Decentralized IAM for IoT: Challenges and Opportunities

Xinxin Fan, Ph.D., CISSP
IoTeX
October 4, 2021

About Me

IoTeX Official blog

Head of Cryptography

Industry IoT Consortium

Co-Chair of Industrial Distributed Leger Task Group

IEEE SA STANDARDS ASSOCIATION

Vice Chair of IEEE P2418.1™ - Standard for the Framework of Blockchain Use in Internet of Things

Chair of IEEE P2958™ - Standard for a Decentralized Identity and Access Management Framework for Internet of Things

CONFIDENTIAL COMPUTING CONSORTIUM

Member of Technical Advisory Council

MOBI

Member of Trusted Trip Working Group

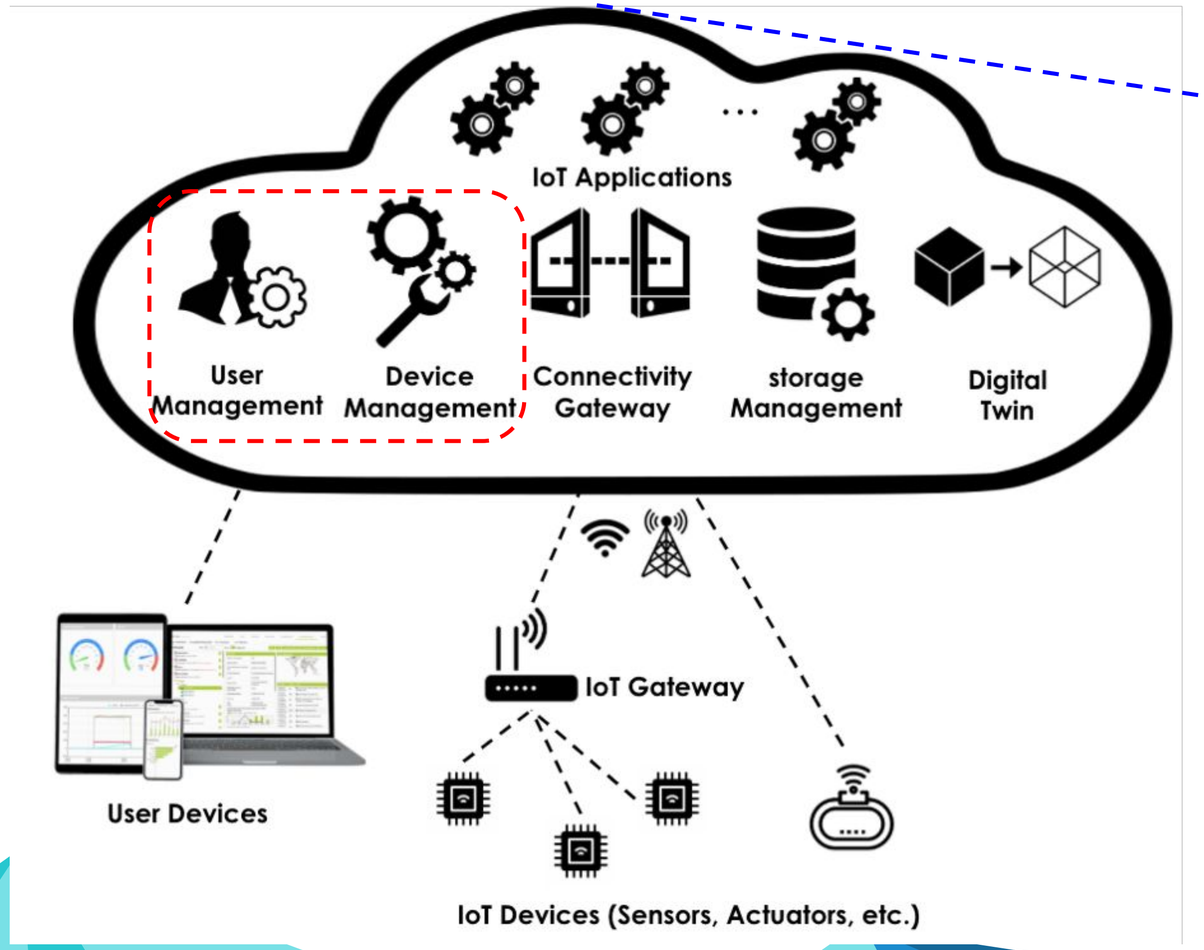
Outline

- IAM for IoT: Centralized vs. Decentralized
- Challenges & Opportunities
- IEEE P2958 Standards Project
- Internet of Trusted Things (IoTT) Platform

