error – 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’.

4.51 User – 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.

4.52 Validation – The process of demonstrating that the system under consideration meets in all respects the specification of that system.

4.53 Verification/Verify – 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’.

4.54 WSQ (Wavelet Transform/Scalar Quantisation) – A compression algorithm used to reduce the size of reference templates.

5. Functions

A biometric system is an integrated hardware/software entity that:

- Captures a biometric sample from the user
- Extracts biometric data from that sample
- Compares the biometric data with that contained in one or more templates
- Decides how well the data and the template(s) match
- Indicates whether or not an identification or verification has been achieved, after which the information is fed to the access control system to provide or deny access.

Figure 1 illustrates the principal biometric system processes. The enrolment process generates the biometric template that will characterize the user in the system. There are two types of templates commonly in use:

- Reference templates generally are associated with credential (e.g., smart card) issuance systems. The template obtained during the issuance process may be stored both on a smart card and in a central database. Its quality will be sufficient to mitigate the likelihood that it “matches” other templates in the database as a means for prohibiting “alias enrolments.” In the event of a lost credential, the user will need to provide a biometric sample that matches his/her reference template in order to obtain a new credential.
- Operational templates generally are associated with verification of users at access points and are system specific. For example, the access to a laboratory may be controlled by a hand geometry reader while access to laboratory computing systems is controlled by fingerprint readers.

As suggested by the illustrations in Figure 1, the verification process compares the biometric data extracted from the sample with the reference template of a single enrollee whose identity is claimed by the user.

In the example of Figure 1, identity is claimed by entering a PIN. Alternatively, it could be claimed with the swipe of a magnetic card or some other means of data entry. The identification process differs from the verification process in that it compares the user’s biometric data with all templates in the system to determine whether it matches any. The identity of the user is inferred from the identity of the enrollee whose template is matched. Details of these processes are further defined in the following paragraphs.

5.1 Enrolment Process

The process whereby a user’s initial biometric sample or samples are collected, accessed, processed, and stored for use in a biometric system.

- **Biometric Devices**
Part of a biometric system containing a sensor to capture a biometric sample from an individual.
- **Algorithm**
A sequence of instructions that tell a biometric system how to solve a particular problem. An algorithm will have a finite number of steps and is typically used by the biometric engine (i.e., the biometric system software) to compute whether a biometric sample and template are a match.
 - **Biometric Sample**
Raw data which represents the biometric characteristics of an end-user captured by a biometric device.

- *Biometric Data*
The information extracted from the biometric sample used to build a template or to compare against a previously created template.
- *Template*
Data which represents the biometric measurement of an enrollee. Used by a biometric system for comparison against submitted biometric samples.
- **Database**
Any storage of biometric templates and related end user information. (Even if only one biometric template or record is stored). Examples include smart card local access control system and centralized database

5.2 Submission Process

- **Comparison**
The process of comparing a biometric sample with a previously stored template or templates. There are two similar but distinct functions:
 - *Verification (1:1)*
The process of comparing a submitted biometric sample against the previously captured biometric template of a single enrollee whose identity is being claimed, to determine whether it matches the enrollee's template.
 - *Identification (1:N)*
The one-to-many process of comparing a submitted biometric sample against all of the biometric templates on file to determine whether it matches any of the templates and, if so, the identity of the enrollee whose template was matched.

While biometric technologies are not fool proof, they can be viewed as a tool to increase security. Error rates and population sizes are major factors affecting the choice of a 1:1 or 1:N implementation.

With a traditional credential based system, the ID number on the credential is compared to a valid list of IDs stored in the access control panel. A lost or stolen credential presents a security risk and we can assume the probability of a lost or stolen card granting access when used by an unauthorized user is 100%. (Unless the system also requires a PIN.)

When a biometric is added, the probability that the request for access will be incorrectly accepted is equal to the probability that the credential or ID number is active (assumed to be 100%) multiplied by the biometrics False Accept Rate (FAR). The FAR is the probability that the unauthorized user's biometric sample would match the stored template of the credential owner.

In a 1:1 comparison the expected result of an unauthorized user being incorrectly granted access is calculated as the probability of an active ID multiplied by the FAR multiplied by the number of comparisons. The performance of a biometric using a one-to-one comparison is independent of the size of the enrolled population, because only one comparison is made.

