



## Problem Statement

There has been much discussion of how to issue HSPD-12 PIV cards, including how to vet the identity of personnel that carry them. But to actually use an HSPD-12 identity card, your security personnel must have a way to electronically read it and verify the credential.

For most security officers, this is a big change, since the information they care about will no longer be printed on the face of the card. Security personnel will need an easy, reliable way to read data from a PIV card, verify its electronic signature, and look up the cardholder's record in the on-site Physical Access Control System (PACS).

In many cases, the ideal solution is a portable handheld card reader that can read and compare data from all the relevant data systems.

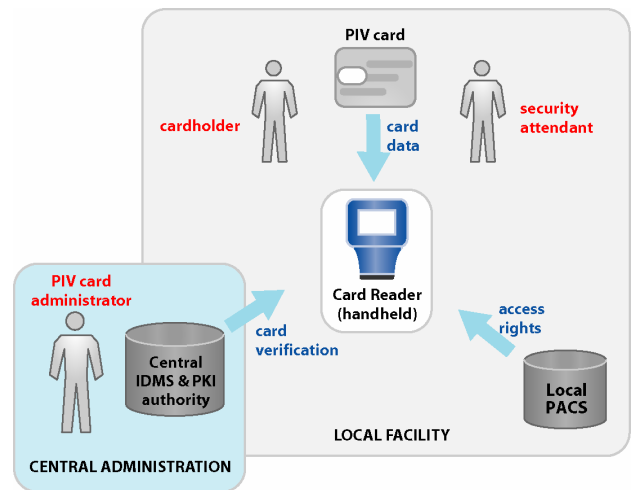
## Background

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 system, defined by the FIPS-201 standard as the Personal Identity Verification (PIV) card system, promises incredible benefits – a vastly more secure card, electronically verifiable, that can be issued, tracked and revoked using a centralized identity management system (IDMS); and a standardized process for enrolling cardholders and vetting their identities.

For the first time, buildings and campuses in different locations can be interconnected and share a common notion of identity. The new benefits will be felt not just by the federal government, but also by state and local agencies, and by corporations in the private sector, which will be able to draw new solutions and technology from the standard in order to improve their own security.

But to enjoy these benefits, all PIV card adopters will need to overcome a number of formidable execution challenges.

How can you quickly deploy HSPD-12 card readers, connect them to central administration, and integrate them with local access control systems?



The first challenge stems from the design of the card itself: in a PIV card system, detailed information about the cardholder is no longer printed on the face of the card – it is embedded electronically. To inspect that data, every security attendant will need a PIV-compatible card reader that can quickly retrieve data from the card and verify it.

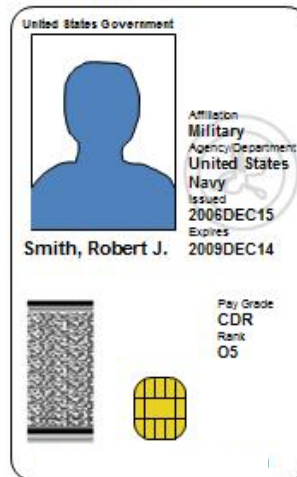
#### OLD CARD

Important identity data is visible on card surface



#### NEW HSPD-12 CARD

Most data must be accessed via electronic reader



**A comparison of old access cards vs. new PIV cards. Notice that some important cardholder data, such as weapons clearance, is no longer visible on the card – it must be read electronically.**

The second challenge arises from the multifaceted nature of the data. Cardholder data comes in two flavors – authentication data, which verifies the identity of the cardholder and the validity of the PIV card; and authorization data, which declares the facilities and resources the cardholder has permission to access. Most often, these distinct facets of the data are stored and maintained in different systems. While identity data is maintained centrally (in the IDMS) and stored securely on the PIV card, a cardholder's physical access privileges are typically assigned and stored at the local facility, in its Physical Access Control System (PACS). To fully and automatically process a cardholder, the PIV card reader should be flexible enough to pull data from multiple sources – including the central IDMS, the associated PKI certificate authority, and the local PACS – and then compare it to the data on the card itself.

