MATTER – MAKING SMART HOMES MORE SECURE

Networked electronic products make homes more convenient, comfortable, safe, efficient, and enjoyable. Unfortunately, every connected device has the potential to open a back door for unauthorized network access, device hijacking, personal information exposure, data breaches, and bogus sensors and actuators. Increasingly aware of these vulnerabilities, consumers are asking questions like these:

- Who can listen to audio from this smart speaker?
- Can someone on the Internet view video from this camera?
- Can hackers access my home network through this smart dishwasher?
- With access to my home network, can hackers control my devices?
- Can the manufacturer update this product to patch security problems?

Security and confidentiality concerns influence purchase decisions and affect brand reputations. Manufacturers must address these issues head-on by making connected devices increasingly safe, secure, and private with each new product generation.

Matter, a new smart home standard from the Connectivity Standards Alliance (CSA), defines the next generation of consumer electronics (CE) connectivity. This new industry-standard protocol seamlessly interconnects smart home devices and applications from multiple manufacturers over networks that already exist in most homes. Backed by some of the biggest names in consumer electronics, Matter promises universal product interoperability, better user experiences, and secure, reliable connectivity. "Matter – Making Smart Homes Smarter" provides a detailed explanation of Matter — what it is, how it works, and why it's essential to the consumer electronics industry. Matter is poised to accelerate smart home growth, but only if consumers are confident that new devices are secure and trustworthy.

Is Matter "secure enough?" In other words, are homes with a large and rapidly growing set of Matter-connected CE products more secure and private than today's smart homes with a hodgepodge of non-interoperable connectivity schemes? To find out, we researched Matter's security and privacy and summarized our findings in the first two sections of this paper. Because Matter security is built-in, not added-on, we then looked at the security aspects of Matter product design, manufacturing, and deployment. Finally, we evaluated the practicality of building secure Matter products within existing CE supply chains. We used NXP Semiconductor's extensive Matter portfolio to show

how Matter-enabled chips, software, and services combine to make Matter product development fast and efficient.

MATTER SECURITY OVERVIEW

Security and privacy are fundamental Matter design tenets — built into the specification from the start. Standardized, proven, widely deployed security technologies from PC, mobile, and cloud platforms are at the core of these specifications. Matter adapts these mainstream techniques for consumer products in residential environments. This approach ensures that Matter security is comparable to the devices we use daily for communication, e-commerce, work, and entertainment.

Matter takes a layered approach to security, starting with robust, certified, trustworthy devices. These devices connect securely with existing wireless networks and communicate with other Matter devices using encrypted messages. Matter products are easy for consumers to set up and use, cryptography is modular so that algorithms can change as security technologies evolve, and over-the-air updates extend product life.

This layered approach is key to understanding Matter security — *trustworthy devices* communicating over *secure networks* using *protected messages*. In this section, we walk through these three layers to see how Matter security principles apply.

TRUSTWORTHY DEVICES

A smart home is only as trustworthy as its least secure devices. Matter raises the bar on device security by establishing comprehensive technical specifications that ensure all devices are trustworthy by design. Matter product certification testing enforces compliance with these specifications by verifying that products are functionally secure and interoperable across manufacturers. Let's look into Matter device security in detail to see how it works.

Industry-standard cryptography

Matter adapts broadly deployed, industry-standard security technologies for use in embedded devices. For example, device identity confirmation uses public key infrastructure (PKI) with NIST P-256 elliptic curve cryptography. Devices encrypt all messages with the industry-standard AES block cipher. Matter uses Symmetric Password-Authenticated Key Agreement (SPAKE2+) to establish initial communication with new devices. These and other proven, globally deployed, broadly supported cryptographic technologies provide a solid foundation for Matter security.

Certification

The Matter logo on a product means it has passed tests by independent, accredited labs confirming compliance with Matter specifications and verifying multivendor interoperability. The logo assures consumers that products are functionally secure, easy to install, and interoperable with other Matter products.

Certification is also a prerequisite for inclusion in the CSA's Distributed Compliance Ledger (DCL). This blockchain-based distributed database lists the certification status and roots of trust for all Matter products, plus other information helpful in updating and maintaining device firmware. After a test lab successfully tests a new product, the CSA issues a Certification Declaration certificate (CD) and updates the DCL with a unique Certification Declaration ID. When a consumer installs a new Matter device, its CD ID must match the corresponding entry in the DCL, confirming its certification status.

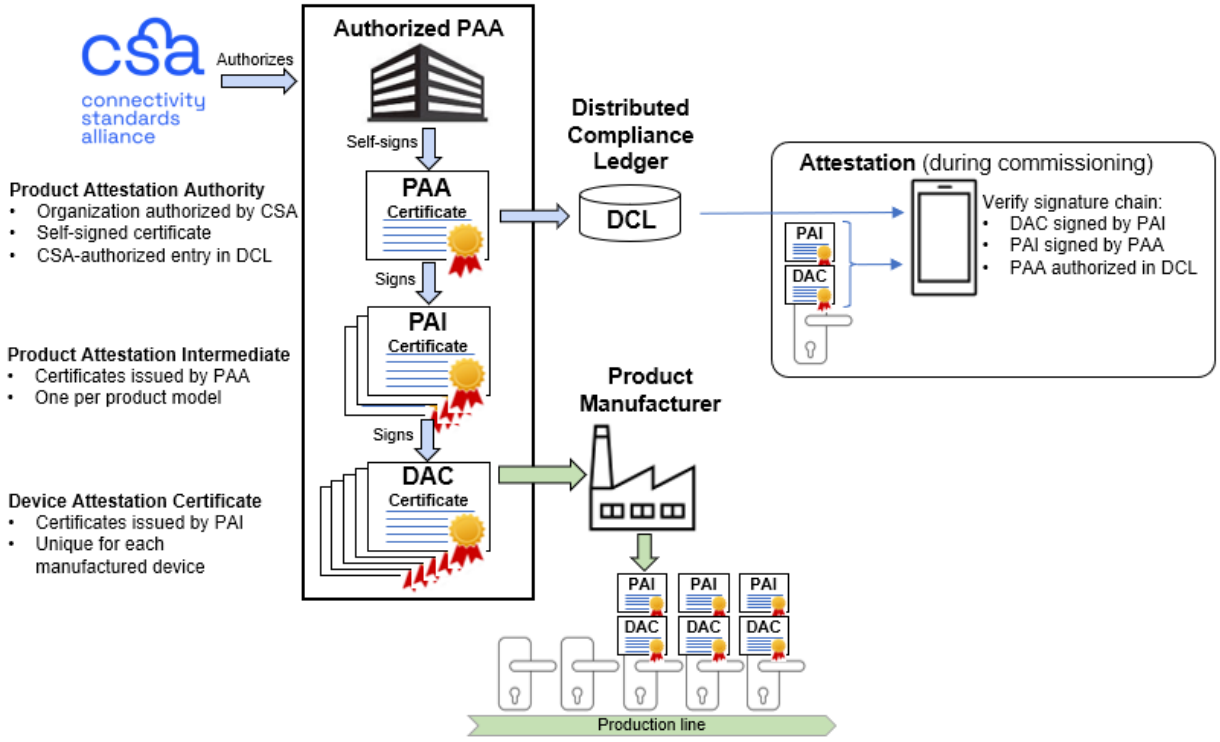
Unique device credentials

Consumers expect smart home devices to work "right out of the box" with little or no user intervention. Users don't like typing in credentials, pressing buttons in mysterious sequences, interpreting LED blink codes, or using unique apps to set up each device. Users want to install new devices with a single tap on a mobile device, and that's how Matter works. Easy installation requires built-in credentials that prove each device is genuine, made by an accredited manufacturer, and certified Matter compliant.

Manufacturers inject every device with immutable, cryptographically verifiable credentials that attest to its authenticity. Matter does this with a Device Attestation Certificate (DAC) signed by a Product Attestation Authority (PAA), a company authorized by the CSA to issue Matter device root certificates. PAAs are typically silicon suppliers, device manufacturers, or other companies in the device supply chain. PAA security requirements are stringent because the DAC establishes device trust. Specifically, the PAA is the root of the DAC certificate chain shown in Figure 1. These signatures attest to the authenticity of a device's manufacturer and certification status. The PAA signs a Product Attestation Intermediate (PAI) certificate for each product. Then, the PAI creates and signs a unique DAC certificate for every device.

Although the DAC validates the device's manufacturer and certification status, copying a DAC to a bogus device is technically possible, so how do we know that a device is genuine? In addition to the DAC, manufacturers provision each device with a unique private key. The corresponding public key is tied to the device-specific DAC, guaranteeing that it applies only to that specific device.

