



NERC CIP Compliance

How XTEC can help you comply with 33 NERC CIP requirement parts

If your organization has medium or high impact assets and BES Cyber Systems, XTEC can help you save significant amounts of time and money in complying with the requirements of CIP-003-8 through CIP-011-3 – by deploying XTEC PIV cards, AuthentX (XTEC’s Identity Management System) and XNode (the XTEC PACS edge appliance). The table below lists CIP requirements and requirement parts, as well as how XTEC can help you comply with each one.

Note that in the table, we have identified the ways XTEC can help you with CIP compliance:

- Through deployment of AuthentX and XTEC PIV cards (column 2)
- Through deployment of XNode (column 3)
- Through implementation of AuthentX in the XTEC data center (column 4)

Since all XTEC implementations include all of these components, your organization will be able to benefit from everything listed in the table, if you implement XTEC’s solution.

Because the items in columns 3 and 4 have to do with XTEC’s products and services, and because we want to take on as much of your work for compliance documentation as we can, we will provide you with CIP compliance documentation for all of the requirement parts that have entries in columns 3 or 4. The documentation will be based on templates provided by a former CIP auditor for one or more of the NERC Regional Entities. XTEC will coordinate with your organization to make sure the documentation we prepare will meet your needs.

Please note that the entries in column 4 are included under the assumption that your organization has decided that your user database constitutes BES Cyber System Information (BCSI). If you do not treat it as such, then the activities performed in the XTEC data center as part of the XTEC offering are not in scope for NERC CIP at all, and column 4 can be ignored.

Please also note that you can deploy AuthentX so that all IT and OT systems, users and physical assets are enrolled in AuthentX; almost all of our customers have deployed it this way. However, you can also limit AuthentX to some subset of those systems, users and assets, perhaps as part of a pilot project.

NERC CIP-004: Personnel and Training

Requirement Part	AuthentX and XTec PIV cards	XNode (PACS)	AuthentX in XTec data center
<p>CIP-004-6 R2.2 Require completion of the training specified in Part 2.1 prior to granting authorized electronic access and authorized unescorted physical access to applicable Cyber Assets, except during CIP Exceptional Circumstances.</p>	<p>The employee’s training status, including expiration date, can be stored on the PIV card. A new employee can be prevented from obtaining logical access to BES Cyber Systems (BCS), or to physical assets like Medium impact substations, until they have completed their training.</p>		<p>XTec’s data center employees will be prevented from having physical access to any system containing your organization’s data until they have completed your specific training.</p>
<p>CIP-004-6 R2.3 Require completion of the training specified in Part 2.1 at least once every 15 calendar months.</p>	<p>If the employee has not renewed their training before the renewal date, they can be prevented from obtaining logical or physical access to BES Cyber Systems (BCS).</p>		<p>After 15 months, XTec’s data center employees will be prevented from having physical access to any system containing your organization’s data, until they have re-completed your training.</p>
<p>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.</p>	<p>XTec can provide the attestations or redacted PRAs that you require for compliance with R3.4.</p>		<p>Some of XTec’s data center employees will have physical (although not logical) access to the systems containing your organization’s user database. Because we serve many 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 up to every five years. We can provide documentation of our PRA process in the required format, as well as records verifying when the last background check was performed, for every XTec data center employee with physical access to systems that store your user database.</p>



NERC CIP-004: Personnel and Training

Requirement Part	AuthentX and XTec PIV cards	XNode (PACS)	AuthentX in XTec data center
<p>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.</p>	<p>The date of the employee's most recent personnel risk assessment can be stored on the PIV card and read from there when needed. If the employee has not had a new PRA seven years later, physical and electronic access to BES Cyber Systems can be prevented.</p>		
<p>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.</p>	<p>A single XTec PIV card can be used to authorize both electronic access to BCS, EACMS and PACS, and physical access to a PSP. All access is logged.</p>		
<p>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.</p>			<p>XTec stores the customer's user database in our three data centers. Our data centers are staffed entirely by vetted XTec employees and contractors. Therefore, XTec can provide power industry customers the specific access authorization evidence required for compliance with this requirement.</p>
<p>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.</p>	<p>Whenever needed, AuthentX can provide a list of all users provisioned for physical or electronic access to any Cyber Asset, including BCS, EACMS and PACS. This can be compared to the list(s) of users authorized to access each asset to identify any discrepancies.</p>		
<p>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.</p>	<p>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.</p>		



