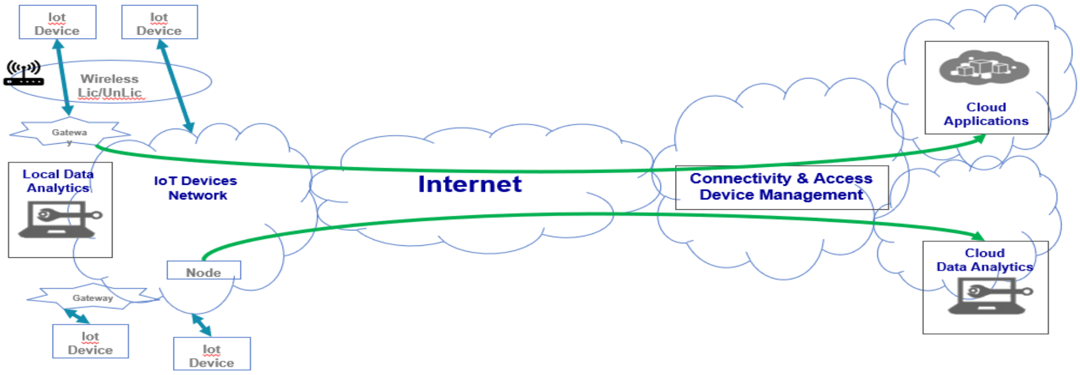
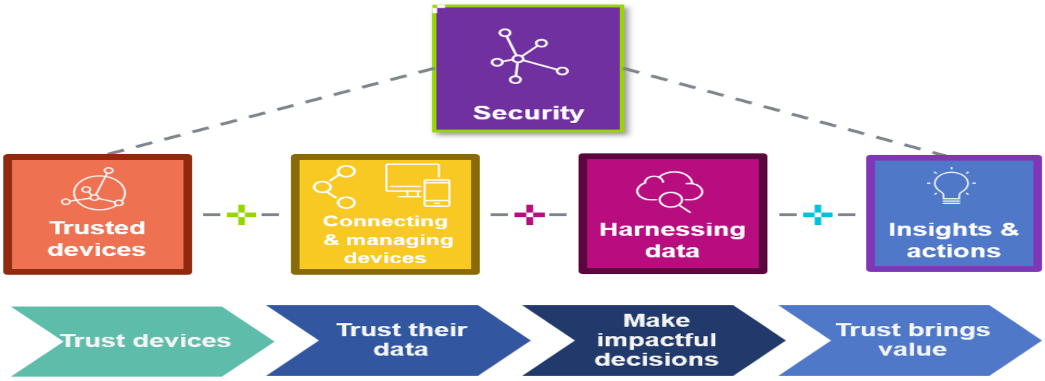
Identity in IoT

By Marc Canel, Vice President of Strategy - Security, Imagination Technologies

The world of the Internet of Things (IoT) is characterized by a very large number of devices extracting data from their operational environment and reporting information to analytics systems in their network or in the cloud. These devices reside beyond the edge of the network. Sometimes they have communications capabilities, in other cases they report their data through an edge node that passes the data to the analytics systems. The data created is information about the environment (e.g. temperature, speed). It can also be metadata that describes the operations of the devices or the system.



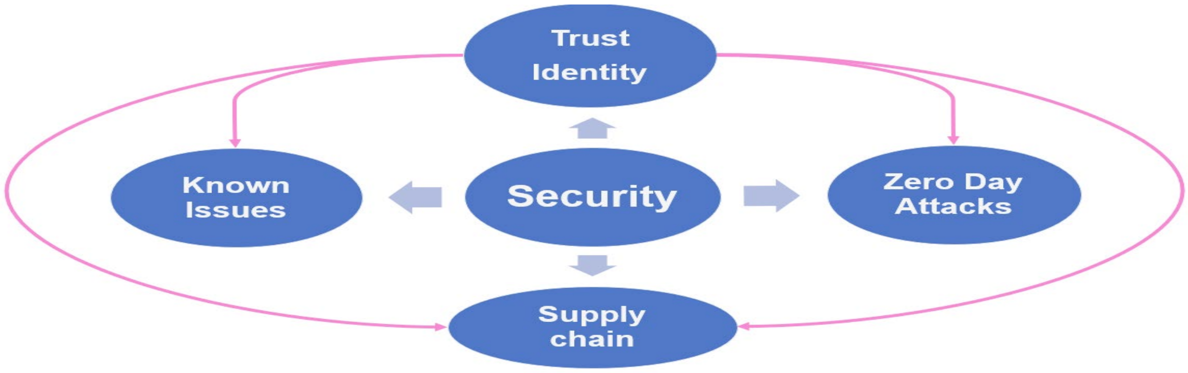
The analytics applications handle large volumes of data. They make decisions based upon this data that will impact the safety of the system and its users. The financial considerations behind the decisions may be considerable. The data plays a key role and it is fundamental that it is trusted. If the data cannot be relied upon, it is not worth much. Expensive and complex systems making decisions on safety or operations need to trust the data that they process. Trust in the data brings value to all the systems. Effective reliance on the data from the IoT devices is built upon a security architecture that will start with the devices. Trusted devices enable trusted data.