FIGURE 1: DEVICE ATTESTATION CERTIFICATE CHAIN



Source: Moor Insights & Strategy

Attestation

We'll cover attestation in detail in the upcoming "Commissioning" section, but here's an overview. When adding a new product to a Matter network, a commissioner (typically a smartphone) retrieves the DAC and the PAI from the device and validates the signatures. The commissioner verifies PAA authenticity by checking its certificate in the DCL (or a cached copy). Next, the commissioner retrieves the Certification Declaration (CD) from the device, verifies that the CSA signed it, and checks for a corresponding CD ID in the DCL. Finally, the commissioner confirms the device's authenticity by challenging it to prove possession of the private key corresponding to the public device key in the DAC.

Resilience, agility, and longevity

Products like lighting systems, HVAC equipment, thermostats, irrigation controllers, large AV devices, and major appliances have long lifespans. After installation, consumers expect these products to operate reliably for many years – decades in some cases. Consumers won't tolerate lifespan reductions or additional maintenance costs as these products become Matter-enabled. The Matter specifications enhance product

longevity by enabling over-the-air firmware updates, modular cryptography primitives, and the updateable Distributed Compliance Ledger.

Firmware updates – Matter cannot specify how to update device firmware – only manufacturers can do that. Matter provides mechanisms to inform devices about available firmware versions, obtain user permission to initiate updates, and deliver updated code over Matter device networks. Matter also specifies how to use the Distributed Compliance Ledger for managing firmware update metadata, such as the latest firmware version ID for a specific type of device. The objective is to use the same firmware update request and delivery workflow for all devices, regardless of manufacturer.

Modular cryptography – New threats sometimes require new security algorithms, so cryptography evolves continuously. The Matter core specification allows modular addition of cryptographic primitives without widespread implementation changes. Matter also allows using new devices with updated security alongside older ones on the same network, using the best security available across all devices in an "operational group." Matter operational groups define logical sets of nodes that share a common security domain. Operational group keys have a "group security info" value to specify the type of operational group keys. This approach allows new devices to upgrade security mechanisms without breaking compatibility.

DCL – The CSA's blockchain-based Distributed Compliance Ledger is a repository where device manufacturers, vendors, test houses, and certification centers distribute device information. The DCL is a central "source of truth" regarding vendors, devices, device models, and certifications. Future versions may include information about measured boot, software maintenance, and firmware updates. Storing detailed device information in a distributed, queryable, universally accessible database provides considerable security agility and is essential for product longevity.

Secure Networks

Matter currently supports two types of wireless networks – Wi-Fi and Thread. We'll cover network setup in the section on commissioning, but from a user's point of view, configuring a Matter device to join these networks is almost entirely automatic.

Wi-Fi and Thread are secure IPv6 networks that already encrypt over-the-air data. Matter adds another layer of security on top of network-level security to prevent unauthorized devices on the same network from communicating with Matter nodes. Please refer to the "Matter data protection" section for details.

PROTECTED DATA

Matter specifications address data protection within Matter networks. However, these specifications do not extend to higher-level home automation ecosystems that utilize Matter devices. Matter is ecosystem-independent, so consumers may choose from several providers. Here's an overview of data protection on Matter networks and higher-level automation ecosystems.

Matter data protection

Matter encrypts all network communication with symmetric (AES) session keys. The key negotiation process between Matter nodes is comparable to the certificate-based TLS sessions we use daily to view secure websites, indicated by the lock symbol on your browser's URL line. In both cases, each endpoint uses public key cryptography to authenticate the other and agree on a shared key for efficient (symmetric) encryption during a connection session.

Matter symmetrically encrypts unicast messages from node to node and multicast messages within a group of nodes. The standard defines three multicast groups (all nodes, all non-sleepy nodes, and all proxies), and it's easy to set up others, such as "all lights" or "all outside lights." Each unicast or multicast (group) message has a unique session key, ensuring that only intended recipients can decrypt a message.

Home automation (cloud) ecosystem data protection

Smart speakers, smartphone apps, hubs, and other interactive products from home automation ecosystems such as Amazon Alexa, Apple HomeKit, Google Home, and Samsung SmartThings make great Matter controllers. However, Matter specifications don't extend to these ecosystems. For example, when using a smart speaker to control lighting with Matter, the voice recognition application and the logic to translate spoken language into Matter messages are not governed by Matter specifications. Each smart home ecosystem defines its own security and privacy technologies and policies. So, if you trust your smart home ecosystem, you should still trust it as you add Matter devices. Matter is vendor independent, so you can switch ecosystems or add new ones anytime.

Consumers can use more than one Matter-enabled home automation ecosystem. Each ecosystem acts as a Matter Administrative Domain Manager (ADM, or "Admin") and forms a Matter "fabric" with any or all of the home's Matter devices. For instance, both Alexa and HomeKit can control a home's Matter devices. Each ecosystem functions as

an ADM, creating its own Matter fabric with a unique root of trust. Matter refers to this feature as "multi-admin."

Although multi-admin provides users with considerable configuration flexibility, adding a new ADM requires re-installing existing devices on the new fabric. The process is almost identical to the initial installation, but an existing ADM must authorize the installation and generate a new device commissioning passcode. Using a device's original public passcode (i.e., a QR code) would allow anyone passing through a house to add devices to a new fabric without the owner's authorization, so an existing ADM must generate a new code and put the device in pairing mode. Multi-admin device management can be confusing and tedious, especially for large installations, and it's not standardized. Matter's scope is limited to the Matter network, so it's up to the ecosystem vendors to make multi-admin practical, consistent, secure, and easy for consumers to set up.

PRIVACY

The security pillars described above – certified devices, authenticated using asymmetric cryptography, communicating via symmetric encryption – support Matter's three privacy principles:

1. **Share a minimum amount of data with every transaction.**
   Matter interactions send the minimum amount of data required for operating the Matter protocols. Minimizing the information shared between nodes reduces the potential for information leakage.
2. **Communicate only with a defined purpose.**
   Matter specifications require a defined Matter-related purpose for all shared information. Data related to higher-level device operations above the Matter protocol layer is not within Matter's scope.
3. **Prevent IP address and device ID eavesdropping.**
   The core Matter specification incorporates many privacy-preserving features, such as non-trackable IP addresses, sessions with private message headers, random node IDs, and encrypted node IDs.

In the previous section, we explained that Matter security specifications do not extend into the domain of home automation ecosystems. The same limitation applies to privacy. However, Matter does allow consumers to choose which automation ecosystems to deploy. Security breaches and privacy leaks have severe brand reputation consequences, so competitive pressures motivate ecosystem providers to

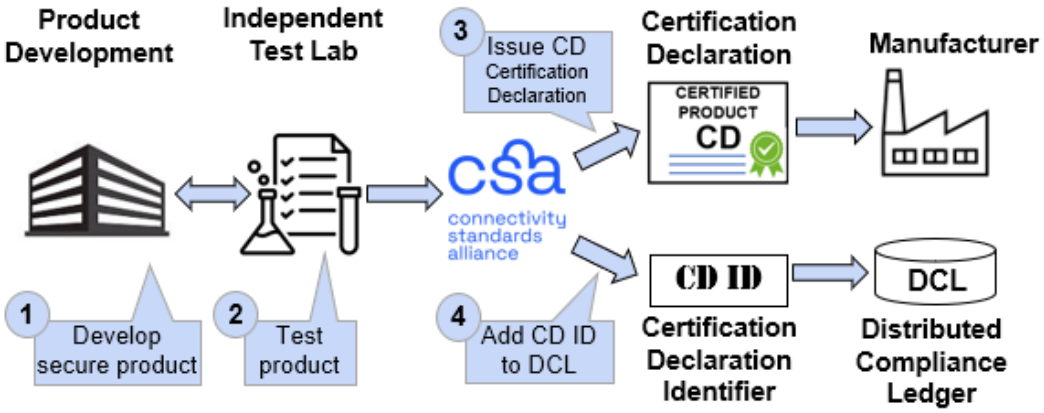
protect customer information that travels beyond Matter's scope. Let's all watch carefully to make sure they do.

MATTER COMMISSIONING – ASSURING CERTIFIED, GENUINE DEVICES

The previous section of this paper presented an overview of Matter security specifications – devices, networks, data, home automation ecosystems, and privacy. Formal certification assures consumers that all products with Matter logos are functionally trustworthy. However, when installing a new device on a home network, how does a consumer know the device is genuine and certified? That's the job of Matter's commissioning process.

Commissioning depends on two pieces of information baked into each product – the CD and the DAC. These certificates are the "passports" that allow devices to join Matter fabrics. The following sections explain how product companies obtain CDs during development and inject unique DACs into each device during manufacturing. The DAC and CD combine to automate the commissioning process during device installation.