Finally, local security personnel must often overcome a third challenge – a lack of infrastructure. At some facilities, it may not be cost-effective or even possible to install a permanent card reader and electronic turnstile; consider for example a leased building that does not permit the agency to make structural changes. And many agencies need to manage temporary sites or roaming perimeters, where permanent security gates simply do not exist.

To solve these problems, a federal agency must have access to a card reader solution that can quickly process PIV cards, reliably connect to local and central data systems, and enable rapid deployment to any secure facility or physical perimeter.

And most important of all, the card readers must be fast and very easy to use. This is especially critical because security officers will no longer be able to rely on a visual inspection of the card to gather certain important details about a cardholder (such as vital statistics, or permission to carry a weapon - see picture on the preceding page). Every security office will need a card reader that it can quickly and easily adopt.

One way to meet these requirements is to construct the card reader as a mobile handheld device. A handheld can be deployed anywhere, and can operate without a network connection by periodically downloading fresh data about cardholder status, access permissions, and other customizable attributes of the cardholders. The handheld can be programmed with software that is able to extract all data from a PIV card, validate its PKI certificates, and compare the data to permissions information stored in the PACS and other attributes stored in the IDMS. The handheld can also be designed to capture a log of all successes and failures, and upload these transactions to the PACS and/or IDMS.

Since such a handheld can process two kinds of data – identity data and access permissions – and perform a variety of functions on both, we can refer to it as a Hybrid Handheld solution.

## **The Hybrid Handheld – how it works**

The Hybrid Handheld derives its value from the ability to combine and clearly visualize data from four different systems – the central IDMS, the PKI system, the local PACS, and the PIV card itself.

The first system, the IDMS, creates the common, agency-wide concept of identity by enrolling cardholders, assigning them cardholder-unique IDs (CHUIDs), and issuing PIV cards. After a rigorous enrollment and vetting process, the IDMS adds the cardholder's identity data, along with the CHUID, to a central database. With this database, the IDMS becomes the authoritative master of all cardholder identity data, driving all other authentication systems, including PKI data. The Hybrid Handheld card reader must be able to process CHUIDs and records issued by the IDMS, and ideally should be able to receive updates directly from the IDMS.

The second system, the PKI authority, safeguards data on the PIV card by issuing digital certificates, which are used by the IDMS and its card issuance systems to sign the data on each PIV card as it is created. These digital signatures enable a card reader to test the integrity of the data, and ensure that the card was issued from a trusted source, thereby protecting the PIV card

from forging and tampering. The signatures also provide a convenient way to revoke a card, since PKI authorities regularly publish certificate revocation lists to the internet. This means that to revoke or cancel a card, the IDMS administrator need only revoke the card's certificate; from that point forward, anyone with access to the internet can verify the revocation status of the card, without ever connecting to the IDMS. In order to test the authenticity and revocation status of a PIV card, the Hybrid Handheld must be able to download and process data from the PKI authority.

The third data component is the PIV card, which contains even more data to protect itself from unintended use. PIV cards are required to store fingerprint biometric data and a secure PIN code to validate the cardholder; this data is likewise signed, encrypted and stored on the card. To use this data, and ensure that the PIV card is only used by the cardholder it was intended for, the Hybrid Handheld must be equipped with a biometric fingerprint reader and a PIN code entry function to verify the cardholder.

The fourth system, the Physical Access Control System (PACS), links the PIV card to a facility's electronic locks, gates, and other physical access control points. The PACS maps the CHUID to the cardholder's access rights. In order to authorize the cardholder, and ensure that he or she has permissions to enter a given facility, the Hybrid Handheld must be able to read locally issued PACS records and compare them to the PIV card records issued by the IDMS.

