International biometric standards – Worldwide impact on personal authentication applications

By Fernando L. Podio, U.S. National Institute of Standards and Technology, Chair of ISO/IEC JTC 1/SC 37, Biometrics

Biometric technologies are able to establish or verify personal identity against previously enrolled individuals and are essential to support more secure personal authentication applications. In addition to supporting homeland security and preventing ID fraud, biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. Using biometrics for identifying human beings offers some unique advantages as only biometrics can identify you as you. Other technologies such as tokens can be lost or stolen or left at home. Passwords can be forgotten, shared, or observed. For decades, biometric technologies were primarily used in law enforcement applications and they are still a key component of these important applications, but over the past several years, the marketplace for biometric-based solutions has widened significantly. Currently, used alone or together with other authentication technologies, biometrics are also required in many public and private sector applications worldwide to authenticate a person's identity, secure national borders and restrict access to secure sites including buildings and computer networks. Biometric technologies are also associated with the management of welfare, identification cards and loyalty programs. Diverse environments such as amusement parks, banks, mobile devices, passports, driver's licenses, college dormitories and school lunch applications are already using biometric technologies.

Deployment of standards-based biometric solutions

As the marketplace for biometric-based solutions has widened significantly, the importance of these biometric technologies has also dramatically increased. Homeland security is the highest priority for many countries. These countries are now seriously considering or have already approved new legislation that calls for the investigation and use of biometric technologies as soon as possible for homeland security applications. The prevention of ID theft will also become a significant market for biometrics in the future. Commercial applications are already using biometrics or are considering the role that biometrics will play in current or future personal authentication systems.

The deployment of standards-based biometric technologies is expected to significantly raise levels of security for critical infrastructures than have not been possible to date with other technologies. Deploying these systems requires a comprehensive set of international, technically sound standards that meet the customer's needs. Biometric standards promote the availability of multiple sources for comparable products and of competitive products in the marketplace. In addition to benefiting end-users, system developers and the IT industry, biometric standards benefit other customers such as the standards bodies that are developing other personal authentication standards.

The international standards committee responsible for the development of biometric standards is ISO/IEC JTC 1/SC 37. The scope of JTC 1/SC37 is the standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file structures; biometric application programming interfaces; biometric data interchange formats; related biometric application profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting, and cross jurisdictional and societal aspects. Excluded is the work in JTC 1/SC 17 to apply biometric technologies to cards and personal identification and the work in JTC 1/SC 27 for biometric data protection techniques, biometric security testing, evaluation, and evaluation methodologies.

JTC1/SC 37 has recently completed the "first generation" of international biometric data interchange formats standards for a number of biometric modalities including finger minutiae data, finger pattern spectral and skeletal data, finger image data, face image data, iris image data, signature/sign time series data, vascular image data and hand geometry silhouette data. These ten standards were published as ISO/IEC 19794-x standards. In addition, a number of biometric interface standards were completed. These standards include the BioAPI-Biometric Application Programming Interface Specification, BioAPI Biometric Archive Function Provider Interface, the Common Biometric Exchange Formats Framework (CBEFF) Data Element Specification and the CBEFF Procedures for the Operation of the Biometrics Registration Authority. In addition, two parts of a biometric performance testing and reporting multi-part standard under development and two conformance testing methodology standards have been published. As shown in Figure 1, eighteen standards developed by JTC 1/SC 37 have been published to date.

The role of biometric standards in national and international programs

Deleted: ¶

A number of the "first generation" biometric standards are already being required by customers of personal authentication applications. Large organizations such as the International Civil Aviation Organization – ICAO (for Machine Readable Travel Documents), the International Labour Office of the United Nations (for the Seafarers Identification Credential program) as well as the European Union have published requirements that include the use of biometric standards. ICAO Doc 9303 Part 1, Volume 2 (Sixth Edition) considers only three types of biometric identification systems. These are facial recognition (listed as mandatory), and fingerprint and iris technologies (optional). ICAO's MRTD Report [1] refers to parts of the ISO/IEC 19794 standards developed by JTC 1/SC 37 and states that that Issuing States are required to conform to these specifications for the technologies used. ILO's requirements for the seafarer's ID card include the use of two fingerprint templates to be stored in a barcode which is placed in the area indicated by ICAO's 9303 standard. ILO's requirements also specify the use of the finger minutiae data interchange format standard developed by JTC 1/SC 37.

