MATTER SERIES

tech talks UPCOMING SESSIONS

FEB 9TH	Matter: Evaluation to Certification
MAR 9TH	Certifying a Matter Device: Thread and Wi-Fi
APR 6TH	Getting Started: Matter Over Wi-Fi
MAY 4TH	Start Your Matter Development Journey
JUN 1ST	Future-Proofing Matter Security with Secure Vault

2023 tech talks
WEBINAR SERIES

Welcome

Future-Proofing Matter Security

Mike Dow

SILICON LABS

Agenda

01 Matter Security Relevant Nomenclature

02 Matter Secure Commissioning

03 Matter Security Requirements

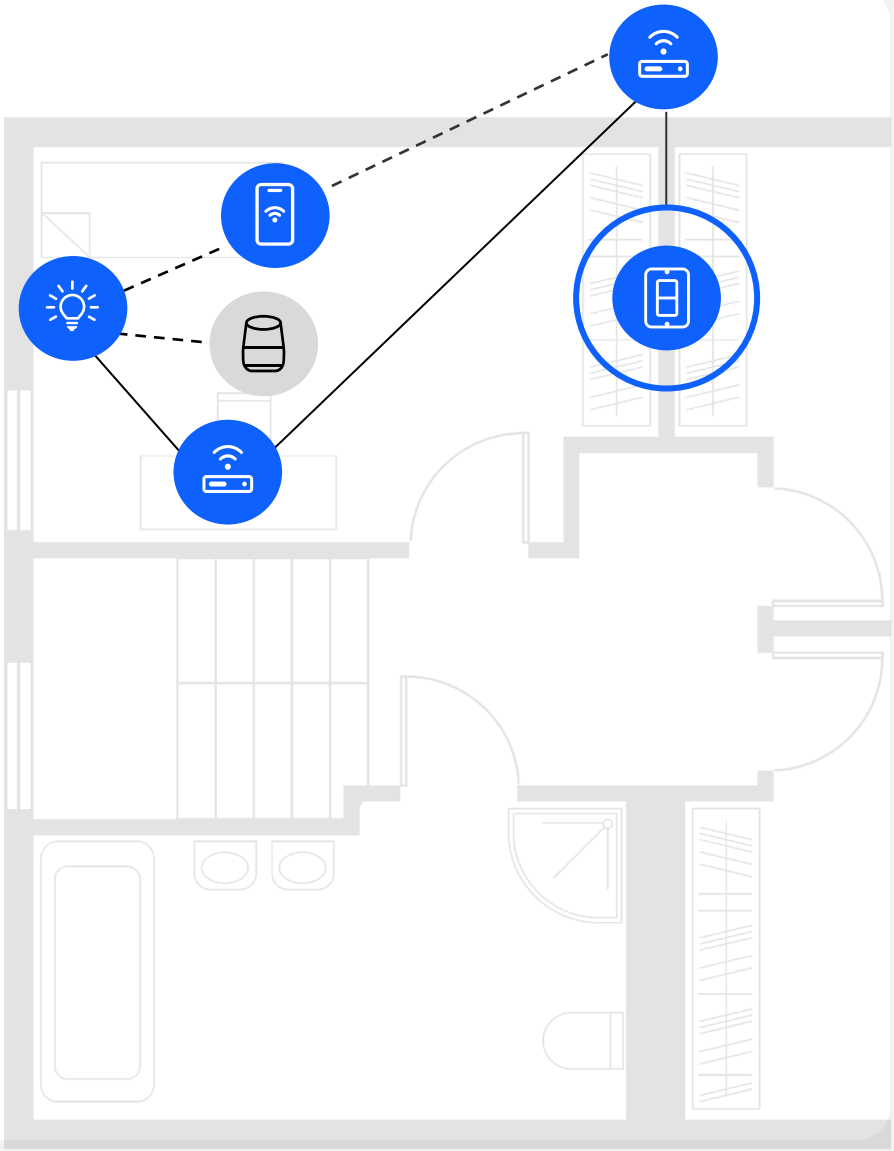
04 Matter Secure Manufacturing

05 Summary and Q&A

Matter Raises the Bar for IoT Security & Privacy

