White Paper
Tom Corder and Colin Stevens, IDFACTORS, Inc., June 2024

Affordable PKI Authentication in a PACS, without Replacing the PACS Infrastructure

Yes, you can transform a PACS into a secure platform that is forward compatible to OSDP and FICAM compliance…on your budget and schedule.

Why it matters:

- Up to 50% of the access cards in use today are based on insecure 125 KHz Prox 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 fool's gold to migrate to OSDP before legacy cards are replaced by a secure card.

In the aftermath of 9/11, the Federal Government 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. HSPD-12 aimed to fix that model by creating the Personal Identity Verification (PIV) credential, which is now the standard for securely accessing Government networks and facilities.

PIV invoked the use of digital certificates and Public Key Encryption (PKI), which was new to PACS providers 20-years ago. 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 system in multiple ways:

1. Secret keys in proprietary cards and readers can be eliminated with PIV.
2. Because PIV utilizes digital certificates, the end user can load their own certificate or source a certificate from a 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 by-pass proprietary vendors with a more secure solution.

The basic PKI platform is now being used by industry solutions such as FIDO (Google and Yubico) and PK-PACS (Taglio), further confirming it is time for the security industry to change perceptions about "PKI in PACS." Ill-formed perceptions have held the industry back from implementing PKI for 2-decades, but they are out-of-date today. Below are 2 perceptions that need to change:

- PKI is too costly: Not true. In fact, the price to implement PKI in a PACS is dropping to levels competitive with the current non-secure card technology. New smart cards based on PIV are emerging and innovative use of PKI at the door will continue 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 3rd party. In addition, PIV delivers the comfort of conformance to international standards.

How PKI in a PACS works:

There is more than one option for implementing PKI in a PACS. The first option requires installation of 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, primarily in the Federal Government, and admittingly it is expensive.

A second implementation works with OSDP-based access systems and requires panels that are also PKI enabled. In addition, access readers must be replaced with OSDP enabled "transparent" readers that execute instructions from the panel to retrieve information from a credential and send it to the panel for "centralized" PKI processing.

;BVHBJNKKH JGHBA third implementation currently, being introduced by IDFACTORS, "distributes" the PKI functionality to each reader, allowing the 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 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 and the second implementation requires a full system replacement including OSDP panels, readers, software and potentially re-carding and re-enrolling the individual users.

The distributed PKI 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 cards signed by the certificate issuer when used at the door.

Distributed Authentication:

Authenticating a PIV credential at the door involves a "shared processing" system where individual readers are equipped with a cryptographic processing capable of supporting PKI functionality in real time when a door access request is made. The design intent is to make PKI fast by eliminating the need to forward certificate information to a centralized access panel and affordable by not loading the panel with the capability of managing PKI for several doors at peak loads.

When a PIV card is initially created it is populated with a Digital Certificate. The Signer of the Certificate is the enterprise's trusted Certificate Authority (CA) or the Certificate could be signed by the enterprise. The Certificate data includes - at a minimum - the card ID number (FASCN, GUID or legacy Prox ID) and an expiration date. This data is called the Message in cryptography-speak.

