

Problem Statement

Before your security personnel can start processing HSPD-12 identity cards at secure entry gates, they must have a way to register the cards in the on-site Physical Access Control System (PACS) they use. Registering cards is far from automatic, since cards are issued by a central office, using a different system. But, there's a solution that makes it easy - an on-site Provisioning Kiosk, which can quickly extract data from an HSPD-12 identity card, and inject it into the PACS.

Background

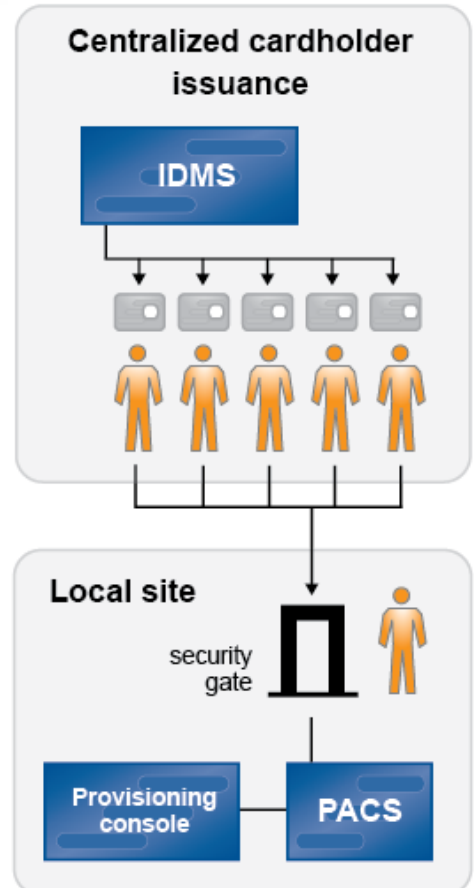
To secure any building or facility, one must have a way to quickly and accurately identify all the people who enter it. With the issuance of Homeland Security Presidential Directive 12 (HSPD-12), federal agencies will soon have a common ID card standard (the "PIV" card standard, as defined by the FIPS-201 specification) that will greatly facilitate this task. The new ID card standard promises many benefits – including a more secure card, a standardized enrollment and vetting procedure, and centralized administration.

But deploying this standard also poses many challenges. One key challenge is the task of integrating the new cards with the multitude of physical access control systems (PACS) that local facilities use.

PACS systems are a critical component for enabling security at a site, since they control the electronic gates and doors where cards will actually be used. But HSPD-12 cards are issued from a different system (the identity management system or IDMS), by a central administration office typically located elsewhere. So before a security officer can grant building access to a cardholder, the cardholder's centrally-issued identity data must first be registered, or 'provisioned', within the local PACS system.

At some facilities, it may be possible to register the data automatically, by building a dedicated, secure data link connecting the PACS to the centralized identity management system (IDMS). But more often than not, such a link will not be available, perhaps due to a lack of networking infrastructure, or to technology constraints imposed by the PACS system, or to other deployment

Are your secure facilities ready for the approaching wave of HSPD-12 cardholders?



hurdles. And even if such a link were available, it still would not accommodate all of the 'unexpected' cardholders and visitors who arrive at a site every day. In such cases, the burden of manually registering cardholders in the PACS system falls to the local security officer, who must perform an often tedious data entry procedure any time a cardholder visits their facility for the first time.

Registering cardholders by hand can create difficulties for both the security officer and the cardholders. A manual registration process can create bottlenecks at the security gate, generating significant wait-times during any PIV card rollout. The process can also create frustrating delays for regional managers and contractors who must travel often to a variety of different physical sites. And it can create hurdles in providing visitors with access to a site. Worst of all, the manual process leaves room for error and increases security risks.

The PACS Provisioning Kiosk

Fortunately, it is possible to solve these problems. A great benefit of the FIPS-201 security standard is that it requires the cardholder's authentication data to be stored electronically on the access card itself. This makes it possible for a local security attendant to scan and verify the cardholder's ID data, and to quickly add that data to the local PACS system, without requiring any network connection to the IDMS – the only equipment needed is a low cost electronic card reader and any PC. In this scenario, the security attendant, having used the card reader to verify and store the identity of the new cardholder, can then choose whether to give the cardholder access to the physical site (perhaps by checking a manifest, or by reviewing the authorization data already stored in the local PACS). The security attendant can then store this access decision directly in the local PACS database, along with the newly stored electronic ID.

