



Problem Statement

To use HSPD-12 identity cards at your facility, your security personnel will need a way to download ID card records into the Physical Access Control System (PACS) they use. The best way to do this is with a dedicated, secure data link that connects the on-site PACS with the central office, where cards are issued. But creating this data link can be challenging. You need a solution that can bridge the different technologies and data formats used at each site, and that can provide protection against network and equipment failures.

Background

With the announcement of Homeland Security Presidential Directive 12 (HSPD-12), the U.S. Government has begun the monumental task of implementing a common ID card system for all federal employees and contractors. The new cards, known as “PIV” cards (Personal Identity Verification) and defined by the FIPS-201 standard, promise incredible benefits, including:

Greatly enhanced security. Cards are electronically verifiable and protected by digital certificates, biometric data, and a PIN code.

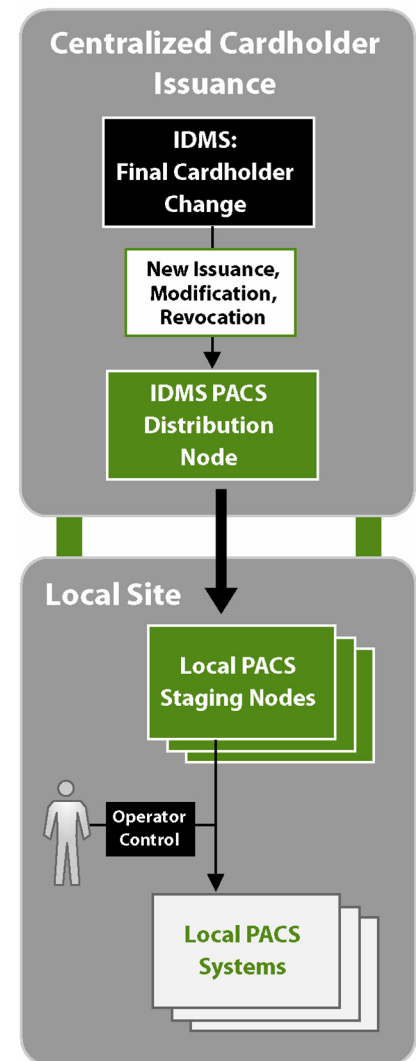
Central management. Cards are issued, tracked and revoked from a central system (the IDMS).

Standardized enrollment and vetting procedures, including rigorous background checks.

But to enjoy these benefits and use PIV cards in daily operations, all federal agencies must first overcome a significant challenge – that of integrating the new centrally managed PIV card systems with the physical access control systems (PACS) already installed at geographically dispersed buildings and campuses.

For many agencies, the integration challenge is made even more difficult by the multitude of various PACS systems in use at their secure locations. These longstanding, proprietary PACS systems must now be integrated together and interconnected for the first time.

How do you populate your PACS systems with HSPD-12 credential data without interrupting operations?



The ideal way to integrate a PACS system with a centralized ID card management system (IDMS) is with an automated program that regularly pushes PIV card data over a network from the central IDMS to the local PACS. With the right 'data connector' technology in place, the IDMS and PACS databases can be integrated into a unified, automated system.

Downloading data from the IDMS to the PACS

One way to transfer data between the IDMS and the PACS is through a process known as 'bulk provisioning' – the act of periodically downloading IDMS data, in bulk, to every PACS facility. This download process could be triggered automatically whenever a cardholder is added, updated, or deleted from the IDMS; alternatively, downloads could be performed on a regular schedule (for instance, a nightly batch process).

Either way, it is possible to build a system to provide timely updates to PACS facilities, with a robust defense against equipment failures and outages in the data network. Every PACS system can be kept up-to-date, even if the connection to the central IDMS is intermittent.

With bulk provisioning, local security personnel can regularly review new cardholder data, and assign their cardholders the appropriate access permissions to any part of the local facility. And because the PIV card data is downloaded before the cardholders arrive at the facility, the local security officer can pre-assign access privileges in bulk too – well before new cardholders arrive at the facility. This enables the local security office to prevent long delays and lineups at the security gate, which would otherwise be quite problematic, especially during the initial wave of any PIV card rollout.