FIGURE 2: MATTER PRODUCT CERTIFICATION PROCESS FLOW



Source: Moor Insights & Strategy

CERTIFICATION PROCESS

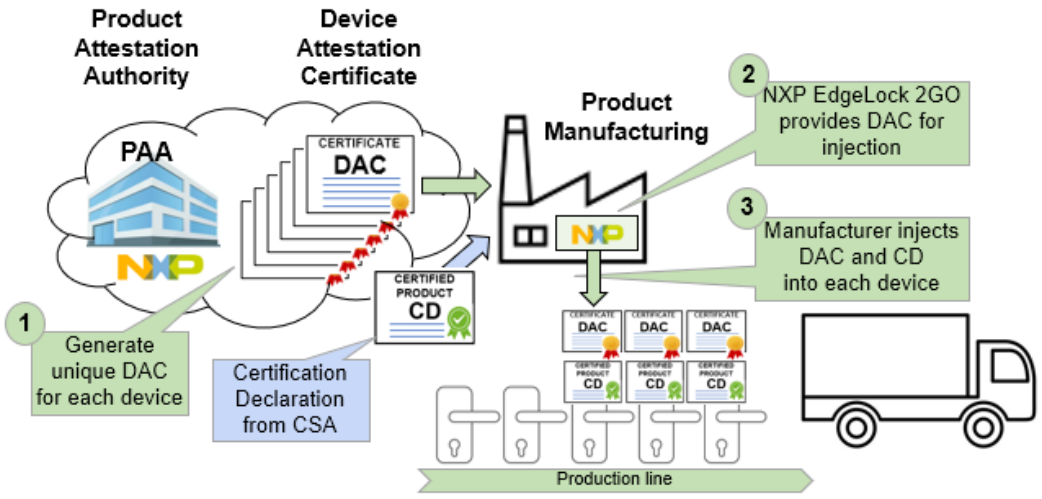
Figure 2 illustrates the certification process flow. The CSA authorizes a global network of independent laboratories to test products for compliance with Matter specifications. When a product passes all tests, the labs notify the CSA. After verifying the test results from the lab and reviewing conformance documents provided by the manufacturer, the CSA issues a CD certificate for injection into each manufactured device. The CSA also

updates the DCL with a corresponding CD ID record, later used to confirm the authenticity of the device's CD.

DAC Certificates (in Each Device)

As previously explained in the "Unique device credentials" and "Attestation" sections, manufacturers inject a unique DAC into each device. Figure 3 summarizes the process. In this example, NXP is the PAA, and the manufacturer uses NXP EdgeLock® 2GO to inject the credentials. The PAA generates unique DACs for each device. During manufacturing, EdgeLock 2GO downloads the DACs and provides them to the manufacturer for production-line injection.

Figure 3: Matter Product Manufacturing



Source: Moor Insights & Strategy

Another alternative not shown in Figure 3 is for a silicon provider such as NXP to pre-inject the DAC into Secure Elements or Secure Authenticators during chip fabrication. This method simplifies device manufacturing by eliminating the need for secure DAC download and injection. This method best suits high-volume production because it requires vendor-dependent chip SKUs.

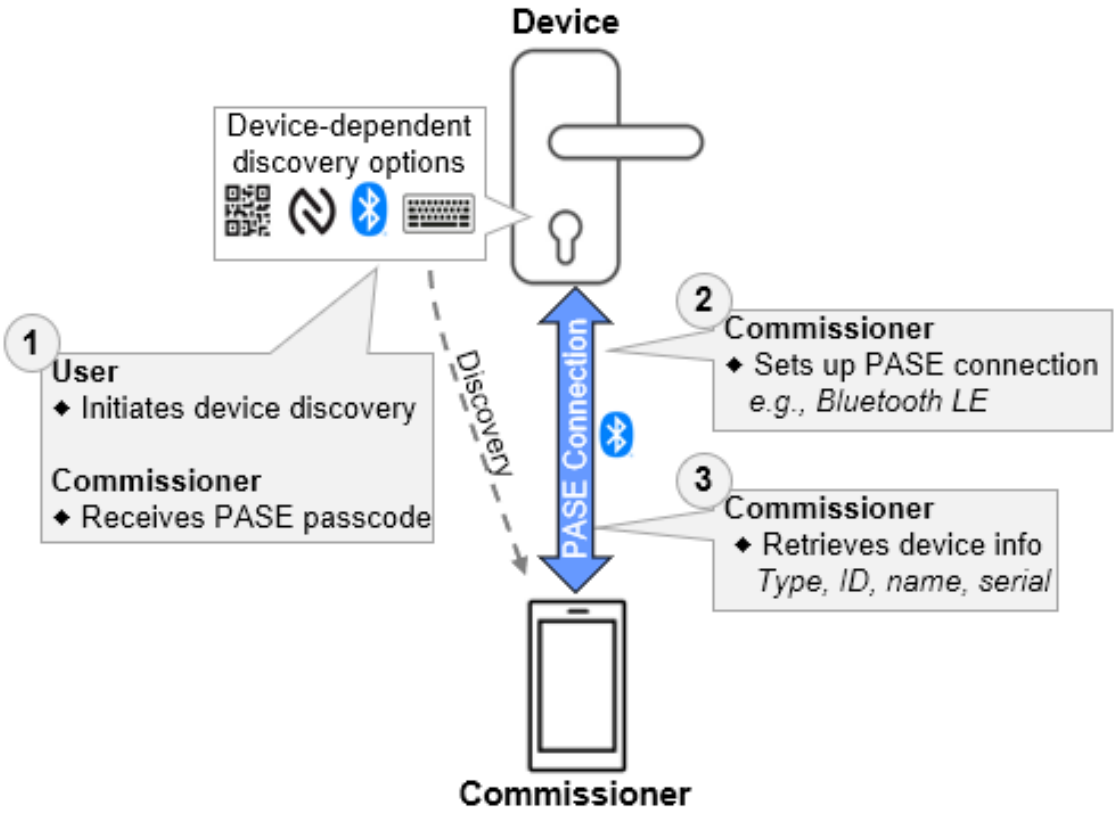
Matter Device Commissioning

In this section, we cover the device commissioning (installation) process in detail, showing how the DAC and the CD, combined with the device's private key, convey the chain of trust that proves each Matter device is genuine and trustworthy.

Matter's commissioning process ensures that every device on a Matter network conforms to the security specifications outlined in the previous sections of this paper. Commissioning is technically complicated but operationally robust and easy for consumers to manage. The user identifies the device (e.g., QR code or NFC) and authorizes the installation – that's it! Everything else is automatic, based on the DAC and the CD.

The consumer installs the new device using a Matter "commissioner," typically a smartphone with a Matter-enabled app from a home automation ecosystem such as HomeKit, Google Home, Alexa, or SmartThings. Each such ecosystem is a Matter Administrative Domain Manager (ADM) – a root certificate authority authorized by the CSA to create and manage Matter network fabrics.

FIGURE 4: STAGE 1 – DISCOVERY AND INITIAL CONNECTION



Source: Moor Insights & Strategy

The Matter commissioning process progresses through four stages. First, the commissioner opens a temporary out-of-band connection to the new device (e.g.,

Bluetooth LE). Then, it performs Matter device attestation by retrieving the DAC ("passport") from the device, unpacking its certificate chain, confirming that a valid PAA signed it, and checking the DCL to see if the device type is certified. If the device is genuine and certified, the commissioner then provisions the new device to join the local network and the Matter fabric. In the final stage, the commissioner discovers the new device on Matter fabric, and the commissioning session ends.

The commissioning procedure differs slightly for "multi-admin" situations where users create an additional Matter fabric (administrative domain). In this case, the existing ADM puts the device into pairing mode, and the new domain's commissioner connects to the device with IETF DNS-SD instead of Bluetooth LE.

Here's an outline of these four commissioning stages. The consumer begins by powering up a new Matter device for the first time.

In Stage 1, the commissioner initiates an out-of-band commissioning session with the new device.

