



Sagem Morpho Inc.
SAFRAN Group

HSPD-12 Implementation with Smart Terminals and Legacy PACS

Federal Agencies, specifically security managers, face many challenges in determining the most cost effective way to implement HSPD-12 (PIV) requirements. Large investments have been made in existing Legacy PACS (Physical Access Control Systems) which are not compliant with the new requirements. Few security managers have the resources to completely upgrade their entire PACS. Most will need to adopt a phased approach to meet the new requirements. An effective approach to this problem is to integrate “smart” terminals into the front end of an existing legacy system.

Many legacy PACS use a “dumb” terminal to read a proximity card and transmit the card number on the card to the PACS. The terminal is unable to process the card number that it reads. It merely reads the card, and then sends the number to the PACS. The access control system grants or denies access depending upon the card holder permissions associated with the card number received as specified in the PACS database.

The HSPD-12 (PIV) solution requires a smart card having a CHUID (Cardholder Unique Identifier). The CHUID contains agency data, cardholder data and the card expiration date which is read from the card as a 40 or more digit number. A “smart” terminal is able to read and parse the CHUID into its separate data elements, and validate the card expiration date. Legacy readers can not perform this critical function. The Sagem Morpho Biometric “smart” terminal (MorphoAccess™) has processing capability and storage capacity to store up to 48,000 finger print records and associated user information. The MorphoAccess™ also has the ability to read and parse all data in the CHUID and then utilize all of the data for verification of the credential owner. Additionally, MorphoAccess™ allows for the transition of multiple legacy PACS through a single reader technology. In essence, the MorphoAccess™ becomes the “bridge” between the multiple legacy PACS.

In a transitional phase, MorphoAccess™ terminals are deployable initially as smart card readers. The existing biometric capability may be activated to meet short term, variable security level changes. As security requirements dictate and agencies are able to fund the migration to more advanced PACS systems, the biometric capability may be permanently activated, allowing for hardware investment made today to continue providing value in the future.

Local database management embedded in the “smart” terminal maps the cardholder CHUID to the legacy PACS card identification number contained in today’s proximity card readers. Once the individual has been identified, the corresponding Weigand signal is sent to the PACS for disposition, otherwise a denial signal is sent (see attached figure).

FIPS 201 and the PACS Implementation Guidance, Version 2.3 document (TIG) specify three levels of assurance to validate the authenticity of the card and the identity of the card holder for implementation by Federal Agencies depending upon specific security requirements. FIPS 201 provides specifications for PACS using contact card readers while the TIG provides specifications acceptable for PACS using contactless readers.

PACS With Contact Reader Assurance Levels		PACS With Contactless Reader Assurance Levels	
Low Assurance Some Confidence	Read CHUID; parse and determine expiration date to assure card is valid	Low Assurance Some Confidence	Read CHUID; parse and determine expiration date to assure card is valid
Medium Assurance High Confidence	Perform low assurance + PIN + Biometric	Medium Assurance Some Confidence	Perform low assurance + Hashed Message Authentication Code
High Assurance Very High Confidence	Perform medium assurance + Cryptographic Key Exchange	High Assurance	Perform medium assurance + Biometric

One of the key requirements for the HSPD-12 (PIV) solution and challenges for legacy PACS is how to seamlessly and automatically determine if a card has been revoked due to a lost or stolen card or the card holder is no longer an employee. The first step of this process is to read the digital certificate stored on the card. The key challenge is how to enable communication between the legacy PACS and the preferred method for the PKI (Public Key Infrastructure) management process. Federal Agencies may use one of the following PKI management options:

1. Internal management of Agency PKI certificates.
2. Use the Federal Bridge as an existing PKI repository.
3. Implement OCSP (Online Certificate Status Protocol)

Setting up communication between a fully functional PKI management process and the legacy PACS to meet HSPD-12 (PIV) requirements is a very large endeavor. As part of a phased approach, an interim solution may be to implement a manual system to manage the agency digital certificates locally until a fully integrated and automated solution is available. Under the manual process, security personnel would review a daily printout of invalid (lost or stolen) certificates and identify those certificates belonging to their staff list. Any revisions are then entered into the enrollment database in the MorphoAccess Enrollment Suite (MEMS). After the information is entered into the MEMS database, it is then pushed out to the individual biometric terminals to remove the biometric templates from the terminals. The Legacy PACS is only updated in the case when a cardholder is no longer employed. This model will also work when there are multiple PACS systems in the single Federal Agency model. The MEMS becomes the single database solution for the multiple PACS platforms.

The final PKI solution requires the development of a PACS software interface to periodically go out and check the appropriate external databases to determine the digital certificates that have been revoked and ascertain whether any revoked certificates match current cardholders.

According to HSPD-12 (PIV), all decisions about PACS are made by the local Federal Agency regarding how to handle visitors. An interim NACI is not required to be stored on the visitor's smart card. During the enrollment process, the agency may decide to grant the visitor full access or limited access. The visitor would also have to be entered into the Legacy PACS with a temporary 4 digit identification number that is associated with the CHUID.

Another interesting feature of the Sagem Morpho reader technology is that there are readers from the same product family for both the PACS and LACS (Logical Access Control Systems). This will enhance the full use of the CHUID for verification as well as greatly reduce integration issues between multiple readers to accomplish the overall smart card implementation.

In summary, Federal Agencies face the daunting task of implementing the HSPD-12 (PIV) requirements on a limited budget. A phased implementation approach using "smart" terminals allows the agency to begin the process of meeting these requirements while leveraging their investment in existing legacy systems. Most importantly, the new "smart" terminals and enrollment software will continue to be a vital part of the overall PACS as additional upgrades are made. Every dollar invested in Sagem Morpho systems will provide lasting value for the Federal Agency.

MorphoAccess™ Standard Access Control Architecture