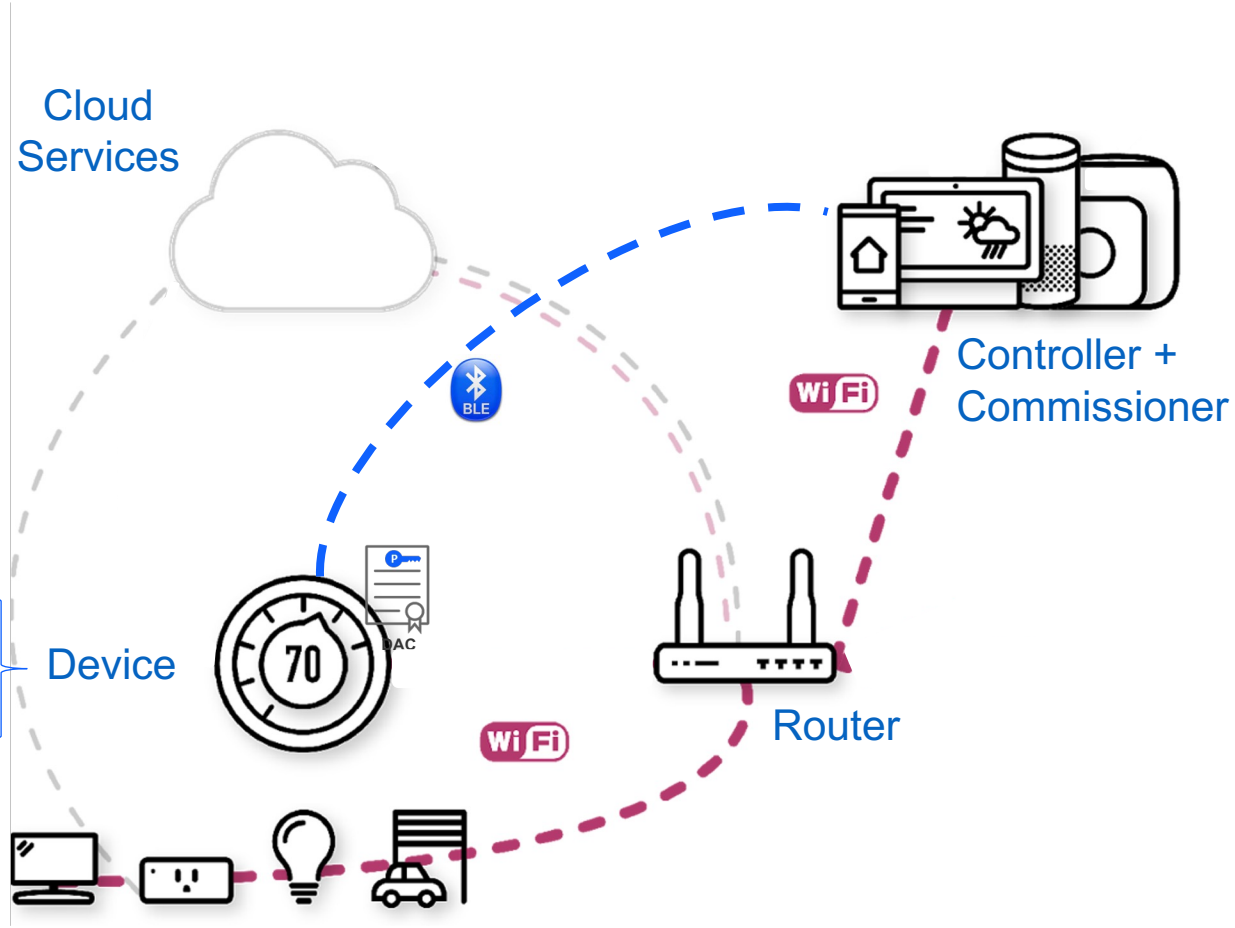
10 Security Tenants Promoted by CSA

1. Easy, secure, and flexible device commissioning
2. Validation that each device is authentic and certified
3. Up-to-date info via Distributed Compliance Ledger
4. Strong device identity so only your devices can join
5. Secured communications protecting confidentiality, etc.
6. Even group communications secured
7. Multiple administrators and controllers, maximizing choice
8. Verified access controls to prevent unauthorized actions
9. Secured, standard software updates
10. Remote monitoring of software integrity



