IDFACTORS™

OWN THE KEY PAIR. VERIFY AT THE DOOR.

A Practical Path to Compliance for DoD Agencies and Contractors

AUTHARA DELIVERS IDENTITY VERIFICATION and CONFIDENCE FOR ANY PACS.

OVERVIEW

Most enterprises don't even know if their physical access control system is already compromised. Credentials in use today are little more than a number with no cryptographic identity. Popular options like Mifare cards offer only the illusion of security — their encryption keys can be defeated in seconds, allowing cards to be cloned without the PACS ever knowing.

Replacing the PACS does nothing to fix this; the vulnerability travels with the credential.

To mitigate this vulnerability, most government contractors are required to issue secure physical access credentials to personnel who do not hold a government issued PIV or CAC card.

Regardless of their size, all Contractors face the same challenge: achieving compliance-grade physical access, without the cost and complexity of traditional PKI infrastructure.

WHY IT MATTERS

Existing Physical Access Control Systems (PACS) are often ripped out and replaced with a “more compliant” system at great expense. This White Paper introduces AUTHARA, a PKI Credentialing Engine that delivers secure HSPD-12 compliance with no modification to the existing PACS. It does this by adding an identity verification layer.

With Authara, SMB and even government agencies with a non-PIV eligible workforce can meet government requirements on an affordable budget.

1. Legacy cards are replaced with secure PIV-Compatible credentials, leaving the enterprise owning the asymmetric key pair and free from vendor control.
2. All PIV and PIV-Compatible Cards are securely verified at the door, defeating rogue cards.
3. The legacy access system is preserved, saving a significant investment.

2. The Problem: Two Distinct Compliance Gaps

The physical access credential compliance problem manifests differently for government agencies and their contractors.

2.1 Government Agencies: The Non-PIV Personnel Problem

Agencies operating under FISMA and HSPD-12 have well-established PIV card programs for federal employees. The gap is with the personnel who surround those employees: contractors, new hires pending PIV issuance, temporary personnel, and visitors requiring recurring access.

These individuals need access to controlled facilities but do not hold a PIV or CAC card. The options available to agencies today are inadequate:

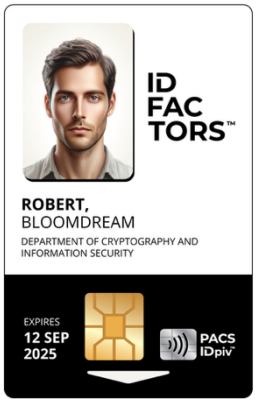
Current Approach	The Resulting Problem
Issue a proximity or Mifare card	Provides no cryptographic identity. Any card number can be cloned. The audit log records a number, not a verified person.
Wait for full PIV issuance	PIV issuance timelines for contractors can be weeks or months. Blocking access during this period is impractical.
Deploy full Federal PKI Bridge	Requires the contractor to be enrolled in a federal trust anchor chain, which is complex and expensive.

2.2 SMB Defense Contractors: The CMMC Infrastructure Problem

CMMC Level 2 certification requires defense contractors to satisfy the Physical Protection (PE) domain controls under NIST SP 800-171 Rev 3. These controls require - among other PACS functionality - verifiable audit logs tied to individual identity.

Proximity and Mifare cards fail these requirements in multiple ways. But the alternative — a full PKI deployment with OCSP infrastructure — presents its own barriers for SMB contractors, which is often a full replacement of the PACS.

The result is that many SMB contractors enter CMMC assessments with proximity or Mifare card systems, generating findings that delay certification and put contract eligibility at risk.



The PIV Credential

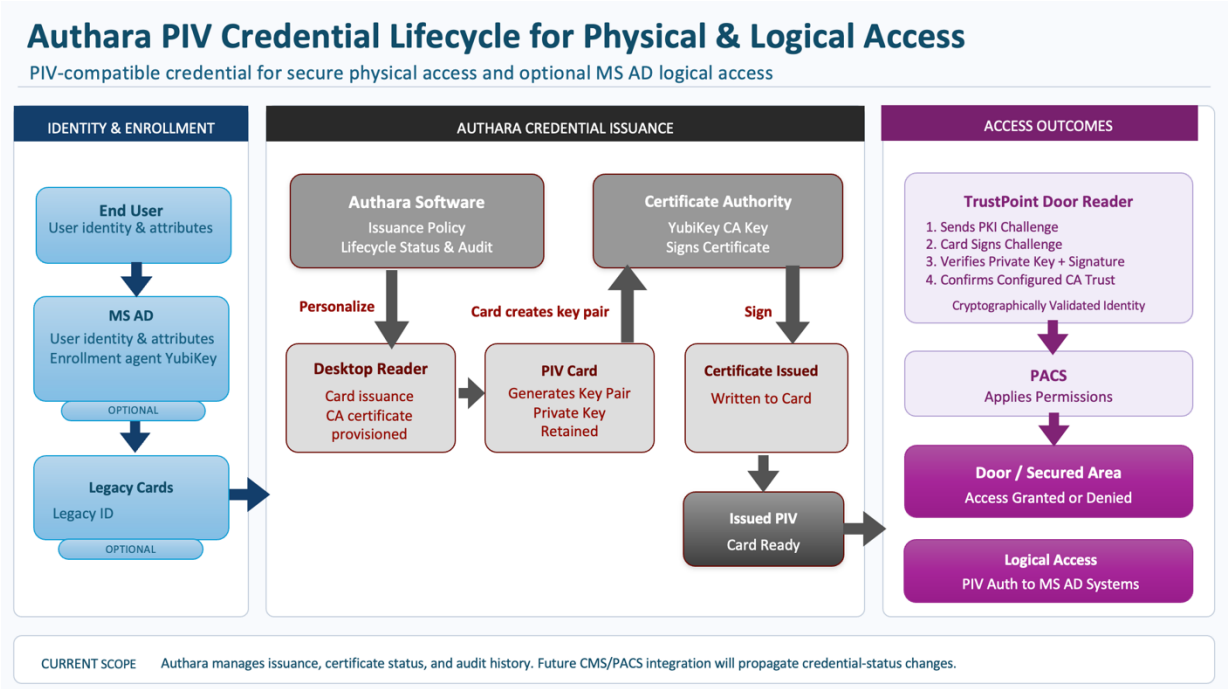
3. The IDFACTORS Solution: ZeroTrustPACS™

