AppID Registry
A Foundation for Trusted Interoperability

Ian Deakin - Head of Innovation

12th July 2017

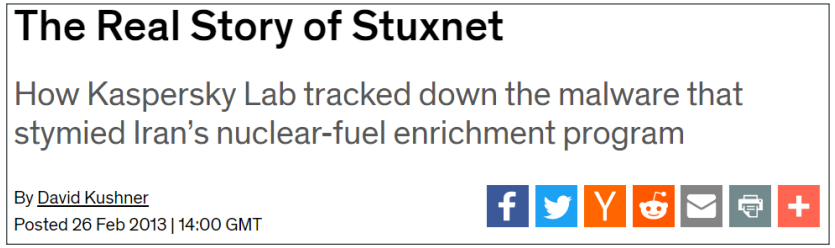
iconectiv®

IoT Trust, Security and Privacy Issues

DDoS service targeting PSN and Xbox powered by home Internet routers

Lizard Squad's for-hire services made runs on thousands of home routing devices.

DAN GOODIN - 1/9/2015, 3:35 PM



The Real Story of Stuxnet

How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program

By David Kushner
Posted 26 Feb 2013 | 14:00 GMT

World's largest 1 Tbps DDoS Attack launched from 152,000 hacked Smart Devices

Tuesday, September 27, 2016 Swati Khandelwal

A New Era of Internet Attacks Powered by Everyday Devices

By DAVID E. SANGER and NICOLE PERLROTH OCT. 22, 2016 The New York Times

LILY HAY NEWMAN SECURITY 03.02.17 10:30 AM

MEDICAL DEVICES ARE THE NEXT SECURITY NIGHTMARE

IoT security today is a fragmented environment of proprietary technical implementations, often with weak security, creating silos and restricting interoperability. Solving for secure trusted interoperability of IoT data will allow economic value growth.

iconectiv®

Current IoT Authenticity and Trusted Data
Problem Statement

Connection by an IoT devices application layer with a system needs to ensure that it can be trusted

- Not all 'things' are cellular based with authentication using SIMs
- IoT devices can be compromised at the application layer any time after they are connected

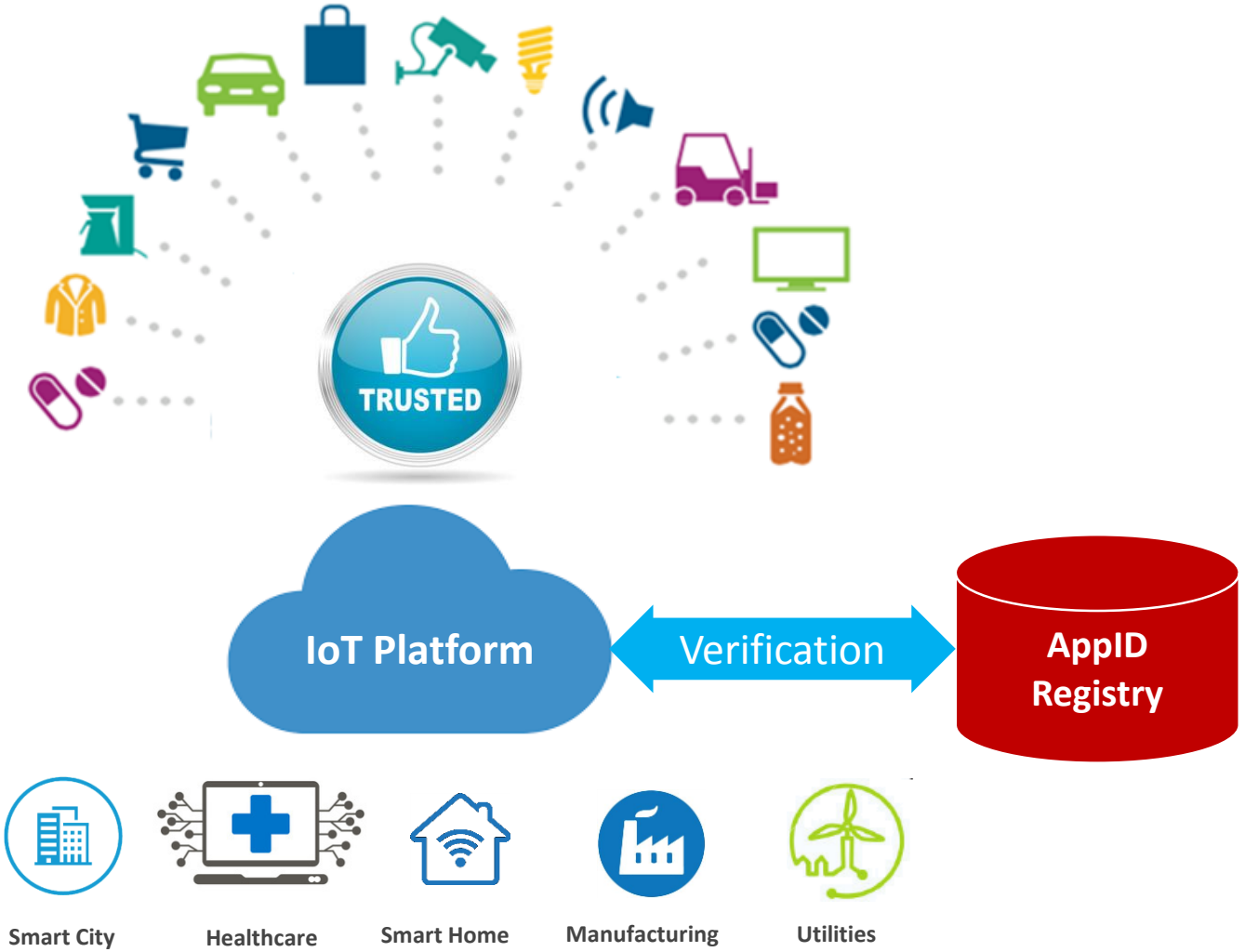
IoT authenticity and data security problems

