Whitepaper –

SEALSQ

INeS PKI-aaS platform for managing the DAC for Matter

INeS

Certificate Management System for IoT

A State-of-the-art example of end-to-end device security, implemented by SEALSQ as the result of over 20 years hardware security, device provisioning, and PKI experience

Table of Contents

1. Introduction 3
2. Overview of Matter Spec 1.1 4
   2.1. Specific terms in Matter 4
   2.2. Device attestation & PKI 6
   2.3. Workflow of device commissioning 8
   2.4. Best practices on security 11
3. INeS PKI-as-a-Service 13
   3.1. Device attestation hierarchy for Matter 13
   3.2. INeS for Matter 14
4. Certificate provisioning 17
   4.1. DAC generation in a Batch 17
   4.2. DAC generation through RESTful/EST APIs 18
   4.3. DAC pre-provisioned in the SE 18
5. Conclusion 20
6. References 21
7. Abbreviation and Acronym 22

1. Introduction

The Matter protocol, formerly known as the Connected Home over IP (CHIP) protocol, is an open-source connectivity standard designed to make it easier for smart home devices to work together. Matter specification 1.1 is defined by CSA (Connectivity Standards Alliance) which major companies in the technology industry have joined, including Apple, Amazon, Google, and the Zigbee Alliance…etc.

The goal of the Matter protocol is to create a unified standard for smart home devices, a more connected, interoperable, and secure smart home ecosystem for users. Therefore, users can simplify the process of setting up and managing smart home devices from different smart home vendors.

Matter is built on existing technologies such as Wi-Fi, Bluetooth Low Energy (BLE), and Thread, and uses a secure, end-to-end encryption system to protect user data. The protocol also provides a simple and secure onboarding process for new devices, SEALSQ, a WISeKey company, can provide a complementary solution on PKI that is required for Matter smart home devices during the secure onboarding process.

2. Overview of Matter Spec 1.1

In the following sections, you will find the summary of security requirements related to PKI that are defined in the Matter specification 1.1.

2.1. Specific terms in Matter

Node: An addressable entity that supports the Matter protocol stack and (once Commissioned) has its own Operational Node ID and Node Operational credentials. A device may host multiple Nodes.

Fabric: A logical collection of communicating Nodes, sharing a common root of trust, and a common distributed configuration state.

Commissionee: An entity, a new device, that is being commissioned to become a Node that will be added/commissioned to a Fabric.

Commissioner: A Role of a Node that performs Commissioning for adding new devices to the Fabric. The commissioning will be done by a Smartphone which is in themselves Nodes of the Fabric.

Administrator: A Node having Administer privilege over another Node.

Product Attestation Authority (PAA): An entity that operates a root-level Certificate Authority for the purpose of Device Attestation.

Product Attestation Intermediate (PAI): An entity that operates an intermediate-level Certificate Authority for the purpose of Device Attestation.

Device Attestation Certificate (DAC): An RFC 5280 [https://www.rfc-editor.org/rfc/rfc5280] compliant X.509 v3 document with attestable attributes.

Certification Declaration (CD): A digitally signed token that conveys Matter certification status of a vendor's certified Device. Device vendors need to apply it from CSA.

Vendor ID (VID): A 16-bit number that uniquely identifies the Vendor of the Device. Device vendors need to apply it from CSA.

Product ID (PID): A 16-bit number that identifies the type of a Device, uniquely among the product types made by a given vendor. Device vendors need to apply it from CSA.

Node Operational Certificate (NOC): The NOC consists of the Root CA (acting as Fabric's trust anchor) and a Node unique certificate and private key. The Root CA will be used by the Commissioner to authenticate after commissioning has ended. The NOC and private key are used for communication between different Fabric Nodes.

Distributed Compliance Ledger (DCL): The DCL is a secure distributed point of device metadata and Product Attestation Authorities (PAA) certificates. It's used for tracking certification status and vendor-maintained information such as product name, product description and upgrade firmware URL …etc.

