

Advanced Solutions for Critical Infrastructure Protection

*Complying with the North American Electric
Reliability Corporation Critical Infrastructure
Protection standards*

Get this
White Paper



Contents

Introduction	3
NERC Critical Infrastructure Protection	4
Multifactor Authentication for Physical & Logical Access Control.....	6
Proven Authentication Solutions for NERC CIP Compliance.....	7
Compliance Summary	12
Entrust — Simplifying NERC CIP Compliance.....	14
A Single Integrated Platform.....	15
Entrust & You	18

Introduction

An attack on a utility — either through a cyberattack or physical entry to the facility — will have serious ramifications to citizens, causing severe economic damages and life-threatening situations.

In fact, recent evidence from the FBI indicates that terrorists are planning for such an attack. According to a [news release](#) by the U.S. Senate Committee on Homeland Security & Governmental Affairs, “An Al Qaeda video calling upon the ‘covert Mujahidin’ to commit ‘electronic jihad’ demonstrates the rapidly increasing threat of cyber-attack and underscores the pressing need for cybersecurity standards for the nation’s most critical networks.”¹

The committee went on to confirm that terrorist objectives targeting critical infrastructure.

“This is the clearest evidence we’ve seen that Al Qaeda and other terrorist groups want to attack the cyber systems of our critical infrastructure,” Homeland Security and Governmental Affairs Committee Chairman Joe Lieberman, ID-Conn., said. “Congress needs to act now to protect the American public from a possible devastating attack on our electric grid, water delivery systems, or financial networks, for example.”

This is clear, undeniable evidence for the immediate and ongoing need for advanced security solutions that protect the critical infrastructure managed by both private and government entities.



It is estimated that the destruction from a single wave of cyberattacks on U.S. critical infrastructures could exceed \$700 billion — the equivalent of 50 major hurricanes hitting U.S. soil at once.



— U.S. Cyber Consequence Unit

¹ [“Senators say video urging electronic jihad underscores need for cybersecurity standards.”](#) U.S. Senate Committee on Homeland Security & Governmental Affairs, May 22, 2012

NERC Critical Infrastructure Protection

In North America, the North American Electric Reliability Corporation (NERC) created the Critical Infrastructure Protection standards that each organization must comply with or face fines of up to \$1 million per day.

There are eight individual NERC CIP standards:

- **CIP-002 Critical Cyber Assets**
- **CIP-003 Security Management Controls**
- **CIP-004 Personnel & Training**
- **CIP-005 Electronic Security**
- **CIP-006 Physical Security**
- **CIP-007 Systems Security Management**
- **CIP-008 Incident Reporting & Response Planning**
- **CIP-009 Recovery Plans**

Compliance Definitions

The compliance process starts with a facilities-wide assessment addressing the requirements outlined in NERC CIP-002 Critical Cyber Asset Identification.

CIP-002 outlines definitions and a methodology to be used in defining Critical Assets (CA) and Critical Cyber Assets (CCA). NERC Standard CIP-002 requires that each facility develop a list of CCAs that are essential to the operation of its CA.

The NERC CIP Definition for Critical Assets (CA):

- “Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.”

The NERC CIP Definition for Critical Cyber Assets (CCA):

- “Cyber Assets essential to the reliable operation of Critical Assets.”
- The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter (typically TCP/IP).

Critical Infrastructure Protection: A Global Requirement

While the policies for protection vary around the world, the basic needs remain the same: ensure only authorized, trusted users are granted access to electronic and physical perimeters. We recommend a vendor that can take the best practices from the NERC CIP standard and apply them to a specific critical infrastructure as it makes sense.

The NERC CIP Definition for Electronic Security Perimeter:

- CIP-005 defines the Electronic Security Perimeter as the logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled. An access point, as defined by the NERC FAQ, is “any place where electronic traffic crosses the Electronic Security Perimeter.”

The NERC CIP Definition for Physical Security Perimeter:

- CIP-006 defines the Physical Security Perimeter as the physical, completely enclosed, border surrounding computer rooms, telecommunication rooms, operations centers and other locations in which Critical Cyber Asset are housed and for which access is controlled.

