KEYFACTOR

EBOOK

Matter – a cybersecurity perspective

Table of contents

Subject Matter Expert:

Guillaume Crinon

Director of IoT Business Strategy, Keyfactor

Guillaume has 28 years of experience in the semiconductor and software industry, IoT security, radio-frequency circuit design, project, team management and business-development. For the past 8 years he has been focusing on IoT security technologies and the way to bridge the security gap between IT / Enterprise platforms and low-power connected devices.

Guillaume joined Keyfactor as Director of IoT Business Strategy with the global IoT team in 2022.

Before transitioning to this role, he was the IoT Strategy Manager for security and connectivity with the AVNET Global IoT team in charge of Avnet-specific products, such as a family of reprogrammable SIM cards (eUICC) and leading the development of a management platform focusing on delivering secure over-the-air provisioning and upgrade services to IoT devices.

Guillaume graduated from SUPELEC in Paris (MSc in EE) in 1994 and has co-authored 13 international patents in wireless systems, IC architectures and security to date.

Introduction

Formerly known as domotics, home automation and smart homes is the idea of using devices and appliances to measure, control, take action, and automate processes in our homes, and it's been slowly materializing since the first personal computers in the 1980's.

Early systems were not connected to anything outside the home. They mostly used point-to-point or point-to-multipoint remote controls that operated with proprietary wireless or powerline communications. Given their proprietary nature and limited communication, security was not a major concern. This means of communication can still be seen in many new systems today.

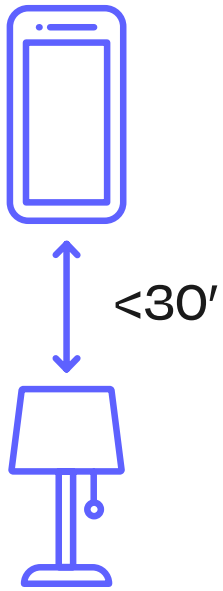
For decades, standardization and interoperability were afterthoughts; only proprietary systems existed. As consumers pushed for systems to work together, repeated attempts to solve interoperability between appliances from different brands only considered the connectivity side of the problem (e.g., Zigbee). Security was always seen as a constraint, making product usage too complex, and was, at best, delegated to the connectivity layer.

To meet the needs of the market, in December 2019, Amazon, Apple, Google, Samsung SmartThings, and the Zigbee Alliance announced the Connectivity Standards Alliance (CSA), a collaborative effort with the goal of simplifying smart home product development utilizing IP. On October 4, 2022, version 1.0 of the Matter specification was published. Today, Matter sets the bar for standardization and communication in the smart home market.

A history of device communication

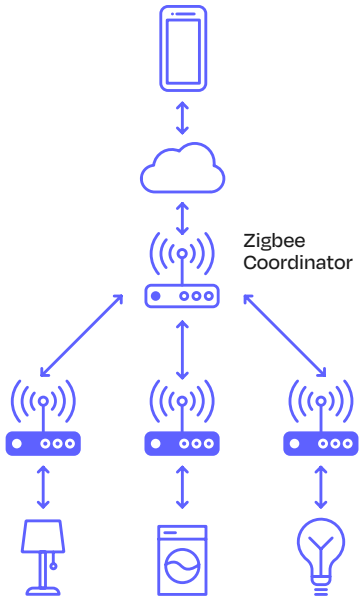
Bluetooth

When Apple gave birth to the first iPhone, iPad, and the App Store, Bluetooth was the only widely available communication method for an application to have more sophisticated control of a home appliance. Initially designed to connect nearby printers to desktop computers, Bluetooth evolved with lower energy, higher bitrate, and slightly longer-range versions enabling close-range control of lamps, toys, kitchen appliances, etc. But Bluetooth's 30-foot maximum range was still a problem for most home applications as radio waves also had to travel between tiny, embedded, lossy antennas through concrete and plaster walls. Bluetooth security also relies on symmetric keys. While they have a smaller memory footprint and lower power requirements than asymmetric keys, they are also vulnerable to man-in-the-middle attacks.



