XTEC™

Authentication and security solutions you can trust™

Identity First

Increased Security, Lower NERC CIP Costs

Using PIV cards to increase security and lower CIP compliance costs

In 2004, the US government committed to a new standard for identity and access management across all civilian agencies: PIV (Personal Identity Verification for government) . The military adopted the technology for the CAC (Common Access Card for military) cards. Today, almost all federal government and military personnel carry a PIV or CAC card, which authenticates their access both to physical facilities and to systems that support their work. (In this paper we will refer to the technology as PIV for brevity.)

In the electric power industry, this same technology can both make your organization more secure and greatly reduce the amount of time and money you spend on NERC CIP compliance. In this white paper, we will discuss the five most important ways in which PIV cards can help your organization achieve both of these goals.

Unified Access

Use one system to authenticate both physical and logical assets

One of the most important features of PIV cards is that the user only has to carry one card. It authenticates both physical access to buildings and other facilities, and logical access to computers and other intelligent devices the employee uses to perform their work. Of course, this is a big convenience for the user, since they just need to carry one card and remember one simple PIN.

However, PIV cards are an even bigger convenience for the organization that implements them. There are several reasons for this:

1. Both physical and logical access can be provisioned at once, based on the person's role.
2. When the person changes jobs, their previous accesses can be quickly disabled and their new accesses immediately provisioned.
3. When the person leaves the organization, all of their physical and logical access can be removed in one step.

Having a single access management platform for both physical and logical access can save your organization a lot of time in complying with the following CIP requirement parts:

CIP-004-6 R4.1 through R4.4: A single identity management system can authorize, provision, review, and remove an individual's access both to systems and physical facilities. A full roles capability makes this very easy, when roles have been defined by your organization.
CIP-004-6 R5.1 through R5.5: Your organization can quickly remove access to the systems, physical facilities and information repositories (including those for BES Cyber System Information), to which an individual had access; this is done at a single console and with minimal delay. You can do this whether the individual was terminated, left voluntarily, or changed roles within the organization.

CIP-006-6 R1.2, R1.3 and R1.8: PIV cards provide multi-factor authentication and logging at all physical facilities.

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

Multifactor authentication

Multiple NERC CIP guidelines call for multifactor authentication to both the Physical Security Perimeter and the Electronic Security Perimeter.

You probably already understand the principle behind multi-factor authentication (MFA): your security is greatly enhanced if the user needs to supply more than one "factor" whenever they enter a building or logon to a computer. There are three types of factors:

- Something You Know (a PIN)
- Something You Have (a card that contains an electronic identifier)
- Something You Are (a biometric "template " like a fingerprint)

A PIV card allows use of all three of these factors in authentication:

Upon inserting their PIV card for access to a building or a system, the user is prompted to enter their simple PIN – something they know.

The card contains an X.509 digital certificate, which cannot be copied or altered – something the user has.

A template of the user's fingerprint is stored on the card. Some PIV card readers have a fingerprint scanner, which compares the fingerprint of the user to the fingerprint scan template that's stored on the card. This provides a third means of authentication – something the user is.

With PIV cards and card readers in place, you can have multi-factor authentication literally anywhere in your organization, i.e. a) for access to all devices on both your IT and OT networks, and b) for access to physical facilities including office buildings, substations, generating stations, etc. For some systems or facilities requiring a higher level of security, you can also require the fingerprint scan (or you might require it everywhere). Conversely, in lower-security situations you can require just the card, not a PIN.

One note: If you prefer contactless single-factor authorization in some cases – e.g. doors in low-risk areas - many PIV cards also have contactless capability, as long as contactless card readers are deployed.

There are two CIP requirement parts that require MFA, and one part where it would be a good idea, but it's not required. If your organization uses PIV cards, you already have everything you need to comply:

CIP-003-8 R2 Attachment 1 Section 2: PIV cards allow your organization to implement multi-factor authentication at low impact NERC CIP assets, as well as medium and high impact assets.

CIP-005-6 R2.3: If the remote system (e.g. in an employee's home) is protected with a PIV card reader, the employee can be multi-factor authenticated for Interactive Remote Access using their normal card and PIN.

CIP-006-6 R1.3: The employee's PIV card, PIN and (optionally) fingerprint scan provide MFA for access to High impact Control Centers.

Passwordless Environment

Eliminating passwords removes the most common threat vector of hackers and helps to get rid of shared accounts and shared passwords.