In a 1:N implementation we can ignore the probability that the credential ID is still active, because there are no credentials. By that, we refer to a system whereby the operational biometric—say, facial recognition—asks the data base to compare the user with the entire data base every time he seeks entry., rather than by first identifying himself, as with a card or PIN, so that the system only needs to retrieve and compare a single set of data. The expected result of an unauthorized user being incorrectly granted access is calculated as the FAR multiplied by the number of comparisons.

Biometric System

Consider the following general biometric system:

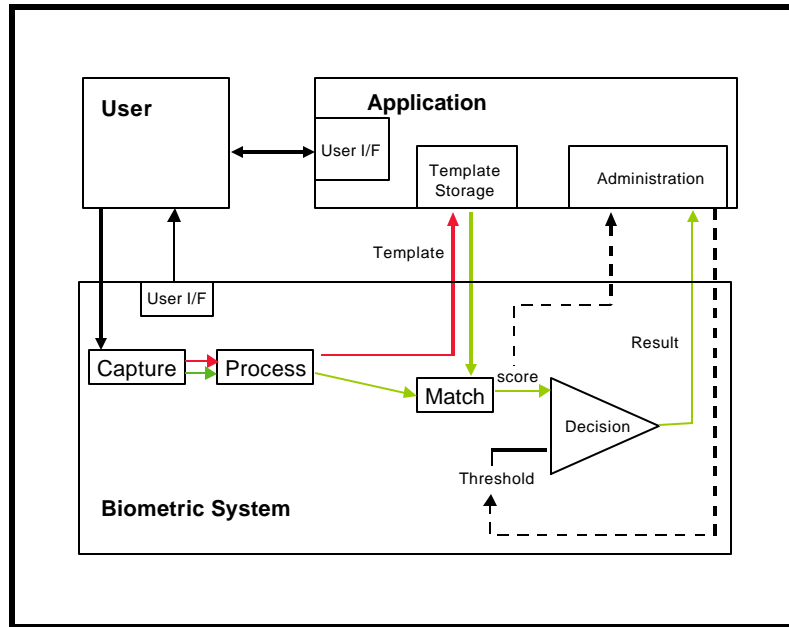


Figure 2. General Biometric System

The basic components of the general biometric system are:

- Capture
Capture of a raw biometric sample.
- Process
Conversion of the raw sample into a set of features or image sections (this component is also sometimes known as Extract).
- Create Template
Creation of the biometric template. This step may include conformance with a standard such as CBEFF [4] and/or addition of User Credentials as “payload” [1].
- Match
Matching (verify or identify) of the candidate (live) sample with a reference template
- Decision
Comparison of the score output from Match with a pre-defined threshold.

Note that Capture, Process and Create Template may be compiled by the biometric system developer into a convenience function known as *Enroll*, and that Capture, Process, Match, and Decision may be correspondingly compiled into a convenience function, *verify* (or *identify*). The templates may be stored on the biometric device, or they may be stored by the security system, as shown above.

Relationship between Biometric System and Application

The purpose of this section is twofold:

1. To distinguish between the enrollment of an individual and the registration of the user (within the application)
2. To describe the relationship between verification and authorization.

The role that biometric systems play within a general application or security system is to provide evidence (referred to as “verification”) that an individual is who they claim to be; or to establish that they represent a unique identity (referred to as “identification”).

In this section, we distinguish between the individual's *identity*; an *identifier* (see [5]) by which they are known to an application; and the *verification* process that verifies that they are the valid owner of the identifier.

As an example, consider the various steps comprising the *registration* of a new user within an application (for example, an operating system, or a passport issuance process).

- An administrator of the application will establish the unique *identity* of the individual. This is typically achieved through the use of so-called “breeder documents” such as birth certificate, passport etc.

This step may also include a search over a biometric database to establish the uniqueness of the individual's claim according to the range of that database. This is accomplished through the use of *biometric identification*.

- If the individual is identified as unique, the security system will establish the individual as a new *user* of the system, and assign a unique *identifier* by which they are known to the system. An example of an identifier would be a passport number.
- The individual will be instructed to *enroll* their biometric and the biometric system will create a biometric *template* that is associated with the user.
- The template will be *bound* to the identifier, either by physically storing them in related locations in the biometric or application, or by binding them together using encryption (see figure 2 below) or a digital signature mechanism, to create a *user record*.

