

Trusted Energy
Interoperability Alliance

EXECUTIVE BRIEF

Open standards compliance is now a market access question

Why interoperability is becoming a
condition of sale for device manufacturers.



Contents

Executive summary	3
Why adoption stalls and requirements move	4
What unreadiness costs when requirements arrive	6
Who gains when compliance becomes a selling point	7

Founders



intertrust®



Executive summary

For a decade, the case for open security standards in distributed energy was framed as a standards argument: lower development cost, faster integration, future-proofing.

Those benefits are real, but rarely move a manufacturer by themselves. A standard may protect product quality, reduce support risk, strengthen trust, and differentiate a device, yet those gains compete with roadmap work and shipping deadlines.

That calculus is changing because open compliance is becoming a customer access issue. Utilities and virtual power plant (VPP) operators are writing open-standard compliance into procurement and program requirements. This brief explains why voluntary adoption stalls, what unreadiness costs, and how manufacturers can prepare before a buyer makes compliance urgent.

A standard may protect product quality, reduce support risk, strengthen trust, and differentiate a device, yet those gains compete with roadmap work and shipping deadlines.



Why adoption stalls and requirements move

Standards in distributed energy do not spread the way better products spread. A superior device can win buyer by buyer on its own strengths.

Once regulators and large utilities commit, their requirements cascade: a utility requirement becomes a VPP requirement, which becomes a manufacturer procurement condition.

A standard cannot, because its value to any one participant depends on others adopting it too. That changes the decision. Adoption follows the chain of influence, not the chain of technical argument. Once regulators and large utilities commit, their requirements cascade: a utility requirement becomes a VPP requirement, which becomes a manufacturer procurement condition.

Device makers sit at the receiving end. A manufacturer may see the value of open compliance but lack the power to move the ecosystem alone. That is why a voluntary standards argument underperforms at the device level while a customer access argument changes priorities.

The business case and the access case

The same standard, presented two ways, lands differently depending on who asks and why. The business case says the standard protects product integrity, lowers integration cost, reduces customer friction, strengthens trust, and differentiates a device. It can earn interest, but still asks the manufacturer to act before the market forces the issue. The access case says a major customer now requires compliant devices. That produces commitment: keep the contract you hold, win the next one, and avoid being screened out.



Customer requirements are already appearing

The cascade is not hypothetical. In one current example, a major VPP operator made open-standard compliance a procurement requirement for a Tier-1 inverter manufacturer it sources from.

The device maker adopted a compliant security model because its customer tied compliance to procurement, not because architecture alone changed its roadmap. In another, a flexibility-market engagement between a large operator and a device manufacturer is forming the same kernel. Different companies and geographies, same mechanism: the buyer set the condition, and the supplier moved.

Why one requirement spreads

Each case is a kernel, a single required relationship, and kernels matter out of proportion to their size because adoption compounds. Once a critical buyer requires a standard, every supplier to that buyer must comply.

Each supplier then carries that capability into other customer relationships. A standard that struggled to spread by persuasion can spread quickly once the first buyer requirements take hold. ‘Why would I do this?’ has a new answer. The buyers you depend on are starting to require it, and the first ones already have. These procurement conversations are no longer hypothetical.

The market is moving toward open compliance

Standards in distributed energy do not spread the way better products spread. A superior device can win buyer by buyer on its own strengths.

The distributed energy resources market is projected to grow from \$86.95 billion in 2024 to \$293.59 billion by 2034 (Precedence Research, 2025), and its highest-growth segments—virtual power plants, demand response, and grid services—are precisely the multi-vendor environments that cannot function without interoperability. For buyers running those programs, open compliance is becoming table stakes.

That is what makes the requirement durable. A VPP operator requires compliance because multi-vendor coordination is the business, and a non-compliant device imposes integration and trust costs the operator refuses to absorb. As these segments grow, the addressable market that screens for compliance grows with them. A proprietary model risks forfeiting a rising fraction of where the market is heading.



What unreadiness costs when requirements arrive

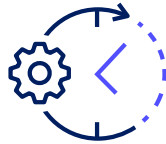
For years, non-adoption was framed as a missed efficiency. The real cost is when a requirement arrives and the manufacturer isn't ready.

The market-access case reframes it as a deal you were positioned to win, lost on an attribute unrelated to your hardware. Once a buyer requires open compliance, a proprietary security model becomes a disqualifier applied before the product is judged. The costs concentrate when a requirement arrives and the manufacturer is not ready.



Compressed response time

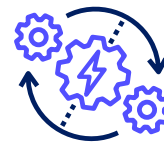
A customer requirement carries a deadline. A manufacturer that begins re-architecting security only after compliance is required is racing a clock it did not set, at a premium driven by urgency.



Once a buyer requires open compliance, a proprietary security model becomes a disqualifier applied before the product is judged.

Lost procurement cycles

A buyer standardized on open compliance can exclude a non-compliant device at the screening stage, before the hardware is evaluated on product performance. The deal is lost on an attribute, not on the product itself.



Diverted engineering

Meeting each requirement with a bespoke build pulls engineers toward security work outside the core competency. A common open baseline ends that diversion and returns effort to power efficiency, reliability, and cost.

Per-market recertification

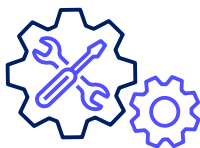
Each market entered under a proprietary model repeats certification cost and lead time. An open baseline can be certified once and recognized across markets, reducing repeated work at every border.

Who gains when compliance becomes a selling point

Reframed around market access, open compliance stops being a defensive expense and becomes a commercial asset.

The market-access case shows the cost is becoming the price of staying in the room, and that early readiness can turn a potential disqualifier into a differentiator.

The same capability that keeps a manufacturer eligible for required procurement also differentiates it among buyers moving that way.



Device manufacturers

redirect engineering away from proprietary security toward what differentiates the product: power efficiency, reliability, cost, and customer experience. Compliance converts security from a feature customers must be persuaded to value into one they require and reward..



Utilities and VPP operators

gain devices that are interoperable and trustworthy by default, clear review faster, and onboard into multi-vendor deployments without custom integration.



Early movers

gain more than eligibility. By engaging while the standard still takes shape, a manufacturer helps shape specifications that suit its architecture and builds ecosystem relationships before the market consolidates.



Buyers screening for lock-in

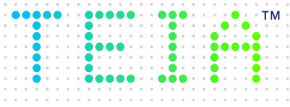
gain a clear basis to prefer one device over another. A compliant product incorporates evolving cryptographic and regulatory requirements by update rather than re-architecture, protecting the investment.



Achieving readiness

The addressable market is bifurcating into buyers who require open compliance and buyers who do not yet, and the first group is the one growing. Readiness is how a manufacturer stays eligible for the expanding half.

The reframe: the old standards case asked a manufacturer to absorb cost for a future benefit. The market-access case shows the cost is becoming the price of staying in the room, and that early readiness can turn a potential disqualifier into a differentiator.



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**](https://www.trusted-energy.org)