Zigbee

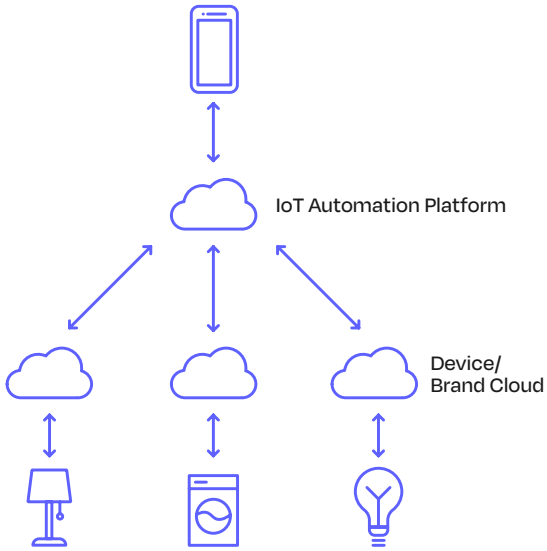
A new IEEE standard - 802.15.4 - emerged with better modulations and lower power consumption onto which Zigbee mesh networking was mapped. However, despite excellent range and power properties, smartphone manufacturers never added Zigbee to their radio stack and gateways had to be deployed with every appliance. These gateways provided the connection of the devices to remote servers that bridged to web and smartphone applications. From a security standpoint, like Bluetooth, Zigbee utilizes symmetric keys, therefore suffering from the same vulnerabilities. As a result, Zigbee was never as widely adopted as it should or could have been in the smart home industry.



Wi-Fi

At the same time, Wi-Fi was put into smartphones and was rapidly adopted as the go-to for communication. Security then became a concern for our home networks as more systems and devices began to communicate externally. Security would be tackled with TLS (Transport Layer Security), PKI (Public Key Infrastructure), and X.509 certificates, all relying on IP connectivity.

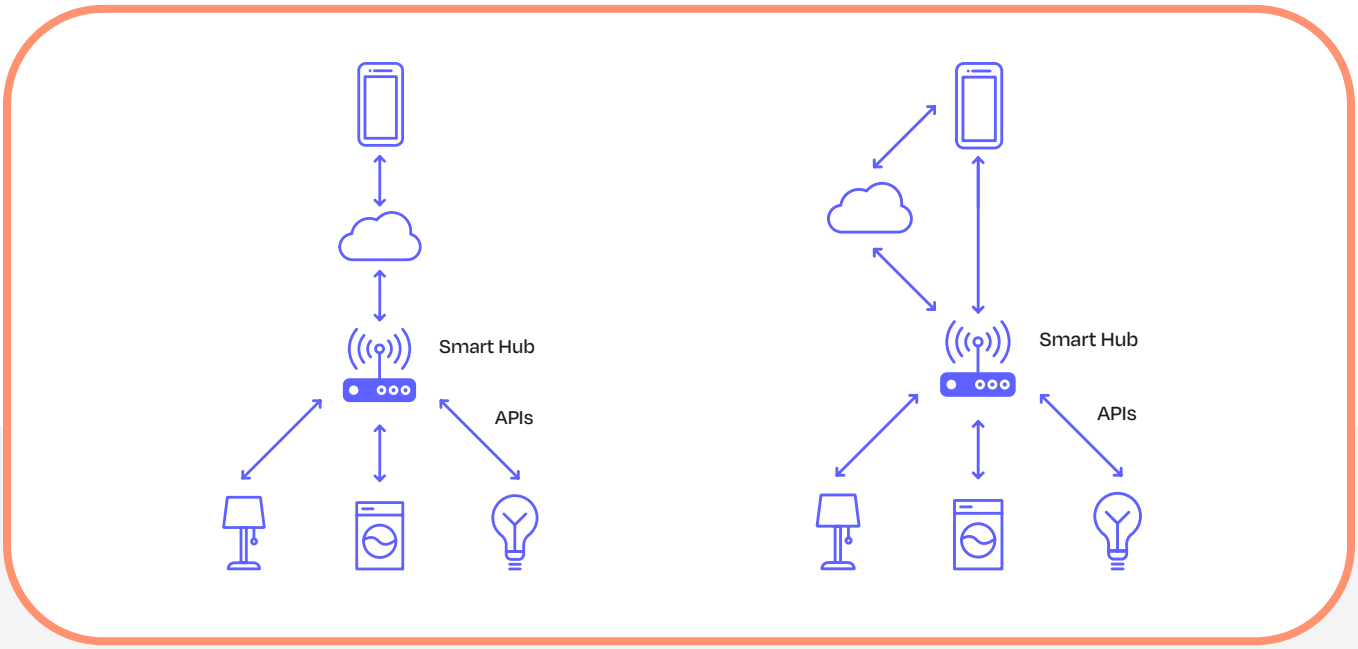
With the convergence of the connectivity boom, SaaS, smartphones, and technology platforms, the Internet of Things (IoT) was born. IoT envisioned IPv6 as the ultimate unifying protocol. Zigbee spun off Thread, allowing IP addressing with 6LoWPAN and DTLS certificate-based security. With these new communication technologies and opportunities, service providers like Tuya and IFTTT started offering applications that allowed users to build control scenarios across different brands and makes of sensors, appliances, and connectivity technologies. However, provisioning and security were still a concern. Additionally, there was the architectural requirement that a smart light switch and lamp in the same room both needed an internet connection to an external server to interact.



