Trusted Energy Interoperability Alliance™

Is your trust model protecting the device layer—or just the network?

Secure every endpoint with trusted, interoperable communications.

The challenge

Energy operators rely on perimeter security to protect network boundaries but leave devices like smart meters and EV chargers exposed and unverified.

The solution

TEIA secures the data, not the network, through cryptographic identity, message-level authentication, data protection, and interoperable key management.

4 key steps to device-layer trust

1. Authenticate every device cryptographically

Assign verifiable identities to each endpoint so only authenticated devices participate in grid operations and market signals.

2. Enforce trusted device messaging

Use application-layer protocols that verify commands at the device, independent of network path or vendor.

3. Protect device data end-to-end

Apply cryptographic integrity to data in transit and at rest—across clouds, vendors, and legacy infrastructure.

4. Manage keys at device scale

Deploy interoperable key provisioning that supports PKI, blockchain, and quantum-safe methods across thousands of endpoints.

Learn how TEIA secures every device in the energy ecosystem.

Read the brief