Connected Products
ioTrust Security Solution

Ranjeet Khanna
Director, IoT & Embedded Security
Entrust Datacard
Digital Economy and Trust Foundation
Digital business is the creation of new business designs by blurring the digital and physical worlds. ... Digital business promises to usher in an unprecedented convergence of people, business, and things that disrupts existing business models

Objectives

• Optimize current business model

• Transformative growth

The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment - Gartner
IoT Unlocks The Growth Opportunities

26B+
Connected Devices by 2020

10x
Actionable Data by 2020

New Business Models
Diversification of Revenue Streams
Global Visibility
Efficient, Intelligent Operations
Real-time information on mission-critical systems

CONVERGENCE OF PHYSICAL AND DIGITAL ASSETS
Digital Enterprise and Connected Ecosystem

CONNECTED SYSTEMS

CONNECTED USERS

CONNECTED THINGS
IoT Platform: IIC Reference Architecture

Platforms (can be multiple) can be bought or built
Key Considerations: Device Lifecycle in IoT

### Device Manufacturers – Endpoints (OEM)

- Control Module (MCU / ECU)
- Controllable Sensing things

- System Capability
  - Low
  - High
- Bit Processors – 8/16/32/64
- Memory – RAM/SRAM
- Operating System – Linux / windows

### Operators of OEM

- Oil & Gas
- Power Generation
- Natural gas / Pipeline
- Industrial Manufacturing
- Auto Manufacturers
- Telecom
- Remote monitoring
- Enterprise / OEM Cloud infrastructure
- Connected Solutions (Apps)
- Gateway (MQTT, AMQP, REST)

### Security

#### Identity Set up
- Establishing Root-of-Trust
- Addition of Device attributes & bootstrap certificate / token

#### Secure Identity
- HSM, TPM, E-Sim, SE, TEE
- Key Management
- Ownership transfer

#### Identity Provisioning
- Discovery
- Device Authentication
- Provisioning & Authorization

#### Lifecycle Mgmt.
- Secure Data & Identity
- Identity & Security Updates
- Activate / Suspend / Terminate
- Device Update – Firmware, Cert
Device Manufacture's Opportunity and Responsibility
Chip and component manufacturers are in a unique position to enable end-to-end IoT security by securely producing product with root of trust.
Manufacturing Challenges

- Geographic separation and contract manufacturing
- Verification of software authenticity
- Secure updates post manufacture
- Secure enrollment services post manufacture
- Secure storage and generation of private keys
Leading Use-Cases

TOP USE CASES

Device Manufacturing
- Unique Device Identity
- Geo Separation & Contract Mfg.
- Firmware Signing
- Key Management

Device Operations
- Device Provisioning
- Identity Lifecycle Management
- Secure Communications
- Over the Air Updates
- Ownership Transfer
- Endpoint Monitoring
Use-Case: Supply Chain Integrity and Operations

1 – Establish Initial Identifier

2 – Create Managed Identity and Device Role

3 – Device Enrollment and Registration

4 – Establish User and Device Identity Relationship

5 – Secured Service Delivery
ioTrust Security Solution
Connected Things

Ensure the safety of your business, your customers and our connected world with trusted protection for your devices and apps across every interaction—from sensor to cloud. Defend against hacks, failures, botnets and the threats of tomorrow.

BUSINESS GOALS

• New Revenue Streams from Connected Products
  Provide customers and internal stakeholders with new offerings built on connected products and real-time data

• Optimize Operations
  Enhanced visibility over operations and system automation

OUR SOLUTIONS

• Supply-Chain Integrity: Make devices easily identifiable and ready to be secured from the earliest stages of manufacturing

• Trusted Infrastructure: Rapidly deployable and scalable security for your operational infrastructure, from endpoint to enterprise data hub, with an added view to the users

• Data Acquisition Management: Granular control of your data as it transits the network
Trust Enablers

IDENTITY

AUTHENTICATION & AUTHORIZATION

CREDENTIAL LIFECYCLE / KEY MANAGEMENT

EQUIPMENT DATA MODEL MANAGEMENT

DATA SECURITY

SUPPLY CHAIN INTEGRITY

DELIVERING VALUABLE, ACTIONABLE DATA
ioTrust Security Solution

- Cloud ready, Application and Data platform agnostic
- Integrated Device and Data Security
- Identity Management: Manufacturing to Operations
- Authentication and Authorization for every class of device
- Data Acquisition Management
- Supply Chain Integrity
- Secure Auto Enrollment and Provisioning

ioTrust Value: delivering secured infrastructure between “things” and applications