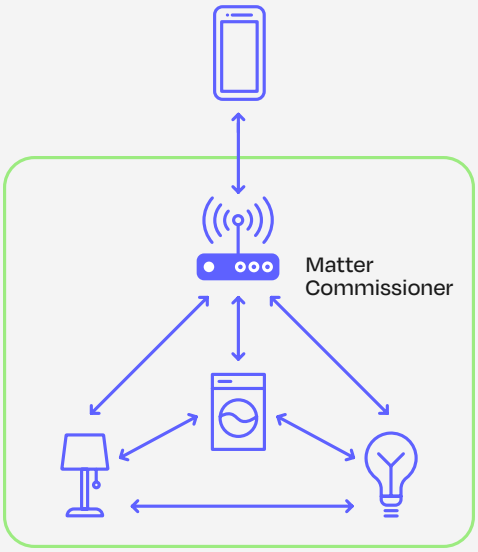
The Smart Hub and Matter

Home assistants were next into homes. These smart devices served as a “hub” for smart homes but still suffered from interoperability requirements. The consumer market made it clear: devices needed to work together without any middleware. Manufacturers agreed, but they still had to figure out how to standardize provisioning, security, application data interfaces, and other services across different brands.

This need became the foundation for Matter.



Matter is not a new radio connectivity standard requiring the development of a net-new technology. Instead, it maps onto existing ethernet, Wi-Fi, Thread, and IP connectivity to tackle the challenges of provisioning, lifecycle management, and data exchange between devices and applications, as well as security. It is the culmination of global smart device manufacturers coming together for the greater good of the consumer market while simultaneously streamlining their own development processes.



Matter Security Architecture

Introduction to PKI

To understand the security architecture of Matter, it is best to start with an introduction to what it is based upon: Public Key Infrastructure (PKI).

The crux of security based on PKI is a digital certificate. Think of a certificate as a unique digital ID that is put on a device to show that it is genuine and trustworthy, like a passport for international travel. Therefore, the certificate must be produced in a secure way. To do this, PKI relies on a chain of trust within a hierarchy of Certificate Authorities (CAs) to generate the certificates.

At the top of the hierarchy is the root CA. The role of the root CA is to generate certificates that will be used by intermediate CAs, which, in turn, issue certificates to end devices. Each certificate produced for a device is signed by the intermediate CA, which is signed by the root CA. This means that the root CA needs to be highly secure, because if its certificate is compromised, every intermediate CA, and therefore every device certificate is then compromised and insecure.

Many PKI operators keep their root CA offline and in a secure location, on a hardware security module (HSM). They are brought online only to sign intermediate CA certificates.

Just like a passport, a certificate has an expiration date. Often times, this is set to match the expected lifespan of the device. However, depending on the use, a certificate may have a shorter expiration period and require the ability to be renewed.

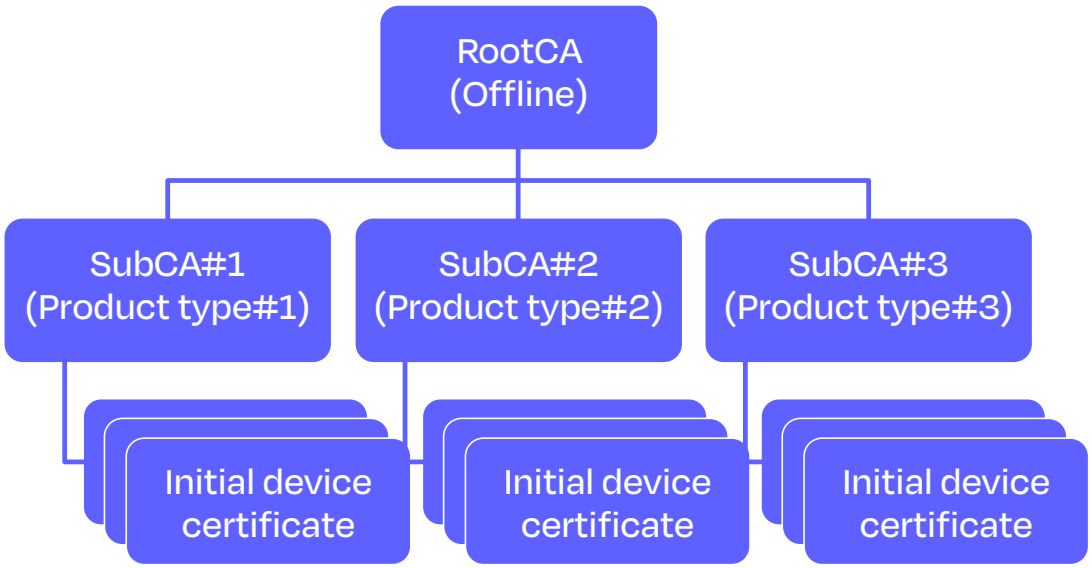
A PKI can be deployed in any number of architectures based on the needs of the manufacturer. It can be placed on the factory floor, hosted in a private cloud environment, offered in a SaaS model, or a hybrid of any of these. While outside the scope of the document, there are pros and cons to be weighed in choosing the correct setup.

