

# AN13445

## Enable Matter in smart home solutions using EdgeLock SE05x/A5000

Rev. 1.1 — 10 February 2023

Application note

### Document information

Information	Content
Keywords	EdgeLock SE05x, A5000, SE051H, smart home, Matter, secure element, secure attestation
Abstract	The Matter standard provides a secure, reliable, and seamless user experience when integrating IoT devices from different vendors in the smart home ecosystem. This application note describes how EdgeLock SE05x/A5000, and in particular EdgeLock SE051H, can be leveraged to easily deploy in your smart home IoT solution the security required by the Matter standard and much more.



## Revision history

Revision history

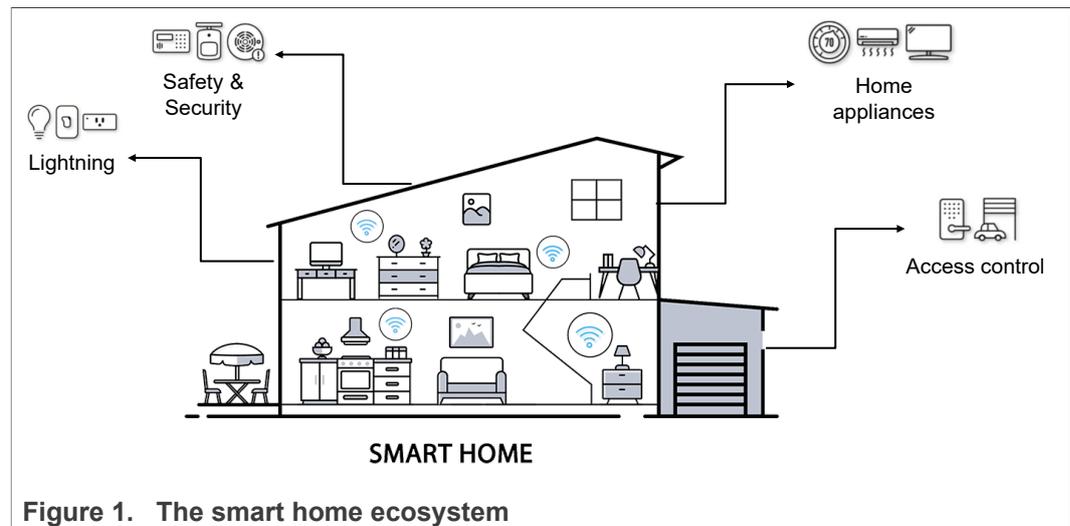
Revision number	Date	Description
1.1	2023-02-10	Updated document to include EdgeLock SE051H
1.0	2022-11-08	Initial version

## 1 The smart home ecosystem

Connected IoT devices are an essential part of our homes: they range from small devices such as smart bulbs, door knobs and smart speakers to big appliances such as refrigerators, washing machines and ovens. By leveraging on increased computational capabilities, high-speed connectivity and machine learning, smart home devices increasingly provide new and improved functionalities, increased energy efficiency and the ability to configure and control them from everywhere in the world using intuitive interfaces.

However, even if smart home devices are all part of the same ecosystem, integration and interoperability between different models and brands have notoriously been difficult due to the lack of a single, unifying protocol accepted by the majority of IoT manufacturers. This resulted in a fragmented ecosystem, which ultimately slowed down user adoption of smart home solutions.

Moreover, the smart home ecosystem is increasingly exposed to sophisticated security threats, especially as device connectivity becomes more pervasive. In this scenario, attackers can exploit vulnerabilities and insecure communication protocols to compromise user privacy, steal sensible data and disrupt the normal operation of devices. Implementing strong security mechanisms must therefore be a core requirement of any smart home IoT solution.



### 1.1 Introducing Matter

[Matter](#) (previously known as Project CHIP) is a single, unified connectivity standard that aims at providing a simple way for developers to connect and build reliable, secure smart home IoT ecosystems while at the same time increasing compatibility and interoperability for users of smart home solutions. Matter is open-source and backed by the [Connectivity Standard Alliance](#) (CSA) and leaders of the smart home ecosystem.

Matter is built around three main pillars:

- **Simplicity:** Matter devices are easy to purchase, configure and set up. With Matter, users are able to add devices to their smart home network through a simple and smooth onboarding process.

- **Interoperability & compatibility:** with Matter, devices from different brands work natively together. Users are no longer forced to buy devices from the same manufacturer to ensure they are compatible with one another.
- **Security:** respecting user privacy and protecting sensitive data from attackers is of utmost importance, especially in the domestic environment. With Matter, security is no longer an accessory, but a core feature around which the whole protocol is built. State-of-the-art, robust security is built into Matter, while keeping it as streamlined as possible for both developers and users.

## 1.2 Introducing NXP secure solutions for Matter

NXP provides scalable, flexible and secure platforms for the variety of use cases Matter addresses. For an overview of the manifold NXP solution for Matter, please refer to [www.nxp.com/matter](http://www.nxp.com/matter). Enabling top-notch security on these and other platforms is as easy as integrating the NXP [EdgeLock SE05x/A5000](#) secure element: a ready-to-use SE solution tailor-made for the IoT that provides a secure, CC EAL 6+ certified tamper-resistant hardware to protect mission critical cryptographic credentials as well as a secure environment to offload cryptographic operations. It also comes with a pre-installed applet and a middleware package that ease the integration of the secure element in the customer's MCU/MPU.

Enabling Matter security is further simplified by integrating [EdgeLock SE051H](#): an EdgeLock SE051 variant specifically designed to meet the full suite of cryptographic requirements mandated by the Matter security stack. It comes with pre-injected Matter credentials and an NFC interface that simplifies the onboarding of Matter devices.

Moreover, to abstract the complexity of key and certificate management in secure elements, NXP offers [EdgeLock 2GO](#): a fully managed cloud platform that allows customers to create and manage secure objects, such as symmetric roots of trust, key-pairs and certificates, which are then securely provisioned (either remotely or locally) into the secure elements of IoT devices. Through EdgeLock 2GO, customers can provision all the keys and certificates required for the secure commissioning of Matter devices.



This document describes how EdgeLock SE05x/A5000 can be used to enable Matter in your IoT devices and to meet the security requirements mandated by the Matter standard, including secure commissioning and onboarding of Matter devices. Step-by-step instructions are provided to run examples demonstrating how EdgeLock SE05x/

A5000 integrates with Matter and how it can conveniently be used to deploy security in smart-home devices and applications.

## 2 The Matter standard

Matter is a connectivity standard for the smart home ecosystem that is being developed by the Connectivity Standard Alliance (CSA). It defines a common **application layer** and data model on top of widely supported TCP/IP protocols (IPv6, TCP and UDP) as shown in [Figure 3](#).

Multiple IP-compatible communication protocols can be used with Matter: from traditional wired protocols such as Ethernet and DSL to wireless protocols such as Wi-Fi and cellular. The Thread protocol, a low-power mesh networking technology for the IoT, is supported as well. In the first stages of development, Matter will support Wi-Fi and Thread as operational communication technologies and Bluetooth Low Energy (LE) as a way to simplify device commissioning and setup.

The application layer protocol defined by Matter can be further divided in sub-layers to better separate the different responsibilities and introduce a good level of encapsulation. These layers range from IP framing and transport management up to the data model structure and the application itself. An important layer is the **security sub-layer** which takes care of applying cryptographic security to the transmitted data. In this layer messages are encrypted and appended with a message authentication code to ensure data remains confidential and authentic between sender and receiver.