IAM for IoT: Centralized vs. Decentralized

1

Cloud-Native IoT System Architecture



Microsoft Azure IoT Suite

Google Cloud's IoT Platform

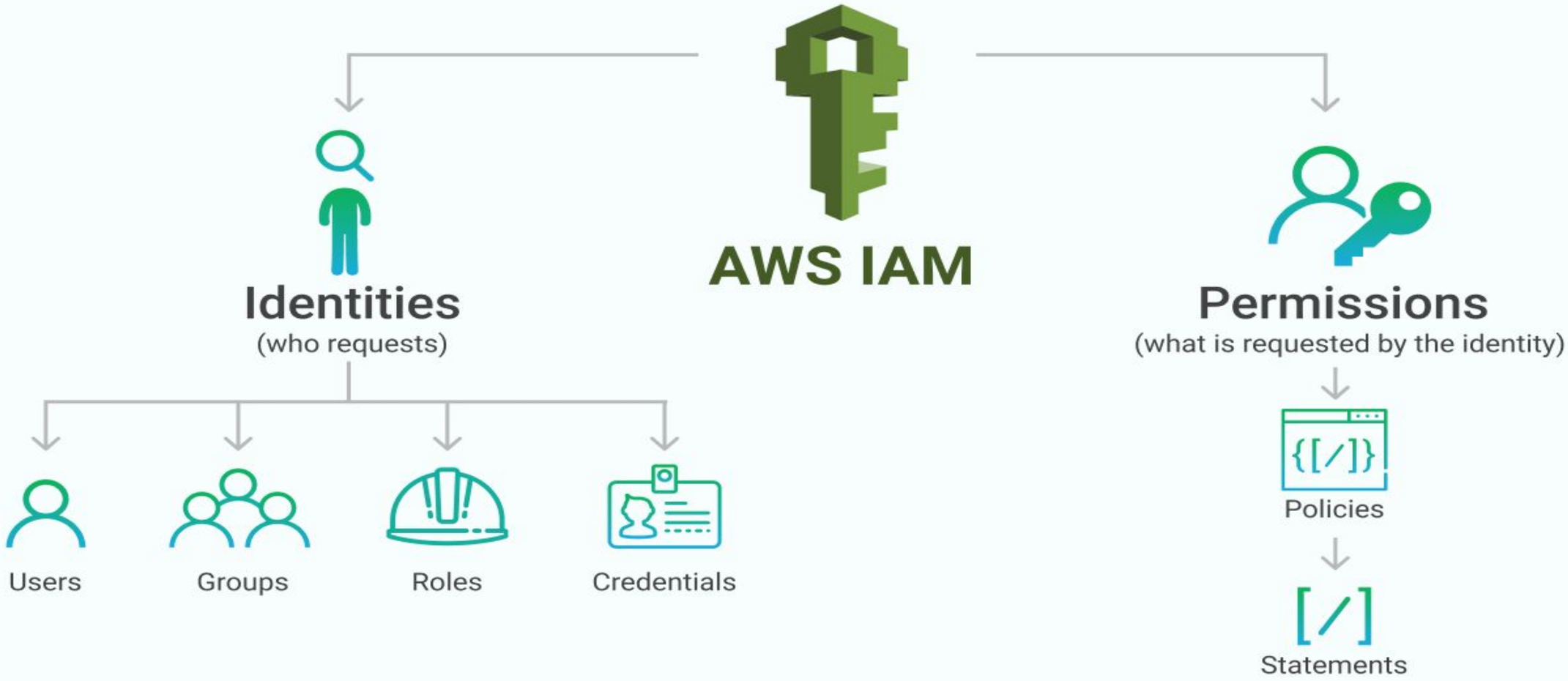
AWS IoT Platform

Cisco IoT Cloud Connect

Oracle IoT Platform

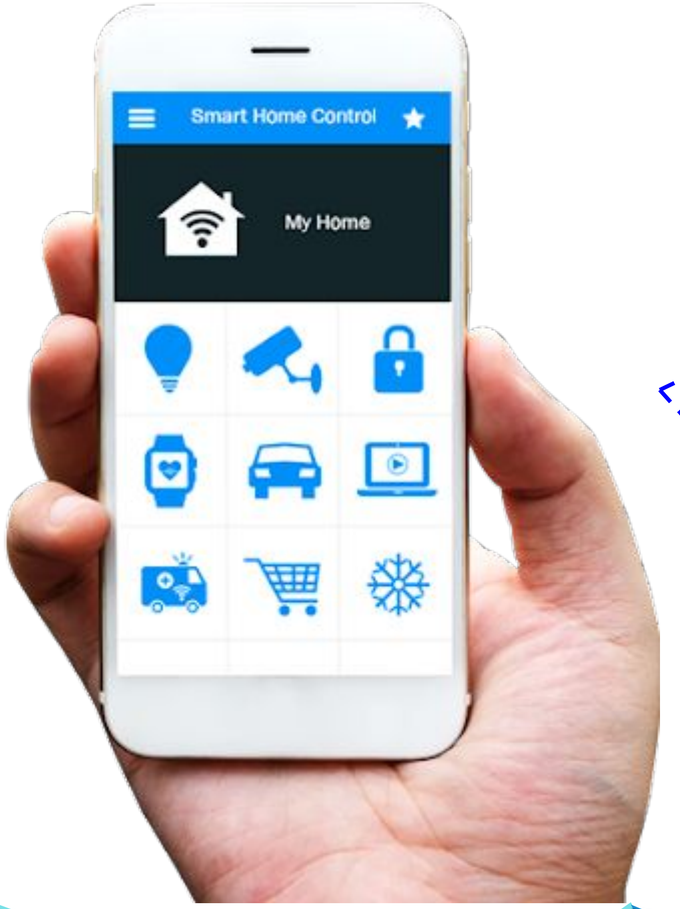
IBM Watson IoT Platform

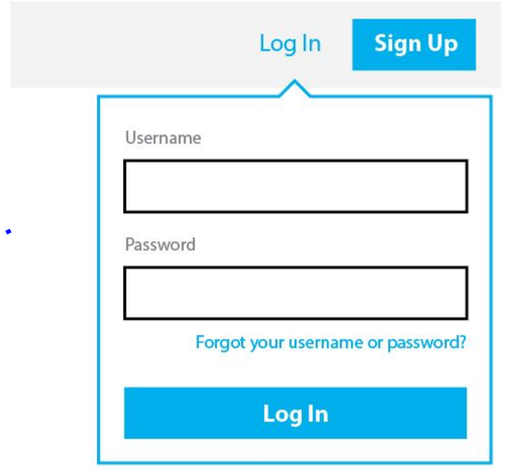
Cloud-Native IAM - User Management



Credit: https://www.msp360.com/resources/blog/aws-iam-policy/

User Login

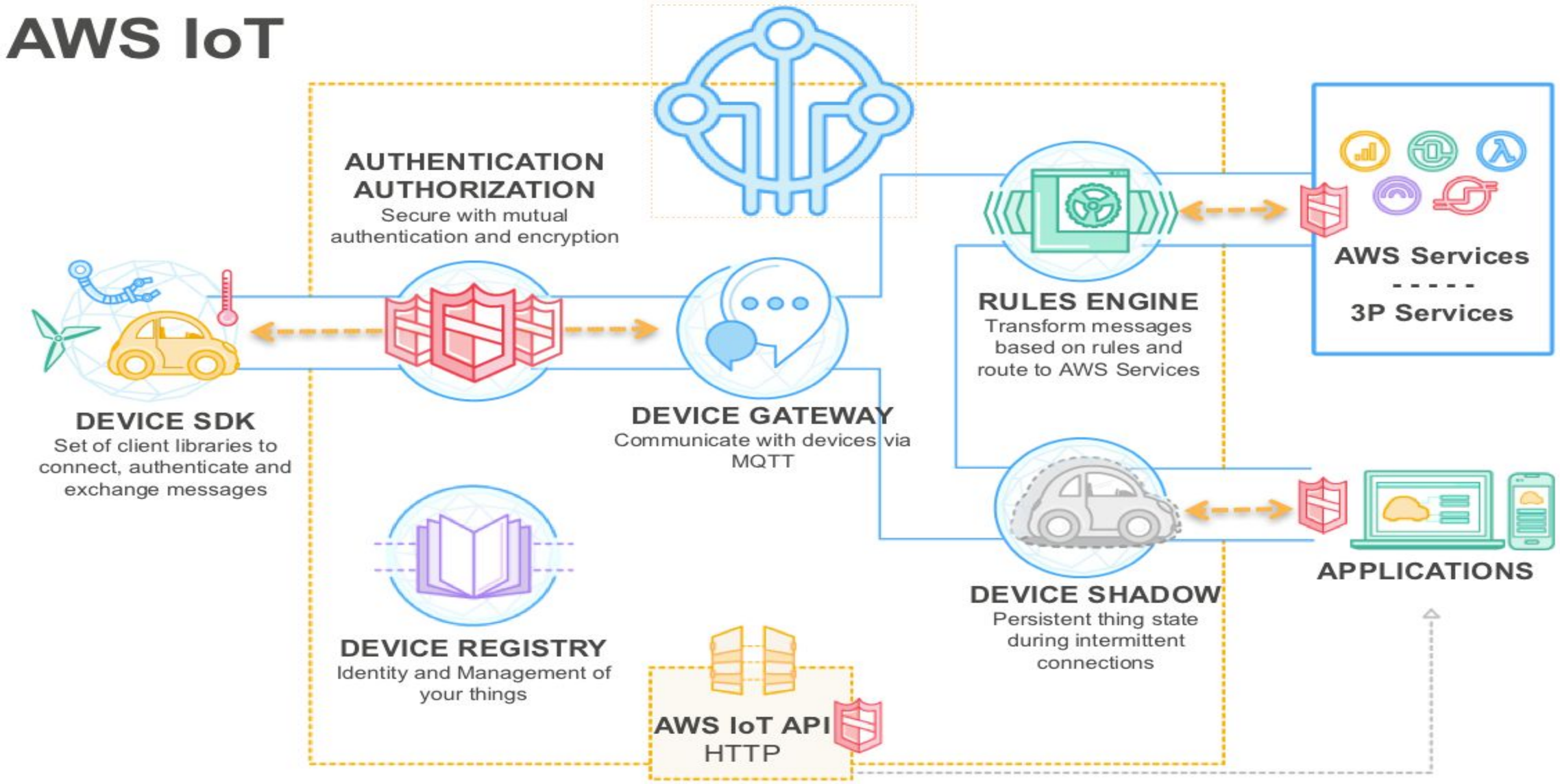




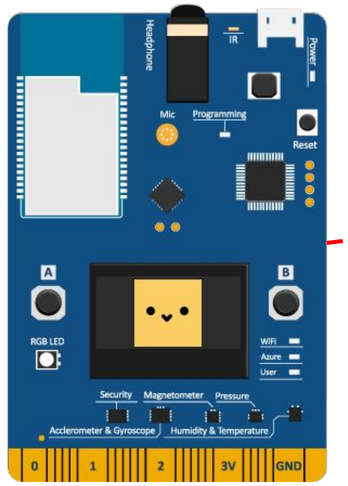
Centralized Identity

Federated Identity

Cloud-Native IAM - Device Management



X.509 Certificate & PKI



Certificate created!