On the device itself, there needs to be a way to securely store certificates, cryptographic algorithms, and other secrets. A Root of Trust (RoT) is a secure element, trusted platform module (TPM), or microcontroller, where device secrets can be stored. A RoT can be either secure hardware, or it can also be secure software on non-secured hardware.

For a certificate, a cryptographic algorithm on the RoT generates a public/private key pair, which becomes the foundation for a Certificate Signing Request (CSR). The CSR is the request by a device to an intermediate CA to generate and sign a certificate for the device, based on the key pairs sent over. If accepted, the CA signs and issues the certificate back to the device, where it is stored on the RoT.

Now that the device has an identity, when it communicates with another device, it can present its certificate to show that it comes from a trusted source and is therefore safe to communicate with.

How to choose an RoT will be based on many factors including cost, security requirements, and physical space on the board.



Matter security

Matter device vendors can be thought of as belonging to one big family. It is a family where members trust one another, but where admission requires more than just a membership fee.

A vendor must:

01 **Set up a vendor PKI with a CA hierarchy, structured according to the Matter specification**

02 **Design the product by the Matter specification using a defined RoT**

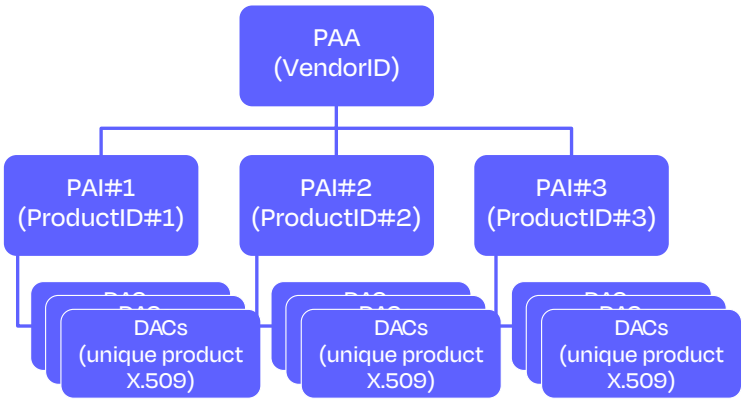
03 **Receive a Certificate Declaration (CD) from a Matter-accredited lab to show design compliance**

04 **Publish their Product Attestation Authority (PAA) certificate in the public Matter Distributed Compliance Ledger (DCL)**

05 **Be designed to only trust devices from other vendors with their root certificates published in the DCL**

The Vendor CA hierarchy: PAA-PAI-DAC

The security of a Matter ecosystem, also know as a Fabric, starts by manufacturing devices with a unique Matter-compliant identity that other Matter devices will recognize as genuine and trusted. This is achieved by the Vendor CA hierarchy.



The Vendor CA hierarchy is based on a standard PKI hierarchy:

PKI	Vendor CA
Root Certificate Authority	Product Attestation Authority (PAA)
Intermediate Certificate Authority	Product Attestation Intermediate (PAI)
Device Certificate	Device Attestation Certificate (DAC)

A Vendor must establish a PKI, starting with the self-signed Product Attestation Authority (PAA). The tree then grows with as many Product Attestation Intermediates (PAIs) as there are Matter product types to be manufactured. More product types with their corresponding PAIs can be added in the future. The PAI will be the working instances that issue Device Attestation Certificates (DACs) at manufacturing upon request – one per physical product.

The PAA certificate, and optionally the PAI certificates, are then declared to and registered in the Distributed Compliance Ledger (DCL). Matter appliances constantly check the DCL so devices from different vendors can recognize and trust one another as a genuine part of the Matter family.

The Matter specification details the exact certificate formats to implement at each of the three levels.

The DCL is a public ledger shared among the vendors and administered by CSA.

