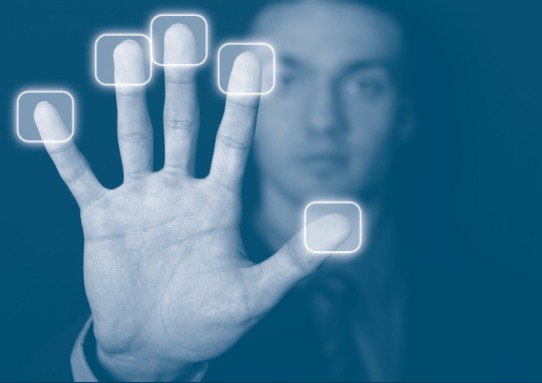








Authentication and security

solutions you can trust.™



## Features

-  Web-based Control
-  Interoperability
-  Built-in OCSP
-  Cloud Capabilities
-  Strong Authentication
-  NIST SP 800-116 Compliance
-  PIV-I Support
-  PKI Authentication
-  Symmetric Authentication

### Contact Us:

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

## AuthentX™ Physical Access Control

As tactics for intrusion and theft become increasingly sophisticated, AuthentX Physical Access Control offers much-needed protection for your enterprise. Our solution ensures that your physical facilities — and the logical assets they house — are accessible only to authorized individuals.

XTec leads the industry in deploying end-to-end physical access control solutions for Federal Agencies that must comply with HSPD-12, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116, FIPS 201, and FICAM guidance.

Our solution has the functionality to act as an enterprise PACS or to enable a quick, low-cost approach for enhancing legacy PACS implementations to provide strong authentication. The AuthentX solution performs PKI and symmetric key authentication to ensure only valid, unaltered PIV cards are accepted. The XTec Access Control solution also works with PIV-Interoperable and PIV-Compatible credentials.

The XTec PACS solution is designed with the AuthentX IDMS as a core infrastructure component. Other solution components include:

- ✓ Access control readers.
- ✓ AuthentX XNodes.
- ✓ AuthentX OCSP+ Modules.
- ✓ Web-based application control.
- ✓ The ability to authenticate multiple agency's PIV cards.



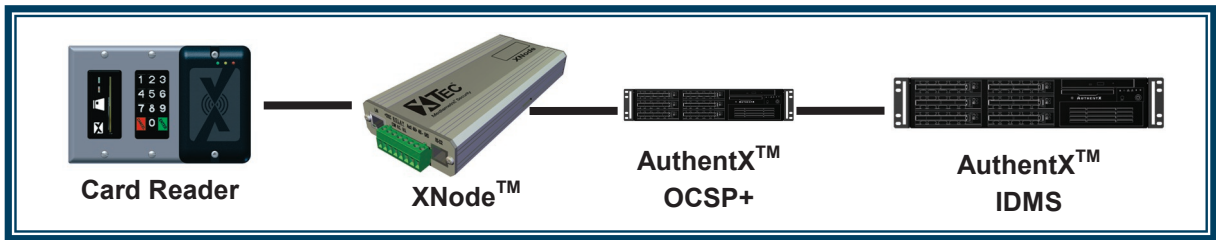
### Strong Authentication

AuthentX PACS is distinguishable because it performs multiple facets of authentication. Our access control readers and patented IP-addressable XNodes are equipped to perform cryptographic functions such as a challenge/response, path validation, symmetric authentication and checking digital certificate status. AuthentX PACS components also perform traditional authentication techniques such as the use of personal identification numbers (PINs), fingerprint matches, unique identifier matches and verification of signed attributes.

# AuthentX™ Physical Access Control

## Flexible Implementation

Federal Agencies can struggle with integrating the multiple access control solutions that often support individual locations or databases. This piecemeal approach creates dangerous gaps in security. The AuthentX Physical Access Control, with the AuthentX IDMS as the core, has a built-in web service interface to support legacy PACS. This unique feature is the most secure method to extract data and is one of the features that allows AuthentX PACS to be a full enterprise solution. AuthentX performs the strong authentication of the PIV card while legacy PACS can continue to manage permissions or unlock functions at the local or facility level. AuthentX PACS operates on the network eliminating the need for users or administrators to be present at a dedicated workstation for the assigning of permissions. AuthentX PACS can be a vendor hosted and managed solution or a locally hosted and administered solution for enterprise access control. The AuthentX IDMS and PACS has met NIST and FISMA systems security guidelines, proving the security and integrity of the system.



AuthentX PACS may create access permissions based on specified attributes or on organizational policy. With the AuthentX IDMS and AuthentX OCSP+ physical resources are secured in the same manner as logical resources, performing strong authentication and rational access decisions. For example; an individual uses a credential to access the network from their remote computer at home but then enters the building minutes later, the enterprise solution can be configured to alert administrators to this type of suspicious activity.

## “Cloud First”



AuthentX PACS easily operates as SaaS (“Software as a Service”) as it is an IP-based solution. SaaS is proven to reduce operations and maintenance, change management, administrator and hardware costs. A secure cloud solution eases implementation, expansion and configuration changes. Flexibility and mobility are necessary for maintaining control of various buildings and locations; cloud solutions offer this option and AuthentX PACS has operated in a secure cloud environment for over five years.

### 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