**A summary of the data components used in a PIV card security system.**

<b>Data Source</b>	<b>What data it contains</b>	<b>Who controls it</b>
<b>PIV Card</b>	<ul style="list-style-type: none"> <li>• Personal data – vital stats, photo</li> <li>• Organizational data – role , classification</li> <li>• Card data – expiry date, PKI signatures</li> <li>• PIN code and biometric data</li> <li>• Cardholder unique ID (CHUID)</li> </ul>	<b>Central Card Administrator</b>
<b>IDMS</b>	<ul style="list-style-type: none"> <li>• Master copy of all PIV card data</li> <li>• Status of cardholder (enrollment, revocation)</li> <li>• Log of all card data transactions</li> </ul>	<b>Central Card Administrator</b>
<b>PKI</b>	<ul style="list-style-type: none"> <li>• List of revoked PKI certificates (driven by IDMS)</li> </ul>	<b>Central Card Administrator and PKI Certificate Authority</b>
<b>PACS</b>	<ul style="list-style-type: none"> <li>• Local access permissions, such as:               <ul style="list-style-type: none"> <li>- physical security access permissions</li> <li>- equipment/weapons clearance</li> <li>- guest/visitor privileges</li> </ul> </li> <li>• Connections to electronic locks and turnstiles</li> <li>• Log of all local access events</li> </ul>	<b>Local Security Office</b> <b>(control could be shared with Central Administrator, depending on security policy)</b>

The Hybrid Handheld can simplify the integration of all four systems by extracting data from each of them, comparing the records, and displaying all the data to the security officer in a unified user interface. Consider the following sample screen, which depicts how the handheld could present data about a cardholder from all four systems on a single form. In this example, the handheld has already read the PIV card, extracted its data, reviewed its certificate's chain of trust and compared it to a recently downloaded PKI revocation list, and used the card's CHUID to look up the PACS record. The handheld then displays all the data in an easy-to-read format. The handheld could also compare the PIV card data to data downloaded from the IDMS, thereby providing extra security, and then offer a link to display the IDMS record, which contains even more detailed information about the cardholder. In this example, the handheld also includes an on-board thumbprint reader and a PIN pad, so that the local security officer can test the identity of the cardholder and see the results on the screen.



To fulfill all of these functions, the Hybrid Handheld must be able to connect and retrieve data from the appropriate systems. Complicating matters is the fact that the IDMS, PKI, and PACS systems are typically managed by different

parties and housed in separate locations. Worse, the PACS systems themselves are often dispersed, with the possibility that each facility is using its own unique system; a Hybrid Handheld with PACS lookup capabilities must be able to connect to the PACS system at every facility where it will be used.

Fortunately, the concept of the Hybrid Handheld is very malleable; an agency could decide to implement only a subset of the functions described above. If the agency's security policies are flexible, it may be feasible to adopt a handheld card reader that only connects to one or a few of these systems, or perhaps none of them (only reading data from the PIV card itself). Such policy decisions could be made to reduce the amount of integration required, and simplify the implementation effort. The chart below provides a useful guide to analyzing the pros and cons of a reduced-functionality Hybrid Handheld.