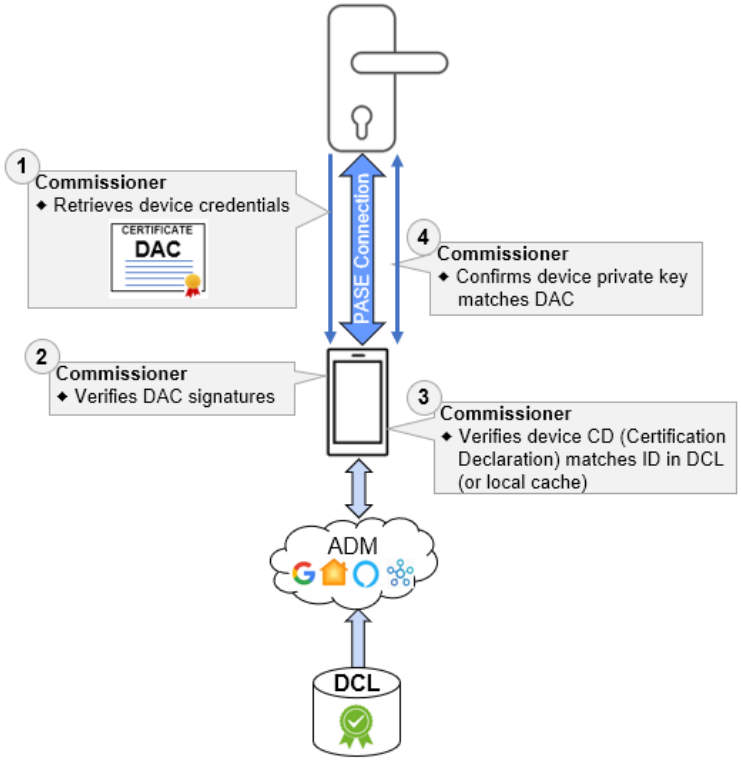
1. **Device initiates discovery**
   - The device advertises itself to the commissioner – a smartphone in this example. The advertisement includes a passcode that the commissioner uses to set up a temporary connection.
   - The device may advertise its passcode in several ways such as QR code, NFC, Bluetooth LE, Wi-Fi soft AP, or manual code entry.
   - The passcode proves physical possession of the device and authenticates an out-of-band commissioning session in the next step. The passcode plays no other role in Matter.

2. **Commissioner connects to device, typically via Bluetooth LE**
   - The commissioner uses the advertised passcode to establish an out-of-band commissioning session with the device through a secure process called Passcode Authenticated Session Establishment (PASE). In our example, this connection is over Bluetooth LE.
   - The commissioner arms a fail-safe mechanism in the device so that if the commissioning process fails, the device reverts to its original state.

3. **Commissioner retrieves device information**
   - The commissioner uses the new device PASE connection to read basic onboarding information from the device, including the type of device, vendor ID, product ID, product name, and serial number.

4. **Commissioner configures device**
   - The commissioner configures the device's regulatory situation, i.e., location and country code. (Figure 4 does not illustrate this step.)

FIGURE 5: STAGE 2 – ATTESTATION

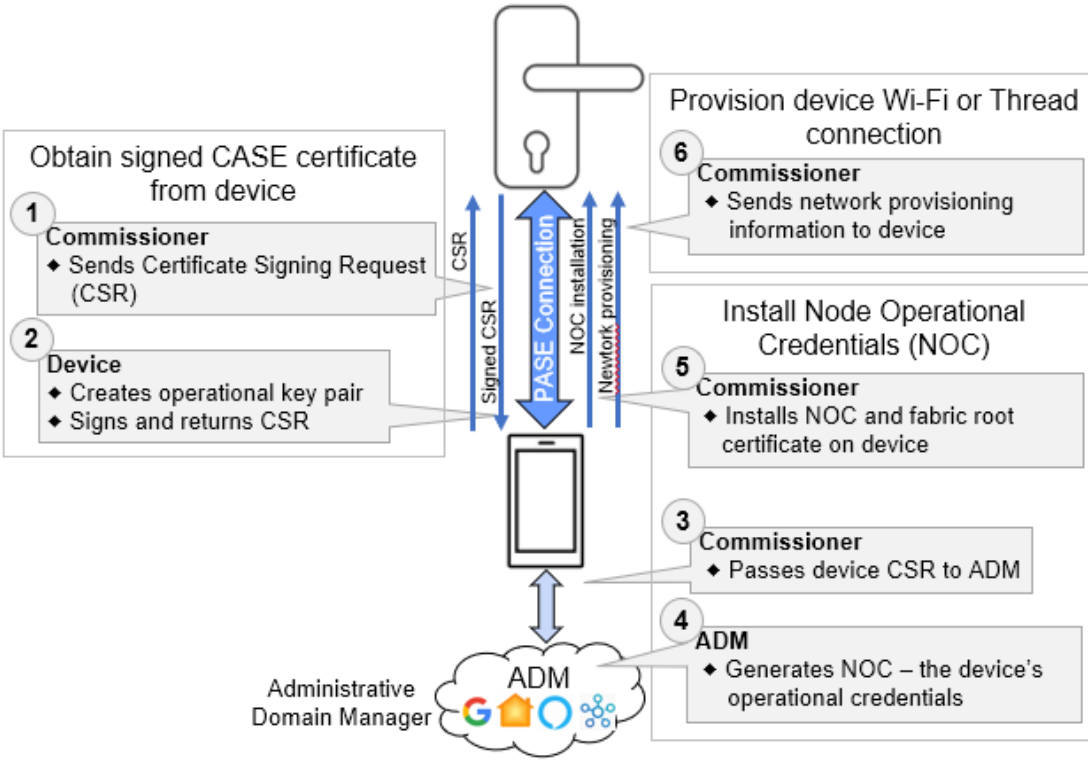


Source: Moor Insights & Strategy

In Stage 2, the commissioner validates the device's attestation credentials.

1. **Commissioner retrieves device attestation credentials**
   - Credentials include the device's DAC and PAI certificates.
2. **Commissioner verifies signatures**
   - The commissioner confirms the DAC's signature chain – i.e., an approved PAA signed the credentials of the PAI that signed the DAC.
3. **Commissioner checks the device's certification status**
   - The identity of the CD on the device must match the corresponding entry in the DCL.
   - The commissioner may use any reasonable method for checking certification status. For example, the CD IDs may be cached in the ADM's cloud service or within the commissioner application.
4. **Commissioner verifies that the DAC matches the device**
   - The device's private key (exists only within the device) must match the public key in the DAC.
   - The commissioner uses the device's attestation public key to issue a challenge request.
   - The device signs its challenge response using its attestation private key.
   - The device is genuine if the commissioner can verify the signature of the response with the device's public key.

FIGURE 6: STAGE 3 – PROVISIONING



Source: Moor Insights & Strategy

Stage 3 sets up credentials for joining the Matter fabric and the home network.

1. **Commissioner obtains a signed CASE certificate from device**
   - Matter uses the Certificate Authenticated Session Establishment (CASE) protocol for device-to-device communication over the home network. Setting up devices for CASE communication is the ultimate goal of the commissioning process.
   - The commissioner sends a certificate signing request (CSR) to the device.

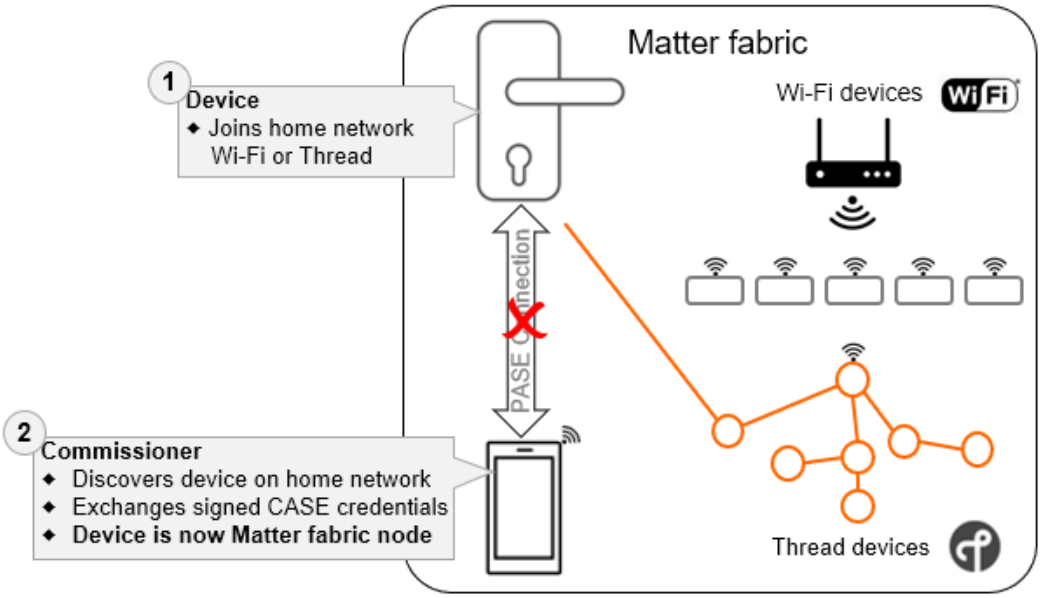
2. **Device creates unique operational key pair; returns CSR**
   - The device sends the signed CSR information back to the commissioner.
   - The commissioner later uses this key pair to establish routine communication over the home network.

