WHITEPAPER

DECEMBER 2021

END TO END TRACEABILITY OF IP

GLOBAL SEMICONDUCTOR ALLIANCE INTELLECTUAL PROPERTY GROUP

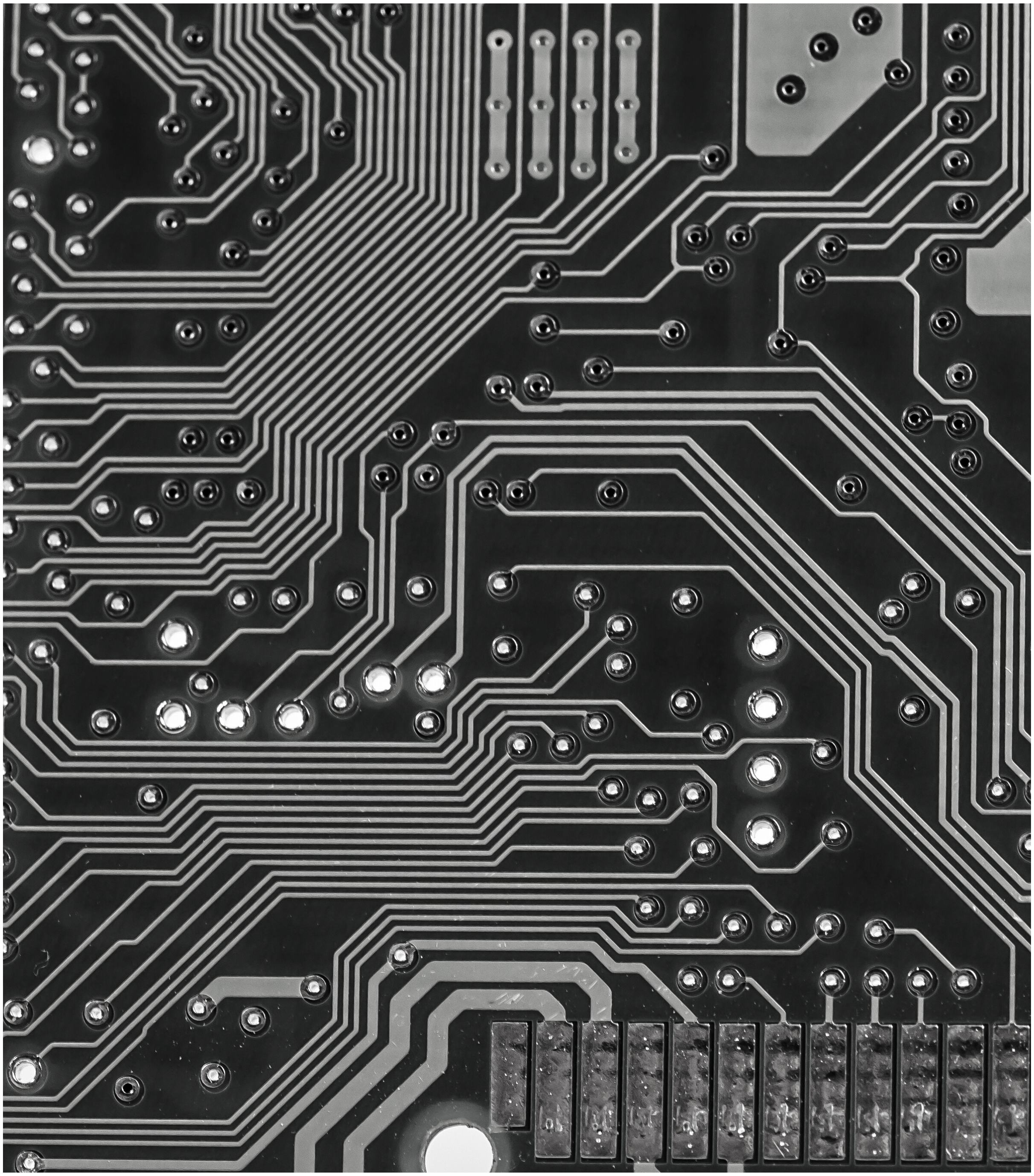
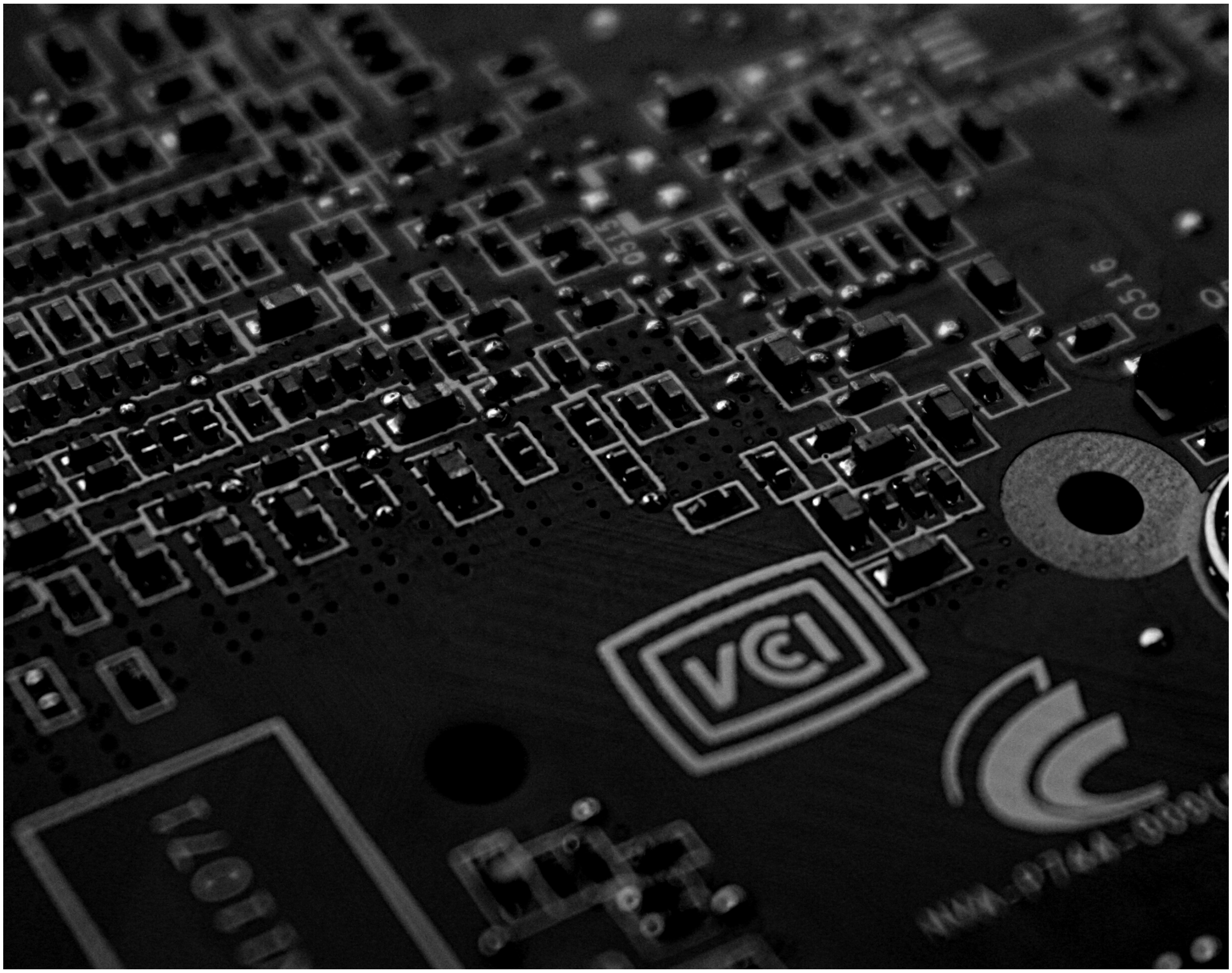


