Trusted Energy Interoperability Alliance

EXECUTIVE BRIEF

One trust layer for all

Bring identity and authenticity to your energy protocols

Contents

Founders

Executive summary

VPP operators, OEMs, and utilities need an identity and trust layer that works alongside the protocols they already run. Distributed energy has crossed from pilot to production, and scale exposed a gap those protocols were never built to close.

Protocols made distributed energy possible, including OCPP for charging and OpenADR for demand response, so devices can speak to platforms across vendors. These protocols define how devices communicate.

Yet, they were never designed to prove who is communicating, that a message is authentic, or that what was dispatched is what actually happened. This brief explains that gap, why a protocol standard alone cannot close it, and why a common trust layer pays off for every participant.

AI-driven virtual power plants and distributed battery networks now execute market transactions at machine speed, often without human approval.

The problem: Scale exposed a gap the protocols do not cover

When a single aggregated portfolio spans dozens of manufacturers and feeds a wholesale market, a communication protocol faces questions it was never built to answer.

Distributed capacity has become load-bearing. When fleets carry real grid responsibility, the tolerance for assets you cannot verify and dispatch you cannot prove drops sharply. The blocker is rarely the device or the protocol. It is trust at scale, and most stalled integrations, procurement reviews, and security sign-offs come down to one unanswered question: how do we know we can trust what this fleet tells us and what it does when we dispatch it?

Identity that survives change

A device has to be the device it claims to be, and that identity has to hold through a firmware update, a network change, or a change of owner. A communication protocol assumes the endpoint is genuine. Across a fleet drawn from many vendors, that assumption is the first thing to break, because nothing in the message itself proves the sender is who it says it is.

Authenticity of every message

A command or a meter reading has to come from an authorized source and arrive unaltered. Protocols standardize the payload and the transport, then trust the channel to carry it honestly. That holds inside a controlled deployment. It breaks down when devices talk over cellular, Wi-Fi, and the public internet, and increasingly call home to vendor clouds outside any operator network.

Provability after the fact

When a dispatch crosses platforms, vendors, and jurisdictions, someone has to produce a verifiable record of what was instructed and what was delivered. Protocols say nothing about proof after the event. Today that record gets built the expensive way, through bespoke integrations, per-vendor reviews, and manual audits rebuilt every time a protocol revs or a partner joins. The cost compounds with every device added, running the marginal economics backwards from where a scaling business needs them.

When fleets carry real grid responsibility, the tolerance for assets you cannot verify and dispatch you cannot prove drops sharply.

The solution: A protocol-agnostic trust and identity layer

Protocols and a trust layer solve different problems, and one was never meant to do the other's job. A protocol standardizes the message.

A trust layer establishes who is sending it, whether it is authentic, and what can be proven afterward. TEIA supplies four elements that sit alongside the protocols already deployed, rather than replacing them.

Verifiable identity

Every device carries a cryptographic identity that proves what it is, independent of the message it sends. This is the foundation the protocols assume but do not provide, and it persists across firmware updates, network changes, and ownership transfers.

Message-level authentication

Each command and reading is verified as authentic and unaltered on its own terms, not trusted because it arrived over an expected channel. Authentication travels with the data rather than depending on the network it crossed.

Portability across boundaries

Trust attestation survives protocol translation, so an instruction passing from one standard to another carries its credentials the whole way. The layer holds across protocols, networks, and organizational boundaries, including data that leaves the operator perimeter.

Provable audit trails

The layer produces immutable, independently verifiable records of what was instructed and what happened. Settlement and compliance evidence is generated automatically rather than reconstructed by hand. Your protocol makes devices interoperable; TEIA makes them trustworthy.

A trust layer establishes who is sending the message, whether it is authentic, and what can be proven afterward.

The pressure is rising now

Markets like ERCOT have moved aggregated distributed resources from the margins toward a real role in meeting demand. Meanwhile, U.S. and EU policy is converging on interconnection and interoperability as renewable deployment and grid-modernization investment accelerate.

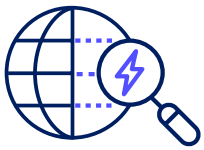
As distributed capacity becomes essential to grid reliability, regulators and operators have far less room for assets they cannot verify.

That pressure lands on exactly the three questions a protocol standard leaves open. Participants who resolve identity, authenticity, and provability now, on top of the protocols they already run, scale into that role. Those who defer keep paying the compounding cost of bespoke trust, one integration and one audit at a time, and risk stalling at the security review just as demand for their capacity rises.

As distributed capacity becomes essential to grid reliability, regulators and operators have far less room for assets they cannot verify.

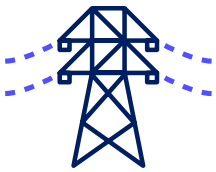
What this means for each side of the ecosystem

The same trust layer pays off differently for everyone, and that's why it works. A device shipped with verifiable identity is one a VPP can onboard and a utility can accept without custom work, so value compounds on a shared foundation.



VPPs, operators and aggregators

Integration cost stops scaling with device count. New vendors and device types onboard against one framework, dispatch runs on data whose provenance is verified before algorithms act, and settlement trails are generated automatically rather than rebuilt by hand.



Utilities and grid operators

A utility leaning on aggregated capacity accepts risk from assets it did not build. The questions that gate a sign-off, authenticating every asset and proving what happened, are answered consistently across a multi-vendor fleet rather than vendor by vendor.

OEMs and device manufacturers

Proprietary security has become a sales liability, because procurement teams screen for lock-in. Shipping to an open trust standard turns that into a selling point: devices clear review faster, onboard without custom work, and engineering returns to product differentiation.

Regulators and market operators

Oversight scales as portfolios grow into the hundreds of thousands of devices, because verification and audit follow one standard. Provable dispatch records support reporting requirements without manual reconstruction for each participant.

The path forward

The industry faces a fork. One path keeps trust fragmented, rebuilt for every vendor and every audit. The other establishes trust once, as a shared layer that works alongside the protocols already in place.

This pattern is familiar. The public-key infrastructure behind web commerce, the chip standards that made payment cards interoperable, and the certificate systems underpinning secure email all succeeded by separating identity and trust from the protocols carrying the data. Energy is reaching the same threshold.

With TEIA, trust becomes a shared foundation rather than a recurring cost. Open specifications and an open partner program are how it gets built—but the larger opportunity happens once trust is set.

Distributed energy scales without renegotiating confidence at every device and every audit. Those who establish that layer now define how the grid's next phase operates instead of just inheriting it.

TEIA separates identity and trust from the protocols carrying the data.

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**