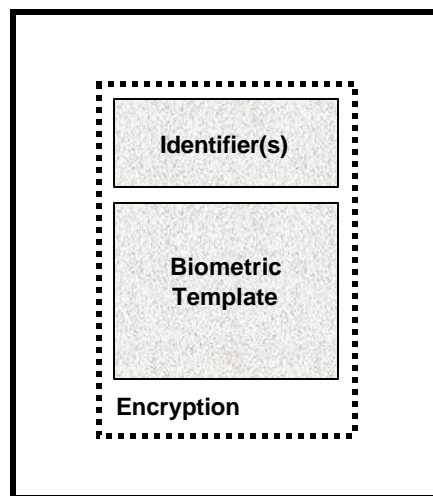


Figure 3. Example of a User Record

Subsequently, when the individual requests to use a service or initiate a transaction, the following steps are undertaken:

- An individual establishes a *claim* to the application that they are a valid user of the system. This is usually achieved either by inputting the username associated with the user, or by presenting a card or other credential (such as a USB token, or passport) to the system to make the claim.

- The application ensures that the user record of the claimed user is available to the biometric system (either by transmitting it to the biometric system, or by selecting it within the biometric system), where it will be *unbound* to produce the template and identifier. Note that as part of this step, either the application or the biometric system (or both) may verify the authenticity of the user record, by, for example, checking a digital signature.
- The individual is requested to *verify (biometric verification)* that they are the valid owner of the user record, by comparing a live biometric sample with that represented by the template in the user record.
- If a successful match occurs, the identifier that was stored in the user record is relayed to the application (see figure 3 below) where the user is *authorized*, according to their application rights and privileges, to complete the service or transaction.

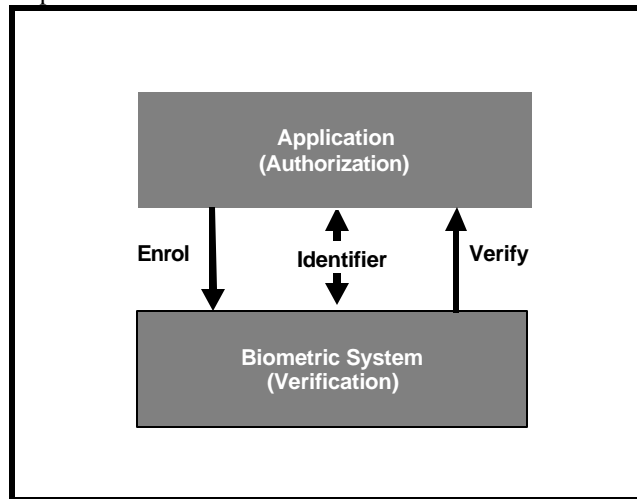


Figure 4. The interaction of identifier between user verification and application authorization.

This separation between the verification of the individual and authorization of the user within the application is key for successful integration of biometric systems into general applications. It provides an explicit segregation between the verification process in the biometric system and the rights and privileges that the user is assigned by the application. This is especially important when considering issues such as the revocation of a user's rights and privileges, and the fact that any individual may appear as multiple users to the application (for example, as a normal user and as an administrator). The use of encryption or similar binding mechanism also mitigates the potential of an identity theft.

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.

A.3 Requirement List

A.3.1 Tables for Biometrics Templates

A.3.1.1 Finger Minutia Format

Item	Question/Feature	Reference	Template Status	Profile Status

A.3.1.2 Face Recognition Format

Item	Question/Feature	Reference	Template Status	Profile Status

A.3.1.3 Finger Pattern-based Format

Item	Question/Feature	Reference	Template Status	Profile Status

A.3.1.4 Iris Recognition Format

Item	Question/Feature	Reference	Template Status	Profile Status

A.3.1.5 Finger Image Format

Item	Question/Feature	Reference	Template Status	Profile Status

A.3.2 Tables for BioAPI Specification

Item	Question/Feature	Reference	BioAPI Status	Profile Status

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.

