

DoD's approach to biometric standards

The US Department of Defense (DoD) has a growing need to control access to its many assets. Similarly, DoD organisations must always be ready to identify "friend or foe". The terrorist attacks of 11 September 2001 reinforced the need for technologies that can enhance homeland security, force protection, and counter terrorism measures. DoD recognises the value of technologies such as biometrics in this area and has taken an active role in their development, particularly in the area of standardisation.

In the USA, Congress, the White House and DoD leadership recognise that biometrics can be an enabling technology to provide better security through identity assurance.

Biometric systems take identity assurance beyond the basic "something you have" and "something you know", to "something you are", such as fingerprints, hand geometry and iris patterns. The association between an individual and a "trusted identity" is the foundation for identity management. A trusted identity is something that proves beyond a doubt that you are who you say you are – your identity has been "vetted" – and that another person cannot "assume" your identity or masquerade as you. In other words your identity has been "fixed".

Identity management is the process that creates and maintains the use of trusted identity. With vetting and fixing a trusted identity, identity management can be further associated with a set of assigned permissions and access rights. Before the information age, DoD faced its greatest challenge in the area of physical access control. However, the exponential growth and use of IT throughout DoD has dramatically increased the security challenge for logical access control, of which trusted identity is essential, particularly with the emphasis on net-centric warfare.

Developing standards

The DoD aims to promote greater interoperability of biometric technology through the development and adoption of standards. These standards will prevent DoD from building stovepipes, discourage adopters from "reinventing the wheel", and encourage DoD organisations to use technologies that contribute to joint war fighter capabilities.

On 25 August 2003, deputy secretary of defence Paul Wolfowitz announced his Department of Defense Biometrics Enterprise Vision. He directed the DoD Biometrics Management Office (BMO) to "ensure that a scalable biometric component of the Global Information Grid (GIG) infrastructure is in place, and that the appropriate standards, interoperability tools, testing frameworks, and approved product validations are available to assist the DoD community in using this technology."

The BMO established the BMO Standards Working Group to coordinate biometric standards activities within DoD. The BMO SWG membership includes the US Army, US Air Force, US Navy, the National Institute of Standards and Technology (NIST), the National Security Agency (NSA), the Defense Information Systems Agency (DISA) and other US Government organisations.

One of the BMO Standards Working Group's major efforts has been developing the *DoD Biometrics Standards Development Recommended Approach*. This details an approach for identifying, participating in, and developing biometric standards. The document coordinated and integrated DoD priorities for developing biometric standards across DoD agencies and services.

The first step toward developing the DoD approach document was to identify the current state of biometric standards. Figure 1 depicts the biometric standards building blocks and the current state of each standard.

Coordination

The DoD biometrics approach document provides the first step toward coordinating the development of biometric standards with other Federal agencies and organisations. As a next step, the BMO, along with the NIST, NSA, and the Department of Homeland Security (DHS), is jointly sponsoring and hosting the "US Government workshop on biometric standards and its support to the global war on terrorism".

The various agencies and organisations invited to participate in this Workshop include the Central Intelligence Agency

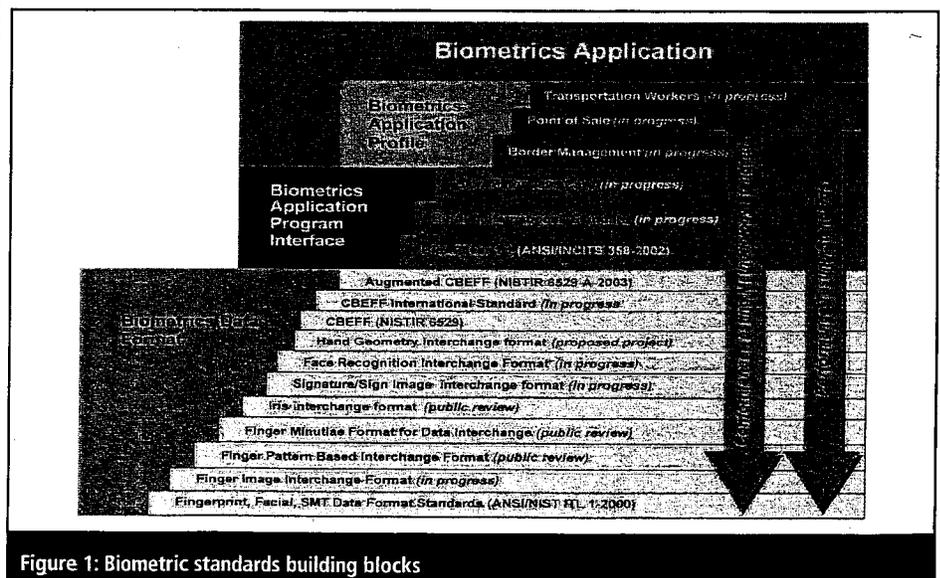


Figure 1: Biometric standards building blocks

(CIA), the Defense Advanced Research Projects Agency (DARPA), various DoD agencies and services, the Department of Justice (DOJ), the Department of Transportation (DoT), the Federal Bureau of Investigation (FBI) and the National Biometrics Security Project (NBSP).

