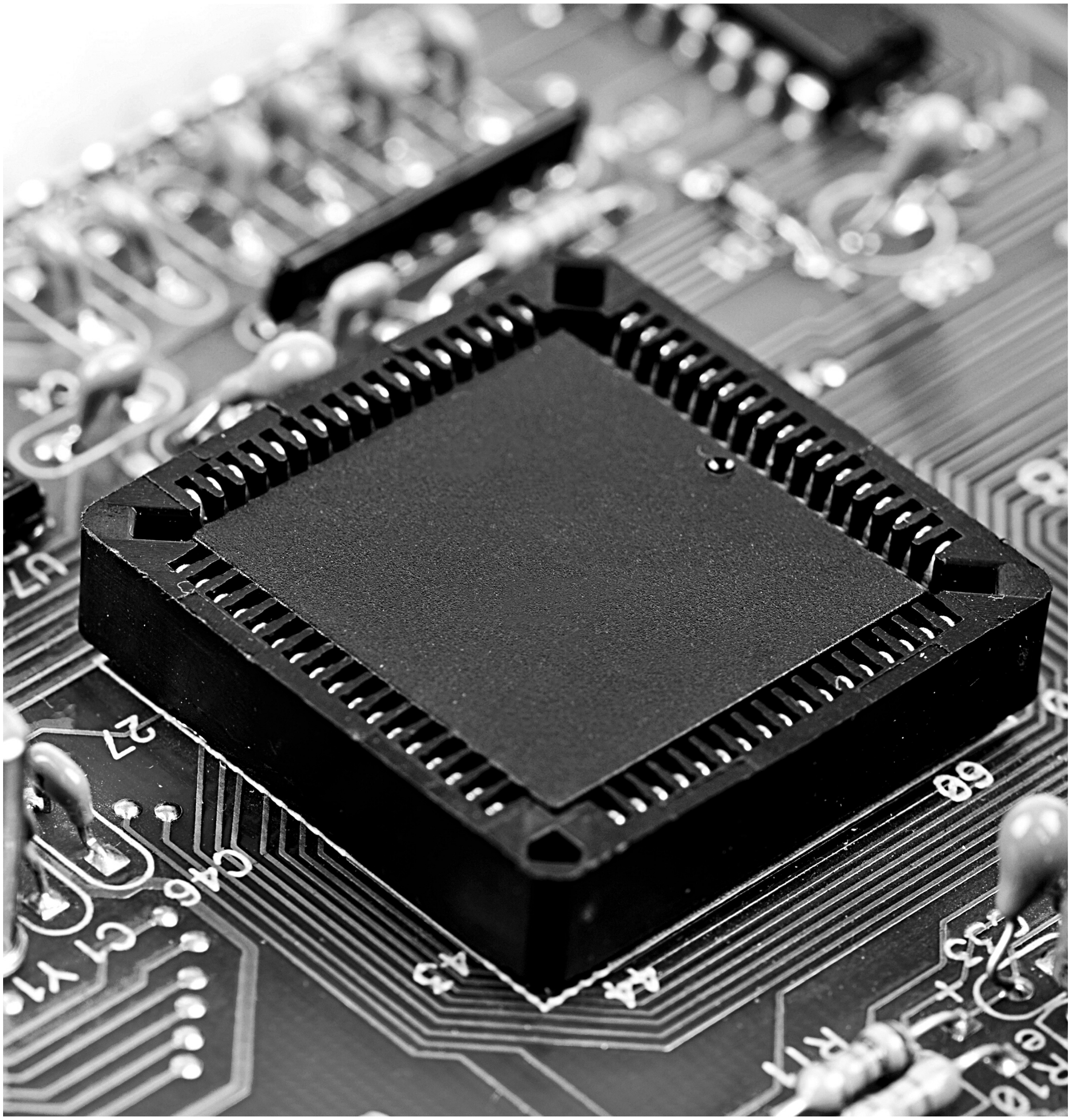
WHITEPAPER

DECEMBER 2021

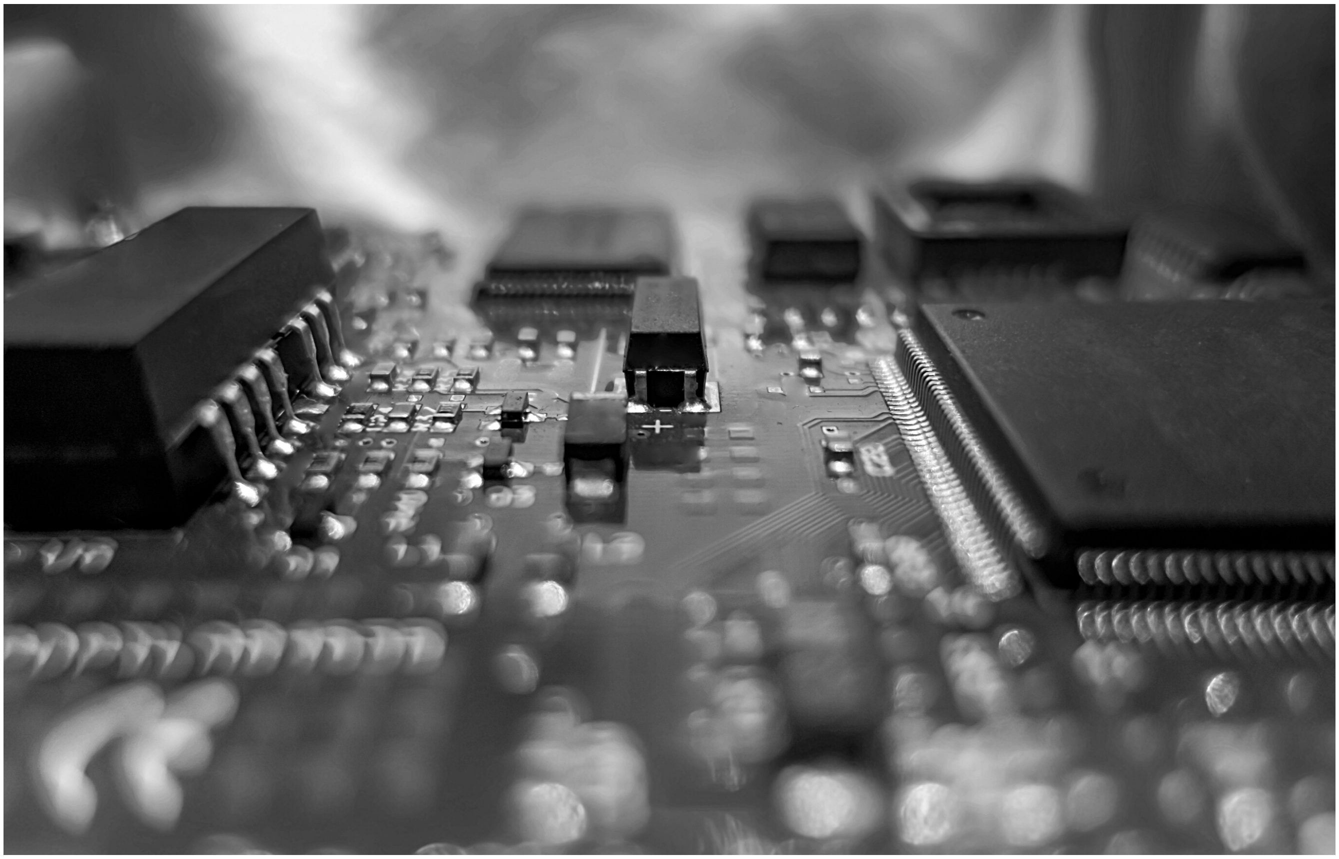
MANAGEMENT OF IP

GLOBAL SEMICONDUCTOR ALLIANCE INTELLECTUAL PROPERTY GROUP



GSA IP

TABLE OF CONTENTS



DEFINITIONS

Device: this term designates the finished product created by a manufacturer. This product is complete and it gets shipped to a consumer, or a services provider or an enterprise that will integrate it into its operations. This product may require some parametrization or configuration work when it gets installed. But when shipping, it is a fully finished entity that does require any new hardware.

IP / Block of IP: this term designates either the hardware or software design of one of the building blocks of the device: It can refer to the underlying design of the CPU, or the GPU, or the SerDes sub-system. It can also refer to the software building blocks such as the Device Drivers, the hypervisor, the operating system.

AUDIENCE

This document is targeting all the actors along the semiconductor and device supply chains. It is also targeting the organizations that will consume these devices, especially within the IoT industry. The document is written for the executives, the product managers and the senior architects of these companies. Its objective is to expose that IoT data reporting and management systems need to be built around end to end architectures that integrate the management of the devices and their various blocks of IP. Secure management of the devices and their sub-elements is a fundamental process to achieve secure and robust operations of the full system.

1. EXECUTIVE SUMMARY

The objective of this document is to present the need for common schemes to manage devices and their sub-elements, bind them dynamically to applications and manage them during their lifecycle.

Multiple initiatives led by industry actors across the value chains and the supply chains are establishing common schemes to identify devices, bind them to cloud applications and manage them. International standards have come together with the support and the active involvement of companies worldwide recognizing the need for cooperation around fundamental concepts such as Identity and security.

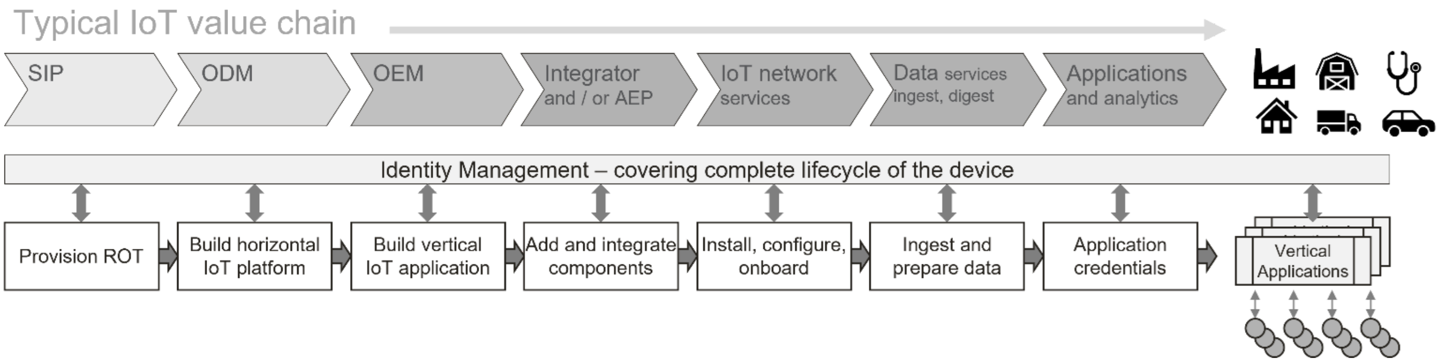
