intertrust®

EXECUTIVE BRIEF

Eliminating data hurdles for VPPs

Intertrust XPN enables trusted data communications from the edge to AI

Building trust for a connected world.

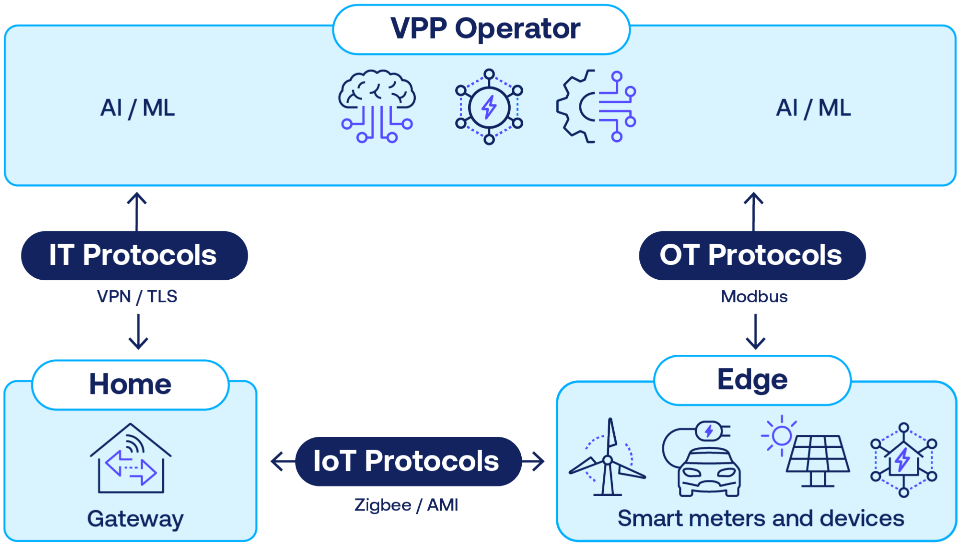
A successful future for VPPs through greater data authenticity

At the vanguard of energy innovation, virtual power plants (VPPs) stand out by optimizing distributed energy resources to support the stability and resiliency of the grid.

VPPs manage a network of distributed energy resources to provide reliable power, often integrating renewable energy. This technological leap promises enhanced energy efficiency but also opens the gates to potential cyber threats that could undermine VPP operational integrity.

As VPP providers interweave automation and artificial intelligence (AI) into their energy framework, the reliance on the authenticity and integrity of data used by AI applications becomes essential to safeguard these advanced energy systems.

VPP operators use AI to optimize a diverse set of devices and systems across IT, OT, and IoT protocols.



Navigating data integrity and AI challenges in VPPs

Virtual power plants are driving the energy sector towards a more distributed and efficient future. However, this advancement brings critical challenges, especially in maintaining the security and reliability of the data they utilize.

VPP operators must navigate a wide range of risks, vulnerabilities, and shortfalls when operating and managing a virtual power plant, including:

Data authenticity and integrity risks

- Unverified data risks undermining AI-driven automation, leading to unreliable operations
- Compromised data inputs can result in AI “hallucinations,” with severe operational impacts

IT protocol vulnerabilities

VPN

- Prone to data leaks and misconfigurations
- Difficult to establish interoperability between vendors

TLS

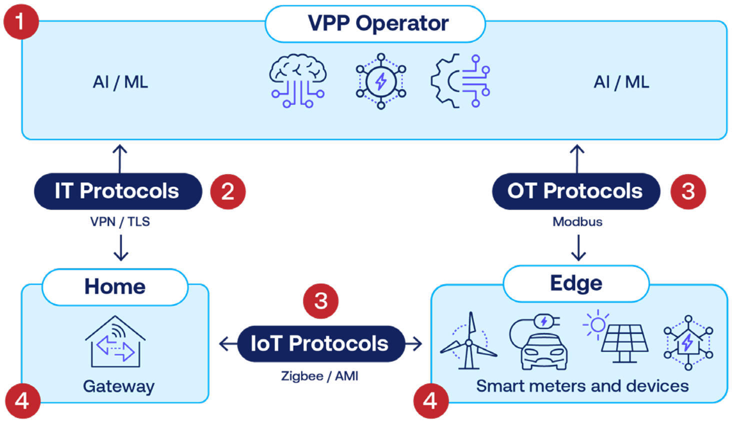
- Designed for high compute end points,not suitable for resource-constrained devices
- Susceptible to replay attacks where an attacker resends valid requests to perform unauthorized actions without detection
- A long list of existing vulnerabilities including POODLE and browser exploit attacks

IoT/OT protocol security shortfalls

- IoT protocols, including Zigbee and AMI and OT protocols such as Modbus are vulnerable to replay attacks and device identifier exposure
- Weak encryption and authentication protocols fail to secure device communications adequately

Protection gaps for data at rest

- Existing IT/OT protocols focus on securing data in transit, and often neglect protecting data stored at rest
- Insufficient end-to-end protection across diverse IT and OT environments, leaving gaps in data security



1. Data authenticity and integrity risks
2. IT protocol vulnerabilities
3. IoT/OT protocol security shortfalls
4. Protection gaps for data at rest