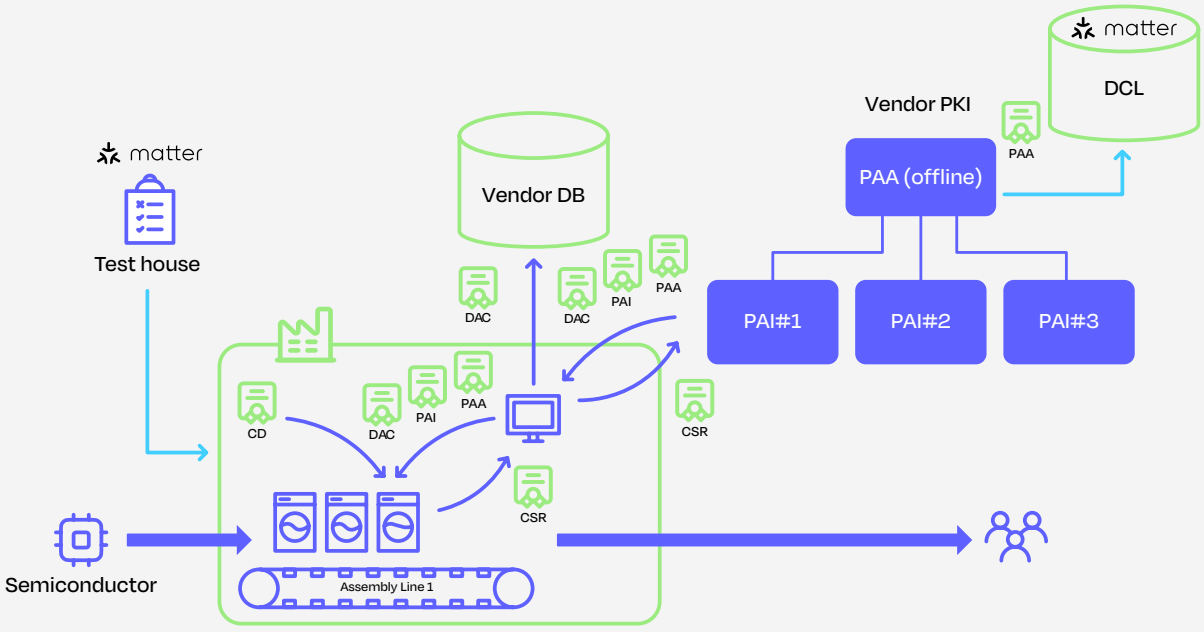
Device Identity Issuance for a Matter device

After establishing the Vendor PKI, DACs are ready to be issued. DACs can be issued during manufacturing by the vendor themselves, before manufacturing by a silicon vendor, or after deployment through an over-the-air (OTA) update.

The most flexible option for a vendor is to issue the identities during the manufacturing process as follows:

1. The device RoT generates a new Elliptic Curve Cryptography (ECC) private/public key pair
2. The device RoT generates a Certificate Signing Request (CSR) for the public key
3. The CSR is submitted to the Vendor PKI and signed by the PAI
4. The PAI creates a new DAC
5. The DAC is sent back to the device and stored into the RoT

During manufacturing, other sensitive data such as secure boot verification keys, firmware signature verification certificates, the Matter CD, and firmware measured boot vectors, should also be programmed into the devices.



If the device RoT is a secure element, the silicon vendor may offer to have these steps executed inside their factory instead. This requires additional processes to ensure that the DACs are still attached to the Vendor PKI and that the other sensitive data is still applied to the device, but this may be preferable in some manufacturing settings. Additionally, the DAC may be applied upon first power up and boot in the field. This is more complex but offers benefits if regionally specific certificates are required and manufacturing is not done on a regional basis.

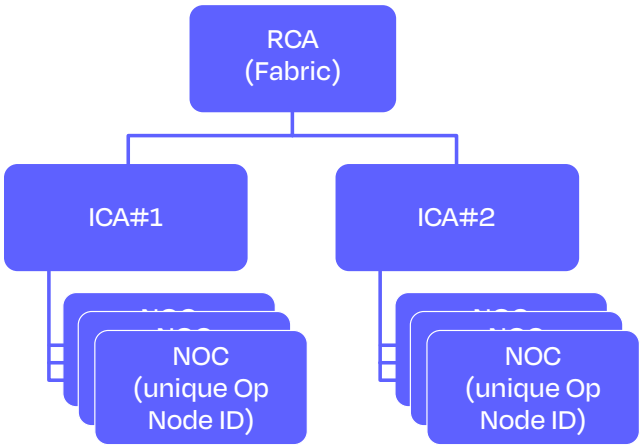
The purpose of the DAC is to prove the genuineness of a Matter device when trying to join a Fabric or upon request by a Fabric Commissioner. Securing the data exchanges of devices within a Fabric is handled by a different chain of trust: the operational CA hierarchy.

Fabric Commissioner: A device that is responsible for onboarding new devices into a Fabric and assigns them credentials.

Operational CA hierarchy

Matter connects devices across different networking technologies and manufacturers into a collection of communicating devices, known as a Fabric. The Fabric is managed and maintained by an administrative node, the Commissioner. The Commissioner runs its own chain of trust: the operational CA hierarchy.

While the Vendor CA hierarchy delivers life-long DACs, which prove a device's genuineness, the operational CA hierarchy delivers short-lived Node Operational Certificates (NOC) to be used to secure end-to-end communications between devices within the Fabric. How short-lived is dictated by the security policy of the Fabric.