Cloud companies and device vendors see the need to break down walled gardens on functions such as the binding of devices to enable growth across the whole marketplace. Collaboration removes inefficiencies in the supply chains and adds security to the parametrization and authentication of the IoT devices. It enables competition and creates opportunities across markets and supply chains for all participants in the IoT market.

The IP is also the root of the blockchains that track the transactions performed with the device and its blocks of IP. The data generated by the devices and its IP is organized in blockchains across multiple distributed ledgers. These blockchains play a key role in the binding of the data to the device and its IP, all the way to the applications.

Users of the devices and consumers of the services that they generate benefit from the common schemes to manage the IP throughout its life, bind the devices to the applications. By working with standardized management and applications binding schemes, manufacturers of devices and services providers optimize their operations and benefit from higher levels of security.

2. MANAGEMENT OF MULTI-PARTY ASSETS

Rob Brown (Jitsuin)


Typical IoT value chain
SIP
ODM
OEM
Integrator and / or AEP
IoT network services
Data services ingest, digest
Applications and analytics
Identity Management – covering complete lifecycle of the device
Provision ROT
Build horizontal IoT platform
Build vertical IoT application
Add and integrate components
Install, configure, onboard
Ingest and prepare data
Application credentials
Vertical Applications

Multiple parties contribute to a device, from the vendor of the main SoC to the board vendor and the software developers. Each element that makes up the device may have a different owner. Each element will have its own metadata, its own characteristics and in some cases, certification credentials. All these elements need to be tracked as they contribute together to the identity of the device and the data that it generates. The device is a multi-tenant environment that needs to be managed as such.
To survive in today's complex, zero-trust shared data environment, everyone must prove they know who did what when to the assets they rely on.

Connected Things are multi-party assets which are only secure until they are not. Just because you built, bought, or installed a device, does not mean you own all its data or intellectual property but also means some owners of IP contained within it must maintain a lifeline to keep it secure.

