intertrust®

CASE STUDY

Major energy company secures grid data with Intertrust XPN

Every command, signal, and device is now cryptographically verified–without replacing a single system.

SOLUTION
Intertrust XPN

INDUSTRY
Energy / Critical Infrastructure

USE CASE
OT Security and Interoperability

Zero-Trust security for complex, multi-vendor distribution grids

One of Europe's largest energy network operators, is implementing a cryptographic trust overlay across its grid infrastructure. The initiative protects data, devices, and commands without replacing existing systems, addressing rising cybersecurity requirements and multi-vendor complexity.

Key challenges

Traditional perimeter security leaves grid data and commands unprotected. Multi-vendor complexity and rapid DER expansion increase exposure to spoofing and data poisoning.

Key outcomes

Spoofed devices and tampered data are detected in real time. New devices onboard securely with verified authenticity. The company's grid now supports AI-ready operations.

Real-time detection

Spoofed devices and tampered data identified instantly.

Zero disruption

Overlay complements existing VPN and TLS setups.

AI-ready data

Verified streams support next-generation grid management.

"With countless devices across our grid, we needed trust at the data level, not just the network. XPN delivers that."

The challenge

Perimeter security alone cannot protect data-centric grid operations.

The company's distribution grids face threats that traditional channel-based security cannot address. Data left unprotected. Traditional VPN and TLS secure communication channels but cannot protect data itself against tampering or injection.

Device identity unverified. Existing security mechanisms do not cryptographically enforce device identity, leaving grids exposed to spoofed or manipulated devices. Compliance requirements tightening. NIS2 and the Cyber Resilience Act demand stronger, verifiable security across critical grid infrastructure.

The solution

Intertrust XPN adds cryptographic trust at the data layer.

This energy major is deploying Explicit Private Networking (XPN), a cryptographic trust overlay aligned with Trusted Energy Interoperability Alliance (TEIA) principles. XPN sits on top of existing infrastructure, binding digital signatures and authentication directly to data and commands rather than network paths.

Every device must prove its identity before communicating, and data integrity persists across OT, IT, and cloud domains even if network components are compromised. The overlay works alongside existing VPN and TLS setups without replacing them.

The results

A grid that detects threats, onboards devices, and scales securely.

By shifting trust to the data layer, it addresses security, operational complexity, and long-term scalability in a single deployment—without replacing existing infrastructure.

Threats detected in real time
Spoofed devices and tampered telemetry are identified immediately across the organization's grid, eliminating delays that previously obscured manipulation attempts.

Device onboarding simplified
New devices—from solar inverters to power analyzers—integrate with verified authenticity, reducing vendor effort in multi-vendor environments and removing vendor lock-in risk.

AI-ready from day one
Tamper-evident, cryptographically verified data streams satisfy the core requirement for AI-driven grid management, including fault isolation, voltage control, and autonomous operations.

intertrust®

Building trust for a connected world.

Learn more at: intertrust.com/energy

Contact:
+1 408 616-1600 | energy@intertrust

Intertrust Technologies Corporation
2140 Shattuck Avenue, Suite 1201,
Berkeley, CA 94704