The hierarchy of the operational CA mirrors that of the Vendor CA:

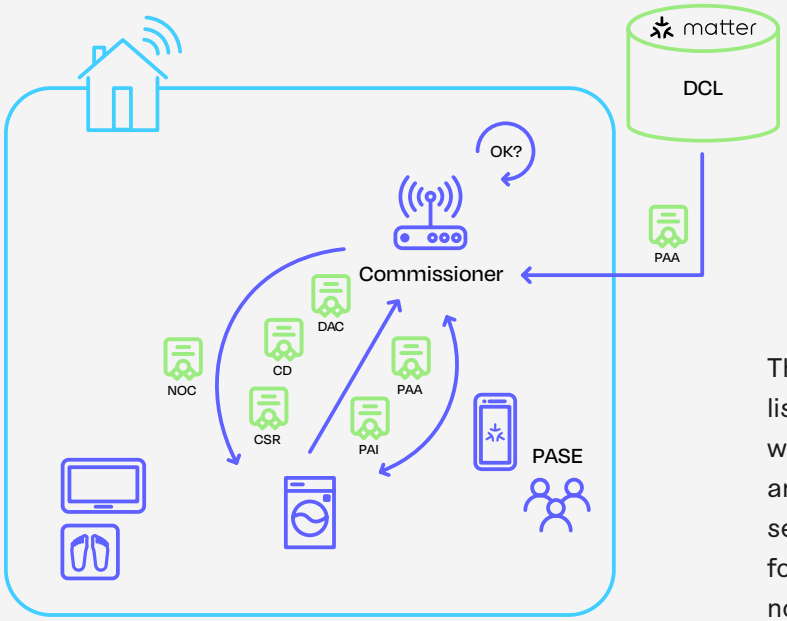
Vendor CA	Operational CA
Product Attestation Authority (PAA)	Root Certificate Authority (RCA)
Product Attestation Intermediate (PAI)	Intermediate Certificate Authority (ICA)
Device Attestation Certificate (DAC)	Node Operational Certificate (NOC)

The process of a device receiving a NOC and joining the Fabric is known as commissioning.

Commissioning

Commissioning obeys a strict protocol to ensure only genuine and authorized devices can join the Fabric. For commissioning to occur, the Commissioner must be running with an internet connection, its internal clock must be synchronized to UTC, and a Fabric must be established. Once these prerequisites have been met, the commissioning process is as follows:

1. The device and Commissioner discover one another (or are introduced by a user) on a network interface (BLE, Wi-Fi, Thread, or Ethernet)
2. A secure channel is established with a Password Authentication Session Establishment (PASE) process
3. The Commissioner updates the device's Real Time Clock (RTC) to UTC time
4. The Commissioner establishes the authenticity of the device by verifying both its DAC and CD against the online DCL
5. Device sends a CSR to Commissioner
6. Commissioner answers with a NOC
7. Commissioner sets access control policies for the joining device and shares operational network access
8. The Commissioner terminates the PASE connection
9. Device reconnects to the Commissioner and opens a secure session using Certificate Authenticated Session Establishment (CASE)



The Certificate Authenticated Session Establishment (CASE) protocol then allows two nodes within the same Fabric to exchange their NOC and derive symmetric session keys to efficiently secure their communication channel. This allows for direct communication within the Fabric with no need for communication to external servers.

Other Security Considerations

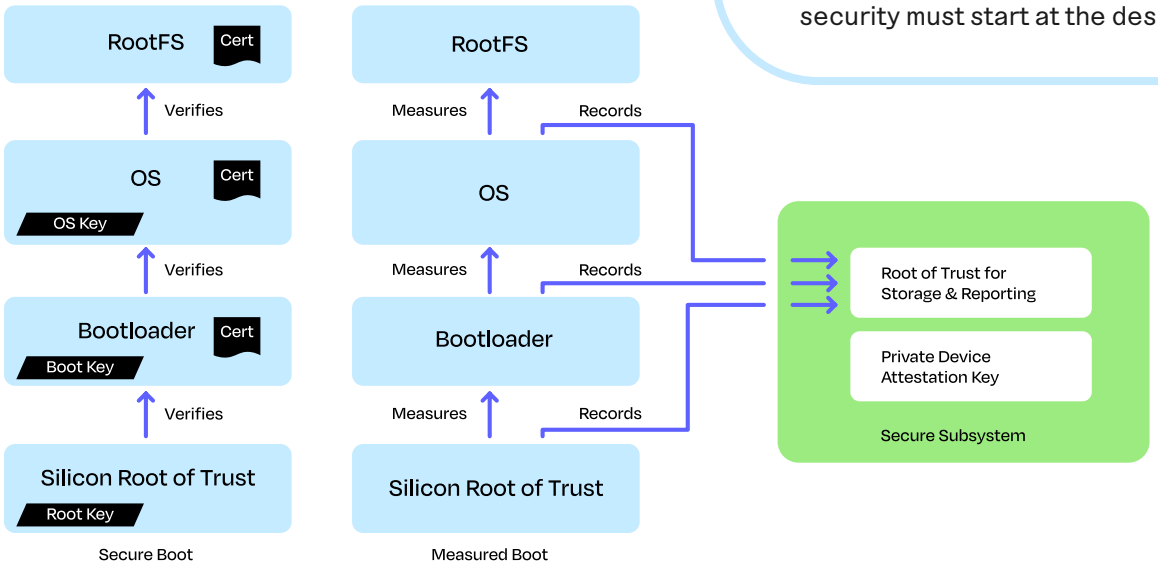
Beyond identities, Matter also lays the groundwork for other critical security functions, including securing updates to software and firmware, while laying the foundation for secure boot requirements in the future. Additionally, consideration must be given to what levels of permissions devices have when communicating with one another.