TABLE OF CONTENTS



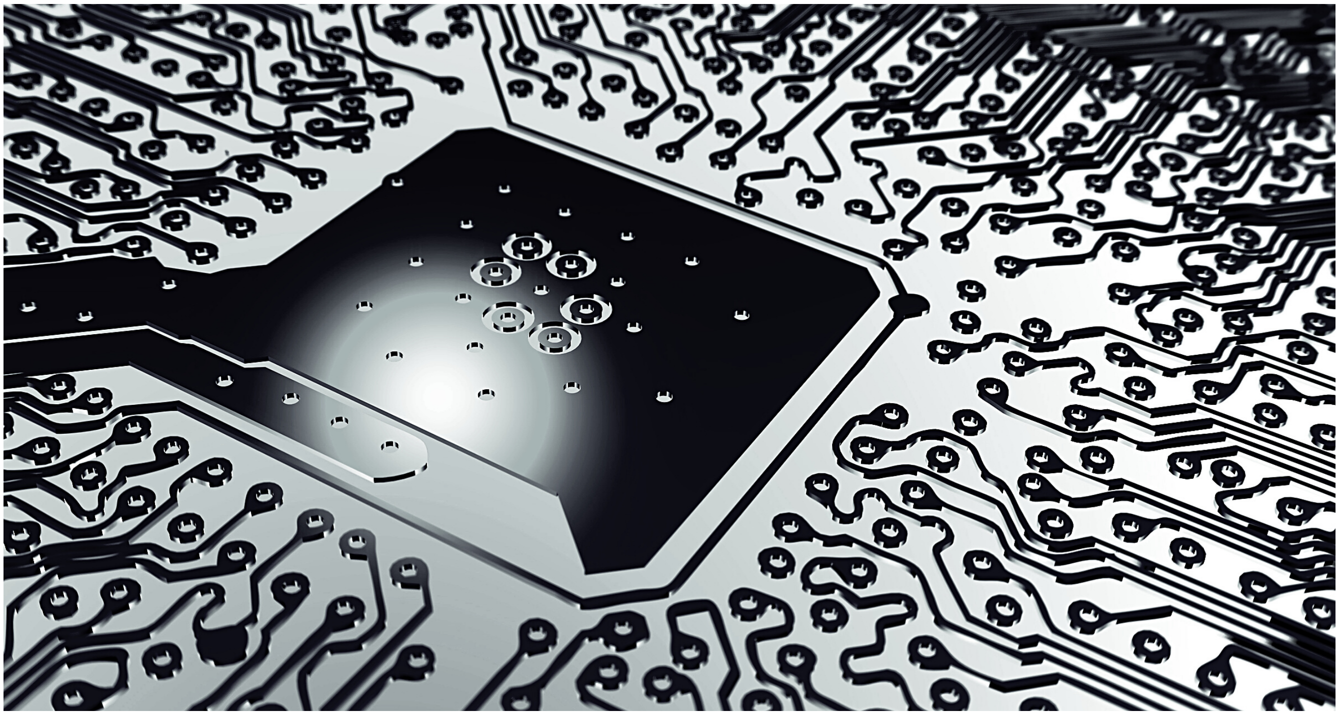
DEFINITIONS

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 Identity and security as fundamental building blocks. To create value chains that take advantage of competition, cooperation between all the suppliers around the identity and security models is fundamental. Ideally, the systems used standardized design concepts to enable the consistent tracking of all the building blocks.



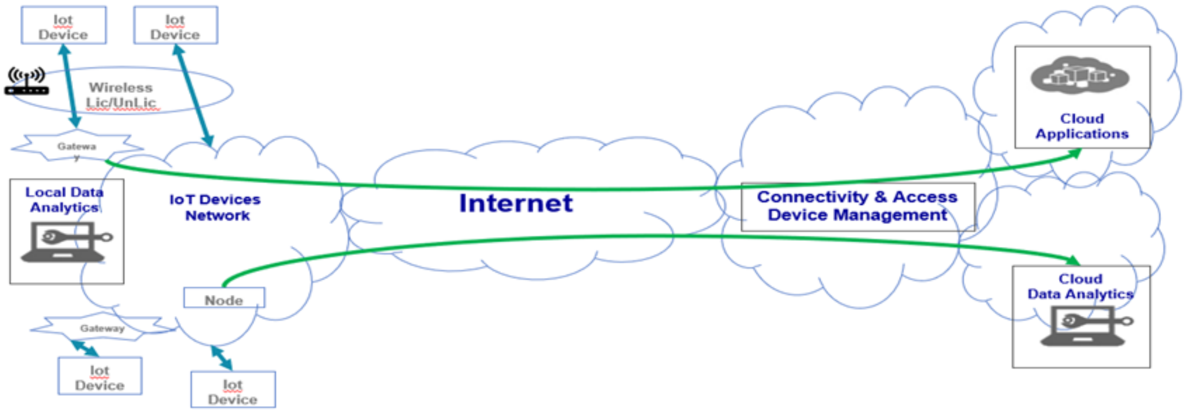
1. EXECUTIVE SUMMARY

The device industry is characterized by the fragmentation of the supply chains. The lack of consistent identity schemes for IoT devices is driving leading services providers to build walled gardens. When data generated by devices is not tagged by an identifier, its worthiness is degraded.