Download these files and save them in a safe place. Certificates can be retrieved at any time, but the private and public keys cannot be retrieved after you close this page.

In order to connect a device, you need to download the following:

A certificate for this thing	fdd885eb3a.cert.pem	Download
A public key	fdd885eb3a.public.key	Download
A private key	fdd885eb3a.private.key	Download

You also need to download a root CA for AWS IoT:
A root CA for AWS IoT Download

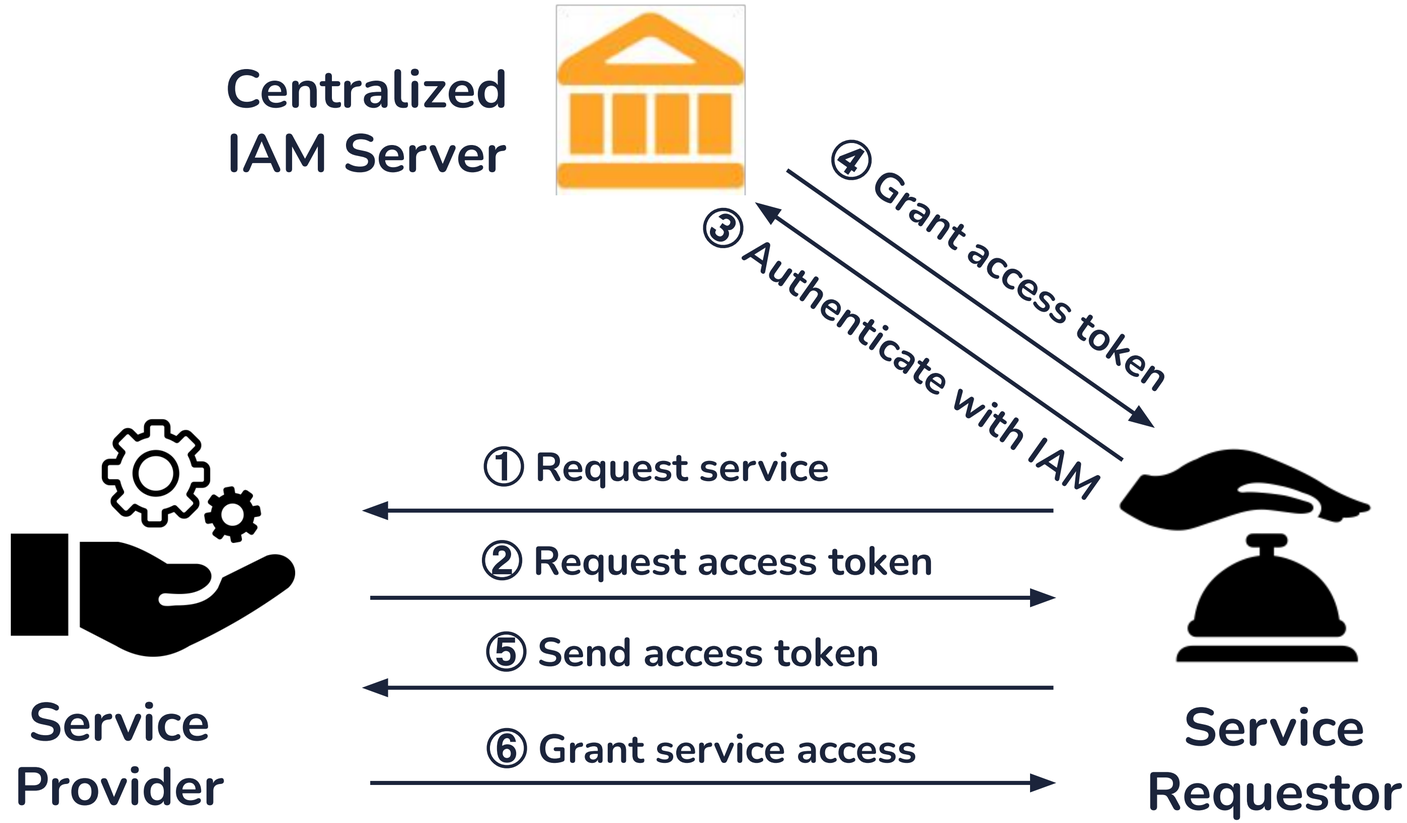
Activate

Cancel | Done | Attach a policy

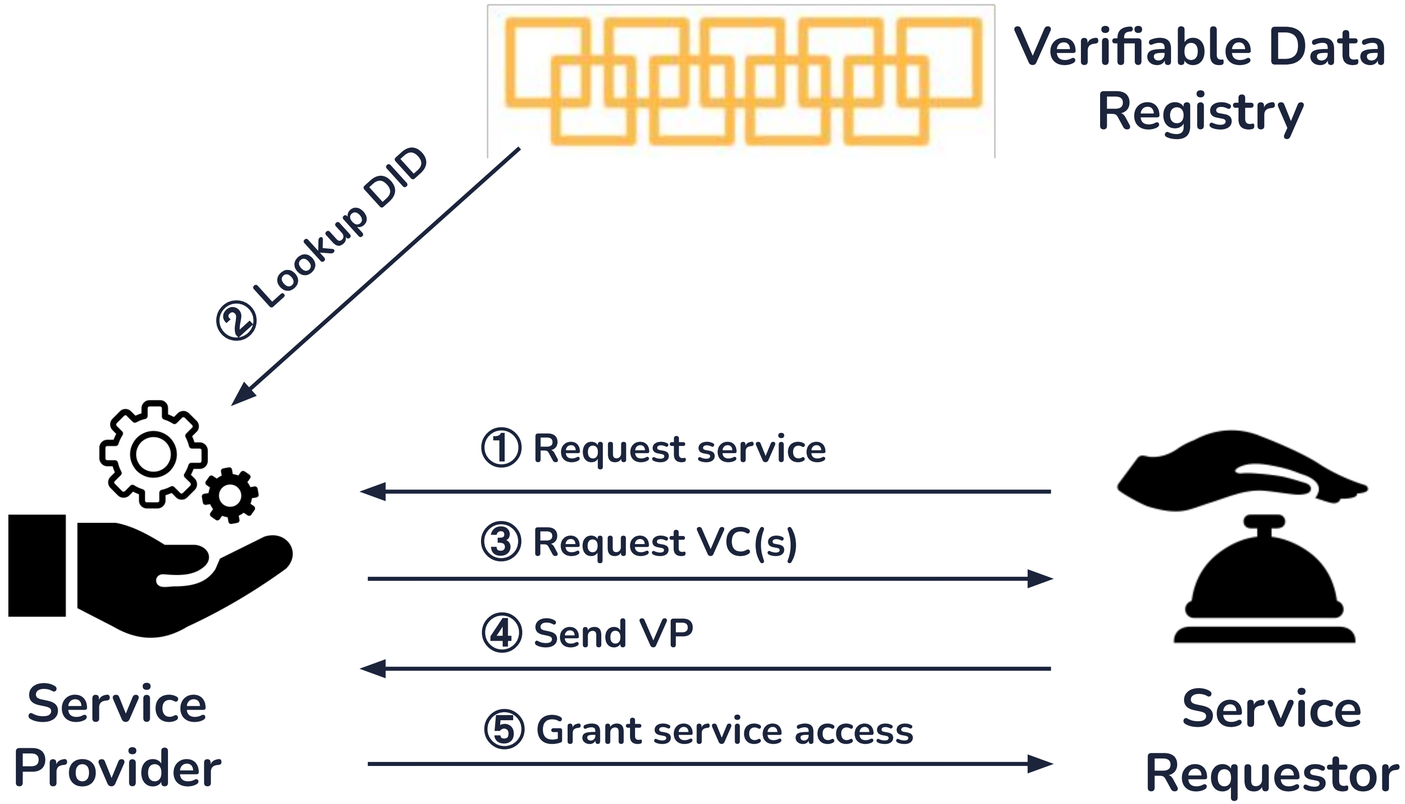
Certificate

- Version
- Certificate Serial Number
- Certificate Algorithm Identifier for Certificate Issuer's Signature
- Issuer
- Validity Period
- Subject
- Subject Public-Key Information