Write access: Restricted to CSA members

Read access: Public to anyone

Requestors: In the Matter PKI, the Requestor is the entity named in the RAD (Requestor Agreement Document). An authorized representative of the Requestor, as a Certificate Applicant, completes the Certificate issuance process established by the CA.

2.2. Device attestation & PKI

The device attestation provides mechanisms for Commissioners and Administrators to determine whether a Node is a genuine certified product before sharing sensitive information such as keys and other credentials. The device attestation feature relies on a Device Attestation Certificate (**DAC**) chain and on a Certification Declaration (**CD**).

All commissionable Matter Nodes SHALL include a Device Attestation Certificate (DAC) and corresponding private key, unique to that Device. The DAC is used in the Device Attestation process, as part of Commissioning a Commissionee into a Fabric. The DAC SHALL be a DER-encoded X.509v3-compliant certificate as defined in RFC 5280 and the DAC SHALL be issued by a Product Attestation Intermediate (PAI) that chains directly to an approved Product Attestation Authority (PAA), and therefore SHALL have a certification path length of 2.

The DAC also SHALL contain specific values of Vendor ID (OID: 1.3.6.1.4.1.37244.2.1) and Product ID (OID: 1.3.6.1.4.1.37244.2.2) in its subject field to indicate the vendor and product type of the specific node. The validity period of a DAC is determined by the vendor and MAY be set to the maximum allowed value to indicate that the DAC has no well-defined expiration date.

The Device Attestation PKI hierarchy consists of the PAA, PAI and individual DAC. The public key from the associated PAI certificate is used to cryptographically verify the DAC signature. The PAI certificate in turn is signed and attested to by the Product Attestation Authority (PAA) CA. The public key from the associated PAA certificate is used to cryptographically verify the PAI certificate signature. The PAA certificate is an implicitly trusted self-signed root certificate. In this way, the DAC chains up to the PAI certificate, which in turn chains up to the PAA root certificate. A PAI SHALL be assigned to a Vendor ID value. A PAI MAY further be scoped to a single Product ID value. If a PAI is used for multiple products, then it cannot be scoped to a Product ID value, otherwise the Device Attestation Procedure will fail policy validations.

Commissioners SHALL use PAA and PAI certificates to verify the authenticity of a Commissionee before proceeding with the rest of the Commissioning flow.

The subject of all DAC and PAI certificates SHALL be unique among all those issued by their issuer through the use of Relative Distinguished Name that ensure the uniqueness, such as for example a unique combination of commonName (OID 2.5.4.3), serialNumber (OID 2.5.4.5), organizationalUnitName (OID 2.5.4.11), etc.

The exact additional constraints, including for the subject field, for PAA, PAI and DAC certificates, are presented in the following subsections.

The following figure illustrates the PKI hierarchy of Device Attestation of Matter.