We face an avalanche of risk that stems from misplaced trust in the shared data critical to the success of the connected, digital economy. Organizations' inability to discern precisely and quickly exactly who did what when to critical assets threatens to slow progress, hamper growth and leave the door open for malicious actors to wreak havoc. Regulations, legislation and even Presidential Orders will have little impact on the problem without an automated approach to prove provenance, governance, and integrity of assets in a zero-trust world. These are essential foundations for the networked economy.

1.Do you trust your supply chain?
Organizations today, consciously, and unconsciously, rely on data and information about critical assets from a complex network of partners, suppliers, and customers. Data sharing is a business necessity – it is simply impossible to succeed the digital economy without relying on data over which you have little control. From supply-chain documentation to data protection compliance, decisions must be made at every step as to the veracity, completeness and integrity of the information provided. Increasingly complex digital supply chains see software components from hundreds of sources working to process critical data on behalf of organizations. How can they be sure that every line of code, every AI model and every digital supply chain is not only secure and resilient, but doing what it is meant to be doing, at exactly the right time with exactly the right data? How do you trust data that's processed by unknown software running on someone else's computer?

2.Manual cross-check will not scale for Connected Things

The short answer is that you can’t. Today’s connected enterprises are already struggling to acquire, manage and trust the data they need to be confident about the assets they rely upon. First principles of information theory tell us an anomaly is either the most useful data packet you’ll ever receive from a connected thing or an attacker subverting your system. Now choose which it is!

Increasingly adopting a zero-trust approach is regarded as best practice. This means that every piece of information about an asset is checked – nothing is taken for granted or accepted at face value.

Zero-trust processes means continuously cross-checking who did what when to every asset. It is essential to minimize risk and create resilient and robust operations. But with ever increasing complexity and volumes of shared data it is clearly beyond management with spreadsheets.

3.Automation: solution and problem

Manual, paper-based processes are too slow, too labor intensive and too prone to human error or manipulation to meet the demands of flexible, agile, and secure enterprises. Automation and digitalization of these data flows creates efficiency and reduces costs. But without similar automation and continuous assurance of data, they also increase the efficiency and speed at which incorrect, or malicious data can propagate and cause significant harm. Gartner predicts that by 2023 businesses that promote data sharing will outperform their rivals across the board. But at the same time less than five percent of data sharing programs will correctly locate and identify trusted data and data sources.

4.Unsustainable risk

These trends are accelerating the introduction of unsustainable risk into the very fabric of the connected digital economy and are already fueling more than $75 billion cost of audits, manual compliance, and ransomware. Cybercrime alone is expected to cost the global economy $10 trillion by 2025 – and that does not include the trillions of unseen costs caused by bad decisions, litigation and even loss of life resulting from misplaced trust in bad data. Failing to notice, or act upon the smallest anomaly could be catastrophic – acting with blind trust in unverified data could be even worse!

5. Regulation alone will not help

Regulators, legislators, and market forces are already reacting to this threat and are demanding action. The US Presidential Executive Order on Improving the Nation’s cybersecurity is just one example. The Software Bill of-Materials (SBOM) it demands will enforce catalogues of exactly what’s in the software that federal offices use. The use of SBOMs will become more prevalent and a standard item in the Terms and Conditions of purchase agreements and contracts. In other sectors the concept of auditable, trustable AI is gaining traction, and yet others are looking to automate robust and immutable ledgers of exactly who and what has accessed critical assets.

But software cannot work without hardware. The security capability of hardware matters when it comes to processing secrets that protect data which each party relies upon. How those secrets end up in connected devices matters too. A full Digital Bill of Materials would attest to a device’s ability to defend itself detailing secure enclaves to protect keys, secure boot mechanisms, operating system integrity, application update capabilities, in fact everything needed to work out whether the data you receive can be trusted or whether a device has securely injected poisoned data into your enterprise.

But currently, there are no effective solutions and no commonly agreed methods for sharing data about trusted assets. Each organization, and each application has a bespoke solution operating in silos that do not support sharing of assurance information. It’s a hard problem that most development teams across the industry would struggle to divert resources toward solving. Consequently, most organizations remain unaware of the variety, scope and scale of vulnerabilities lurking in their data assets.

6. Continuous assurance as a service

A common approach to continuous assurance of critical assets is needed. It should allow any parties to define for themselves the data they want and need to trust but establish the principles and routines through which that data is audited, checked, and assured. To be effective it must be able to establish and share the provenance and integrity of data relating to any asset. It must also allow for precise governance over who can see what about that asset balancing transparency, privacy, and security to promote the agility required by multistakeholder connected organizations.

The first step is the critical sharing, provenance, and integrity of SBOMs. Having an SBOM solves nothing unless it can be dynamically shared. Ensuring the right people see the right information at the right time is essential for SBOMs to work as intended and reduce risk in cyber supply chains. Continuous assurance is necessary to match the ever-changing nature of software and its application in any organization.

7. Provenance, Governance, Integrity

Three fundamental factors are key to each of these diverse applications, and to any other circumstance where continuous assurance of assets is required. Whatever the asset, and whatever the data required about it, it must be possible to determine its provenance, apply precise governance and attest its integrity.

8. Capturing life history

Understanding the lineage and pedigree of any asset is the first step in assurance. Provenance establishes not only where an asset came from but creates a sharable history of the asset, who owns, and maintains it and the data about it. It is vital that as well as the origin of the asset every change is recorded as it passes along complex, extended supply chains. Capturing and sharing this ‘life-history’ of every event that impacts the asset from cradle to grave delivers the provenance required to assure it is what it purports to be.