In some cases, it may even be possible to completely automate the process, so that cardholder data and local security permissions are added directly to a given PACS system. If the local security rules are well understood by the central administrator, or if any of the rules have been standardized, then cardholders, badges and permissions could be automatically configured in the PACS system using a centrally managed, rules-based policy engine. Such a system could be implemented in cooperation with the local security office, with a logging system that allows the local office to quickly and regularly review all changes made to the PACS system.

In order to illustrate the benefit of bulk provisioning, consider the process of assigning local access privileges, from the security officer's point of view. The diagram below depicts a computer screen that could be presented to a security attendant, immediately after a successful bulk provisioning cycle:

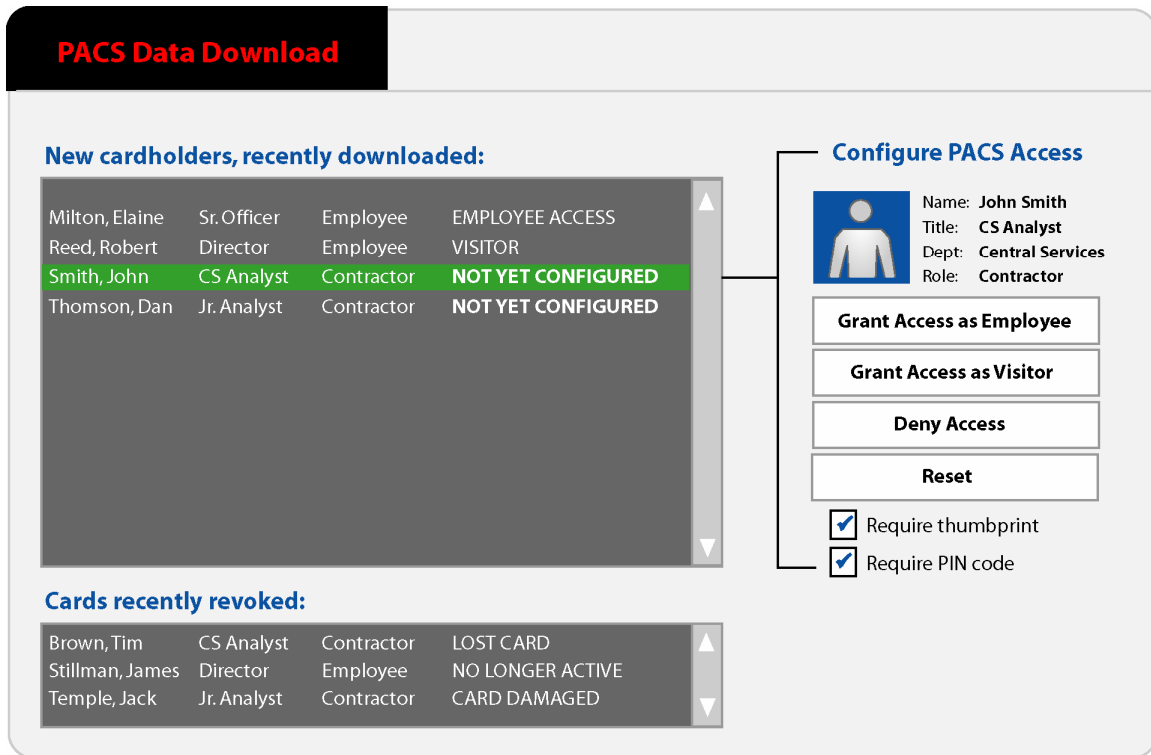


Figure 1 – a Provisioning Console display screen, made available to local security officers

This screen would be generated by a secure console, connected to the PACS system, and would present the security officer with data about every PIV cardholder recently downloaded by the system. The screen would also include buttons and controls that enable the security officer to assign access privileges to each cardholder. And, the screen would include a list of previously configured cardholders whose cards were recently revoked.

This screen could be consulted every morning before new cardholders arrive, and subsequently reviewed by every security attendant at the beginning of their shift.