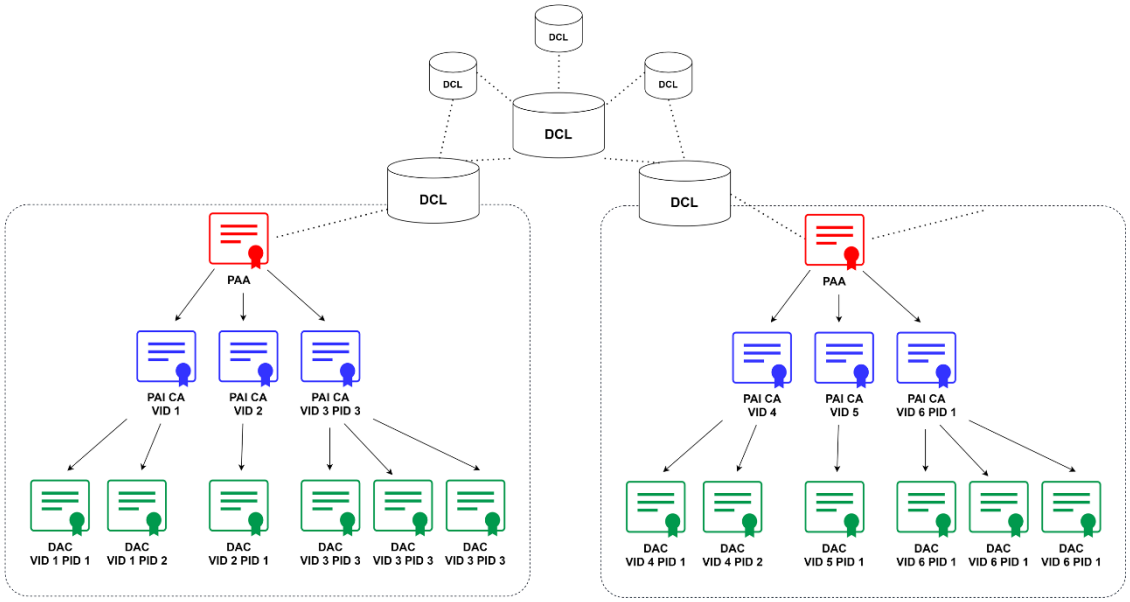

Figure 1. The PKI hierarchy of Device Attestation of Matter with DCL

2.3. Workflow of device commissioning

Device commissioning is the process of joining a node to a Fabric and establishing a secure PASE (Passcode-Authenticated Session Establishment) session using a shared passcode with a PAKE (Password-Authenticated Key Exchange) protocol is required and defined in Matter specification. During the PASE session, verifying the DAC of Matter smart home device is also a mandatory process. The below figure illustrates the workflow of commissioning a new Matter smart home device.

