The ANSI/NIST-ITL standard update for 2011 (data format for the interchange of fingerprint, facial and other biometric information)

Bradford J. Wing

Information Technology Laboratory,
National Institute of Standards and Technology (NIST),
100 Bureau Drive, Mail Stop 8940,
Gaithersburg, Maryland, USA
E-mail: brad.wing@nist.gov

Abstract: This article describes the ANSI/NIST-ITL standard: its origin, contents, and how it is used and updated. It is the principal standard used for the formatting and encoding of biometric data and related textual information for law enforcement, homeland security, and military applications throughout the world. The first version of the standard appeared in 1986, and it has been updated several times since then. The most recent update was a major revision, with final publication in November 2011. This version is titled ANSI/NIST-ITL 1-2011, NIST Special Publication 500-290.

Keywords: biometrics; ANSI/NIST-ITL; biometric standards; fingerprint; iris; DNA; plantar; palmprint; latent prints; facial; scars; tattoos; friction ridge; information assurance; extended feature set; EFS; forensics.

Reference to this paper should be made as follows: Wing, B.J. (xxxx) ‘The ANSI/NIST-ITL standard update for 2011 (data format for the interchange of fingerprint, facial and other biometric information)’, *Int. J. Biometrics*, Vol. X, No. Y, pp.000–000.

Biographical notes: Brad Wing is the Biometrics Standards Coordinator at NIST. He is the editor of the ANSI/NIST-ITL standard and participates actively in several other standards organisations, such as ISO, INCITS and OASIS. He has over 20 years experience in the field of biometrics, having worked previously at the US Department of Homeland Security as Biometrics Coordinator, and he also served as Co-Chair of the Subcommittee on Biometrics and Identity Management of the White House Office of Science and Technology Policy.

1 Introduction

The American National Standards Institute/National Institute of Standards and Technology – Information Technology Laboratory (ANSI/NIST-ITL) standard defines the content, format and units of measurement for the exchange of biometric and forensic information that may be used in the process of either identification of an individual person (subject) or verification of the identity of that person.

It is vitally important that information associated with the biometric data be transmitted to the receiving organisation. This ensures that there is no confusion on the meaning of the data. The type of information that is needed varies by biometric modality. The biometric modalities currently included in the standard are: fingerprint, palm print, plantar (foot and toe prints), DNA, facial, and iris images. In addition, images of other body parts (such as arms), scars, needle marks, and tattoos, and audio/video clips that may be beneficial in establishing or verifying identity may be included in an ANSI/NIST-ITL conformant transaction.

Specialised forensic analysis results can be included in a transaction (such as latent fingerprint image mark-ups, and facial image mark-ups). General information concerning the subject is included in user-defined data fields.

In addition, original source data such as video recordings, and associated information such as photographs of the crime scene where the biometric sample was collected, are now included in the standard, along with geographic location and other related metadata. Information assurance capabilities and data handling records have been added to ensure data integrity.

2 History of the standard

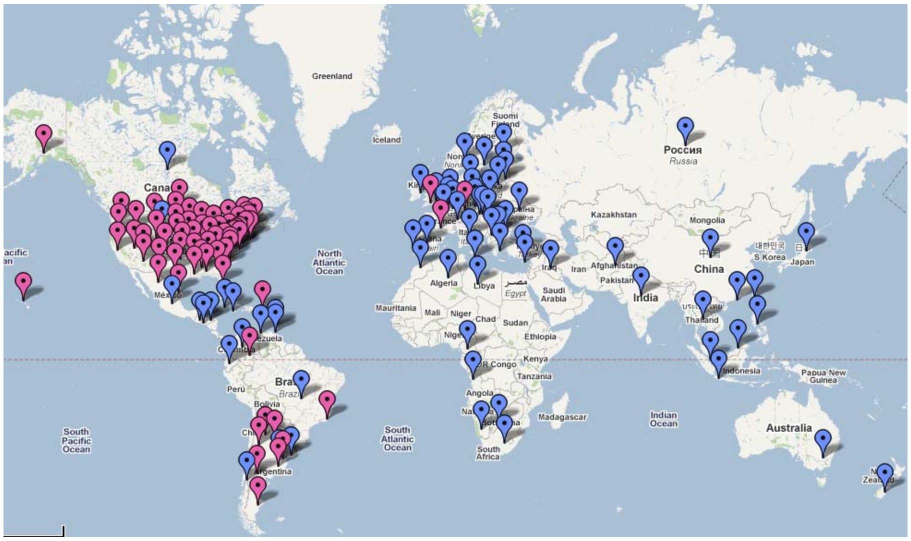
In 1986, the United States National Bureau of Standards (now the National Institute of Standards and Technology – NIST) published the first version of the standard that was to eventually become the “Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information”. The standard’s original purpose was to facilitate state and local electronic fingerprint submissions to the Federal Bureau of Investigation (FBI) in the USA. In 1986, the standard focused solely upon the exchange of fingerprint minutiae, and was designed to require a minimum of memory for exchange and storage of fingerprint information.

