White Paper
Tom Corder and Colin Stevens, IDFACTORS, Inc., January 2025

Deploying Affordable PKI Authentication in a PACS

Today you can transform a PACS into a secure platform that is forward-compatible with Open Supervised Device Protocol (OSDP) and Federal Identity Credential and Access Management (FICAM), on your budget and schedule.

Why it matters:

- Up to 50% of the access cards in use today are based on insecure 125 KHz Proximity technology.
- These cards are a big risk for any enterprise. They can be cloned using a device that is available online for under $20.00.
- It is foolish to migrate to OSDP before legacy cards are replaced by a secure card.

The Background of PIV

In the aftermath of 9/11, the U.S. realized there was no government-wide policy to regulate who could be issued a card for facility access, how cards were issued, or what technology was used. The Homeland Security Presidential Directive-12 (HSPD-12) created the Personal Identity Verification (PIV) credential, which is now the standard for securely accessing government networks and facilities.

PIV for the first time invoked the use of digital certificates and Public Key Encryption (PKI). Today, PKI is the standard for security on the Internet, providing authentication, encryption, and data integrity. These advantages can be applied to PIV-based access systems in multiple ways:

1. Secret keys in proprietary cards and readers can be eliminated with PIV.
2. Because PIV utilizes digital certificates, a non-government entity can load their own certificate or source a certificate from a 3rd party Certificate Authority.
3. Data on the card can be validated by using PKI challenge-response and digital signature verification, which is the bedrock for digital security.
4. Cards with a PIV applet can be purchased from reputable domestic sources, giving the end user the freedom to bypass proprietary vendors using a more secure solution.

Understanding the PKI Platform

The basic PKI platform is now used by industry solutions such as FIDO (Google and Yubico) and PK-PACS (Taglio). Ill-formed perceptions have held the industry back from implementing PKI in a PACS for two decades. For example, many organizations believe that

- PKI is too costly: In fact, the price to implement PKI in a PACS is dropping to levels competitive with current proprietary card technology. New smart cards based on PIV are emerging, and innovative use of PKI at the door continues to drive prices down.

- PKI is too complicated: Again, not true. PKI can work transparently in the background to ensure that a credential presented for access is authentic.

PIV-based cards are available from multiple sources, which affords the end user the opportunity to avoid vendor lock-in to cards and readers. The end user can load their own corporate certificate or one from a trusted third party. In addition, PIV delivers the comfort of compliance with international standards.

How PKI in a PACS Works

More than one option exists for implementing PKI in a PACS. The first requires installing a network of hardware appliances that "cache" certificate status and report the status to the PACS panel whenever an access request is made. This solution was designed to work with Wiegand systems in the federal government.

A second implementation works with OSDP-based access systems, requiring new panels that are PKI-enabled and OSDP "transparent" access readers. These readers execute instructions from the panel to retrieve information from a credential and send it to the panel for centralized PKI processing.

A third implementation, currently being introduced by IDFACTORS, allows a PKI-enabled reader to autonomously process the PKI challenge response and signature verification locally in the reader. Upon a positive authentication, the reader sends the access information to the panel.

Which PKI Option is Best for You?

Each implementation has advantages based on the end user PACS profile, requirements, and budget. It should be noted that the first implementation requires a parallel authentication network, while the second demands a full system replacement including OSDP panels, readers, software, and potentially re-carding and re-enrolling the individual users.

The third autonomous authentication solution has the potential to be less expensive and disruptive because it works with both Wiegand and non-PKI enabled OSDP panels.

Implementation only requires replacing the legacy reader with the IDFACTORS reader and loading the public key used by the certificate issuer. With the public key, the reader can authenticate any compliant PIV card signed by the certificate issuer when used at the door.

Investing in Autonomous Authentication

The goal of the more recent autonomous authentication is to make PKI fast and affordable by eliminating the need to forward certificate information to a centralized access panel, and for the panel to support PKI for multiple readers.

Here is how it works: When a PIV card is initially created, it includes a digital Certificate. The Certificate is signed by the enterprise's trusted Certificate Authority (CA) or by the enterprise. Its certificate data includes a card ID number (FASCN, GUID, or legacy Prox ID) and an expiration date. This is called the Message in cryptography-speak.

