Trusted Energy Interoperability Alliance

SOLUTION BRIEF

Compliance-ready energy interoperability

How TEIA helps OEMs and VPP operators build trusted, compliance-ready energy ecosystems.

Contents

Founders

The pressure on distributed energy markets

Distributed energy markets are growing more connected and more regulated at the same time, and the security models built for isolated systems no longer hold.

Regulatory requirements will keep evolving. A single trust model keeps security, interoperability, and reporting all aligned.

Centralized generation is giving way to distributed energy resources: rooftop solar, battery storage, and EV chargers coordinated across many operators and markets. As these assets multiply, so do the rules that govern them. OEMs and VPP operators must now secure interconnected devices, govern AI-driven dispatch, and report incidents across NIS2, GDPR, the EU AI Act, the Cyber Resilience Act, and NERC CIP at the same time.

Three pressures are converging. Assets and market participants grow more interconnected each year. Cybersecurity, AI governance, and reporting obligations keep expanding. And supply-chain exposure rises across software, devices, and service providers. Each framework carries its own technical demands, penalty regime, and reporting timeline, and fragmented vendor-specific stacks cannot satisfy them together.

The stakes are concrete. NIS2 can impose penalties up to €10 million or 2 percent of global turnover, with personal liability for executives, and NERC CIP violations in North America can reach $1 million per day per violation.[1] The risk is not hypothetical: in 2024, 67 percent of energy organizations were hit by ransomware, and 45 percent of breaches in the sector originated in supply-chain weaknesses.[2,3]

Fragmented security stacks leave gaps at exactly the integration points where these risks emerge. Closing them across jurisdictions, protocols, and partners calls for one trust model rather than many.

$10m
NIS2 penalties up to €10M.

$1m
NERC CIP fines reach $1M / violation.

67%
of energy orgs hit by ransomware.

How TEIA reduces digital risk

TEIA takes a different approach: it secures the data itself, not the network path, so trust travels with every transaction.

TEIA is a protocol-agnostic, zero-trust framework for distributed energy markets. Rather than securing the network path, it secures each identity, device, application, and transaction, and records each in a cryptographically protected audit trail. Protection travels with the data across protocols and organizational boundaries.

That continuous verification spans standards such as OCPP, OpenADR, and IEEE 2030.5, so operators gain secure interoperability without opening new trust gaps. The immutable audit trails give verifiable evidence of dispatch decisions and AI-driven actions, which turns regulatory reporting from a manual reconstruction into a query and simplifies audits.

Because TEIA unifies protection across industrial control systems and IT infrastructure, it closes the gap that fragmented stacks leave at converged IT/OT integration points, where threats most often emerge.

Its libraries extend existing systems rather than replacing them, so deployment is faster, compliance costs fall, and prior investments stay productive. Cross-border cryptographic attestation then carries that trust into multi-jurisdiction transactions, dispatch transparency, and renewable-certificate reporting.

Framework	Key requirement	TEIA capability
EU NIS2	Zero-trust, supply chain security, incident reporting	Zero-trust architecture and verifiable audit trails
GDPR	Data protection and privacy	Secure data exchange and encryption by design
EU AI Act	Transparency and accountability for high-risk AI	Immutable decision records and AI auditability
Cyber Resilience Act	Security-by-design from day one of deployment	Security embedded into TEIA specifications
NERC CIP	Critical infrastructure protection, $1M/day penalties	Trusted interoperability across converged IT/OT environments

TEIA secures the message, not just the network path, so protection persists across protocols, organizations, and borders.

Who benefits, and what comes next

Every group in the distributed energy market gains from one shared trust model rather than a patchwork of vendor-specific stacks.

One trust model that works with any standard, any device, any application, without replacing what you already run.

TEIA gives every group in the distributed energy market one trust model instead of many. OEMs and device manufacturers bring products into regulated markets without redesigning security architectures: they extend existing systems, reduce integration complexity across protocols, and avoid vendor lock-in through open standards.

VPP operators and energy service providers build trust across distributed assets, partners, and markets. They onboard diverse DER assets faster, verify dispatch and market transactions cryptographically, and audit AI-driven optimization with confidence. Regulators and standards bodies gain verifiable reporting and consistent trust standards, which speeds the adoption of flexibility services without adding industry burden.

Four core strengths make this possible:

1. Zero-trust verification

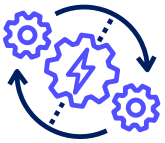
of every identity, device, and transaction, across any network condition.

2. Message-level security

and immutable audit trails that persist across protocols and boundaries.

3. Brownfield integration

that extends existing systems rather than replacing them.



4. A future-ready architecture

with cross-border attestation and framework alignment built in.

Regulatory requirements will keep changing, but fragmented architectures will keep creating risk. TEIA gives distributed energy markets a more secure, scalable foundation that reduces digital risk while enabling innovation and cross-border growth.

Sources

[1] North American Electric Reliability Corporation, Sanction Guidelines. The maximum penalty for a Reliability Standard violation in the United States is $1 million per day, per violation.

[2] Sophos, "The State of Ransomware in Critical Infrastructure 2024." Reports that 67 percent of energy, oil/gas, and utilities organizations were hit by ransomware in 2024.

[3] SecurityScorecard and KPMG, "Third-Party Cyber Risk in the Energy Sector" (October 2024). Finds that 45 percent of breaches in the sector originate in third-party, supply-chain weaknesses.

Trusted Energy Interoperability Alliance

Learn more at: trusted-energy.org
Contact us at: contact@trusted-energy.org
+1 408 616 1600

TEIA membership is available to all organizations active in the digital energy ecosystem. OEMs can join the partner program at no cost.

To learn more about TEIA standards, membership, or to request a technical briefing, visit **www.trusted-energy.org**