intertrust®

Securing Energy IoT devices using next-generation PKI

Product Brief

Platform

Introduction

IoT-enabled products are helping electrical energy and utility companies achieve new levels of efficiency and sustainability. Smart meters, automation control systems, home IoT sensors, electric grid automation and protection devices, and power monitoring and control equipment—these connected devices provide deep visibility and control to organizations remotely. They can monitor and tune asset performance, investigate incidents remotely, identify performance issues, plan for predictive maintenance strategies, and improve overall operating efficiency. Yet these same technologies expose utilities and their infrastructure to enormous risk.

Electrical Energy IoT security challenges

IoT devices can serve as entry points for attacks that steal sensitive data, transmit false information, take control of a device's functionality, and even compromise development and manufacturing systems. Attacks on IoT devices increased by 300% last year[1] and 57% of IoT devices are vulnerable to severe attacks.[2]

At the same time, the energy industry is increasingly targeted by hackers. A recent study by Siemens and the Ponemon Institute found that 56% of the global utilities they surveyed suffered at least one cyberattack in the past 12 months leading to the loss of private data or an outage.[3]

Given this landscape, how can energy and utility companies balance the need to scale up their IoT operations while strengthening their security posture? How can they prevent unauthorized command and control, protect customer data, and comply with emerging regulations for both new deployments and brownfield devices already in the field?

Key benefits

Extend device lifetime

- Securely update software and firmware
- Reconfigure identities, embed custom attributes, and control access and actions
- Capitalize on new capabilities and meet the changing regulations of the energy sector

Meet increasing demand cost effectively

- Provision upwards of 10 million device identities per day
- Save 50-85% over the cost of provisioning device identities in-house

Establish trust in devices and their data

- Strongest cryptographic key protection
- Ensures that connected devices, and the data they gather and transmit, are legitimate and secure
- Securely communicate with other devices and services

Comply with regulations

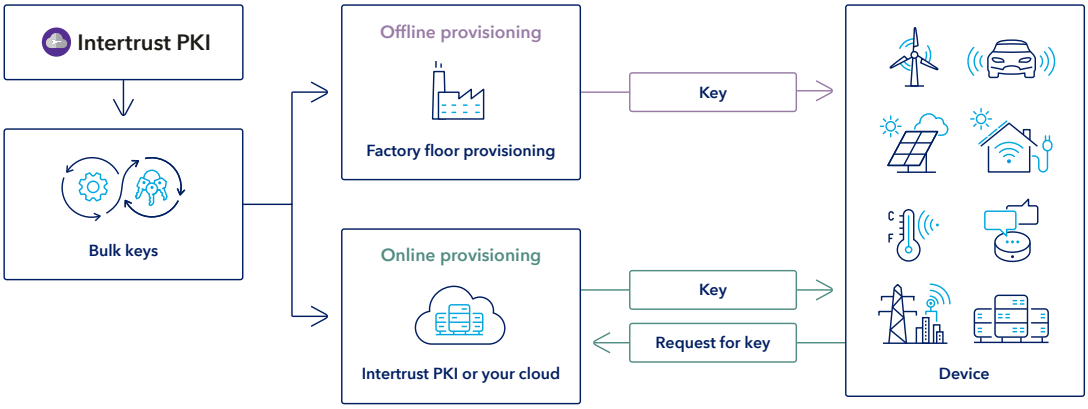
- Ensures that secure identity protocols are compliant with current industry requirements
- WebTrust compliant and ISO 9001:2015 certified
- Supports compliance with NIST's IoT device cybersecurity guidelines (NISTIR 8259A)

Best practices dictate a defense-in-depth approach to IoT security, however the core must be built into connected devices themselves.

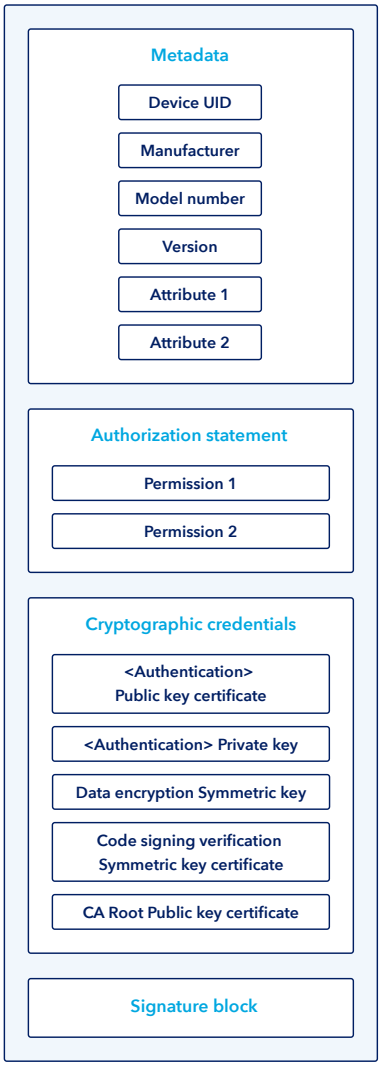
Building a trusted Energy IoT data ecosystem