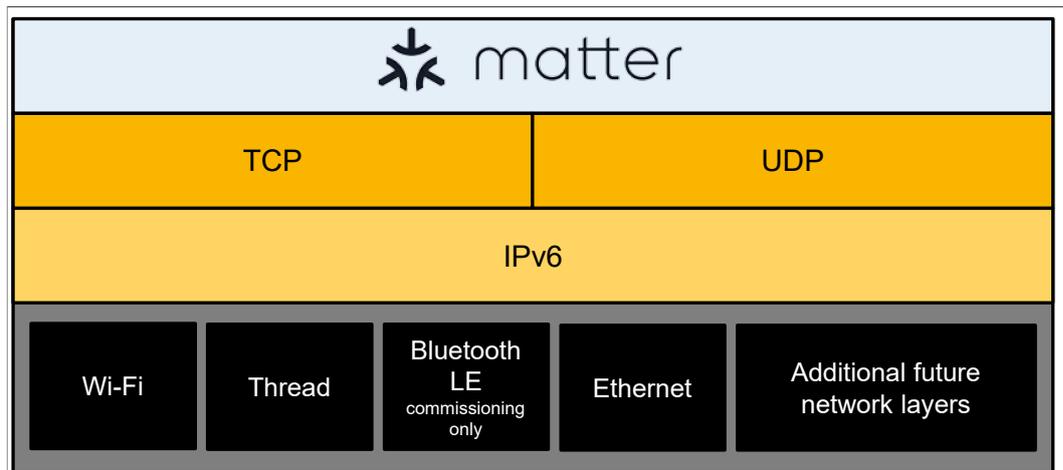
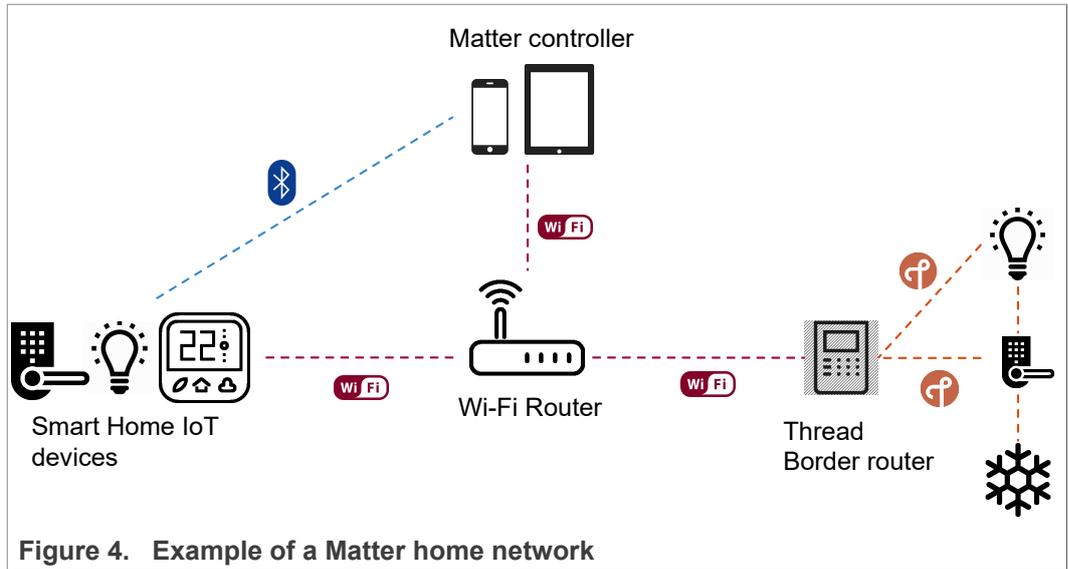


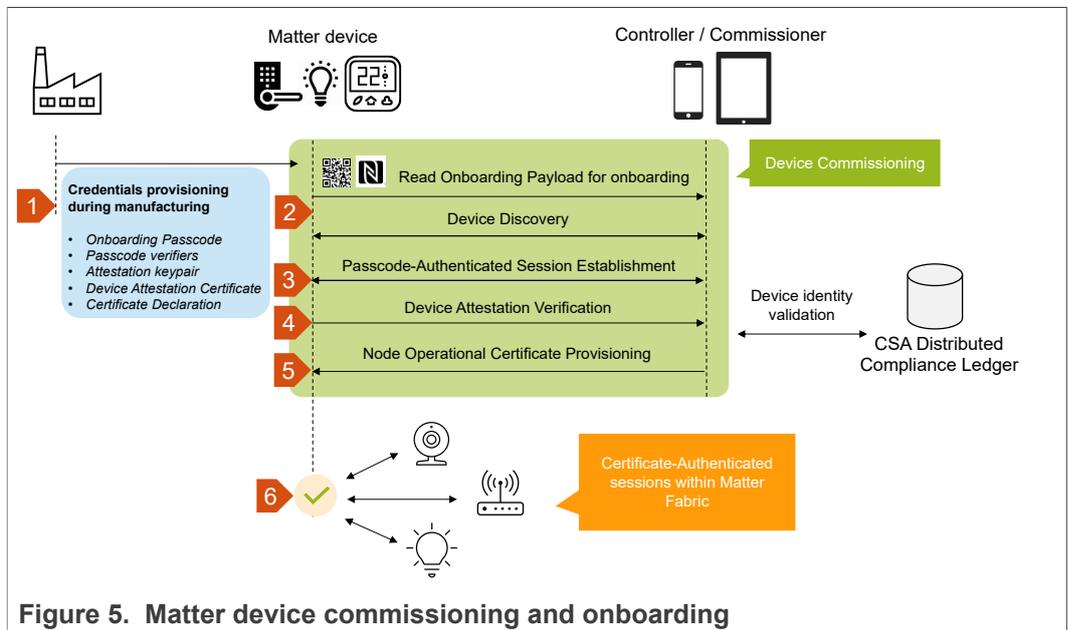
Figure 3. Matter high-level architecture

An example of a Matter home network is shown in [Figure 4](#). A Matter controller device (e.g. a smartphone, tablet or smart panel) is connected to the local Wi-Fi or Ethernet network and is responsible to securely commission and onboard other Matter devices. Depending on the networking technologies supported by Matter devices, the commissioning can be performed through Bluetooth LE, Wi-Fi or the local IP network if the Matter device already joined it. Onboarded devices, called **Matter Nodes**, join the Matter home network, also known as **Matter Fabric**, and can then communicate with each other and with the Matter controller to send or receive data and commands. Thread devices can also join the network through Thread border routers, which act as bridges between the Wi-Fi and Thread networks. Even if device-to-cloud communication is beyond the scope of Matter, connection of Matter devices to external cloud applications or services is supported as well.



### 2.1 Secure commissioning and onboarding of Matter devices

Before a Matter device can join the a Matter fabric, it must go through a secure commissioning and onboarding process whose objective is to verify the authenticity of the new device and to establish the credentials required to securely communicate with the other devices of the fabric. The secure commissioning and communication process defined by Matter is depicted in [Figure 5](#):



- 1. Credentials provisioning:** Matter credentials are typically provisioned during the manufacturing of the device. These credentials must be injected in the IoT device and

properly protected since they are essential for the establishment of all subsequent Matter secure channels. The credentials that must be injected are listed in [Table 1](#).

**Table 1. Pre-provisioned Matter credentials**

Credential	Description
Onboarding passcode	The onboarding passcode is a device-unique, randomly generated 27-bit integer which is used as a shared secret in the Passcode-Authenticated Session Establishment (PASE) protocol described in Step 3. The onboarding passcode must be provisioned in a location separate from the device memory and facilitated to the commissioner through an out of band channel, typically a QR code, an NFC tag, or a manual pairing code printed on the device.
Passcode verifiers	Passcode verifiers are records used as part of the SPAKE2+ protocol during PASE to establish secure session keys. Verifiers can be computed offline from the onboarding passcode through multiple iterations of a Password-Based Key Derivation Function (PBKDF). Even in case an attacker gets access to the verifiers, the associated passcode could only be computed with considerable computational effort.
Device attestation key, Device Attestation Certificate (DAC) and Certificate Declaration (CD)	Keys and certificates required to determine whether a device is a genuine and certified Matter product before commissioning it into a Matter fabric, See <a href="#">Section 2.2</a> for more details about the attestation process and the required certificate chain.

- 2. Reading of the onboarding payload and device discovery:** during this phase the Matter controller reads the onboarding payload (typically stored in a QR code or NFC tag) which contains the onboarding passcode and other metadata information required during the commissioning process. The controller then proceeds to discover the device to be commissioned using network interfaces such as Bluetooth LE, WiFi, or an existing IP network. A commissioning channel is then established between the controller and the Matter device.
- 3. Passcode-Authenticated Session Establishment (PASE):** the PASE protocol is executed on top of the commissioning channel established in Step 2. This protocol aims to establish the first secure and authenticated session between a controller and a Matter device. During PASE, SPAKE2+, a Password-Authenticated Key Exchange (PAKE) protocol, is used to generate and verify the session keys that will later encrypt all communication over the commissioning channel. To authenticate with one another, the commissioner and the Matter device use respectively the onboarding passcode obtained out-of-band in Step 2 and the pre-provisioned passcode verifiers.
- 4. Device attestation verification:** after successful establishment of the passcode-authenticate channel, the controller verifies the Matter device authenticity, i.e., whether a particular device is certified for Matter compliance and has been legitimately produced by the certified manufacturer. This is done by using the pre-provisioned attestation key, DAC and CD. More information on the required keys and certificates are provided in [Section 2.2](#).
- 5. Node operational certificate provisioning:** upon successful device identity verification, the Matter device generates an operational credential key pair and provides to the commissioner its public key. The commissioner then generates the Node Operational Certificate (NOC) and provides it to the Matter device. Operational credentials are only trusted within a particular Matter network and are used to initiate all subsequent secure communication. More information on operational credentials is

provided in [Section 2.2](#). At the end of this step the Matter device is also onboarded to the operational network if it is not already part of it.

6. **Certificate-Authenticated Session Establishment (CASE)**: finally, the CASE protocol is used for secure device-to-device communication within the Matter home network. Through this protocol an encrypted and mutually authenticated channel is established using the operational credentials provisioned in Step 5.