Many cybersecurity professionals will tell you that the biggest source of cyber risk in their organization is passwords. "*The password is by far the weakest link in cybersecurity today.*" Michael Chertoff, former head of Homeland Security.

In other words, it is far too easy to steal or guess passwords. In an industry leading survey, almost half of respondents answered that they used similar login credentials for both IT and OT networks, making it much easier for the hackers to penetrate the OT network.

Passwords present a fundamental problem: They need to be as complex as possible in order to be secure, but they also need to be as simple to remember as possible so that users don't write them down, use the same password across systems and on the internet, etc. In the electric power industry, passwords are often shared, because of the need for multiple people to be able to quickly access the same systems at different times (for example in substations or Control Centers).

While there are some commercial solutions available to partially address this problem, wouldn't it be great if you could deploy the ultimate solution: eliminate passwords altogether? With PIV cards, you can do that! PIV cards contain a digital certificate that is unique to the individual and can't be copied or altered. This, along with a simple PIN entered by the user, provides a higher level of security than even the most complex password. And you can always require a fingerprint scan as well, when you believe the highest level of security is required.

There are many NERC CIP requirements that are based on passwords; PIV cards can help you comply with all of these, likely at a much lower cost in staff time and money than you are incurring now. Here are some of the most important examples:

CIP-004-6 R5.5 and **CIP-007-6 R5.3** both apply to shared accounts. If your organization deploys PIV cards to employees (and contractors, if needed), there will no longer be any need for shared accounts. This is because the user will only need their card and an easy-to-remember PIN. In fact, you will always be able to require a fingerprint scan as well, for the highest level of security.

CIP-007-6 R5.4 requires changing default passwords. If a system is protected with a PIV card reader, any default password that might be on the system is irrelevant; there is no pathway to access the system, even if a user knows the default password.

CIP-007-6 R5.5 and **R5.6** require controls on password length and complexity as well as password changes, but they only apply to systems with "password-only authentication". Any system with a PIV card reader is out of scope for both of these requirements!

Compliance Assurance

Fully automated tracking of Personnel Risk Assessments and trainings allow your utility to never be out of compliance by revoking access to out of date users.

Beside the digital certificate and fingerprint scan template, other information (for example, certifications) can be stored on the card and read by the card reader to control access. Four very important pieces of information for NERC entities are whether a user – who has been granted electronic and/or unescorted physical access to BES Cyber Systems - has had a personnel risk assessment and CIP training after being hired, and when each of those was last conducted. The PRA needs to be renewed in seven years and the training needs to be renewed at least every 15 months.

Specifically, there are three CIP requirement parts involved:

CIP-004-6 R2.2: If the user has not yet completed their CIP training, an employee can be prevented from accessing High and Medium impact BCS, EACMS and PACS, or having unescorted physical access to assets like Medium impact substations or High impact Control Centers.

CIP-004-6 R2.3: If the employee has not renewed their training before the renewal date, they can be prevented from accessing High and Medium impact systems and facilities until they have renewed it. Access will be automatically blocked starting the day after their training expires.

CIP-004-6 R3.5: If a new employee has not completed their Personnel Risk Assessment, or if an existing employee has not renewed their PRA in the last seven years, they can be prevented from accessing High and Medium impact systems and facilities until they have had a new PRA.

Emergency Response

Large scale recovery operations have many moving parts. An interoperable identity card has proven to provide a more secure and better operational response.

When one electric utility has experienced a natural disaster, other utilities will often provide skilled workers to help the impacted utility recover. When this happens, it is usually quite hard for the impacted utility to follow all of the personnel security requirements in CIP-004-6, at the same time as they're authorizing and authenticating emergency workers.

While a declaration of CIP Exceptional Circumstances will normally protect the utility against any CIP violations being assessed as a result of not strictly following the **CIP-004-6** requirements, the fact remains that emergency response situations open up a security hole that might be exploited by a resourceful adversary.

XTec has worked with federal agencies, primarily FEMA, to develop capabilities based on PIV cards, that can mitigate much of the security risk associated with emergency response situations. These include:

- Mobile enrollment and authentication facilities;
- Capability to accept PIV cards issued by other organizations (government agencies, other utilities, and vendors);
- Capability to create a "derived credential" on a smartphone, laptop, tablet or other mobile device; and
- Capability to document exactly who had access to which facility at what time, even at the height of the crisis.

AUTHENTX™

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