The objective of this document is to present the need for common schemes to identity devices, bind them dynamically to applications and manage them during their lifecycle. The document will describe the importance of having trustworthy data and metadata from IoT devices to applications.
Cloud companies and device vendors see the need to break down walled gardens 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.
Users of the devices and consumers of the services that they generate benefit from the identity schemes that track the devices and their sub-elements throughout the life of the device. The services providers have robust and standardized models by which to identify devices and their blocks of IP. They can authenticate the data generated by the devices. The services are built on trustworthy systems that can be securely managed throughout their life.

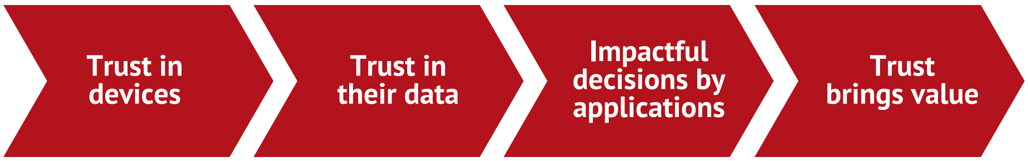
2. END TO END PROCESS TO GUARANTEE THE ORIGIN OF DATA TO APPLICATIONS

Marc Canel (Imagination)



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. Other devices will perform operations based upon instructions sent to them by applications. 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 receive data from the IoT devices. They make decisions impacting the safety of the system and its users. They send instructions to the IoT devices with large potential financial and safety implications. The data plays a key role, and it is fundamental that it is trustworthy. If the data cannot be relied upon, it is not worth much, and in some cases cannot be acted upon. Trust in the data brings value to the systems. Trust in the data is built upon a security architecture that will start with the devices. Trusted devices enable trusted data.



Trust in devices

Trust in their data

Impactful decisions by applications

Trust brings value

With so many different IoT devices to manage, services providers need consistent architectures to authenticate the identity of the devices that they manage and use for their operations.

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.

Remote device attestation plays a key role in the evaluation of a device and its trustworthiness. It 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
- Proof of the make and model of the processor, particularly for security-oriented chipsets
- Proof of BOM in PCB Assembly and profiling that can be used for attestation
- 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).

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.

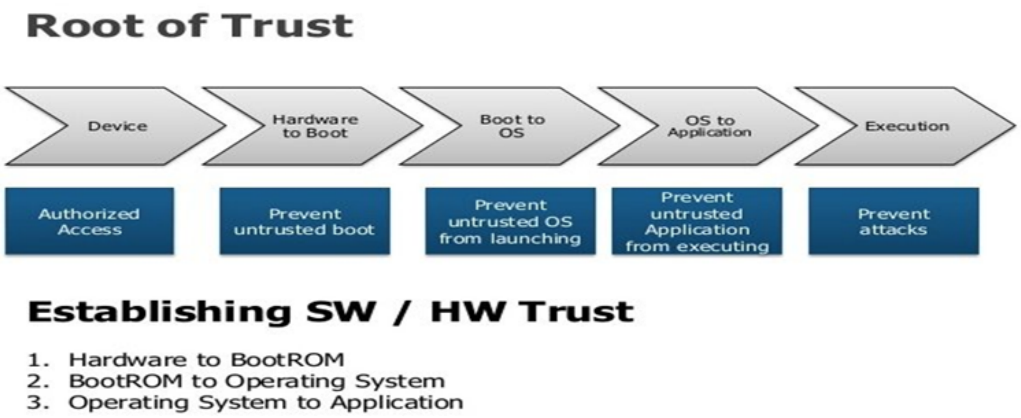
The concept of Entity Attestation Tokens is based on CBOR tokens which are themselves standardized within the IETF. Multiple data types can be supported. The format is compact enough that it can be implemented in small IoT devices. The attestation materials can be defined as claims. The EAT at the level 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 identify 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.

3. ROOT OF TRUST

Vincent Van der Leest (Intrinsic ID), Sylvain Guilley (Secure-IC), Imen Baili (Menta), Marc Le Guyader (Crypto Quantique), Teddy Kyung Lee (ICTK Holdings)



Root of Trust

Device → Hardware to Boot → Boot to OS → OS to Application → Execution

Authorized Access | Prevent untrusted boot | Prevent untrusted OS from launching | Prevent untrusted Application from executing | Prevent attacks

Establishing SW / HW Trust

1. Hardware to BootROM
2. BootROM to Operating System
3. Operating System to Application

The root of trust of the device is the physical entity in the device that contains one or, ideally, several unique uncorrelated identifier(s) for the device that cannot be altered after initial manufacturing. It is the fundamental building block of the identity of the device.

The root of trust will be used to identify that the device is genuine, the signature of the firmware code that runs on the device, creates an identity on a connected network and an identity to register users or services.