Matter Security Relevant Nomenclature

Matter network example



Matter Secure Commissioning

Commissioning – Onboarding Payload (1)

- **It is the information used by the Commissioner to ensure interoperability between commissioners and devices.**
- **It can be encoded in different formats:**
  - Human-readable (numeric string)
  - Machine-readable (QR code and NFC tag)

Commissioning – Onboarding Payload (2)

Onboarding Payload Element	Description
Version	Provides versioning of the payload
Vendor ID	Assigned by CSA. Allows a way to identify the maker of the device.
Product ID	Vendor specified. Unique for each certified product within a Vendor ID.
Custom Flow	Indicates to the Commissioner the steps needed before commissioning can take place. - **Standard commissioning flow:** A device, when uncommissioned, always **enters commissioning mode upon power-up**. - **User-intent commissioning flow:** Device **requires user action** (pressing a button, for example) to enter commissioning mode. - **Custom commissioning flow: Interaction with a service** provided by the manufacturer is required for initial device setup.
Discovery Capabilities Bitmask	Indicate device's available technologies for device discovery: - Soft-AP - BLE - On IP Network (device is already on the IP network)
Discriminator	Helps to further identify potential devices during the setup process.
Passcode	Establishes **proof of possession** and is also **used as the shared secret for the initial secure channel** before further onboarding steps.
TLV Data	(Optional) TLV (Tag-length-value) data. Indicates manufacturer-specific information elements and/or elements common to Matter. For instance, kTag_NumberOfDevices: Number of devices that are expected to be onboarded using this payload when using the Enhanced Commissioning Method

Commissioning Steps

1

Device Discovery

- Device announces its availability for commissioning over initial network
- Commissioner finds Device
- Commissioner connects to Device
- Uses
  - Discriminator
  - Vendor ID (optional)
  - Product ID (optional)

2

Secure Channel (PASE)

- Commissioner establishes secure unicast channel to Device
- Protocol PASE = **P**assword **A**uthenticated **S**ession **E**stablishment
- Based on SPAKE2+ protocol
- Uses
  - Passcode
  - Verifier

3

Device Attestation

- Commissioner verifies Device's:
  - Vendor id (vid)
  - Product id (pid)
  - Certification status
- Uses
  - Device Attestation Credentials
  - Distributed Compliance Ledger (DCL) or
  - Certification Declaration (CD)

4

Configuration

- Commissioner configures Device:
  - Node Operational Credentials
    - Fabric ID
    - Node ID
    - Trusted Root Cert
    - ICA Cert
    - Operational Cert
    - Node Operational Key Pair
  - Access Control List (ACL)
  - Operational Network
  - Time (optional)

Commissioning Steps

1

Device Discovery

- Device announces its availability for commissioning over initial network
- Commissioner finds Device
- Commissioner connects to Device
- Uses
  - Discriminator
  - Vendor ID (optional)
  - Product ID (optional)

2

Secure Channel (PASE)

- Commissioner establishes secure unicast channel to Device
- Protocol PASE = **P**assword **A**uthenticated **S**ession **E**stablishment
- Based on SPAKE2+ protocol
- Uses
  - Passcode
  - Verifier

3

Device Attestation

- Commissioner verifies Device's:
  - Vendor id (vid)
  - Product id (pid)
  - Certification status
- Uses
  - Device Attestation Credentials
  - Distributed Compliance Ledger (DCL) or
  - Certification Declaration (CD)