Annex C

Biometrics Phasing (informative)

A key element of integrating biometrics with an access control system is the means of transporting a reference template to the biometric reader. This data transport mechanism generally falls within three categories:

1. Smart Cards – Reference templates are encoded to smart cards and are hand-carried to the biometric device by the associated employee. While this approach offers a relatively low level of complexity, there are certain interoperability issues that should be addressed:
2. Dedicated Biometric Networks – Dedicated biometric data networks can be utilized for transmitting reference templates to the biometric devices. Such networks should be based on industry-standard cabling and network topologies. In the event that multiple biometric technologies are implemented, efforts should be made to allow a common network to serve all such devices.
3. Access Control System Network/Panels – Reference templates can be transmitted to the biometric devices by way of the access control system network and field panels. While this approach offers a number of advantages, there are several interoperability issues that should be addressed:
 - Data Storage at Head-End – In order to accomplish an open architecture solution, systems should support the storage of reference templates using industry-standard database formats.
 - Data Storage at RAC Panels – As with the data storage at the head-end, data storage at the panels should be based upon industry-standard database formats. This precludes proprietary relationships between access control system and biometric suppliers and allows biometrics and/or access control system equipment to be upgraded or replaced in the future without mutual impact.
 - Data Transmission – Data transmissions between RAC panels and biometric devices should be based upon industry-standard cabling and protocols, appropriate to the level of communications required.

The following is a discussion of implementing biometrics with existing access control systems. Using the three transport mechanisms identified above, there are four basic approaches identified for integrating biometrics with existing access control systems. While there may be variations on these four approaches, it is felt that they represent the four basic models that are currently available to transportation operators wishing to integrate biometrics with existing access control systems.

While some of the approaches identified include the use of smart cards, biometrics can be implemented without the use of such cards.

C.1 Approach 1 – Reference Template Transport Through Smartcards

The approach shown in Figure A-1 relies upon the physical transport of the biometric “reference template” to a biometric reader via an employee’s smart card (i.e., “sneaker net”). The smart card also contains an encoded card number that is derived from the airport’s access control system. The biometric reader compares the reference template to the biometric data presented by the card holder. If the card holder is authenticated, the biometric reader emulates a typical Weigand-output card reader and sends the encoded card number to the access control system RAC panel for access verification. Due to the minimal data to be transported (i.e., card holder number) such data can be transmitted over standard/existing card reader data cables.