3. **Commissioner passes the device's CSR to its ADM**
   - The commissioner app is a local agent of its ADM. The ADM acts as the root certificate authority (CA) for the consumer's Matter network fabric, generating the operational certificates that authorize devices to participate in the fabric.

4. **ADM generates a trusted Node Operational Certificate (NOC)**
   - These are the device's operational credentials.

5. **Commissioner installs Matter fabric root certificate and NOC on device**
6. **Provision device Wi-Fi or Thread network connection**
    - The commissioner usually has the home's Wi-Fi and Thread wireless network credentials (i.e., Wi-Fi SSID and WPA password). Matter automated device network provisioning by providing these credentials to new devices.
    - The commissioner sends network provisioning information to the device.

FIGURE 7: STAGE 4 - DEVICE JOINS MATTER FABRIC



Source: Moor Insights & Strategy

In Stage 4, the device becomes a member of the Matter fabric.

1. **Device connects with home network**
    - The device connects to Thread or Wi-Fi using the credentials provided in the previous step.
2. **Commissioner discovers device on home network; establishes CASE network session.**
    - Until now, the commissioner and the device have used the PASE-authenticated, out-of-band Bluetooth LE connection established in Stage 1.
    - The commissioner uses multicast DNS (for Wi-Fi) or DNS-SD (for Thread) to discover the device's new IP address and port.
    - The commissioner and the device exchange the signed CASE credentials, enabling the device to participate in the Matter fabric.
    - Routine communication over the home network begins, and the Bluetooth LE connection ends.
3. **Commissioning session ends**

- The device is now a member of the Matter fabric.
- The commissioner uses CASE to send the "Commissioning Complete" command to the newly commissioned device, which disarms its fail-safe timer. Commissioning is complete, and the device is a member of the Matter fabric.

DEVELOPING AND MANUFACTURING SECURE MATTER DEVICES

Security is integral to every Matter product. This section covers the five essential development and manufacturing elements that ensure that every Matter device is secure and easy for consumers to install:

1. **Secure silicon** – The foundation of Matter security
2. **Secure software** – Broadly deployed, open-source Matter implementations
3. **Product certification** – Proven compliance with Matter specifications
4. **Device provisioning** – Factory-installed device attestation credentials
5. **Long-term support** – Satisfy consumer product longevity expectations

SECURE SILICON

Matter software runs on two types of computing platforms – microprocessors (MPUs) and low-power microcontrollers (MCUs). In both cases, manufacturers require highly integrated, low-cost SoCs with all the function blocks needed to implement Matter, including processing, memory, storage, wireless networking, I/O, and security. Matter security depends on four silicon-enabled capabilities:

- **Secure storage** – Protect credentials in an enclave or Secure Element
- **Secure computation** – Protect processing of private data
- **Crypto accelerators** – Required for low-power applications
- **True random-number generator** – Enable trustworthy cryptography

Recently, NXP and other semiconductor companies introduced Matter-ready chips integrating almost all the functions developers need to build secure Matter products. These highly integrated SoCs are complete platforms capable of running certifiably secure Matter software stacks with few external components and minimal product-specific customization. We'll present examples of Matter-ready NXP chips in the upcoming "NXP Accelerates Matter" section.

SECURE SOFTWARE

Matter platform software is complicated. It's a deep stack with a complete Matter implementation, security protocols, OS, board support packages (e.g., boot, drivers,

debug, and tools), networks (OpenThread or Wi-Fi), software update procedures, and dozens of other packages.

Instead of customizing, porting, and testing the whole stack, developers can use a prototyping platform with a complete, thoroughly tested Matter software implementation. Downloading the whole platform-specific stack from GitHub® reduces risk and time-to-market, and it's a big reason we at Moor Insights & Strategy are bullish on Matter. Developers have a whole industry behind them, providing Matter-ready chips, boards, and software. It's surprisingly easy to get the whole Matter stack up and running quickly by following cookbook-like procedures with little or no system-level coding. Application development often begins a day or two after obtaining a prototyping kit.

PRODUCT CERTIFICATION

Matter certification confirms compliance with CSA specifications, indicates interoperability with other Matter products, allows products to use CSA logos, lists the products on the CSA website, and grants the CD required to join Matter networks.

Independent labs test for Matter protocol conformance and check "dependent" network certifications (i.e., Thread and Wi-Fi). Matter testing is thorough, so manufacturers are highly motivated to minimize risk, cost, and time. The best way to streamline the process is to use hardware and software components that have already been successfully certified in other Matter products. NXP and other semiconductor companies offer Matter-ready platforms with conformant protocols, security components, network stacks, and radio subsystems. The certification path for products based on these platforms is smooth and well-marked – and a much better option than blazing a new trail with custom mashups.

DEVICE PROVISIONING

Matter product manufacturers must factory-install security information into every device to attest that it is genuine, certified, and trustworthy. The automated commissioning process previously described validates these credentials and provisions the operational certificates that enable network participation.

Automated commissioning requires three significant manufacturing steps:

- **Certification** – All Matter products must demonstrate compliance with Matter specifications.
- **DAC creation** – An authorized PAA generates a unique DAC for each device.

- **Credential injection** – Manufacturers inject the unique DAC into each device, along with the CD, a unique private device key, and a random commissioning passcode for the initial out-of-band PAKE connection (unless the device dynamically generates the passcode).

Generating and managing DACs is a surprisingly onerous process. The DAC is the root of trust for each device, and only CSA-authorized Product Attestation Authorities (PAAs) may generate them. As root certificate authorities (CAs) for Matter devices, PAAs are the linchpins of device trust, so the CSA defines strict requirements for this vital role. Becoming a PAA requires costly and ongoing security and privacy protocols, operational controls, physical security, and regular audits. Most product manufacturers should outsource this function to vendor-independent (non-VID Scoped) PAAs that generate DACs for multiple manufacturers. NXP offers a comprehensive service for managing this process, which we'll cover in the "Manufacturing Matter Products – EdgeLock 2GO" section.

NXP Accelerates Matter

The first three sections of this paper introduce Matter's security architecture, explain the commissioning (onboarding) process, and outline requirements for developing and manufacturing secure devices. When learning about Matter, many product companies find the overall development and certification process complicated and often daunting. However, Matter is an industry-standard specification with open-source implementations, so product companies don't have to start from scratch. Silicon and platform vendors offer Matter-ready hardware, software, and services that are easy to productize. This section examines NXP's Matter portfolio, showing how Matter-enabled chips, development kits, software, and services combine to simplify and accelerate product development.

NXP has deep Matter expertise. Over ten years ago, Freescale was among the first semiconductor companies to actively develop and promote universal, IP-based embedded device connectivity – a disruptive concept at the time. Consistent with this vision, the company co-founded the Thread Group in 2013, bringing secure IP networking to low-power, consumer-friendly embedded devices. After merging with NXP in 2015, the company remained committed to IP networking and doubled down on Thread support in its product portfolio. In 2019, NXP partnered with other industry leaders to create "Project Connected Home over IP," later named Matter.

Today, NXP continues to invest heavily in the industry standards that make secure, open, interoperable device communication possible – and in a product portfolio that makes it practical. Matter security and privacy are critical success factors, so let's look at NXP's Matter portfolio from a security point of view.

NXP Matter-Ready SoCs, Software, Services

NXP is "all-in" on Matter, offering Matter-enabled silicon ranging from coin-cell powered microcontrollers (MCUs) to advanced microprocessors (MPUs) with AI and graphics. This section focuses on three Matter-enabled SoCs – the K32W148 MCU, the i.MX™ 8M Mini MPU, and the new i.MX™ 93 MPU. We'll outline NXP's hardware security options for Matter, show the security features of each chip, and show how NXP supports product developers with secure Matter software components, prototyping hardware, and EdgeLock 2GO services.

NXP Matter-Ready Security

NXP offers two Matter-ready hardware security options: a secure enclave built into the SoC and an external Secure Element or Secure Authenticator chip.