“

London 2012 authorities got cyber-attack warning on eve of Games; Security services warned of possible threat against Olympic power supply days before opening ceremony.

— **The Guardian, August 2012**

”

Multifactor Authentication for Physical & Logical Access Control

The Critical Infrastructure Protection standards require that the network be segmented to prevent an attack on one network being spread to the next network, and that strong two-factor authentication be used to ensure only authorized individuals may have physical and logical access to the critical assets.

Strong two-factor authentication is utilized for:

- Remote access to the networks
- Access to the Physical Security Perimeter
- Access to the Electronic Security Perimeter
- Access to specific Critical Assets

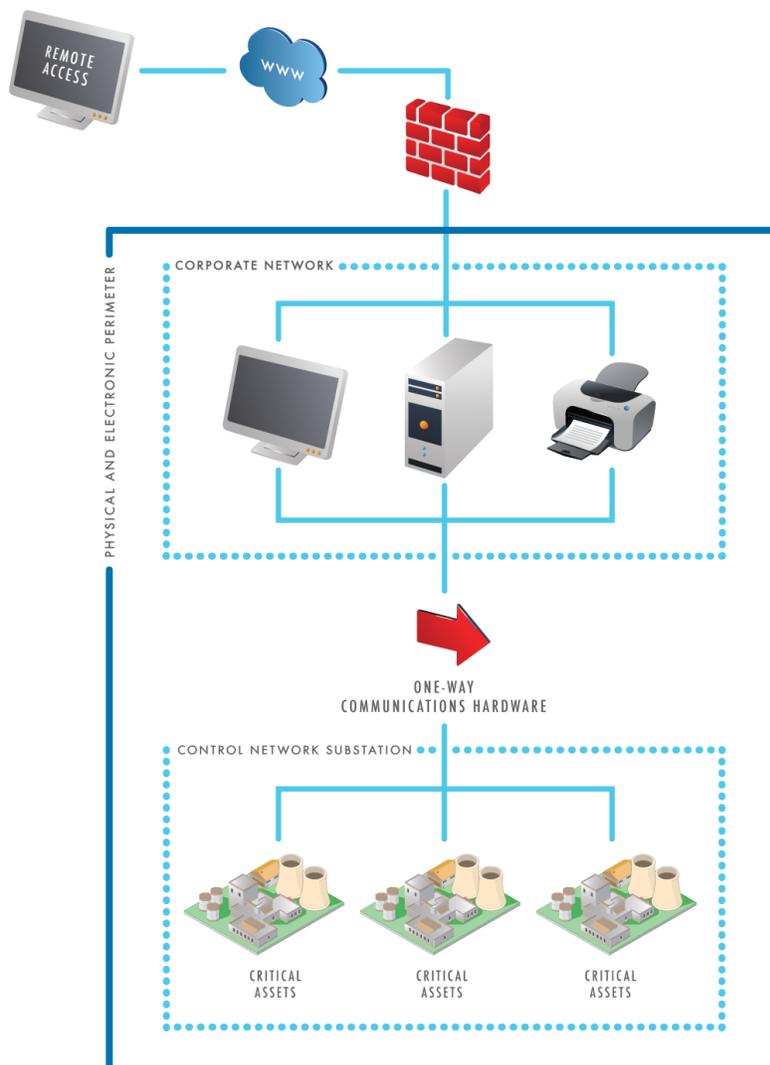


Figure 1
A high-level view of secure enterprise and control networks working to protect critical assets.

Proven Authentication Solutions for NERC CIP Compliance

Not every authentication solution can help organizations properly comply with NERC CIP standards. Outlined below is how a capable authentication platform should align with the CIP requirements.

CIP-004

Revoke Access to CCAs within 24 Hours for Personnel Terminated for Cause, and within 7 Days for Personnel who no Longer Require Access to CCAs

When a smart credential is issued or revoked using a strong authentication solution, the Certificate Revocation List (CRL) is instantly updated to deny access to Windows, Macintosh or Unix systems employing smartcard login, or FIPS-201 (PIV) systems using the PKI authentication option.

