Building in PIV Support—Without Boxing in Your Application

Certicom BSP for Personal Identity Verification

THE CHALLENGE

In 2004, the White House issued a new Presidential directive, Homeland Security Presidential Directive 12 (HSPD-12). It proclaimed that:

> **Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).**

This prompted NIST (the National Institute of Standards in Technology) to establish FIPS 201, a two-part Federal Information Processing Standard governing the Personal Identity Verification of Federal Employees and Contractors. Part I of FIPS 201 establishes the minimum requirements for systems to meet the aims of HSPD-12. Part II details technical specifications. By the end of 2005, compliance with FIPS 201 Part I was mandatory throughout the United States; Part II compliance will be required by October 2006.

A unified approach to personal identity verification (PIV) has both security-related and administrative advantages, but it presents a challenge to developers selling into the U.S. federal government. That challenge is: How to build applications that support a common PIV standard and at the same time provide the architectural flexibility, portability and down-the-road compatibility that will allow the applications to remain practical and valuable over the long term?

REQUIREMENTS SCENARIOS

HSPD-12 and FIPS 201 ultimately apply to a broad range of devices and applications—some of which are expressly related to security, such as door-mounted smart-card readers that control access to physical premises, and others that have more generalized productivity-related functions, such as PDAs and other mobile data devices.

For the sake of example, consider a smart phone: a wireless device capable of voice and data communications, assigned to an authorized government user. Such a user might already take advantage of the basic built-in security provided by the manufacturer and, for instance, control access to the data stored on the device by means of a password.

Common Access Cards: What They Do

A Common Access Card is a form of personal identity verification used by the US Department of Defence. It contains the end user and root certificates that have been issued by the DOD Certificate Authority. The public keys are contained in the certificates and the encrypted private keys are stored on the card and are PIN protected. The CAC provided two or more forms of authentication: something you have (CAC) and something you know (PIN or password).

This remains a valuable security factor, but it is not sufficient for the device to operate within a FIPS 201-compliant environment. For that to be the case, the smart phone must subsequently be able to read the user's Common Access Card (CAC) and authenticate that card against the user's CAC password (which is distinct from the device password).

Once these further actions have been performed, the user can process protected data according to his or her level of authorization. Yet in a fully secure environment even those data-handling operations must conform to security protocols, such as U.S. Department of Defense policies governing CAC-protected email, wireless communications and the associated cryptographic functions.

We can easily envision four scenarios in which all these various security demands come into play:

ACCESSING THE DEVICE

As described above, this would involve the following steps:

- **Activation of the device**
- **Inputting of user's local smart phone password**
- **Swiping of CAC card in phone**
- **Inputting of user's CAC PIN**
- **Completion of local authentication and verification, giving user access to device services**

DELETING LOCAL DATA

An authenticated user has the ability to delete data stored locally on the device. To ensure that this data is not somehow latently recoverable, files to be deleted should be:

- **Encrypted using a one-time AES key**
- **Overwritten seven times per NSA Orange Book/CCEVS (after which the key should be zeroized to prevent data recovery)**

SENDING SIGNED AND ENCRYPTED MESSAGES

In this case, the authorized user composes an email and signs it using a private signing key stored on the CAC. The process is as follows:

- **The user is prompted for his or her CAC PIN**
- **A signing certificate is appended to the outgoing message along with the signed data**
- **The application retrieves the public key from the certificate of the intended recipient**
- **The application bulk encrypts the message and uses the recipient's public key to encrypt the symmetric key**
- **The signed and encrypted message is sent**

RECEIVING S/MIME EMAIL

Here, the above process is essentially reversed—the capacity for which must reside on the device itself:

- **An encrypted message is received**
- **The device accesses the user's private key on the CAC to decrypt**
- **The sender's signature is verified by retrieving the public key from the certificate appended to the message**

Other examples include using CAC to authenticate a VPN instead of pre-shared secrets, or using CAC to perform web based client authentication for secure browsing. The purpose of reciting these various examples is to show the degree of versatility a device must possess to function effectively within an HSPD-12, FIPS-governed environment.

Using the Certicom Security Architecture (CSA) and its assorted Security Builder modules, developers can build in all of these capabilities—and more—easily, efficiently and in a way that enables future flexibility as standards evolve and change.