**Options for integrating the Hybrid Handheld card reader with other data systems.**

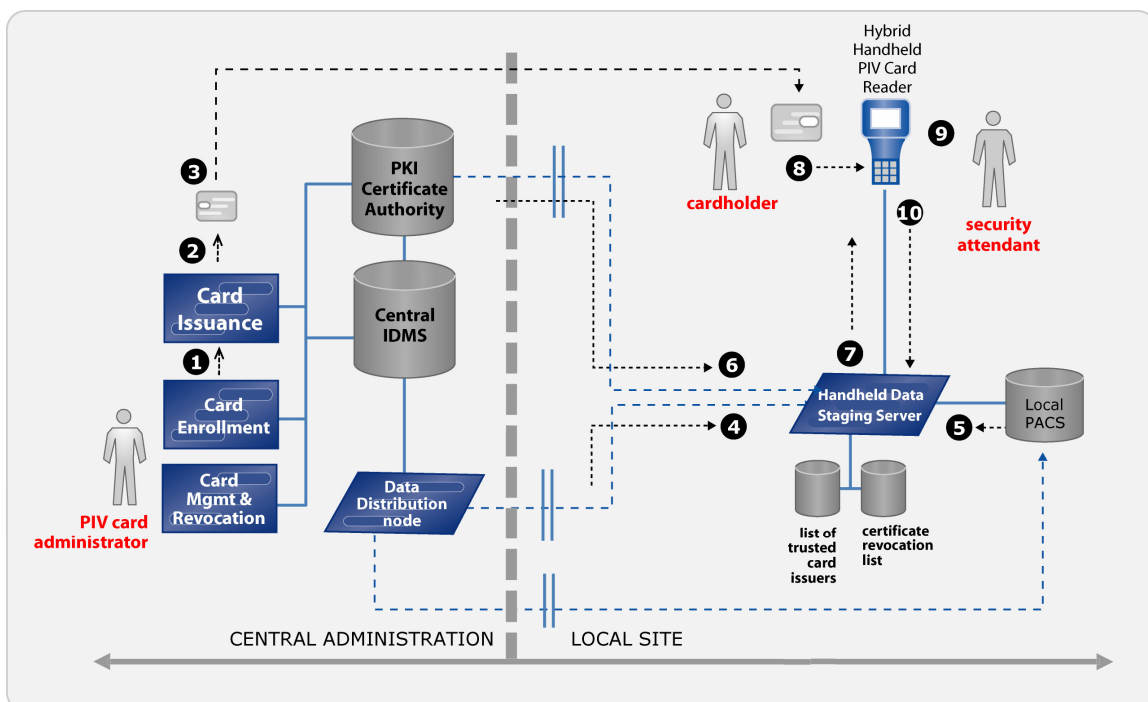
Data Source	Data the Hybrid Handheld could use	What the Hybrid Handheld could do with it	Without this data...
PIV Card	Authentication tests: biometric/ fingerprint data and PIN code	Verify that the cardholder is who he/she claims to be	...the security attendant cannot reliably verify the cardholder's identity.
	Identify data stored on the card	Review personal information about the cardholder	But...if policy allows, the attendant can still visually inspect photograph & name on card, and manually query permissions using separate PACS console interface.
IDMS	Master record of cardholder identity, and enrollment status of the card	Review additional information about cardholder and his/her status	...the security attendant can still check enrollment and revocation status using data from PKI authority.
PKI	Digital certificate chain of trust (pre-provisioned on handheld)	Verify that the card was issued from a trusted source (Useful to detect forgeries and verify PIV cards from other agencies)	...the security attendant cannot determine whether the card issuer is trusted.  But, if policy allows, the attendant could accept cards based on other criteria, such as PACS match, or secondary form of identification.
	Certificate revocation lists (useable across all agencies)	Verify that the card has not been revoked	...the security attendant can still check enrollment/ revocation status using data from IDMS, or the PACS (if the PACS has access to PKI data).
PACS	Local access permissions	Verify that the cardholder has permission to enter the facility.	...the security attendant cannot automatically determine if the cardholder has permissions to access to the facility.  But...if policy allows, the security attendant could manually query the record using a separate PACS console interface.

To implement its functions, the Hybrid Handheld must first possess a mechanism to download and store a copy of the data records from the relevant data systems. Because the handheld has limited storage, it can greatly benefit from the presence of a staging server, which can connect to the various systems, extract the subset of data needed by the handheld, and compress it. Ideally, the staging server will be installed at the local facility along with the handhelds, so that it can manage all of the data connections and shield the handheld implementation from complexity. This makes it easy for the handheld to dock and connect to the staging server, and receive regular updates of data.

Second, the Hybrid Handheld and its staging server must be conversant in the data protocol used by each system it connects to. Connecting the handheld to PACS systems may pose its own unique challenge, since an agency may be using several different PACS technologies across its many facilities. Today, there are many different PACS technologies in common use, each with its own data protocol and data connection mechanism. To be useful across an agency, a Hybrid Handheld must be able to speak to all of the agency's PACS systems.