9. Intelligent sharing

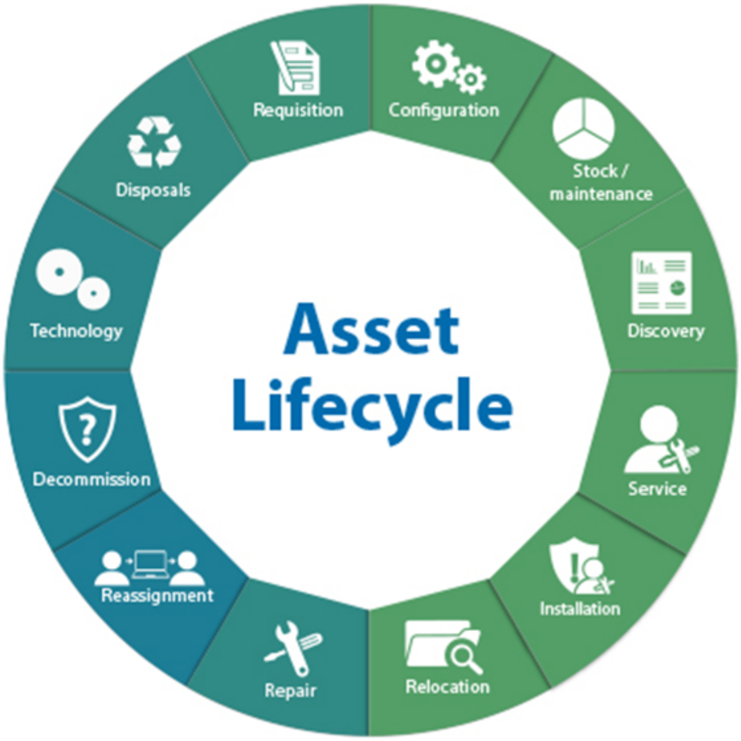
But commercial, security and privacy concerns mean that not all information can, or should, be shared with everyone all the time. Governance provides the fine control over exactly who sees what when. Every organization and every asset will have different parameters over what should be shared and what must remain confidential. Responsible disclosure should allow reasonable timeframes to propagate fixes. Different suppliers and consumers will need to see different information. Privacy, security, and transparency can coexist, and it is important that continuous assurance allows them to do so. Organizations must be empowered to set and enforce the right access policies to protect themselves and their supply chains.

10. Proving Integrity

To rely on continuous assurance all parties must be confident of the integrity of the data they are sharing and consuming. They must know, without doubt, that there is a tamper-proof, golden thread of evidence that connects every element. Blockchain technology could ensure that every event detailing every interaction and every change is immutably recorded. This guarantee would boost assurance at every stage and underpin confidence in every asset with every party, supporting the work of governance, risk, and compliance teams. Developers need to integrate and continuously assure the data they use for critical business decisions. Whether through publishing and subscribing to SBOMs or DBOMs, recording multi-party events that impact assets in complex supply chains, or providing legally robust auditability of machine-learning decisions, it is their responsibility to create assurance around the assets the business needs. Every organization seeking transformation with shared data must publish and consume it with continuous assurance. A digital archivist would do just that.

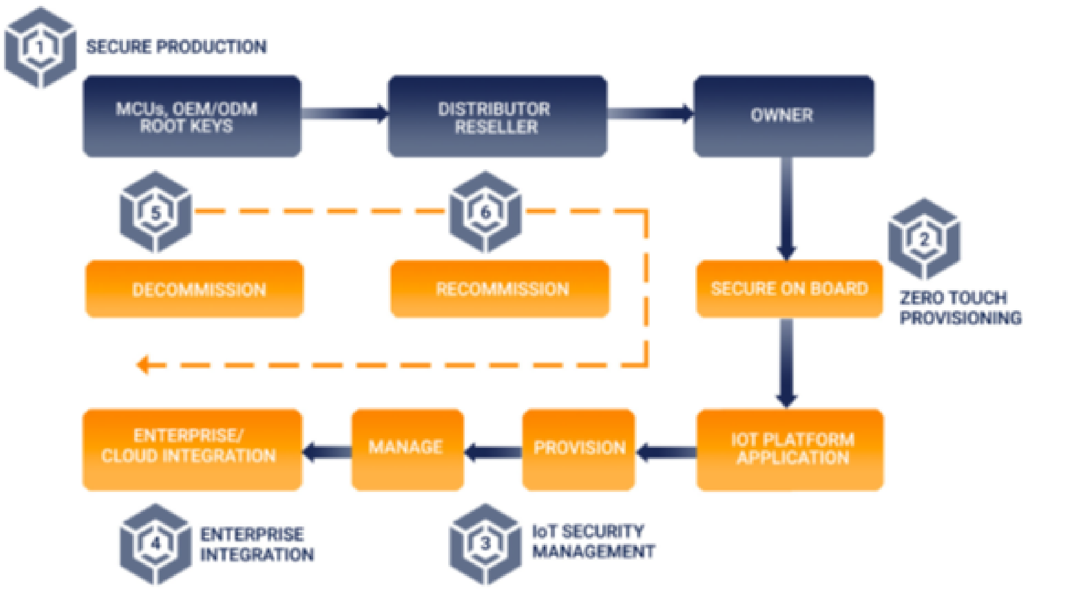
3. LIFE CYCLE MANAGEMENT OF THE DEVICE AND ITS IDENTITY

Rob Dobson (Device Authority)



As devices migrate from the factory to their operational environment, they get code updates, the keys that authenticate them get refreshed. These functions play a fundamental role in the operations of the device and its security. An up-to-date device with the with the right time stamp on its code is much more trustworthy than when it runs with obsolete and possibly compromised software and keys.

A Root of Trust (RoT) is a fundamental component in a devices lifecycle, typically provisioned in the MCUs/processors/systems. Without this strong foundation of trust a device is not trustworthy throughout its lifecycle. The lifecycle of a device encompasses many steps and is an important aspect for any device deployment. Enterprise IoT security solutions need to implement Security Lifecycle Management to meet the needs of the use cases they are fulfilling. A typical device journey requires Trust and Automation during its lifecycle across six key fundamental steps, these being:



1. Secure Production

Provision initial identities, Root Keys and Certificates at the Time of Manufacturing to provide a strong RoT.

- The root key along with other device parameters like serial number can act as registration information (whitelisting).
- Registration keys should be rotated with a new key at the time of onboarding the device.
- Secure mastering, production and foundation for secure updates need to be included in this step.

2. Secure Onboarding - Zero Touch Provisioning.

Today's manual processes do not work well for IoT devices, scale, and security. This step is required to transfer the device ownership and connect to an owner-controlled environment without human intervention.

3. Security Management

Provision and Manage Owner-Controlled Security for devices: This functionality is delivered by device identity centric IAM platforms.

