Blue Planet-works

Safety for the Connected World

TRUSTICA

Safety for the Connected World

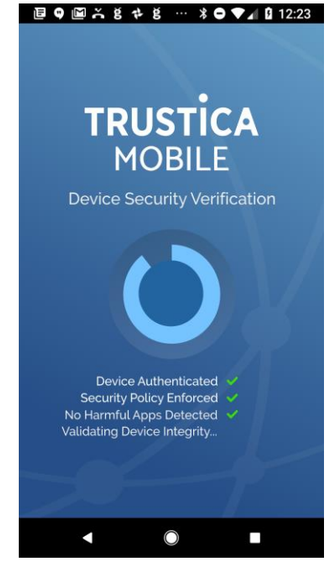
Aiming to be the Global Leader in Cyber Security,
starting from Japan

AppGuard and TRUSTICA

Endpoints
Servers

APPGUARD

Cloud
Native
Computing



TRUST and Privacy Framework: Attestation, EPID, Small Crypto Footprint

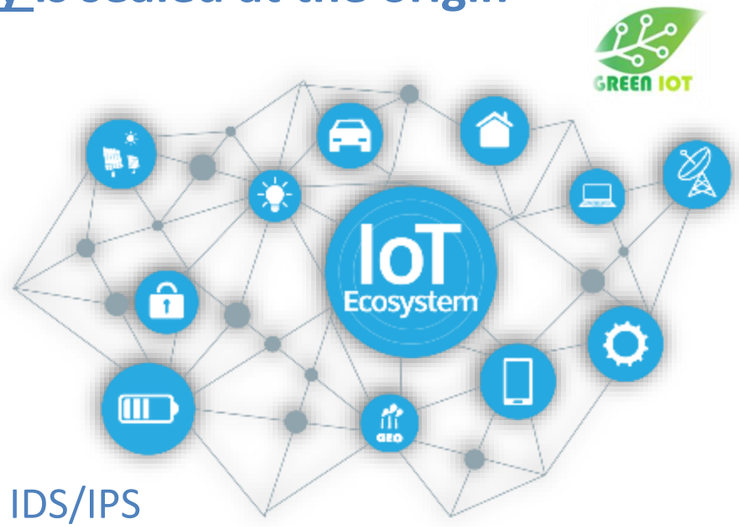
SGX, TXT, VBS
SEV SME
TPM
HW Protected Key Store

TRUSTICA

Old Way: Perimeter Defense

Perimeter Melt down: 0-Trust network and 0-Trust Peers

Data Privacy is sealed at the origin



IDS/IPS
Anti-Virus
Signature and constant Signature Updates
Detection Oriented

Traditional Security

Trust and Attestation: Patterns

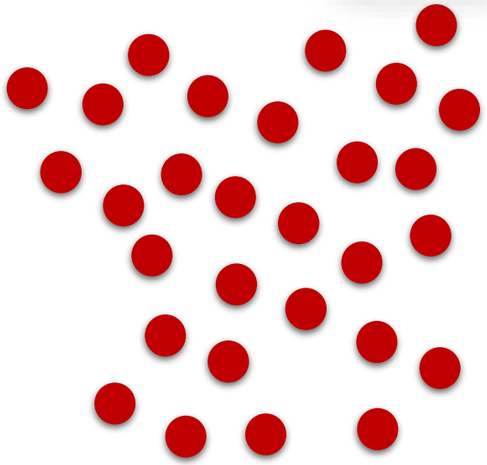
- **Sensitive Data sharing among “Circle of Trust” members:**
  - Data is encrypted the moment it is created
  - Can only be viewed by Group Members: Financial Transactions, Shared Video, Shared Evidence
- **Allows each member share information with designated group members without exposing the information to outside.**
- **Anonymity: No other group member can know the originator unless the publisher of the data wants to reveal**

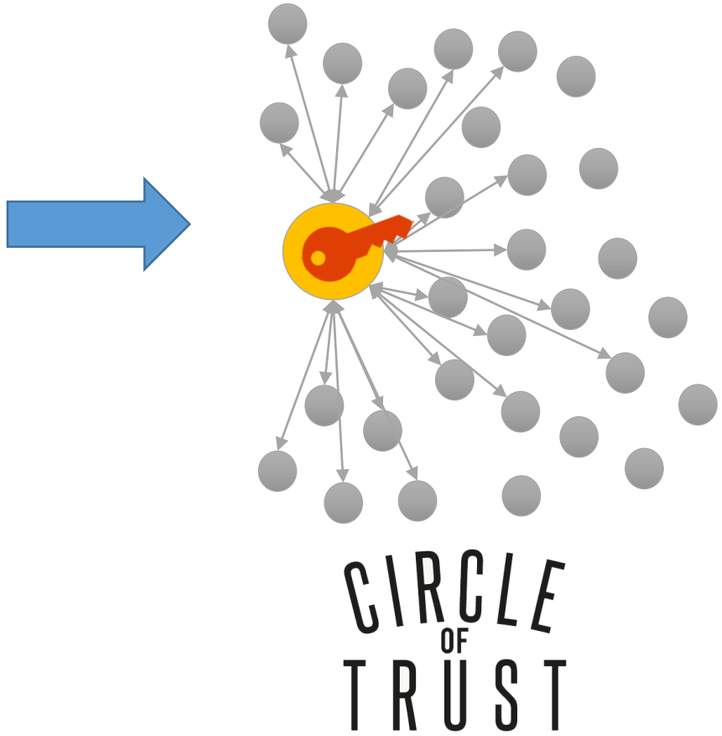
Foundation for End-to-End IoT Security: “Operating System for the IoT Eco System”