Firmware and Secure Boot

The first release of Matter did not require secure boot on the device, but rather leaves it to the capabilities of the MCU and the choice of the vendor. This allows a vendor's developer to implement anything from no security to secure or measured boot. However, it is recommended to implement secure or measured boot as a component of sound cybersecurity. This requires cybersecurity be thought of during product design.

If measured boot can be implemented, boot vectors are to be signed by the device attestation private key and the assembled firmware digests reported alongside the CD to the Fabric Commissioner. The Commissioner can then check these digests against their reference values kept up to date in the DCL every time a new firmware version is released.

> Since secure boot starts in the RoT, it cannot be added as an update. Cyber-security must start at the design.



Matter also does not specify how firmware images are signed, delivered, or verified. How and if firmware image signing is implemented is left to the vendor to decide. However, since firmware image signing is a common practice, the format for Matter-encoded certificates has design considerations for encoding firmware signing certificates.

Code signing is highly recommended to eliminate altered or malicious code being put on devices.

Access Control

Just because a device is trusted and onboarded to a Fabric does not mean that it should have carte blanche access to all the features and functionality of all other devices on the Fabric. The Access Control features of Matter aim to ensure that only authorized devices are permitted access to certain application-layer functionalities exposed by the Data Model, through the Interaction Model. Access Control is the fundamental link between the Secure Channel and the Interaction Model.

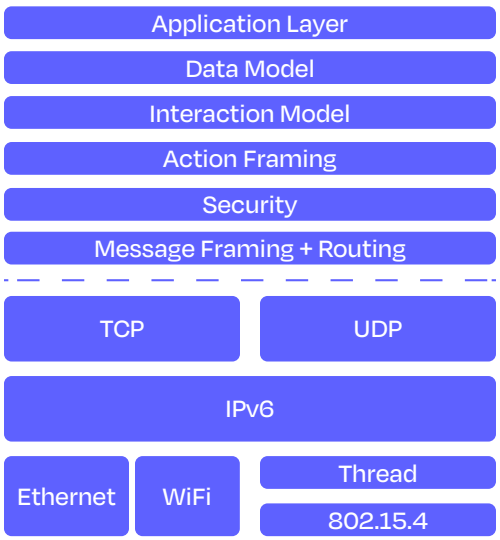
In order to implement a policy of Access Control, Administrators of the Fabric create and maintain a consistent distributed configuration of Access Control Lists (ACLs) across all Nodes. Each Node has an ACL containing Access Control Entries that codify the policy. The Access Control Cluster exposes a data model view of a Node's ACL which enables its maintenance.

Matter compared to other industry standards

Matter and 802.1AR

The IEEE 802.1AR standard “Secure Device Identity” specifies the structure of a device identity (DevID) operating on 802.1X networks. In short, a DevID is composed of several X.509 certificates with their corresponding private keys and verification chains:

- IDevID: Initial device certificate issued by the device manufacturer PKI with a lifetime validity
- LDevID: operational certificate issued by the network commissioner (local PKI) the device connects to with a short validity (depending on network security policy)



Matter mirrors the architecture of 802.1AR:

802.1AR	Matter
IDevID	DAC
IDevID certificate chain	PAA-PAI-DAC Vendor PKI chain
Device manufacturer PKI	Vendor PKI
LDevID	NOC
Local network PKI	Operational PKI

The main difference resides in the fact that commissioning an 802.1AR device requires manually loading the OEM IDevID PKI Root CAs in both the device joining and the network admin appliance, whereas a Matter network will rely on a publication of the PAA in the DCL to check a new device.

Matter and ETSI EN 303 645

The ETSI EN 303 645 standard provides a set of baseline security recommendations applicable to all consumer IoT devices. It is intended to be complemented by other standards defining more specific provisions with fully testable and/or verifiable requirements for specific devices and markets.

Together, ETSI EN 303 645 and Matter provide both the high-level recommendations and the details necessary to implement cybersecurity in smart home devices. These can be distilled to the following guiding principles for security.