For more information on the Matter protocol and the security mechanisms involved, you can access the following resources or refer to the official Matter specification:

- [Matter official website](#)
- [Matter official Github repository](#)
- [NXP Matter web page](#)

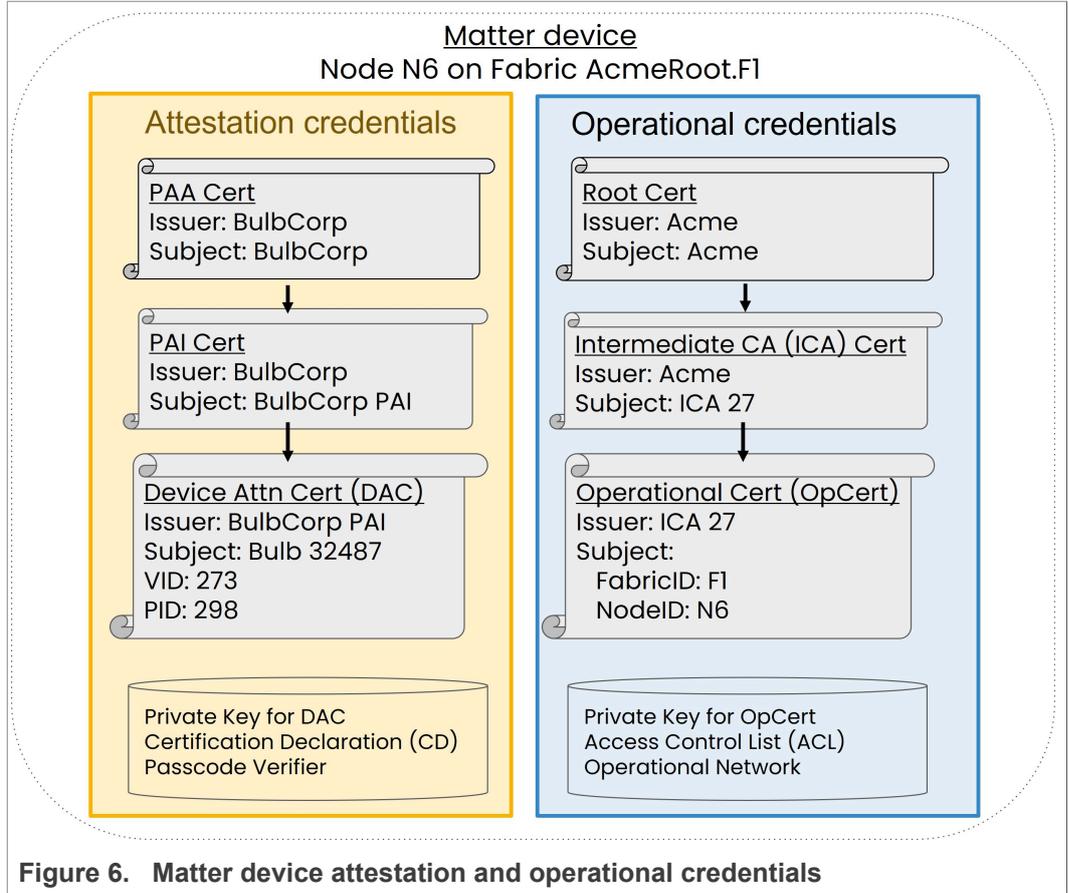
## 2.2 Attestation credentials and operational credentials in Matter

The commissioning and onboarding process described in [Section 2.1](#) requires that the Matter device is provisioned with a unique identity that can be verified using well-established cryptographic primitives and processes. To achieve this, every Matter device is provisioned with a device-unique **Device Attestation Certificate (DAC)** and its corresponding private key. The DAC contains parameters such as the public key of the device, the signature algorithm that must be used for verification (*ECDSA with SHA256*), the Vendor ID (VID) and the Product ID (PID). The VID and PID are unique identifiers released by CSA after the device successfully passes the Matter certification process and whose validity can be verified through a digitally-signed **Certificate Declaration (CD)** statement issued by the CSA (also injected in the device).

The DAC must be signed by a **Product Attestation Intermediate (PAI)** certificate which in turn must be signed by a root certificate issued by an approved **Product Attestation Authority (PAA)**. By verifying the certificate chain up to the PAA certificate, the Matter commissioner can verify the authenticity of the Matter device that is joining the network. As part of this process, the VID and PID provided in the DAC are verified to conform with the CD.

The Matter device operational credentials, injected in the device after successful onboarding, behave similarly to attestation credentials: in this case, the device will store the **Operational Certificate (OpCert)**, and the associated private key, signed by a locally trusted root certificate and Intermediate CA (ICA) certificate. The OpCert contains the **Fabric ID**, an identifier that is shared between devices belonging to the same Matter network, and the **Node ID**, a device-unique identifier within the Matter network.

[Figure 6](#) shows the structure of the Matter certificates and credentials described above.



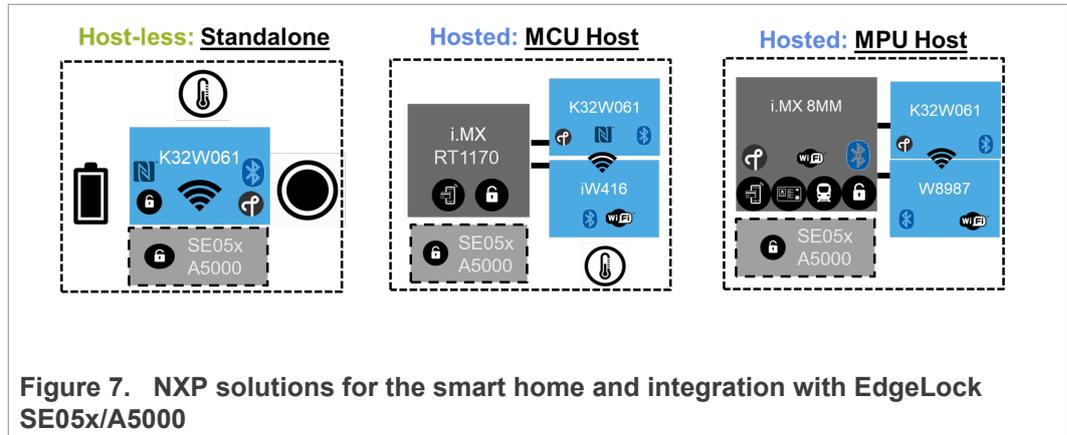
### 3 Leverage on NXP solutions to build secure Matter devices

The Matter smart home ecosystem consists of devices with the most diverse requirements and computational capabilities. NXP provides scalable, flexible and secure platforms – from end nodes to gateways – for the variety of use cases Matter addresses as described in [Table 2](#).

**Table 2. Type of Matter devices and NXP solutions**

Matter device type	Description	NXP solution
End nodes	Simple, standalone devices such as light bulbs, switches and doorknobs requiring very low energy and computational power.	<ul style="list-style-type: none"> <li>• <a href="#">NXP K32W061/41 multiprotocol MCU</a> is the ideal low-power solution to implement simple, standalone end nodes with support for Bluetooth LE and Thread protocols.</li> </ul>
Edge nodes	End devices requiring more computational power to run complex applications such as thermostats, security systems and smart plugs.	<ul style="list-style-type: none"> <li>• MCU-hosted platforms:                             <ul style="list-style-type: none"> <li>– <a href="#">NXP i.MX RT Crossover MCUs</a></li> </ul> </li> <li>• MPU-hosted platforms:                             <ul style="list-style-type: none"> <li>– <a href="#">NXP i.MX 8 Series MPUs</a></li> </ul> </li> <li>• Wi-Fi and Thread connectivity can be enabled respectively by <a href="#">NXP IW416 SoC</a> and <a href="#">NXP K32W061/41 MCU</a>.</li> </ul>
Gateways / hubs	Devices that need to support computational intensive applications, including audio / video streams, such as smart displays, smart speakers and IP cameras. Such devices can also act as Matter controllers or Thread border routers to control and onboard other smart-home devices to the Matter network.	<ul style="list-style-type: none"> <li>• The <a href="#">NXP i.MX 8 Series</a> multi-core, high-performance Linux-hosted MPUs are the ideal solution to implement gateway/hub devices.</li> <li>• The <a href="#">NXP W8987 SoC</a>, supporting Very High Throughput (VHT) applications, is most suited to enable Wi-Fi connectivity in gateway devices.</li> <li>• Thread connectivity can be enabled using <a href="#">NXP K32W061/41 MCU</a>.</li> </ul>

Even though most of the above-mentioned solutions have integrated hardware and software security mechanisms, the EdgeLock SE05x/A5000 SE is the go-to NXP solution to deploy top-notch, uncompromising security in smart-home devices and applications. EdgeLock SE05x/A5000 supports Matter and can be easily integrated with the whole range of NXP solutions for the smart home: from simple standalone devices to complex MCU-hosted and MPU-hosted devices as shown in [Figure 7](#).



EdgeLock SE05x/A5000 even goes beyond Matter and can be used as a full-fledged IoT solution to enable use cases such as sensor data protection, secure cloud onboarding, device-to-device authentication and device integrity protection among many others (see [EdgeLock SE05x/A5000 documentation page](#)).

NXP IoT security offer is complemented by [EdgeLock 2GO](#): a fully managed cloud platform operated by NXP that provides secure provisioning services for easy deployment and maintenance of IoT devices that integrate EdgeLock SE05x/A5000 secure elements. Through EdgeLock 2GO, Matter attestation keys and certificates can be provisioned in EdgeLock SE05x/A5000.