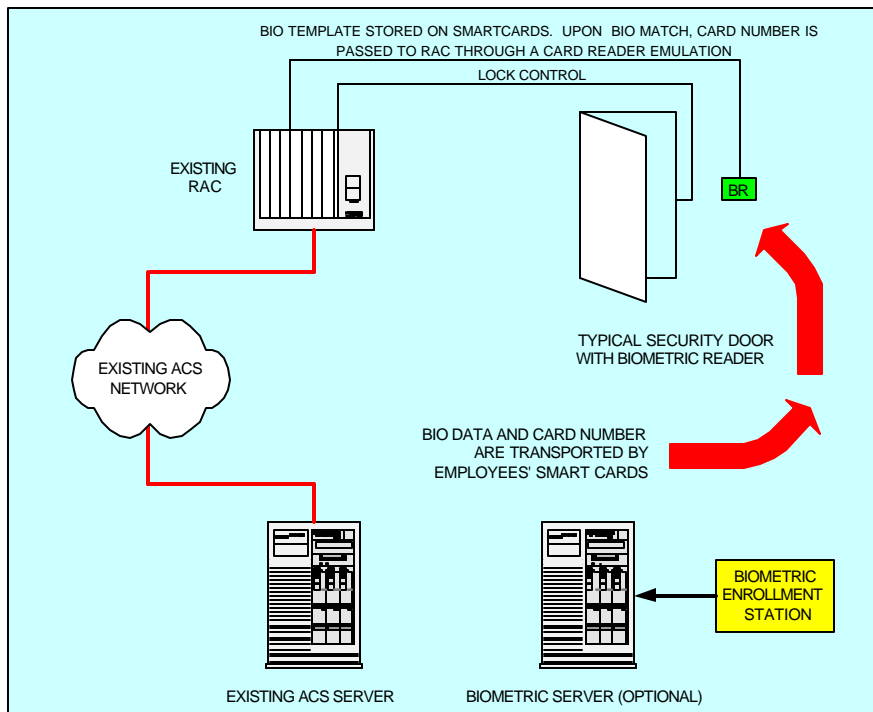


Figure C.1: Reference Template Transport Through Smart cards

APPROACH 1	
ADVANTAGES	DISADVANTAGES
<ul style="list-style-type: none"> Easily integrated with legacy access control systems (i.e., biometrics device simply emulates existing card readers). 	<ul style="list-style-type: none"> Sophisticated adversaries may be able to duplicate cards with their own biometric reference template (level of security can be greatly enhanced if data encryption scheme is utilized).
<ul style="list-style-type: none"> No biometrics infrastructure costs (e.g., network connections, etc.). 	<ul style="list-style-type: none"> Basic interface between biometric devices and ACS (i.e., card holder number is only transmitted if authentication of the biometric data is accomplished) potentially limits the ability to identify the unauthorized use of cards. Biometric-specific error messaging would not be supported.
<ul style="list-style-type: none"> Existing ACS hardware and software remains unchanged. 	<ul style="list-style-type: none"> Requires maintenance of separate, stand-alone biometrics database (depending on whether the Airport elects to maintain a centralized biometric database as a back-up to those records stored on the smartcards).
<ul style="list-style-type: none"> Costs limited to biometric readers, biometric enrolment station, and dual technology card upgrade. 	<ul style="list-style-type: none"> Access media may need to be replaced with dual-technology cards (e.g., smart card and proximity, smart card and magnetic stripe, etc.) to support both the smart card function and the existing access readers.
<ul style="list-style-type: none"> Supports wide range of biometric technologies and allow multiple technologies to be used at a given site. 	
<ul style="list-style-type: none"> Access authorization remains under the control of the existing ACS administrator. 	
<ul style="list-style-type: none"> ACS can be upgraded with little/no impact on biometric systems 	
<ul style="list-style-type: none"> Employee privacy concerns regarding biometric data can be alleviated if reference templates are stored only on the smart cards – no centralized database. Biometric data is kept within the employees' possession. 	
<ul style="list-style-type: none"> Solution supports only a “verification” process (1:1) which is preferred over an “identification” process (1:n) 	

C.2 Approach 2 – Reference Template Transport Through Dedicated Biometrics Network (with ACS Interface)

Under this approach, reference data can be transported to local biometric devices via a dedicated biometric data network. As in Approach 1, once an individual’s identity is authenticated by the biometric device, it then emulates a card reader and transmits a cardholder number (obtained via biometric network) to the access control system for access validation. There are two basic ways of communicating templates/card numbers to the biometric devices: 1) the data can be transmitted to a given biometric device where it can be stored locally (i.e., all templates/card numbers authorized access to a given door can be stored locally at that door’s biometric device), or 2) templates can remain on a biometric server and can be requested by the appropriate biometric device upon each access attempt. In either event, the biometric device should be equipped with a pinpad, card reader, or similar device to identify the biometric reference template to be used for comparison, i.e., “verification” (1:1) process as opposed to an “identification” (1:n) process.

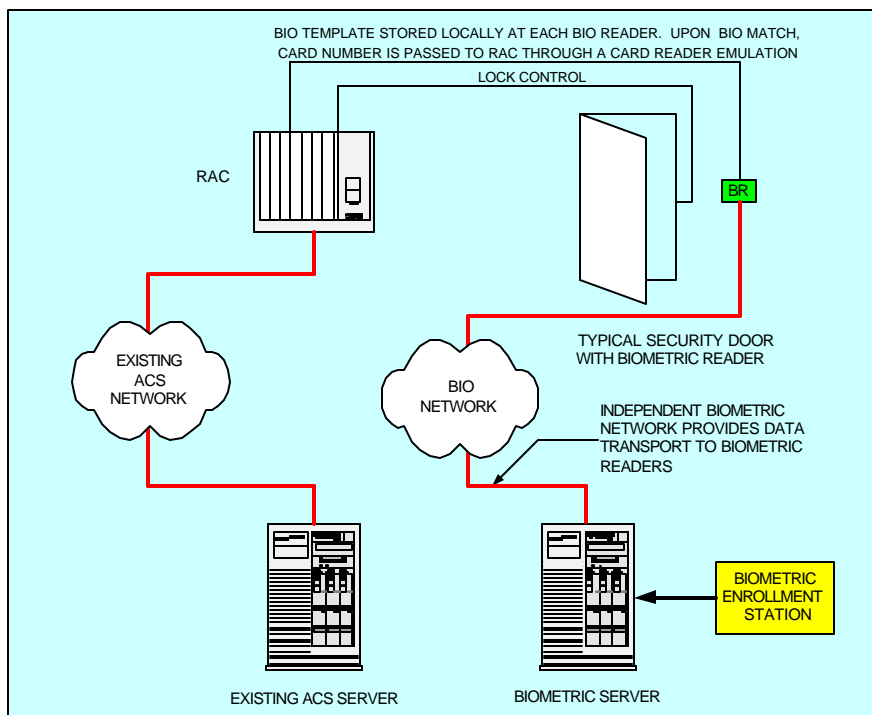


Figure C.2: Reference Template Transport Through Dedicated Biometrics Network (with ACS Interface)