4

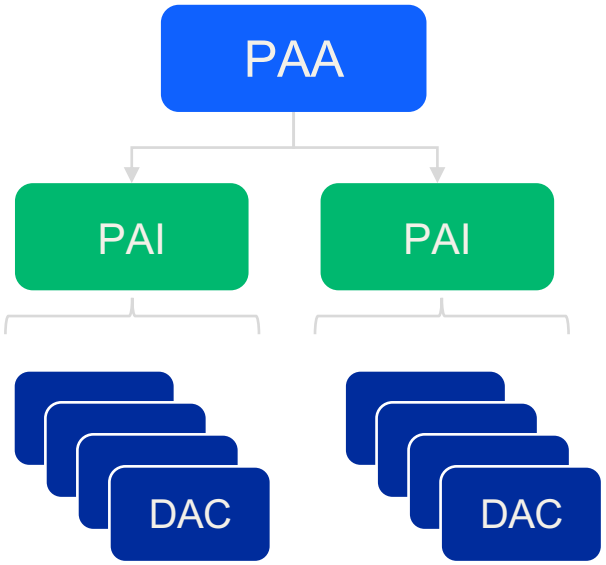
Configuration

- Commissioner configures Device:
  - Node Operational Credentials
    - Fabric ID
    - Node ID
    - Trusted Root Cert
    - ICA Cert
    - Operational Cert
    - Node Operational Key Pair
  - Access Control List (ACL)
  - Operational Network
  - Time (optional)

Public Key Infrastructure (PKI)

- A PKI is a set of roles, policies, and procedures used to create, manage, distribute, and revoke digital certificates and manage public-key encryption.

- The Matter Certificate Policy defines the rules and methods by which the Matter PKI Policy Authority (PKI-PA) is governed.



The Matter PKI for Device Attestation is comprised of:

- **Certificate Authorities:**
  - PAA (Product Attestation Authority)
  - PAI (Product Attestation Intermediate)
- **Authorized entities:**
  - DAC (Device Attestation Certificate)

Example Matter Device: Light Bulb from “Bulby Corp.”

KUDELSKI IOT THINGS

LIGHT BULB

Initial Device Credentials

NON-VID-Scoped Product Attestation Authority (PAA) Certificate (Cert)
Issuer: PAA Name
Subject: ?

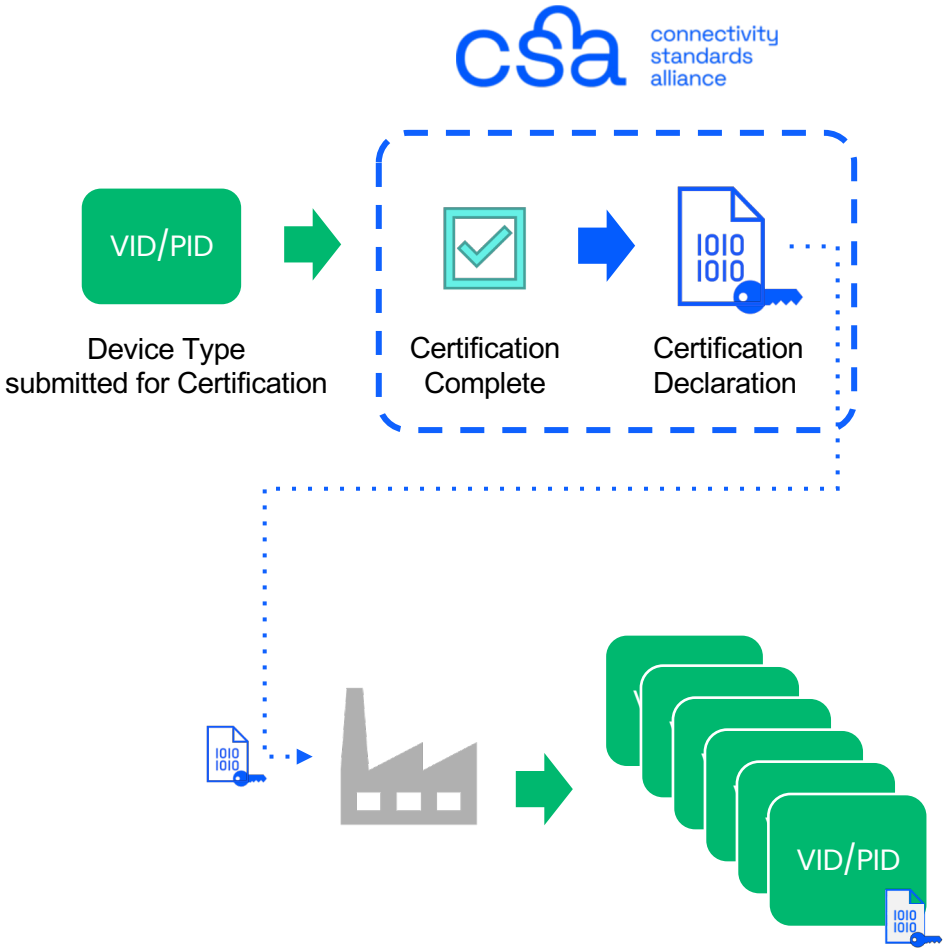
VID-Scoped Product Attestation Intermediate (PAI) (Cert)
Issuer: Silicon Labs PAI
Subject: Bulby PAI