### 3.1 EdgeLock SE05x/A5000: the ideal solution to deploy Matter security

To onboard and securely connect smart home devices to the home network, Matter defines a range of security requirements, credentials and cryptographic protocols. Even if security requirements can be satisfied using software implementations and/or MCU/MPU hardware features, integrating a dedicated secure element to store sensitive credentials and to offload critical cryptographic operations guarantees a higher protection level. By offloading the cryptographic protocol implementation to the secure element, you do not need to worry about secure coding and can integrate the same secure element with different MCUs/MPUs.

The EdgeLock SE05x/A5000 SE provides a Common Criteria (CC) EAL 6+ certified **tamper-resistant hardware** where you can generate and store Matter cryptographic keys and credentials as well as credentials required to implement other use cases (e.g. secure cloud onboarding). Keys and credentials can either be generated on-demand by the customer, pre-provisioned during manufacturing in NXP secure facilities or even remotely provisioned through the **NXP EdgeLock 2GO** platform.

Thanks to the pre-installed **IoT applet**, EdgeLock SE05x/A5000 provides out-of-the-box support for the security protocols and algorithms required by Matter, including:

- **Encryption and decryption** using state-of-the-art symmetric (AES CTR) and asymmetric algorithms (RSA, ECC) with high key length and future proof curves (NIST, Brainpool, Edwards and Montgomery curves among others);
- **Signature generation & verification** using both RSA and EC cryptography (ECDSA);
- **Key agreement & key derivation** using respectively ECDH and HMAC;
- **Secure device attestation**
- **True Random Number Generator (TRNG)** to generate random data or nonces whenever they are required by cryptographic algorithms or protocols.

Cryptographic operations are always executed in EdgeLock SE05x/A5000 secure environment so that sensitive credentials are never exposed to the outside, non-secure environment.

If you integrate the **EdgeLock SE051** SE in your IoT solution, you can take advantage of the **SEMS Lite technology** to update the SE on-the-field, both online or offline, so as to always get the latest security patches from NXP and the latest updates required to keep up with the Matter specification as it evolves over time. With EdgeLock SE051, devices can take advantage of the latest features and security improvements as soon as they are available and always enjoy a high protection level for stored credentials.

To ease integration of EdgeLock SE05x/A5000 security features in smart home IoT solutions, NXP provides a fully-featured **EdgeLock SE05x Plug & Trust middleware package**. The middleware is pre-integrated with many micro-controller platforms and contains several examples and demo projects that can be used as a starting point to develop custom software implementations and use cases. A stripped-down version of the EdgeLock SE05x Plug & Trust middleware, implementing all the functions required by the Matter crypto stack, is already integrated in the [official Matter Github repository](#).

### 3.1.1 EdgeLock SE051H: a turnkey solution for Matter

Enabling Matter security features is further simplified by integrating the [EdgeLock SE051H](#) SE. By integrating EdgeLock SE051H in your Matter device you get access to all the features offered by EdgeLock SE05x/A5000 (see [Section 3.1](#)) plus a set of additional features specifically designed to meet Matter-specific security requirements:

- **Pre-injected Matter attestation credentials:** EdgeLock SE051H is pre-provisioned with a device-unique attestation key that can be used for Matter device attestation. The DAC can be either pre-provisioned by NXP or injected at a later time by the customer through the EdgeLock SE05x Plug & Trust middleware or through the EdgeLock 2GO platform.  
*Note: pre-provisioning of DACs by NXP is only available upon definition of custom SE types. Please contact your NXP representative.*
- **SPAKE2+ protocol support and pre-injected SPAKE2+ verifiers:** the IoT applet installed in EdgeLock SE051H supports out-of-the-box the SPAKE2+ protocol that is required by Matter in the commissioning phase. Both the verifier and prover roles are supported, so customers can integrate the SE both in Matter devices and Matter controllers. On top of this, a set of SPAKE2+ verifiers are pre-injected in the SE for different iteration values of the PBKDF.  
*Note: passcode and salts used to generate the verifiers are also injected in the SE. These can be read out and added to the onboarding payload, but must be deleted before the Matter device is shipped.*
- **Internal signature generation:** the IoT applet installed in EdgeLock SE051H supports the generation of digital signatures (ECC and RSA) using a specified input securely stored in the SE. This feature can be leveraged in the Matter device attestation phase to sign pre-determined, device-specific data securely stored in the SE (e.g. a concatenation of the CD, a random challenge and some firmware information) to prove that the signature has indeed been generated by the SE.
- **NFC Type 4 Tag (T4T) capabilities:** EdgeLock SE051H comes with a T4T applet compliant with NFC T4T specification v1.0 that be accessed through the NFC interface of the SE. The applet can be used to store NDEF messages that can be read out by compatible NFC devices (e.g., a smartphone). In the context of Matter, the T4T applet can conveniently be used to store the onboarding payload required to start the device commissioning.

### 3.2 How to integrate EdgeLock SE05x/A5000 in your Matter IoT solution

EdgeLock SE05x/A5000 can be easily integrated in your Matter smart home IoT solution to provide increased security during the Matter device onboarding phase as well as during the normal operation of the device after it has been onboarded. [Figure 6](#) outlines how EdgeLock SE05x/A5000 contributes to the secure implementation of the Matter protocol.

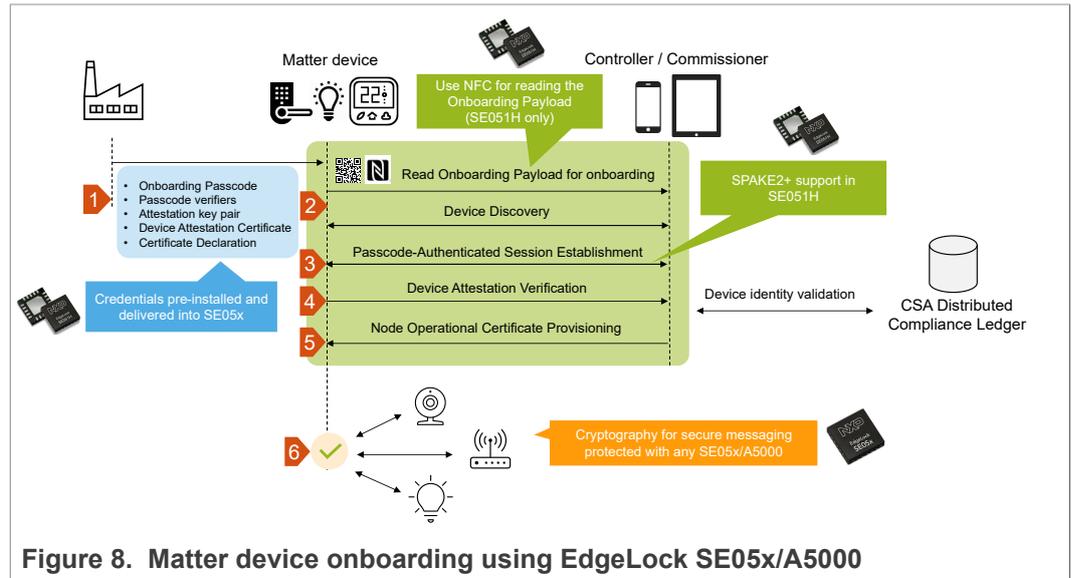


Figure 8. Matter device onboarding using EdgeLock SE05x/A5000

1. **Credentials provisioning:** cryptographic credentials required by Matter are either pre-provisioned or they can be easily injected in EdgeLock SE05x/A5000 as described in [Table 3](#):

Table 3. Pre-provisioned Matter credentials in EdgeLock SE05x/A5000

Credential	Description
Onboarding passcode	<ul style="list-style-type: none"> <li>• <b>EdgeLock SE051H:</b> a pre-provisioned passcode is stored in an erasable secure object. The passcode can be read out and added to the onboarding payload of the device (QR code or NFC tag).</li> <li>• <b>EdgeLock SE05x/A5000:</b> no pre-provisioned passcode.</li> </ul>
Passcode verifiers	<ul style="list-style-type: none"> <li>• <b>EdgeLock SE051H:</b> multiple SPAKE2+ verifiers are computed for several iterations of the PBKDF algorithm and pre-provisioned in the SE.</li> <li>• <b>EdgeLock SE05x/A5000:</b> no pre-provisioned passcode verifiers (no support for SPAKE2+ algorithm).</li> </ul>
Device attestation key, Device Attestation Certificate (DAC) and Certificate Declaration (CD)	<p><b>EdgeLock SE051H:</b> pre-provisioned attestation key and, optionally, pre-provisioned DAC (only for custom SE types upon agreement with NXP). DAC can be provisioned at a later time using EdgeLock 2GO or the EdgeLock SE05x Plug &amp; Trust middleware.</p> <p><b>EdgeLock SE05x/A5000:</b> attestation keys and certificates can only be provisioned by customers using the EdgeLock SE05x Plug &amp; Trust middleware or through the EdgeLock 2GO platform.</p>

2. **Reading of the onboarding payload:** the onboarding payload containing the passcode and other metadata can be stored as an NDEF message in the **T4T applet** of EdgeLock SE051H. It can then be read by any compatible device using the NFC interface of the SE.
3. **Passcode-Authenticated Session Establishment (PASE):** thanks to pre-provisioned passcode verifiers and **out-of-the-box support for the SPAKE2+ protocol**, EdgeLock SE051H can be used by the Matter device to offload all cryptographic operations required during PASE.
4. **Device attestation verification:** any EdgeLock SE05x/A5000 SE can be used to securely store the attestation key-pair and certificate (DAC) required to verify the authenticity of the Matter device. The controller / commissioner is then responsible for validating the certificate chain as described in [Section 2.1](#). The proof-of-possession required to validate the DAC can be generated directly by the SE using the ECDSA algorithm.
5. **Node operational certificate provisioning:** any EdgeLock SE05x/A5000 SE can securely generate and store in its secure memory the operational credentials issued when the device is commissioned into the network. The operational credentials never leave the boundaries of the SE.
6. **Certificate-Authenticated Session Establishment (CASE):** any EdgeLock SE05x/A5000 SE supports the certificate-authenticated protocol that is used to establish a secure connection between Matter devices using operational credentials. All required ECC-based cryptographic operations are natively supported by EdgeLock SE05x/A5000 and can therefore be offloaded to the secure element.

