U.S. Government Leverages Personal Identity Verification from INCITS M1 and JTC 1/SC 37 Biometric Standards

Background

Historically, U.S. government agencies required the identity of federal employees and contractors to be authenticated prior to entering government facilities and using government information technology (IT) systems. Some agencies also implemented authentication mechanisms for access to specific areas or systems. The methods and levels of assurance for authentication and authorization, (i.e. identification and permissions) varied widely from agency to agency, and even within a single agency.

In 2004, Homeland Security Presidential Directive (HSPD) 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, was issued to address the lack of government-wide secure identity mechanisms for federal employees and contractors. Under HSPD's authority, the National Institute of Standards and Technology (NIST) developed Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*. PIV was developed through a public-private partnership utilizing biometric standards developed by the InterNational Committee for Information Technology Standards (INCITS) M1, *Biometrics Technical Committee*, and International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1/Subcommittee 37, *Biometrics*, (ISO/IEC JTC 1/SC 37). INCITS M1 is the ANSI-accredited U.S. Technical Advisory Group (TAG) administrator to JTC 1/SC 37 and has been instrumental in the development of biometric data format standards.

Problem

Until the PIV program was developed there were wide variations in the quality and security of identifications used for federal employees and contractors. No standards existed specifying the requirements for an interoperable electronic ID card that could be used to authenticate federal employees and contractors across all agencies to gain access to secure government facilities and IT resources/systems. Post 9/11, the lack of a secure, reliable form of identification was recognized by the government as an issue that had to be addressed.

Approach

HSPD 12 required the development and implementation of a government-wide standard for secure, reliable forms of identification for federal employees and contractors. As required by HSPD 12, NIST developed FIPS 201 in coordination with other government agencies and the private sector. FIPS 201 defines a reliable, government-wide PIV card as a smart-card based solution with on-card common credentials that can be used to verify the identity of federal employees and contractors. FIPS 201 also defines the authentication mechanisms to be used with the credentials of the PIV card.

The PIV card contains identity credentials such as cryptographic keys and biometrics to achieve graduated levels of security, from least secure to most secure, ensuring flexibility in selecting the appropriate level of authorization. The identity credentials are securely stored and protected

on the Integrated Circuit Chip (ICC). Cryptographic keys used in authentication events use NIST-approved algorithms, while a personal identification number (PIN) provides protection and enables cardholder consent to release public key infrastructure (PKI) certificates.

To enable interoperable implementation of FIPS 201, NIST issued several special publications (SP). NIST SP 800-76, *Biometric Data Specification for Personal Identity Verification, NIST, February 2006*, specified the mandatory format for biometric data carried in the PIV data model consisting of:

- A full set of fingerprints used to perform law enforcement checks as part of the identity proofing and registration process;
- An electronic facial image printed on the card for performing visual authentication during card usage; and,
- Two electronic fingerprints stored on the card for automated authentication during card usage.

Implementation requirements for storage of biometric data on a PIV card depends on its use, as specified in NIST SP 800-76. In addition to requiring a certified scanner according to Appendix F of the Electronic Fingerprint Transmission Specification, *Criminal Justice Information Services, Federal Bureau of Investigation, Department of Justice, May 2, 2005*, the biometric specifications in NIST SP 800-76 required conformance to a number of American National Standards (ANS) specifying biometric data formats for a number of modalities developed by INCITS M1.

The biometric records are required to be wrapped in a PIV instantiation metadata structure specified in INCITS 398-2005, *Information Technology - Common Biometric Exchange Formats Framework (CBEFF).* Conformance requirements for fingerprint records are found in INCITS 378-2004, *Information Technology - Finger Minutiae Format for Data Interchange*, and INCITS 381-2004, *Information Technology - Finger Image-Based Data Interchange Format.* And conformance requirements for facial image records are found in INCITS 385-2004, *Information Technology - Face Recognition Format for Data Interchange*.

The latest versions of FIPS 201-2 and NIST SP 800-76-2 includes specifications of an optional iris biometric record which affords an alternative to fingerprint based authentication and chain-of-trust maintenance. Iris image requirements conform to ISO/IEC 19794-6:2011, *Information Technology - Biometric Data Interchange Formats - Part 6: Iris Image Data,* developed by JTC 1/SC 37. Also included are specification for on-card comparison leveraging ISO/IEC 19794-2:2011, *Information Technology - Biometric Data Interchange Formats - Part 2: Finger Minutiae Data,* also developed by JTC 1/SC 37. And NIST SP 800-76-2 guides implementers to numerous other standards developed by JTC 1/SC 37.

Outcome

According to the White House of Office of Management and Budget (OMB), as of September 1, 2012, over five million federal employees and contractors (over 97 percent of federal employees and over 88 percent of contractors) have been issued PIV cards.