VID-Scoped Device Attestation Cert (DAC)
Issuer: Silicon Labs PAI
Subject: Bulb 32487
Vendor ID (VID): 273
Product ID (ID): 298

Private Key for DAC Certification Declaration (CD)Verifier

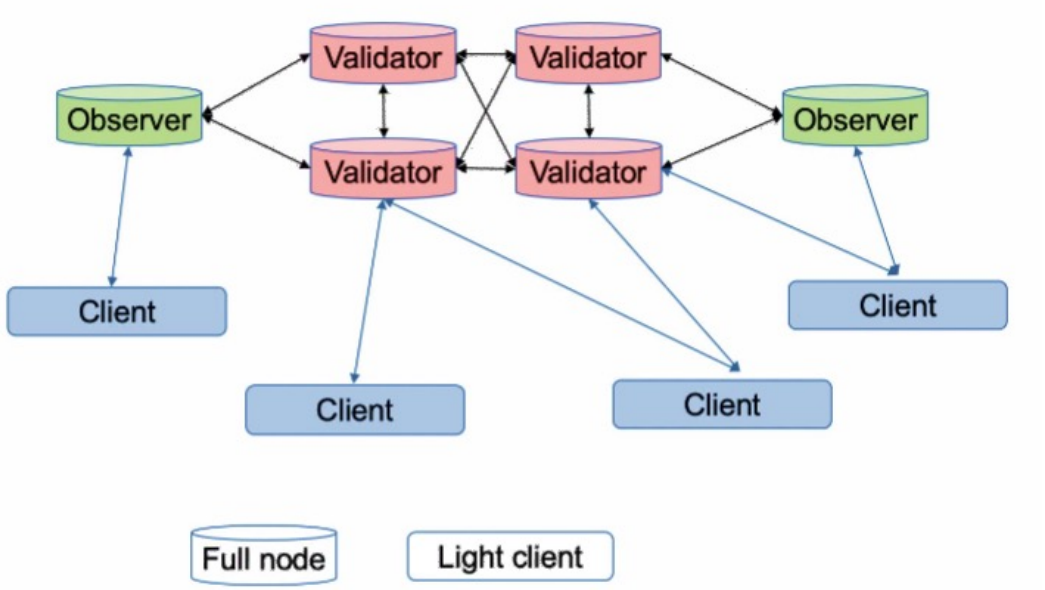
Certification Declaration

- Another data construct that is necessary for Device Attestation is the Certification Declaration... Or CD
- The CD is cryptographically signed by CSA… and contains the Vender and Device info as well as the PAA of the device
- The CD must be put into the device during manufacturing to be used during the Device Attestation process
- The Commissioner will ask for the stored CD during the commissioning of the Node



Distributed Compliance Ledger (DCL) – The immutable single source of truth

- **Blockchain-based distributed ledger of data records**
- **It contains many records about the device itself like:**
  - VID, PID,
  - Product Name,
  - Part Number and version,
  - Software and Firmware versions,
  - special Commissioning instructions
  - and URLs to product pages and user manual
- **It also contains the Root PAA certificate for that device which is needed to complete the Device certificate chain verification**
- **The DCL also contains Certification Declaration ID number that will be compared with the CD pulled from the device**



Commissioning Steps

1

Device Discovery

- Device announces its availability for commissioning over initial network
- Commissioner finds Device
- Commissioner connects to Device
- Uses
  - Discriminator
  - Vendor ID (optional)
  - Product ID (optional)

2

Secure Channel (PASE)

- Commissioner establishes secure unicast channel to Device
- Protocol PASE = **P**assword **A**uthenticated **S**ession **E**stablishment
- Based on SPAKE2+ protocol
- Uses
  - Passcode
  - Verifier