All other authenticators issued, such as OTPs, passwords or grid cards, are also denied any future authentications by sharing a common authentication platform and administration. These approaches are used for situations where the CCA is not smartcard-capable.

The authentication platform should be integrated into the enterprise's human resources system so any change to employee status is automatically acted on to avoid delays and mistakes.

CIP-005

The authentication platform should meet the following requirements:

- Provide for a range of authenticators, as not all applications support all authenticators
- The cost of the strongest authenticator may be too expensive for less-critical systems
- If an authenticator should be compromised by a future attack, the switch to the new authenticator needs to occur quickly
- The platform should support grid cards and one-time passcodes (OTP), which meet the needs of remote access at a low cost

With the introduction of CIP-007 version 5, the complexity of passwords standardizes on a range between 15 to 25 characters, depending on the type of account. Coupled with the need for random characters and frequent password changes, the enterprise should consider the usage of smartcards. This would eliminate the need for passwords and costly password resets.

Combining physical access, Microsoft Windows login access and remote access simplifies logistics, management and auditing for the enterprise. For the employee, it means just a single authenticator to carry and a simple PIN to remember.

The authentication platform should allow for multiple authenticators for the following purposes.

- Easy migration from one authenticator to another, such as one-time passcodes (OTP) to smartcards, at a pace the enterprise can support.
- The enterprise applications may only support specific authenticators.
- Allow the flexibility of using the best security for a low cost of a specific application.

A capable security vendor will use the modern FIPS-201 smartcard standard that allows for interoperability with a wide range of third-party products also compliant to the standard, such as Microsoft Windows 7 and several physical access systems. This approach also ensures the solution is certified by the NIST so the organization is sure the implementation does not have poor quality, security and privacy.

Smartcards, when utilized with a secure PIN entry device, is resistant to malware loaded onto the machine. A key-logger cannot steal the PIN to use in a future fraudulent authentication. (Any compromised machine, however, should be immediately removed from the network. In addition, the use of a layered security approach will help defend against attacks that defeat a single solution.)

When the card (employee) is not present, access will be denied. Placing the FIPS-201 application on a smartphone allows the range before denying access to be extended up to 80 feet. This is achieved by using near-field communication (NFC) or Bluetooth found on modern smartphones.

CIP-005

Only Authorized Machines Can Access the Electronic Security Perimeter

A compliant authentication solution should be able to issue digital certificates to laptops, desktops, servers and mobile devices so that only authorized devices can connect to the network.

CIP-006

Physical Access Controls

The authentication solution should support physical security in depth by combining the card authentication with a PIN or biometric for high-impact cyber systems, while simultaneously allowing for quick access to low-impact cyber systems.

Many of the existing physical access solutions have been compromised over the years, with easy-to-follow, low-cost instructions on the Web. Entrust suggests the migration to more secure physical access standards such as FIPS-201.

The NIST FIPS-201 standard is designed specifically for this type of deployment with four types of authentication:

1. *Card Holder Unique ID (CHUID)*

A numerical value representing the employee is digitally signed by the enterprise that issued the card, then stored on the card and transmitted to the reader when the card is energized by the reader.

The digital signature prevents an attacker from making their own card from scratch — if they know a valid employee number — because the attacker does not possess the enterprise's key to sign the CHUID. Any attempt to modify the CHUID will invalidate the signature when checked by the reader.

2. *Card Authentication Key (CAK)*

The reader will send the card a random challenge. The card digitally signs the challenge with its CAK private key and returns the challenge to the reader. As the private key cannot be taken from the card, the card cannot be cloned. The key cannot be extracted as defined by the FIPS-201 standard and enforced by the chip hardware.

The CAK private key is paired with a digital certificate that contains the identity. This certificate states the identity is an anonymous employee of the company. Since there is no privacy to protect, the PIN does not need to be entered. CAK should be used for fast access (no PIN) to a secure location where a specific person's identity is not required.