  - Algorithm Identifier
  - Public-Key Value
- Issuer Unique Identifier (Optional)
- Subject Unique Identifier (Optional)
- Extensions (Optional)
  - Extension Fields (optional)
- Certification Authority's Digital Signature

Interact with a Centralized IAM



Interact with a Decentralized IAM



What do DIDs and VCs matter for IoT?

- DIDs offer a unified representation of identity for people, IoT devices, servers, organizations, etc. ⇨ Simplified identity management and interoperability

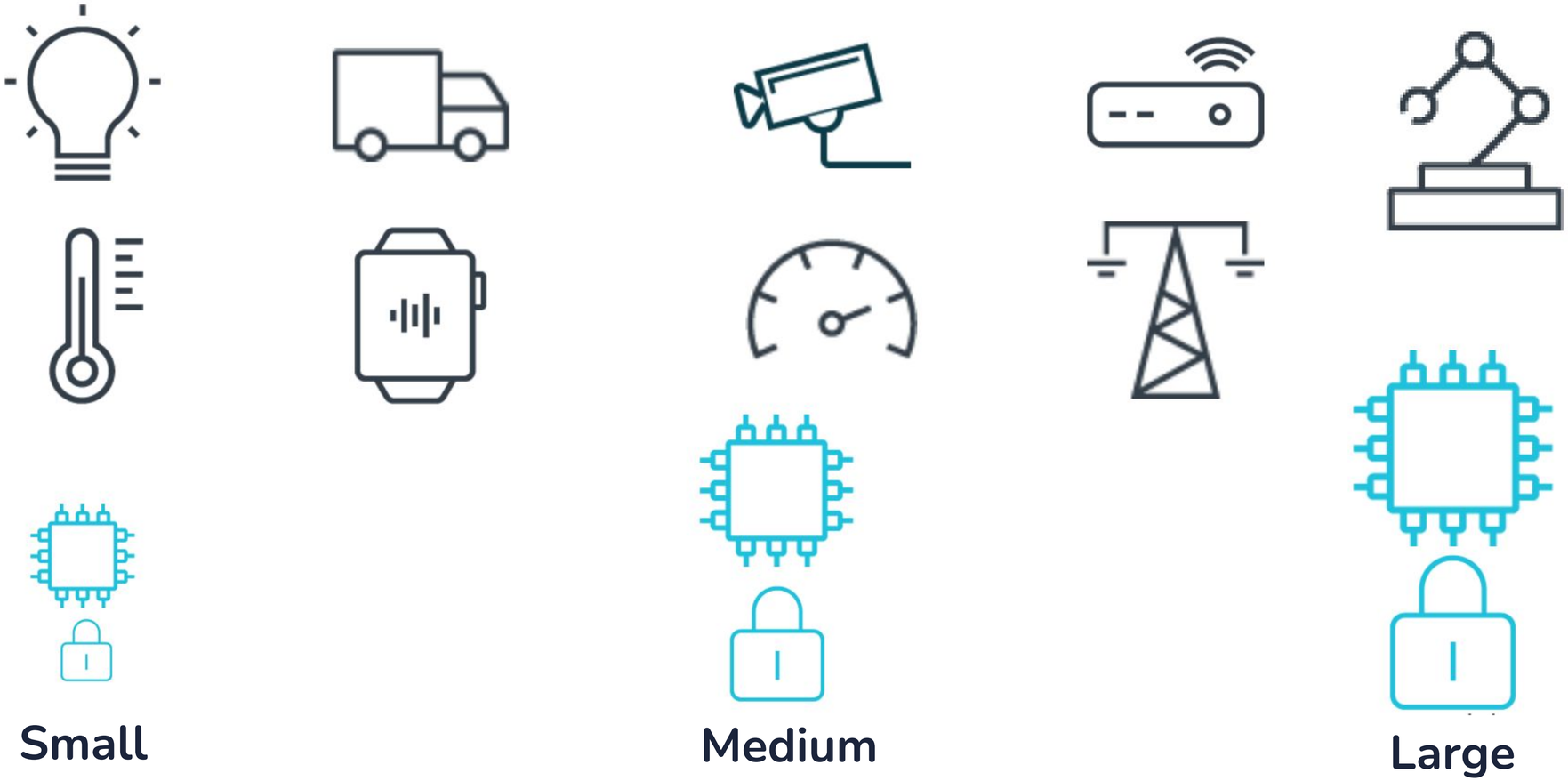
- VCs enable stakeholders to attest different attributes regarding IoT devices ⇨ Fine-grained levels for security and trustworthiness

- DIDs and VCs make it possible for building large-scale, decentralized, and interoperable IoT applications