Security, Identity and services providers

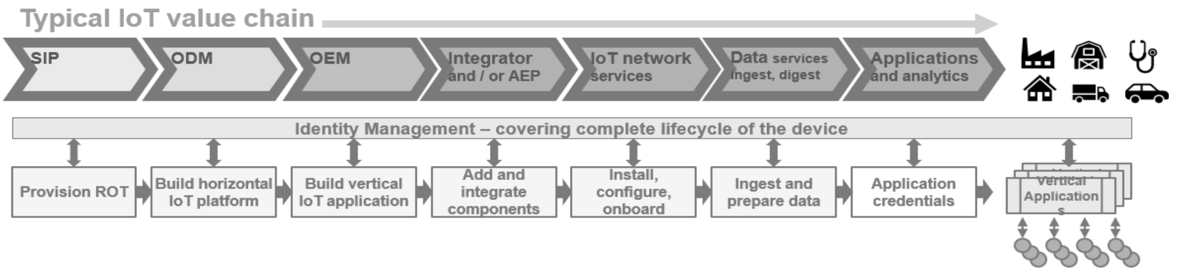
Successful services that handle high value materials are based on robust security models. They balance the cost of security and the needs of the services, its users and the data that they handle. Identity is almost always a target of attacks. It is either the identity of a user, or an application, or a device. Theft of identity is not limited to consumers. It affects multiple aspects of the IoT systems.

Identity is a fundamental building block of security. It is a complex concept that gets implemented in multiple dimensions. It is the mean by which trust gets established between actors in the ecosystem. It drives security in supply chains and in the operations of products.



Building the identity of a device

The identity of an IoT device is the aggregate information of all the sub-elements that make up this device. A device has multiple building blocks: some of them are physical, others are logical. Building blocks are nested within other ones: the board is made up of the main applications processor and other processors such as DSPS, GPUs and NNAs. The board has an identity and so do the individual applications processors. The software includes device drivers, a hypervisor, virtual machines in which run operating systems and applications run: each one of these elements has an identity.


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 Application s

- Identity is a cumulative ledger - based on all the functional blocks in the device
- Distributed - Involves all the actors along the supply chain until end of life

Each element in the device, either physical or logical, has attributes. It may have been certified; it may have dependencies upon other elements. It may include data that represents a standardized identity such as an IP address, a MAC Address. In some cases, the element is a very secure container such as a SIM, or an eSIM that will represent an identity with the cellular operator and certain rights to the regulated airwaves.

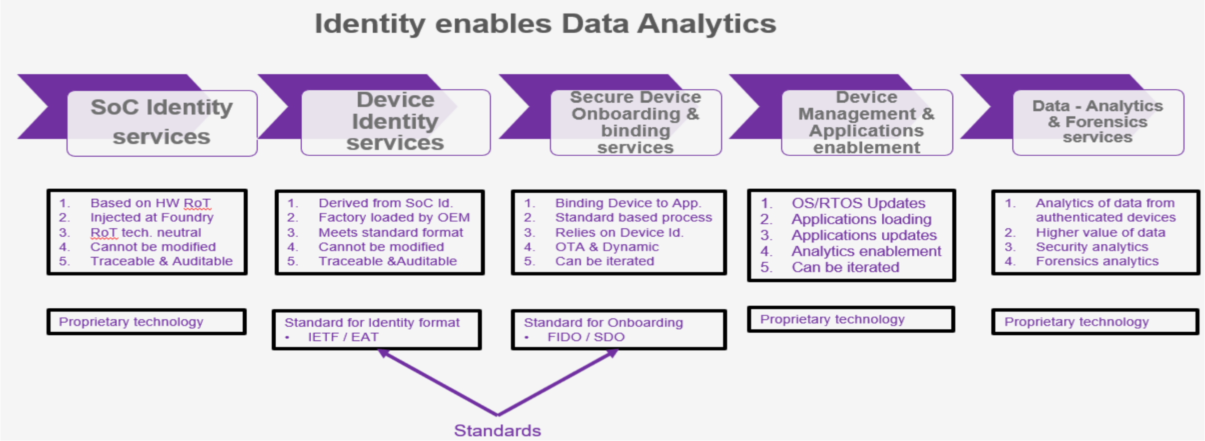
Identity of these elements can change over time. IP Addresses and eSIM information can vary depending upon the service provider that owns the resource that is accessed from the device. The device will update its software, new capabilities and application get installed: they are rolled out within the framework of new hardware or software functions whit their own provisioning materials and credentials. These new elements bring identity materials with attributes and they contribute to the overall identity of the device.