3. *PKI User*

This approach uses the same challenge-response process as CAK, but in this case the digital certificate has the employee name in it.

As such, to protect privacy and to allow the employee to approve the authentication, the PIN must be entered before the challenge is signed and returned. This approach is used when high security is required, and the enterprise needs to know the specific employee identity.

4. *Biometrics*

The FIPS-201 standard supports two types — IRIS and the more popular fingerprint. The physical access reader requests the previously stored fingerprint from the card. And because it contains private data, the employee must enter their PIN. The biometric is compared within the reader, and if they match the employee is allowed to enter.

To prevent the threat of a fraudulent fingerprint, the fingerprint is digitally signed during issuance by the enterprise.

The highest security is when the PKI user and the biometric are both required.

CIP-007

Establish an Auditable Workflow for Credential Issuance

A proper authentication solution will come with a workflow engine with multiple roles, allowing for independent groups with differing policy requirements and approvals.

In the case of a smartcard, an employee can be enrolled by *Role_A*, the issuance be approved by the senior manager as *Role_B*, and then the smartcard printed and distributed by *Role_C*. This separation of duty prevents the issuance of fraudulent authenticators.

The authentication solution should have the same workflow regardless of the authenticator type (e.g., a one-time passcode shares the same approvals as a smartcard).

Proper workflow allows for the step to perform a background check to be easily added prior to authenticator issuance. To satisfy periodic audits, an advanced solution will issue reports on all issued authenticators, as well as those that are active, along with the archived approvals. No other authenticators will have access to the physical or logical system.

The vendor of the authentication solution should proactively provide bulletins of any compromises of the technology put in place as the sophistication of attackers improves over time. This will support the annual NERC compliance audits while protecting assets from attack.

Compliance Summary

A capable security vendor should provide an integrated solution for both physical and logical access control, while also allowing for the easy migration from less-secure legacy systems to modern solutions — all without impacting the productivity and uptime of the entire system. The smartcard should simultaneously support both the legacy and modern systems.