The European Union (EU) password specification working document [2] describes solutions for chip enabled EU passports, based on EU's Council Regulation on standards for security features and biometrics in passports and travel documents issued by Member States [3]. The specification relies on international standards, especially ISO standards and ICAO recommendations on Machine Readable Travel Documents, and includes specifications for biometric face and fingerprint identifiers; thus the specifications are underpinned by ISO standards resulting from the work of JTC 1/SC37. A number of standards are referred to in this EU document including an ICAO New Technology Working Group's Technical Report [4] as well as the ISO/IEC 19794-4:2005 and ISO/IEC 19794-5:2005 standards.

Some National Body members of JTC1/SC 37 refer to certain international standards developed by the Subcommittee. In Spain, two official documents store biometric data using JTC 1/SC 37 standards. The electronic national identity card (DNIe) includes personal information of the citizen, details of electronic certificates and the biometric information. The image of the face is stored following ISO/IEC 19794-5 and ICAO standards. Finger minutiae are stored using the ISO/IEC 19794-2 standard. In addition, the biometric data

included in Spanish e-Passports is the image of the face based on ISO/IEC 19794-5 and ICAO standard compliant stored in JPEG2000 format (ISO 15444) [5].

In the United States of America, several organizations require selected biometric data interchange standards developed by JTC 1/SC 37 and use some of the performance testing methodology standards developed by the Subcommittee. Examples include applications and tests performed by government organizations, private industry and consortia. The Transportation Security Administration (TSA) of the Dept. of Homeland Security (DHS) has issued guidance for use of biometric technology in airport access control systems and is performing tests to establish a qualified products list of biometric technologies which meet standards set forth in the aforementioned guidance. Products tested in TSA Qualified Product List (QPL) Testing include enrollment stations and biometric sensors/readers that can be deployed at access points to secure airport areas [6]. The International Biometric Group is conducting these tests on behalf of TSA. The test requirements reference two parts of the multi-part standard developed by JTC 1/SC 37 on biometric performance testing and reporting: ISO/IEC 19795 Part 1 and Part 2, both published in 2007 [7].

The U.S. National Institute of Standards and Technology (NIST) used ISO/IEC 19795-2 for the "Minutiae Interoperability Exchange Test (MINEX)" tests. This testing program was established to determine the feasibility of using minutiae data (rather than image data) as the interchange medium for fingerprint information between different fingerprint matching systems [8].

The Registered Traveler Interoperability Consortium (RTIC) uses some of the JTC 1/SC 37 standards as well. As specified in the RTIC Specification for the U.S. Registered Traveler [9], the enrollment process optionally includes the collection of iris biometrics. The document specifies that iris images selected for enrollment shall conform to quality recommendations of Annex A of ISO/IEC 19794-6:2005 (Iris image capture). Furthermore the document specifies a format defined in this standard as a requirement for the RT card data.

Current efforts and next steps

JTC 1/SC 37 continues to focus on an ambitious development portfolio of international standards. Currently, the program of work includes fourteen projects subdivided into fifty-three subprojects. JTC 1/SC 37 standing document 1 (SD1), available from the

Subcommittee web site [10] provides detailed information on JTC 1/SC 37's program of work and the status of each of its standards projects.

Responding to technology innovation and new customer's needs, JTC 1/SC 37 has initiated the development of the "second generation" of standards. This includes revision projects for the biometric data interchange formats to complement and enhance functionality of the existing standards, the development of a number of conformance testing methodology standards and new parts of the performance testing and reporting multi-part standard. JTC 1/SC 37 is also enhancing the capabilities of the technical interface standards by adding new parts to the Biometric Application Programming Interface standard (BioAPI specification) and the Common Biometric Exchange Formats Framework (CBEFF) standard. These enhancements include BioAPI's support for interchange for certificates and security assertions and other security aspects and the development of an additional part of the CBEFF multi-part standard that will specify standard formats for the CBEFF security block.

A joint work effort with ITU-T SG17 Question 8 is also underway on a BioAPI Interworking Protocol.

Deleted: .

In addition, JTC 1/SC 37 contributes to the development of related personal authentication standards in other JTC 1/SCs such JTC 1/SC 27- IT Security Techniques.