Trust and Attestation: Key Elements

- **Immutable Identity for Every IoT Device**
- **IoT Onboarding with “call-home” and provisioning**
- **Establishes Platform Identity**
- **Based on Hardware root of Trust: Private key is in Silicon (i.e. TPM’s Endorsement Key)**
- **Rich Privacy Protection**
  - Mapping Attack Defense
  - Anonymous Trusted Business Transactions
- **Authenticates “platform” identity through remote attestation using asymmetric (public and private key) crypto.**
- **Built-in Identity for Device Registration and Provisioning**

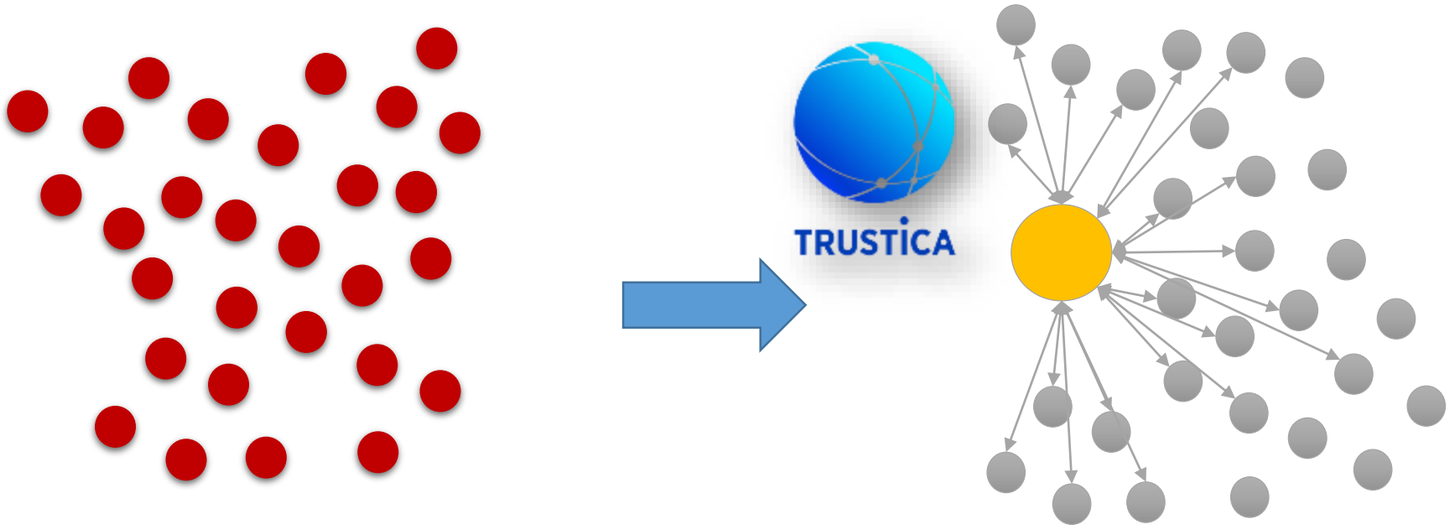
TRUSTICA Management System: Trust and Control





Group Identity
TCG Remote Attestation
Dial-Home on boarding
Anonymity Preserved within

TRUSTICA Management System: Trust and Control



IoTGuard Management System Establishes Trust for:

- Discovery/Revoke
- Device Identity, Credentials, Authentication
- **Attestation**
- Data-At-Rest (Containers)
- Data-In-Motion with Standard Protocols
- Policy Management
- Auditing
- Monitoring
- Alerting