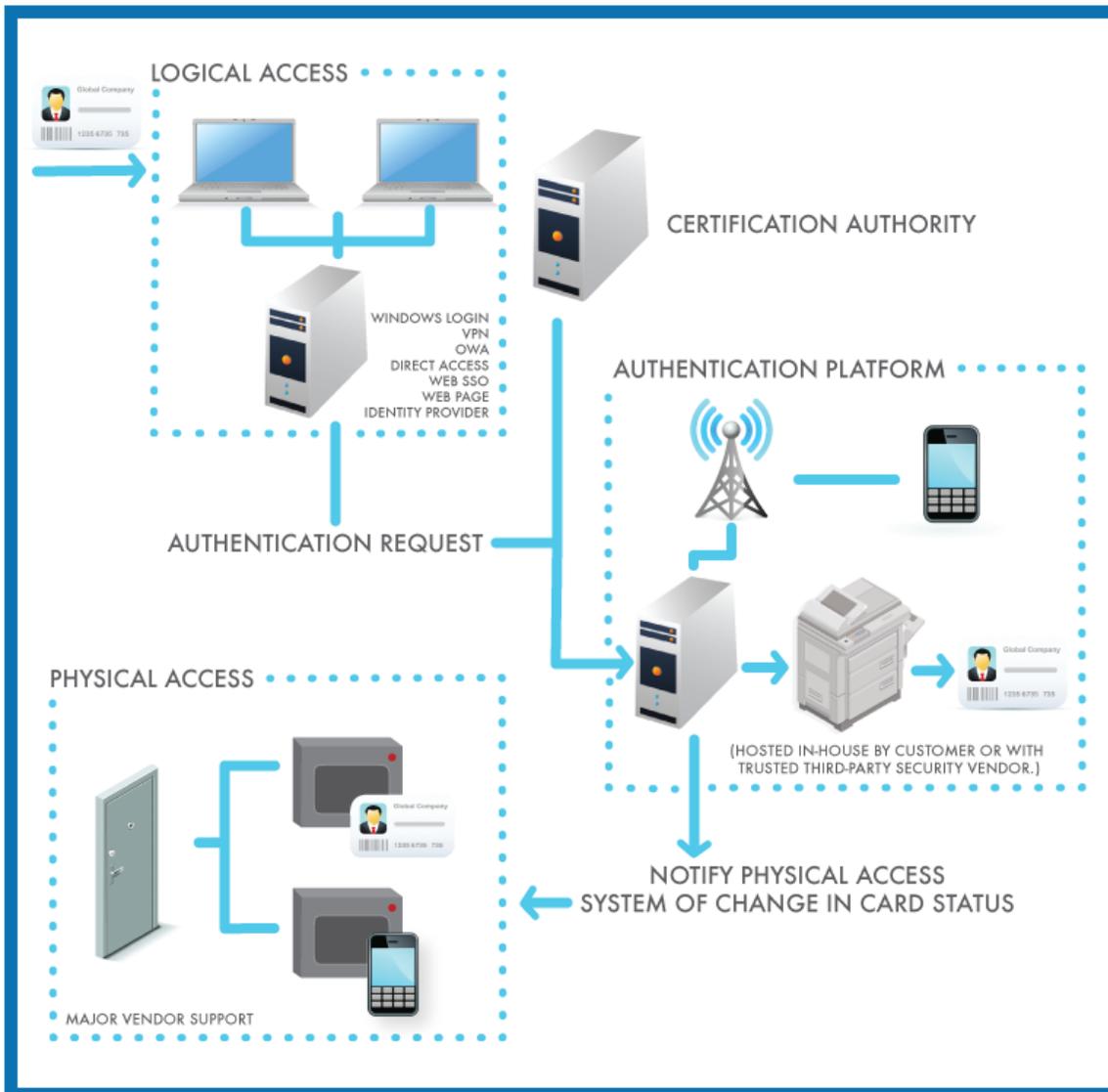


Figure 2: A cost-effective solution to meet the requirements of CIP-005, CIP-006 and CIP-007 offers a multifunction smartcard with a single platform for issuance, management and revocation. The platform also should allow for quick migration from a compromised authenticator. The solution should be tied into an HR system to control who is issued a credential and what they are authorized to access.

Employees need access to enterprise systems, but not all are smartcard-capable. As such, utility companies require a platform that supports a wide range of authenticators — often with one employee using more than one authenticator. Implement a central location to issue all authenticators and set consistent policies to meet CIP standards.

Historically, smartcards were cost-effective, but the logistics of card issuance proved to be complicated. Evolution in technology and critical security investment has made advanced smartcard solutions more realistic — and affordable.

Look for a vendor that has the capability to quickly issue temporary credentials that do not negatively affect employee productivity or compromise security. For example, this is important for the situation where the employee has left their credential at home.

“

Historically, smartcards were cost-effective, but the logistics of card issuance proved to be complicated. Evolution in technology and critical security investment has made advanced smartcard solutions more realistic — and affordable.

”

Entrust — Simplifying NERC CIP Compliance

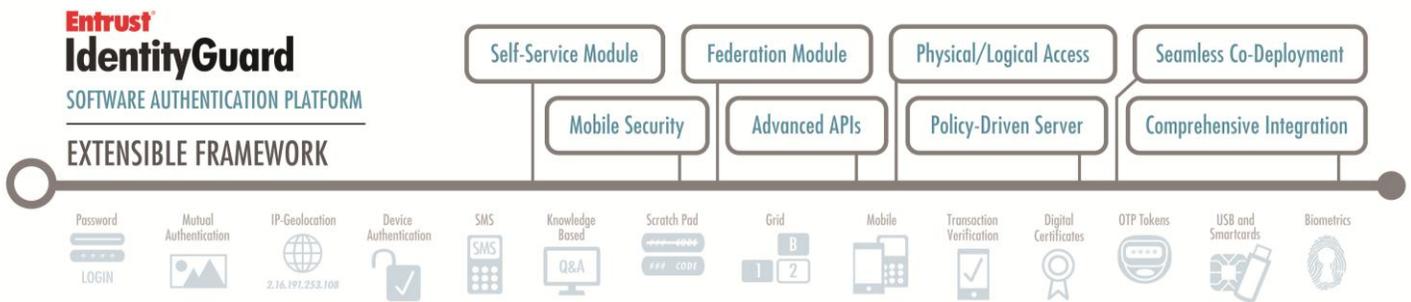
Entrust's comprehensive management framework serves as an organization's single software-based security platform that bridges emerging technologies for strong mobility, cloud and smart credentialing offerings.