Challenges & Opportunities

2

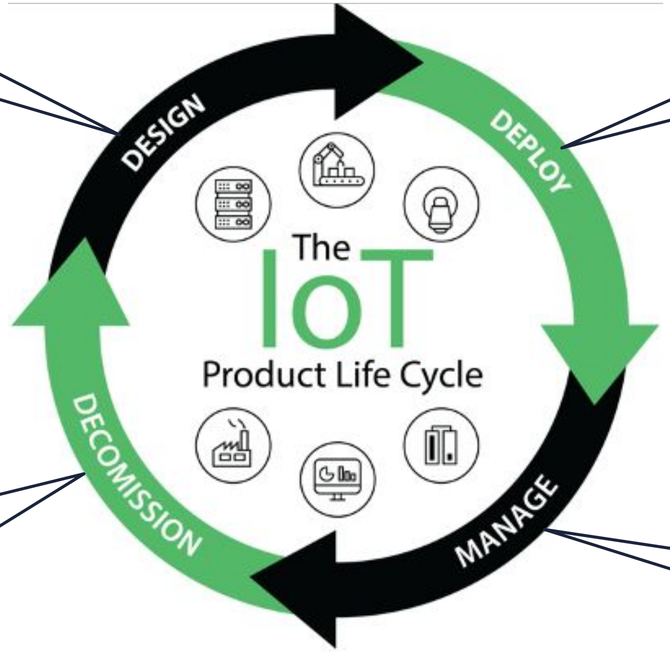
Challenge I - Different IoT Devices



Challenge II - Complex Device Lifecycle

- Device Provisioning
- Identity Generation

- Network Onboarding
- Application Onboarding



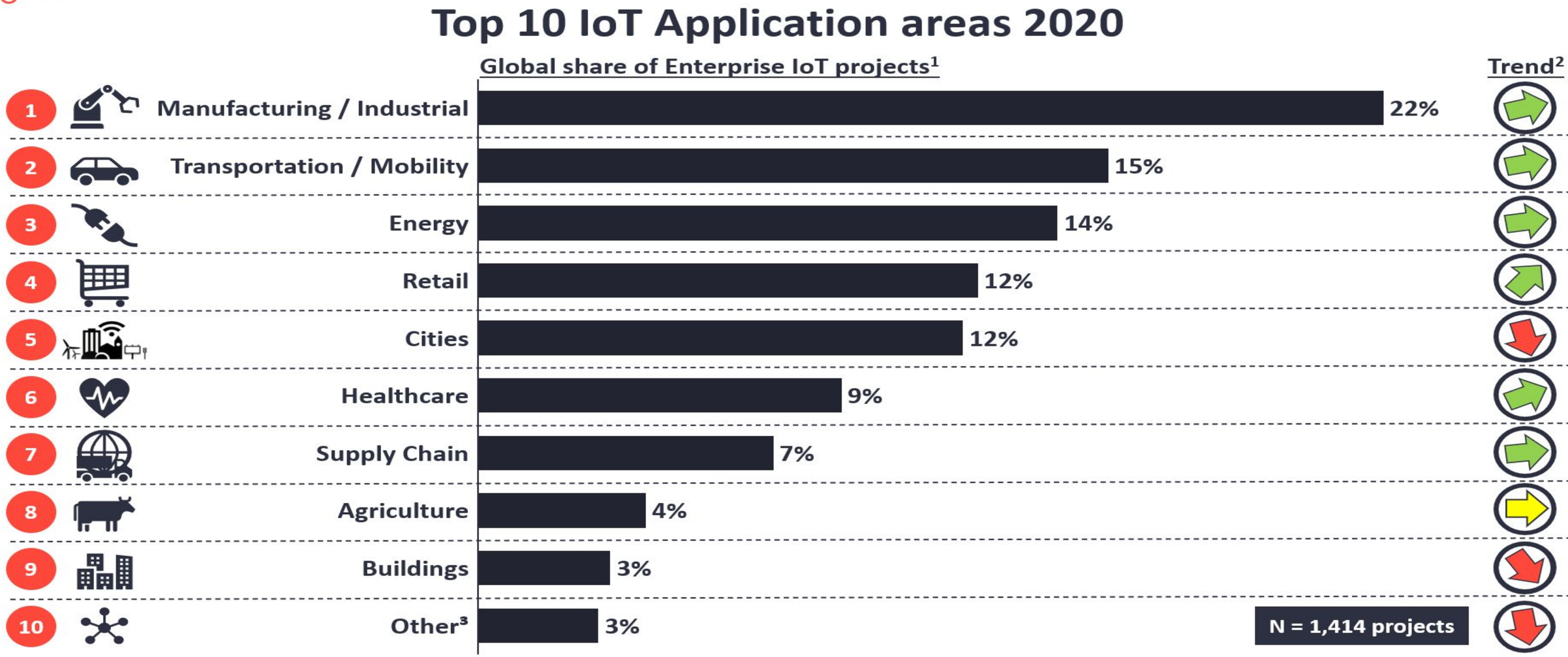
- Device Decommission
- Credential Revocation

- Over-the-air Update
- Ownership Transfer

Challenge III - Unlimited Use Cases

IOT ANALYTICS

Insights that empower you to understand IoT markets



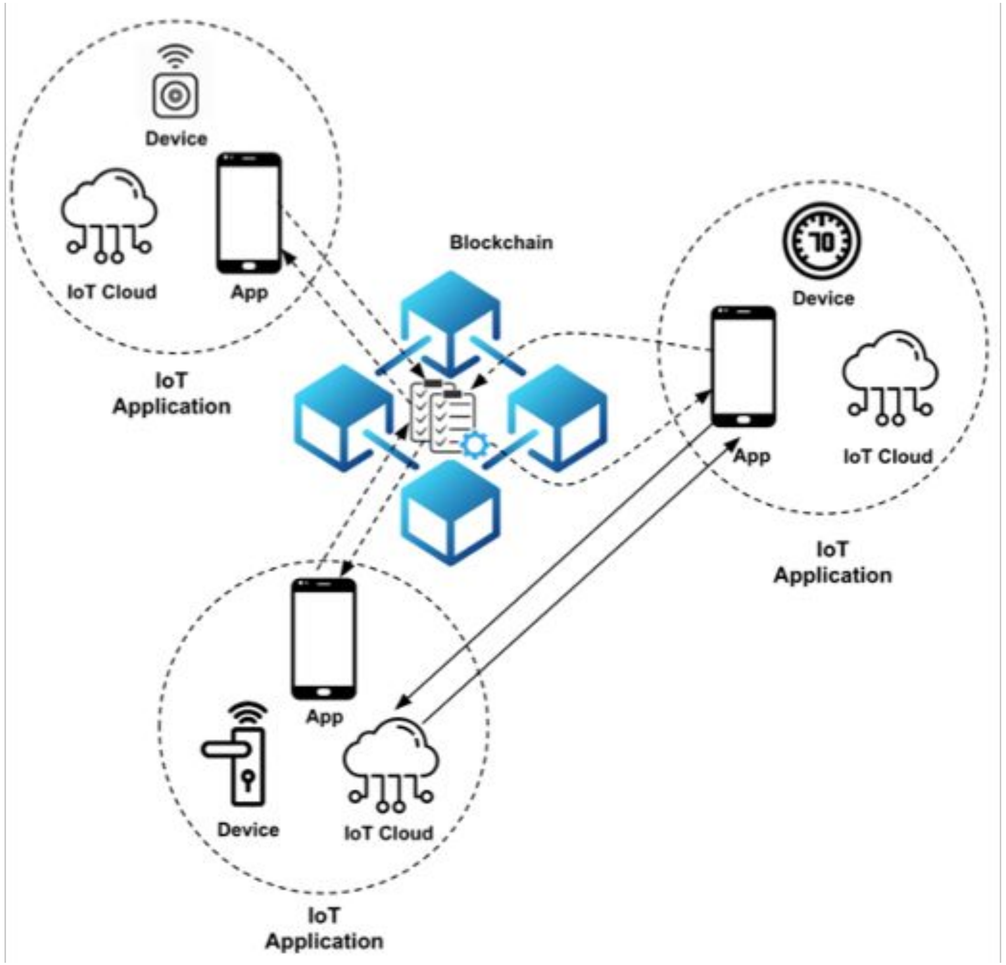
Note: 1. Based on 1,414 publically known IoT projects (not including consumer IoT projects eg smart home, wearables, etc.) 2. Trend based on relative comparison with % of projects in the 2018 IoT Analytics IoT project list e.g., a downward arrow means the relative share of all projects has declined, not the overall number of projects. 3. Other includes IoT projects from Enterprise & Finance sectors. **Source**: IoT Analytics Research - July 2020

Additional Considerations

- What are the minimum hardware requirements for implementing SSI for IoT?
- What do DIDs and VCs look like for IoT devices?
- How do we implement an efficient SSI SDK for embedded devices?
- How many DIDs does an IoT device need in its lifetime?
- Who can issue VCs in the IoT ecosystem?
- How should we deal with privacy for IoT?
- .....

