



Trusted Energy
Interoperability Alliance

SOLUTION BRIEF

Scaling a VPP with TEIA

Onboarding and authentication
with less operational overhead.



Contents

The scaling wall	3
How TEIA changes the model	4
Onboarding and operational savings	5
Getting started	6

Founders



intertrust®



The scaling wall

Distributed energy markets reward scale, but the architecture that makes early scaling easy starts working against a VPP somewhere past the first tens of thousands of endpoints.

Distributed energy markets reward scale, but the architecture that makes early scaling easy starts working against a VPP somewhere past the first tens of thousands of endpoints.

Every asset you add expands the capacity you can bid into flexibility markets. Past a certain fleet size, the security model built for isolated systems no longer holds. Traditional VPP security inherits an operational-technology assumption: a physically protected zone where everything inside is trusted by default.

That assumption breaks once assets sit behind consumer broadband, talk directly to vendor clouds, and join and leave the fleet daily. The symptoms show up as cost and latency. Repeated authentication handshakes add delay to time-sensitive dispatch. Cloud and data-transfer bills climb faster than the fleet earns. Each new vendor protocol becomes another integration to build, test, and maintain.

The system built for flexibility becomes its own constraint, and perimeter controls cannot make a heterogeneous, internet-exposed fleet structurally trustworthy. The bottleneck is not the cloud. It is where trust lives in the stack. Closing that gap is what lets a VPP keep growing without re-architecting every time the fleet expands.

The bottleneck is not the cloud. It is the architecture. A trust layer that travels with the data lets a VPP scale securely and affordably without breaking under its own growth.



How TEIA changes the model

TEIA moves trust verification off the network and into the data layer, so identity, authorization, and provenance travel with each message rather than with the network path.

TEIA is an open, vendor-neutral trust layer founded by E.ON, JERA, Origin Energy, GS Energy, GivEnergy, and Intertrust. It does not replace the protocols a VPP already runs, including IEEE 2030.5, OCPP, OpenADR, and Matter. It adds identity, authority, and accountability across them.

The change that matters operationally is the authenticate-once model. In a handshake-per-interaction system, every dispatch signal, telemetry push, and status check re-establishes trust from scratch.

At a hundred thousand assets, that overhead becomes seconds of added dispatch latency and a bandwidth bill that scales with message volume. TEIA replaces the repeated handshake with a persistent, continuously verified trust association. A device authenticates once and joins the fleet, then transacts many times. Each command is still authorized in real time against current policy and device posture, so you get persistent trust without persistent handshaking.

TEIA adds identity, authority, and accountability across common VPP protocols.

Four interlocking trust functions layer over existing orchestration:

Identity	Cryptographic identity for every device, service, and platform, so only authenticated actors join aggregation and dispatch.
Secure messaging	Application-layer trusted communication, independent of the underlying network and resilient to protocol translation.
Protection	Cryptographically secured data in transit and at rest, giving integrity across vendors and clouds.
Key management	Interoperable key provisioning and rotation, built to operate at fleet scale where it usually breaks.



Onboarding and operational savings

Onboarding cost stops scaling with fleet diversity, because one protocol-agnostic trust enrollment per device replaces one custom integration per vendor and protocol.

One protocol-agnostic trust enrollment per device replaces one custom integration per vendor and protocol.

A real fleet mixes EV chargers on OCPP, distributed resources on IEEE 2030.5, demand-response assets on OpenADR, smart-home devices on Matter, and proprietary industrial systems. The conventional response is a custom integration per vendor, so onboarding cost grows with diversity and never amortizes. Because the TEIA trust layer is protocol-agnostic, the same identity and provenance model covers the whole fleet without rip-and-replace. Brownfield is a deployment path, not a weakness: legacy devices enroll at a lower assurance tier, and hardware with a secure enclave reaches the highest.

A VPP team should instrument a pilot cohort and expect reductions across these key areas:



Authentication overhead

Authenticate-once removes repeated handshakes from the dispatch path, cutting latency and the compute spent re-establishing trust.



Cloud and bandwidth cost

Fewer round trips per interaction means data-transfer cost tracks fleet value, not raw message count.



Integration and maintenance labor

Protocol-agnostic trust replaces per-vendor custom integrations, so engineering effort stops scaling with fleet diversity.



Compliance and audit effort

Cryptographic audit trails are generated continuously as a property of the trust model, replacing manual evidence-gathering.



Revocation handling

Fleet-wide signed identity and revocation make removing or quarantining a device a single, fast operation.

Getting started

A TEIA integration does not begin with a platform migration. It begins with two assessments and a narrow pilot.

First, assess architecture readiness for scale: identify where repeated authentication, per-protocol integration, and reconnection gaps already constrain growth, and where they will bind next at twice and 10 times the current fleet. Second, map fleet exposure by protocol, vendor, firmware, and hardware trust capability.

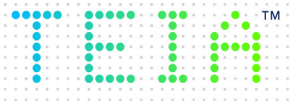
Asset-mapping routinely surfaces concentration risks operators did not know they had; in one cooperative, a single switch failure would have dropped all generation and distribution.

Then pilot continuous verified trust on a high-value cohort, such as vendor maintenance connections or assets in regulated markets, where authenticate-once and protocol-agnostic onboarding deliver immediate, measurable benefit. Prove the metrics, then scale on the evidence.

TEIA is evolutionary and it works alongside the standards you already run and preserves existing investments. The objective is not to rebuild your VPP. It is to remove the architectural ceiling so the VPP you have can keep growing.

TEIA works alongside standards you already run and preserves existing investments.





Trusted Energy
Interoperability Alliance

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

Copyright © 2026 TEIA. All rights reserved.

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