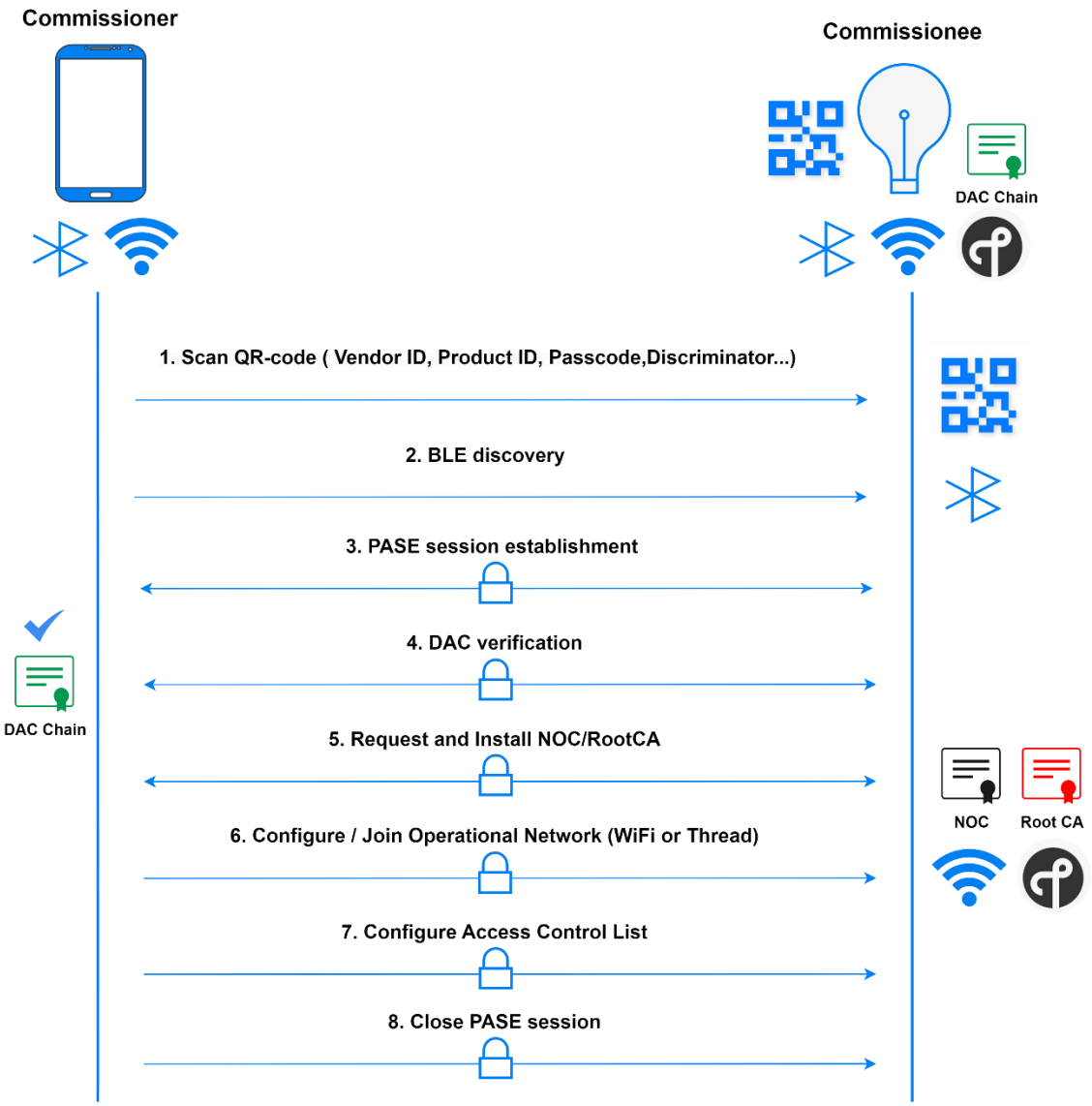

Figure 2. The workflow of commissioning a new Matter smart home device

1. The Commissioner scans the QR-Code on the device to get all the needed information to set up the Commissionee into commissioning mode. This QR-Code contains base38 encoded binary including the Version, Vendor ID, Product ID, Passcode…etc.
2. Once the Commissionee is in commissioning mode, the Commissioner will start a Bluetooth Low Energy scan to find the Commissionee.

3. Starting from this step, the PASE session between the Commissioner and the Commissionee will be established and secured based on the PAKE protocol and deriving the encryption key by key derivation function (PBKDF) from the passcode that the Commissioner obtained from QR-code.
4. The Commissioner requests a Device Attestation Certificate (DAC) chain and the Certification Declaration (CD) from the Commissionee. Since the DAC is a certificate chain that chains up to a root certificate Product Attestation Authority (PAA), the Commissioner will verify if the PAA is verified and managed by the CSA and if the CD, which is provided by the CSA as part of the Product Certification process, contains the needed information of DAC for verification.
5. Following the Device Attestation Procedure and the Commissionee is verified, the Commissioner will request operational Certificate Signing Request (CSR) from the Commissionee using the CSRRequest command in order to generate the NOC for the Commissionee and the Commissioner will install the NOC on the Commissionee using the AddTrustedRootCertificate and AddNOC commands.
6. The Commissioner configures the operational network at the Commissionee using commands such as AddOrUpdateWiFiNetwork or AddOrUpdateThreadNetwork.
7. The Commissioner configures the Access Control List on the Commissionee in any way it sees fit. The ACL will include information about the Fabric, privilege level, authentication mode, subjects…etc.
8. The commissioning process is completed and the Commissioner closes the PASE session and BLE session.

2.4. Best practices on security

- Devices and Nodes SHOULD include protection against known remote attacks that can be used to extract or infer cryptographic key material.
- Devices SHOULD protect the confidentiality of attestation (DAC) private keys. The level and nature of protection for these keys may vary depending on the nature of the Device.
- Nodes SHOULD protect the confidentiality of Node Operational Private Keys. The level and nature of protection for these keys may vary depending on the nature of the Nodes.
- Cryptographic keys SHALL be randomly chosen using a cryptographically secure random number generator in accordance with algorithms.
- Manufacturers SHOULD control the number of DACs issued under their Vendor ID.
- A Commissioner or Administrator SHOULD only add Root Certificates that it trusts to a Node.
- Protection against physical attacks (especially those that impact cybersecurity) MAY be needed for some Devices, as determined by the manufacturer.
- Requestors SHALL sign a RAD (Requestor Agreement Document) detailing Requestor responsibility, which includes the requirement that the Requestor SHALL protect the private keys and use the Certificates and private keys for authorized purposes only.

