Trusting the Team: Identity Protection and Management

Defense-Wide Information Assurance Program

Identity protection and management is at the heart of establishing and maintaining a secure and interoperable infrastructure. We must be able to trust the identity of information producers, service providers, and consumers of the information and services. The article highlights the Department of Defense's (DoD's) primary initiatives in this area.

Information superiority is heavily dependent on establishing and maintaining a secure and interoperable infrastructure. At the heart of it all is identity protection and management. We must be able to trust the identity of information producers, service providers, and consumers. In pursuing these objectives, many goals over the past 15 years have been achieved, primarily through the efforts of three DoD initiatives: Common Access Card (CAC), Public Key Infrastructure (PKI), and biometrics.

The CAC provides the standard identification card for authorized DoD users – the DoD credential enabling physical and logical access. The DoD has issued more than 11 million identity cards (more than 3.5 million are in current circulation). Use of the CAC and the PKI certificates on the token eliminates the need to use passwords when authenticating. This mitigates a major problem with protecting DoD networks from unauthorized intruders.

In addition to improving the security of our networks, the CAC, with its PKI credentials, is also accelerating our migration to the Web. By allowing the use of digital signatures in systems like the Defense Travel System, labor-intensive paper processes are being eliminated. The CAC also provides the means to improve physical access security at DoD installations around the world. When a base or a theater of operations implements rapid electronic authentication, hundreds of fake identification cards are confiscated every week and unauthorized accesses are prevented (more than a million in Europe alone in just one year). Our DoD CAC initiative is one of the most award-winning and successful smart card efforts in the world.

PKI utilizes a combination of software, encryption technologies, and services that enable enterprises to protect their communications and business transactions on networks. PKI integrates digital certificates, public-key cryptography, and certificate authorities into a total enterprise-wide network security architecture. The DoD has initiated one of the largest PKI implementations in the world with more than 20 million certificates issued across the DoD. Since the mandate to move to cryptographic log-in on our networks, the DoD reduced successful intrusions into its networks by 46 percent.

Biometrics provide a measurable identity factor that can be bound to an electronic identity for use during authentication. Measurable physiological or behavioral characteristics – including fingerprints, iris recognition, voice analysis, and handwriting dynamics – can be used to validate an established identity. In 2006, the Deputy Secretary of Defense established the defense research and engineering as the Principal Staff Assistant for Biometrics and the Army established the Biometrics Task Force to lead, consolidate, and coordinate all biometric information assurance activities and ensure biometrics technologies are integrated across DoD. Every day in Iraq and other area of responsibility sites, biometrics of visitors and workers are being checked against terrorist watch lists and Red Force databases. We are detaining people whose fingerprints were left behind on improvised explosive devices and denying access to those individuals on these watch lists.

To align the efforts of these three program offices into one coordinated venture across the DoD, the Identity Protection and Management Senior Coordinating Group (IPMSCG) was established in January 2004. The IPMSCG oversees DoD policy, strategy, and capability implementation and has developed the DoD Road Map to Identity Superiority. Also critical in the Global War on Terror is the need to align these DoD efforts with similar initiatives within the federal government, law enforcement agencies, state and local governments, and allied coalition forces.

Homeland Security Presidential Directive No. 12 <www.whitehouse.gov/news/releases/08/20040827-8.html> establishes the framework for a common identification standard for all federal government employees and contractors. The standards-based credential will facilitate electronically validated entry to federal facilities and electronic credential-based authentication to virtual spaces, enabling more secure information sharing within the federal government. To meet these requirements, the DoD's pursuit of next-generation identity-based technologies, standards, and processes must include such key elements as the following: identity proofing, credentialing, directory services, authentication, authorization, privacy, and a tighter link between the identity proofing and credentialing processes.

Identity Superiority

As detailed in the DoD Road Map to Identity Superiority, the success of the DoD's approach to identity management is crucial if we are to advance to a broader, next-generation identity protection and management capability or identity superiority. Identity superiority will enable *secure*, *integrated*, *interoperable*, and *scalable information sharing solutions* for people, systems, and services in a net-centric warfare environment. In implementing the DoD's approach to identity superiority, a number of initiatives that take advantage of CAC, PKI, and biometrics are under way:

- Mandated use of the CAC to log-on to DoD networks decreases the use of passwords, significantly decreasing successful DoD network intrusions by 46 percent and socially engineered email attacks by 30 percent.
- DoD Interoperability Root Certificate Authority is being established (~March 2007) as a first step in enabling the DoD to have the ability to successfully interoperate with non-DoD entities (on a limited basis).
- Automated Biometric Identification System is currently a repository of Red Force biometrics data. This data is used in identifying potential national security threats.

There is still significant work that needs

to be done. Achieving identity superiority requires more than the efforts of the three program offices. Actions required to achieve identity superiority include aligning initiatives under way in each of the three program offices, expanding the focus to accommodate the continually evolving warfighting environment, and identifying additional enabling processes and technologies that are needed but not yet supported. Identity is key to being able to take full advantage of the power of the Internet.

With a well-defined and trusted identity management architecture, the DoD can evolve its current access control model to where consumers with authorized credentials can access information without having to pre-register with the information provider. For this evolution, the DoD is pursuing the concept of Attribute Based Access Control; where policy-based, fine-grained access control processes use validated attributes to authenticate users and devices and make authorization decisions. Attributes are qualities or characteristics inherent in or ascribed to an identity (human or device) such as mission, function, area of interest, name, rank, role, citizenship, location, or organization. This is the new direction of authorization needed for information sharing. It is the combination of *identity*, knowing who you are, and *information release* – knowing who can see a piece of information. Authorization is the process that joins these two pieces of knowledge together.

The DoD has long emphasized using state-of-the-art technology to secure and protect its most vital assets: people, information, and equipment. Our quest for identity protection and management or identity superiority will continue that tradition and provide our warfighters and supporting workforce with the enabling technology and tools necessary for tomorrow's challenges.◆

About Defense-Wide Information Assurance Program

This article was a combined effort of several members of the Defense-Wide Information Assurance Program (DIAP). The DIAP is within the Information Assurance Policy Directorate of the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD [NII]) DoD Chief Information Officer (CIO) and is responsible to the ASD (NII) DoD CIO for ensuring Information Assurance (IA) is pursued and implemented throughout the DoD, as well as the intelligence community, as a critical operational readiness issue. The DIAP Office coordinates, integrates, and oversees IA processes of the DoD and is the central focal point for organizing and marshalling the resources to execute its mission. The program's operations are focused on linking and integrating IA management into the DoD planning, programming, budgeting, and execution process; the requirements generation process, the acquisition process, and readiness reporting process. More information on the DIAP can be found at <www.defenselink.mil/cio-nii/infoassurance/diap/index.html>.