Over time, more law enforcement organisations started to use the standard and requested that other types of data and extended capabilities be incorporated into the standard. Electronic memory became less expensive and better biometric sample capture equipment, matching algorithms, and automated data quality analyses became available. Biometric modalities beyond fingerprint became viable for law enforcement use. As a result of all of these factors, the standard evolved through several versions, with the latest being approved and published in 2011.

The standard is now used by law enforcement, homeland security, military and other governmental organisations around the world. Figure 1 shows locations where NIST is aware that the standard is being used by government organisations, such as the Royal Canadian Mounted Police, the Government of Argentina, the German Bundeskriminalamt, the European Union Visa Information System, INTERPOL, and many others.

The ANSI/NIST-ITL standard is designed to facilitate interoperability for biometric and biometric-related forensic data among law enforcement-related organisations. Data may be in original and/or processed versions. Original data may be images, DNA electropherograms, video sequences, or other formats. In order to facilitate transmission and / or storage, such original data may be compressed or selected portions may be used (such as a few frames from a video sequence).

Figure 1 Systems using the ANSI/NIST-ITL standard (known to NIST) (see online version for colours)



Notes: Blue: National System;
Red: State/Provincial/Local System

The ANSI/NIST-ITL standard specifically states which types of compression and data selection are allowed for certain modalities in order to maintain data integrity. An example is that wavelet scalar quantisation (WSQ) is required for friction ridge images (fingerprint, palmprint or plantar print) stored at 19.69 pixels per millimetre (ppmm), which equates to 500 pixels per inch (ppi).

Information associated with a biometric sample such as the coordinates in an image that define the latent print, the type of impression (such as latent palm tracing or latent photo), image capture date, and other pertinent information are defined within the standard.

The latest version of the standard (ANSI/NIST-ITL 1-2011) is content-based and allows for multiple encodings (transaction formats). At present, two encodings have been fully specified: Traditional (binary) and eXtensible Markup Language (XML). The XML is in accordance with the specifications and naming conventions of the National Information Exchange Model (NIEM). Other encodings are possible, but users must fully specify them to the same level as the encodings specified in the standard itself. There must be interoperability across all encodings of the standard.

NIST maintains a website (http://www.nist.gov/itl/iad/ig/ansi_standard.cfm) where ANSI/NIST-ITL 1-2011 and prior versions of the standard are available at no cost. That webpage also lists information relevant to the standard.

Future additions to the standard may include:

- dental records and traumatic injury images/bite marks
- voice recognition
- conformance testing assertions and requirements specifications.

Committees now exist that are working on these areas. These committees are open to participation by any interested party.

3 Data interchange structure

An ANSI/NIST-ITL conformant transaction consists of records. See *Table 1* for a list of the record types in the standard.

Table 1 Record types in the ANSI/NIST-ITL standard

Record identifier	*Record contents*
1	Transaction information
2	User-defined descriptive text
3	Low-resolution greyscale fingerprint image (deprecated)
4	High-resolution greyscale fingerprint image
5	Low-resolution binary fingerprint image (deprecated)
6	High-resolution binary fingerprint image (deprecated)
7	User-defined image
8	Signature image
9	Minutiae data
10	Face, other body part, scar, mark tattoo (SMT) image
11	Voice data (future addition to the standard)
12	Dental record data (future addition to the standard)
13	Variable-resolution latent friction ridge image
14	Variable-resolution fingerprint image
15	Variable-resolution palmprint image
16	User-defined variable-resolution testing image
17	Iris image
18	DNA data
19	Variable-resolution plantar image
20	Source representation
21	Associated context
22–97	Reserved for future use
98	Information assurance
99	CBEFF biometric data record

Note: The data in Type 99 is exchanged in a format that conforms to INCITS 398-2005, the Common Biometric Exchange Formats Framework (CBEFF)

There is a minimum of two records in a transaction and a maximum of 1,000 records per transaction. Each transaction must include a record that describes the general content of the transaction (record type-1) and at least one other record type.