THE SOLUTION

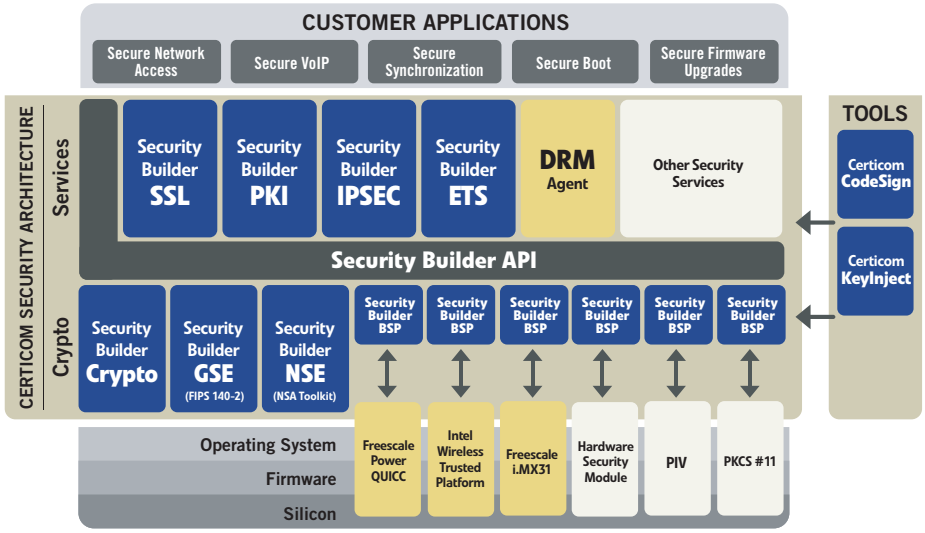

FIGURE 2. Certicom Security Architecture

As this illustration shows, the Certicom Security Architecture contains several modules of relevance to developing applications for HSPD-12 environments—from Security Builder BSP modules within the Security Builder API itself that interface with functions embedded in the device silicon to a Security Builder PKI toolkit for certificate-management services. Here's how they work:

SECURITY BUILDER BSP FOR PIV

This module provides a software interface between the application and PIV-compliant tokens, readers or interfaces. It is ready-made to support NIST's smart card interoperability specification and ISO 7816. This component interoperates with the CSA's Security Builder PKI-C and GSE-C toolkits for higher-level functionality.

SECURITY BUILDER GSE (GOVERNMENT SECURITY EDITION)

Pre-validated to FIPS 140-2 and NSA Suite B enabled, this crypto module is designed specifically to satisfy U.S. government guidelines for security in communications products. Supporting a code-size range of 50KB to 4MB, it handles a long list of FIPS-approved algorithms—both symmetric and asymmetric—as well as digital signature algorithms. The list includes: AES, DES, 3DES, DSA ECDSA, HMAC, RSA, PKCS#1, RNG and SHA-1 through SHA-512. It also supports DH, ECDH, ECMQV and RSA key-agreement and transport schemes.

SECURITY BUILDER PKI

The PKI module enables robust standards-based management of ECC and RSA based X.509 certificates, supporting ANS.1, DOCSIS, Check 21 image validation and more.

SECURITY BUILDER BSP FOR PKCS #11

This module supports PKCS #11, the Cryptographic Token Interface Standard. PKCS #11 specifies the Cryptoki API to devices that store cryptographic information and perform cryptographic functions. Taking a simple object-based approach, Cryptoki addresses the goals of technology independence and resource sharing, presenting a common, logical device view to applications. This BSP provides PKCS#11 support on over 30 different operating systems.

Our example of the smart phone from Part II illustrates how these elements of the Certicom solution work together:

- Security Builder BSP for PIV was used to establish an interface between the device and the CAC reader/ authentication mechanisms.[1]
- Security Builder GSE-C provided FIPS 140-2 Level 1 AES to enable local encryption of data stored on the smart phone.
- Security Builder PKI-C was used to manage digital certificates and cryptographic message syntax (CMS) functionality to support encryption and digital signing of email messages.
- The Security Builder BSP for PKCS #11 established a link between the security components' PKCS #11 interface and the application's PKCS #11 interface, enabling communication with the CAC reader.

Because the Certicom Security Architecture is standards-based and FIPS-validated, and because its various components and toolkits interoperate seamlessly, developers are assured that their applications will remain highly portable and future-proof, satisfying the requirements of standards and specifications such as those contained within the NSA's oft-mentioned Suite B.

SUMMARY

By taking advantage of the various components available today within the Certicom Security Architecture, the smart phone application developer in the example above produced a device that accorded fully with the requirements of HSPD-12 without compromising functionality or constraining the phone's potential future uses in the ever-evolving realities of the wireless workplace. Using Certicom's Security Builder BSP for PIV, it is easy to build security applications 'from the ground up', as it were, embedding key functions for optimum security while maintaining higher-level flexibility to adapt to changing requirements.

[1] Another good example of this comes from LRW Digital's use of the Security Builder BSP for PIV to establish communications between Pocket PCs with Extensia™ email and Tactel smart cards. Security Builder BSP for PIV used the standard ISO 7816 interface to create a secure connection between the two.

about certicom

Certicom Corp. (TSX: CIC) is the authority for strong, efficient cryptography required by software vendors and device manufacturers to embed security in their products. Adopted by the US Government's National Security Agency (NSA), Certicom technologies for Elliptic Curve Cryptography (ECC) provide the most security per bit of any known public key scheme, making it ideal for constrained environments.