- Requestors SHOULD perform cryptographic operations on cryptographic modules rated at a minimum of FIPS 140-3 Level 1 or Common Criteria (EAL 4+).
- Requestor key pair generation MAY be performed by the Requestor or CA. If the Requestors themselves generate private keys, then private key delivery to a Requestor is unnecessary.
- If the private keys generation is performed by CA, the Requestor SHALL acknowledge receipt of the private key(s) after delivery of the private key to the Requestor.

3. INeS PKI-as-a-Service

3.1. Device attestation hierarchy for Matter

The hierarchy of device attestation for Matter is introduced in section 2.2 above, the INeS CMS is capable of issuing the DAC which is chained up to the PAI, which is created and managed by SEALSQ, and the PAA which is the self-signed root certificate that is certified by the CSA.

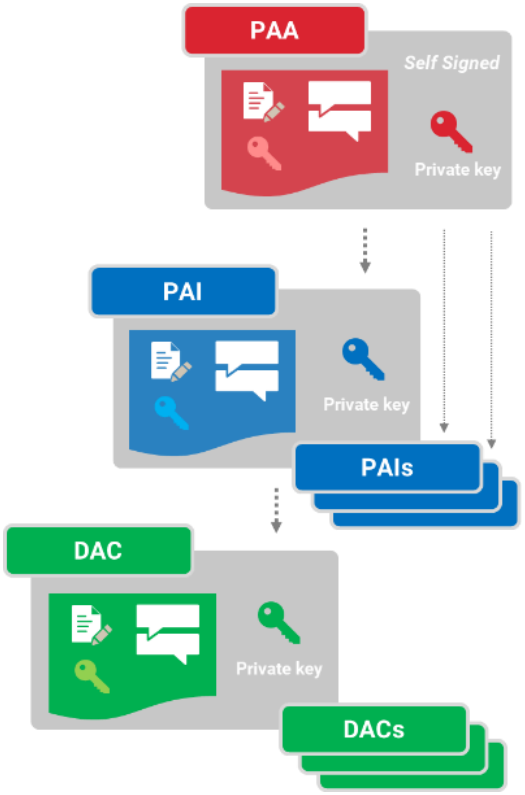

Figure 3. The PKI hierarchy of Matter DAC

SEALSQ is a WISeKey company, and WISeKey is one of few Matter certified non-VID scoped PAA at the moment. It means that SEALSQ is able to deliver managed PKI service for the smart home device makers to create their own PAI with their own VID through an offline PAI signing ceremony. The signing ceremony takes place in WISeKey PKI infrastructure based in Switzerland. Once the PAI is established, the

device makers can easily access the PAI through INeS CMS web portal and start defining the certificate template of DAC and issuing the DACs for each of the smart home devices.

3.2. INeS for Matter

INeS is a managed PKI service (PKI-aaS) that provides a set of features for managing the life cycle of certificates. In INeS web portal, there are three different modules that cover certificate management, device provisioning, and administration.

Certificate Management Service (CMS) – The features around PKI are under this module.

- Dashboarding – Users can view the statistical data of certificates in the dashboard
- Certificates management – Defining certificate templates, issuing standalone certificates or certificates in a batch, and managing the issued certificates (i.e. monitor, revoke, re-key).
- Certificate Authorities – Configuring the issuing CA for certificate issuance and integrating with the public cloud platform.
- EST enrolment – configuring the EST server for managing the certificate signing request from the EST client (Gateway/Server).

Device Provisioning Service (DPS) – The features for associating the certificate and the IoT devices.

- Device type – Defining the properties of the specific device model and configuring the mappings by associating the certificate template.
- Device inventory – The device can be generated along with the certificate issuance so that the associated subjects of the certificate will be written in the device property.
- EST enrolment – configuring the EST server for managing the certificate signing request from the EST client (IoT devices).
- External CA for authentication – INeS DPS supports certificate-based authentication and the device certificate for authentication can be issued by an external CA.

Administration – the features around user management, logs audit, and API access control.