Implementing the above-mentioned functionalities is as easy as activating the [Matter crypto stack implementation for EdgeLock SE05x/A5000](#) which has already been integrated in the official [Matter Github repository](#). The implementation leverages on [EdgeLock SE05x Plug & Trust middleware mini package](#). For more information, please refer to the documentation provided in the Matter Github repository and in the EdgeLock SE05x Plug & Trust middleware package.

## 4 Run the Matter onboarding demo using EdgeLock SE05x/A5000

This section describes how to run a demo application that showcases how to onboard a Matter client device to a Matter network using a Matter controller device. In the demo, the Matter client device will run the *thermostat example*, while the Matter controller device will run the *Matter CHIP tool*:

- **Thermostat example:** an example available for different devices and operating systems that simulates a smart thermostat device and shows the usage of Matter. In this document, the Linux thermostat example is used.
- **Matter CHIP tool:** a Matter controller implementation that allows users to commission a Matter device into the network and to communicate with it using Matter messages. In this document the Matter CHIP tool will be used to commission the Matter client device running the *thermostat example* and onboard it to an existing IP network. More information on the CHIP tool and the commands available can be found in the [CHIP tool page](#) of the Matter repository.

During the onboarding of the Matter client device, attestation and other cryptographic operations will be performed using cryptographic features of EdgeLock SE05x/A5000 and keys and credentials generated and stored in the SE.

### 4.1 Hardware and software required

This section lists the hardware and software material required to run the Matter onboarding demo:

Table 4. Boards required

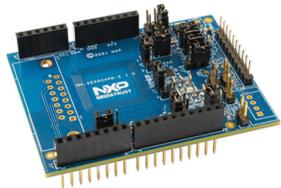
Name	Description	Picture
Raspberry Pi 4 Model B with 4 GB RAM or more	ARM-based general purpose board. In this document, a single board will be used to simulate both the Matter client device (thermostat) that wants to join the Matter network and the Matter controller device. It is also possible to use two separate Raspberry Pi boards: one acting as client, the other as controller. <b>Note:</b> it is strongly recommended to use an SD card of at least 64 GB.	
<a href="#">OM-SE050ARD-E/-F</a> (EdgeLock SE050) <a href="#">OM-SE051ARD</a> (EdgeLock SE051) <a href="#">OM-SE051ARD-H</a> (EdgeLock SE051H) <a href="#">OM-A5000ARD</a> (EdgeLock A5000)	EdgeLock SE05x/A5000 Arduino compatible development kit. <b>Note:</b> some cryptographic features might not be available in all boards. Please refer to the boards' datasheets to learn which features are supported.	

Table 4. Boards required...continued

Name	Description	Picture
<a href="#">OM-SE050RPI</a>	<b>Optional.</b> The OM-SE050RPI adapter board allows an easy integration of OM-SE05xARD and OM-A5000ARD development kits with Raspberry Pi boards.	

Table 5. Other required devices

Name	Description
Windows/Linux/macOS laptop	A laptop is required to flash the Raspberry Pi SD card with the Ubuntu Server OS image. The laptop will also be used to connect remotely to the Raspberry Pi board using SSH.

## 4.2 Preliminary steps before running the demo

Before building and running the Matter onboarding demo, prepare the system by executing the following steps in order:

- Prepare the SD card for the Raspberry Pi:** use the official [Raspberry Pi Imager](#) tool to flash the SD card with Ubuntu OS. To prepare the SD card, follow the instructions provided in the official [Ubuntu website](#). It is strongly recommended to flash the SD card with **Ubuntu Server 20.04.05 LTS (64 bit version)**;
- Connect the OM-SE05xARD/A5000ARD to the Raspberry Pi:** follow the instructions provided in [AN12570](#) (*hardware setup* section) to configure the OM-SE05xARD/A5000ARD jumpers and connect it to the Raspberry Pi using either wires or the *OM-SE05xRPI* adapter board;
- Connect Raspberry Pi to the local network and boot it up:** connect the Raspberry Pi to the local network using an Ethernet cable, insert the micro SD card and finally power up the Raspberry Pi using the USB-C connector and a suitable power supply (5 V, 3 A).  
*Note: you can also connect the Raspberry Pi to the local network using WiFi. In this case additional configuration steps are required (not covered in this document).*  
*Note: if you are using two Raspberry Pi boards, make sure that both are connected to the same local IP network.*
- Connect to the Raspberry Pi using SSH:** find the IP address of the Raspberry Pi in your local network, then use any SSH client to connect to it (e.g. [Putty](#) on Windows). At first login, you must provide the default Ubuntu credentials (username: *ubuntu*, password: *ubuntu*). You will then be asked to change the default password.  
*Note: alternatively, you can interact with the Raspberry Pi using a keyboard directly connected to the board and an HDMI display connected to the mini HDMI port of the Raspberry Pi. In this document, an SSH connection will be used.*

## 4.3 Prepare the build environment and clone the Matter repository

Connect to the Raspberry Pi board using SSH, then follow these steps to install in Ubuntu Server the dependencies and build tools required to compile the code and examples available in the Matter repository:

Enable Matter in smart home solutions using EdgeLock SE05x/A5000

1. First, update the Ubuntu Server software packages to the latest available version:

```
sudo apt-get update
sudo apt-get upgrade
```

2. Then, install the additional software packages required to compile and run the Matter software stack:

```
sudo apt-get install git gcc g++ pkg-config libssl-dev libdbus-1-dev \
libglib2.0-dev libavahi-client-dev ninja-build python3-venv python3-dev \
python3-pip unzip libgirepository1.0-dev libcairo2-dev libreadline-dev \
pi-bluetooth avahi-utils
```

3. Clone the NXP's Matter repository fork in the user home folder (e.g., `/home/ubuntu/`), then activate the Matter environment. If the activation is successful, you should see the message shown in [Figure 9](#).

**Note:** the Matter software repository is continuously evolving. To ensure that the Matter onboarding demo can be executed correctly as described in this document, make sure to checkout the exact commit shown in the commands below.

**Note:** downloading all the required repositories and activating the Matter environment might take several minutes.

**Note:** if you need to compile Matter examples, the `activate.sh` script must be run each time the Raspberry Pi is reinitialized.

```
git clone https://github.com/NXPmicro/matter.git
cd matter
git checkout 9ffcf50a59281d25a6465680bed8249a5a68fe70
git submodule update --init
source scripts/activate.sh
```

