EXECUTIVE BRIEF

Integrating XPN into public key infrastructure (PKI)

Greater security, authentication, and scalability of the energy ecosystem

Introduction

Integrating public key infrastructure (PKI) with Intertrust Explicit Private Network (XPN) helps energy organizations to fortify the authentication security and scalability of their data and device ecosystems.

PKI, a trusted framework for secure data transmission, combines asymmetric cryptography and secure key management. XPN provides a decentralized encryption schema that protects data at rest and in transit across any disparate set of device and protocol networks. This amalgamation elevates data security to new heights, reducing the risk of cyberattacks and single points of failure.

In today's data energy ecosystem management, data and device vulnerabilities are multiplying and evolving as IT and OT infrastructures converge. Authentication security is crucial for safeguarding these newly connected systems. By leveraging PKI's encryption and identity verification capabilities, augmented by XPN's network decentralized and tamper-resistant nature, energy organizations can find the robust protection they need.

PKI and XPN solve fundamental problems such as the ability to protect and manage legacy IoT devices and integrate proprietary AI software platforms from a multitude of third party vendors. Attacks and vulnerabilities stemming from insecure networks and protocols are fully mitigated. Scalability is equally vital, given the expanding complexity of energy data management. XPN's decentralized structure, combined with PKI's ability to manage authentication and encryption efficiently, facilitates seamless scaling for managing diverse energy data sources and connected devices.

Enhanced security

Data gets wrapped in an XPN packet within a secure enclave and it only gets unwrapped and verified when it arrives at the XPN service, where it's then fully governed and managed. XPN's encryption algorithms protect the data and the channel, enabling data protection at rest or in transit, making it more challenging for attackers to decrypt sensitive information. This increased security is crucial in safeguarding data integrity and confidentiality.

XPN is a standalone solution that can be easily integrated into software platforms independently of vendor or technology, and it provides end-to-end, persistent trust for IoT devices and the data they transmit.

Intertrust XPN allows you to conveniently and safely make data resources available for internal and external use, assuring that your explicitly defined usage policies are enforced in various environments. It is an effective way of demonstrating compliance with data usage requirements.

- The XPN device SDK is available on multiple chipsets, and as a C library for easy portability
- The XPN service in the cloud provides a simple interface to access data collected and transmitted from devices

XPN features:

Resistance to quantum computing
As quantum computing advances, traditional encryption methods become vulnerable. XPN paired with blockchain technologies can help withstand quantum attacks, ensuring the long-term security of PKI systems.

Improved key management
XPN can provide more secure key management processes, simplifying the secure issuance, revocation, and rotation of cryptographic keys. This streamlines PKI administration and reduces the risk of unauthorized access.

Interoperability
XPN can enhance PKI interoperability, enabling secure communication with a wider range of devices and systems. Because it sits at the application layer of a communication stack, XPN is inherently more agnostic to protocols and devices. This is particularly important in today's diversely interconnected IT environments.

IT/OT integration
XPN offers modern IoT computation and a layer of data trust to the nexus of IT/OT devices, making them both more resilient and interoperable.

Scalability
XPN is designed with scalability in mind, making it easier to accommodate the growing number of users, devices, and applications that rely on PKI. This is essential for businesses experiencing digital growth and rapid modernization.

Reduced maintenance
XPN requires less frequent updates and maintenance compared to older encryption methods, reducing the workload on PKI administrators and minimizing potential vulnerabilities.

Improved performance
XPN offers great performance and does not introduce latency into data transmissions or impact faster encryption and decryption processes.

Compliance
Many industries and regulatory bodies require specific encryption standards and compliance. Integrating XPN can help organizations meet these requirements and avoid penalties.

Future-proofing
By adopting XPN, organizations can future-proof their PKI infrastructures. This means they are less likely to face costly and time-consuming overhauls as encryption standards evolve.

Improved user experience
Enhanced encryption with XPN can lead to a more seamless and secure user experience. Users can trust that their data is protected, which leads to increased confidence in digital transactions and interactions.

Global accessibility
The flexible governance of XPN allows it to easily adhere to international standards, allowing organizations to operate on a global scale while maintaining security and compliance.

XPN verses VPN

A VPN protects data as it is being transmitted over the internet, by creating an encrypted “tunnel” for the network link.

Once the data leaves the VPN connection, it is no longer protected and is dependent on whatever security features are present in its new environment. XPN’s persistent data protection consistently protects the data regardless of where it resides. And while a VPN requires detailed configuration, XPN packets always know their routing destination.

Going beyond traditional encryption

Encryption turns data into an unreadable blob that can only be read if the reader holds a secret key. This protects the data from an unauthorized party reading it but does little else.

XPN’s persistent data protection and entity attestation tokens add metadata to the data to help establish the provenance and secure state of the device that transmitted the data. It also authenticates that the data has not been altered after it was transmitted by the device.