There may be multiple instances of a record type (except for record type-1) within a transaction. For example, there may be several facial images of a person. Each image would be in a separate record type-10, since the image has specific information associated with it that must not be confused with another image.

The information in a transaction consists of a variety of mandatory and optional items. This information is primarily intended for interchange among law enforcement administrations or organisations that rely upon automated identification systems or use other biometric and image data for identification purposes.

4 How the standard is used

Typically, a group of agencies or organisations agree to use pre-assigned data fields with specific meanings (typically in record type-2) for exchanging information unique to their installations by establishing an application profile (implementation domain). An application profile may also contain additional conditions, such as specifying certain data that are listed as optional in the standard be mandatory for this domain or for particular types of transactions.

Within the standard, the principal application profile for a transaction is called the implementation domain. A transaction may be conformant to multiple application profiles.

Examples of application profiles are:

- North American Domain (NORAM) used by the US FBI, Royal Canadian Mounted Police, and several state, provincial and Federal agencies of the USA and Canada
- INTERPOL (called INT-I) used by nations to transmit information to INTERPOL
- other regional profiles (such as for the European Union Visa Information System)
- national profiles (such as for Germany, Afghanistan, Argentina, and other nations)
- state/provincial profiles (such as for Florida and Texas).

Information that is exchanged between parties that accept ANSI/NIST-ITL standard-based input is checked for conformance to the standard prior to acceptance of the transaction as input. The level of conformance checking is determined by the organisation(s).

Some parties, such as a local police department may initiate a transaction and send it to a state/provincial authority. That authority may then add information to the original transaction and send it to a national organisation (such as the FBI). The 2011 version of the standard allows for exact logging of when, why, and how transactions have been modified before reaching the final recipient.

5 Transaction content

As mentioned in ‘data interchange structure’ above, a transaction is comprised of records relating to a single person. Each record is comprised of fields. A field may contain a single value, or contain subfields. The subfields in a field must all have identical structure, which is comprised of ‘information items.’ Subfields can be repeating groups and the number of times that a subfield may be entered is specified by the standard.

The data entered in a field or information item are clearly defined as to their type (alphabetic, alphanumeric, numeric, hexadecimal, binary, or base-64). Additionally, if ‘special characters’ such as periods are allowed in the data, the standard specifies which special characters are allowed. The standard also states other data restrictions, such as a minimum number and maximum number of characters, and value ranges (such as positive integer less than 100) for a particular datum.

Some fields and information items are mandatory; others are optional. Yet others appear only if a different field or an information item in another field has a particular value. In some cases, a field can only appear if the biometric data, source representation or associated data is of a particular type, such as a video recording. As an example, descriptive information about video recordings would have no meaning for a still photographic image. These data dependencies are described in the standard for each field and information item, where applicable.

6 Backward compatibility

Backward compatibility is important, since organisations adhering to an earlier version of the standard may create transactions according to that version, and such transactions may still be received by organisations that have updated to conform to a newer version of the standard.

Due to historical reasons, and to maintain backward compatibility, record type-1 can only use those 128 characters that are present in the 7-bit American Standard Code for Information Exchange (ASCII). Other record types can accommodate the character sets in Unicode Transformation Format 8 (UTF-8) for text fields. This allows the user to enter descriptions and comments in languages that have characters different from or additional to those used in English.

The fields and format of type-4 (fingerprint images) and type-8 (signature) records cannot change between versions of the standard due to restrictions in the Traditional encoding format (in traditional encoding, they are ‘binary’ data with a fixed structure). Since the time when these record types were defined, users have needed more flexibility in defining the metadata associated with the fingerprint image data. Thus, type-14 was developed to replace type-4 fingerprint image records. However, since several systems use Type-4 to transmit fingerprint images, that record type is retained in the standard.