By seamlessly integrating co-deployment measures, federation security, advanced APIs and self-service management tools, Entrust strengthens security, maximizes staff efficiency and reduces overall costs.

Entrust's flagship authentication solution, Entrust IdentityGuard, continues to lead the industry as one of the most robust software authentication platforms, delivering an unmatched breadth of capabilities and flexibility to meet the most demanding security environments.

The solution enables organizations to layer security — according to access requirements or the risk of a given transaction — across diverse users and applications.

Entrust's authentication capabilities include smartcards and USB tokens, soft tokens, grid cards and eGrids, IP-geolocation, questions and answers, mobile smart credentials, out-of-band one-time passcode (delivered via voice, SMS or email), biometrics, and a range of one-time-passcode tokens.



A Single Integrated Platform

Compliance to NERC CIP calls for a truly integrated physical and logical solution that's compatible with both legacy and modern systems.

Entrust IdentityGuard may be deployed as an easy-to-use, fully integrated in-house solution, or as a managed service where card issuance is managed offsite and delivered to the utility organization as a service.

Entrust IdentityGuard issuance-approval workflow, along with the related logs, will serve as evidence for CIP audits to prove compliance.

Secure Remote Access

Aligning with Entrust's aforementioned suggestions for CIP compliance, Entrust IdentityGuard issues both one-time passcodes and smartcards for authentication.

Entrust smartcards are FIPS 201-compliant, allowing for seamless interoperability with the most popular third-party products also compliant to the standard.

Using an optional CodeBench ID-Sync module, all Entrust IdentityGuard physical access systems are instantly notified of card revocation, which stops any further access.

Optionally, the Entrust IdentityGuard credential creation/revocation capability may be integrated with the corporate identity management solution through an easy-to-use Web services API.

When a person joins or leaves the enterprise, all systems are instantly and automatically made aware, meeting the 24-hour CIP requirement, and removing the chance of human error.

Smartcard Issuance & Interoperability

Entrust IdentityGuard not only integrates with both card-issuance and physical access control, but Entrust tests a wide variety of physical access equipment to ensure expertise in what systems are more secure, and which systems are interoperable with each other.

Unlike an OTP, the private key representing the employee is only stored on the Entrust IdentityGuard-issued smartcard and cannot be stolen off the device and used to create a duplicate or cloned identity card. It is protected by sophisticated hardware controls.