Other industry definitions:

1. The Root of Trust (RoT) is a source that can always be trusted within a cryptographic system. The RoT safeguards the security of data and applications. It helps to build trust in the overall ecosystem.
Ref: https://cpl.thalesgroup.com/faq/hardware-security-modules/what-root-trust

2. A hardware Root of Trust is the foundation on which all secure operations of a computing system depend. It contains the keys used for cryptographic functions and enables a secure boot process. It is inherently trusted, and therefore must be secure by design. The most secure implementation of a root of trust is in hardware making it immune from malware attacks. As such, it can be a stand-alone security module or implemented as security module within a processor or system on chip (SoC).
Ref: https://www.rambus.com/blogs/hardware-root-of-trust/

3. The Hardware Root of Trust is a set of core functional elements consisting of hardware and software components that can be trusted and cannot be altered during the lifetime of the product. It is something that the computer’s operating system can rely on all the time in any circumstances. Therefore, the hardware secure components must be consistent and reliable regardless of any environmental conditions such as process, voltage, and temperature variations.
Ref: https://ictk.com/puf-technology/

Multiple technologies can be used for the generation of the root of trust. There are techniques to verify that a root of trust data is genuine and authentic. It can be tracked throughout the life cycle of the product.

In case the root of trust has multiple uncorrelated identifiers, the security life cycle can benefit from these to rotate the root identity of the device or to provide uncorrelated identifiers to different users or services. The root of trust can either be injected, usually during the manufacturing cycle, or self-generated by the device using the physical manufacturing variation of each device.

Key factors to measure the quality of the root of trust are:

1. Risk analysis: it is mainly related to the number of parties involved in the secret creation and keeping
2. Entropy quality: entropy variation between two devices' root of trusts
3. Robustness to physical attacks: the root of trust secret must be kept safe. Ideally it should not be stored, and its content should not be easily reproduced by a mathematical model
4. Generation cost:
    - Key injection requires a manufacturing infrastructure and secure storage on the device
    - Device generated requires extra silicon to extract the manufacturing variation

More and more applications leveraging IoT devices are coming online, especially those allowing devices to communicate with each other. Such applications rely of Machine-to-Machine (M2M) collaboration at the organizational level and Systems-on-Chips (SoCs) at the device level. Long-term security in the IoT sphere is based on two pillars: the release of secure-by-design systems, and the implementation of post-deployment "cyber-security hygiene". In digital environments (where human supervision is absent, due to the massive amount of IoTs), roots-of-trust (RoT) are becoming pervasive. We analyze in this white paper how this is currently happening.

There is no ambiguity that in the context of Internet of Things (IoTs), **lifecycle management** is now a must have. The catalyst which enables device management is innate to the IoT. Those objects, in essence, are connected, support various complex resources (memory, computing, etc.), and are endowed by remote management features.

Therefore, they are ready to be remotely managed from a cyber-security standpoint as well. By leveraging their resources, IoT devices have the same security issues and, often capabilities, as the IT infrastructure. They can be patched when a CVE is disclosed, they can adapt when cryptography standards evolve (e.g., key size upgrade, protocol version, or even switch to other algorithms, as is the case for post-quantum cryptography – aka PQC), and they can also automate the reporting of cyber-physical incidents.
The security functions of IoT devices must be flexible enough to manage local geographic requirements. After manufacturing, a chip/device/system will be subject to the regulations of the country and the environment where it operates. This situation requires functional customization per region, and implementation of specific access control in accordance with local laws (e.g., GDPR policy in Europe, related to data management and pseudonymity).

In this end-to-end security context, it is important to understand what are the "ends". From the physical device standpoint, the security can end at the application, or at the OS, or even lower, in an embedded or an integrated secure element. The choice is determined according to the trust at the endpoint. If the application needs to run in a trusted execution environment, then the RoT is located within this TEE. If the OS is untrusted, then the trust shall come from lower levels of the system. It is typically in those conditions that code running in the privileged modes of the CPU is treated as a RoT. If the device platform can be subverted, at least in the threat analysis, the RoT needs to be a hardware integrated secure element.

For example, many user applications consider a smartphone secure, or implement some anti-reverse techniques as the only protection. When liabilities play a role, as in industrial applications or in the automotive markets, a “zero-trust” strategy is required. It will be assumed that all COTS can be “trojaned”, driving the requirement for a hardware RoT.

Physical Unclonable Functions (PUF)

A method to provide the identity required by a RoT is with a Physical Unclonabe Function (PUF). A good definition of what a PUF is can be found in “Physically Unclonable Functions: Constructions, Properties and Applications” by Roel Maes:

“Physically unclonable functions (PUFs) are innovative physical security primitives that produce unclonable and inherent instance-specific measurements of physical objects; in many ways they are the inanimate equivalent of biometrics for human beings. Since they can securely generate and store secrets, they allow us to bootstrap the physical implementation of an information security system.”

How does this work inside a chip? It all starts with deep submicron manufacturing process variations, which cause every transistor in a chip to have slightly different physical properties. These variations create small differences in terms of electronic properties, such as transistor threshold voltages and gain factor. Since the process variations cannot be controlled during manufacturing, these physical device properties cannot be created at will, which makes them unclonable.

Security properties of a PUF have been standardized in ISO/IEC 20897-1. Specified security requirements concern the output properties, tamper-resistance and unclonability of a single and a batch of PUFs. Since it depends on the application which security requirements a PUF needs to meet, this documents also describes the typical use cases of a PUF.

Making use of these process variations turns out to be good way to create unique identifiers for any given chip. This requires circuitry within the chip that converts the tiny variations into a digital pattern of 0’s and 1’s, which is unique for that chip and that is repeatable over time. This pattern is often called a “silicon fingerprint,” which is comparable to its human biometric counterpart.

PUF: Deriving a root key

Using algorithms for error correction and entropy extraction, the silicon fingerprint can be turned into a cryptographic key that is unique for that individual chip and is used as its root key. This root key is reconstructed from the PUF whenever it is needed by the Root of Trust, without a need for storing it in any form of memory. So, when the device is powered off, the root key is not present in any memory. This means that the root key is “invisible” to attackers, which makes storage of keys with PUFs very secure.

PUF: Protecting all keys and sensitive data

From the root key, a virtually unlimited number of additional cryptographic keys (symmetric and asymmetric) can be derived by using cryptographic key derivation. Like the root key, these derived keys have no requirement for storage, because they can be derived from the root key whenever needed. This means that the security level of these derived keys is equal to that of the root key as they are also not present when the chip is powered down.

