Who is Who? Biometrics provides answers for public and private sectors

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

Customers Needs for Biometrics

One of the critical issues related to secured Information Technology (IT) systems and applications is the verification of the users' identity. Biometrics provides for secure transactions, positive identification and augmentation to human judgment. The relationship between a biometric characteristic (e.g., something that you are) and the users of a system or application provides a binding that is stronger than the binding that can be achieved between a user and other technologies that are currently in use for "personal authentication" such as passwords (e.g., something that you know) and tokens (e.g., something that you have). Tokens can be lost, stolen or left at home and passwords can be forgotten, shared, or observed by a third party. Used alone, or together with these technologies, biometric technologies can provide higher degrees of security than the other technologies employed alone and can also be used to overcome their weaknesses.

Subcommittee 37- *Biometrics* of the ISO/IEC Joint Technical Committee 1, Information Technology (JTC 1/SC 37) defines biometrics as "automated recognition of individuals based on their behavioural and biological characteristics". Examples of biological characteristics are finger, face, hand, and iris. Behavioural characteristics are traits that are learned or acquired, such as dynamic signature verification and keystroke dynamics. It is usual to find, in the literature, biometric characteristics identified as two different types: biological and behavioural . According to JTC 1/SC 37 experts "behavioural" and "biological" characteristics cannot be completely separated. For example, a fingerprint image results from the biological characteristics of the finger ridge patterns and the behavioural act of presenting the finger. Biometric recognition encompasses biometric verification and identification. Automated recognition implies that a machine based system is used for either the full recognition process or is assisted by a human being.

Marketplace for biometric-based solutions

For decades, biometric technologies were used primarily in law enforcement applications, However, over the past several years, the marketplace for biometrics solutions has significantly widened. Currently, they are increasingly being required in 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. Biometrics are being used for the protection of buildings from unauthorized individuals, in employee IDs, in retail, banking and financial institutions (e.g., employee-based / customer-based applications), associated with the management of welfare programs and in health care applications (e.g., service provider security to protect patient privacy, patient delivery verification protecting patient and provider). Other applications include verification of users' identity in mobile devices, colleges (e.g., online identity verification) and amusement parks. Consumer uses are also expected to significantly increase for personal security and convenience in home automation and

security systems, retail, gaming and hospitality industries and even in childcare/school applications (e.g., lunch programs, guardian verification for child release).

Need for International biometric standards

The success of biometric applications is particularly dependent on the interoperability of biometric systems. Deploying these systems requires a portfolio of technically sound international biometric standards that meets customers' needs. As discussed above, the deployment of standards-based, high-performance, interoperable biometric solutions is expected to increase levels of security for critical infrastructures that has not been possible to date with other technologies. An important consideration and rationale for the development of a comprehensive portfolio of biometric standards is that they promote the availability of multiple sources for comparable products. These standards must provide support for a diverse range of systems and applications designed to provide reliable verification and identification of individuals. They should benefit the customers for whom these standards are developed including end-users, system developers, the IT industry as well as other standards developers working in related standards (e.g., security, token-based).

A portfolio of biometric standards in support of secured IT systems and applications

In the International arena, ISO/IEC Joint Technical Committee 1, *Information technology*, Subcommittee SC 37, *Biometrics* (JTC 1/SC 37) is responsible for the development of a large portfolio of biometric standards in support of interoperability and data interchange. Including published standards and ongoing projects, the Subcommittee is currently responsible for over one-hundred projects. Topics addressed by these standards include biometric data interchange formats for a number of biometric modalities, biometric technical interface standards, performance and conformance testing methodology standards, sample quality standards, and standards in support of cross jurisdictional issues related to the utilization of biometric technologies in commercial applications. The Subcommittee is also developing a harmonized biometric vocabulary to serve the standards community as well as other customers. To date, forty-four International standards (including amendments) and six Technical Reports have been published. These standards are aimed at helping customers to achieve higher levels of security and interoperability in personal authentication and identification applications using biometric-based open systems solutions. JTC 1/SC 37 works in close collaboration with two other JTC 1 Subcommittees responsible for developing related standards. They are JTC1/SC 27, *IT Security techniques* and JTC 1/SC 17, *Cards and Personal Identification*.

Impact of biometric standards in the marketplace – Who benefits from these biometric standards?

A number of international and national organizations have adopted or are considering adopting many of the biometric standards developed by JTC1/SC 37. The International Civil Aviation Organization (ICAO), for example, selected facial recognition as the globally interoperable biometric for machine-assisted identity confirmation for Machine Readable Travel Documents (MRTD). ICAO requires conformance to the face recognition standard developed by JTC 1/SC 37. Other JTC 1/SC 37 standards adopted by ICAO are the fingerprint data interchange formats, the iris recognition interchange format and an instantiation of the Common Biometric Exchange Formats Framework (CBEFF). The adoption of JTC 1/SC 37 standards by this organization is expected to significantly impact the use of biometrics for

MRTD in the countries represented within ICAO. The International Labour Organization of the United Nations (ILO) developed requirements for a Seafarers' ID Card which includes the use of two fingerprint templates to be stored in a barcode. ILO's requirements specify the use of some of the standards approved by JTC 1/SC 37; specifically finger minutiae and finger image data interchange formats (published as International Standards in 2005). JTC1/SC 37, in collaboration with ILO, developed a biometric profile for Seafarers. The document, already published as an international standard, includes normative requirements to several of the JTC 1/SC 37 standards.

Several countries represented in JTC 1/SC 37 are also adopting the JTC 1/SC 37 standards. For example, Spain has two official documents that store biometric data using JTC 1/SC 37 standard data interchange formats; the electronic national identity card (DNIe) and the Spanish e-Passport. The DNIe card includes the personal information of the citizen, details of electronic certificates and the biometric information. The Spanish e-Passport contains the face image conforming to a face image data interchange format developed by JTC1/SC 37. In the United States of America, several organizations require selected biometric data interchange standards developed by JTC 1/SC 37 and some of the ongoing biometric testing programs use performance testing methodology standards developed by the Subcommittee. The latest significant adoptions are the biometric standards that the Planning Commission of the Unique Identification Authority of India has recommended for the Unique Identity project. After reviewing international standards and current national recommendations, the Biometric Committee established by the Indian government concluded that the ISO series of biometrics standards for fingerprints, face and iris data interchange formats developed by JTC 1/SC 37 were the most suitable for the project.

Standards Roadmap

JTC1/SC 37 is planning to continue the development of international standards, keeping in mind the customer's needs and the support for the mass market adoption of biometrics-based solutions. JTC 1/SC 37 concluded the development of most of the "first generation" of biometric standards. Recent technology innovations and new customers' needs are being addressed by the Subcommittee through the development of the "second generation" of biometric standards. They include revision projects for the biometric data interchange formats, the development of new biometric technical interface standards, performance (and conformance) testing methodology standards and biometric sample quality standards. The Subcommittee is also responding to other standards organization needs by initiating new projects in support of their standards and requirements.