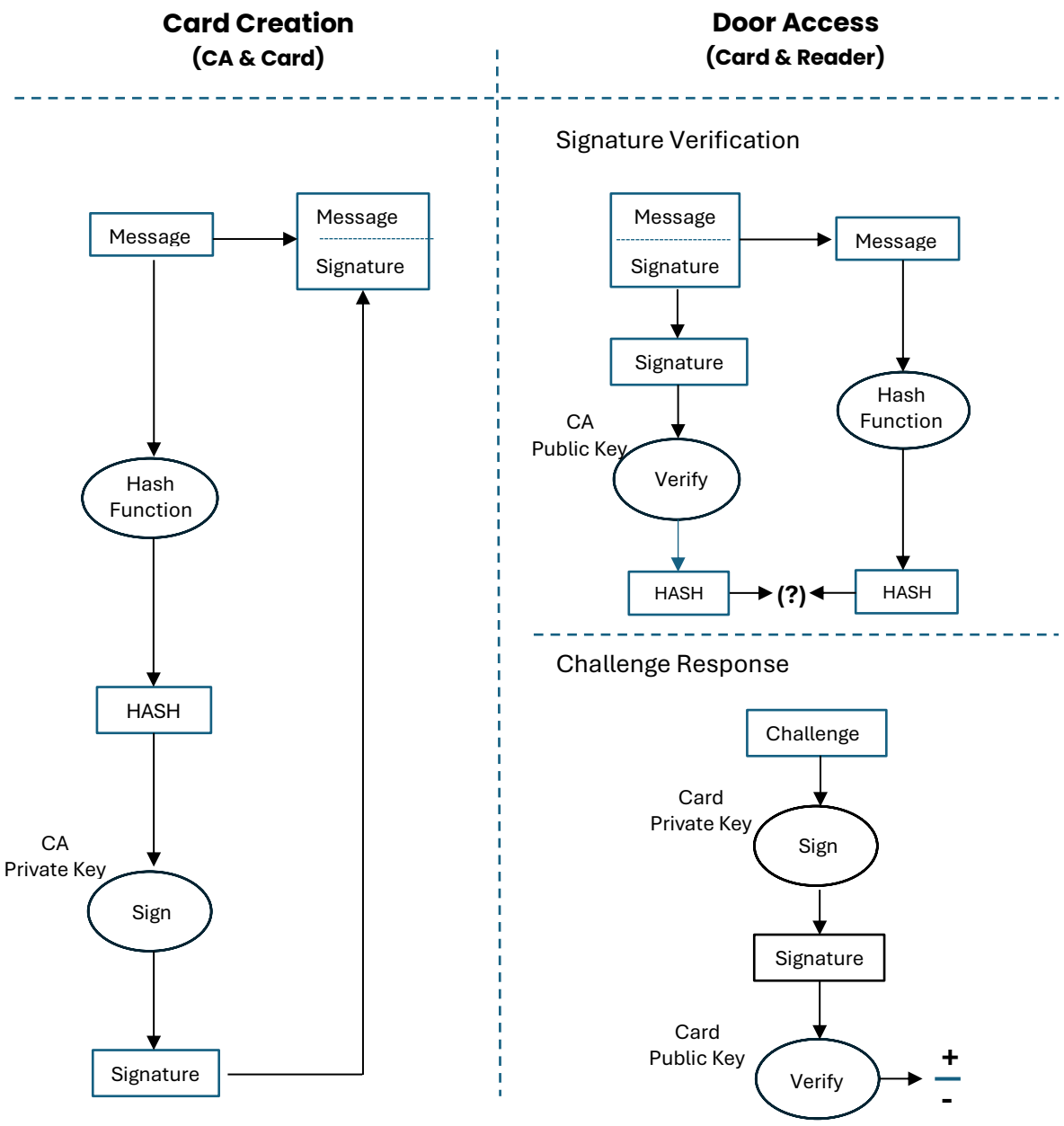
The Signature of the Certificate is computed by the Signer by first creating a hash of the Certificate data and then encrypting the hash with the trusted CA's private key. The Message plus the Signature comprises the entire Certificate, which is written to the card.

In the distributed 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 then 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. This is called Signature Verification and means the Reader can trust the Certificate has not been altered.

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.


Card Creation
(CA & Card)
Door Access
(Card & Reader)
Message
Message
Signature
Hash Function
HASH
CA
Private Key
Sign
Signature
Signature Verification
Message
Signature
Message
Signature
CA
Public Key
Verify
Hash Function
HASH
(?)
HASH
Challenge Response
Challenge
Card
Private Key
Sign
Signature
Card
Public Key
Verify
+
-