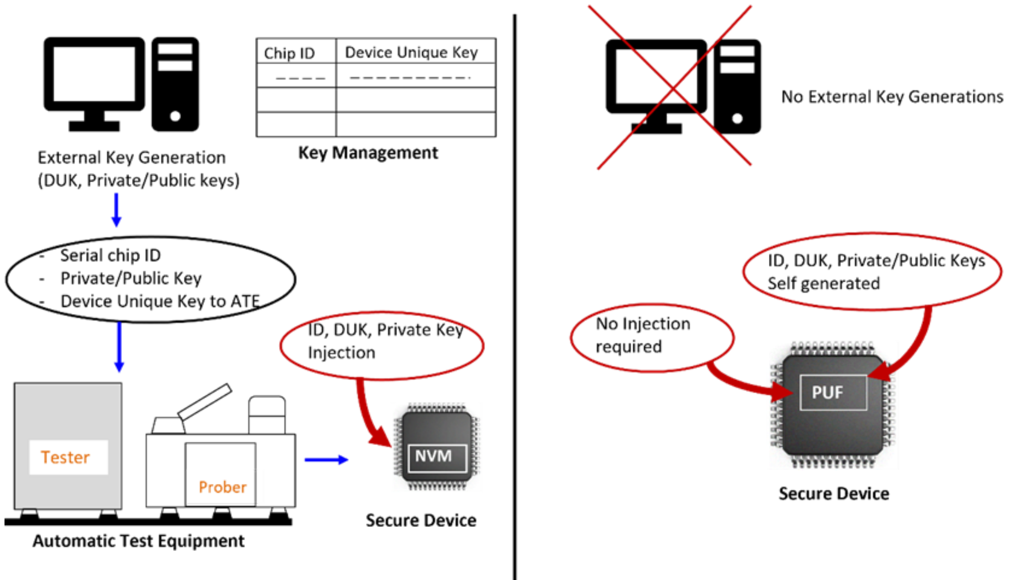
Keys derived from the PUF can also be used to encrypt additional keys that do not come from the PUF itself but have been externally provisioned. These keys can be stored in non-volatile memory, but do not need to be protected, since they are encrypted with a key from the PUF. Similarly, a PUF can also be used to encrypt dedicated memory regions and in this way provide protection for any sensitive data stored on the IC. Tokens are typically created by a random number generator, which a PUF typically also is as it produces high-quality entropy. When a token is created it can be stored securely on the device by encrypting it with a key derived from the PUF.

Injected keys vs Inborn keys: industry trend

Currently there are two ways in the industry of establishing credentials inside the secure devices: the injection of device unique key (DUK) and the self-generation of PUF-driven inborn unique key as shown in the Figure below. The DUK injection requires a secure environment where data transactions across the units are securely protected against any illegal external accesses. The provisioning process of DUK can start with the generation of the serial chip ID and a random number as a DUK using a computer program running in the secure server. The chip ID and the DUK are transmitted to an automatic test equipment (ATE) for being injected into Non-Volatile Memory (NVM) of a secure device. The DUK can be used as an encryption key for the device private key when necessary. The chip ID and the DUK are typically managed using a software tool like a spreadsheet for future reference. The entire key provisioning and the key management process are done in manufacturer’s facility where maintaining a secure environment is crucial. This is quite costly.

On the other hand, the PUF technology can eliminate the costly process. The DUK is the PUF key, the self-generated inborn identity. No injection is required to establish the credentials. By removing the injection process from external sources, it would elevate the security to the next level and contribute to cut down the manufacturing and assembly costs. Embedding a PUF IP inside a chip is the industry trend.

The embedded PUF IP is integrated into an SoC design using a standard EDA flow during the chip design stage. After the chip manufacturing stage, thus, the PUF-based Root of Trust function is activated right upon the first chip power-up which leaves no room for external intervention for attacks.