References

[1] Optimizing Security and Efficiency Through Enhanced ID Technology, ICAO MRTD Report – Volume 2 Number 1 2007, International Civil Aviation Organization (ICAO).

[2] Biometrics Deployment of EU-Passports, The European Union password specification working document (EN) – 28 June, 2006.

[3] Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States. Official Journal of the European Union, L 385/1.

[4] ICAO NTWG, Biometrics Deployment of Machine Readable Travel Documents, Technical Report, Version 2.0, 05 May 2004

[5] Communication from Dr. Angel L. Puebla, president of AEN CTN71/SC37 (Spanish Subcommittee of Biometric Identification), Economic and Technical Coordination Division of the Spanish Main Directorate of the Police and the Civil Guard, July 2007.

[6] Biometric Sub-System Qualification Testing, Dept. of Homeland Security, Transportation Security Administration (TSA):
http://www.tsa.gov/join/business/biometric_qualification.shtm
[7] Testing Facility for Initial TSA Qualified Product List (QPL) Testing announcement, International Biometric Group, 30 January, 2007.
http://www.biometricgroup.com/press_releases/pr_2007_QPL.html
[8] Minutiae Interoperability Exchange Test (MINEX) web site:
http://fingerprint.nist.gov/minex04/index.html
[9] Technical Interoperability Specification, Version 1.2, 2 May, 2007, Registered Traveler Interoperability Consortium (RTIC).
[10] JTC 1/SC 37 Web site: www.jtc1.org, select SC 37 – *Biometrics*.

Insert:

Figure 1: ***Published International Biometric Standards Developed by JTC 1/SC 37***

Biometric Data Interchange Format Standards

- ISO/IEC 19794-1:2006, *Information technology --Biometric Data Interchange Formats – Part 1: Framework*
- ISO/IEC 19794-2:2005, *Information technology --Biometric Data Interchange Formats – Part 2: Finger Minutiae Data*
- ISO/IEC 19794-3:2006, *Information technology --Biometric Data Interchange Formats – Part 3: Finger Pattern Spectral Data*
- ISO/IEC 19794-4:2005, *Information technology -- Biometric data interchange formats -- Part 4: Finger image data*
- ISO/IEC 19794-5:2005, *Information technology -- Biometric data interchange formats -- Part 5: Face image data*
- ISO/IEC 19794-6:2005, *Information technology --Biometric Data Interchange Formats – Part 6: Iris Image data*
- ISO/IEC 19794-7:2007, *Information technology -- Biometric data interchange formats -- Part 7: Signature/sign time series data*
- ISO/IEC 19794-8:2006, *Information technology --Biometric Data Interchange Formats - Part 8: Finger Pattern Skeletal Data*
- ISO/IEC 19794-9:2007, *Information technology --Biometric Data Interchange Formats – Part 9: Biometric data interchange format – Part 9: Vascular Image Data*
- ISO/IEC 19794-10:2007, *Information technology -- Biometric data interchange formats -- Part 10: Hand geometry silhouette data*

Biometric technical interface standards

- ISO/IEC 19784-1: 2006, *Information technology --BioAPI-Biometric Application Programming Interface – Part 1: BioAPI Specification*
- ISO/IEC 19784-2:2007, *Information technology --BioAPI-Biometric Application Programming Interface – Part 2: Biometric Archive Function Provider Interface*
- ISO/IEC 19785-1:2006, *Information technology --Common Biometric Exchange Formats Framework (CBEFF) - Part 1: Data Element Specification*
- ISO/IEC 19785-2:2006, *Information technology --Common Biometric Exchange Formats Framework – Part 2: Procedures for the Operation of the Biometrics Registration Authority*

Biometric Performance Testing and Reporting Standards

- ISO/IEC 19795-1: 2006, *Information technology --Biometric Performance Testing and Reporting – Part 1: Principles and Framework*
- ISO/IEC 19795-2:2007, *Information technology -- Biometric Performance Testing and Reporting – Part 2: Testing Methodologies for Technology and Scenario Evaluation*

Biometric Conformance Testing Methodology Standards

- ISO/IEC 24709.1: 2007, *Information technology -- BioAPI Conformance Testing - Part 1: Methods and Procedures*
- ISO/IEC 24709.2: 2007, *Information technology -- BioAPI Conformance Testing - Part 2: Test Assertions for Biometric Service Providers*