Authentication and security solutions you can trust™

PIV Access Solutions

Zero Trust Identity for Physical and Logical Access

At a Glance

- Unified physical and logical access system
- Open standards based on federal guidelines
- Passwordless Multifactor Authentication
- Secure end-to-end encryption
- Operates on Public Key Infrastructure
- Interoperable between government and utilities

Comprehensive Security Solutions

Modern utilities are taking a defense in depth approach to today's cyber-physical threats. Identity is your first perimeter. XTec offers the most secure solution for Identity and Access Management available to utilities today. With over 15 years of experience delivering secure access solutions to the federal government and military, XTec is the partner your utility can trust.

Zero Trust Identity Architecture

Over 80% of breaches are caused by compromised passwords

Critical Infrastructure Is Vulnerable

Utilities, and the nation's energy supply, is the most important critical infrastructure in the US. A remote access hack or an internal compromise presents a highly damaging compromise.

Where are the biggest vulnerabilities?

Group Accounts For a variety of reasons, utilities rely on group accounts and shared passwords in areas such a substation control houses and operations centers. This can result in passwords that are written down—and thus easily discoverable or that are not complex enough. Neither is an attractive option.

Password Complexity There are many problems with passwords, but the most fundamental is the contradiction between

- The fact that more secure passwords are longer and more complex, and
- The fact that longer and more complex passwords are harder to remember.

Password Reuse

Far too many people reuse passwords– not only at work, but their personal passwords as well. With the large number of breaches at organizations such as retail stores and hotels, there is a high degree of probability that those breaches can compromise your utility.

Physical Access

Most physical access is controlled by a swipe card. A swipe card certainly has many advantages over a metal key, but they are also very easy to duplicate. In many ways this is the same as a weak password for controlling access to secure spaces.

High Assurance Protection

Eliminate Passwords

Using a PIV SmartID card for access allows you to do away with complex passwords that are easily forgotten and get rid of unsecure group user accounts.

Authentication

Use a PIV card for multifactor authentication (MFA) including possession of a digital certificate, knowledge of a PIN and biometric template to ensure access is secured against intrusion.

Validation

Real time validation occurs through a series of Online Certificate Status Protocol (OCSP) responders to quickly and securely manage access across the largest of organizations.

Authorization

Manage authorization independently or in conjunction with Microsoft AD to create a secure environment for Least Privilege granting access only to those who are allowed.

The PIV card contains high security features that prevent the tampering with or counterfeiting of the card.

Unified Access Control

Keeping today's utilities safe from unauthorized intrusion requires security you can trust. XTec's Physical and Logical Access Control System (PACS/LACS) delivers the security your utility needs.

One System

XTec's AuthentX Identity Management System (IDMS) gives you a comprehensive physical and logical access control system that deploys across the organization. The PIV SmartID card can grant highly secure access inside both your Physical and Electronic Security Perimeters.

Interoperability

The PIV solution is based on open standards that include interoperability. Cooperating utilities, contractors and agencies will be able to read external PIV cards and grant access in times of emergency or planned coordination.

Open Standards Based

XTec solutions are all based on open standards for interoperability. You won't get locked into proprietary technology when you partner with XTec.

Reporting

The AuthentX IDMS offers robust tracking, logging and reporting tools to ease the compliance burden.

Data Centers

XTec's AuthentX solution is FedRAMP High certified and deployed across three geographically dispersed and highly secure data centers.

Data Security

All data is encrypted at rest and in transit. Only secure communications are used and all media use encrypted drives, which are destroyed after use.

Public Key Infrastructure

AuthentX utilizes a certificate issuance infrastructure based on FPKI (Federal Public Key Infrastructure). All digital certificates come from an established environment of trust. The certificate issuance architecture is protected by stringent policies and practice statements.

Single Purpose System

The AuthentX (IDMS) and PACS system with XNodes are provided as single-purpose systems; all appliances are purpose-built to prevent tampering. XTec performs all updating and patching remotely.

Card Security

Our PIV cards can't be tampered with (without invalidating them) or replicated.

Email Security

The certificate on a PIV card can be used to digitally sign emails. With phishing and ransomware attacks on the rise, and with an increased number of employees working remotely, locking down emails is a top priority for all organizations, especially utilities.

AUTHENTX™

- High Assurance IDMS
- Passwordless Environment Solution
- ESP and PSP Protection in One Solution
- End to End IDMS
- Comply with many NERC CIP Areas
- Protect Logical and Physical Access
- Best Paired with High Risk Areas
- Low Cost and Easy to Implement
- Highest Level of Security Available
- Proven Technology

Overview

AuthentX for Utilities by XTec is an enterprise Identity Management System (IDMS) that manages identities, credentials and permissions keeping your utility highly secure. The system lets you know who your employees and contractors are and what they have access to. It's design provides your utility with a complete end-to-end solution that ensures the bonds between Identity, Credential and Permissions are never broken.

The AuthentX IDMS offers a simple implementation that scales with your organizations needs. The goal is to give your organization complete control over all digital identities and includes full identity life cycle management incorporating employee onboarding to termination. This means a short time frame from enrollment to credential use and revocation of credentials and permissions when critical.

The system gives you the flexibility to move to a passwordless environment. By removing username and password use you prevent the most common method of unauthorized access – a password breach.

AuthentX can be used across your utility's IT, OT and physical access platforms to allow a single, converged identity and access management system. The system has multiple features that will assist you in being compliant with NERC CIP requirements for your Physical and Electronic Security Perimeters.

All of this is built on open standards so you don't get locked into proprietary technology. The standards themselves have been in use for many years and have been proven to work in high risk environments.

To learn more about how to secure your IT, OT and Physical assets to be in compliance with NERC CIP, please contact us.

Steve Lindsay
Director Critical Infrastructure
slindsay@xtec.com
(305)588-6731

Danny Vital
Senior Software Engineer
dvital@xtec.com
(305)905-0760