NERC CIP Compliance

This document is intended to give a point by point summary of how the AuthentX^{TM} Identity Management System for Physical and Logical Access Control both complies with and can help your utility achieve NERC CIP compliance.

NERC CIP-004: Personnel and Training	
CIP-004-6 R3.4 Criteria or process for verifying that personnel risk assessments performed for contractors or service vendors are conducted according to Parts 3.1 through 3.3.	XTec's vetted employees and contractors will have access to your organization's user database. Because we serve federal clients all of our data center employees have at least a Secret clearance. Background information for this clearance goes back between ten years and the person's lifetime. The clearance is renewed every five years.
CIP-004-6 R3.5 Process to ensure that individuals with authorized electronic or authorized unescorted physical access have had a personnel risk assessment completed according to Parts 3.1 to 3.4 within the last seven years.	The date of the employee's most recent personnel risk assessment can be stored in AuthentX and read from there when needed. If the employee has not had a new PRA seven years later, their physical and electronic access to BES Cyber Systems will be disabled, although you can set a different expiration period if preferred.
CIP-004-6 R4.1.1 and R4.1.2 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.1. Electronic access; 4.1.2. Unescorted physical access into a Physical Security Perimeter .	A single XTec PIV card can be used to authorize both physical access to facilities and electronic access to personal systems and the network(s) they are attached to. All access is logged.
CIP-004-6 R4.1.3 Process to authorize based on need, as determined by the Responsible Entity, except for CIP Exceptional Circumstances: 4.1.3. Access to designated storage locations, whether physical or electronic, for BES Cyber System Information.	XTec stores the customer's user database in our three geographically dispersed data centers. Our data centers are staffed entirely by vetted XTec employees and contractors. Therefore, AuthentX can provide XTec's power industry customers the specific access authorization evidence required for compliance with this requirement.
CIP-004-6 R4.2 Verify at least once each calendar quarter that individuals with active electronic access or unescorted physical access have authorization records.	Whenever needed, AuthentX can provide a list of all users provisioned for physical or electronic access to any Cyber Asset. This can be compared to the list(s) of users authorized to access each asset.

NERC CIP-004: Personnel and Training	
CIP-004-6 R4.3 For electronic access, verify at least once every 15 calendar months that all user accounts, user account groups, or user role categories, and their specific, associated privileges are correct and are those that the Responsible Entity determines are necessary.	AuthentX includes a full Roles capability. The Roles module shows all permissions that are tied to each role, allowing the administrator to determine whether they are appropriate and make changes as required.
CIP-004-6 R4.4 Verify at least once every 15 calendar months that access to the designated storage locations for BES Cyber System Information, whether physical or electronic, are correct and are those that the Responsible Entity determines are necessary for performing assigned work functions.	Some NERC entities classify their user database as BCSI. XTec stores the customer's user database in our three data centers. Our data centers are staffed entirely by vetted XTec employees and contractors. Both physical and logical access to the database is strictly controlled, and we regularly verify that all access is necessary. Therefore, XTec can provide our power industry customers the required evidence that we have verified employee access to BCSI storage locations at least every 15 months.
CIP-004-6 R5.1 A process to initiate removal of an individual's ability for unescorted physical access and Interactive Remote Access upon a termination action, and complete the removals within 24 hours of the termination action.	All of an individual's physical access to facilities and electronic access to systems will be removed within one hour or less of the termination being entered in AuthentX. Also, if the remote system used by the individual to conduct Interactive Remote Access is authenticated by AuthentX, the user will not be able to conduct IRA as soon as their account is disabled in AuthentX.
CIP-004-6 R5.2 For reassignments or transfers, revoke the individual's authorized electronic access to individual accounts and authorized unescorted physical access that the Responsible Entity determines are not necessary by the end of the next calendar day following the date that the Responsible Entity determines that the individual no longer requires retention of that access.	All of an employee's physical access to facilities and electronic access to systems will be revoked within one hour of the reassignment or transfer being entered in AuthentX.
CIP-004-6 R5.3 For termination actions, revoke the individual's access to the designated storage locations for BES Cyber System Information, whether physical or electronic (unless already revoked according to Requirement R5.1), by the end of the next calendar day following the effective date of the termination action.	XTec stores the customer's user database in our three data centers. Our data centers are staffed entirely by vetted XTec employees and contractors, all of whom have Secret clearances. Therefore, XTec can provide our power industry customers the specific access revocation evidence required for compliance with this requirement.

NERC CIP-004: Personnel and Training	
CIP-004-6 R5.4 For termination actions, revoke the individual’s non-shared user accounts (unless already revoked according to Parts 5.1 or 5.3) within 30 calendar days of the effective date of the termination action.	All of an employee’s access to non-shared user accounts will be revoked within one hour or less of the termination being entered in AuthentX.