- Unsecured supply chain for IoT devices: **spoofing of device and/or compromised data.**
- **No controls to manage unknown IoT devices**
  - Consumer IoT services will enable connection of devices outside of control (same as BYOD)
  - Smart Cities , will need to allow nomadic devices provide data to make decisions, i.e. vehicles
- **IoT devices support different security mechanisms,** X.509 Certs, pre-shared keys, raw public keys
- When supporting critical infrastructure, healthcare, smart cities, etc., **device compromise can be a significant concern, potentially catastrophic**
- Vertical solutions requiring bespoke configuration of even expected devices **hampers administrative scale**

Being able to validate identity integrity for a connecting IoT application is critical to securing IoT services

iconectiv®

Using AppID Registry
Trusted and Secure IoT Application Data



AppID Registry metadata

Provides an independent root of trust for IoT identities in industry verticals

- **IoT Identity Registration –** The IoT device application layer has a unique identity to enable an IoT platform to authorize connecting applications
- **IoT Authentication –** Metadata, to characterize the registered IoT application and the mechanism used to authenticate it. Access controls that must be observed for each unique instance.
- **IoT Trusted Data –** Metadata to characterize the data model for the registered IoT application, so that IoT platforms can enforce that only valid data be used perform analytics or take actions.
- **IoT Data Privacy –** Provide an application-specific privacy profile to the IoT platform, based on the unique instance of the specific IoT application, ensuring the device and its application data can only be used for the relevant purpose by approved entities.

iconectiv®

AppID Registry – Enhancement
Metadata information Fields

- **Registered IoT Identity (Globally Unique)**
  - IoT Device/Application type, Application Identity ‘AppID’
  - Identity Format: I.e. oneM2m: Reverse DNS format, i.e. Ra1.com.supplier.healthcare.pulsesensor
  - Range of Unique Entity Identifiers that are valid.
- **Application data profile**
  - IoT device/application characterization
  - Type of device, Class of device, Certification(s)
  - Data Resource consumption: periodic, real-time streamed, burst, etc.
  - Data definition mapping to a base ontology.
- **Authentication method**
  - Security type, X.509, pre-shared key, raw public key, challenge, none
  - Root Certificate
  - Certificate authority and trust level
- **IoT Entity Identity (instances)**
  - Unique Entity identifiers, to identify the specific instance
    - Serial number of the AppID to uniquely identify the instance\
    - Can accommodate many formats such as oneM2M AE ID
  - License Controls, permissible use,
  - State: Warehouse/Active/Stolen/Blocked
  - Subscription owner / service provider
  - Privacy profile