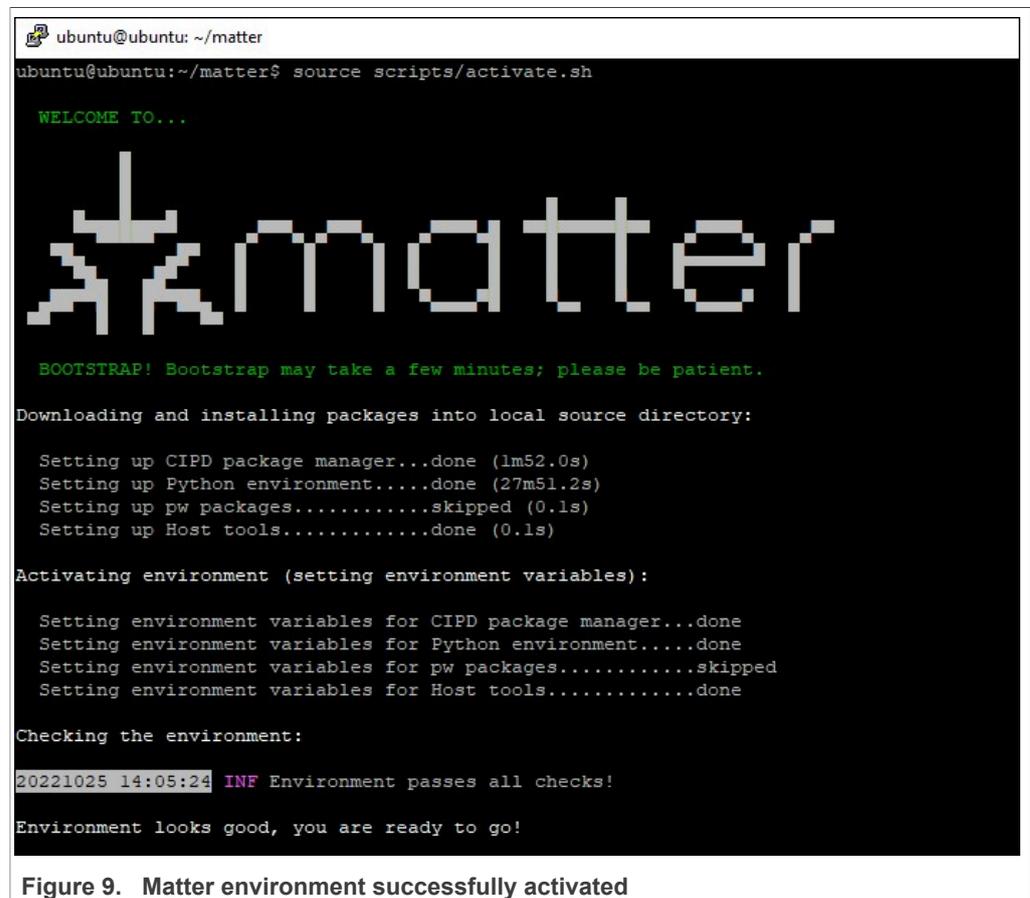


Figure 9. Matter environment successfully activated

## 4.4 Run the Matter thermostat example

This section describes how to compile the Matter *thermostat* example with EdgeLock SE05x/A5000 support and execute it in the Raspberry Pi board:

- [Section 4.4.1](#) describes how to correctly configure the Matter crypto stack and the Plug & Trust middleware to use EdgeLock SE05x/A5000 to perform cryptographic operations;
- [Section 4.4.2](#) describes how to compile and run the *thermostat* example.

### 4.4.1 Configure the Matter crypto stack

Now that the Matter software stack is correctly configured in your system and all required dependencies have been installed, you can configure the Matter Hardware Secure Module (HSM) crypto stack and the Plug & Trust middleware to use the cryptographic capabilities of EdgeLock SE05x/A5000. Follow these instructions:

1. Open the file *CHIPCryptoPALHsm\_config.h* in a text editor (e.g. *nano*) to configure the Matter HSM crypto stack:

```
nano ~/matter/src/crypto/hsm/CHIPCryptoPALHsm_config.h
```

Enable Matter in smart home solutions using EdgeLock SE05x/A5000

2. Enable the crypto features that you want to be performed using EdgeLock SE05x/A5000. To do this, set the appropriate flags in *CHIPCryptoPALHsm\_config.h* as shown in [Figure 10](#):

(1) Enable or disable SPAKE verifier and SPAKE prover. Please note that these cryptographic operations are currently supported only by *EdgeLock SE051H* and should be activated only if you are using this SE variant.

(2) Enable or disable any of the other features available.

For example, you can activate *ENABLE\_HSM\_GENERATE\_EC\_KEY* and *ENABLE\_HSM\_HMAC\_SHA256* to use EdgeLock SE05x/A5000, respectively, to generate ephemeral EC keys and to perform HMAC operations;

(3) If you want to use EdgeLock SE05x/A5000 for ECDSA verify operations, uncomment the *#define ENABLE\_HSM\_ECDSA\_VERIFY* line.

(4) The Matter stack can be configured so that the device attestation phase is performed using keys and credentials securely stored in EdgeLock SE05x/A5000. If you want to use EdgeLock SE05x/A5000 for device attestation:

- Uncomment the *#define ENABLE\_HSM\_DEVICE\_ATTESTATION* line;
- Set *#define ENABLE\_HSM\_GENERATE\_EC\_KEY 1*

Make sure to save the changes to the file by sending *CTRL-X*, followed by *Y* and *Enter*.



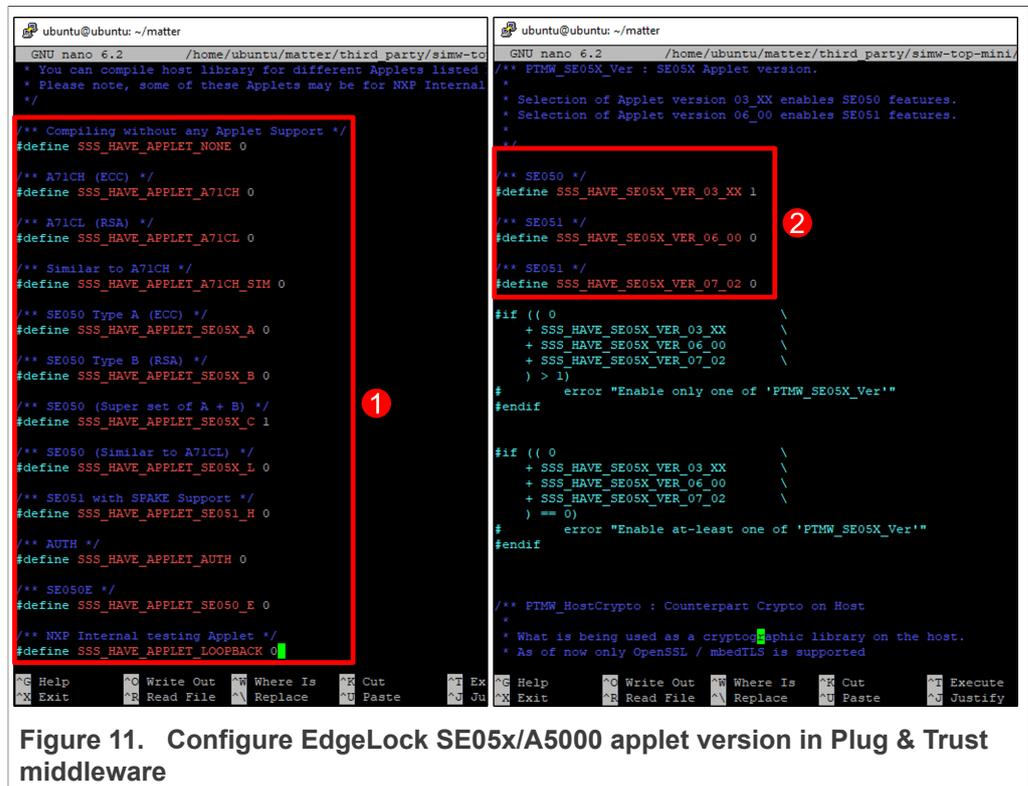
3. Configure EdgeLock SE05x/A5000 by setting the correct applet configuration in the *fsl\_sss\_ftr.h* file. Open the file using a text editor (e.g. *nano*):

```
nano ~/matter/third_party/simw-top-mini/repo/fsl_sss_ftr.h
```

Enable Matter in smart home solutions using EdgeLock SE05x/A5000

4. Set the EdgeLock SE05x/A5000 applet configuration in the `fs/_sss_ftr.h` file as shown in [Figure 11](#):
  - (1) Select the applet installed in your SE by setting the appropriate flag to 1:
    - If you are using an *OMSE05x-ARD* board, select `SSS_HAVE_APPLET_SE05X_C`
    - If you are using an *OMSEA5000-ARD* board select `SSS_HAVE_APPLET_AUTH`
    - If your are using an *OM-SE051ARD-H* board select `SSS_HAVE_APPLET_SE051_H`
  - (2) Select the applet version installed in your SE by setting the appropriate flag to 1:
    - If you are using an *OMSE050-ARD* board, select `SSS_HAVE_SE05X_VER_03_XX`
    - If you are using an *OMSE051-ARD* board, select either `SSS_HAVE_SE05X_VER_06_00` or `SSS_HAVE_SE05X_VER_07_02`
    - If you are using an *OMA5000-ARD* board or an *OM-SE051ARD-H*, select `SSS_HAVE_SE05X_VER_07_02`

Make sure to save the changes to the file by sending `CTRL-X`, followed by `Y` and `Enter`.



5. Change the access permissions of the `i2c` interface so that all users can read/write to it. The `i2c` interface is used to communicate with EdgeLock SE05x/A5000. This step is required to allow the `thermostat` example and other applications to use the `i2c` interface without root permissions.
 