The device is a network of elements, some of them are nested within each other. Each element brings its own credentials to participate in the overall definition of the device's identity. Each element may have a different 3rd party that can validate its identity and attributes. Authentication of devices and their elements is a key function of Identity. Claims based applications need to have an identity to authenticate themselves with secure applications and they will need a 3rd party to authenticate their claims. The device becomes a complex system of elements relying on 3rd parties for authentication.

The leading challenge of Identity is its fragmentation. There are several standards-based identity schemes (e.g. MAC address (IEEE), IP address (IETF), Cellular SIM (GSMA), TCG/TPM). There are also de facto industry standards such as Android where one company can impose the architecture of the identity on an ecosystem. However, when it comes to applications, virtual machines, various hardware elements, there are no standards and the fragmentation of markets makes it challenging to define consistent schemes.

Identity in the supply chain

Without Identity, trust cannot be established between systems. Tracking the identity of hardware and software parts on a board enables the customer to understand its source. Identity when it is injected at the foundry of the part enables traceability in the supply chain and security during operations. A device where all the parts are identified in a consistent scheme and are traceable in the supply chain can be trusted.



Identity enables Data Analytics

SoC Identity services

1. Based on HW RoT
2. Injected at Foundry
3. RoT tech. neutral
4. Cannot be modified
5. Traceable & Auditable

Proprietary technology

Device Identity services

1. Derived from SoC Id.
2. Factory loaded by OEM
3. Meets standard format
4. Cannot be modified
5. Traceable &Auditable

Standard for Identity format
- IETF / EAT

Secure Device Onboarding & binding services

1. Binding Device to App.
2. Standard based process
3. Relies on Device Id.
4. OTA & Dynamic
5. Can be iterated

Standard for Onboarding
- FIDO / SDO

Device Management & Applications enablement

1. OS/RTOS Updates
2. Applications loading
3. Applications updates
4. Analytics enablement
5. Can be iterated

Proprietary technology

Data - Analytics & Forensics services

1. Analytics of data from authenticated devices
2. Higher value of data
3. Security analytics
4. Forensics analytics

Proprietary technology

Standards

Remote device attestation is a fundamental service that allows a device such as an IoT device, or other endpoint to prove itself to a relying party, a server or a service. This allows the relying party to know characteristics of the device and judge its trustworthiness. This concept applies to sub-elements of the device.

Remote attestation underlies other protocols and services that need to know about the trustworthiness of the device. One example is biometric authentication where the matching is done on the device. The relying party needs to know that the device can perform secure and correct matching. Another example is content protection where the relying party wants to know that the device will protect the data. Enterprises need to know that a device is trustworthy before allowing it to access corporate data.

The notion of attestation includes:

- Proof of the make and model of the device hardware (HW)
- Proof of the make and model of the processor, particularly for security-oriented chipsets
- Measurement of the software (SW) running on the device
- Configuration and state of the device
- Environmental characteristics of the device such as its GPS location

To achieve this objective of consistent identity across the IoT marketplace, the industry defined the concept of Entity Attestation Token (EAT) which is being standardized within the Internet Engineering Task Force (IETF).

Standardization of the Identity format

Cooperation is the key to solving this problem. Very few industry actors can successfully impose their own identity norms on an industry. Participation in standards body is the key to success. Through cooperation and transparency, it is possible to define schemes that are validated, fit within global standards and meet security objectives.

