Trusted Energy Interoperability Alliance

From **what if?** to **what now?**

When security architecture stalls deals

OEMs

Trusted Energy Interoperability Alliance

From **what if?** to **what now?**

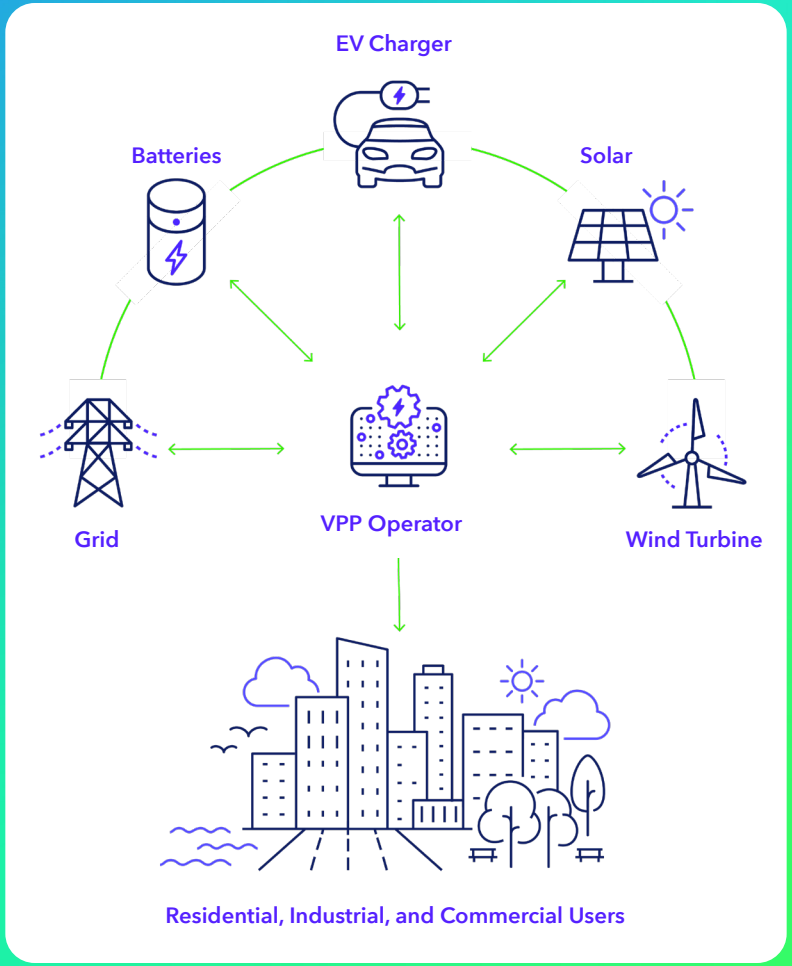
OEM readiness scenario

Picture this

Your grid-connected commercial battery systems are certified, field-tested, and priced right. Then security reviews stall everything:

- Utility A needs alignment with its internal PKI and device identity
- Utility B mandates compatibility with the aggregator's trust framework
- Utility C flags your proprietary stack as a vendor lock-in risk

The devices work. The business doesn't scale.



OEMs

Learn more at: trusted-energy.org

Trusted Energy Interoperability Alliance

Traditional fix

Custom security work that compounds

To keep deals alive, OEMs typically respond with tactical fixes.

CONVENTIONAL PLAYBOOK	ACTUAL RESULT
Customer-specific security adaptations	Fragmented codebases, higher defect risk
Proprietary protocols	Ongoing operational and liability burden
Custom compliance documentation	Repeated audits, inconsistent outcomesInteroperability breakdown
Security treated as differentiation	Increased buyer hesitation, slower sales

Each new utility adds marginal revenue—but also compounds cost and complexity.

Learn more at: trusted-energy.org

OEMs

Trusted Energy Interoperability Alliance

The TEIA way

A security foundation buyers already accept

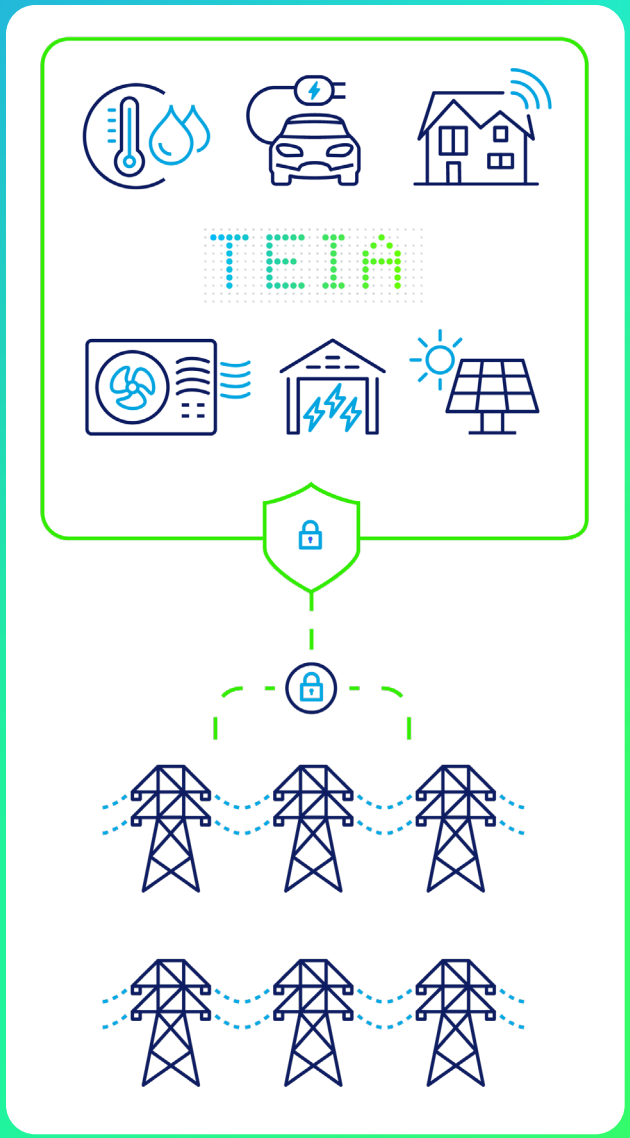
Standards-based trust and identity
Devices ship securely aligned to industry frameworks

Interoperable by default
Devices are onboarded without custom integrations

Procurement-ready
"No lock-in," reduces red flags during security reviews

Lifecycle simplicity
Updates, audits, and future devices follow a shared standard. The blocker wasn't device capability—it was trust at scale.

With TEIA, OEMs stop negotiating security deal by deal and start competing on performance, reliability, and cost.



OEMs

Learn more at: trusted-energy.org