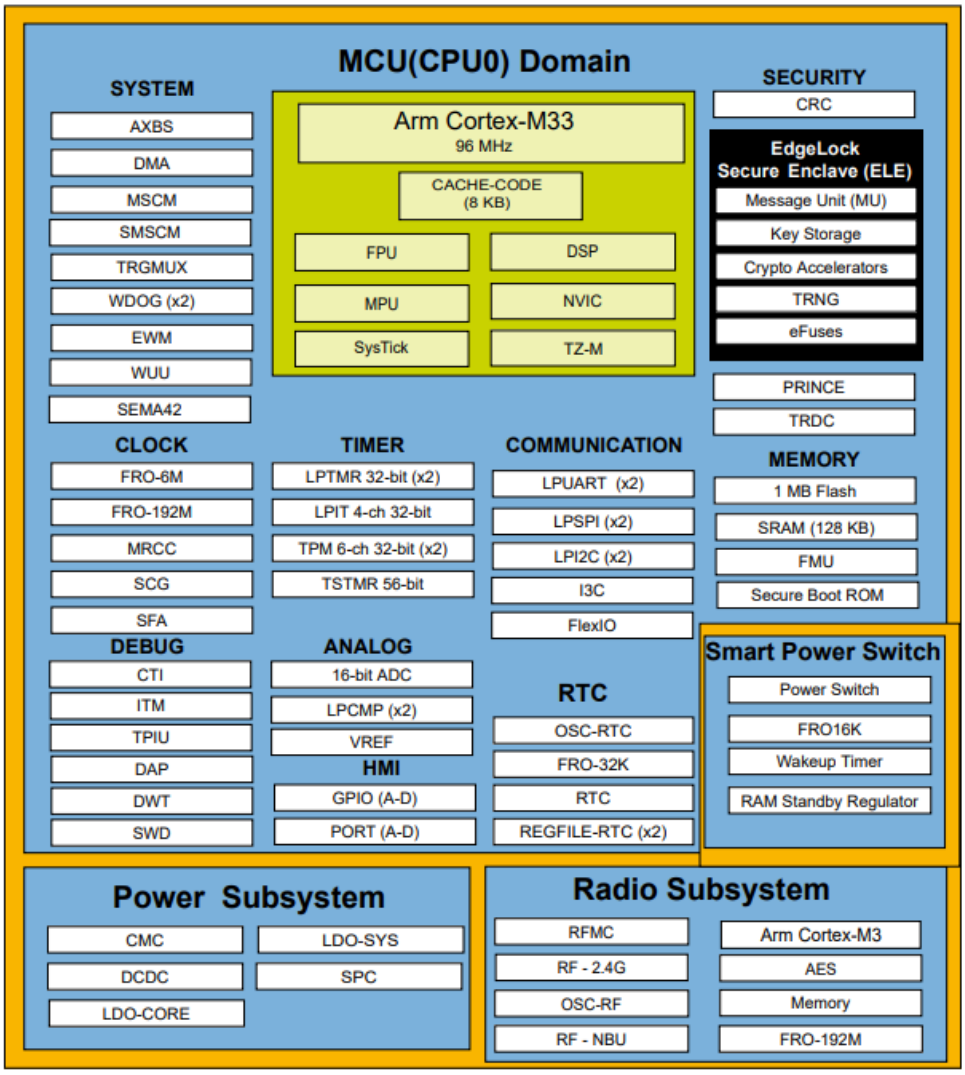
A Secure Enclave is an isolated security subsystem integrated into an SoC. Enclaves in the K32W148 and i.MX 93 provide the required Matter hardware security capabilities – credential protection, secure computation, crypto acceleration, and "true" random number generation. This integrated solution also supports NXP EdgeLock 2GO Matter security services.

NXP's EdgeLock SE05x Secure Element and A5000 Secure Authenticator components provide additional capabilities beyond the basic Matter requirements. For example, these chips have Common Criteria EAL 6+ certification for protection against advanced hardware attacks. But for many manufacturers, the most compelling benefit is support for NXP's EdgeLock 2GO pre-injection option, which installs Matter attestation keys and certificates into the secure storage of the chip before delivery to the device manufacturer, thereby eliminating secure credential delivery from the production line. The chips are small (3mm x 3mm) and use a simple I2C connection for integration with the host MCU or MPU. Different variants of these products are available, such as the new EdgeLock SE051H with complete support for Matter cryptographic functions such as SPAKE2+. This variant also has NFC capabilities for device discovery – a better option than QR codes for many applications.

K32W148 Matter-Enabled Low-Power MCU

NXP's K32W148 is an MCU-based SoC suitable for a broad spectrum of sensing and control applications. It's Matter-ready, with built-in Thread and Bluetooth LE networking. The required hardware functions for Matter security are on-chip, including an isolated EdgeLock secure Enclave (ELE).

Figure 8: K32W148



Source: NXP

The ELE (highlighted in black in Figure 8) includes hardware cryptographic accelerators, a random number generator, key generators, key storage, secure debug, and optional Flash memory encryption. These functions are sufficient for Matter, but

developers can use an external EdgeLock SE05x Secure Element or EdgeLock A5000 Secure Authenticator for enhanced security. All options support NXP's EdgeLock 2GO credential delivery and injection service, and the SE05x/A5000 offer pre-injection in the silicon fab.

FIGURE 9: K32W148-EVK EVALUATION KIT

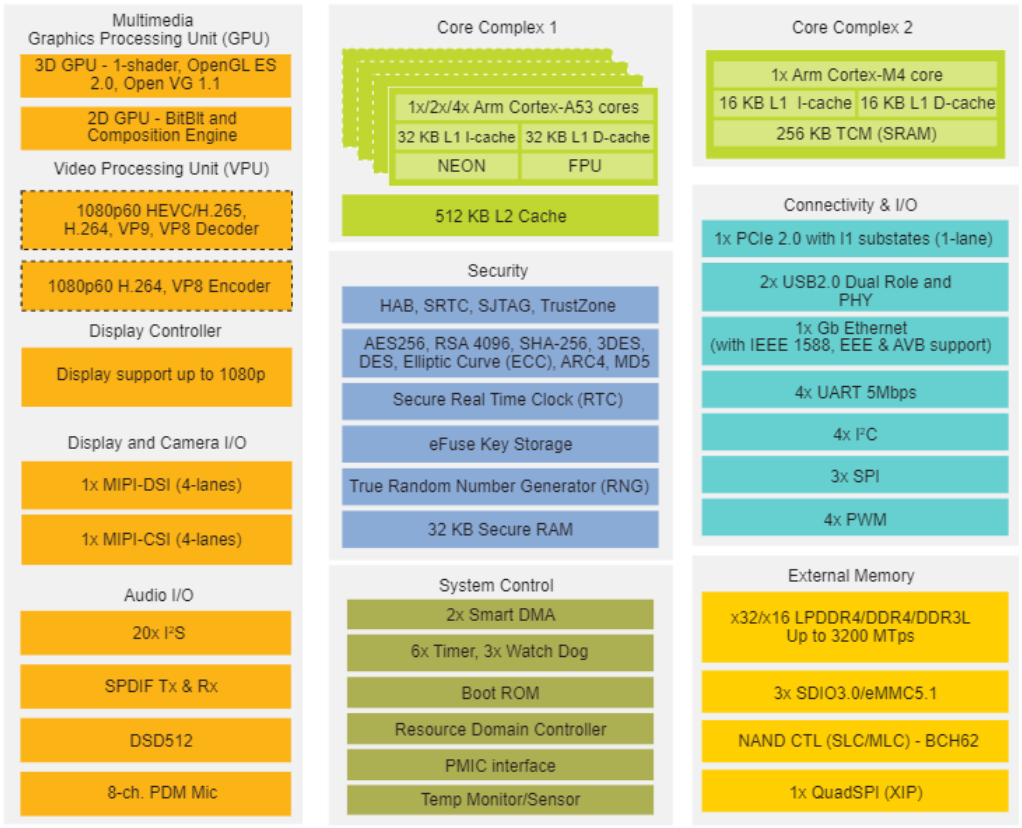
Source: NXP

NXP offers the K32W0148-EVK, an evaluation kit for the K32W148 platform. It's now available for ordering on the company's website. This EVK lets developers begin writing microcontroller-based Matter applications immediately without hardware development or customization.

I.MX 8M MINI MATTER-ENABLED HIGH-PERFORMANCE MPU

At the high end of the Matter platform spectrum, NXP offers the "i.MX 8M Mini," an advanced MPU-based (Arm Cortex-A53) SoC for smart speakers, video hubs, cameras, gateways, routers, bridges, and other Matter applications requiring edge intelligence.