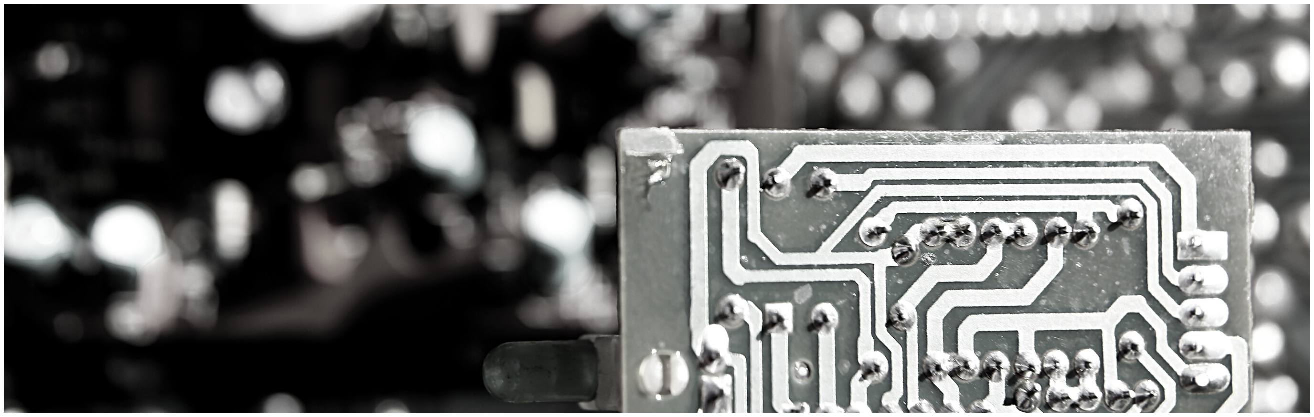
- Provision and manage owner/application required keys and/or credentials.
- Provision and manage application required identity/authentication.
- Policy-based automation for identity, authentication, and data security keys.

4. Enterprise Integration

Most Enterprise IoT security implementations need to take existing IT security controls into account and seamlessly interoperate with IoT devices. The challenge is integrating IAM for Devices, typically know as IoT IAM, with the traditional Enterprise IAM, Hardware Security Modules (HSMs), and Data Security Platforms.

- Enterprises use HSMs for Root of Trust, secure storage of keys, and secure crypto operations. HSMs are used for identity provisioning and data security operations.
- Enterprises already use data security platforms for key management and policy-based data access authorization. Integration with these systems is essential for end-to-end data security and compliance.

IoT IAM and Enterprise traditional IAM need to interoperate to authorize and share data between the devices, Enterprise systems, and users.

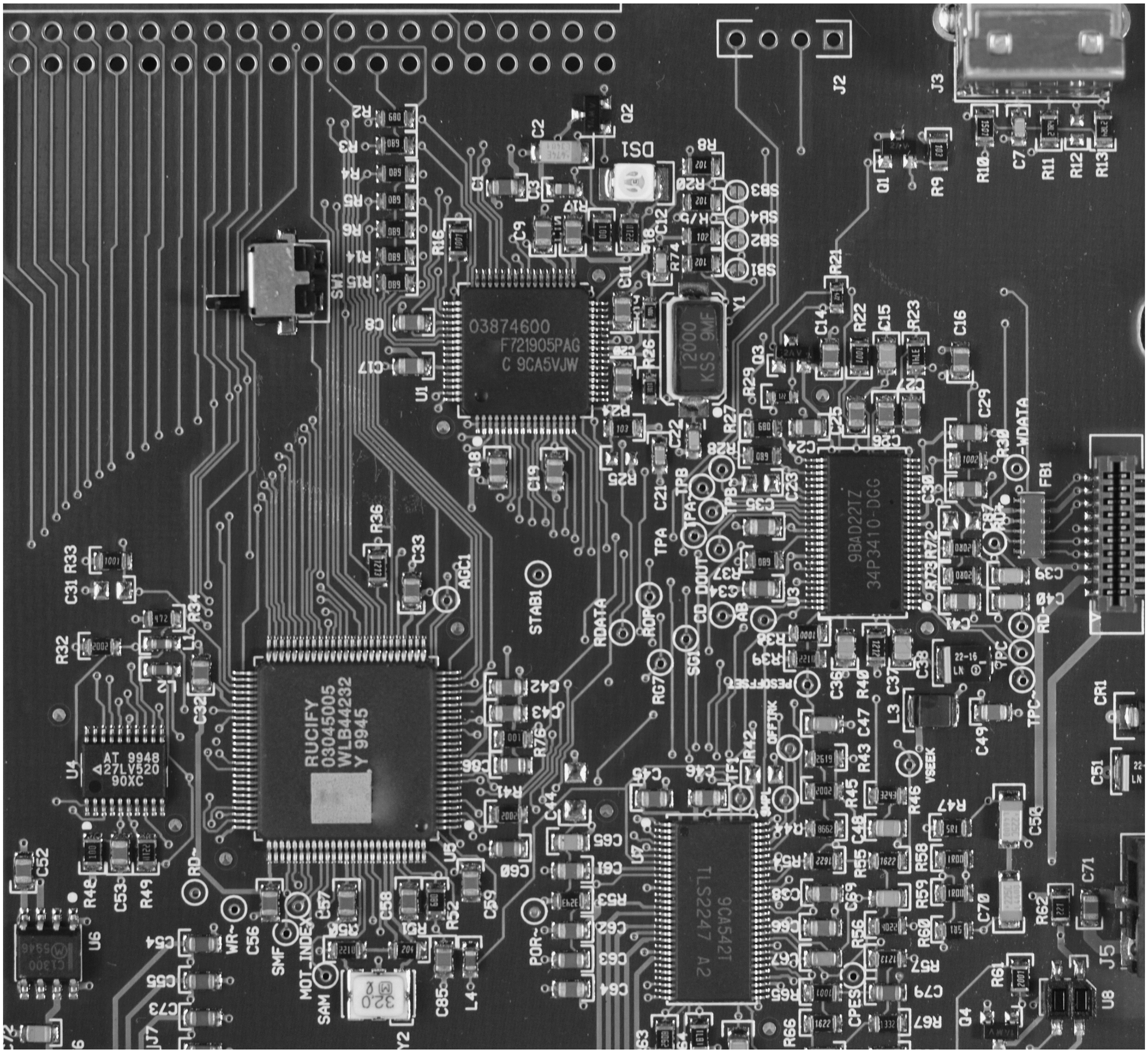


5. Device Decommission

The lifecycle of a device refers to the operational phases of a thing in the context of a given application or use case. The phases mentioned above assume a new device is going into operation. For devices with a lifespan of several years, occasional maintenance cycles may be required. During each maintenance phase, the software and operational data may be upgraded. Depending on the operational changes to the device, it may be repurposed at the end of the maintenance cycle. However, the end-of life of a device doesn't necessarily mean that it is defective, but rather decommissioned with the existing service and current owner. It can be moved to a new owner and start the device lifecycle from the beginning. During the decommissioning of the device, the security management must remove all sensitive data and proprietary applications and revert the device to a factory-fresh state.