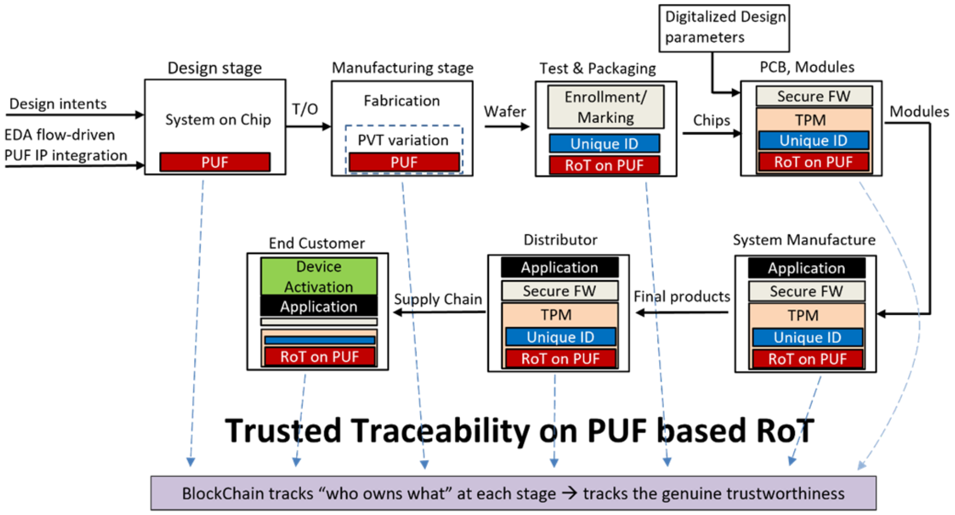


(a) Key injection by ATE

(b) Inborn keys using PUF

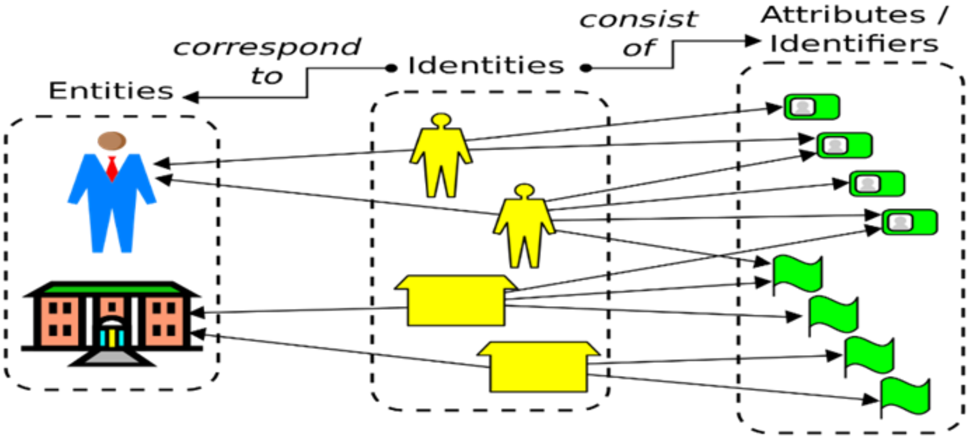
End to end protection

The trusted supply chain starts from the design stage of a chip where the Root of Trust function can be "seeded" in the design. The PUF IP can be integrated into the chip design along with cryptographic engines using Electronic Design Automation (EDA) flows where the "seed" of Root of Trust is set to be triggered later when the chip is powered up for the first time. The wafer undergoes the Process, Voltage, and Temperature (PVT) variations during the fabrication process, resulting in the random entropy property of the embedded PUF IP. The unique inborn ID is obtained, marked, and certified when the chip is powered up for initial testing. Note that the blockchain technology can provide the trusted traceability along the supply chain. It tracks "who owns what" at each stage based on credentials protected by the embedded RoT. The PCB module manufacturers receive the certified RoT chips as components along with digitalized design parameters so that manual input can be avoided. Each time the medium products are handed off to the next stage, the "trust" is also transferred, and the credentials are verified and recorded in the blockchain. Zero-touch enrolment at the end of the supply chain activates the device. Secure firmware update over the air (FOTA) plays an important role.



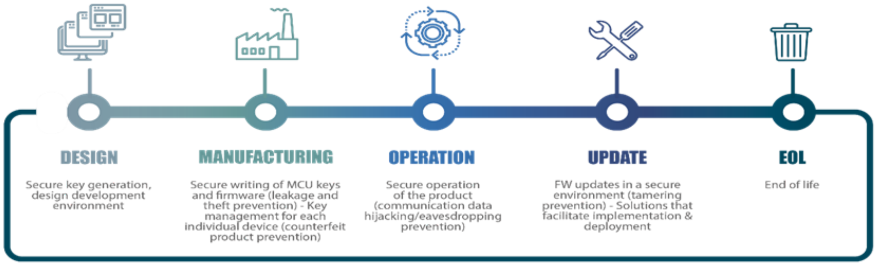
4. IDENTITY OF SoC & DEVICE

Vincent Van der Leest (Intrinsic ID), Sylvain Guilley (Secure-IC), Imen Baili (Menta)



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. All these elements make up the identity of the device. The CPU and its root of trust have usually been the most important and most basic element of the identity of the device. It is the root of the chain of trust of the device.

Security management requires the collaboration of two consecutive steps: supply chain (before market) & value chain (after market). Hence, it is an activity made possible by an ecosystem, in which the various roles are IP provider, chip architect, OEM, service operator, etc. Multiple parties need to collaborate and require coordination. Multiple technology building blocks need to be rolled out securely to control the supply chains and value chains. The systems require the ability to perform remote configuration, to verify and endorse the security elements, to certify and homologate them by third party laboratories or by sovereign authorities. Complex infrastructures need to be deployed, as cyber-security is often complex. Regarding risk, we point out that even small footprint attacks (e.g., a hardware Trojan made up of only a dozen of gates) can ruin one's business. On the positive side, security creates opportunities, such as the need to imbed the security model of the customer in the devices.



DESIGN

Secure key generation, design development environment

MANUFACTURING

Secure writing of MCU keys and firmware (leakage and theft prevention) - Key management for each individual device (counterfeit product prevention)

OPERATION

Secure operation of the product (communication data hijacking/eavesdropping prevention)

UPDATE

FW updates in a secure environment (tamering prevention) - Solutions that facilitate implementation & deployment

EOL

End of life

In general, three basic classes of security services are requested: **key injection, firmware update over-the-air (FUOTA), and monitoring**. Those functions provide tangible and controllable security measures. For instance, the ETSI EN 303645 standard specifies 13 rules for secure operation of IoT objects. They are mandatory when shifting from non-connected secure elements (e.g., former smartcards) to IoT (with an impact of physical world), where system updates become a requirement.

The secure updating of credentials (keys, code, bitstream, etc.), including versioning are now base-line functions of connected IoT systems. Those functions are already available, from a technology standpoint. In this respect, your chip / device / system needs a root-of-trust. The industry can already provide you with:

1. A silicon root-of-trust (to manage device assets, such as status, keys, code, etc.).
2. Connectivity to host (to provision the keys, install a certificate, to flash a bitstream, etc.).
3. API for remote management across zero-trust networks.

One example of use-case can be found in the automotive industry. Remote security management enables security traceability from the OEM to the different tiers, thereby making it possible to reconfigure ECUs (over-the-air updates) with approved packages.

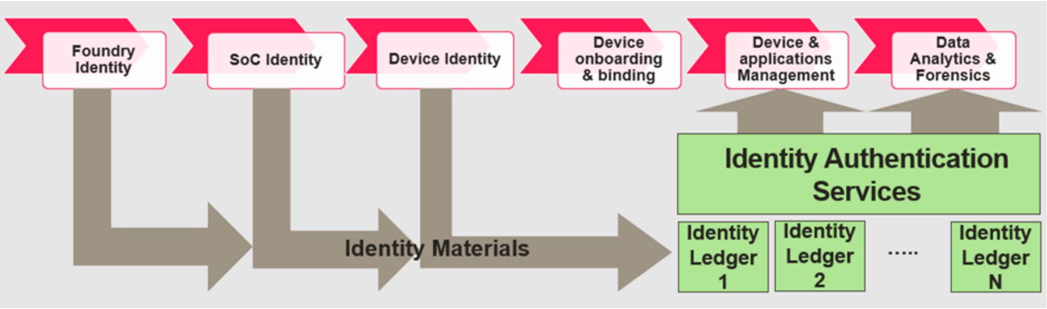
For **integrated Secure Element (iSE)**, the cryptographic algorithms must remain flexible, e.g., by allowing them to transition from elliptic curve cryptography to PQC. Also, depending on the targeted certification level, different levels of countermeasures (of various strengths) are required.