**Note:** this step should be executed only for demo purposes. Access to the `i2c` interface should be customized by the system administrator according to the security requirements of the system.

```
sudo chmod 666 /dev/i2c-1
```

6. If you enabled attestation in Step 2, you need to inject in EdgeLock SE05x/A5000 the attestation key and the corresponding attestation certificate. The Plug & Trust

middleware, included as a dependency in the Matter repository, contains an example that can be used to inject a set of sample credentials. Execute the commands below to compile and run the example. If the execution is successful, you should see the message shown in [Figure 12](#).

```
cd ~/matter/third_party/simw-top-mini/repo
cd demos/se05x_dev_attest_key_prov/linux
gn gen out/debug
ninja -C out/debug
out/debug/se05x_dev_attest_key_prov
```

**Note:** if the execution fails with "Mismatch Applet version Compiled for 0x<applet\_version>. Got older 0x<applet\_version>" make sure that you have correctly set the applet version of the SE you are using in the `fsl_sss_ftr.h` file as described in [Section 4.4.1](#).

```
ubuntu@ubuntu:~/matter/third_party/simw-top-mini/repo/demos/se05x_dev_attest_key_prov/linux$ ./out/debug/se05x_dev_attest_key_prov
App :INFO :if you want to over-ride the selection, use ENV=EX_SSS_BOOT_SSS_PORT or pass in command line arguments.
SIMW : Nothing to do in enable_se05x_contact_interface
sss :INFO :atr (Len=35)
      00 A0 00 00 03 96 04 03 E8 00 FE 02 0B 03 E8 08
      01 00 00 00 00 64 00 00 0A 4A 43 4F 50 34 20 41
      54 50 4F
sss :WARN :Communication channel is Plain.
sss :WARN :!!!Not recommended for production use.!!!
Set DA key at location - 7d300000
Set DA cert at location - 7d300001
Attestation key and cert Provision successful
ubuntu@ubuntu:~/matter/third_party/simw-top-mini/repo/demos/se05x_dev_attest_key_prov/linux$
```

Figure 12. Attestation key and certificate successfully injected in EdgeLock SE05x/A5000

#### 4.4.2 Compile and run the Matter thermostat example

Follow these instructions to compile the *thermostat* example and run it:

1. Compile the Matter *thermostat* example:

```
cd ~/matter/examples/thermostat/nxp/linux-se05x
gn gen out/debug
ninja -C out/debug
```

2. Run the *thermostat* example by issuing the following command:

```
out/debug/thermostat-se05x-app
```

The thermostat example will start running and will wait for the onboarding commands from the Matter controller. The logs will print the device discriminator (by default 3840)

Enable Matter in smart home solutions using EdgeLock SE05x/A5000

and the device PIN (by default 20202021) as shown in [Figure 13](#). This information must be provided to the Matter controller as described in [Section 4.5](#).

**Note:** the example can be stopped with CTRL-C. It is strongly recommended to clean temporary files before running the example again. Use the command below to clean the temporary files directory:

```
rm -rf /tmp/chip_*
```

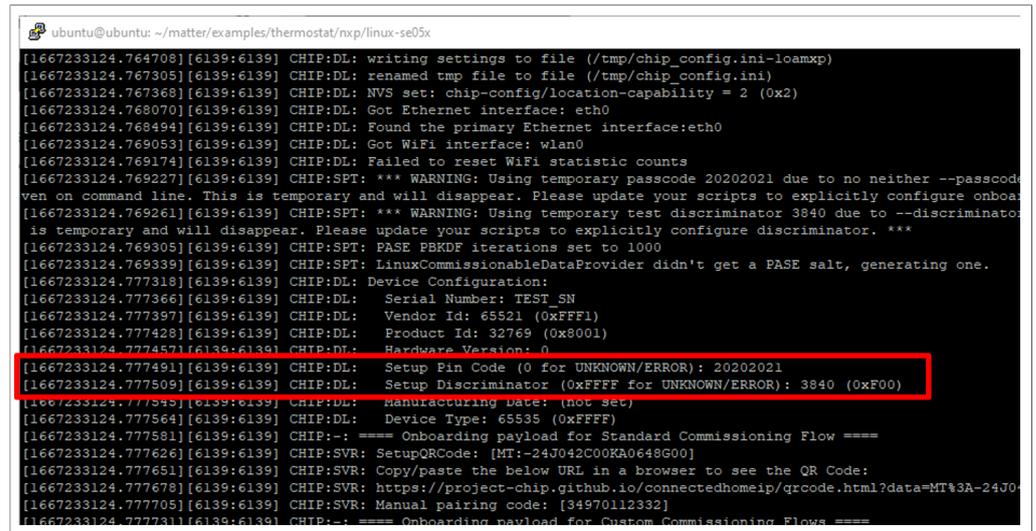


Figure 13. Matter thermostat example is running and showing the discriminator and PIN

4.5 Onboard the device with Matter CHIP tool

The CHIP tool is a Matter controller device implementation that allows the users to commission a Matter client device into the network and to communicate with it using Matter messages. In this section we will compile the CHIP tool and use it to onboard the Matter client device running the *thermostat* example to the Matter network. Before starting this section make sure that the *thermostat* example is running on the Matter client device as described in [Section 4.4](#).

**Note:** the instructions provided in this section can be executed in a different Raspberry Pi board. For simplicity, the same instructions can be executed on the same Raspberry Pi that is running the *thermostat* example. In this case, make sure to open a new SSH session before running the CHIP tool.

1. Compile the CHIP tool by issuing the following commands. The CHIP tool executable will be generated in the `~/connectedhomeip/out/chip-tool` folder.

```
cd ~/matter
./scripts/examples/gn_build_example.sh examples/chip-tool out/chip-tool
```

2. Onboard the Matter client running the *thermostat* example to the Matter network by issuing the command below:

```
out/chip-tool/chip-tool pairing onnetwork 3840 20202021
```

The *pairing onnetwork* command onboards a Matter device that is already connected to the same IP network of the Matter controller. The first parameter is the device discriminator (in this case 3840), while the second parameter is the device PIN (in this case 20202021).

Enable Matter in smart home solutions using EdgeLock SE05x/A5000

- After issuing the command in the previous step, the Matter controller and the Matter client will start exchanging the messages required for the onboarding. If the onboarding is successful, you should see in the CHIP tool logs the entries shown in [Figure 14](#) (*new secure session created for device*). In the logs generated by the *thermostat* example, you should see several entries indicating that EdgeLock SE05x/A5000 has been used to perform the cryptographic operations specified in [Section 4.4.1](#) (e.g. generating ECC keys, performing ECDH, etc.) as shown in [Figure 15](#).

```

ubuntu@ubuntu: ~/matter
[1667238611.119762][6936:6941] CHIP:DIS: Checking node lookup status after 201 ms
[1667238611.119937][6936:6941] CHIP:DIS: OperationalSessionSetup[1:000000000000F00]: Updating device address to UDP:[fe80::e65f:1:5540 while in state 2
[1667238611.119995][6936:6941] CHIP:CTL: OperationalSessionSetup[1:000000000000F00]: State change 2 --> 3
[1667238611.120234][6936:6941] CHIP:IN: SecureSession[0xffff70029660]: Allocated Type:2 LSID:45088
[1667238611.120311][6936:6941] CHIP:SC: Initiating session on local FabricIndex 1 from 0x000000000000B669 -> 0x000000000000F00
[1667238611.121562][6936:6941] CHIP:SC: Including MRP parameters
[1667238611.121808][6936:6941] CHIP:EM: <<< [E:639881 M:238270882] (U) Msg TX to 0:0000000000000000 [0000] --- Type 0000:30 (Secur
al)
[1667238611.122014][6936:6941] CHIP:IN: (U) Sending msg 238270882 to IP address 'UDP:[fe80::e65f:1ff:fead:271b%eth0]:5540'
[1667238611.122347][6936:6941] CHIP:SC: Sent Sigma2 msg
[1667238611.122406][6936:6941] CHIP:CTL: OperationalSessionSetup[1:000000000000F00]: State change 3 --> 4
[1667238611.603851][6936:6941] CHIP:EM: >>> [E:639881 M:115751149 (Ack:238270882)] (U) Msg RX from 0:0000000000000000 [0000] --- T
eChannel:CASE_Sigma2)
[1667238611.603926][6936:6941] CHIP:EM: Found matching exchange: 639881, Delegate: 0xffff7002a018
[1667238611.604003][6936:6941] CHIP:EM: Rxd Ack: Removing MessageCounter:238270882 from Retrans Table on exchange 639881
[1667238611.604082][6936:6941] CHIP:SC: Received Sigma2 msg
[1667238611.604150][6936:6941] CHIP:SC: Peer assigned session ID 48898
[1667238611.611761][6936:6941] CHIP:SC: Found MRP parameters in the message
[1667238611.611854][6936:6941] CHIP:SC: Sending Sigma3
[1667238611.612792][6936:6941] CHIP:EM: <<< [E:639881 M:238270883 (Ack:115751149)] (U) Msg TX to 0:0000000000000000 [0000] --- Typ
annel:CASE_Sigma3)
[1667238611.613174][6936:6941] CHIP:IN: (U) Sending msg 238270883 to IP address 'UDP:[fe80::e65f:1ff:fead:271b%eth0]:5540'
[1667238611.613516][6936:6941] CHIP:SC: Sent Sigma3 msg
[1667238611.619974][6936:6941] CHIP:EM: >>> [E:639881 M:115751150 (Ack:238270883)] (U) Msg RX from 0:0000000000000000 [0000] --- T
eChannel:StatusReport)
[1667238611.620006][6936:6941] CHIP:EM: Found matching exchange: 639881, Delegate: 0xffff7002a018
[1667238611.620044][6936:6941] CHIP:EM: Rxd Ack: Removing MessageCounter:238270883 from Retrans Table on exchange 639881
[1667238611.620079][6936:6941] CHIP:SC: Success status report received. Session was established
[1667238611.622479][6936:6941] CHIP:SC: SecureSession[0xffff70029660]: Moving from state 'kEstablishing' --> 'kActive'
[1667238611.622518][6936:6941] CHIP:IN: SecureSession[0xffff70029660]: Activated - Type:2 LSID:45088
[1667238611.622542][6936:6941] CHIP:IN: New secure session activated for device <000000000000F00, 1>, LSID:45088 PSID:48888!
[1667238611.622565][6936:6941] CHIP:CTL: OperationalSessionSetup[1:000000000000F00]: State change 4 --> 5
[1667238611.622624][6936:6941] CHIP:CTL: Successfully finished commissioning step 'FindOperational'
[1667238611.622646][6936:6941] CHIP:CTL: Commissioning stage next step: 'FindOperational' -> 'SendComplete'
[1667238611.622669][6936:6941] CHIP:CTL: Performing next commissioning step 'SendComplete'
[1667238611.622728][6936:6941] CHIP:DMG: ICR moving to [AddingComm]
[1667238611.622753][6936:6941] CHIP:DMG: ICR moving to [AddedComma]
    
```