How the process works

The process of bulk provisioning includes a number of interactions between central and local data systems and various personnel. The following diagram shows the sequence of events:

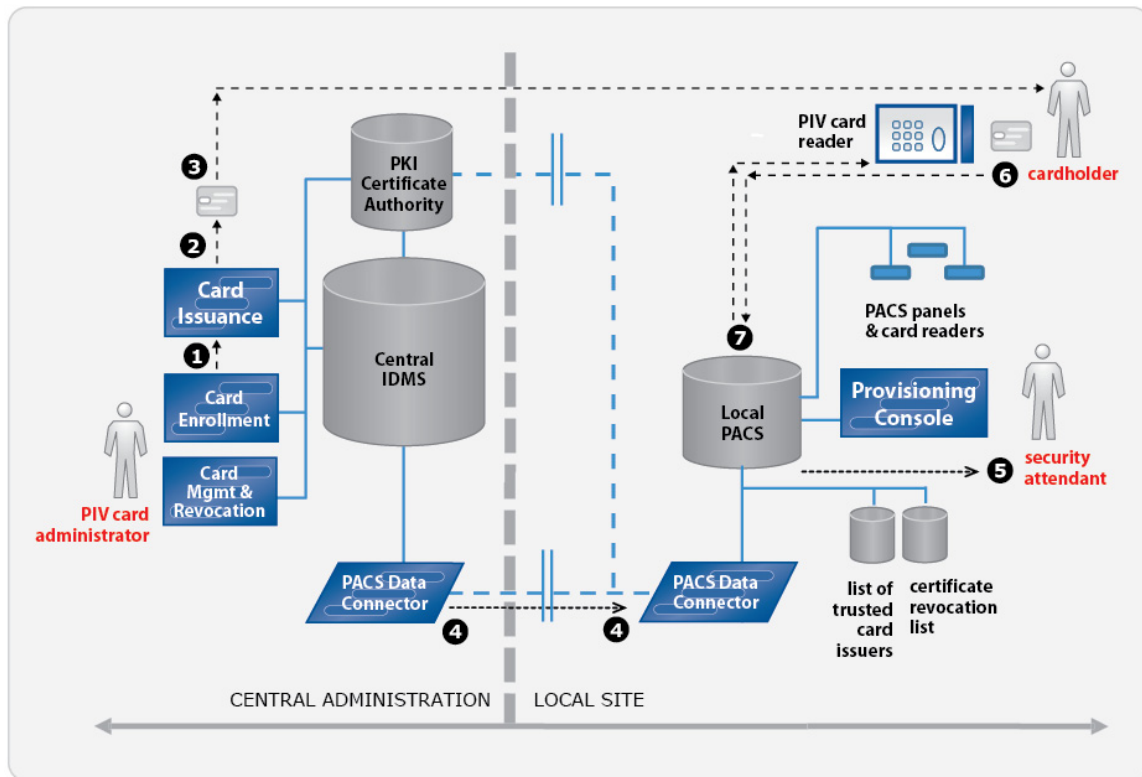


Figure 2 – the bulk provisioning process

- Step 1** – Central PIV card administrator enrolls a new cardholder in the system. During the enrollment process, the cardholder will undergo a variety of vetting steps.
- Step 2** – After a successful vetting, the administrator triggers creation of a new card, which is then physically manufactured, encoded with PIV card data and electronically signed with PKI certificates.
- Step 3** – The new PIV card is delivered to the cardholder.
- Step 4** – During the next bulk provisioning cycle, the PIV card's data is downloaded to the local PACS facility.
- Step 5** – After bulk provisioning is complete, the local security attendant can review the new PIV card entry and pre-assign appropriate local access privileges, based on the cardholder's role and employment status.
- Step 6** – Cardholder arrives at the facility, and attempts to use PIV card for the first time.
- Step 7** – PACS reader automatically inspects the data on the PIV card, compares it to the data previously downloaded, and then determines whether to grant access to the cardholder.

The PACS Data Connector

As shown in the above diagram, the bulk provisioning process relies on a set of PACS Data Connectors to feed data from the IDMS to the PACS system. PACS Data Connectors form the pipeline of cardholder data between the IDMS and the PACS systems, and are designed to do the following:

- ⇒ distribute and synchronize new, modified, or revoked badge information between the IDMS and PACS
- ⇒ manipulate the data in the various proprietary PACS systems used by the agency
- ⇒ withstand intermittent network connections and recover from outages and equipment failures
- ⇒ log failures, and alert administrators and security attendants as failures occur.