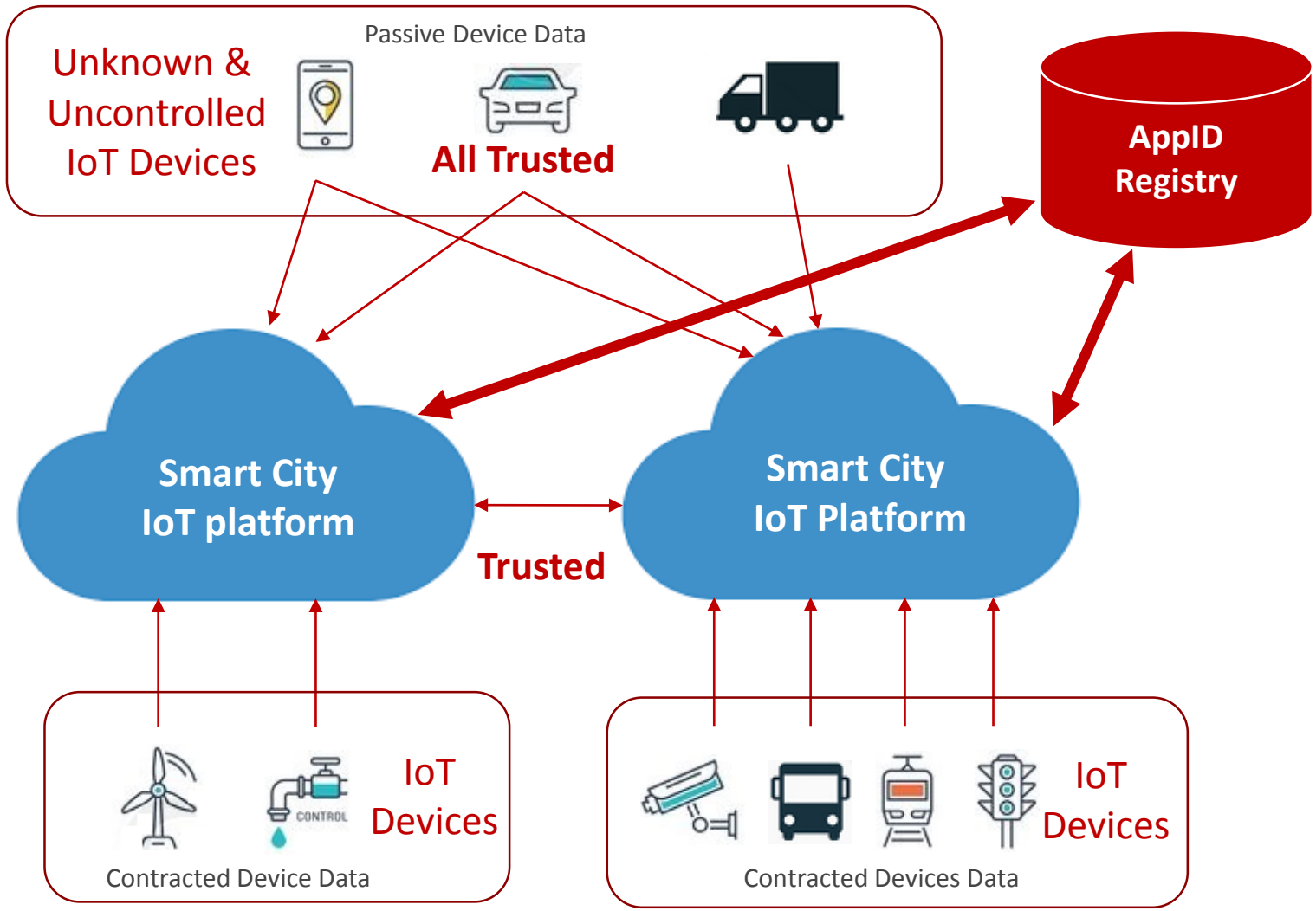
iconectiv®

Benefits to stakeholders
By using an AppID Registry

- **IoT Device/Application Vendors:**
  - Ability for devices to be broadly adopted by any IoT service provider. Improves market reach
  - Ability for applications to be compatible with a greater range of devices. Improves cost effectiveness and richness of dataset. Enhances rate of innovation.
  - Certification has greater integrity, increase brand value and confidence to buyers
- **IoT Platform and System Integrators:**
  - Streamlined onboarding and stronger enrollment, integration with broader range of IoT devices, reduce cost of ongoing management, self engineered for capacity, add value for data privacy, etc
- **IoT Network Operators and Service Providers:**
  - Open access, inclusion for a broader range of IoT devices and their data to be more innovative