FIGURE 10: I.MX 8M MINI

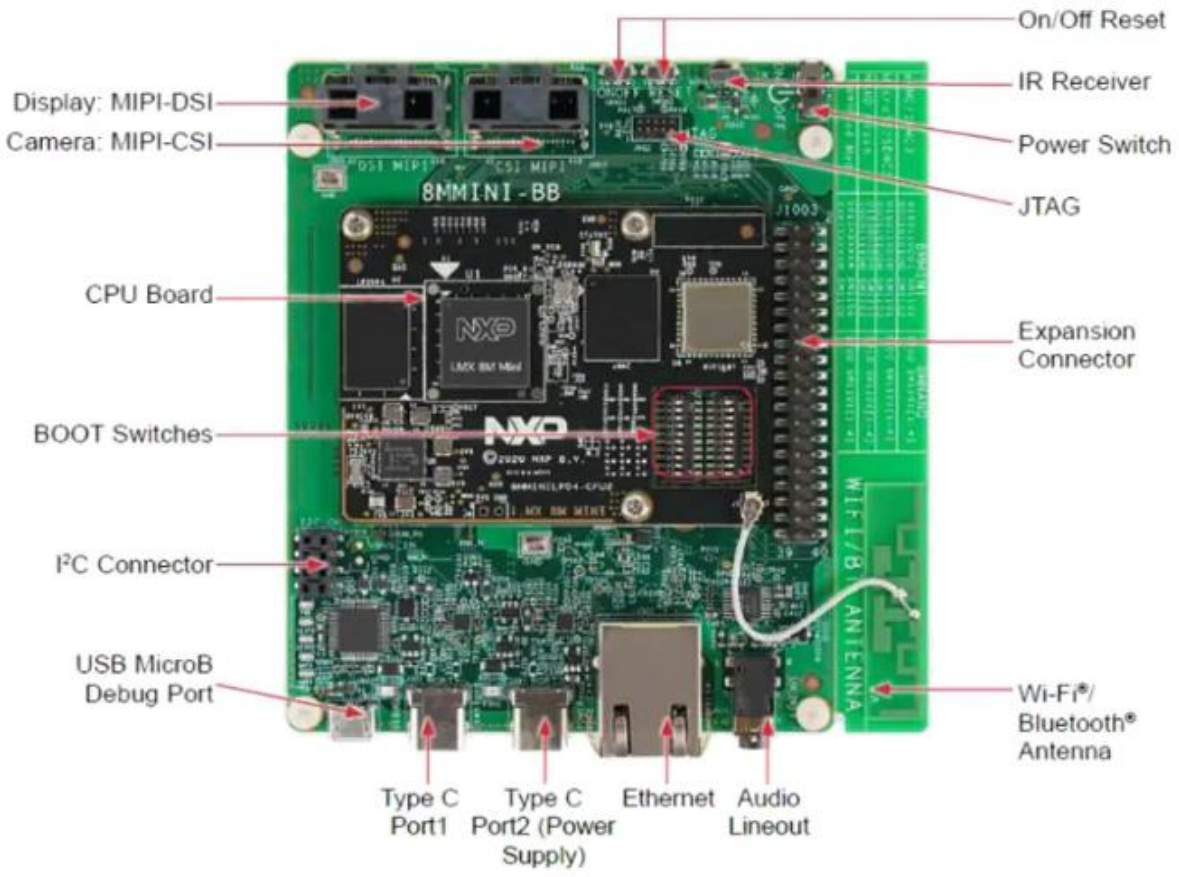


Source: NXP

The i.MX 8M Mini family, diagrammed in Figure 10, supports considerable configuration flexibility. NXP offers options for multiple processor cores (1, 2, or 4 Cortex A-53s). 2D and 3D GPUs and hardware video encode/decode make this chip ideal for multimedia applications. Memory and flash are external, so developers can use whatever the application needs.

Radio and security subsystems are also external, enabling developers to select the appropriate hardware for each application. NXP's IW612 single-chip Tri-Radio subsystem is an excellent choice because it supports all three Matter wireless networks – Wi-Fi®, Thread, and Bluetooth® LE. The three radios share the same 2.4 GHz band, so NXP provides advanced coexistence management to optimize performance. Software enablement for the IW612 is on GitHub®, and module partners can provide evaluation kits. Developers can use an EdgeLock SE05x Secure Element or an EdgeLock A5000 Secure Authenticator chip for enhanced Matter security and support for EdgeLock 2GO credential delivery.

FIGURE 11: 8MMINILPD4-EVKB EVALUATION KIT

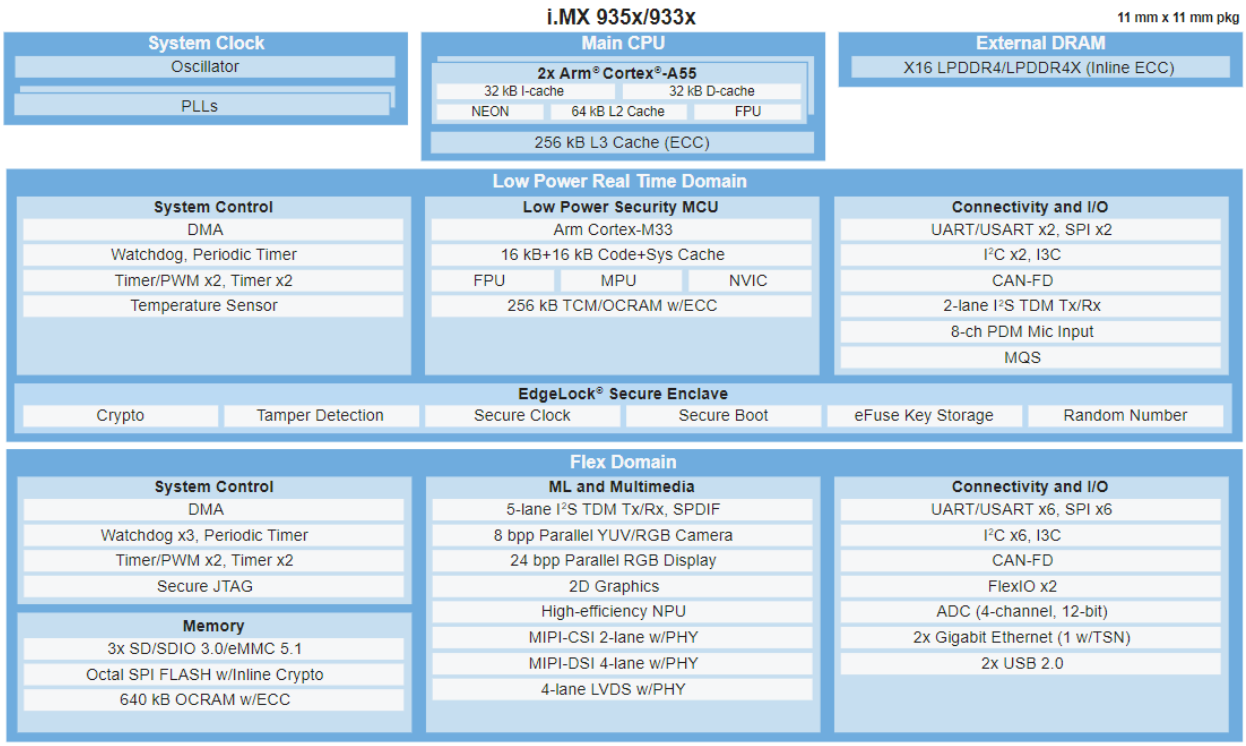


Source: NXP

NXP offers comprehensive development support for the Cortex-A53-based i.MX 8M Mini family. The 8MMINILPD4-EVKB evaluation kit supports the interfaces required for developing advanced Matter products – radio subsystems, security (EdgeLock SE-05x Secure Element or EdgeLock A5000 Secure Authenticator), audio, video, graphics, USB, I/O, radio subsystems, and HDMI.

In addition to i.MX 8M, the i.MX family offers a variety of other configurations, such as the Cortex-A7-based i.MX 6ULL and the Cortex-A55-based, NPU-powered i.MX 93. All these options run Linux with consistent board support packages. Developers can select the optimal platform for each new product with little or no impact on system software, security, or Matter implementation. Platform flexibility and software compatibility are key features of this product line.

FIGURE 12: I.MX 93



Source: NXP

I.MX 93 – MATTER-ENABLED ML-ACCELERATED MPU

The newest i.MX option is the i.MX 93. Paired with the previously described IW612 Tri-Radio chip, this Cortex-A55-enabled MPU is ideal for high-performance, energy-efficient, ML-accelerated Matter applications such as smart speakers and hubs, security and surveillance products, control panels, appliances, AV equipment, and robotics. Its built-in EdgeLock Secure Enclave provides the cryptographic capabilities that Matter requires. Developers can provide enhanced Matter security with the EdgeLock SE05x Secure Element or EdgeLock A5000 Secure Authenticator. NXP's EdgeLock 2GO credential delivery supports all three configurations, and the SE05x/A5000 chips offer the option of pre-injection in the silicon fab.