- User management – INeS supports multi-tenancy architecture and defined three different layers of users with different authorizations to access the INeS web portal.
- Audit logs – INeS logs each operation in CMS, i.e. user login, certificate enrolment, and certificate revocation so that users can monitor the status and historical data of certificates.
- API access control – INeS supports RESTful APIs and EST enrolment for automating the certificate enrolment process and managing the life cycle of each device.

Therefore, the device maker can access the INeS web portal and configure the PAI that was created and well-maintained by SEALSQ. It

requires only a few steps of configuration, the Matter DAC for smart home devices can be issued and managed through INeS.

Once the DACs are issued from INeS, how to provision the DAC in the smart home device will be the next consideration. INeS supports different ways for provisioning the DAC in order to support different use scenarios of smart home device maker, more details will be addressed in the next section.

4. Certificate provisioning

According to the definition of Matter specification, all commissionable Matter smart home devices SHALL include a DAC and its corresponding private key. In the following sections, you will find three different options that SEALSQ offers for provisioning the DAC.

4.1. DAC generation in a Batch

According to the feedback from the device makers, the manufacturing sites usually have limited internet connectivity due to security concerns and strict IT policies.

In order to support this kind of scenario, under the INeS CMS module, the device maker can generate the DACs in a batch. Then, deploy the batch file in the production line for provisioning the DAC in each of the smart home devices. The below figure illustrates the workflow of how SEALSQ supports this use scenario.

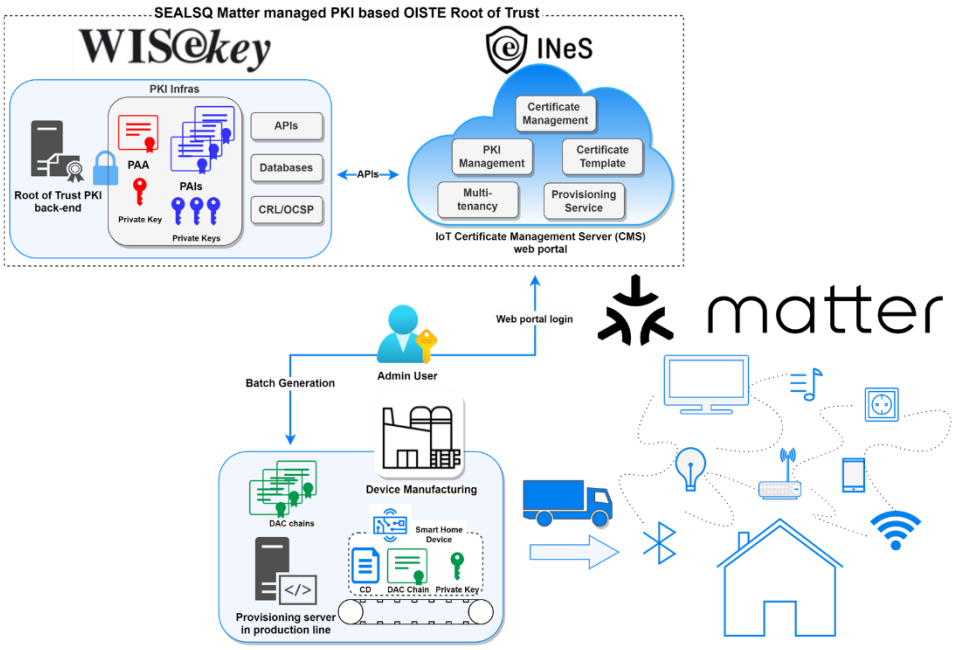

Figure 4. INeS - DAC generation in a Batch

4.2. DAC generation through RESTful/EST APIs

Some other device makers would like to put the unique device ID in the subject field of the DAC so that they can manage the devices easily by associating the hardware ID and its digital identity. Sometimes, this unique device ID is only available when manufacturing the device. Therefore, provision of the DACs on-the-fly will be an option, since INeS supports open interfaces, i.e. RESTful API and EST, for automating the certificate enrolment process. The below figure illustrates the workflow of how SEALSQ supports this use scenario.