Opportunities: DIAM-as-a-Service

DIAM-as-a-Service



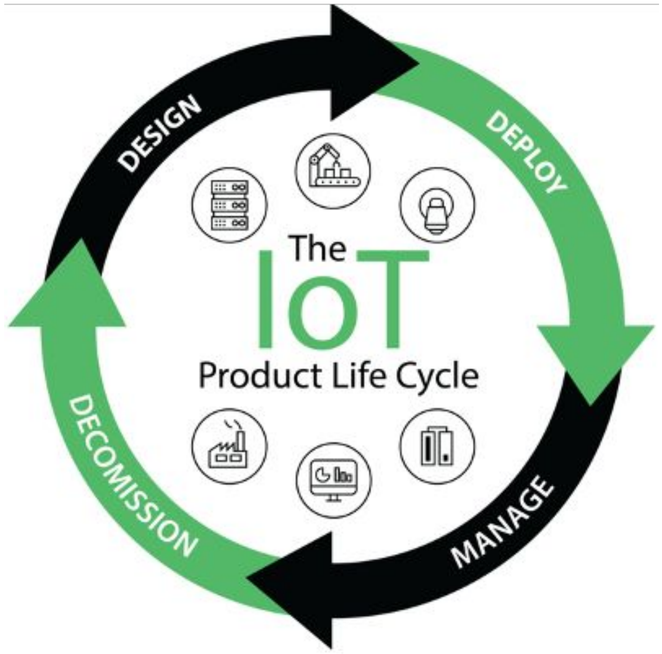
IEEE P2958 Standards Project

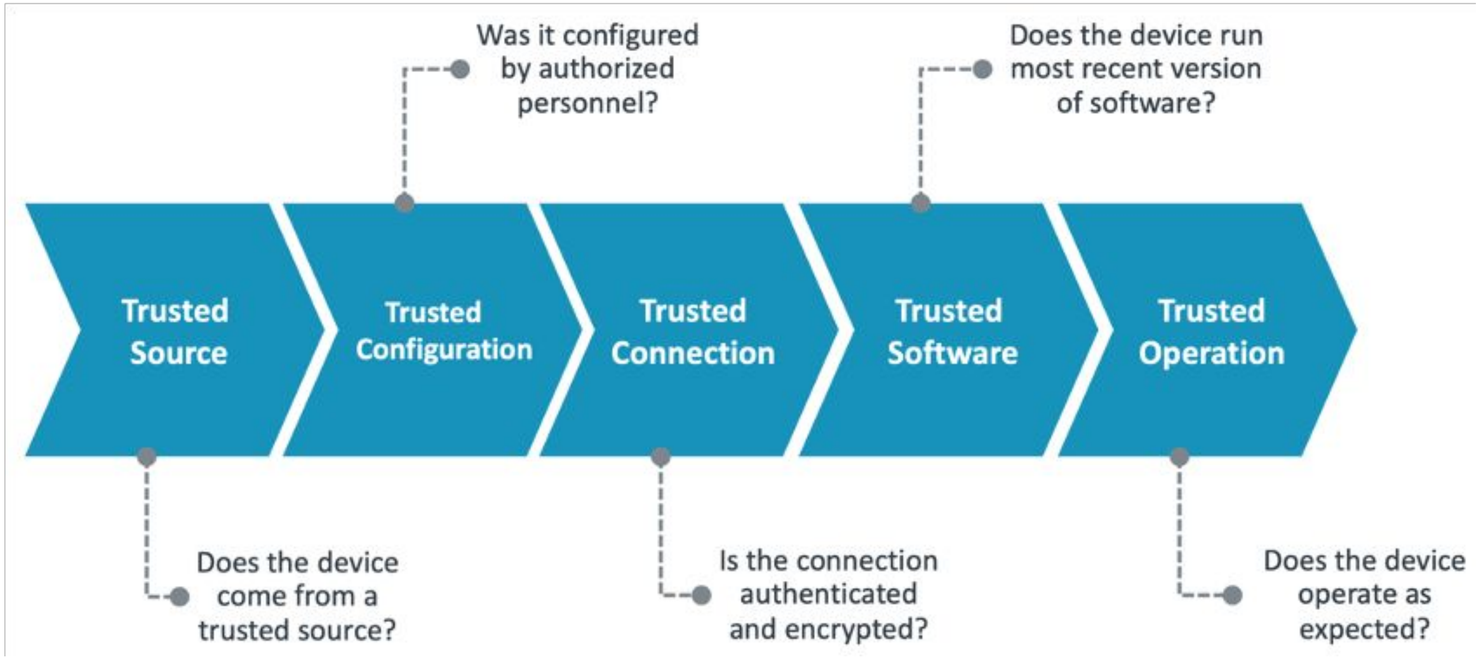
3

Project Overview

- The Project Authorization Request (PAR) https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/8651
- Project Scope: Define a decentralized IAM framework for IoT based on the emerging concepts such as decentralized identifiers (DIDs) and verifiable credentials (VCs)
- Working Group: Identity of Things Working Group (BOG/CAG/IDOTWG)