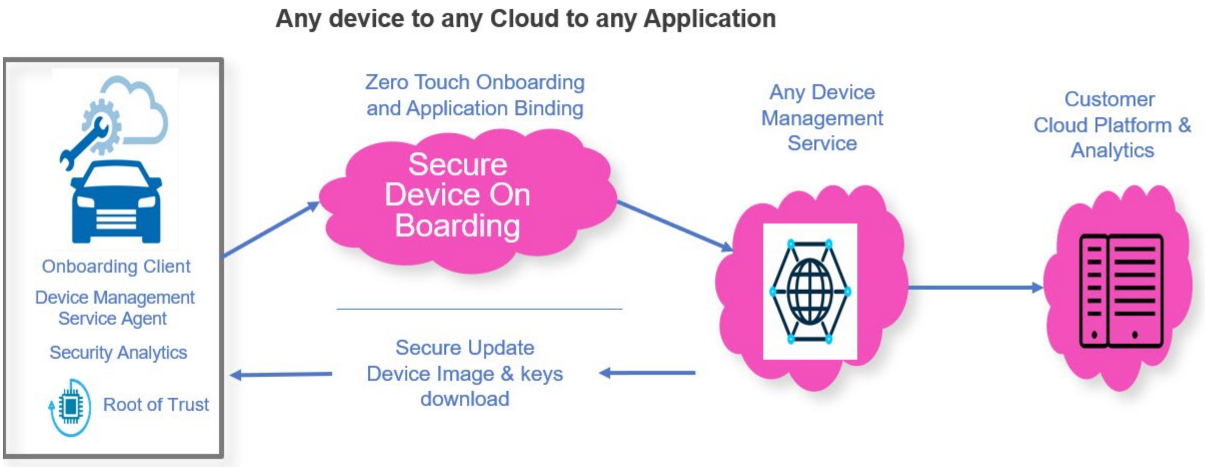
The concept of Entity Attestation Tokens is based on CBOR tokens which are themselves standardized with the IETF with RFC 77049. Multiple data types can be supported. The format is compact enough that it can be implemented in small IoT devices. The attestation materials can be defined as claims. The EAT at the level of the device can be composed of sub-module EATs for sub-entities within the device. Each entity that can create an EAT can do so by the means of its dedicated root of trust. The attestation materials should be cryptographically verifiable by the EAT consumer, typically the relying party.

However, the concept of EAT only defines a high-level architecture to describe the identity of an entity and its attributes. It becomes important to identity specific use cases and scenarios and create standardized profiles for EAT materials. This approach removes fragmentation as it lines up the industry behind one format for identity materials (EAT) and lets individual industries define specific standardized profiles. An example of such industry activity is the FIDO Alliance that is working on IoT Device Attestation/Authentication profiles to enable interoperability between relying parties and IoT devices.

Standardized Identity profiles will considerably enhance the security of IoT systems. They will enable the traceability of all elements within the device as it goes through the full supply chain, all the way to the final user and consumer. They will facilitate forensics analysis. They enable the removal of passwords during onboarding operations. They will enable advanced functions such as the dynamic onboarding and the binding of devices to applications.

Onboarding and binding of devices

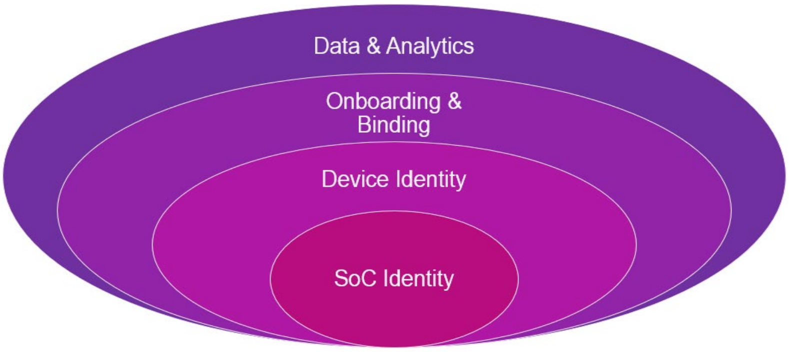
Trusted Data comes from a standardized identity format and from a secure mechanism to bind the devices to the analytics applications.


Any device to any Cloud to any Application
Onboarding Client
Device Management Service Agent
Security Analytics
Root of Trust
Zero Touch Onboarding and Application Binding
Secure Device On Boarding
Secure Update Device Image & keys download
Any Device Management Service
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.

Conclusion and recommendations

Identity is the basis for security and trusted data in IoT systems.



The recommendation is for the GSA to encourage the following initiatives:

1. Standardize on Identity formats: IETF/EAT
2. Standardize on onboarding & binding protocols: FIDO Alliance / IETF
3. Standardize on cloud APIs for tracking of Identity & ownership