PACS Data Connectors can also be designed to download data from PKI certificate authorities – including certificate revocation lists, which according to the FIPS-201 standard must be regularly downloaded and processed by the PACS.

PACS Data Connectors work by spanning the network connection between the central IDMS and the remote PACS system. A robust Data Connector solution will include at least two nodes – one connecting directly to the IDMS, and another connecting to each of the remote PACS systems. In this way, the Data Connectors can work together to bridge the gaps caused by slow or intermittent networks, and shield the IDMS and PACS systems from equipment failures.

PACS Data Connectors could be provided by each of the different PACS vendors, or could be custom-built by the implementer of the IDMS. Alternatively, a vendor-neutral Data Connector could be provided by a single 3rd party technology provider, offering data connections to the most popular PACS systems and IDMS implementations. For an agency using multiple PACS technologies at their facilities, a vendor-neutral solution will cost less and will be easier to implement and maintain.

Today, several solutions exist for providing data connectivity to PACS systems. But most of these systems are very limited in their functionality. Most provide only a very simple data interface, without offering complete, fault-tolerant, end-to-end connectivity to the IDMS. A few of these systems provide a subset of the higher-level functions required of a PACS Data Connector (such as functionality for downloading PKI certificate data and revocation lists) but by themselves do not constitute a complete solution. And most of these systems are compatible with only a single vendor's PACS technology.

By contrast, one solution that provides both the rich functionality required of a PACS Data Connector, and wide compatibility with multiple PACS vendors, is Physical Security Interconnect (PSI), a vendor-neutral product provided by

Enterprise Air. PSI is already the leading solution for data connectivity to PACS systems, and is compatible with the majority of PACS systems currently in use.

Enterprise Air's PSI solution provides a robust set of building blocks for creating PACS Data Connectors, with a fault-tolerant failover mechanism, and a heart-beat monitoring system that can immediately alert a system administrator to connectivity and equipment failures. With PSI, it is now straightforward to implement a reliable PIV data connection, and deploy it quickly and simultaneously to a variety of PACS sites.

A Unified Data Connector

To understand the benefits of a unified, vendor-neutral Data Connector solution, and appreciate the breadth of requirements it must fulfill, consider the primary problems that a PACS Data Connector must solve:

- 1) It must be able to read data from the IDMS, and monitor changes to the data.
- 2) It must be able to add, delete and change data records stored in the PACS system's database.
- 3) It should be able to pause its operation when the network is down or when the IDMS or PACS are unavailable, and then resume at a later point.
- 4) It must be able to log and report errors during data.

Consider first the problem of connecting to the IDMS, and the benefits of a unified solution. Every PACS Data Connector must provide a secure connection to the IDMS, and have the ability to issue queries to it, listen for updates, and understand the IDMS's native data format. Given the sensitivity of the data, and the number of other systems that must also connect with the IDMS (such as enrollment, card issuance, and certificate management), it is highly desirable to keep the data interface simple, and connections limited to the smallest possible number.

If each PACS system implements its own data connector, the complexity of the system can quickly grow, since each system must open its own unique connection to the IDMS, thereby increasing maintenance costs and security risks. By contrast, a vendor-neutral Data Connector can consolidate all the PACS system behind a single data interface, shielding the IDMS from complexity and reducing the exposure to security threats.

On the other end of the data pipeline, the Data Connector needs to manipulate the data records in the PACS system. This requires that the Data Connector know how to properly connect to the PACS database, format the data, and speak the right protocol for performing PACS data transactions. Today, every one of the most popular PACS technologies offers its own unique mechanism for manipulating its cardholder data. If a new PACS system is ever added to a facility, a new Data Connector must be added that can interface with it. As PACS technologies evolve, this may require the upgrade of one more Data Connectors.