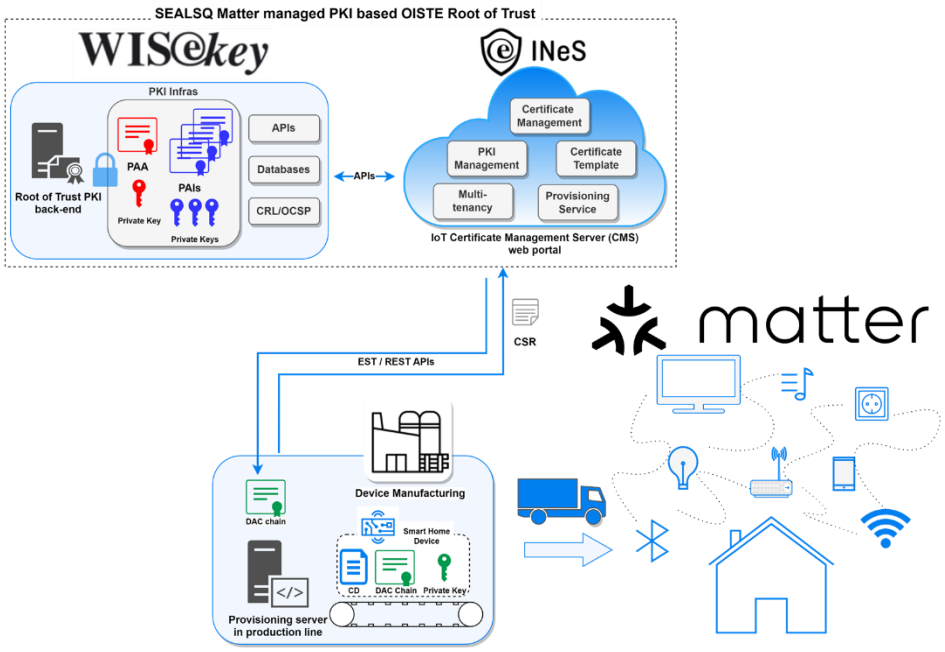

Figure 5. INeS - DAC generation on-the-fly

4.3. DAC pre-provisioned in the SE

As the PKI is mandatory for Matter smart home devices, protecting the private key would be a critical topic that device makers need to consider. The Matter specification 1.1 does not define how device makers protect the private key of DAC, different options may be

available but for many reasons the secure element is one of the most secure ways that we would recommend to the device maker.

SEALSQ has a dedicated portfolio of secure elements, such as VaultIC292 and VaultIC408, for storing the DAC as well as protecting the corresponding private key in a competitive manner. Besides, these chips also provide cryptographic functions for message encryption and are FIPS140-3 certified.

SEALSQ would provision the DAC and the private key in the secure element either at the wafer-level or at the package-level during the secure element manufacturing process, and deliver the pre-provisioned secure elements to the device makers. In this case, the device maker would spend less effort on provisioning the DAC, as they just have to integrate the SEALSQ's secure elements in the smart home devices. The below figure illustrates the workflow of how SEALSQ supports this use scenario.