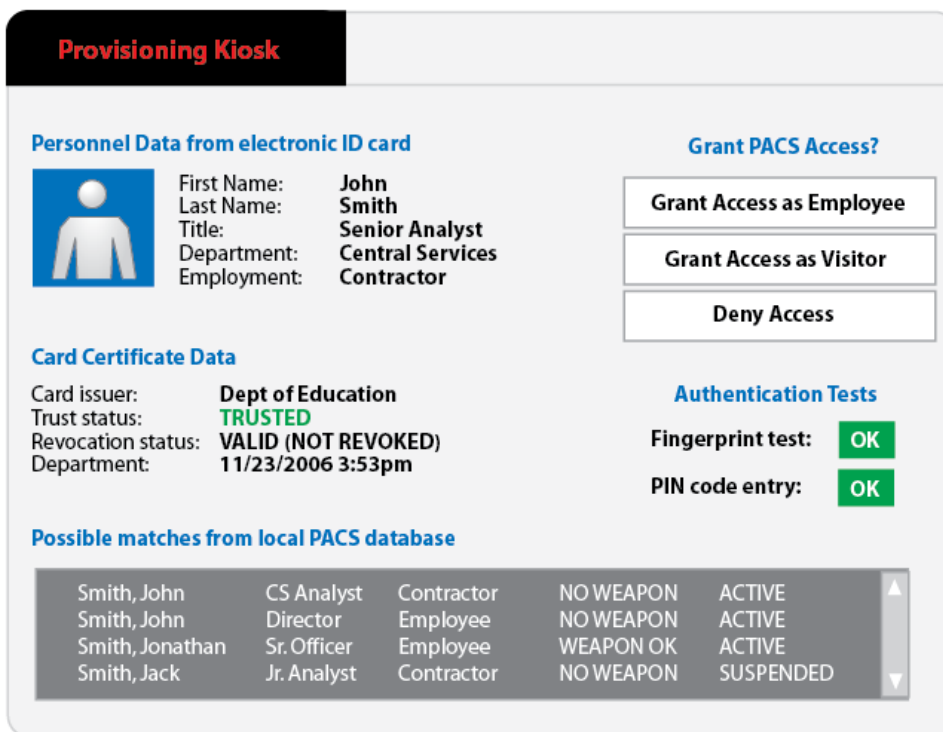


Figure 1 – a sample screen displayed by the Provisioning Kiosk

Optional, automated PACS record lookup

A highly effective solution for fast, secure local provisioning can be provided by an automated Provisioning Kiosk (see Figure 1 on previous page). This kiosk provides a link between the card reader and the local PACS system, and can present the security attendant with a visual representation of the authentication data read from the card. Using this secure ID data, the attendant can then decide whether to grant site access, and store that decision in the PACS.

The diagram below (Figure 2) demonstrates how the kiosk connects with the PACS and IDMS systems, and enumerates the steps in the local provisioning process:

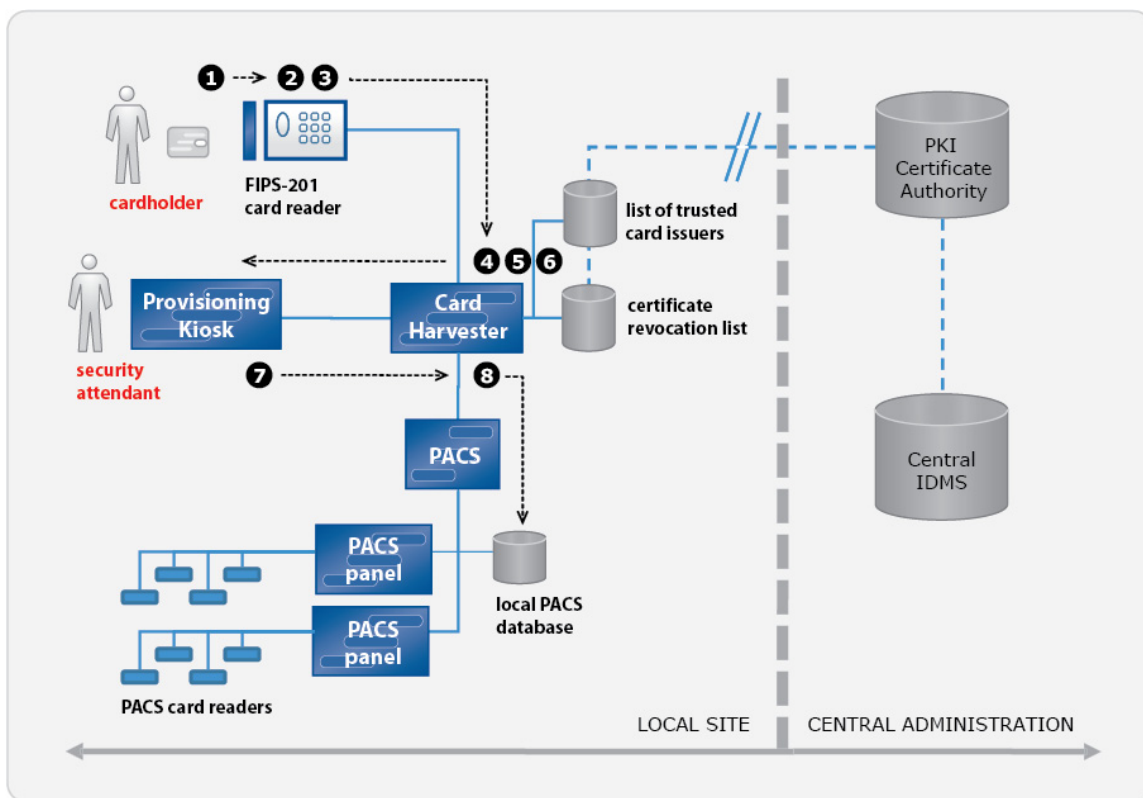


Figure 2 - local provisioning process using the Provisioning Kiosk

- Step 1** – Cardholder inserts electronic ID card into card reader
- Step 2** – Cardholder enters private PIN code
- Step 3** – Cardholder submits biometric verification (fingerprint test)
- Step 4** – Card data 'harvester'* examines and extracts data from the card reader.
- Step 5** – Card harvester performs certificate authentication to verify that card ID has been signed by a trusted issuer

- Step 6** – Card harvester* checks to see if the card's certificate has been revoked, using revocation information made available by the PKI that generated the certificates.
- Step 7** – Provisioning kiosk presents a screen to security attendant
- Step 8** – Security attendant approves access to the cardholder, and stores the decision in the PACS

* In this solution, a 'Card Harvester' component translates the data from the card into a format compatible with the local PACS system. This Harvester also has a data interface to the local PACS system, with the ability to add, change, delete, and query records in the local PACS database.

The PACS Provisioning Kiosk (including the card harvester) could be provided directly by the various PACS vendors, or built by the IDMS implementers. Alternatively, the kiosk could be provided by a single 3rd party technology provider, offering a vendor-neutral solution with data connections to the most popular PACS systems and IDMS implementations.

One such technology solution is Physical Security Interconnect (PSI), provided by Enterprise Air, which provides a rich set of technologies for building data connections between IDMS and PACS systems. PSI is the leading solution for data connectivity to PACS systems, with the ability to query and manipulate cardholder data in all of the top PACS systems in use today. With PSI, it is now straightforward to implement a reliable local provisioning kiosk, and deploy it quickly and simultaneously to a variety of PACS sites.

Kiosk Scenarios

Once delivered to a local security facility, the Provisioning Kiosk could be configured for any of several local provisioning scenarios, including:

Unattended self-provisioning – the kiosk could be configured to automatically provision and grant site access to the cardholder, following a successful biometric/PIN challenge, as long as the kiosk can match the data on the card with a data record in the local PACS database. The kiosk could be configured with various rules for mapping data fields on the card with data fields in the legacy PACS database.

Assisted self-provisioning – the kiosk screen could be presented to every cardholder, within visual sight of a local security attendant. The kiosk could then be configured to automatically provision and grant access to cardholders that match a data record in the PACS database. If the kiosk cannot find a match, it could alert the security attendant, who would then be permitted to step up to the kiosk, submit his or her own authentication, make a decision about site access, and then create a new record in the PACS database.

Controlled provisioning – the kiosk could be positioned behind a security gate, such that it could only be operated by the security attendant. The attendant would then review and approve all provisioning activity.

Visitor kiosk – the kiosk could be configured to grant automatic visitor access to any cardholder presenting a valid ID card and a valid biometric and/or PIN code.

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.

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.