Enabling different classes of “things” existing or greenfield

- STREAMLINED DEPLOYMENT FOR BUSINESS OUTCOMES
- STRONG SECURITY ALIGNED WITH OPERATIONS REQUIREMENTS
- SCALABLE AND ALIGNED TO EVOLVING ECOSYSTEM
A Tiered Offering to Fit a Variety of Needs

**Manufacturing**

**Identity Issuance**
- Secured Devices Manufacturing
- Device manufacturer & Tier-1 component providers
- PKI: Root-of-Trust delivered via IoT centric infrastructure design

**Identity Management**
- Secure channel for acquiring data from devices and submitting to enterprise data hubs
- Device operator focused on operational state of security deployment
- Scalable provisioning of managed identities enabling authentication and authorization policy management

**Identity and Data Security**
- Granular control over access to data and command execution
- Device operators with analytics-driven business use case
- Integrated secured data acquisition and ingestion with policy-driven equipment data management

**Operations**

**Offering**

**Primary Focus**

**Market Segment**

**Tech Foundation**
IIC Reference Architecture: ioTrust Offering

Platforms (can be multiple) can be bought or built
Manufacturing Identity Issuance

Production Line

MES/Provisioning service

IoT Device

- HW Properties
- TPM or SE
- Secure Storage
- Key & Certificate Store
- Applications

Bulk CSR and REST enrollment Service

Manufacturing Proxy

IoTrust

IoT ROT

Management Console

Service Gateway
(On Premise or In Cloud)

Service Gateway
(On Premise or In Cloud)

Customer ROT

Device Meta Data

Customer Platform

Geo 1

Geo n

Private Key

Public Key & Device ID

Device-unique Certificate

Applications

Manufacturing Identity Issuance
Operational Identity Management

Netco Trust Root

Management Console

IoTrust Cloud

Client Cloud

Secured Application(s)

Sensor/Module

Edge Gateway (Physical on premise or In Cloud)

Service Gateway (On Premise or In Cloud)

Service Discovery Transport Security
TPM/Keystore Management Application
Authentication Edge Sensor Authentication
Code Signing*

Identity Lifecycle Management
Security Policy Management
Device Monitoring

Secure Data Routing
Security Policy
Identity LCM
Hardware Telemetry

Customer ROT + CAs

External Agent
Securing the Endpoint

The ioTrust™ Endpoint Agent is a small, lightweight Software binary that can be used to anchor customer security. The pre-built package reduces development effort to achieve secure and feature rich identity Management.

- Identity lifecycle management – enrollment, renew, suspend and terminate in real-time
- Secure Software Keystore with on board key generation capabilities
- Crypto libraries supporting ECC & RSA including TLS 1.2 stack
- Auto enrollment and service discovery leveraging multicast COAP & Signed SCEP services
- Device monitoring via mutually authenticated MQTT telemetry data pipe
Building secure applications requires a chain of trust established from manufacture to operational use case. Tools and infrastructure federating trust must seamlessly facilitate secure identity validation and management across organizations.

- Securely establish & manage device keys in a central PKI and Hardware Security stores
- Autonomous mutual authentication for applications and things
- Manage trust between organizations via secure IoT Root Of Trust provided by ioTrust™
- Restrict trust relationships operationally via secure infrastructure throughout the solution stack
- Migrate and on board legacy systems through CA and device cert Import/Export at Service Gateways
- Create devices and components that are both usable & secure regardless of device class
Creating Trust for Industries

SMART MANUFACTURING

We’ve partnered with one of the largest silicon manufacturers and M2M providers in order to enable distributed manufacturers to uniquely issue trusted identities onto devices.

SECURELY MANAGE INDUSTRIAL NETWORKS

We enable a global leader in industrial automation and energy management solutions to ensure even the most complex, high risk, and distributed IoT systems can operate securely.

VEHICLE-TO-VEHICLE AND VEHICLE-TO-INFRASTRUCTURE

We developed a solution for two of the biggest names in the automotive sector to enable them to embed trusted identities onto vehicular components at all levels of the supply chain.

SMART GRID AND SMART ENERGY

We’re working with energy and utility companies from Canada to the Middle East, enhancing the safety and privacy of smart ‘things’ wishing to connect to the utility network – and authenticating and authorizing data channels that support data collection/analysis and remote device control.

SECURED DATA MANAGEMENT AND ANALYTICS

We’re enabling our Telco/SI/ESP partners to realize value-added service delivery models for their customers, by enabling the secure collection and transfer of dynamic analytic insight from millions of devices.