As IoT technologies rapidly became a business imperative, development generally focused on features and functionality—with cybersecurity as an afterthought. This has left many organizations grappling with a minimally protected, continuously expanding attack surface. There are more than a billion distributed devices, smart meters, grid applications, sensors, and power plants across the energy value chain.[4] It's essential that utilities secure this network of distributed devices, and make sure that the data they generate can be securely and confidently shared both internally and with third-party partners.

Best practices dictate a defense-in-depth approach to IoT security, employing controls such as network segmentation and threat monitoring and response. The core of IoT security strategy, however, must be built into connected devices themselves. Utilities must be able to guarantee the validity of each device, its operational security, and the integrity of its data. Otherwise, their entire grid infrastructure can be compromised.



Provision devices with identities when manufactured or when they boot.



A typical IoT device identity.

Next-generation PKI for Energy IoT with Intertrust

The foundation of a trusted IoT ecosystem begins with embedding secure identities into each device. Public key infrastructure (PKI) is a framework for delivering and managing cryptographically secure device identities to meet critical IoT security needs around authentication, encryption, and code signing.

Intertrust PKI is a certificate authority and managed PKI service specifically built for IoT. PKI for IoT operates at a completely different level of scale and complexity from standard enterprise PKI setups. It must be able to handle provisioning of very large numbers of devices—in the order of millions per day. It also requires a more nuanced data structure that contains various types of metadata, authorization statements, multiple cryptographic credentials, and mechanisms to securely manage and update the device's identity throughout its lifecycle.

Rigorous security

Operating a secure PKI requires specialized facilities, secure hardware and other technologies, and exacting processes. Intertrust maintains secure facilities and HSMs, employing multi-custody protocols, and backed up across multiple physical locations to ensure business continuity. Intertrust PKI is WebTrust compliant and ISO:9001-2015 certified.

Scalable, cost-effective provisioning

Intertrust PKI can deliver device identities directly to the factory floor or in the field through Intertrust's scalable cloud provisioning service at a fraction of the cost of provisioning device identities in-house.

Intertrust Platform™

As a complement to its PKI system, Intertrust offers the Intertrust Platform, an edge-to-cloud data interoperability layer that uses secure data virtualization and identity and access management to enable governed data collaboration in secure workflow environments. It facilitates secure and efficient data collaboration amongst multiple parties, internal or external. It works across data silos and clouds and ensures compliance with security regulations and privacy protections.

Identity and Access Management

Device and user identity, authentication, and authorization; maintains platform objects and their relationships.

Secure Execution Environments

Secure network-isolatable environments for workload execution and controlled, interactive data exploration.

Data Virtualization

Data object definitions, permissions, restrictions. Provides data interfaces, manages DBs and virtualized datasets.

Time Series Database

Scalable, efficient, high performance database designed for time series data.

Partner with Energy IoT and security experts

Intertrust brings deep expertise in PKI, IoT security, and IoT provisioning along with knowledge of the energy sector supply chain and manufacturing environment. Intertrust offers energy and utility companies a cost-effective PKI system that can deliver complex device identities at current and future demand-levels.

Organizations can focus on their core business, secure in the knowledge that sensors, regulators, and other IoT devices can safely authenticate, communicate, and interact within evolving smart grid infrastructures.

Sources

1 Attack Landscape H1 2019, F-Secure, September 2019

2 2020 Unit 42 IoT Threat Report, Palo Alto Networks, Unit 42, March 2020

3 Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?, Siemens Gas and Power, October 2019

4 Scenarios for the IoT Marketplace, 2019, Gartner, August, 2019

intertrust®

Building trust for the connected world.

Learn more at: intertrust.com/platform
Contact us at: +1 408 616 1600 | dataplatform@intertrust.com

Intertrust Technologies Corporation
400 N McCarthy Blvd, Suite 220, Milpitas, CA 95035