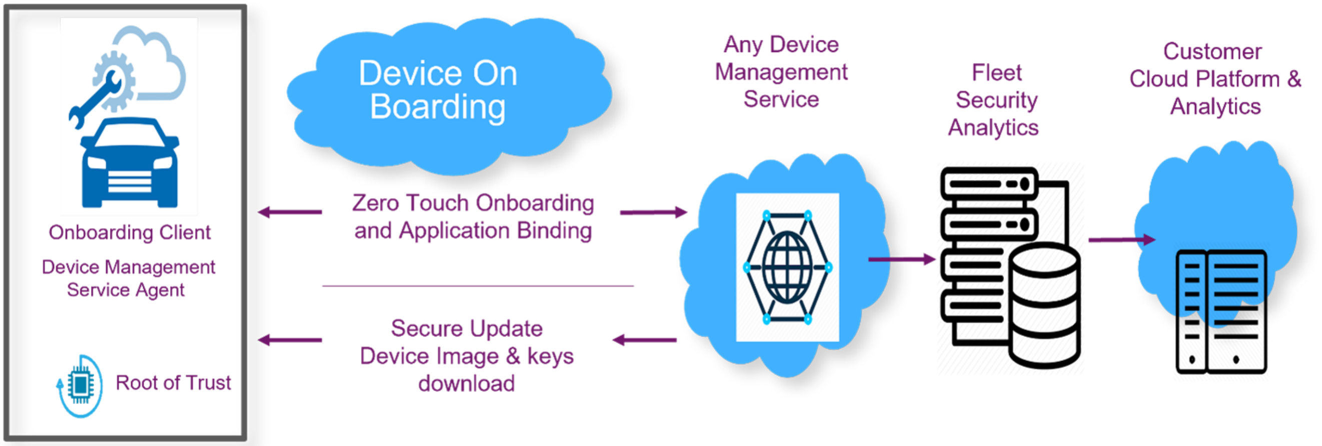
6. Device Recommission

The device recommission can follow the same steps from step 2, provided the old trust anchor is preserved. If not, a new Root of Trust and additional keys required are established/programmed.



4. BINDING OF DEVICE AND ITS IDENTITY TO APPLICATIONS

Geoffrey Cooper (Intel), Rob Dobson (Device Authority)


Onboarding Client
Device Management Service Agent
Root of Trust
Device On Boarding
Zero Touch Onboarding and Application Binding
Secure Update Device Image & keys download
Any Device Management Service
Fleet Security Analytics
Customer Cloud Platform & Analytics

A trustworthy mechanism to bind the devices to their applications is a fundamental aspect of delivering trusted data to analytics systems. The FIDO Alliance is designing these protocols with the objective of standardizing across the IoT marketplace the usage of a common identity format and binding processes.

To benefit from the investment in the end-to-end supply chain, we need a mechanism to attest the provenance information about device sub-components from the board-level manufacturer to the controlling entity that will use the device – the device “owner”. Previously, this has been accomplished by a manual installation of the device into a target network environment. During this installation, the human installer can transfer attestation information. However, this focuses the required trust into the human installer, who might be a lower-paid facility worker or even a subcontractor working for another organization. A human may make a mistake during the manual installation process of the device.

We can disconnect the human factor from this trust chain by automating the device’ installation, where the “owner” of the device is a machine entity, such as a network-based server. If the device can authenticate the prospective machine owner, and vice versa, a device-to-owner trusted connection can be established. Then the provenance information which has been embedded in the device may be transmitted to the owner. Automated installation is both faster and less error prone than manual installation, and these benefits will also give advantage to the solutions provider.

Fortunately, FIDO Device Onboard (FDO), a new protocol from the FIDO Alliance, permits just this trust relationship to be established, even if the target installation environment is not known at the time of board level device manufacture. FDO uses a device attestation which may be based on the device Root of Trust (as mentioned above), to identity and authenticate the device to the prospective machine owner. In essence, FDO uses attestation to transition the trust of the board level manufacturer into the trust between the device and its machine “owner,” without needing a manual login step.

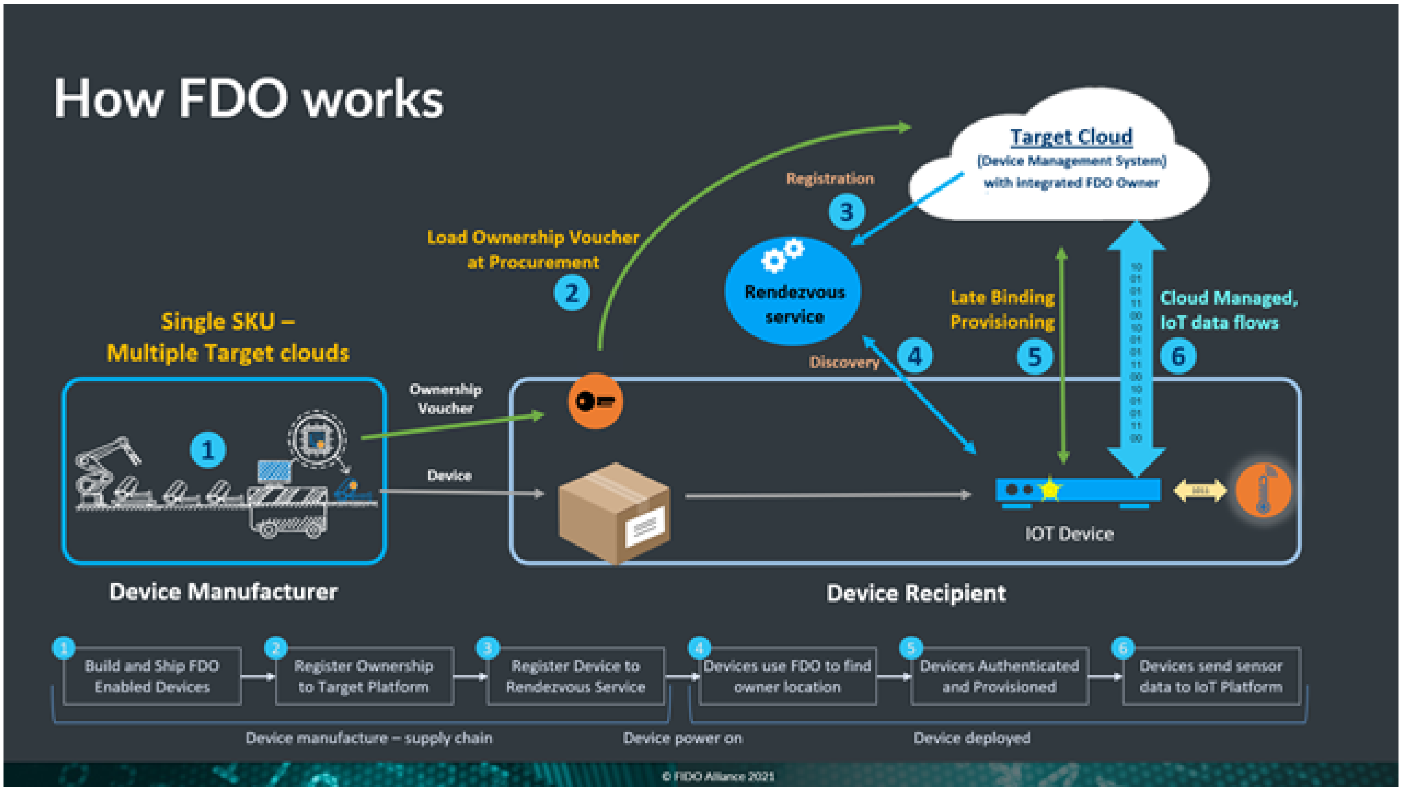
The authentication is two-way. The machine owner identifies itself to the device using a cryptographic attestation over the “ownership voucher,” which is a new attestation object created at completion of board level manufacture. The ownership voucher is extended in the board level supply chain to contain a cryptographic record of the device’ progress. The machine owner attests to being the last entry in the chain of ownership, as the device attests to its RoT.