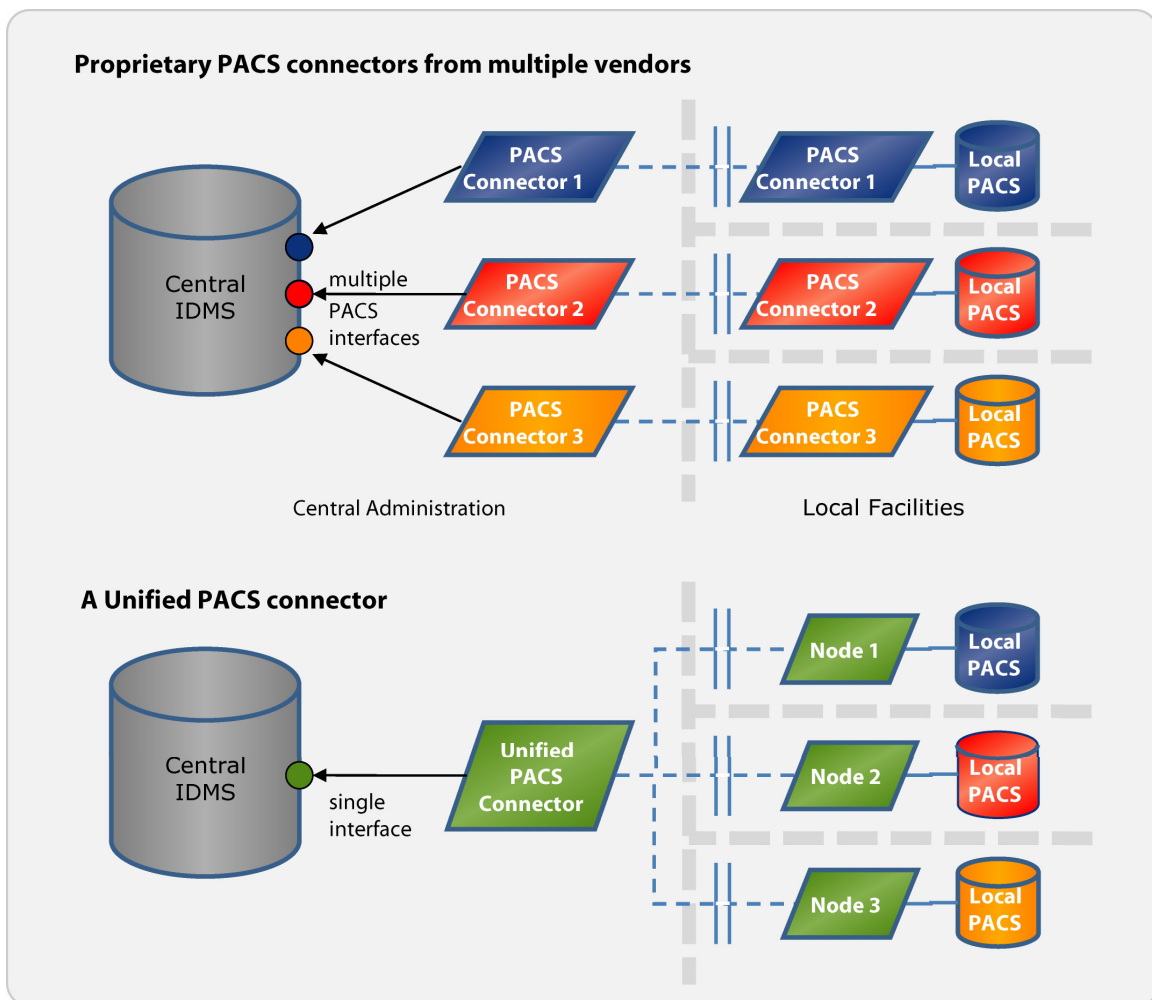


Figure 3 – the benefits of a unified, vendor-neutral PACS Data Connector solution

With a unified Data Connector solution, the PACS Data Connectors can be built to communicate with each other using a common, vendor-neutral protocol, thereby shielding the rest of the Data Connectors from changes in any one PACS system. That way, when a new PACS system is brought online, the only Data Connector affected is the one directly connected to it.

Finally, consider the challenge of providing a fault-tolerant data connection. A Data Connector must be built to withstand network failures and equipment

outages, and to report those failures to an administrator. Creating a fault-tolerant system requires careful planning, implementation and testing. And effective error reporting requires every node to be integrated into the monitoring and alert mechanism of the larger system.

If each PACS system implements its own data connector, then every PACS integrator must solve these problems separately, resulting in potentially redundant effort and higher costs. By contrast, with a single Data Connector solution, the fault-tolerance mechanisms are implemented only once. A single implementation limits the possible points of failure, and enables the PACS and IDMS integrators to remain deeply focused on their core functions.