Record types 9 through 99 may be updated, expanded or introduced with new versions of the standard. New fields in existing records may be added, as well as new data record types. If it is determined that a record type, field, subfield, information item or value is not used or needed, it may be declared ‘deprecated.’ In this version of the standard, the deprecated record type, field, or information item is not included in the description. ‘Deprecated’ in this standard means that ‘it shall not be used if claiming conformance to this version of the standard’. Note that record types 3, 5 and 6 are deprecated. These record types were originally designed for the exchange of fingerprint data, but have not been used since the early 1990s.

There are also certain items that are noted in the standard as being discouraged for use in new applications, but that have not yet been agreed upon by the canvassees to be deprecated.

There is a special category called ‘legacy’ for a record type, field, subfield, information item or value that was valid in previous versions of the standard, but shall not be used for new data. ‘Legacy’ indicates that if there is existing data using this record type, field, information item or value it may still be transmitted in a transaction that claims conformance to this version of the standard.

When a data definition is introduced that causes potential problems with backward compatibility, it is noted in the standard. For example, NIEM-conformant XML encoding has inherent backward compatibility issues due to the need to develop new schemas.

7 Update process

The ANSI/NIST-ITL standard is developed according to processes and procedures approved by the ANSI, which provides the only recognised system in the USA for establishing standards (no matter what their origin) as American National Standards (ANS).

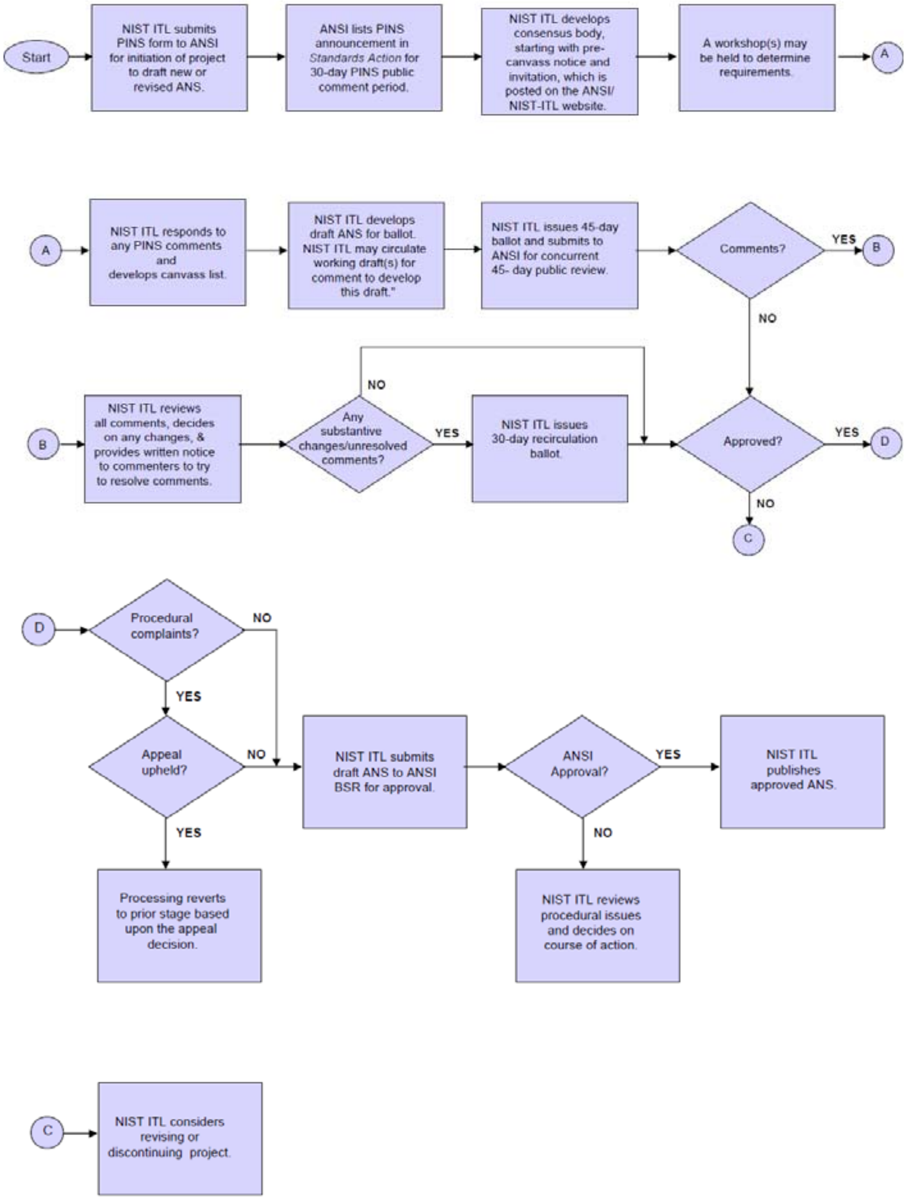
NIST’s Information Technology Laboratory (NIST-ITL) is an ANSI-accredited standards developer. As such, it has a published set of procedures that are followed when developing or modifying the standard. These are available at the website: http://www.nist.gov/itl/iad/ig/ansi_standard-canvass.cfm, which also describes the canvass method used by ANSI/NIST-ITL.