  - Significantly reduce cost over vertically integrated sensor networks, scalable access control policies
  - Broader adoption, increasing return on investment and opens new revenue possibilities, data broker.
  - Supports compliance with data protection
- **Consumers and other End Users:**
  - Ease of access to participate in service using own IoT devices, participation in broader range of services
  - Ensure privacy controls over use of data, potentially in exchange for value

iconectiv®

Using AppID Registry
Smart City – Use Case



Problems For Smart Cities

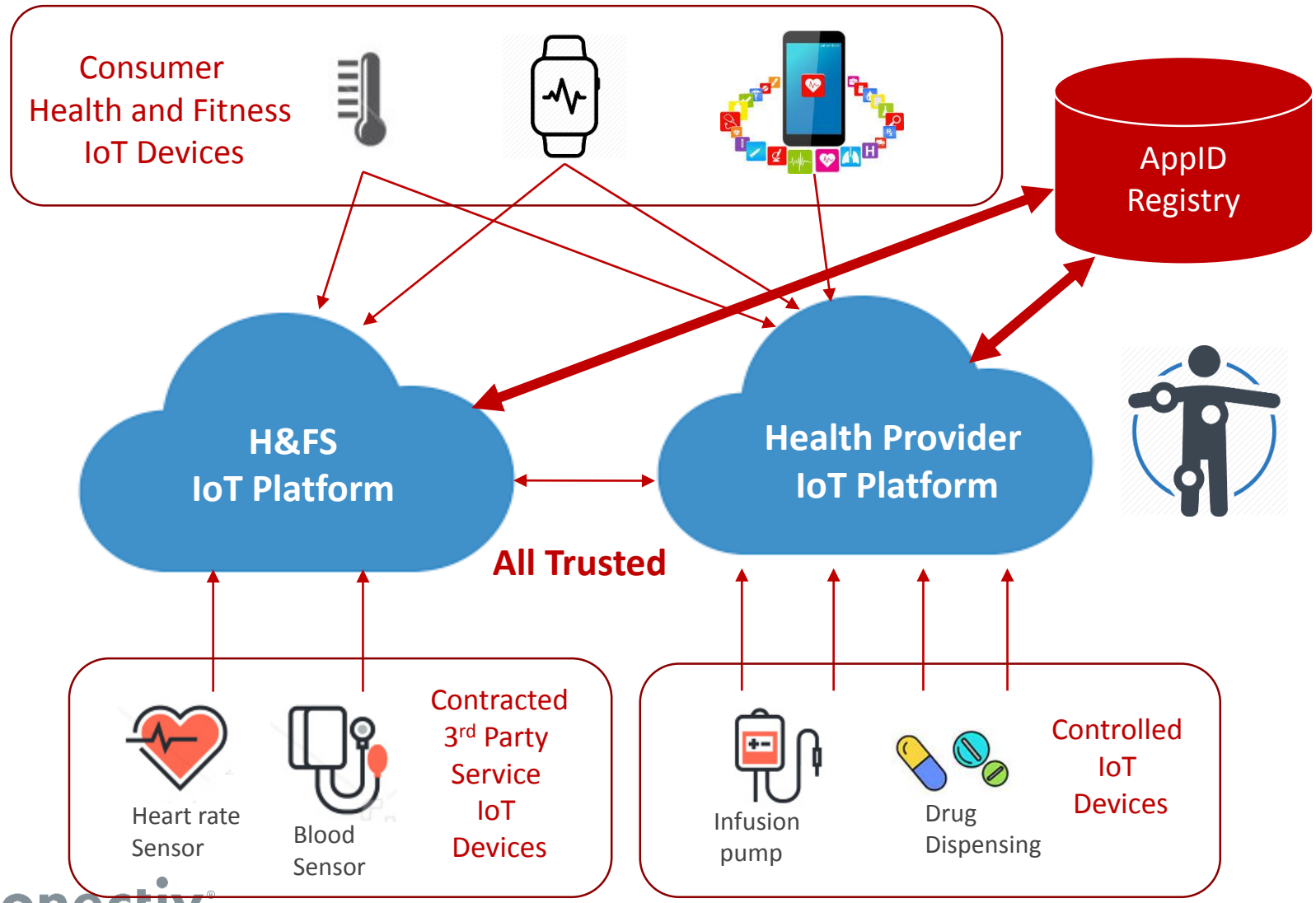
- Unknown devices cannot be pre authenticated.
- Cost efficiencies of scaling own sensors is not viable
- Administrative complexity managing configs for all expected devices