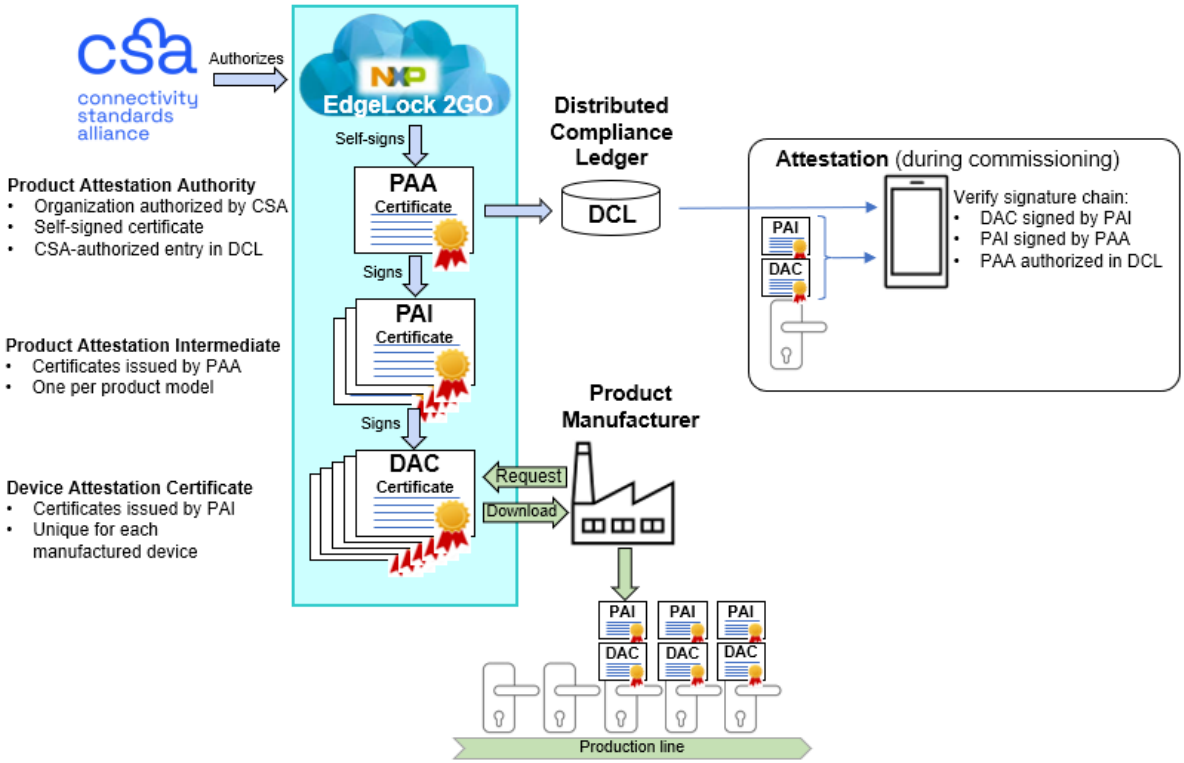
SECURE MATTER SOFTWARE

The software components required to build complete Matter platforms using NXP silicon and reference platforms are available from GitHub®. At the bottom of the software stack, NXP provides board support packages for all hardware options – including

security and wireless networking for MPU and MCU platforms. At the top of the stack, software development for MPU-based Matter products is no different from other embedded Linux applications. Developers grab OS and system software packages from GitHub® and write high-level application code on top. For MCU-based platforms, NXP offers the MCUXpresso IDE. Based on the Eclipse® framework, the IDE supports FreeRTOS™, ThreadX®, Zephyr®, and MQX®.

Developers can build and run the Matter stack on NXP evaluation kits without code porting or customization. Product code development can begin immediately after getting one of these reference platforms up and running. Implementations based on these platforms are secure and easy to certify.

FIGURE 13: EDGELOCK 2GO FOR MATTER



Source: Moor Insights & Strategy

MANUFACTURING AND PROVISIONING MATTER PRODUCTS – EDGELOCK 2GO

In this paper, we described the role of PAAs in creating DACs for every Matter device. Summary:

- DACs are unique, factory-installed credentials that guarantee the authenticity of each device and authorize it to join Matter networks.
- PAAs are the trusted authorities that issue DACs.
- The CSA defines strict rules for PAAs to ensure trustworthiness and enforces those rules via audits.

Product manufacturers can be PAAs, but it's a costly process that adds no differentiating value. Matter specifications address this situation by allowing vendor-independent ("Non-VID Scoped") PAAs to generate DACs and deliver them to manufacturers, either pre-embedded in silicon or downloaded from the PAA's web service and injected during device manufacturing. NXP, one of the first Matter PAAs, offers EdgeLock 2GO, a cloud service for managing this process.

At a high level, the process is simple. Figure 13 illustrates how EdgeLock 2GO works.

- **PAA** – The CSA publishes each authorized PAA's self-signed certificate to the DCL. This certificate is the root of trust for each device the PAA authorizes.
- **PAI** – The PAA creates and signs a PAI certificate for each product type (model number).
- **DAC** – The PAI certificate signs a unique (DAC for each manufactured device. The DAC specifies the device vendor and model, which must match the product's Certification Declaration. During product installation, the commissioner uses information in the DCL to validate the DAC signature chain (PAA, PAI, DAC) and CD identity.
- **Device private key** – Every device has a unique private "attestation" key corresponding to the DAC's public key. The PAA may supply these keys, but some devices generate them internally.
- **Onboarding (commissioning) passcode** – The PAA typically generates a unique commissioning passcode for each device. The manufacturer provides an external representation of this passcode (e.g., QR code or NFC) and also installs the code within the device in secure storage.
- **DAC injection option 1: Production line provisioning** (shown in Figure 13) – Manufacturers request DACs via the EdgeLock 2GO cloud service. NXP provides software tools that securely inject the DAC into NXP silicon on the device production line.
- **DAC injection option 2: Silicon pre-provisioning** (not shown) – For products with an EdgeLock SE05x Secure Element or EdgeLock A5000 Secure

Authenticator, NXP can pre-provision the DAC before shipping the chips to the manufacturer.

The EdgeLock SE05x Secure Element and the A5000 Secure Authenticator enhance product security by providing an isolated environment for storing keys, executing cryptographic operations (e.g., PASE, SPAKE2, CASE), and managing operational credentials. The SE05x and A5000 also improve product manufacturing scalability because the same EdgeLock turn-key credential provisioning solution scales to support all MCU and MPU Matter platforms. Plus, it's easy for software developers to add EdgeLock support to Matter because NXP has already integrated the EdgeLock SE05x/A5000 crypto stack into the official Matter GitHub® repository.

CERTIFICATION

Product certification is the final step of Matter development. Independent test labs exhaustively test products for compliance with Matter specifications and confirm interoperability with other Matter devices. The tests emphasize functional security, including reliable device onboarding in multivendor environments. Certified devices receive the Matter logo and an entry in the Distributed Compliance Ledger indicating certification status.

Test failures significantly delay certification and increase costs, so manufacturers are highly motivated to "get it right the first time." Using software and hardware already certified in other products is the best way to eliminate surprises during testing. NXP's matter-ready silicon and broadly deployed open-source software minimize product-specific system programming and decrease certification risk.

CALL TO ACTION

Matter security and privacy are comparable to the mainstream platforms we use daily for commerce, communication, entertainment, and countless other applications. Matter adapts broadly deployed security standards, practices, and technologies to the unique requirements of connected embedded devices. Adaptations ensure that devices are trustworthy, installation is easy, constrained networks (Thread) are supported, all messages are encrypted, IP header information is private, and firmware updates are enabled.

But what's the cost? Matter's security architecture is more robust than previous generations of smart home devices, but its added complexity raises concerns about platform size and development complexity. Costs may be higher as product

manufacturers climb the learning curve, but developers stand on the shoulders of some of the biggest consumer electronics and semiconductors companies. The Matter community has already done the "heavy lifting" to provide Matter-ready silicon, software, and services that work "right out of the box" with little or no system-level customization. Matter development is rapidly becoming less costly than legacy alternatives and more accessible to application programmers outside the embedded community.

Matter devices are secure, safe to deploy, easy to develop, affordable to manufacture, and supported by many of the biggest consumer electronics and semiconductors brands. Matter is already present in hundreds of millions of homes, including over 100 million Echo devices[1], so deployment barriers are low. At this point, every smart home device maker should have solid Matter migration plans, and consumers should prioritize Matter devices when shopping for new smart home products.

[1] "Alexa … surpasses 100 million Matter-enabled Echos," Amazon press release, May 2, 2023.

IMPORTANT INFORMATION ABOUT THIS PAPER

CONTRIBUTOR
Bill Curtis, Analyst In-Residence, Industrial IoT and IoT Technology

PUBLISHER
Patrick Moorhead, CEO, Founder and Chief Analyst at Moor Insights & Strategy

INQUIRIES
Contact us if you would like to discuss this report, and Moor Insights & Strategy will respond promptly.

CITATIONS
This paper can be cited by accredited press and analysts but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

LICENSING

DISCLOSURES
NXP commissioned this paper. Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

DISCLAIMER
The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.