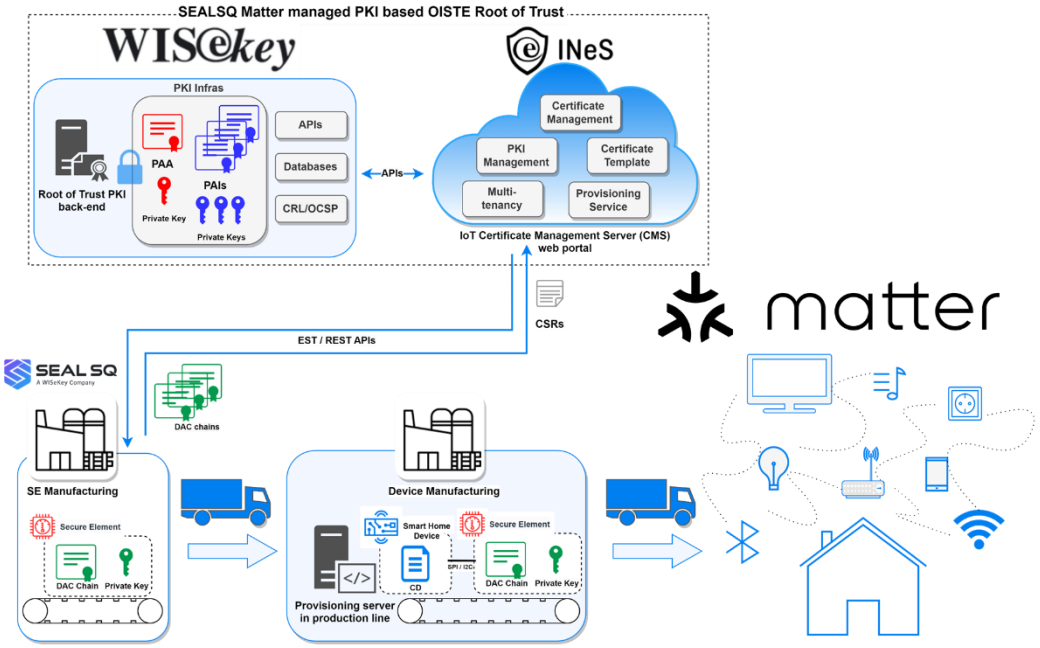

Figure 6. INeS - DAC generation and pre-provisioned in the SE

5. Conclusion

This white paper has provided an overview of Matter, a new messaging protocol designed to enhance the privacy, security, and interoperability of smart home devices, and SEALSQ's INeS PKI-aaS platform for Matter smart home devices.

By utilizing INeS managed PKI solution for Matter, smart device makers can save the time and effort of going through a long process to be verified as a VID-scoped PAA and maintaining the PKI infrastructure for issuing the PAI and DAC for Matter smart home devices. The saving of time and effort can be translated into an increased ROI and device makers can benefit from the scalability, flexibility and interoperability of the INeS PKI-aaS.

Matter represents a significant advancement in the development of secure and interoperable messaging protocols for smart home devices, and in today's increasingly digital world, secure authentication for all kinds of devices by leveraging PKI technology is being considered. Therefore, SEALSQ is offering managed PKI solution, INeS PKI-aaS, for managing the certificates for all kinds of IoT applications. Please contact our sales representatives below to learn more about our security solutions.

Sales contact: sales@wiskey.com

6. References

- Matter Specification 1.1 https://csa-iot.org/developer-resource/specifications-download-request/
- Matter PKI Certificate Policy https://csa-iot.org/wp-content/uploads/2022/11/pki-certificate-policy_april-2023.pdf

7. Abbreviation and Acronym

CA	Certificate Authority, entity that signs digital certificates
ICA	Issuing Certificate Authority
PKI	Public Key Infrastructure https://en.wikipedia.org/wiki/Public_key_infrastructure
ROT	Root of Trust. The foundation for cryptography.
CMS	Certificate Management Server
DPS	Device Provisioning Server
CSR	Certificate Signing Request
ECC	Elliptic Curve Cryptography, a public key cryptography algorithm
RSA	Rivest Shamir Adleman, a public Key cryptography algorithm
IoT	Internet of Things
SSL	Secure Sockets Layer. Secure transportation protocol replaced by TLS
TLS	Transport Layer Security. A secure transportation protocol
REST	Representational State Transfer
EST	Enrollment over Secure Transport
CSA	Connectivity Standards Alliance
ROI	Return of Investment
PASE	Passcode-Authenticated Session Establishment
PAKE	Password-Authenticated Key Exchange
PBKDF	Password-Based Key Derivation Function
RAD	Requestor Agreement Document

Disclaimer

Information in this document is not intended to be legally binding. WISeKey products are sold subject to WISeKey Terms and Conditions of Sale or the provisions of any agreements entered into and executed by WISeKey and the customer.

The products identified and/or described herein may be protected by one or more of the patents and/or patent applications listed in related datasheets, such document being available on request under specific conditions. Additional patents or patent applications may also apply depending on geographic regions.

For more information, visit www.wisekey.com or www.sealsq.com