Once attestation is complete, FDO creates an attested, encrypted channel, and permits the machine owner and the device to exchange information. For automatic device onboarding, this involves downloading software, data, keys, and tokens into the device, so that the device can enter directly into a target application using local certificates and other cryptographic mechanisms. However, the device may also share and attest other information that is stored on it. Specifically, the device can share attestation information about its constituent components, acting as a secure conduit between the component device supply chain and the board-level supply chain.

Imagine that a board level manufacturer assembles components from multiple suppliers, along with attested provenance information about these components. Then the board level manufacturer may embed this information into the newly assembled device, signed by the device' Root of Trust (RoT). Since the RoT is built into the hardware of the device, the signature guarantees that any change to this data is detectable, even after the board-level device is transported through its own supply chain. Since FDO uses this same RoT attestation, the FDO "owner" is also able determine the validity of this data, once the device transmits it to the "owner" over the encrypted channel. Essentially, the RoT embedded in the board level device vouches for the device (automatic) installation and the device' provenance data at the same time.

To make this data more tamper-resistant, an integrated secure element (iSE) may encapsulate or protect the FDO credentials along with the signature for the board-level provenance information.

After FDO transitions the trust of the device into a new machine owner, its credentials are re-issued, so that only the new owner can use FDO. Then FDO goes dormant unless/until the device needs to be repurposed.

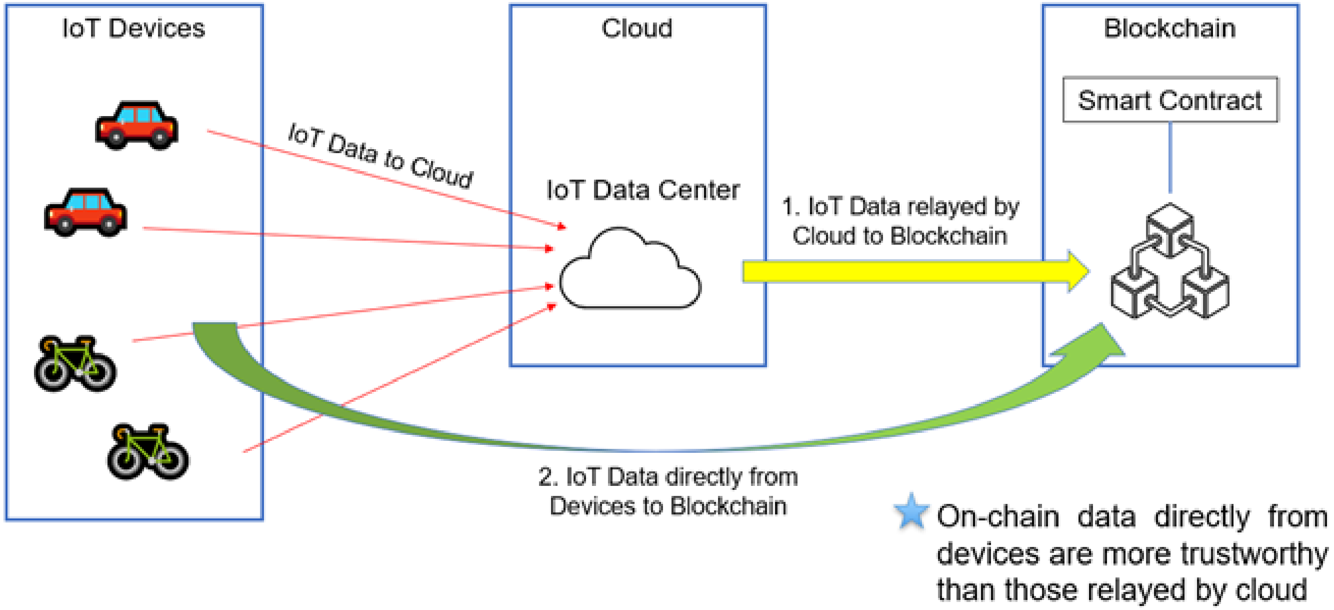

How FDO works
Target Cloud
(Device Management System)
with Integrated FDO Owner
Registration
3
Load Ownership Voucher
at Procurement
2
Rendezvous
service
Late Binding
Provisioning
Cloud Managed,
IoT data flows
Single SKU –
Multiple Target clouds
Discovery
4
5
6
Ownership
Voucher
1
Device
IOT Device
Device Manufacturer
Device Recipient
1 Build and Ship FDO Enabled Devices
2 Register Ownership to Target Platform
3 Register Device to Rendezvous Service
4 Devices use FDO to find owner location
5 Devices Authenticated and Provisioned
6 Devices send sensor data to IoT Platform
Device manufacture – supply chain
Device power on
Device deployed
© FIDO Alliance 2021

5. BLOCKCHAINS

Gary Xu (Aitos.io)

Data in the new age of the digital world is like the oil in the past century. IoT devices generate or collect massive data to feed the industry and thus it's essential that these IoT data are trustworthy and traceable. Distributed ledger, aka blockchain is one of the zero-trust architectures to transfer the trust among all relying parties. Based on the blockchain consensus algorithm, all the participating parties collaborate in a decentralized way to ensure the integrity, consistency, and tamper-resistance of the ledger. Furthermore, there are typically some smart contracts, which are pieces of code, deployed on the blockchain. Smart contracts accept invocation from either a terminal or another contract and process the parameters passed through the invocation.

