Authentication and security solutions you can trust.™

AuthentX™ Visitor PIV Authentication Station (VPAS)

Allowing someone access to a controlled facility or resource requires the person's identity to be validated and authenticated. In the past, verification relied on visual inspection of a photograph or confirming personal information.

VPAS, the Visitor PIV Authentication System, relies on proven electronic authentication methods, including matching fingerprint biometric information with data stored on the PIV or PIV-I card. This feature allows for multi-factor authentication.

Authentication Mechanism	Strength
Legacy Magnetic Stripe	🟩□□□□
Legacy Proximity Card	🟩□□□□
PIV CHUID Read	🟩□□□□
PIV Challenge/Response With Full Path Validation	🟩🟩🟩🟩🟩

The Visitor Station allows each agency to independently verify the validity and status of any PIV card utilizing the Federal Bridge Certificate Authority. VPAS performs full path validation in conjunction with verifying the card and certificate data. This method is the most secure method to determine the true validity and status of a PIV card.

Certificate Authentication

VPAS ensures that the public and private PIV authentication certificates match; it verifies the certificates' issuance date, expiration date and relevant certificate information. The application also builds and checks the PIV Authentication 9A certificate chain. The PIV Authentication certificate is then validated by checking an Online Certificate Status Protocol (OCSP) Responder or Certificate Revocation List (CRL) to ensure the certificate is valid and has not been revoked by the issuing authority.

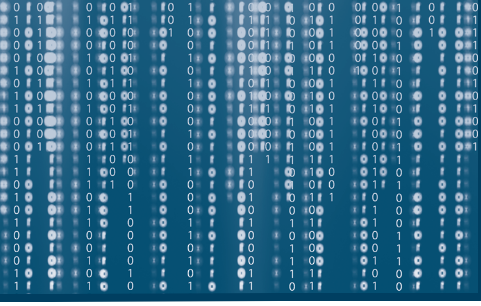
See reverse for enhanced provisioning capabilities

Features

- Identity Verification
- Path Validation
- PIV & PIV-I Solution
- Biometric Verification
- Physical Access
- Logical Access
- OCSP Benefits

Contact Us:

11180 Sunrise Valley Drive
Suite 310
Reston, Virginia 20191
(703) 547-3524
www.xtec.com



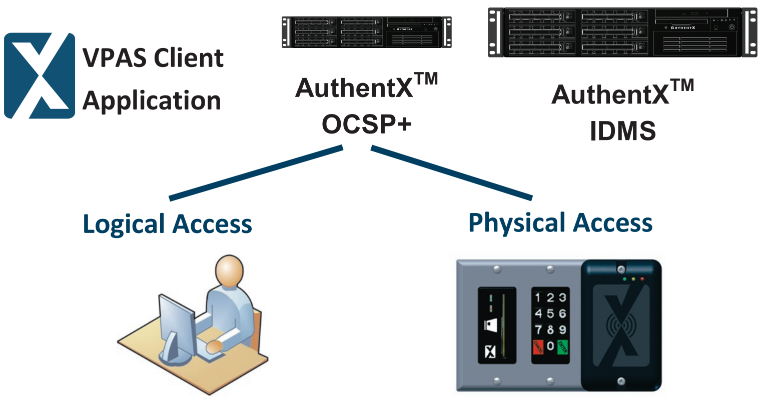
AuthentX™ Visitor PIV Authentication

Enhanced Capabilities

In addition to full path validation of a visitor, the VPAS, with added provisioning capabilities, creates an identity record in the IDMS to enable physical and logical access. The enhanced capabilities hinge on two core XTec products in the AuthentX line of identity products:

- ✓ AuthentX OCSP+
- ✓ AuthentX IDMS

Interoperability



VPAS Client Application

AuthentX™ OCSP+

AuthentX™ IDMS

Logical Access

Physical Access

AuthentX™ OCSP+

XTec's AuthentX OCSP+ services provide real time revocation information for credentials associated with identities stored in the AuthentX IDMS. Relying parties are not burdened by the latency of the CRL information provided by the Certification Authority. The AuthentX OCSP+ has the unique capability to evaluate Public Key Infrastructure (PKI) certificates for each transaction; physical and logical. OCSP+ leverages the technical characteristics of the card, designed for interoperability between PIV, PIV-I and PIV-C cards, to allow for an easily implemented enterprise physical/logical access solution.

> OCSP+ provides immediate, real time status information without the potential delay involved with CRL issuance.

AuthentX™ IDMS

The AuthentX IDMS is the core component for all XTec products and functions as the end-to-end HSPD-12 solution at several Federal Agencies. It is a highly secure identity management system designed using a Service Oriented Architecture (SOA) built upon the secure NSA SE Linux Kernel. The AuthentX IDMS provides full card personalization, card production, flexible card design, workflows, access control and an application interface to various legacy systems and is able to operate in a cloud environment.

The AuthentX suite of identity products:

- IDMS/CMS
- Cloud & SaaS
- Self Service Kiosk
- Physical Access Control Solutions
- Logical Access Control Solutions
- Enrollment & Issuance Solutions
- End-to-end HSPD-12 Solution
- GSA Schedule 70 SIN 132-62
- FIPS 201 Certified Products