intertrust

Case Study

Intertrust PKI

How energy and utility companies can create a secure IoT device ecosystem

Industry
Smart home IoT

Location
Germany, with worldwide scope

Solution
Intertrust PKI

Introduction

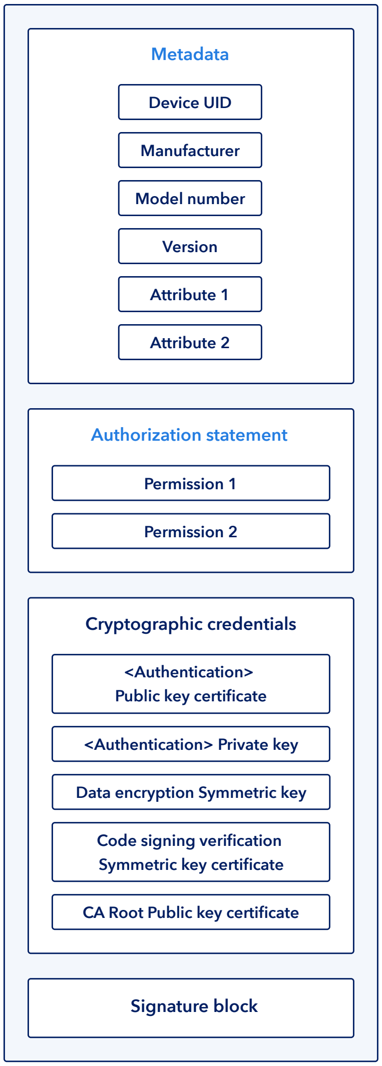
It is no exaggeration to say that the Internet of Things (IoT) has transformed the energy industry. IoT-enabled products such as smart meters, automation control systems, home IoT sensors, power monitoring and control equipment, and electric grid automation and protection relays help energy and utility companies drive efficiency and sustainability. These technologies maximize visibility and control over daily operations, allowing businesses to monitor asset performance, investigate accidents remotely, identify performance issues, plan for predictive maintenance strategies, and greatly improve operating efficiency.

With energy and utility infrastructure spread across multiple generation assets, thousands of miles, and billions of devices (and growing fast), it is easily one of the most complex technology ecosystems to manage and run.

The challenge

Across the energy value chain, from generation to transmission, distribution, and consumption, there are more than a billion distributed devices, smart meters, grid applications, sensors, and power plants communicating with servers and each other. All these devices receive instructions and updates while transmitting data and executing functions in real-time.

Keeping this network of distributed devices secure, and making sure that the data generated can be securely and confidently shared with internal or external partners, is critical. Without the means to guarantee the validity of each device, its operational security, and the integrity of its data, the entire grid infrastructure can be compromised.


Metadata
Device UID
Manufacturer
Model number
Version
Attribute 1
Attribute 2
Authorization statement
Permission 1
Permission 2
Cryptographic credentials
<Authentication> Public key certificate
<Authentication> Private key
Data encryption Symmetric key
Code signing verification Symmetric key certificate
CA Root Public key certificate
Signature block

A typical IoT device identity

The need for next-generation PKI

A secure, reliable IoT device provisioning and authentication system relies on a well-developed public key infrastructure (PKI) framework. Many energy companies and device vendors for this industry initially chose to build their PKI infrastructure in-house.

This may have served their purposes in the early years of IoT. However, as devices grow in scope and complexity, assuming business-critical roles, in-house PKIs are usually not equipped to meet security requisites. Without a steep ramping up in secure infrastructure and dedicated personnel with IoT PKI expertise, organizations may find themselves exposed to significant increases in risk.

Some of the specific challenges facing energy and utility companies include:

- Growing operations at scale
- Regulatory compliance issues
- Preventing unauthorized command and control
- Issues with brownfield devices already in the field
- The growing need to protect customers' sensitive data

Moreover, the energy industry has become an increasing target for hackers. In 2019, a cyberattack on an unnamed U.S. utility company disrupted power grids in Utah, Wyoming, and California. A recent survey of global utilities by Siemens and the Ponemon Institute found that 56% of respondents report their organization experienced at least one attack in the past 12 months that resulted in the loss of private data or an outage. 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.

The solution

While PKI has been around for decades, making sure it works for the scale of IoT brings a completely different challenge. In addition to the ability to handle provisioning of very large numbers of devices, it requires a more complex data structure that includes various types of metadata, authorization statements, and multiple cryptographic credentials, including mechanisms to manage updates to the device's identity throughout its lifecycle.

Operating a secure PKI requires specialized facilities, technology, and processes. Rather than continuing to run their self-built PKI, organizations are turning to Intertrust. Intertrust offers a deep understanding of the energy sector supply chain and manufacturing environment, together with extensive expertise in PKI, IoT devices, and IoT provisioning.

Intertrust's certificate authority and managed PKI service, enables organizations to establish a scalable system to embed cryptographically secure identities into their IoT devices. Keys can be provisioned both on the factory floor as well as remotely through our cloud provisioning service.

Intertrust PKI ensures that connected devices, and the information they gather and transmit, are legitimate, secure, and trustworthy.

The results

With Intertrust PKI, energy and utility companies gain a sustainable and cost-effective PKI system that can handle complex device identities at current and projected demand-levels. They can focus their full attention on core business competencies, secure in the knowledge that sensors, regulators, and other IoT devices can safely authenticate, communicate, and interact within evolving smart grid infrastructures.

Extend device lifetime

Intertrust PKI helps ensure IoT devices stay relevant and safe throughout their lifecycle. Organizations can securely update firmware, reconfigure identities, embed custom attributes, and control access and actions in order to capitalize on new capabilities and meet the changing regulations and demands of the energy sector.

Intertrust also lets businesses bring already deployed legacy IoT devices, that lack these capabilities, into the ecosystem.

Meet increasing demand cost effectively

With Intertrust's scalable PKI services, organizations can provide upwards of 10 million device identities per day at a savings of 50-85% of the cost associated with provisioning device identities in house.

Establish trust in device data

Smart grid effectiveness rests on the integrity of the data it uses. Intertrust PKI ensures that connected devices, and the information they gather and transmit, are legitimate, secure, and trustworthy.

Comply with regulations

Intertrust PKI is Webtrust compliant and ISO 9001:2015 certified, ensuring that secure identity protocols are compliant with current industry requirements. As regulations regarding energy IoT devices continue to evolve, Intertrust provides critical compliance support capabilities.

intertrust®

**Building trust for
the connected world.**

Learn more at: intertrust.com/pki-for-iot
Contact us at: +1 408 616 1600 | iPKI@intertrust.com

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