Eventually, a trusted end-to-end supply chain is thus made possible (see: http://www.latticesemi.com/LatticeSupplyGuard). When the RoT is integrated, at the same time the BoM is reduced (since host chip resources are leveraged), and the security control is finer (since the host reset is conditioned by the RoT) and broader (since even the configuration of critical features at the chip-level, such as power management, memory protection, is made possible). Thus, integrated Secure Elements, are, without surprise, the new way to build security on trustworthy foundations.

Clearly, the RoT identity, when it is a SoC, is limited to this scope. PUFs generate the ID, and the genuine nature of the data can be attested by the DICE protocol, for instance. However, one must keep in mind that the full device identity encompasses other aspects, such as that of the applications, the users, the configuration, etc. which are contextual and might evolved with the life cycle. This aspect is further developed in the next section.

5. AUTHENTICATION SERVICES

Rob Dobson (Device Authority)



Foundry Identity
SoC Identity
Device Identity
Device onboarding & binding
Device & applications Management
Data Analytics & Forensics
Identity Authentication Services
Identity Materials
Identity Ledger 1
Identity Ledger 2
.....
Identity Ledger N

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

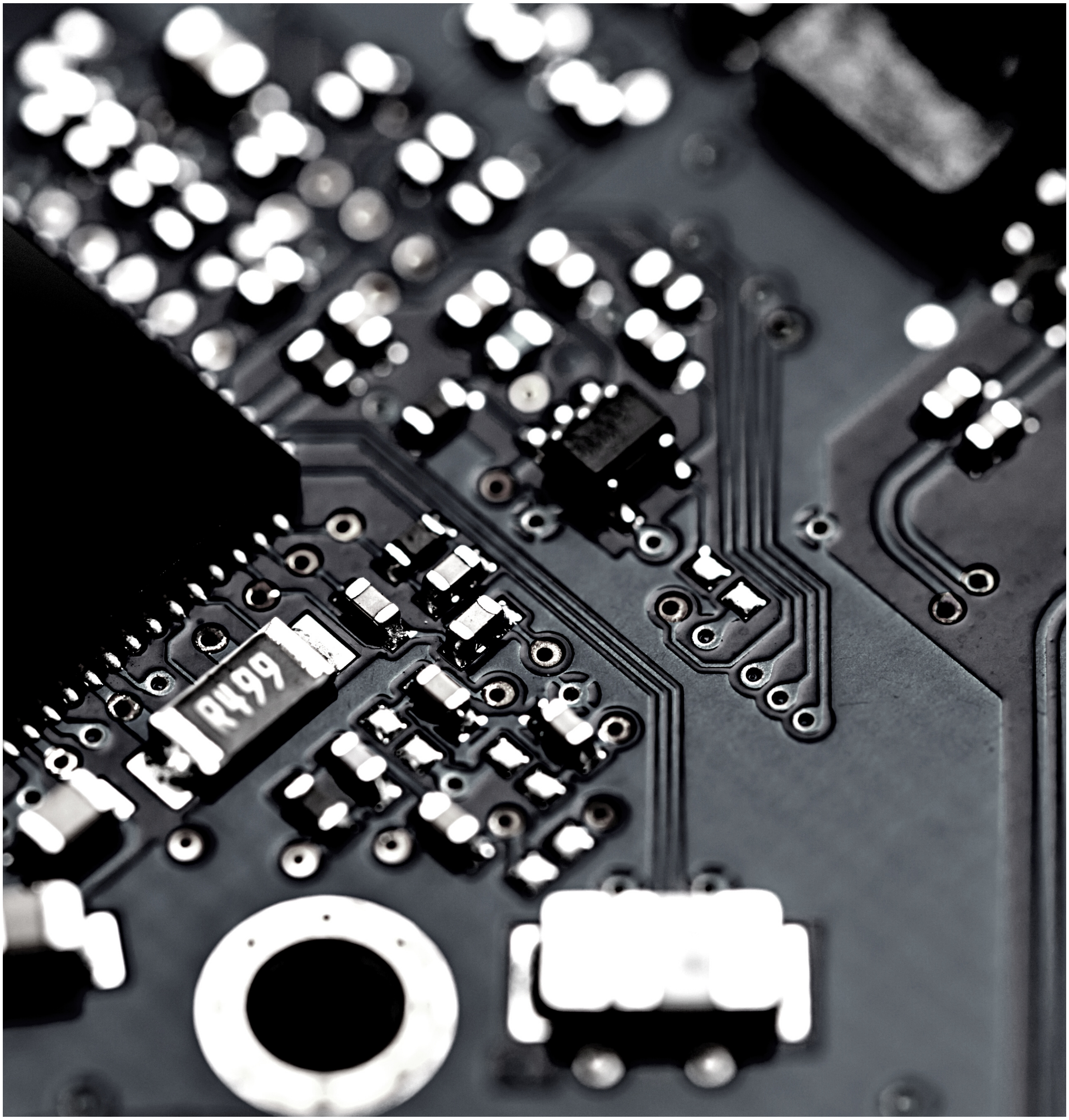
Enterprises need to know that a device is trustworthy before allowing it to access corporate data. Devices and users in these environments must be authenticated AND authorized before being allowed to access both remote and local services. This extends beyond the usual "server side" implementations down to local inter-device communication.

Strong device authentication becomes a mandatory requirement for use cases that are "online" and sometimes "offline", where offline devices are not connected to the internet but still require security management. Any entity that is interacting with the device relies on the device having strong device authentication/attestation and that it can't be spoofed. The fundamental security operations which a device needs to manage requires these authentication services, whether that's from initial device onboarding, requesting a new certificate, updating/rotation of data crypto keys, secure code update keys, manage remote access credentials to name but a few, they all require authentication. With any of these operations it is important that devices remain authentic and are trustworthy.

This application-level authentication is a mandatory requirement and there are scenarios where enhanced authentication above the network level is required for real-time device authenticity validation, coupling relationship between device identity and data, and ensuring only trusted entities can participate in interactions between applications and devices.