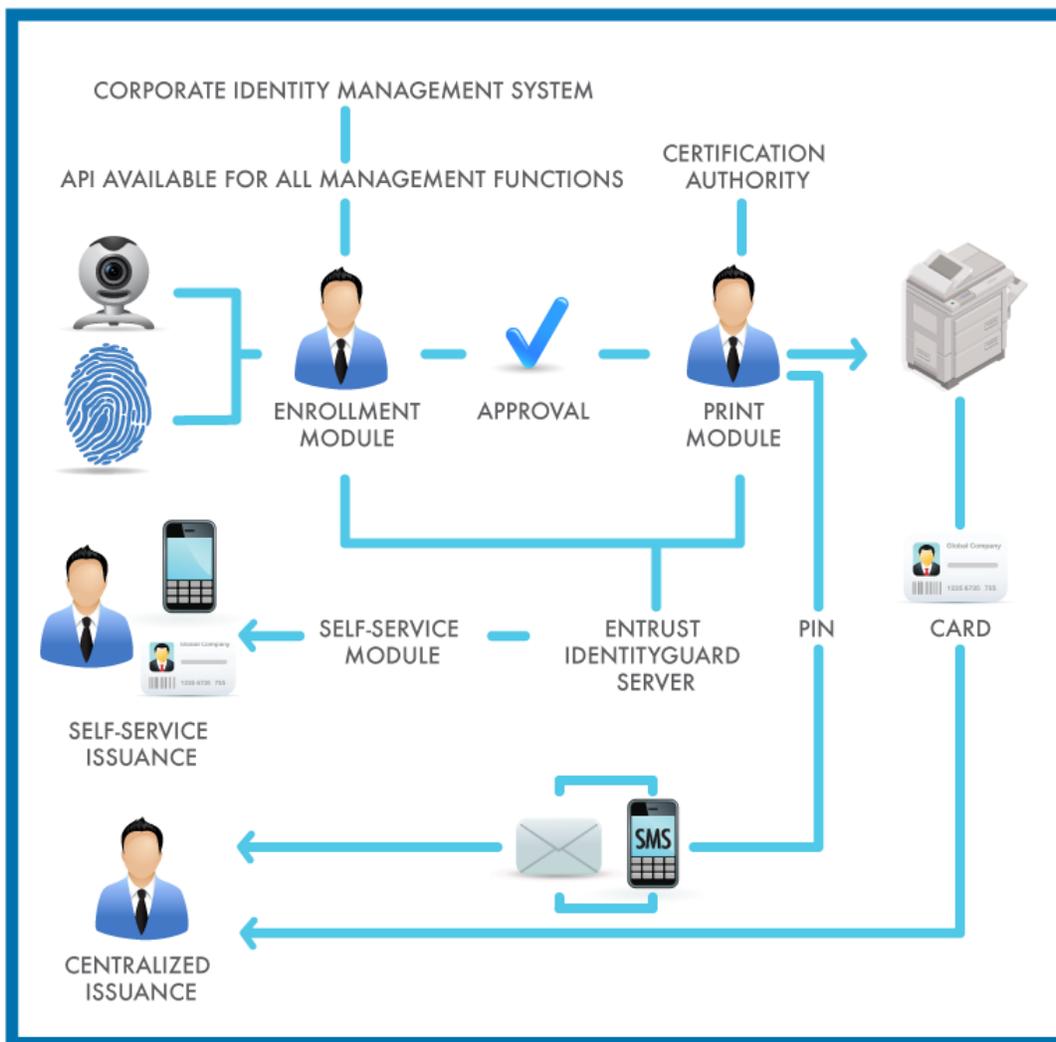


Figure 3: Entrust IdentityGuard serves as a utility company's comprehensive smartcard issuance and management solution for NERC CIP compliance.

Entrust IdentityGuard also leverages near-field communication (NFC) or Bluetooth standards found on modern smartphones. This capability only requires each employee carry one device, enables remote issuance of a strong authenticator, and allows control over the distance an employee must be from a cyber-asset before being logged off.

The Entrust solution makes compliance as simple as printing a card then distributing it to an employee. The smartcard is ready to use by simply inserting it into the computer. For more sensitive assets, the Entrust solution can require a biometric (in addition to the card itself) and a PIN.

Authorizing Machines & Devices

Entrust IdentityGuard issues digital certificates to laptops, desktops, servers, machines and mobile devices so that only authorized devices may connect to the network.

Entrust IdentityGuard also possess an authentication API that may be integrated with cyber-asset systems. The API utilizes industry standards, Web services, SAML and Radius protocols.