NERC CIP-004: Personnel and Training

Requirement Part	AuthentX and XTEC PIV cards	XNode (PACS)	AuthentX in XTEC data center
<p>CIP-004-6 R4.4 Verify at least once every 15 calendar months that access permissions 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.</p>			<p>XTEC stores the customer’s user database in our three data centers. Our data centers are staffed entirely by vetted XTEC employees and contractors. Physical 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, if the customer elects to consider the user database to be BCSI.</p>
<p>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.</p>	<p>All of an individual’s physical access to facilities and electronic access to systems will be removed within one hour 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.</p>		
<p>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.</p>	<p>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.</p>		



NERC CIP-004: Personnel and Training			
Requirement Part	AuthentX and XTec PIV cards	XNode (PACS)	AuthentX in XTec data center
<p>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.</p>	<p>As in the case of access to facilities and systems, AuthentX will revoke an individual’s access to BCSI storage locations within one hour of the termination being entered in AuthentX, as long as those locations have been appropriately designated in AuthentX.</p>		<p>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.</p>
<p>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.</p>	<p>All of an employee’s access to non-shared user accounts will be revoked within one hour of the termination being entered in AuthentX.</p>		
<p>CIP-004-6 R5.5 For termination actions, change passwords for shared account(s) known to the user within 30 calendar days of the termination action. For reassignments or transfers, change passwords for shared account(s) known to the user within 30 calendar days following the date that the Responsible Entity determines that the individual no longer requires retention of that access.</p>	<p>On any supported device, users should not need passwords at all when XTec PIV cards are in use. Someone who doesn’t a) have physical access to the device protected by XTec; b) have a valid PIV card; c) know the user’s PIN; or d) provide a fingerprint scan that matches the template on the card can never access the device. This means there will no longer be any need for shared passwords for supported devices. The only thing the user needs to remember will be their simple PIN.</p>		



NERC CIP-005: Electronic Security Perimeter

Requirement Part	AuthentX and XTec PIV cards	XNode (PACS)	AuthentX in XTec data center
<p>CIP-005-6 R2.2 For all Interactive Remote Access sessions, utilize encryption that terminates at an Intermediate System.</p>	<p>XTec supports any VPN software that supports X.509 certificates. So IRA won't require separate authentication for VPN access, since the VPN software can authenticate the user based on their certificate stored on their PIV card.</p>		
<p>CIP-005-6 R2.3 Require multi-factor authentication for all Interactive Remote Access sessions.</p>	<p>XTec PIV cards can authenticate using a certificate, PIN and/or fingerprint scan, so the same card the remote employee uses to access their system while at work can authenticate them when conducting IRA remotely, if the remote system is also protected by AuthentX.</p>		

NERC CIP-006: Physical Security for BES Cyber Systems

<p>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.</p>	<p>The XTec PIV card provides three authenticators of an individual's identity, including possession of the card itself, a PIN and the fingerprint scan.</p>		
--	--	--	--

NERC CIP-006: Physical Security for BES Cyber Systems

Requirement Part	AuthentX and XTec PIV cards	XNode (PACS)	AuthentX in XTec data center
<p>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.</p>	<p>The XTec PIV card provides three authenticators of an individual's identity, including possession of the card itself (something you have), a PIN (something you know), and the fingerprint scan (something you are).</p>		
<p>CIP-006-6 R1.8 Log (through automated means or by personnel who control entry) entry of each individual with authorized unescorted physical access into each Physical Security Perimeter, with information to identify the individual and date and time of entry.</p>	<p>AuthentX can provide access logs in almost any format required.</p>		