Imagine a scenario where there is a large industrial boiler in an industrial plant, and this boiler is controlled by a cloud-based application. Sending control instructions, such as update temperature, close water outlet etc. There must be mutual trust between the cloud application as a mandatory requirement. However, on top of this, for critical instructions such as these, there can be a requirement to have "real time" authenticity validation. One way to do this is prior to sending a critical instruction to the boiler, request the boiler to attest its authenticity to a relying party or IAM. If the relying party attests the device is authentic and integrity, then the relying party can send a token to the device which it can use to present back to the cloud application. This ensures the application is talking to the correct boiler and it is trustworthy. Then the instruction to perform a critical instruction to update temperature, open valve etc. can be performed, minimizing the risks associated with these types of applications.

A simple mistake that many vendors make is the use of hard-coded credentials, often common to a family or class of devices. Every device needs to have a unique identity and associated set of credentials. The use of hardcoded, common credentials will not only open all the devices up to spoofing/cloning/unauthorized access but will also offers zero recourse or revocation when the credential is finally abused.



6. INDUSTRIAL USE CASES

Teddy Kyung Lee (ICTK Holdings)

Anti-counterfeiting solution

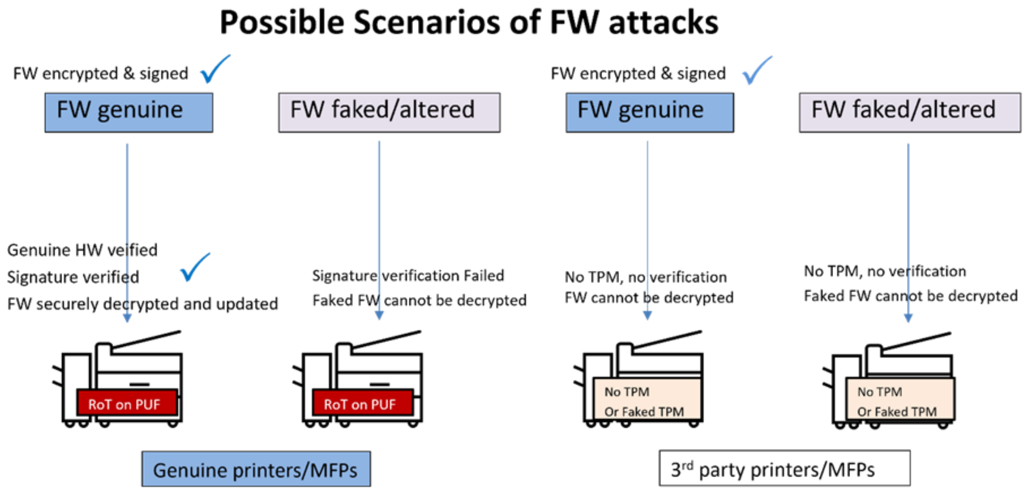
The Global Brand Counterfeiting Report estimated the amount of total counterfeit goods globally had reached 1.2 trillion USD in 2017 and is bound to reach 1.82 trillion USD by the year 2020. The US Government of Accountability Office reported in 2018 that two out of every five products purchased online were counterfeit. Amid the COVID-19 pandemic, there are major shortages of specific products worldwide. The shortage may draw attention to counterfeiters who seek weaknesses in the supply chain and introduce counterfeit products to the market. For example, the counterfeit supplies of printer toner, ink cartridges, and laptop batteries appear on the market in 3 or 4 months after new products are released. Even if the legitimate companies put all the effort to stop the counterfeit products, they keep coming back. Is there any ultimate solution for this? Or at least any solution for delaying their market appearance to a substantially longer period than just 3 or 4 months?

The hardware Root of Trust (RoT) system based on PUF technology can provide the ultimate solution for the counterfeiting issues and the endpoint tampering issues. The technology defines how to prepare the supply components at the manufacturing site where the public key provisioning of CA (Certificate Authority) and signing of a component certificate are performed. The technology also defines how to authenticate genuine parts at consumer end when the components are installed in the host machine. The trusted supply chain based on the PUF technology benefits everyone across the value chain including major brand companies, supply vendors, IC, OEM/ODM, and end consumers.

Firmware protection

Firmware products uploaded to servers are often targets of hacker's attacks. The binary form of firmware can be downloaded, easily modified, and replaced with compromised ones unless properly protected. Hackers install the modified firmware on aftermarket or third-party vendor products, or even on genuine products to take over the control of the devices. The compromised devices may be used as Trojan horses through which unauthorized access to the intranet of a corporation could be granted. This is a serious issue not only for the customer company but for the supplier company.

To overcome the issue, a fundamental solution for protection must be placed against hacking activities like disassembly and reverse engineering. The downloaded firmware should be bound only to genuine hardware products. For example, if we consider the firmware protection on printers or MFPs, we can use the PUF based RoT technology embedded in the printer devices. The genuine firmware needs to be encrypted and signed with the server's private key before being uploaded for further service. The server's public key is properly provisioned to the printer products before being shipped to customers. When a user commits to download and install the firmware on the printer devices at the field, the authentication process is kicked off under the hood. A faked or modified firmware fails to pass the signature verification process and no installation will occur. The second authentication process is also engaged before the firmware is decrypted for the final installation. The authentication process is based on the trusted platform module (TPM) built on PUF-RoT which is available only in genuine printer devices. No third-party device or faked devices can execute the authentication process, so no firmware installation. Other than the case of the genuine firmware running on the genuine hardware devices, all other cases must be failed to execute properly as shown in the figure below.



PUF-USIM applications

Recently the world-first product of PUF-USIM card is commercially debuted as shown in the Figure below. The PUF-USIM is the perfect combination of two technologies between user-friendly USIM functions and the hardware Root of Trust functions powered by the PUF technology, resulting in the birth of a “robust PUF secure element”. The PUF technology can perfectly complement the vulnerability issues of the existing USIM cards such as SIM swapping, SIM cloning, and Man-in-the-middle (MITM) attacks. The hardware inborn identity and the secure storage feature of the PUF technology enable the Root of Trust function in the combined PUF-USIM product.
Ref: https://www.gsaglobal.org/forums/industrys-first-debut-of-puf-usim-chip/

The world's first PUF-USIM card

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