The general process for updating the standard is shown in Figure 2. ANSI/NIST-ITL initiates an update project by compiling a list of comments received on the current version. There may also be committees that were established during previous update cycles that have developed input for the new version (currently there are three such committees). ANSI/NIST-ITL typically produces a first draft update that incorporates changes based upon the comments received by NIST and those recommended by the aforementioned committees. NIST establishes a ‘canvass list’ of parties interested in voting upon the final draft of the updated standard. It does this by contacting participants in previous rounds of the update process, by publicising the process on the standard’s homepage (http://www.nist.gov/itl/iad/ig/ansi_standard.cfm), and by actively soliciting participation by making presentations at biometrics and forensics-related conventions and meetings. There is no fee for participation in the canvass process, and it is open to all who are directly and materially affected by the standard. NIST attempts to balance participation and ensure lack of dominance in the update process among the following categories:

- user
- producer
- consultant
- system integrator.

There is an additional category of General Interest for organisations that do not fall into the above categories.

Figure 2 ANSI/NIST-ITL standard development process (see online version for colours)


Start
NIST ITL submits PINS form to ANSI for initiation of project to draft new or revised ANS.
ANSI lists PINS announcement in *Standards Action* for 30-day PINS public comment period.
NIST ITL develops consensus body, starting with pre-canvass notice and invitation, which is posted on the ANSI/ NIST-ITL website.
A workshop(s) may be held to determine requirements.
A
A
NIST ITL responds to any PINS comments and develops canvass list.
NIST ITL develops draft ANS for ballot. NIST ITL may circulate working draft(s) for comment to develop this draft."
NIST ITL issues 45-day ballot and submits to ANSI for concurrent 45- day public review.
Comments?
YES
B
NO
B
NIST ITL reviews all comments, decides on any changes, & provides written notice to commenters to try to resolve comments.
Any substantive changes/unresolved comments?
NO
YES
NIST ITL issues 30-day recirculation ballot.
Approved?
YES
D
NO
C
D
Procedural complaints?
NO
YES
Appeal upheld?
NO
YES
NIST ITL submits draft ANS to ANSI BSR for approval.
ANSI Approval?
YES
NIST ITL publishes approved ANS.
NO
Processing reverts to prior stage based upon the appeal decision.
NIST ITL reviews procedural issues and decides on course of action.
C
NIST ITL considers revising or discontinuing project.

Notes: PINS is the Product Initiation Notification System of the American National Standards Institute (ANSI). BSR is the ANSI Board of Standards Review.

8 The 2011 update

For major updates (such as that of 2011), NIST convenes workshops so that interested parties can actively participate in discussions concerning what should be incorporated in the standard. There were two workshops, the first occurring 27–29 July 2010 and the second 1–3 March 2011. The participants addressed a total of 42 issues, with 16 working groups formed to work on content revision for the standard, with meetings occurring over a multi-month period. The editor generated updated drafts of the standard periodically for the participants to review and comment. Sixty-eight organisations voted unanimously in the final ballot to approve the standard. It was approved as an ANSI standard in November 2011.