Using an AppID Registry

- Citizens and businesses with their unmanaged things can be included in Smart City data sourcing
- Profiles for controlled devices can be discovered enabling scale
- Smart City can enable a data exchange platform for innovation via trusted sources
- Citizens/businesses can receive value in return for contributing data such as reduced costs for parking, tolls, express lane use, public transport, etc

iconectiv®

Using AppID Registry
Healthcare – Use Case



Healthcare IoT Problems

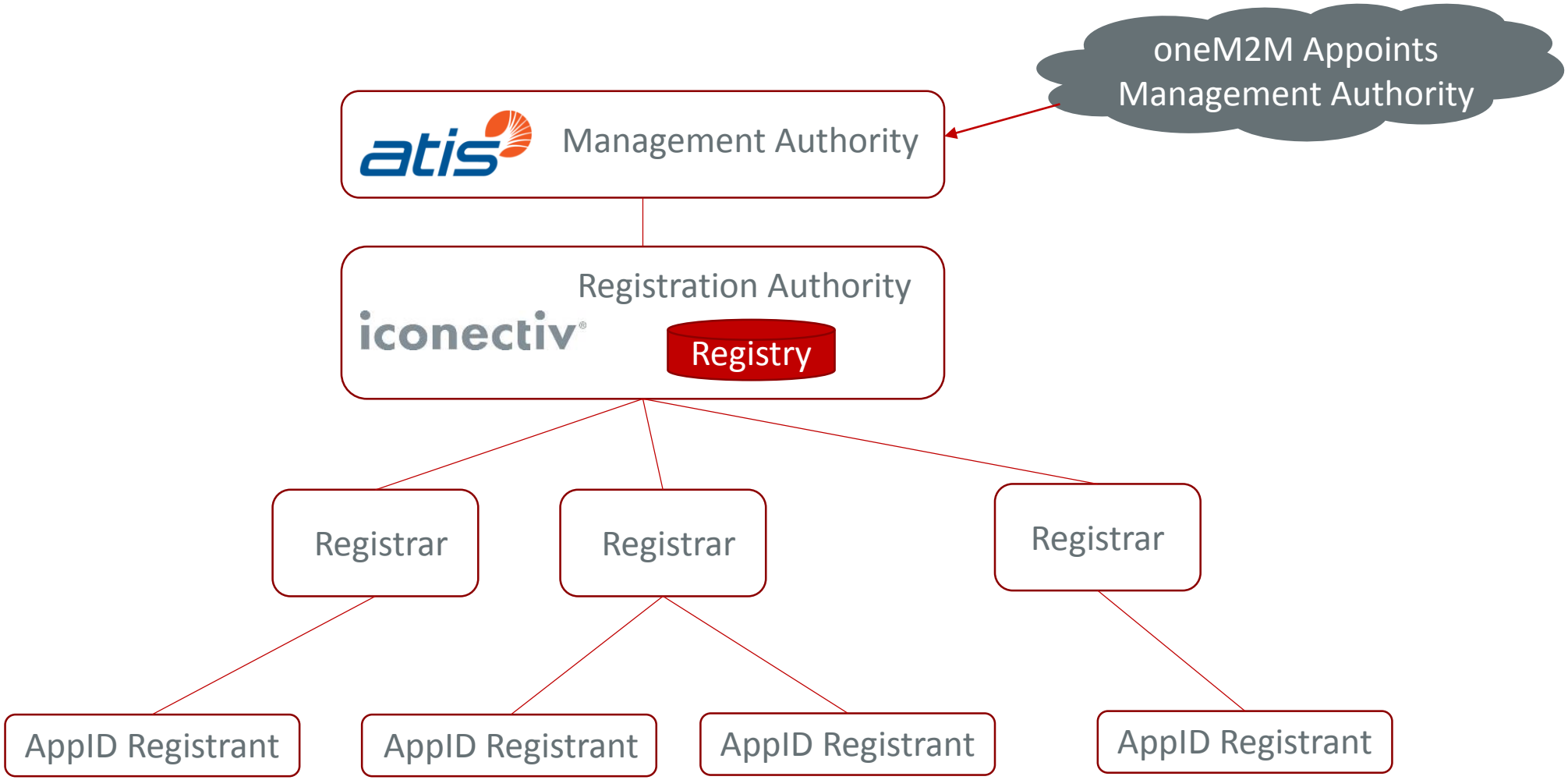
- Cannot identify or classify devices and know how to use the data
- Do not understand what devices are certified or fit for purpose.
- Cannot easily incorporate BYOD consumer devices into therapies