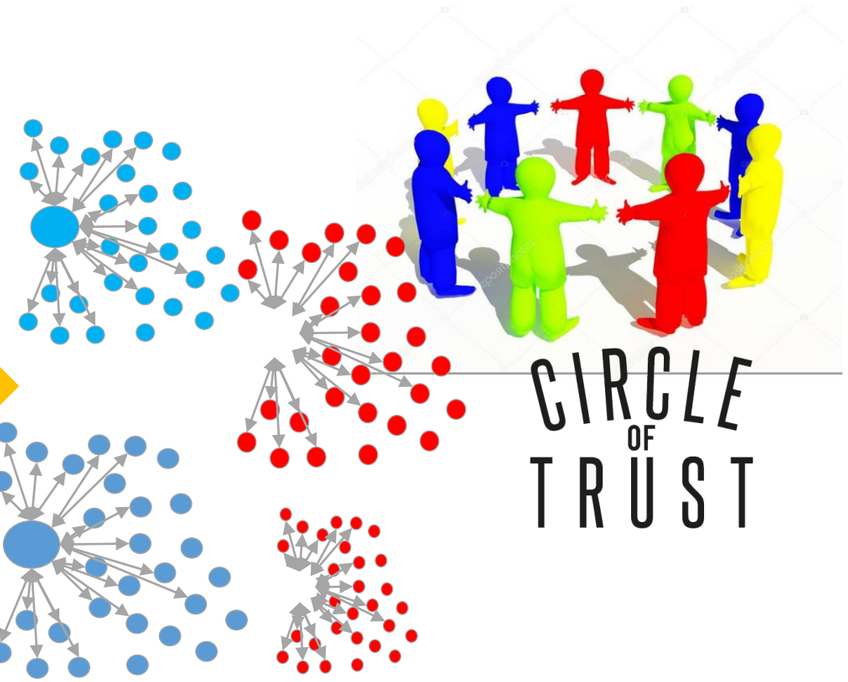
Management System Adheres to IoT Standards

TRUSTICA

Event Bus
Trust Bus
Policy Bus

Authentication
Onboarding
Provisioning
Remote Attestation

IoT
Event
Hub



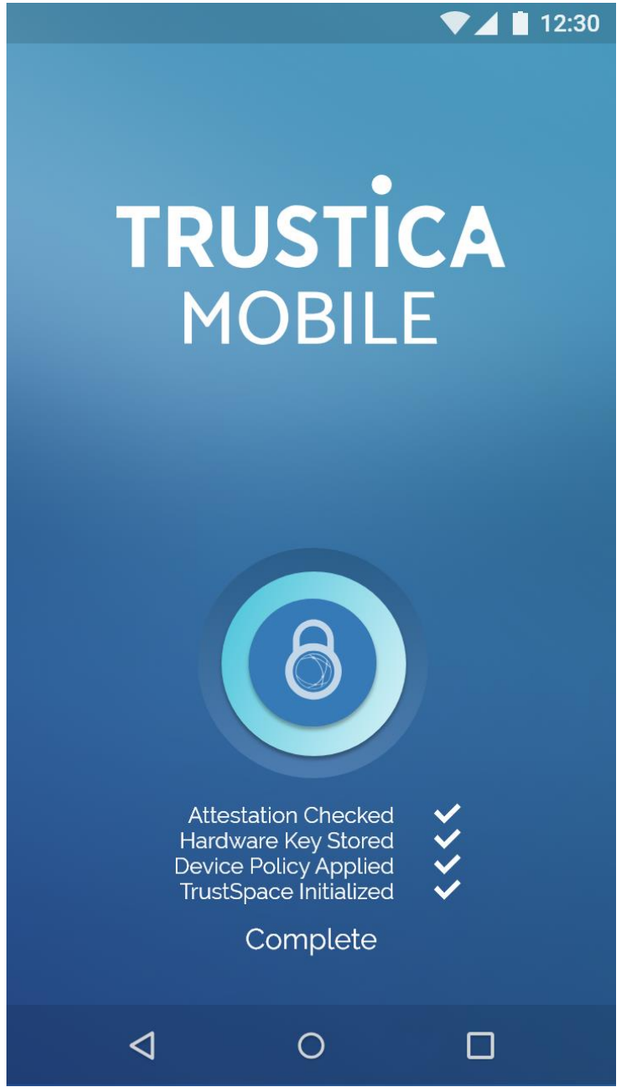
Analytics

IoT Service Platform (TLS, AMQPS and MQTTS)

TRUSTICA

- Kakogawa City and Kobe City
  - Bus Location, Taxi, Traffic Flow Safety
  - Safety Monitoring
  - Crime Reduction for Safe City: For Children and Elderly

- Car Sharing-TRUSTICA Mobile as a Secure Platform for Virtual Keys



TRUSTICA MOBILE

App for mobile devices (Android and iOS)

- ✓ Highly secure end-to-end communication and data exchanges
- ✓ Continuous device validity, safety, and integrity check via remote and dynamic attestation
- ✓ Complete Data protection of information stored in TRUSTICA Mobile's TrustSpace

Technology: Uses open protocols

- ☐ Binding user information with Device H/W credentials
- ☐ Distributed key management
- ☐ Remote and Dynamic Attestation technologies: device validity, safety, and integrity
- ☐ Isolation Technology for secure data containment: complete data protection
- ☐ Policy enforcement via assurance levels: high degrees of authentication
- ☐ Trust relationship management: TRUST Circles

TRUSTICA Final Word

- OS for the Connected World
- Data privacy and integrity the moment is created [SSL, TLS, etc. not secure]
- Working examples
  - Two cities in Japan
  - V2I
  - Currently working with Car Sharing to store Virtual Key
  - TRUSTICA Mobile for Multi-Factor Authentication for Banking applications