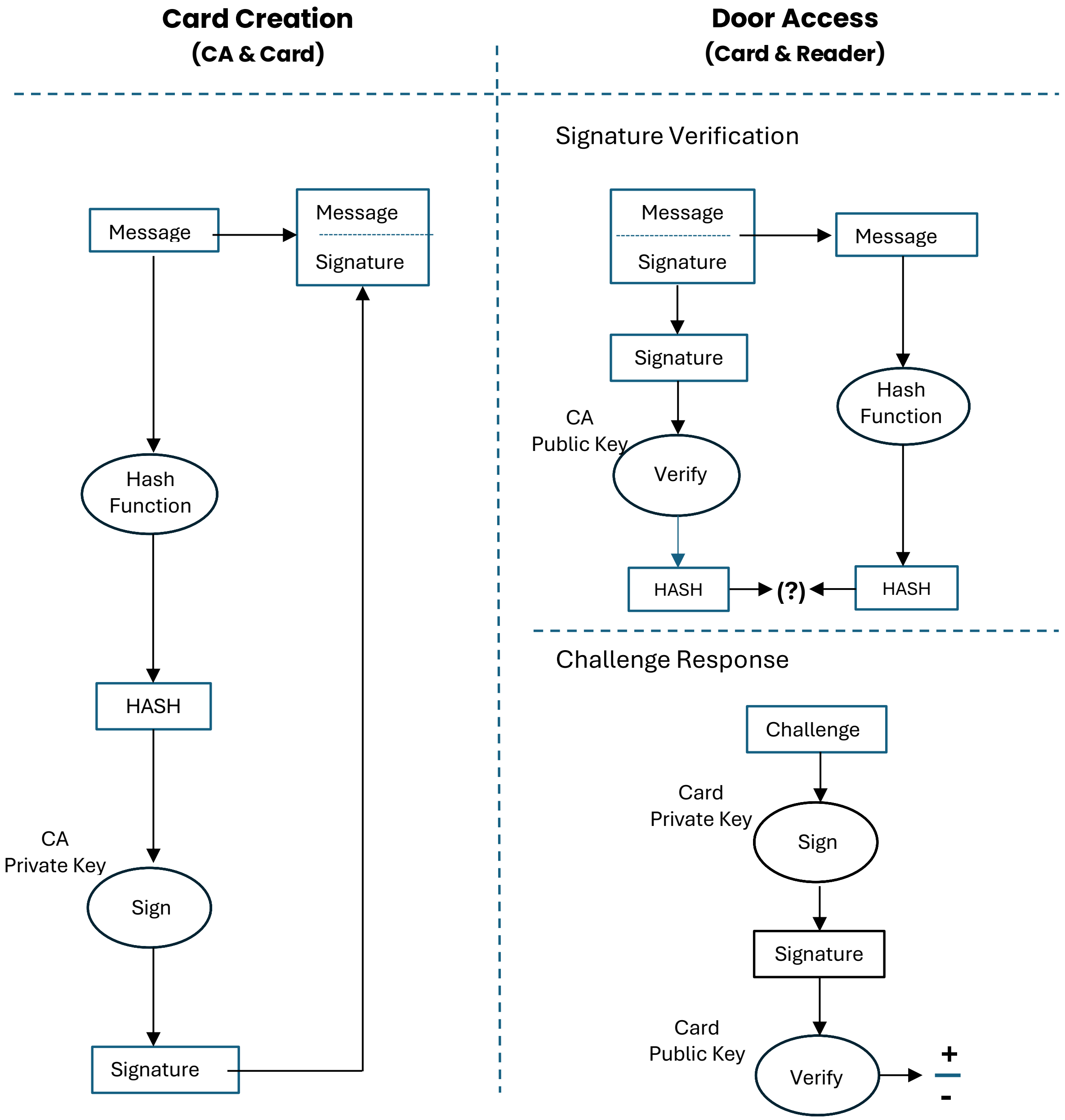
The Signature of the Certificate is computed by first creating a hash of the Certificate data and then encrypting the hash with the trusted CA's private key. The Message plus the Signature comprises the Certificate, which is written to the card.

In the autonomous authentication model, the Door Access Reader functions as the Verifier of the card when it is presented for access. The verification process makes sure that the Certificate has not been changed by a malicious actor, either by replacing the Certificate or by altering the data in the certificate such as the card ID number.

Using the same terms as above, the Reader first retrieves the Message from the card and creates a hash of the Message. The Reader then decrypts the Signature using the trusted CA's public key. If the decrypted signature equals the hash of the Certificate data, then it is verified that the Certificate data has not been altered and means the Reader can trust the Certificate.

It is also necessary to verify that the Certificate data has not been copied from another card by challenging the card to show "proof of possession" of the private key. This is accomplished by a cryptographic process called challenge-response, wherein the card becomes the Signer and the Verifier is still the Reader.

In challenge-response, the Reader creates a random challenge that becomes the Message and sends to the card. The card then encrypts the challenge with its private key to generate the Signature (the response), and the Reader decrypts the response with the card's public key. If the decrypted response matches the original challenge the Reader knows the card has not been copied because there is a valid public key-private key pair. No hash is generated in this process.



Wide variations in the quality and security of identification require safeguarding your facilities to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy. PKI-enabled systems can be used for use cases including protecting agencies, offices, defense sites, schools, and many other high-security spaces.

To learn more, contact security leader IDFACTORS at sales@idfactors.com.