Using an AppID Registry

- Manage trust for BYO health and fitness sensors contribution to patient wellbeing and clinical decisions, etc
- Boarder inclusion for patient remote healthcare monitoring 24x7
- Reduced costs for connected healthcare solutions
- Healthcare service better informed, can better prioritize care services at the right time
- Detect early intervention needs, less chance of chronic or acute illness developing
- Healthcare service is less burdened with non critical patients taking up hospital recourse

iconectiv®

oneM2M App-ID Registry Today



iconectiv

AppID Registry
Participation in a Registry-based Ecosystem

- **IoT Device/Application Vendors:**
  - Registration of IoT devices and application identities within the IoT security registry
  - Define IoT metadata, characterization of capabilities, security and service
  - Declare the trust authority / CA for authentication
  - Certification process (e.g. oneM2M compliance by TTA South Korea)

- **IoT Platform and System Integrators:**
  - API connection with IoT registry for enrollment of connecting IoT devices and applications
  - Implements automated enrolment process to incorporate IoT registry identity and authentication
  - Reporting of rogue devices that attempt to enroll or legitimate devices later compromised

- **IoT network operators and service providers:**
  - Integration with registry service to manage connecting IoT devices and applications at scale
  - Integrate with existing security stacks as per registry metadata to enhance IoT identity and authentication
  - Reporting of rogue devices

- **Buyers/Consumers/End Users:**
  - Awareness of trusted IoT devices and value from being able to share the data
  - Register devices to participate in IoT data sharing
  - Change default passwords!

iconectiv®

Using an AppID Registry
Conclusions

AppID Registry for the industry:

- Provides a foundation for IoT security across the ecosystem, for all stakeholders at scale
- Ensures that IoT applications and the data they produce can be trusted.
- Underpins secure interoperability as a trust framework to share and commercialize IoT data.
- Enables consumer privacy controls over use of data.
- Increases brand value from use of certified and trusted devices

Benefiting the IoT economy for all:

- Enables broader inclusion for IoT device manufacturers and consumers
- Lowers cost of implementation, integration and ongoing management
- Creates data that can be trusted, while protecting privacy of customers.
- Maximizes revenue and limits IoT security vulnerabilities through trust-based open IoT services
- Maximizes service innovation through increased interoperability that is also secure.

iconectiv®

thank you

keep it simple, seamless, and secure

iconectiv®