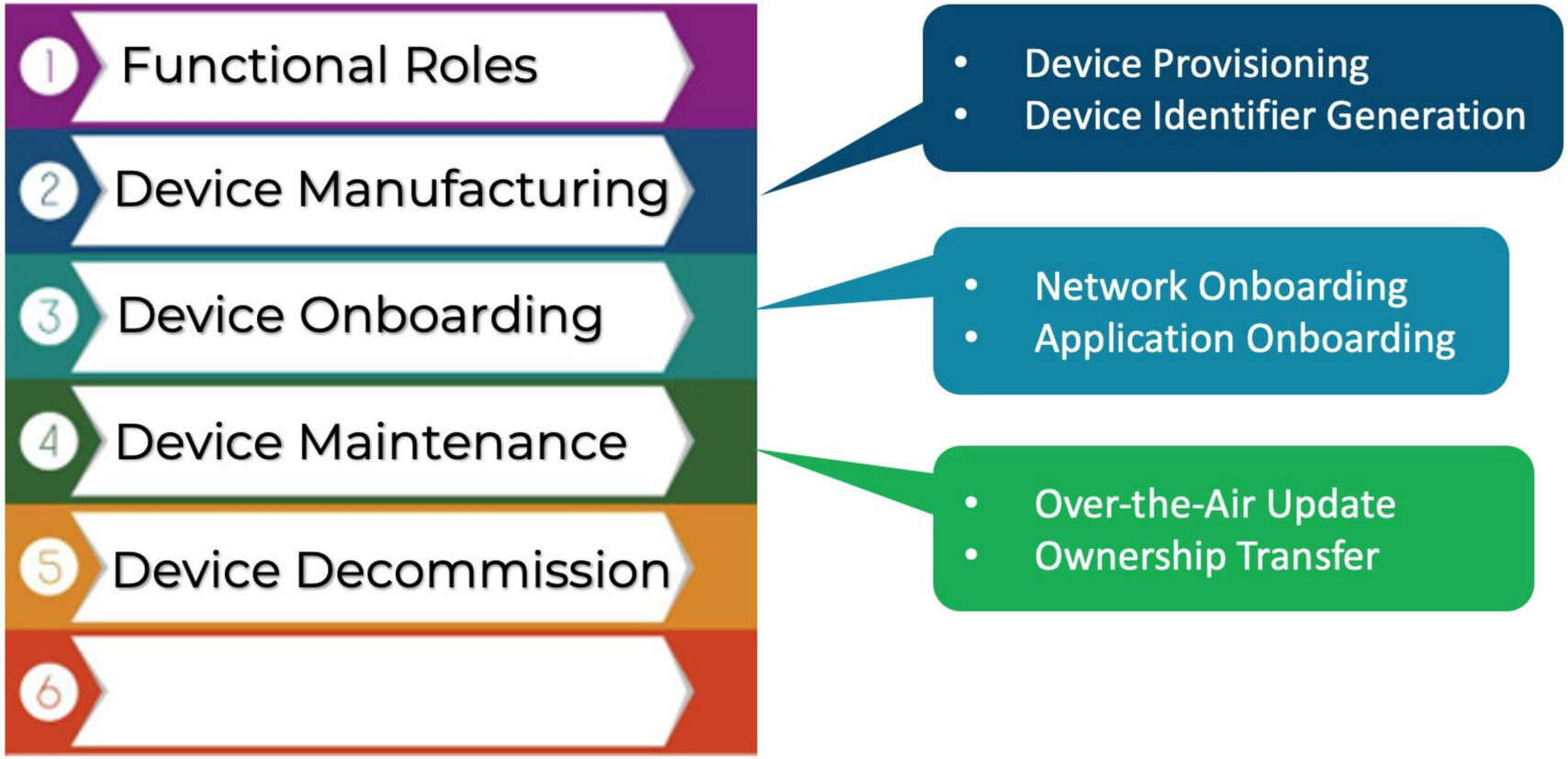
Project Focus





- Integrate DIDs and VCs into the lifecycle of IoT devices
- Specify a suite of decentralized IoT security services including device authentication, data authorization and access control, etc.

Preliminary Table of Contents



Internet of Trusted Things Platform

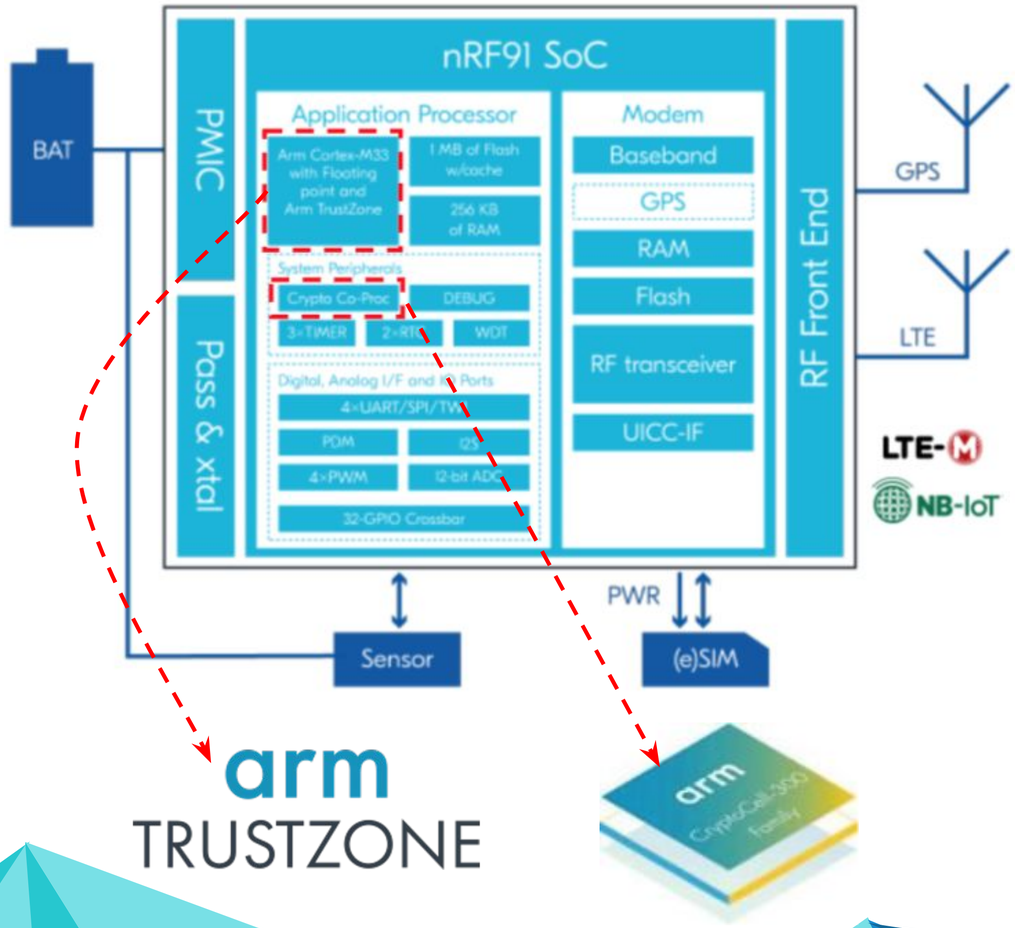
(Hardware + Oracle + Blockchain)

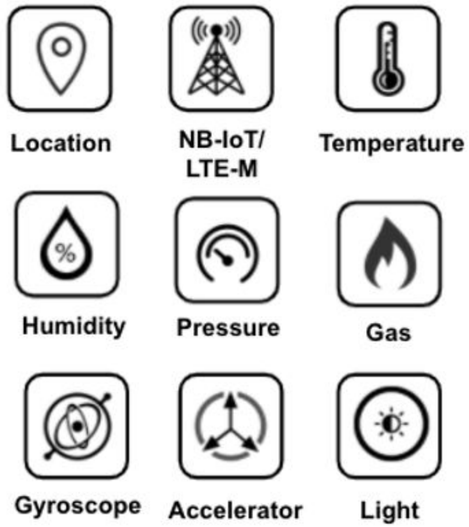
4

Pebble Tracker

- An “Out-of-the-Box” trusted and secure asset tracker development kit with 4G connectivity and wide array of sensor technologies
- Built around the latest low-power nRF9160 System-in-Package (SiP) from Nordic Semiconductor
- Equipped with GPS, climate, motion, and light sensors
- SoC platform security with ARM TrustZone and CryptoCell 310
- Supports LTE-M & NB-IoT (700 MHz to 2.2 GHz) and worldwide operations with IoT SIM cards
- Open-source development tools and SDKs from Nordic Semiconductor and IoTeX

Hardware Overview





Tech Perspective

Using a blockchain for secure asset tracking

IoTeX is combining the security built into Nordic's nRF9160 and its blockchain technology to protect the integrity of critical asset tracking data

The commercialization of cellular IoT asset tracking solutions such as IoTeX's Pebble Tracker has the potential to revolutionize supply chain applications. The product, powered by Nordic Semiconductor's nRF9160 SiP, uses mature, secure cellular infrastructure to provide location, environment and motion tracking data for global asset tracking.

But more than that, Pebble Tracker promises to address problems such as the more than $400 billion in annual losses that result from supply chain errors such as temperature excursions. Each year compensation for these loses and many others are sought, and payouts from penalty clauses and insurance claims rely heavily on asset tracking data. (See WQ Issue 2, 2020, pg22.) Should there be any suspicion that asset tracking information has somehow been tampered with or falsified, claims could drag on for years. And worse, litigation could follow.

IoTeX is tackling the challenge by combining the Pebble Tracker's nRF9160 SiP's Arm TrustZone (for trusted execution) and Arm CryptoCell 310 (for application-layer security) protection features with the company's blockchain for large scale, decentralized and trusted asset tracking applications.