For example, an electric vehicle's on-board monitor device calls a monitor smart contract with the speed, steering wheel angle, brake status and battery/charging status as the parameters. The smart contract may monitor if the vehicle is over speeding, in addition to storing these parameters on the blockchain. In case some accident should occur, these on-chain data could help find out what problem takes place. If the vehicle is driven over the speed limit, the monitor smart contract may trigger an event to a risk assessment smart contract deployed by the insurance company. If the vehicle is in charging, the power consumption can be uploaded to a charging service smart contract which could create a bill.


IoT Devices
Cloud
Blockchain
Smart Contract
IoT Data to Cloud
IoT Data Center
1. IoT Data relayed by Cloud to Blockchain
2. IoT Data directly from Devices to Blockchain
★ On-chain data directly from devices are more trustworthy than those relayed by cloud

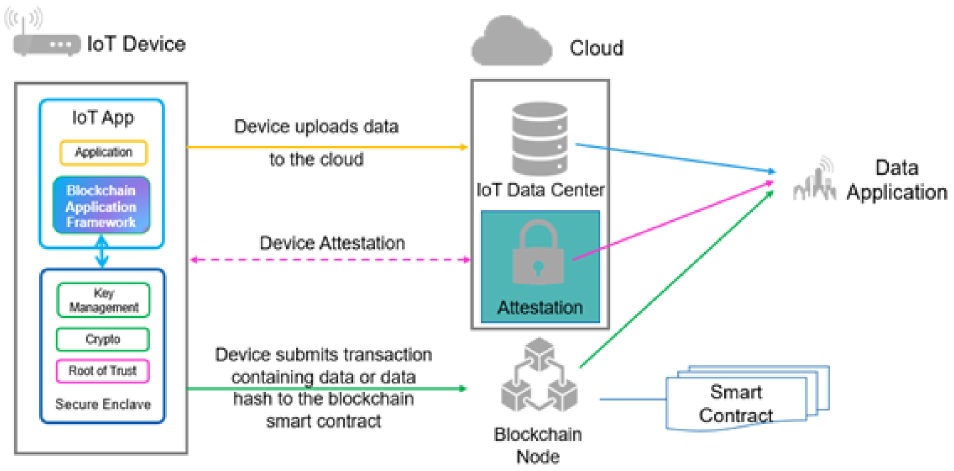
In this example, the on-board monitor device has 2 paths to report status data to the blockchain smart contract. The first one is a Blockchain + IoT Data Center mode, i.e., the device reports data to the IoT Data Center and the IoT Data Center relays them to the blockchain. The second one is a Blockchain + IoT Device mode, i.e., the device directly accesses the blockchain services. In brown field where the IoT infrastructure is already deployed, the Blockchain + IoT Data Center mode allows the blockchain to benefit the scenario without any retrofit on the IoT devices. It's easier but there is a probability that the IoT Data Center may fabricate fake IoT data or tamper with the reported device data. On the contrary, the Blockchain + IoT Device mode provides more trustworthy on-chain data by removing the IoT Data Center from the path.

The identity and the security are 2 essential aspects a blockchain-capable device should concern. The on-chain identity is basically a derivation of a device-specific public-private key pair. For example, Ethereum adopts a key pair of Elliptic Curve Digital Signature Algorithm (ECDSA) with the secp256k1 curve and defines the low 20 bytes of keccak256(PubKey) as the account address representing the device asset, where keccak256 is a non-standard variant of SHA3 hash algorithm. ECDSA curve secp256r1 (NIST-P256), ed25519 and Chinese SM2 are also examples of the signature algorithm used by other blockchains. An IoT device can sign a transaction datagram containing the IoT data and send the signed transaction to a smart contract on the blockchain to permanently store the data for asset tracking or trigger some on-chain execution.

Security is imperative for device identification and data trustworthiness. The device's blockchain key pair is usually generated inside the device and endorsed by the existing RoT (Root of Trust) mechanism. It might also be the RoT itself, which is injected from the production line in a safe environment in manufacture cycle. Whatever the way the blockchain key pair is generated, the private key and the cryptographic computation must be protected securely in a secure enclave such as TEE/SE, in addition to secure boot, remote attestation and other security mechanisms.

Unlike server, desktop computer or mobile phone, IoT devices are so fragmental that no single blockchain solution could fit all IoT devices. It's necessary to define some profiles or design guidelines for IoT devices to support blockchain capability. For example, for small-footprint IoT device profile, aitos.io's BoAT (Blockchain of AI Things) Blockchain Application Framework introduces a C language multi-chain client SDK allowing the devices to invoke smart contract. BoAT also utilizes the security features (TEE, SE, or even special SIM card, etc., if applicable) to securely generate the key pair and protect the sensitive information (private key) during algorithm computation.

There are 2 usual ways for IoT devices to make use of the blockchain. A device could play a role of blockchain oracle and send data (e.g., temperature, humidity) to a blockchain smart contract that either stores the data or executes some logic regarding the data content. Another way is, in addition to uploading the data to the cloud as usual, the device can also calculate the hash of the uploaded data, sign the transaction datagram containing the hash and send the transaction to a smart contract. The hash saved on blockchain could later be used by the 3rd party to verify the data in cloud.



Both ways come with trust transfer, because the blockchain ensures the data integrity since they are stored on blockchain, and the RoT-endorsed key pair identifies the data provenance. So, the device RoT, secure enclave, key pair and blockchain protect the data trustworthiness in their lifecycle, which track the device data assets in an on-chain digital lifecycle history.

AUTHORS (IN ALPHABETICAL ORDER):

IMEN BAILI | MENTA

ROB BROWN | JITSUIN

MARC CANEL | IMAGINATION

GEOFFREY COOPER | INTEL

ROB DOBSON | DEVICE AUTHORITY

SYLVAIN GUILLEY | SECURE-IC

MARC LE GUYADER | CRYPTO QUANTIQUE

TEDDY KYUNG LEE | ICTK HOLDINGS

VINCENT VAN DER LEEST | INTRINSIC ID

GARY XU | AITOS.IO