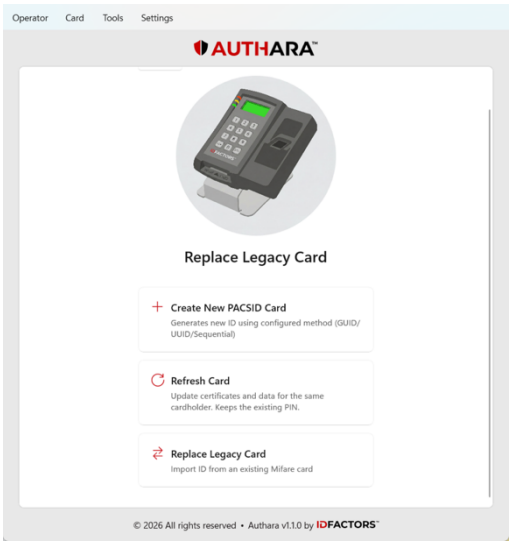
IDFACTORS addresses these problems with three synchronized components that deliver compliance-grade PKI physical access without requiring PACS replacement,

3.1 Authara — The Credentialing Engine

Authara is the central management application for the ZeroTrustPACS™ platform. It functions as the credential lifecycle engine, connects to the credential authority and it is the component that makes ZeroTrustPACS™ both practical and affordable.

PIV-Type Credential Issuance	Authara generates cryptographically verifiable PIV-C credentials for Government contractors and new hires. For SMB contractors, CMMC-compliant credentials can be issued from one domain within the enterprise.
Legacy PACS ID Preservation	Credentials issued by Authara can optionally include the cardholder's legacy PACS ID embedded in the certificate. This means the PACS controllers and database require no modification. PKI verification occurs at the reader layer and the PACS receives the verified access request.
Active Directory Integration	Authara integrates with Microsoft Active Directory and Entra ID, detecting when a user is terminated in AD and initiating a credential revocation. The revocation is pushed to the PACS and an access denial.





Authara Application

3.2 Authara Desktop Station with Reader Security Module (RSM)

The Authara Desktop Station integrates all the functional components required for secure credential management.

Reader Security Module	Supports All PIV Types	Efficient Workflow
Provides the cryptographic trust anchor for credential issuance without requiring a separate, expensive HSM appliance.	PIV, PIV-I, CAC, TWIC, FIDO and PKOC cards in both contact & contactless mode. Includes a keypad for secure PIN change.	Authara and on-Reader display guide the security officer and cardholder through each step - reducing errors and speeding the task.

Why the RSM Matters for SMB Contractors

A HSM is essential for any serious PKI deployment — it ensures that private keys are never exposed. Traditional HSM's cost thousands of dollars and require specialized administration. The Authara Desktop Reader's integrated RSM delivers equivalent cryptographic security as a built-in component of the issuance workstation, at a price point accessible to organizations of any size.



The Desktop Reader with HSM

3.3 TrustPoint Door Readers — Offline PKI Verification

TrustPoint door readers are drop-in replacements for existing access control readers and include the same RSM as in the Desktop Reader, whether Wiegand or OSDP. They perform cryptographic credential verification at the door using standard PKI verification mechanisms that operate without a live network connection to an OCSP responder or CRL server. This happens before any access request reaches the PACS controller

Verification Method	What It Proves
Challenge-Response Key Verification The reader issues a cryptographic challenge to the card. The card signs the challenge using the private key and the RSM verifies the signature against the public key in the certificate.	**The private key is present on this specific card.** A positive verify proves the card has possession of the Private key. Cloning can copy the certificate and card data, but it cannot copy the private key. Therefore, a cloned card would fail the challenge response at the reader before access is ever considered.
Digital Signature Verification Authara creates a digital signature in each credential at issuance. The TrustPoint reader verifies this signature using the CA's public key, which is pre-loaded into the reader. No network connection is required at time of verification.	**The certificate data has not been altered** Any modification to the credential after issuance — tampering with the cardholder identity, authorization scope, or expiration — invalidates the signature. The reader detects the tampered credential and denies access independently of any revocation check.



The Door Reader

3. Summary

Most enterprises don't even know if their physical access control system is already compromised. The credentials in use today are little more than a number with no cryptographic identity, and popular options like Mifare cards offer only the illusion of security — their encryption is defeated in seconds, allowing cards to be cloned silently and undetectably without the PACS ever knowing. Replacing the PACS does nothing to fix this; the vulnerability travels with the credential.

Authara solves this by replacing both the credentials and the door readers, while leaving everything else untouched. PIV credentials are issued and enrolled directly from the enterprise domain, with the legacy credential number embedded in the PKI certificate on the card and the enterprise in full ownership of the key pair.

Authara readers then perform a cryptographic challenge-response at every access event — confirmed credentials pass their number to the PACS exactly as before; failed credentials pass nothing. Door controllers, databases, and access rules remain completely unchanged. The result is a CMMC-compliant access environment that eliminates credential cloning, requires no PACS reconfiguration, frees the enterprise from vendor license fees, and deploys with nothing more than a credential re-issue and a reader swap.