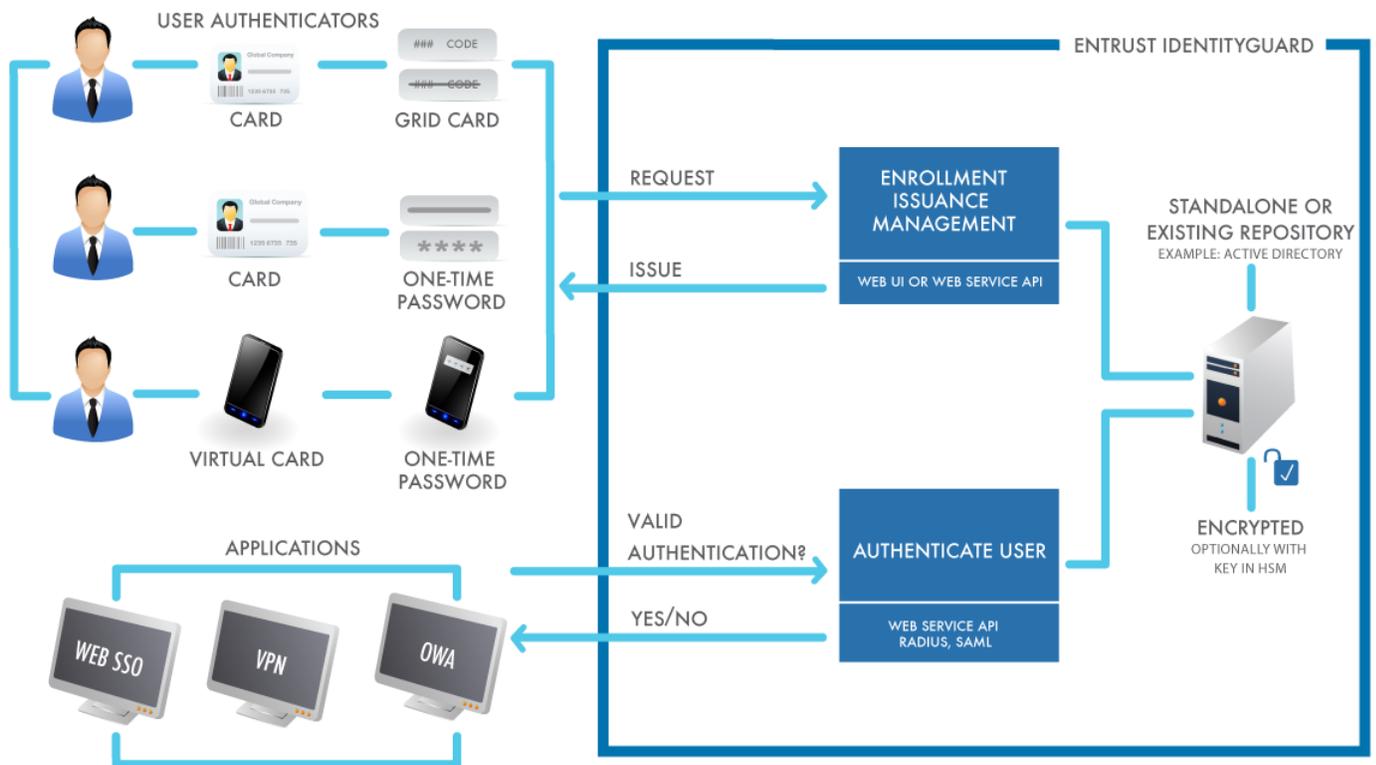


Figure 4: An overview outlining how Entrust IdentityGuard authenticates users while concurrently serving as a comprehensive card management solution.

Entrust & You

More than ever, Entrust understands your organization's security pain points. Whether it's the protection of information, securing online customers, regulatory compliance or large-scale government projects,

Entrust provides identity-based security solutions that are not only proven in real-world environments, but cost-effective in today's uncertain economic climate.

Entrust secures governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL.

For more information about Entrust products and services, call **888-690-2424**, email entrust@entrust.com or visit entrust.com.

Company Facts

Website: www.entrust.com
Employees: 359
Customers: 5,000
Offices: 10 Globally

Headquarters

Three Lincoln Centre
5430 LBJ Freeway, Suite 1250
Dallas, Texas 75240

Sales

North America: 1-888-690-2424
EMEA: +44 (0) 118 953 3000
Email: entrust@entrust.com

follow us on
twitter  **tweet**