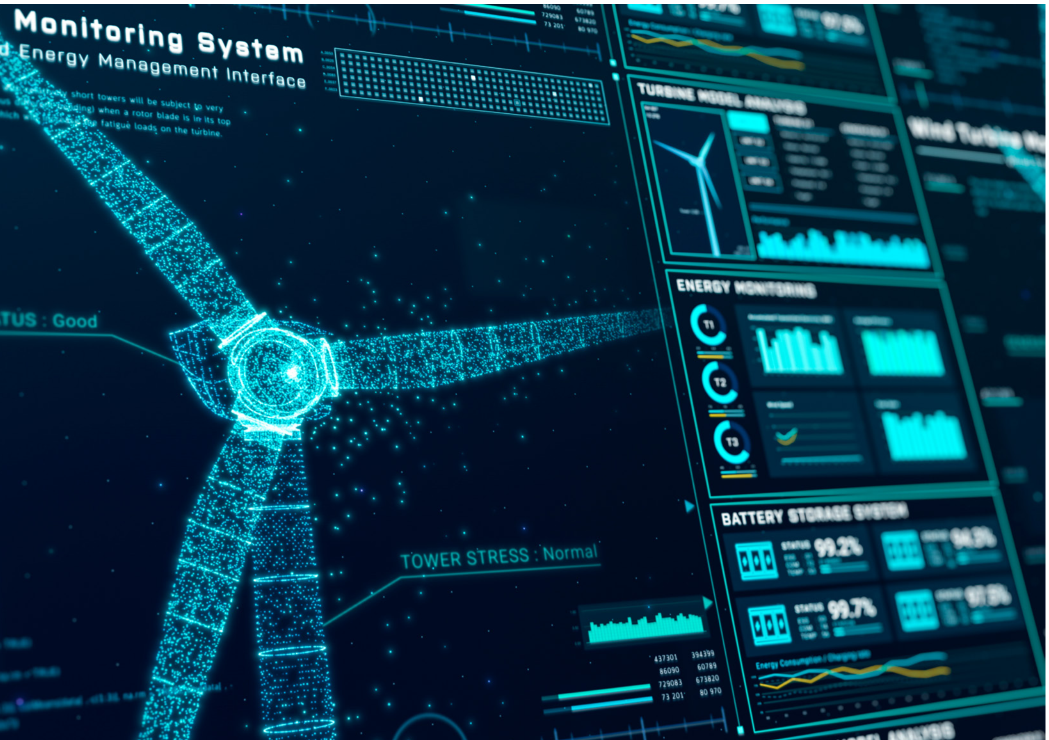
XPN in action: Sample threats it helps to mitigate

A utility transmits unencrypted data from sensors on wind turbines over a secure IPSec tunnel to a gateway device which then encrypts the data and transmits it to the utility’s cloud data repository. However, an attacker has placed malware on the gateway that “poisons” the data. The machine learning algorithms using the wind farm data to monitor its operational health falsely determine that the wind farm is on the verge of a catastrophic breakdown.

The wind farm is then shut down, leading to power instability for the region. XPN would mitigate this threat by allowing the utility’s cloud service to authenticate the data it receives and if it can’t, flagging it as untrustworthy. The data will no longer be used operationally until the issue is resolved.

A building developer uses a cloud application to improve the energy efficiency of one of its buildings. One of the sensor inputs the application uses is temperature data from a legacy SCADA device in the building. Since the SCADA device isn’t equipped with recent hardware security protection and isn’t behind a firewall, an attacker initiates a malformed connection to the device and places malware on the device.

XPN maintains digital twins for legacy devices and the legacy device can only connect to the digital twin. Any other connection to the legacy device must go to the digital twin through a firewall. The attacker’s malformed connection is detected and refused by the firewall.



How XPN can be deployed in energy

Data encryption for communications

Scenario: A wind farm's control systems, turbines, and monitoring devices constantly exchange sensitive data, including operational status, power output, weather conditions, and maintenance information.

- XPN helps secure the communication channels between these devices. This ensures that the data exchanged remains confidential and is protected from unauthorized access during transmission.

Protection of operational data at rest

Scenario: Solar panel arrays accumulate vast amounts of operational data, such as historical performance, maintenance logs, and efficiency data, which are stored in databases or servers.

- XPN's data protection at rest feature envelopes stored data. In the event of physical security breaches or unauthorized access to storage systems, the XPN envelope alerts data consumers of any tampering, safeguarding the integrity and confidentiality of operational information.

Secure remote monitoring

Scenario: Heat pump networks often have remote monitoring systems so operators can assess performance and address issues without being on site.

- XPN secures the remote monitoring infrastructure by encrypting data transmitted between the heat pumps and the remote monitoring center. This ensures that even if the data is intercepted, the monitoring team can be alerted of it.

Prevent unauthorized control access

Scenario: Unauthorized access to control systems can lead to tampering across any IoT network or even operation access or shutdowns.

- XPN's device authentication feature can be applied to control systems, ensuring that only authorized personnel are given access to modify critical settings. This mitigates the risk of malicious interference.

Integrate with energy trading platforms

Scenario: Renewable energy enterprises may participate in energy trading platforms to sell excess energy to the grid or engage in peer-to-peer transactions.

- XPN can enhance the security of transactions and data exchanged with energy trading platforms. This includes encrypting data related to energy trading, ensuring the confidentiality and integrity of financial and operational information.

Conclusion

Instead of patching together multiple tools, XPN gives businesses a single pane of glass into the trust, protection, and health of their IoT devices, the data they transmit, and their data operations.

XPN's edge-to-cloud security also provides businesses an auditable chain of trust for IoT data. This is especially useful for businesses that need to demonstrate the provenance and veracity of their IoT data for business transactions or regulatory requirements.

With XPN, energy organizations and their customers and partners can operate in a "full-trust" environment and a secure data platform for mission critical, data-driven applications.

Learn more: intertrust.com
Contact us: energy@intertrust.com

intertrust®

Building trust for a connected world.