3

Device Attestation

- Commissioner verifies Device's:
  - Vendor id (vid)
  - Product id (pid)
  - Certification status
- Uses
  - Device Attestation Credentials
  - Distributed Compliance Ledger (DCL) or
  - Certification Declaration (CD)

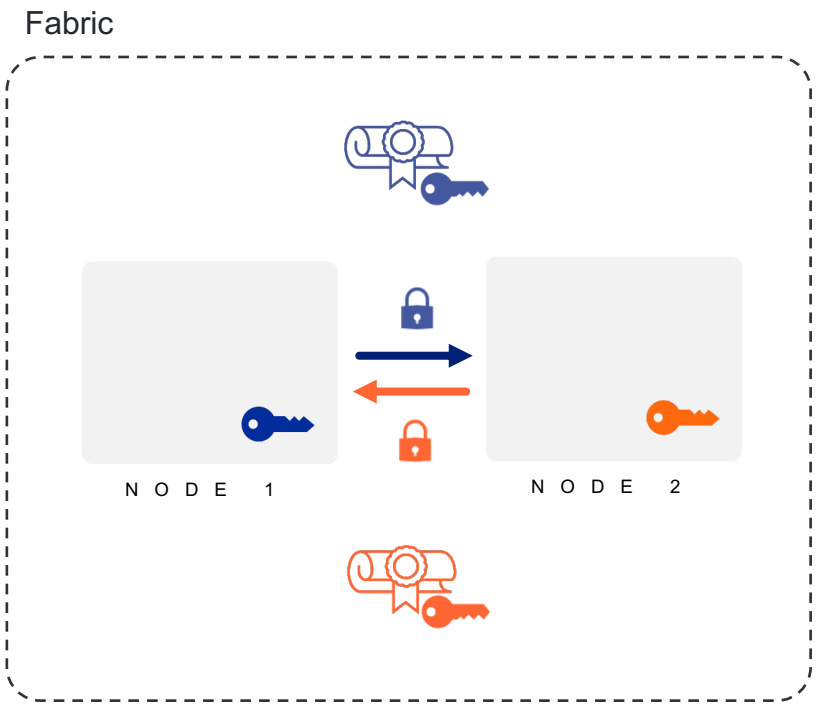
4

Configuration

- Commissioner configures Device:
  - Node Operational Credentials
    - Fabric ID
    - Node ID
    - Trusted Root Cert
    - ICA Cert
    - Operational Cert
    - Node Operational Key Pair
  - Access Control List (ACL)
  - Operational Network
  - Time (optional)

Node Operational credentials

- The Node Operational credentials enable a Node to identify itself within a Fabric.
- A Node receives its initial set of Node Operational credentials when it is commissioned to a Fabric by a Commissioner.
- **The Node Operational credentials include the following items:**
  - Node Operational Key Pair
  - Node Operational Certificate (NOC)
  - Intermediate Certificate Authority (ICA) Certificate (optional)
  - Trusted Root Certificate Authority (CA) Certificate(s)



Note: The Node Operational credentials are distinct from the Device Attestation credentials.

Commissioning Process

Uses DAC to establish that Commissioner is talking to a certified Matter device then loads operational identities for each ecosystem that it joins