NERC CIP-005: Electronic Security Perimeter	
CIP-005-6 R2.2 For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.	XTec supports any VPN software that supports X.509 certificates.
CIP-005-6 R2.3 Require multi-factor authentication for all Interactive Remote Access sessions.	XTec PIV cards can authenticate using a certificate, PIN, or fingerprint scan, so the same card the remote employee uses to sign into their system while at work can authenticate them when conducting IRA remotely, if the remote system is also protected by AuthentX.

NERC CIP-006: Physical Security for BES Cyber Systems	
CIP-006-6 R1.2 Utilize at least one physical access control to allow unescorted physical access into each applicable Physical Security Perimeter to only those individuals who have authorized unescorted physical access.	The XTec PIV card provides three authenticators of an individual's identity, including possession of the card itself, a PIN and the fingerprint scan.
CIP-006-6 R1.3 Where technically feasible, utilize two or more different physical access controls (this does not require two completely independent physical access control systems) to collectively allow unescorted physical access into Physical Security Perimeters to only those individuals who have authorized unescorted physical access.	AuthentX can provide access logs in almost any format required.

NERC CIP-007: Systems Security Management	
CIP-007-6 R1.1 Where technically feasible, enable only logical network accessible ports that have been determined to be needed by the Responsible Entity, including port ranges or services where needed to handle dynamic ports. If a device has no provision for disabling or restricting logical ports on the device then those ports that are open are deemed needed.	**PACS** AuthentX requires only three specific logical ports to be open; XTec can provide the technical reasons why they need to be open.
CIP-007-6 R2.1 A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	**PACS** XTec is the sole patch source for AuthentX. We remotely apply the firmware updates to the XNode. We can provide the documentation needed to comply with all of the parts of CIP-007 R2.
CIP-007-6 R2.2 At least once every 35 calendar days, evaluate security patches for applicability that have been released since the last evaluation from the source or sources identified in Part 2.1.	**PACS** XTec is the sole patch source for AuthentX. We remotely apply the firmware updates to the XNode. We can provide the documentation needed to comply with all of the parts of CIP-007 R2.

NERC CIP-007: Systems Security Management

CIP-007-6 R2.3 For applicable patches identified in Part 2.2, within 35 calendar days of the evaluation completion, take one of the following actions: · Apply the applicable patches; or · Create a dated mitigation plan; or · Revise an existing mitigation plan. Mitigation plans shall include the Responsible Entity's planned actions to mitigate the vulnerabilities addressed by each security patch and a timeframe to complete these mitigations.	**PACS** XTec is the sole patch source for AuthentX. We remotely apply the patches to the XNode. We can provide the documentation needed to comply with all of the parts of CIP-007 R2.
CIP-007-6 R4.1 Log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, Cyber Security Incidents that includes, as a minimum, each of the following types of events: 4.1.1. Detected successful login attempts; 4.1.2. Detected failed access attempts and failed login attempts; 4.1.3. Detected malicious code.	For BES Cyber Systems, BES Cyber Assets, and Protected Cyber Assets protected by PIV card technology, XTec can log successful login attempts, failed access attempts and failed login attempts. **PACS** AuthentX can log successful login attempts, failed access attempts and failed login attempts .
CIP-007-6 R4.2 Generate alerts for security events that the Responsible Entity determines necessitates an alert, that includes, as a minimum, each of the following types of events (per Cyber Asset or BES Cyber System capability): 4.2.1. Detected malicious code from Part 4.1; and 4.2.2. Detected failure of Part 4.1 event logging.	For BES Cyber Systems and Protected Cyber Assets, XTec can generate alerts for detected malicious code from Part 4.1, and for failure of Part 4.1 event logging. **PACS** AuthentX can generate alerts for detected malicious code from Part 4.1, and for failure of Part 4.1 event logging.
CIP-007-6 R5.1 Have a method(s) to enforce authentication of interactive user access, where technically feasible.	XTec's PIV card, along with the AuthentX IDMS, authenticates interactive user access to BES Cyber Systems and Protected Cyber Assets. **PACS** AuthentX authenticates interactive user access to the system itself using the user's PIV card.
CIP-007-6 R5.3 Identify individuals who have authorized access to shared accounts.	The need for shared accounts goes away when each user only has to insert their PIV card in order to access a system.