Fault Tolerance and Monitoring

To illustrate the potential for complexity in a system with multiple PACS Data Connector solutions, consider the effort required to provide fault tolerance in a single solution. Every Data Connector must provide two forms of fault-tolerance:

- 1) Protection against network outages
- 2) Protection against equipment failure

The first issue, protecting against network outages, requires a mechanism for detecting failures, pausing data transmissions, and resuming them later (when the network becomes available again). This requires each node in the system to preserve a copy of each record it wants to transmit, in the form of a queue. The queue keeps track of which records have been transmitted, and which ones have not, so that if a transmission is lost or broken, the data can be resent later in the proper sequence.

Such a queuing system must be carefully designed to account for different network configurations and data update scenarios. For example, if a central node is required to talk to several local nodes at different PACS locations, then its queues must be designed to separately track the download status for each receiving node.

Other factors may further increase the complexity of the queuing system. For instance, if the central and local nodes are expected to exchange data in both directions, then their queuing systems will need to include separate queues for inbound and outbound data. Also, if the design of the overall system allows two nodes to modify a single data record at the same time, then the nodes and their queues must be designed to handle data conflicts. And, each node must be designed to cope with its storage constraints, so that data records can be removed from the queues after a successful transmission, and regenerated in the event that a receiving node has become corrupted or very out of date. Finally, the queues must be designed to provide fast data transfer, without significantly affecting performance when the network is healthy.

To meet all of these constraints requires a very careful design of the queue, and the internal software used to manipulate it.

The second issue – equipment failure – can also be addressed by queues. But many IDMS and PACS systems also rely on a technology known as clustering. In a clustering solution, each node is duplicated in the system, with a primary node and a backup. In the event that any primary node fails, its backup node can immediately start processing transactions. This is typically accomplished by copying all transactions handled by the primary node to the backup node, so that at a moment's notice, the backup node can pick up exactly where the primary node stopped.

IDMS and PACS systems often implement their own clustering mechanisms, each with its own set of primary and backup nodes. To connect to these systems, a PACS Data Connector must be intelligent enough to recognize when an IDMS or PACS has shifted operations to its backup node, and shift its own operation appropriately.

Such design considerations must be carefully weighed by the system administrator, and it is desirable to have a Data Connector solution with the flexibility to support many clustering configurations.

Enterprise Air's PSI technology can provide a highly fault-tolerant, vendor-neutral PACS Data Connector solution. PSI implements fault-tolerance using queues and clustering mechanism like those described above, and its fault-tolerance mechanisms can be easily integrated with those provided by a PACS or IDMS. PSI components are highly configurable and have been proven to work in a variety of network and equipment configurations, with very high reliability and performance.

PSI also implements a heart-beat mechanism for effective monitoring and logging. With this mechanism, each PSI Data Connector can be configured to issue a simple 'heart-beat' message with a short request-response sequence to a neighboring node. PSI can issue heartbeats to other PSI nodes, or to a PACS system, or an IDMS. These heartbeats can be configured to occur on a short interval, with failures (timeouts) reported immediately to neighboring nodes and ultimately to a central monitoring system.

Overall, PSI from Enterprise Air provides a great case study of a robust, highly reliable and widely compatible solution for creating PACS Data Connectors. Its proven ability to interface with widely varying PACS technologies, and its fault-tolerant design, provide a critical component for fulfilling the promise of HSPD-12, and connecting the new wave of central IDMS systems with the many PACS systems in use today.

About Enterprise Air

Enterprise Air is a leading provider of solutions for the physical security and emergency first responder segments of the Homeland Security market.

The Company delivers an integrated suite of data connectivity and mobile software applications that address the security and crisis management needs of roaming guards, law enforcement officers, and emergency response workers. Examples of these applications are Physical Security Interconnect (PSI), Mobile Badge Management (MBM), RapidCount Emergency Management System, Alerting, and Incident Reporting applications. The PACS Data Connectors described in this document provide a great example of a security solution that can be built quickly using these building blocks.

For more information, including detailed product and solution information, contact us at:

Enterprise Air
259 West 30th Street, 9th floor
New York, NY 10001

www.enterpriseair.com
+1 212 941 1988
info@enterpriseair.com

Copyright ©2007 Enterprise Air, Inc. All rights reserved.