NERC CIP-007: Systems Security Management

<p>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.</p>		<p>The XNode requires only three specific logical ports to be open; XTec can provide the technical reasons why they need to be open.</p>	
---	--	--	--



NERC CIP-007: Systems Security Management

Requirement Part	AuthentX and XTec PIV cards	XNode (PACS)	AuthentX in XTec data center
<p>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.</p>		<p>XTec is the sole patch source for the XNode. 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.</p>	
<p>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.</p>		<p>XTec is the sole patch source for the XNode. 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.</p>	
<p>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.</p>		<p>XTec is the sole patch source for the XNode. 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.</p>	



NERC CIP-007: Systems Security Management

Requirement Part	AuthentX and XTec PIV cards	XNode (PACS)	AuthentX in XTec data center
<p>CIP-007-6 R3.1 Deploy method(s) to deter, detect, or prevent malicious code.</p>		<p>The XNode is a sealed appliance. All software updates and patches are loaded remotely, and a digital signature is checked before they are loaded. XTec scans all updates and patches before applying them, meaning there is virtually no way that malicious code could penetrate an XNode. In other words, our method of applying updates and patches to the XNode prevents malicious code. We can provide documentation of that fact, as well as any required evidence of the processes we follow.</p>	
<p>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.</p>	<p>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.</p>	<p>The XNode can log successful login attempts, failed access attempts, failed login attempts, and detected malicious code.</p>	
<p>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.</p>	<p>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.</p>	<p>The XNode can generate alerts for detected malicious code from Part 4.1, and for failure of Part 4.1 event logging.</p>	



NERC CIP-007: Systems Security Management

Requirement Part	AuthentX and XTec PIV cards	XNode (PACS)	AuthentX in XTec data center
<p>CIP-007-6 R5.1 Have a method(s) to enforce authentication of interactive user access, where technically feasible.</p>	<p>XTec’s PIV card, along with the AuthentX IDMS, authenticates interactive user access to BES Cyber Systems and Protected Cyber Assets, without the need for a password.</p>	<p>The XNode authenticates interactive user access to the system itself, using the user’s PIV card.</p>	
<p>CIP-007-6 R5.3 Identify individuals who have authorized access to shared accounts.</p>	<p>The need for shared accounts goes away when each user only has to insert their PIV card (and when needed scan their finger) in order to access a system.</p>		
<p>CIP-007-6 R5.4 Change known default passwords, per Cyber Asset capability</p>	<p>When the user authenticates with a PIV card, default passwords cannot be utilized.</p>		
<p>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.</p>	<p>With XTec PIV cards and card readers, there is no need to have passwords, whether complex or otherwise. 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. In other words, this requirement part doesn’t apply because this isn’t “password-only” authentication.</p>		
<p>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.</p>	<p>With XTec PIV cards and card readers, there is no need for passwords, just a short PIN.</p>		



NERC CIP-007: Systems Security Management			
Requirement Part	AuthentX and XTec PIV cards	XNode (PACS)	AuthentX in XTec data center
<p>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.</p>	<p>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 beyond a certain number of attempts (set by the organization) will be blocked, logged and alerted on.</p>		

NERC CIP-010: Configuration Change Management			
<p>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 1.1.5. Any security patches applied.</p>		<p>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.</p>	



NERC CIP-011: Information Protection

Requirement Part	AuthentX and XTec PIV cards	XNode (PACS)	AuthentX in XTec data center
<p>CIP-011-2 R1.2 Procedure(s) for protecting and securely handling BES Cyber System Information, including storage, transit, and use.</p>			<p>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.</p> <p>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.</p>
<p>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.</p>			<p>XTec is the only tenant in its three data centers, which are operated by XTec employees and contractors.</p> <p>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.</p>
<p>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.</p>			<p>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 possibly containing a customer’s user data was disposed of.</p>



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.

With appropriate permissions, 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. Of course, this same card can be used for access to medium and high impact facilities and BCS as well, if the customer's policy permits that.

CIP-003-9

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 using remote access has deployed PIV cards to authenticate their employees (whether or not they are XTec PIV cards), they can be accepted.