XPN: The security game changer for virtual power plants

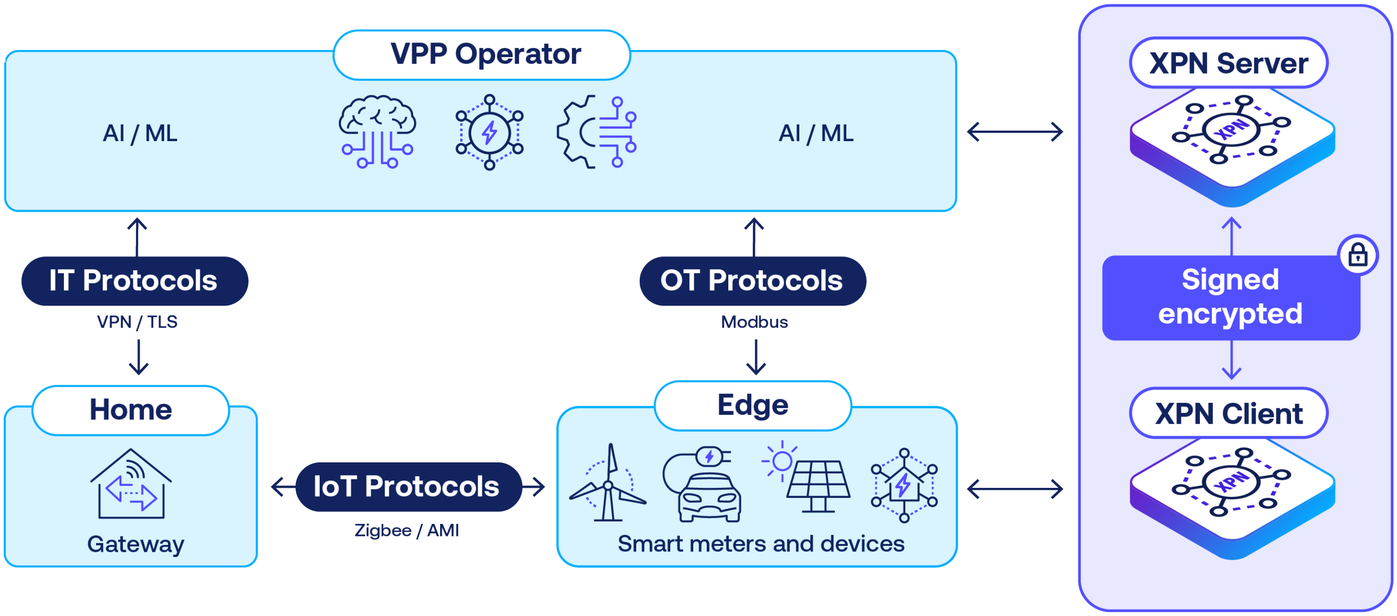
Intertrust XPN offers a comprehensive solution that fortifies devices and data integrity within virtual power plants.

By delivering consistent protection from the edge to the cloud and ensuring authenticated commands, XPN bridges the gap between IT and OT environments. It is easily deployed and integrates with existing infrastructures without a minimal footprint.

Benefits of XPN include:

- **Persistent data protection**
  Seamless edge-to-cloud security protects data in transit and at rest
- **Access control and automation**
  Empowers asset control with authorized commands
- **Unified trust architecture**
  Fosters trust across IT/OT boundaries, strengthening overall network resilience
- **Protocol adaptability**
  Enables secure communication even through protocols not typically associated with robust security
- **Deployment simplicity**
  Designed for swift implementation, XPN's lightweight design and interoperability allow for easy integration with existing setups

XPN solves many challenges VPPs face—from data integrity issues and gaps in protocols to vulnerability risks.



XPN as the keystone in VPP data integrity and authenticity

No doubt the evolution of virtual power plants is a step towards a sustainable and resilient energy ecosystem.

Yet, the integration of advanced technologies brings the challenge of increasing the attack surface. Acknowledging the diversity of vendor equipment and the sophisticated blend of AI and automation underlines the imperative for data authenticity and integrity to avoid operational disruptions.

In the journey of VPPs towards a smarter and more robust energy network, Intertrust XPN plays a pivotal role that addresses the unique security challenges related to IT protocols and OT/IoT protocols vulnerabilities. XPN is based on a zero-trust architecture framework and ensures end-to-end data integrity and authenticity for VPPs.

XPN serves as the foundation for protecting data across the IT, OT, and IoT networks, future-proofing energy management. VPP operators can ensure the economic and operational success of their distributed energy networks, where trust, resilience, and progress are in constant alignment.

What is XPN?

XPN (Explicit Private Networking) is a secure communication service that authenticates devices and protects data across networks.

What does XPN do?

XPN provides interoperability based on open standards, simplifies regulatory compliance, addresses critical infrastructure vulnerabilities, and mitigates risks associated with cyber threats.

What does XPN bring to the table?

XPN enables data protection across value chain with:

- Persistent edge-to-cloud data protection
- Secure control of assets with authorized commands
- Uniform trust model that bridges IT/OT systems
- Zero-trust architecture that tunnels through insecure protocols
- Light footprint and a simple deployment
- Readily slots into existing VPP devices

Learn more at: intertrust.com/xpn
Contact us at: energy@intertrust.com

intertrust®

Building trust for a conected world.