Light Bulb

Node N6 on Fabric AcmeRoot.F1

Stored in the Device at manufacture

On the Block Chain

PAA Cert
Issuer: Bulby
Subject: Bulby

PAI Cert
Issuer: Bulby
Subject: Bulby PAI

Device Attn Cert (DAC)
Issuer: Bulby PAI
Subject: Bulb 32487
VID: 273
PID: 298

Private Key for DAC
Certification
Declaration (CD)
Verifier

Stored in the Device
one set per ecosystem

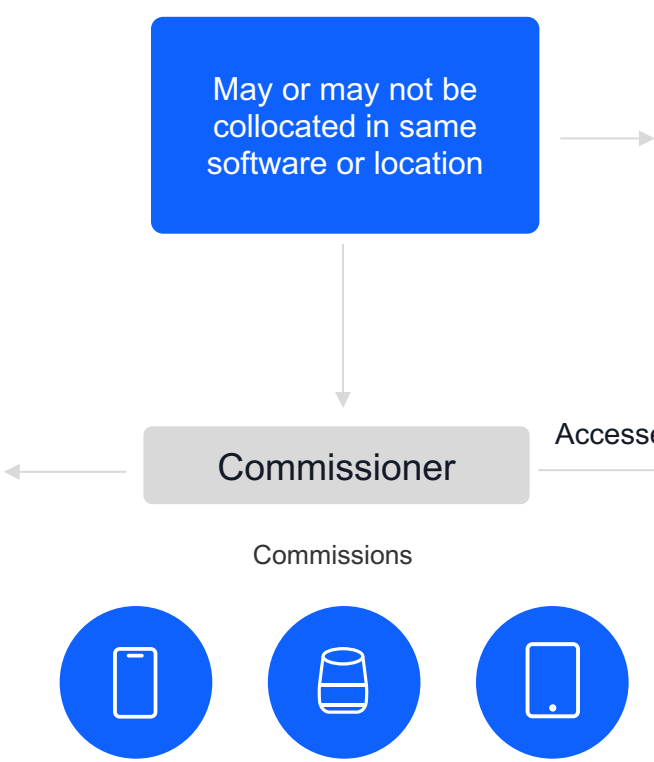
Root Cert
Issuer: Acme
Subject: Acme

ICA Cert
Issuer: Acme
Subject: ICA 27

Operational Cert (OpCert)
Issuer: ICA 27
Subject:
FabricID: F1
NodeID: N6

Private Key for OpCert
Access Control List (ACL)
Operational Network

Blue items added during commissioning



Administrative Domain Manager

ICA 27

Fabric AcmeRoot.F1
Administrative Data

- Nodes central list
- Group state central list
- Proprietary application data model

Commissioning Steps

1

Device Discovery

- Device announces its availability for commissioning over initial network
- Commissioner finds Device
- Commissioner connects to Device
- Uses
  - Discriminator
  - Vendor ID (optional)
  - Product ID (optional)

2

Secure Channel (PASE)

- Commissioner establishes secure unicast channel to Device
- Protocol PASE = **P**assword **A**uthenticated **S**ession **E**stablishment
- Based on SPAKE2+ protocol
- Uses
  - Passcode
  - Verifier

3

Device Attestation

- Commissioner verifies Device's:
  - Vendor id (vid)
  - Product id (pid)
  - Certification status
- Uses
  - Device Attestation Credentials
  - Distributed Compliance Ledger (DCL) or
  - Certification Declaration (CD)

4

Configuration

- Commissioner configures Device:
  - **Node Operational Credentials**
    - Fabric ID
    - Node ID
    - Trusted Root Cert
    - ICA Cert
    - Operational Cert
    - Node Operational Key Pair
  - Access Control List (ACL)
  - Operational Network
  - Time (optional)
  - **Establish Secure Comms with other Nodes using CASE**

Matter Security Requirements

Matter Security as Specified by CSA

MANUFACTURING

Matter devices must be injected with a unique DAC certificate/ private key, Onboarding Payload (QR code delivered), Certification Declaration (CD), and other static/ dynamic data during manufacturing. **(SHALL)**

COMMISSIONING

DAC with VID/PID must be checked against the DCL and CD verified to ensure only authentic and certified Matter devices are commissioned. **(SHALL)**

DEVICE COMMUNICATION

Communication between Matter devices must be secured and encrypted using cryptographic keys and PBKDF. **(SHALL)**

SOFTWARE UPDATES

Devices must support OTA firmware updates to allow vulnerabilities to be patched **(SHALL)**