NERC CIP-007: Systems Security Management

CIP-007-6 R5.4 Change known default passwords, per Cyber Asset capability.	When the user authenticates with a PIV card, default passwords cannot be utilized.
CIP-007-6 R5.5 For password-only authentication for interactive user access, either technically or procedurally enforce the following password parameters: 5.5.1. Password length that is, at least, the lesser of eight characters or the maximum length supported by the Cyber Asset; and 5.5.2. Minimum password complexity that is the lesser of three or more different types of characters (e.g., uppercase alphabetic, lowercase alphabetic, numeric, nonalphanumeric) or the maximum complexity supported by the Cyber Asset.	With XTec PIV cards and card readers, there is no need to have complex passwords. This is because the PIV card provides three authenticators of an individual's identity, including possession of the card itself, a PIN and the fingerprint scan.
CIP-007-6 R5.6 Where technically feasible, for password-only authentication for interactive user access, either technically or procedurally enforce password changes or an obligation to change the password at least once every 15 calendar months.	With XTec PIV cards and card readers, there is no need for passwords, just a PIN .
CIP-007-6 R5.7 Where technically feasible, either: · Limit the number of unsuccessful authentication attempts; or · Generate alerts after a threshold of unsuccessful authentication attempts.	When users are authenticated using PIV cards, there is no password for an attacker to guess. Any attempt to use an invalid PIV card will be immediately blocked, logged and alerted on. Any use of a valid card by a user other than the user whose fingerprint scan is stored on the card will be immediately blocked, logged and alerted on. Any attempt to enter a PIN more than a certain number of attempts (set by the organization) will be blocked, logged and alerted on.

NERC CIP-010: Configuration Change Management

CIP-010-3 R1.1 Develop a baseline configuration, individually or by group, which shall include the following items: 1.1.1. Operating system(s) (including version) or firmware where no independent operating system exists; 1.1.2. Any commercially available or open-source application software (including version) intentionally installed; 1.1.3. Any custom software installed; 1.1.4. Any logical network accessible ports; and	**PACS** The XNode is a sealed device updated remotely by XTec. This means that XTec can provide you the baseline configuration of the XNode whenever you need to have it, including all updates that have been applied.

NERC CIP-011: Information Protection

CIP-011-2 R1.2 Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.	If your organization identifies the user database stored at XTec's data centers as BCSI, we will be able to comply with your information protection plan's requirements for protecting and securely handling BES Cyber System Information, including storage, transit, and use. For example, both the user database and the media on which it is installed are encrypted, and all data in transit both to and from our data centers is encrypted with TLS.
CIP-011-2 R2.1 Prior to the release for reuse of applicable Cyber Assets that contain BES Cyber System Information (except for reuse within other systems identified in the "Applicable Systems" column), the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset data storage media.	XTec is the only tenant in its three data centers, which are operated by vetted XTec employees and contractors. Once a system is no longer needed for use in our data centers, we always destroy the storage media; we do not reuse any media. We can provide all required evidence that we have done this for every device on which your organization's user database was stored, in whole or in part.
CIP-011-2 R2.2 Prior to the disposal of applicable Cyber Assets that contain BES Cyber System Information, the Responsible Entity shall take action to prevent the unauthorized retrieval of BES Cyber System Information from the Cyber Asset or destroy the data storage media.	Because most of XTec's other customers are federal agencies and are required to follow the NIST SP 800-53 framework, XTec already makes all information stored on Cyber Assets unavailable upon disposal, by physically destroying the storage media. XTec can also provide all required evidence that we did this in every instance in which a system containing a customer's user data was disposed of.

The following apply to low impact assets and BES Cyber Systems.

NERC CIP-003: Security Management Controls	
CIP-003-8 R2 Attachment 1 Section 2 Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.	A single XTec PIV card can be used for physical access to a low impact Control Center, transmission substation or generating station, as well as to the low impact BES Cyber Systems located at the asset. This same card can be used for access to medium and high impact facilities and BCS as well.
CIP-003-8 R2 Attachment 1 Section 3.1 Electronic Access Controls: For each asset containing low impact BES Cyber System(s) identified pursuant to CIP-002, the Responsible Entity shall implement electronic access controls to: 3.1 Permit only necessary inbound and outbound electronic access as determined by the Responsible Entity for any communications that are: i. between a low impact BES Cyber System(s) and a Cyber Asset(s) outside the asset containing low impact BES Cyber System(s); ii. using a routable protocol when entering or leaving the asset containing the low impact BES Cyber System(s); and iii. not used for time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR61850-90-5 R-GOOSE).	*A NERC drafting team is currently drafting CIP-003-9, which will possibly require encryption and multi-factor authentication of vendor remote access sessions. If the vendor has deployed PIV cards to authenticate their employees (whether or not they are XTec PIV cards), they will be accepted by AuthentX.*