Finally, the Hybrid Handheld must be able to log all card reader activity and report it back to the IDMS and PACS systems. This is critical so that both local and central administrators can audit how PIV cards are used, and be notified of discrepancies between the IDMS and their local PACS. To create logs, the handheld typically gets help from the local staging server, which can cache new log entries and upload them to the IDMS and PACS systems whenever a network connection is available.

The diagram below illustrates the entire process. This scenario shows the entire lifecycle of a PIV card, how its data is transmitted across the system, and then used by the Hybrid Handheld:



### **PIV card issuance:**

- Step 1** – PIV card administrator creates new cardholder record, and performs a vetting procedure to review that person's identity.
- Step 2** – Once the vetting procedure is complete, PIV card administrator triggers creation of a new card, which is then printed, encoded with the cardholder's identity data, and signed with PKI certificates.
- Step 3** – PIV card is delivered to the cardholder.

### **Data collection at the staging server (each step is optional, depending on the functions implemented by the handheld):**

- Step 4** – On its next download cycle, the staging server could collect the new PIV card record, along with its CHUID. (This record can also be downloaded automatically to the PACS, where the security officer can assign access rights to the cardholder.)
- Step 5** – The staging server could connect with the PACS, and download all new or updated PACS records.
- Step 6** – The staging server could connect to the PKI authority to frequently download the latest certificate revocation list. (These revocation lists are usually quite large and must be significantly compressed before they can be stored on the handheld.)
- Step 7** – The Hybrid Handheld is docked, and downloads any new or updated CHUIDs, PACS records, and compressed revocation lists from the staging server.

### **Operation of the Hybrid Handheld card reader:**

- Step 8** – PIV Cardholder arrives at the secure facility, and presents PIV card to the security attendant.
- Step 9** – Security attendant uses Hybrid Handheld to read the PIV card, and then asks cardholder to perform thumbprint test and PIN code entry. The Hybrid Handheld finds a matching PACS record, which confirms the cardholder's access rights, and the security attendant permits the cardholder to enter the facility.
- Step 10** – The Hybrid Handheld logs the transaction, which is later uploaded to the staging server and in turn reported to the IDMS and PACS systems.

## Procuring a Hybrid Handheld solution

The Hybrid Handheld card reader could be built by the IDMS vendor, the PKI technology vendor, or the PACS vendor. Alternatively, the Hybrid Handheld could be provided by a single 3<sup>rd</sup> party, as a unified, vendor-neutral solution that connects to the most popular IDMS and PACS systems.

The most important factor an agency must consider in choosing any PIV card reader solution is how easily the reader can be interconnected with the other agency systems necessary to support its functions. For an agency that has multiple secure facilities and uses a variety of different PACS technologies across them, the ideal solution will be a vendor-neutral solution, since this will allow the same Hybrid Handheld implementation to be used at every location.


One such vendor-neutral solution is provided by Enterprise Air, through its Physical Security Interconnect (PSI) and handheld Authenticator product offerings. Together, PSI and Authenticator provide a rich set of building blocks for implementing a complete Hybrid Handheld card reader solution, with proven ability to query and manipulate cardholder data in IDMS systems, PKI authorities, and all of the top PACS technologies used today. Enterprise Air has deep experience in delivering ruggedized, field-ready handheld card readers that can connect with an IDMS and PACS, process PKI certificate data, and push data to central logging and alert systems. Enterprise Air can also further extend the Hybrid Handheld solution, by integrating additional functions such as incident reporting, custom alerts, mustering kits and portable credentialing.

With a Handheld Hybrid solution from Enterprise Air, an agency can quickly deploy mobile PIV card readers to any local security office, rapidly adopt the new PIV card standard, and extend their systems with additional enhancements to physical security.

## 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 Hybrid Handheld described in this document is a great example of a mobile handheld solution that can be constructed from 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](http://www.enterpriseair.com)**

**+1 212 941 1988**

**[info@enterpriseair.com](mailto:info@enterpriseair.com)**

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