01 Build hardware which allows secure storage of sensitive security parameters

Although the Matter standard does not oblige vendors to build appliances using secure elements or secure MCUs, it highly recommends doing so to mitigate the risks of being copied/hacked.

02 Give devices unique, strong identities

This is explicitly covered by the obligation for a vendor to own, operate, and control their own Vendor PKI issuing the Device Attestation Certificates to be injected into every device at manufacturing, ensuring a trackable, trusted identity.

03 Ensure code integrity

Although Matter does not specifically require secure boots, measured boots, or firmware signature and verification, this optional implementation should not be mistaken for an opportunity to do nothing.

04 Communicate securely with other devices and servers

Matter defines and implements this as a requirement with Node Operational Certificates to secure the communications between devices, servers, and gateways, end to end.

05 Keep software and firmware updated

With the Cyber Resilience Act and its obligation to fix bugs and report weaknesses, implementing software and firmware over-the-air updates into Matter devices is a must. The Distributed Compliance Ledger keeps track of firmware changes on a device-per-device basis so that any Fabric Commissioner can check that their devices are running the software they should.

06 Upgrade security and renew certificates

Matter does not currently have any provisions for a security upgrade of its algorithms should ECC and ECDSA fall in the next decade. Nevertheless, the usage of long-lived Device Attestation Certificates is restricted to the minimum, whereas operational certificates used to effectively secure communication channels can be renewed at will.

07 Minimize exposed attack surfaces

This is a general recommendation when designing for security: always grant minimum privileges. The Access Control feature in Matter does just this: restricting access to a node's resources from other nodes to the bare minimum required to perform a global function.

08 Make systems resilient to outages

In the Matter standard, this is inherently covered by the self-healing IP networking layers supported, as well as the capability of a node to rejoin a Fabric or to keep a local connection running when internet access is unavailable.

09 Monitor system health

Vendors of Matter devices (including their suppliers of Matter chips, stacks, or subsystems) should have a public vulnerability reporting mechanism and policy for actively monitoring, identifying, and rectifying, in a timely manner, security vulnerabilities throughout the publicly stated security lifecycle policy of the product. Standard responsible disclosure guidelines allow vendors from 60 to 120 days to patch a vulnerability, but the implementation of such a program is at each vendor's discretion.

Conclusion

The expectation of technology for the home has shifted from just existing with proprietary communication, to the requirement of nearly full, seamless integration across brands and products, creating the smart home we've always wanted. With security now also on the minds of consumers, Matter seeks to be the de facto standard. The core of Matter security relies on certificates, digital identities, and signed code. But not all smart home vendors have the know-how to implement these new standards, which can jeopardize future sales.

Keyfactor offers the technology and expertise to implement Matter-compliant security for new and existing devices. With a full end-to-end solution from code signing to identity issuance and certificate lifecycle management, Keyfactor offers the ability to build flexible, scalable PKI and code signing solutions.

Scalable and flexible PKI

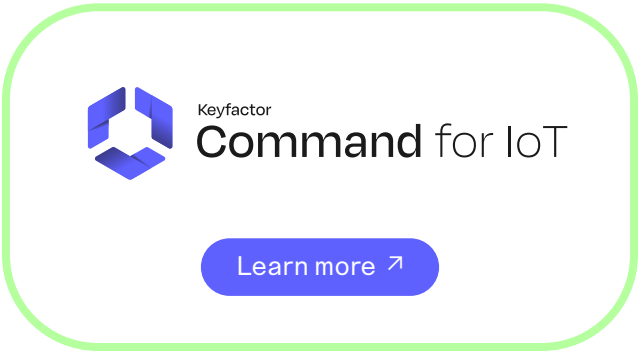
Using EJBCA Enterprise, a highly scalable and flexible PKI platform, security teams can issue trusted certificate-based identities to connected devices at a massive scale, whether during manufacturing or in the field. EJBCA PKI can be deployed within the data center, in the cloud, as a managed service, or even on the manufacturing floor.

Secure code signing

SignServer Enterprise digitally signs firmware and validates signatures to ensure only trusted code is executed on connected devices and systems. The solution can leverage your existing on-premises or cloud-based hardware security module (HSM) or use a built-in HSM with a turnkey hardware appliance.

Certificate lifecycle automation

Combined with Command for IoT, manufacturers get complete visibility and lifecycle management of all keys and certificates issued in their infrastructure and on their devices, allowing teams to revoke, renew, and re-issue millions of certificates in bulk from a single platform to ensure identities remain secure over the device's lifespan.



Want more information about Keyfactor for smart home cybersecurity?

Learn more ↗

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed. For more, visit keyfactor.com or follow @keyfactor.

Contact us

- www.keyfactor.com
- +1 216 785 2946 (North America)
- +46 8 735 61 01 (Europe)