Figure 14. Successful onboarding (CHIP Tool)

```

ubuntu@ubuntu: ~/matter/examples/thermostat/nxp/linux-se05x
[1667238611.122577][6924:6924] CHIP:EM: Handling via exchange: 63988r, Delegate: 0xaaade6135c0
[1667238611.122662][6924:6924] CHIP:IN: CASE Server received Signal message. Starting handshake. EC 0xaaaf4690d50
[1667238611.122712][6924:6924] CHIP:IN: CASE Server disabling CASE session setups
[1667238611.122765][6924:6924] CHIP:SC: Received Signal msg
[1667238611.122852][6924:6924] CHIP:SC: Found MRP parameters in the message
[1667238611.122913][6924:6924] CHIP:SC: Peer assigned session key ID 45088
[1667238611.123370][6924:6924] CHIP:SC: CASE matched destination ID: fabricIndex 1, NodeID 0x000000000000F00
[1667238611.123513][6924:6924] CHIP:CR: SE05x: AllocateEphemeralKeypairForCASE using se05x
[1667238611.140169][6924:6924] CHIP:CR: Creating Nist256 key on SE05X !
[1667238611.348966][6924:6924] CHIP:CR: ECDH_derive_secret: Using SE05X for ECDH !
[1667238611.396102][6924:6924] CHIP:CR: SE05x: SignWithOpKeypair
[1667238611.396157][6924:6924] CHIP:CR: SE05x: SignWithOpKeypair ==> using mPendingKeypair
[1667238611.396201][6924:6924] CHIP:CR: ECDSA sign msg: Using SE05X for Ecc Sign!
[1667238611.602951][6924:6924] CHIP:SC: Including MRP parameters
[1667238611.603111][6924:6924] CHIP:EM: <<< [E:639881 M:115751149 (Ack:238270882)] (U) Msg TX to 0:0000000000000000 [00
annel:CASE_Sigma2)
    
```

Figure 15. Successful onboarding (thermostat example)

Enable Matter in smart home solutions using EdgeLock SE05x/A5000

- 4. Now that the device is onboarded, you can issue commands and read device parameters. For example, you can read the local temperature by issuing the following command using the CHIP tool:

```
out/chip-tool/chip-tool thermostat read local-temperature 3840 1
```

In the output you will find the value of the local temperature parameter as shown in [Figure 16](#).

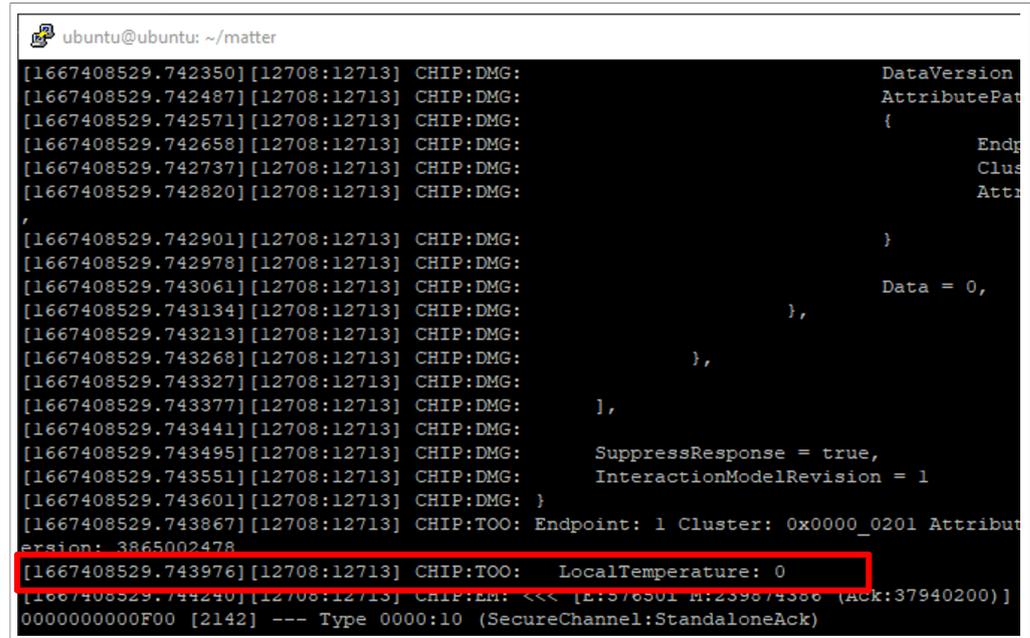


Figure 16. Successful reading of local temperature from thermostat (CHIP Tool)

## 5 Legal information

### 5.1 Definitions

**Draft** — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

### 5.2 Disclaimers

**Limited warranty and liability** — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

**Right to make changes** — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

**Suitability for use** — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

**Applications** — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or

the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

**Export control** — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

**Evaluation products** — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer. In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out of the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages. Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US\$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

**Translations** — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

**Security** — Customer understands that all NXP products may be subject to unidentified or documented vulnerabilities. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately. Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

### 5.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

**NXP** — wordmark and logo are trademarks of NXP B.V.

Tables

Tab. 1.	Pre-provisioned Matter credentials .....	8	Tab. 4.	Boards required .....	16
Tab. 2.	Type of Matter devices and NXP solutions .....	11	Tab. 5.	Other required devices .....	17
Tab. 3.	Pre-provisioned Matter credentials in EdgeLock SE05x/A5000 .....	14			

Figures

Fig. 1.	The smart home ecosystem .....	3	Fig. 10.	Configure Matter HSM crypto stack .....	20
Fig. 2.	EdgeLock SE05x/A5000 secure element .....	4	Fig. 11.	Configure EdgeLock SE05x/A5000 applet version in Plug & Trust middleware .....	21
Fig. 3.	Matter high-level architecture .....	6	Fig. 12.	Attestation key and certificate successfully injected in EdgeLock SE05x/A5000 .....	22
Fig. 4.	Example of a Matter home network .....	7	Fig. 13.	Matter thermostat example is running and showing the discriminator and PIN .....	23
Fig. 5.	Matter device commissioning and onboarding .....	7	Fig. 14.	Successful onboarding (CHIP Tool) .....	24
Fig. 6.	Matter device attestation and operational credentials .....	10	Fig. 15.	Successful onboarding (thermostat example) .....	24
Fig. 7.	NXP solutions for the smart home and integration with EdgeLock SE05x/A5000 .....	12	Fig. 16.	Successful reading of local temperature from thermostat (CHIP Tool) .....	25
Fig. 8.	Matter device onboarding using EdgeLock SE05x/A5000 .....	14			
Fig. 9.	Matter environment successfully activated .....	18			

## Contents

---

<b>1</b>	<b>The smart home ecosystem .....</b>	<b>3</b>
1.1	Introducing Matter .....	3
1.2	Introducing NXP secure solutions for Matter .....	4
<b>2</b>	<b>The Matter standard .....</b>	<b>6</b>
2.1	Secure commissioning and onboarding of Matter devices .....	7
2.2	Attestation credentials and operational credentials in Matter .....	9
<b>3</b>	<b>Leverage on NXP solutions to build secure Matter devices .....</b>	<b>11</b>
3.1	EdgeLock SE05x/A5000: the ideal solution to deploy Matter security .....	12
3.1.1	EdgeLock SE051H: a turnkey solution for Matter .....	13
3.2	How to integrate EdgeLock SE05x/A5000 in your Matter IoT solution .....	14
<b>4</b>	<b>Run the Matter onboarding demo using EdgeLock SE05x/A5000 .....</b>	<b>16</b>
4.1	Hardware and software required .....	16
4.2	Preliminary steps before running the demo .....	17
4.3	Prepare the build environment and clone the Matter repository .....	17
4.4	Run the Matter thermostat example .....	19
4.4.1	Configure the Matter crypto stack .....	19
4.4.2	Compile and run the Matter thermostat example .....	22
4.5	Onboard the device with Matter CHIP tool .....	23
<b>5</b>	<b>Legal information .....</b>	<b>26</b>

---

Please be aware that important notices concerning this document and the product(s) described herein, have been included in section 'Legal information'.

---

© NXP B.V. 2023.

All rights reserved.

For more information, please visit: <http://www.nxp.com>

For sales office addresses, please send an email to: [salesaddresses@nxp.com](mailto:salesaddresses@nxp.com)

Date of release: 10 February 2023  
Document identifier: AN1344510