Trust built on hardware and the blockchain

The Arm TrustZone technology built into the nRF9160 forms a Trusted Execution Environment (TEE). The TEE is a secure area inside the Arm processor that runs in parallel but is isolated from (and often invisible to) the main operating system. Code and data inside the TEE are maintained with the highest level of integrity and confidentiality. Such a system protects the valuable code and data while enabling less valuable code and data to run unencumbered on the main operating system. (See WQ Issue 3, 2019, pg26.)

But a truly secure IoT device requires more than a TEE: additional roots of trust (RoTs) and security mechanisms are demanded. That's the role of Arm's CryptoCell.

CryptoCell is an embedded security platform for devices using TrustZone, comprising a multilayered architecture combining hardware data path, RoT management and operation control with a layer of security firmware. (See WQ Issue 4, 2019, pg26.)

Pebble Tracker sends its data to the IoTeX blockchain-based backend services to orchestrate large-scale, decentralized asset tracking applications. Blockchains are based on the concept of openly verifiable ledgers ensuring that all transactions are publicly confirmed and logged with an uncorruptible digital signature. (Only the transaction is visible, not the private data or content that triggered it.) Because of the use of open ledgers, tampering with blockchain data would quickly be exposed.

IoTeX's blockchain and IoT technology stack, which includes sophisticated middleware to pair with Nordic's hardware, offers SDKs that developers can use alongside one of Nordic's preferred operating systems, the open-sourced Zephyr, to build the trusted applications of tomorrow.

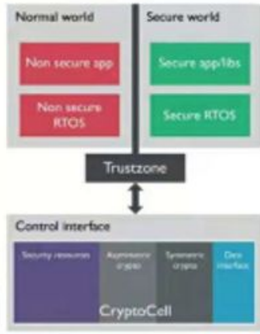
Security and privacy by design

Pebble Tracker makes use of built-in environmental and motion sensors from Bosch and TDK to capture real-time metrics, including GPS location, temperature, humidity, volatile organic compound (VOC) level, light, acceleration and orientation.

The product employs "security and privacy by design" methodology, and equipped with the nRF9160 SiP's powerful security features, it is built to ensure all data the device generates is trustworthy and owned exclusively by the device's owner.

The nRF9160 SiP enables LTE-M and NB-IoT network connectivity and integrated GPS support for precise, long range tracking of asset data. Via this cellular connectivity, Pebble Tracker continuously records real-time data and transmits the digitally signed information to the Cloud or other backend systems including the IoTeX blockchain.

The combination of hardware security and the blockchain ensures protection of all data points produced and brings end-to-end trust to tracking applications. The trusted data can then be used by backend services to fulfill predeployed smart contracts. For example, if a tracker detects an asset is mishandled, the blockchain contract can automatically penalize the company and compensate the customer without human intervention.



The Arm TrustZone technology built into the nRF9160 forms a Trusted Execution Environment. It works together with CryptoCell, an embedded security platform

> The combination of hardware security and the blockchain ensures protection of all data points produced and brings end-to-end trust to tracking applications

Tech Check

Pebble Tracker uses a 750 mAh Li-Po battery, providing up to one week of battery life between recharge for a typical asset tracking application. The nRF9160 SiP has been engineered to minimize power consumption with, for example, support for eDRX and PSM power saving modes

Community-Driven Hardware

CROWD SUPPLY BROWSE LAUNCH ABOUT US Search

Environmental Sensing
Sub-GHz
ARM

Pebble Tracker by IoTeX

A secure, battery-operated, blockchain-ready, cellular-IoT prototyping platform based on the nRF91

$88,355 raised
of $1 goal

Funded! Order Below

10	Mar 25 2021	410
updates	funded on	backers

Last update posted Sep 25, 2021

me@example.com Subscribe to Updates

Recent Updates View all 10 updates.

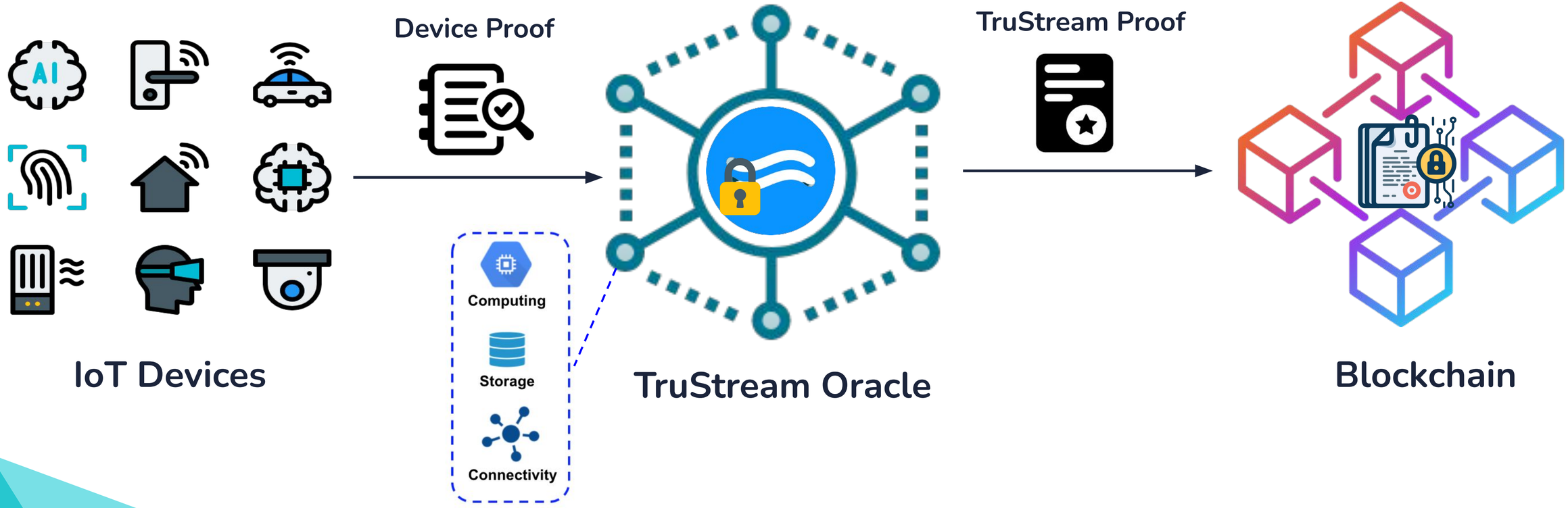
Manufacturing Update #3 Sep 25, 2021
Manufacturing Update #2 Jul 15, 2021

Pebble Tracker $215

Pebble Tracker, along with molded case with OLED display, plastic enclosure, lithium ion battery, LTE antenna, Micro-USB-to-USB-Type-A cable, and a label with your board's IMEI number.

Orders placed now ship Oct 28, 2021.

TruStream: A Decentralized Blockchain Oracle



Internet of Trusted Things (IoTT) Portal

IoTT Portal

Home

Device

Device Status

Apps

My Data

Learn

Home

Welcome to the Internet of Trusted Things (IoTT).

IoTeX is building the Internet of Trusted Things, the first open network where everyday people and businesses can own and control their smart devices, as well as the data and value they generate. Join us!

Connect Wallet

View our Live Network

Xinxin Fan

Head of Cryptography

IoTeX

xinxin@iotex.io

https://www.iotex.io/

LET'S BUILD DECENTRALIZED FUTURE TOGETHER!