APPROACH 2	
ADVANTAGES	DISADVANTAGES
<ul style="list-style-type: none"> Easily integrated with legacy access control systems (i.e., biometrics device simply emulates existing card readers). 	<ul style="list-style-type: none"> Additional costs associated with establishing dedicated biometric data network.
<ul style="list-style-type: none"> Existing ACS hardware and software remains unchanged. 	<ul style="list-style-type: none"> Basic interface between biometric devices and ACS (i.e., card holder number is only transmitted if authentication of the biometric data is accomplished) potentially limits the ability to identify the unauthorized use of cards. Biometric-specific error messaging would not be supported.
<ul style="list-style-type: none"> Access authorization remains under the control of the existing ACS administrator. 	<ul style="list-style-type: none"> Requires maintenance of separate, stand-alone biometrics database.
<ul style="list-style-type: none"> ACS can be upgraded with little/no impact on biometric systems. 	<ul style="list-style-type: none"> Changes in biometric technologies may have an impact on the biometric network.
<ul style="list-style-type: none"> Requires no change to existing access media. 	<ul style="list-style-type: none"> Use of multiple biometric technologies may require multiple data networks.
<ul style="list-style-type: none"> Biometrics data remains under the direct control of system administrator (i.e., not encoded in transportable smart cards). 	<ul style="list-style-type: none"> There may be additional costs associated with providing the local memory needed to store biometric templates/card numbers at each biometric device.
<ul style="list-style-type: none"> Supports both “identification” (1:1) and “verification” (1:n) processes. (1:1 is preferred.) 	<ul style="list-style-type: none"> Potential time delays associated with requesting/transmitting reference templates from the server to a biometric device for each access request.
	<ul style="list-style-type: none"> Storage of biometric reference templates may cause privacy concerns with employees.

C.3 Approach 3 – Reference Template Transport Through Dedicated Biometrics Network (with No ACS Interface)

This approach is somewhat similar to Approach 2 with one important difference: there is no access control system interface. Under this approach, the biometric system assumes sole responsibility for validating/controlling access. This essentially establishes a stand-alone access control system for those doors equipped with biometric devices. Acting as its own access control system, the biometric system would require its own independent command and control elements and would require its own administration of access privileges and alarm monitoring. Due to the duplication of access control/alarm monitoring functions and facilities, this approach is envisioned to represent the least likely scenario for implementing biometrics along with an existing access control system.

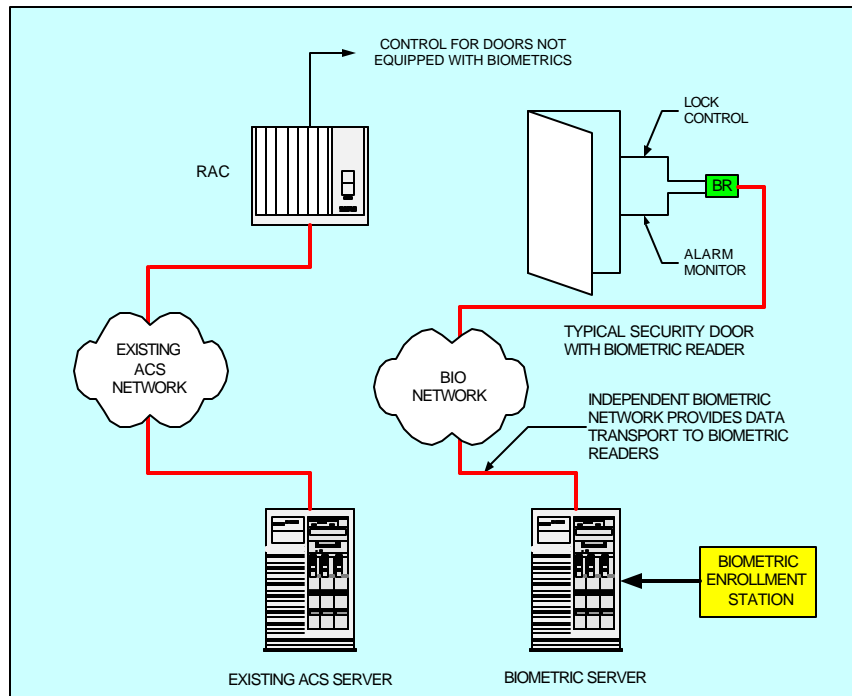


Figure C.3: Reference Template Transport Through Dedicated Biometrics Network (with No ACS Interface)