There are significant changes in this version of the standard. It no longer has separate publications by encoding format, as was the case for the previous version [the NIST Special Publication 500-271 (2007) standard called ANSI/NIST-ITL 1-2007 was in Traditional format and the NIST Special Publication 500-275 (2008) version called ANSI/NIST-ITL 2-2008 which was almost identical in data content coverage was in XML format].

Major content additions include a new record type to handle DNA; a new record type for plantar (footprint) data; the extended feature set (EFS) for forensic mark-ups of fingerprint, palmprint and footprint latent images; forensic image mark-up capabilities for facial and iris images; information assurance capabilities (hashing and digital signatures); data handing and transformation logs; capability to transmit audio and video clips; associated data imaging and metadata specification (such as images of a crime scene); geo-position recordation for sample acquisitions; and the ability to transmit images of all body parts (beyond face, tattoos, needle mark patterns and iris, as was previously the case).

The new DNA record includes the ability to exchange electropherogram data and descriptions, including ladders. Autosomal STR, X-STR, Y-STR and mitochondrial data; sample donor information; and pedigree trees (used to verify claimed or purported relationships); as well as information about the laboratory accreditation are all included within the record.

The EFS establishes a common way to mark up friction ridge prints, whether using automated or manual processes. Examples include pattern classification; ridge quality mapping; core, pore and delta counts and locations; latent substrate specification; and annotation of evidence of fraud.

9 Relationship to other standards

The International Organisation for Standardization (ISO) has issued a set of standards for various biometric modalities. The intended audiences of the ISO standards and the ANSI/NIST-ITL standard are not the same. ANSI/NIST-ITL is oriented towards law enforcement, homeland security and military applications, while ISO biometric standards are oriented towards civilian applications, such as the Unique Identity Project (UID) of India. The International Civil Aviation Organisation (ICAO) has adopted ISO biometric standards for face, iris and fingerprint for inclusion in travel documents.

However, a high degree of interoperability is desired, since there may be some organisations with a need for both types of standards. An example is a border management agency that reads travel documents, verifying the traveller's identity against a biometric stored on the document, and also processes biometric samples taken directly from the traveller against large centralised databases. Thus, there has been a conscious effort to harmonise the standards where possible and appropriate. For example, the data specifications for iris images are the same in both sets of standards. The only difference is the addition of some law enforcement related metadata in the ANSI/NIST-ITL standard that would be inappropriate in the ISO standard. The DNA record in ANSI/NIST-ITL 1-2011 was developed in a manner to ensure maximum interoperability with the proposed ISO standard (which has not yet been adopted).

10 Conclusions

The ANSI/NIST-ITL standard is used throughout the world by law enforcement. Military, intelligence and homeland security organisations utilise it for the exchange of biometric and forensic data, along with related data and metadata. The standard is updated periodically to reflect the developing needs and requirements of such organisations. In 2011, a major update occurred. The standard is available at http://www.nist.gov/itl/iad/ig/ansi_standard.cfm. The latest version (ANSI/NIST-ITL 1-2011) incorporates many new capabilities, such as the ability to transmit DNA information, plantar images, and forensic mark-ups of friction ridge, iris, and facial images. Several major groups have already announced plans to base their systems upon this version of the standard, such as the US Department of Defence, the US Department of Homeland Security US-VISIT program, NATO, the US FBI, the national biometrics system of Argentina, and INTERPOL. More organisations are expected to adopt ANSI/NIST-ITL 1-2011 in the near future.

References

INCITS 398-2005 (2005) *The Common Biometric Exchange Formats Framework (CBEFF)*, Washington, DC, USA.

NIST Special Publication 500-271 (2007) *American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information, Part I*, April, ANSI/NIST-ITL 1-2007, Gaithersburg, Maryland, USA.

NIST Special Publication 500-275 (2008) *American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information, Part II*, August, ANSI/NIST-ITL 2-2008, Gaithersburg, Maryland, USA.

NIST Special Publication 500-290 (2011) *American National Standard for Information Systems – Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information*, September, ANSI/NIST-ITL 1-2011, Gaithersburg, Maryland, USA.