Enabling Secure Access to IoT Data

ioTrust™ is an end-to-end security solution based on enterprise-grade encryption technologies. It unlocks business value by securing your connected ecosystem.

- Scalable identity management
- Authentication for IoT infrastructure
- Dedicated private trust chains
SOLUTION HIGHLIGHTS

An experienced security partner

ioTrust leverages decades of expertise in cryptography, embedded systems, and trusted infrastructures to ensure the right security level for every device, application, system, and user.

It accelerates IoT deployments and time-to-value by enabling a secure and trusted network of people, applications, and things for sectors such as:

- Industrial manufacturing
- Energy/utilities
- Automotive
- Healthcare

KEY FEATURES & BENEFITS

Security

- Scalable device trust and identity management
- Maintain crypto agility for your deployed endpoints with fully managed crypto
- Authentication and authorization for IoT infrastructure
- Prevent unauthorized command and control
- Ensure data integrity
- Dedicated private trust chains
- Bring your own trusted CA chain

Control

- Manage identity lifecycle from one central console
- Deploy certificates throughout your distributed system
- Embedded OCSP service for easy validation of certificates

Adoption

- Reduce time-to-market
- Ensure supply-chain integrity
- Technology-agnostic deployment
- Solutions for highly constrained devices and networks
- Fast deployment with low complexity
- Private issuing CA chain per organization
- Security starts at time of manufacturing
- Complete control on devices that can go operational
- Lightweight endpoint agent providing crypto capabilities and dynamic discovery organization

IoTrust security solution offerings

Endpoint Agent - Enables secure management of device certificates, secure key generation, device monitoring, and automated service discovery/provisioning

Edge Gateway - Provides auto configuration service and secure proxy for Endpoint Agent

Device management - Allows administrator to manage the lifecycle of the device from activation to suspension or termination

Whitelisting and rules - Allows administrators to list the devices that are allowed to enroll at a specific gateway

Third-party trust chains - Administrators can trust OEM IDs issued by a third-party CA by uploading the third-party CA certificate as a Vendor Certificate

Managed HSMs (high assurance offering) - Provides protection for your data and systems in the cloud, while giving you complete control over your keys
ioTrust™ Security Solution

HOW IT WORKS
The IoTrust Security Solution Illustrated

ioTrust is a tiered solution that enables enterprises to build in security, identity, and encryption solutions that seamlessly interoperate with their traditional security and IT systems.

**Identity Management**
- Secure agents for identity management across devices, systems, and applications
- Operator focused, providing managed crypto libraries and automated provisioning to cloud service providers
- Scalable provisioning of managed identities, enabling authentication and authorization policy management

**Identity Issuance**
- Secured device and user provisioning
- Device and service provisioning component providers
- PKI: root-of-trust delivered via IoT-centric infrastructure design
ioTrust™ Security Solution

SYSTEM PREREQUISITES

<table>
<thead>
<tr>
<th>Component</th>
<th>System Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Agent (EPA) (C language)</td>
<td>400-500kb RAM, 200-300kb flash/storage; Intel X86/64 or 32/64 bit ARM Cortex processor with CENTOS or LINUX OS</td>
</tr>
<tr>
<td>Edge Gateway (EGW) (Java)</td>
<td>512 MB RAM, 4 GB flash/secondary storage, Intel X86/64 or 32/64 bit ARM Cortex processor with CENTOS or LINUX OS</td>
</tr>
<tr>
<td>Approved development boards</td>
<td>Broadcom Raspberry PI 3, TI Beagle Bone Black, VMware Virtual Machine, Docker Container (Debian 8.x)</td>
</tr>
</tbody>
</table>

Technical Features

**Endpoint Protection**
- Hardware-agnostic endpoint agent
- RSA and ECC key management
- Hardware security enabled from endpoint to cloud: TPMs and HSMs
- Supports dynamic discovery and configuration of endpoint
- On-board/Off-board key generation workflows

**Secure Workflow Transactions**
- Securing data at rest: PKI encryption
- Securing data in motion: TLS, DTLS, SSL
- Secure communication: HTTPS, MQTTS
- Certificate lifecycle management
- Validation: CRL and OCSP

**Security Configuration and Management**
- Enrollment mechanism: SCEP, EST, and REST
- API interface to provisioning platform
- Securing root in a FIPS level 3 HSM
- Dynamic whitelisting rules for granular and automated enrollment control

Learn more at entrust.com

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com