APPROACH 3	
ADVANTAGES	DISADVANTAGES
<ul style="list-style-type: none"> • Completely independent of legacy access control systems and therefore has minimal impact on existing access control systems. 	<ul style="list-style-type: none"> • Additional costs associated with establishing dedicated biometric data network.
<ul style="list-style-type: none"> • Existing ACS hardware and software remains unchanged. 	<ul style="list-style-type: none"> • Two independent systems required to maintain the access control function.
<ul style="list-style-type: none"> • Access authorization remains under the control of the existing ACS administrator (assuming ACS administrator also administers biometric system). 	<ul style="list-style-type: none"> • Requires two separate monitoring and control systems.
<ul style="list-style-type: none"> • ACS can be upgraded with no impact on biometric systems. 	<ul style="list-style-type: none"> • Requires maintenance of separate, stand-alone biometrics database.
<ul style="list-style-type: none"> • Requires no change to existing access media. 	<ul style="list-style-type: none"> • Changes to biometric technologies may have an impact on the biometric network.
<ul style="list-style-type: none"> • Biometrics data remains under the direct control of system administrator. 	<ul style="list-style-type: none"> • Use of multiple biometric technologies may require multiple data networks.
<ul style="list-style-type: none"> • Because system has direct control over the access function at designated doors, it should provide a complete accounting of access activities/biometric-specific messaging. 	<ul style="list-style-type: none"> • There may be additional costs associated with providing the local memory needed to store biometric templates/card numbers at each biometric device.
<ul style="list-style-type: none"> ○ Supports both “identification” (1:1) and “verification” (1:n) processes. (1:1 is preferred.) 	<ul style="list-style-type: none"> • Potential time delays associated with requesting/transmitting reference templates to a biometric device for each access request.
	<ul style="list-style-type: none"> • Storage of biometric reference templates may cause privacy concerns with employees.

C.4 Approach 4 – Reference Template Transport Though ACS Network

The approach shown in Figure A-4 includes a fully integrated biometric and access control system. Under this approach, the existing access control system infrastructure is utilized to transport reference templates to the individual biometric devices. Templates may either be stored at the RAC or at the individual biometric devices. Under this scenario, the biometric devices would communicate with the access control system through a direct interface (as opposed to a card reader emulation) thereby allowing maximum efficiencies and operability. By combining all access elements (card readers, biometrics, alarm monitoring equipment, etc.) into an integrated system, costs are minimized and there is a minimum administrative burden. While this approach offers theoretical advantages over the others described above, at the writing of this document there are still numerous obstacles to overcome. Currently, there are no universally accepted standards for reference templates/database formats and APIs for such integration. Consequently, there are no open architecture solutions currently available. The current state of the industry offers only proprietary relationships between access control system and biometric manufacturers. These relationships include customized RAC panels and database structures to support a given biometrics partner. Due to these proprietary relationships, airports currently have limited choices in selecting biometric technologies that might be compatible with their existing access control system (and will likely require that RAC panels be replaced/upgraded). In addition, future changes in biometric technologies may not be compatible with the existing access control system.