The purpose of this workshop is to discuss the coordination of biometric standards and their support in the Global War on Terrorism. Although some of the agenda is non-public, the workshop topics will include an overview of biometric standards and the Global War on Terrorism, a discussion of biometric standards policy and an explanation of biometric security standards. The workshop also will discuss the need to create a conformity assessment programme for biometric technology. During the workshop, the US Government agencies will share their needs and plans for developing biometric standards in order to coordinate the development of biometric standards.

Other DoD participation

Instead of creating proprietary, non-consensus standards, the National Technology Transfer and Advancement Act of 1995 (Public Law 104-113) requires Federal agencies to adopt commercial standards – particularly those developed by standards developing organisations – wherever possible. Through active participation in national and international standards organisations, the DoD BMO tries to exert its influence to facilitate and promote DoD interests in the biometric arena, working closely with NIST

and other US Government partners. As a result, the standards developed through these national and international organisations will better reflect and support the interests of DoD biometric-related activities.

Within the United States, the International Committee for Information Technology Standards (INCITS) is the recognised standards development organisation for IT and operates under the rules of the American National Standards Institute (ANSI). INCITS does not restrict membership and attracts participants in its technical work from 13 countries. The INCITS M1 Biometrics Standards Committee, established in November 2001, is one of several committees that develop US national commercial standards related to IT. The M1 Committee is the primary body responsible for developing national biometric standards. Fernando Podio of NIST, an advisor to the BMO Director and a member of the BMO Standards Working Group, chairs the INCITS M1 Biometrics Standards Committee.

Two other INCITS committees also are involved in biometric-related issues. The B10 Committee addresses identification cards and related devices (for example, issues related to smart cards). The T4 Committee undertakes security techniques that include a broad range of data security issues, such as biometric data security. In addition, X9 is another ANSI-chartered organisation responsible for developing, establishing, publishing, maintaining and promoting financial services industry standards.

ANSI is the official representative for the US to the International Organisation for

Standardisation (ISO). The SC37 Committee of the ISO/International Electrotechnical Commission Joint Technical Committee 1 (JTC 1) is responsible for developing international biometric standards. SC37 is the counterpart biometric standards body to INCITS M1. INCITS M1 represents the United States in JTC1 SC37.

Figure 2 shows the relationship between the US standards bodies working on biometric technology and their international counterparts. Currently, the BMO actively participates in INCITS M1, T4, B10 and JTC 1 SC 37 (through INCITS M1).

Within INCITS M1, the BMO is also developing a standard: *DoD Application Profile – Standards Guidance for DoD Implementation of Biometrics*. This will include capturing best practices and facilitating an increase of interoperability and data interchange in DoD deployments of biometrics.

Summary

A significant amount of work on developing standards for the Department of Defense is under way. Standards and interoperability are crucial for deployment of biometric systems. With this goal in mind, the *DoD Biometrics Standards Development Recommended Approach* is a solid starting point for a comprehensive, coordinated approach to DoD's use of biometrics.

The BMO will ensure that this approach serves as a framework for standards within DoD and receives consideration from other US Federal agencies in their biometric technology implementation. Ideally, US Government agencies should work together for a collaborative strategic approach, using the resources of participating agencies in the spirit of cooperation. This will advance the development of the necessary standards as well as accelerate the establishment of an environment of interoperability.

DoD's coordination with NIST in accelerating national and international biometric standards development, DoD's related conformity assessment and interoperability efforts, and other US Government initiatives will support DoD's goals to provide high-performance, interoperable and scalable biometric solutions to the DoD community.

This article was provided by John Woodward, the director of the DoD Biometrics Management Office. For more information, please visit www.biometrics.dod.mil.

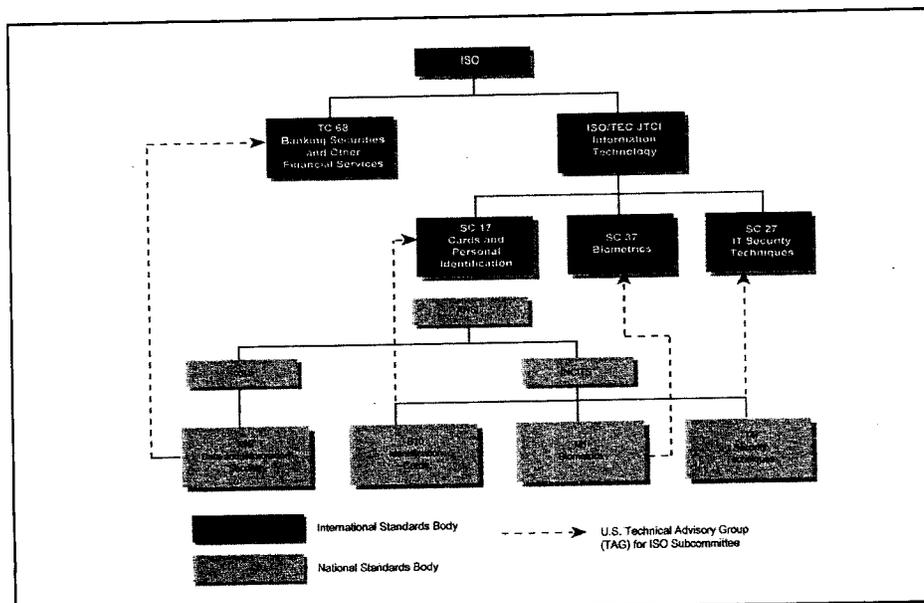


Figure 2: Relationship between US biometric standards bodies and their international counterparts