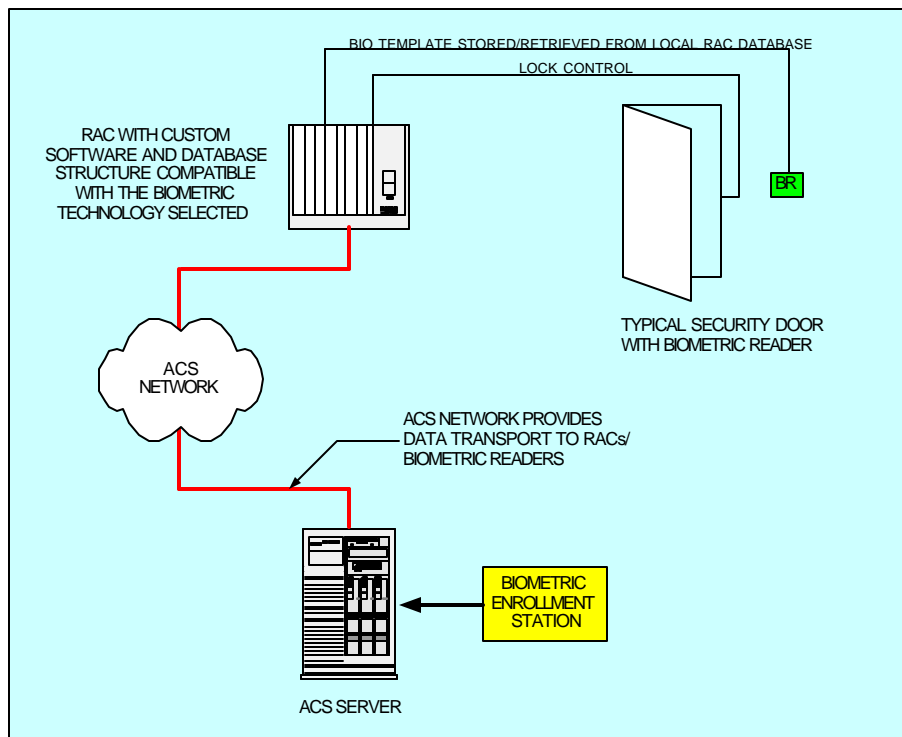


Figure C.4: Reference Template Transport Through ACS Network

APPROACH 4	
ADVANTAGES	DISADVANTAGES
<ul style="list-style-type: none"> • Single access control system allows integrated monitoring, control and administration. 	<ul style="list-style-type: none"> • Future changes in biometric technologies and/or manufacturers may not be compatible with current ACS..
<ul style="list-style-type: none"> • Biometrics data remains under the direct control of system administrator. 	<ul style="list-style-type: none"> • Future changes in ACS systems and/or manufacturers may not be compatible with current biometrics.
<ul style="list-style-type: none"> • Because access control system has direct control over the access function at designated doors, it should provide a complete accounting of access activities, to include biometric-specific error messaging. 	<ul style="list-style-type: none"> • May require higher speed cables between biometric devices and RAC panels to support data communications.
<ul style="list-style-type: none"> • The ability to utilize the ACS data network eliminates the need for a separate biometrics network. 	<ul style="list-style-type: none"> • Initial implementation may require replacement/upgrades to existing RAC panels.
<ul style="list-style-type: none"> • Distributed processing functions of RACs can be utilized to maintain access functions and store historical transactions if communications with host server are disrupted. 	<ul style="list-style-type: none"> • Storage of biometric reference templates may cause privacy concerns with employees.
<ul style="list-style-type: none"> • Supports both “identification” (1:1) and “verification” (1:n) processes. (1:1 is preferred.) 	

Annex D

Performance (informative)

Table D.1 lists common biometric system performance metrics and provides guidance regarding performance requirements appropriate to access control systems for the transportation environment. Biometric system performance is dependent upon the technology and product used, the application, the environment, and the user population, including their familiarity with system operation.

The guidance offered below characterizes performance available today in laboratory and office environments. Biometrics is an evolving discipline and performance characteristics do not yet have the maturity of conventional id mechanisms and performance levels expectations need to be adjusted accordingly. Also there is a substantial variation in cost among biometric devices available for access control.

Table D.1 – Performance Metrics

Performance Metric	Guidance
Accuracy:	
<ul style="list-style-type: none">False Acceptance Rate (FAR): the probability that the system will accept an impostor (i.e., someone not enrolled in the system)	1.5%
<ul style="list-style-type: none">False Rejection Rate (FRR): the probability that the system will fail to accept an enrollee	1.5%
<ul style="list-style-type: none">Failure to Enroll (FTE): The probability that an individual will not be able to provide a template and confirming biometric data during the enrollment process of sufficient quality to support participation in system operation.	1.00%
Transaction Time: The time interval required for a biometric system user to gain access through a portal	1-1.5 seconds
Throughput Rate: The combined number of users a biometric system can process within a specified time interval	100 per minute