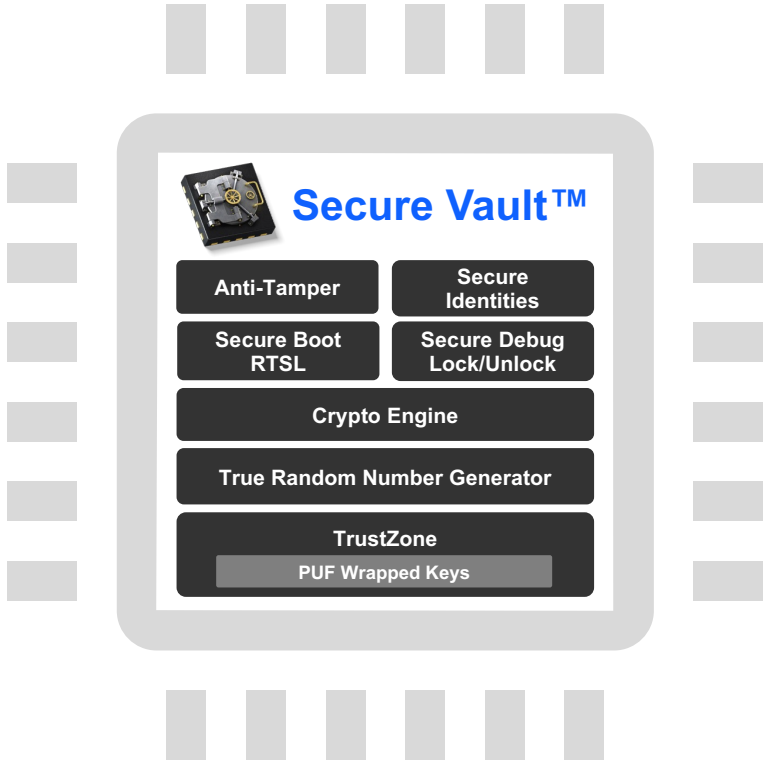
OTHER SECURITY SPECIFICATIONS

- Authentication and encryption keys must be generated by a “Deterministic Random Bit Generator” Seeded by NIST 800-90B TRNG **(SHALL)**
- Debug interfaces and access to secure boot trust anchors should be disabled to only allow authorized access (fusing) **(SHOULD)**
- DACs and operational private key confidentiality should be protected from *remote* attacks **(SHOULD)**
- Vendors should have a public policy & mechanism to identify and rectify security vulnerabilities in a timely manner **(SHOULD)**
- The software should be encrypted *at rest* to prevent unauthorized access to core IP **(MAY)**
- Some devices should be protected against *physical* attacks to prevent tampering, side-channel, or debug glitching attacks. **(MAY)**

Matter Compliant Security Solution

- Secure Vault Mid or High supports all Matter security functionalities now (Shall) and future (Should, May)
- Uncrackable keys are generated by the True Random Number Generator (TRNG)
- For DAC, secure boot, secure debug, OTA, software image and communication encryption
- The Crypto Engine assists with special algorithms like SPAKE2+ and CASE with side channel protection
- Secure key storage at PSA/SESIP Level 2 (Mid) and Level 3 (High):
  - Private keys are stored with a TEE/TZ (SV Mid), or PUF Wrapped (SV High)
- Secure Matter Identities (DACs) securely programmed at our factory
- Secure Boot with RTSL ensures code running on the device is trusted.
- Secure OTA firmware updates in conjunction with Secure Boot prevents the installation of malicious software and allows for vulnerability patching
- Glitch Mitigated Secure Debug Lock/Unlock only allow authorized access with security tokens that can be revoked
- Anti-Tamper protects from physical attacks (SV High)

RTSL – Root of Trust and Secure Loader
TEE – Trusted Execution Environment
TZ – TrustZone
SV – Secure Vault



PSIRT Monitors & Rectifies Security Vulnerabilities

Matter Secure Manufacturing

Secure Programming for Matter - Process Summary

What Needs to Happen Before Secure Programming

Certify the Product for Matter with CSA
- Get Certification Declaration (CD)

- Code
- Certification Declaration from CSA

Generate Secure Boot and Debug Key Pairs (HSM)
- Acquire DACs

- Secure Boot/Secure Debug Private/Public Key Pairs
- DACs

Sign Code + Bootloader with a Private Key

- Signed Code + Bootloader
- DACs

Store Private Keys in HSM
- Deliver DACs and Private Keys securely to CM or silicon vendor
- Deliver CD and Factory Data to CM or silicon vendor

HSM – Hardware Security Module

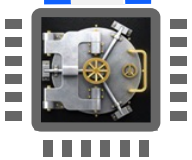
Programming…. Secure?

Secret Keys
- Secure Boot & Debug Public Keys written to OTP Memory
- Custom Keys
- OTA Decrypt Key

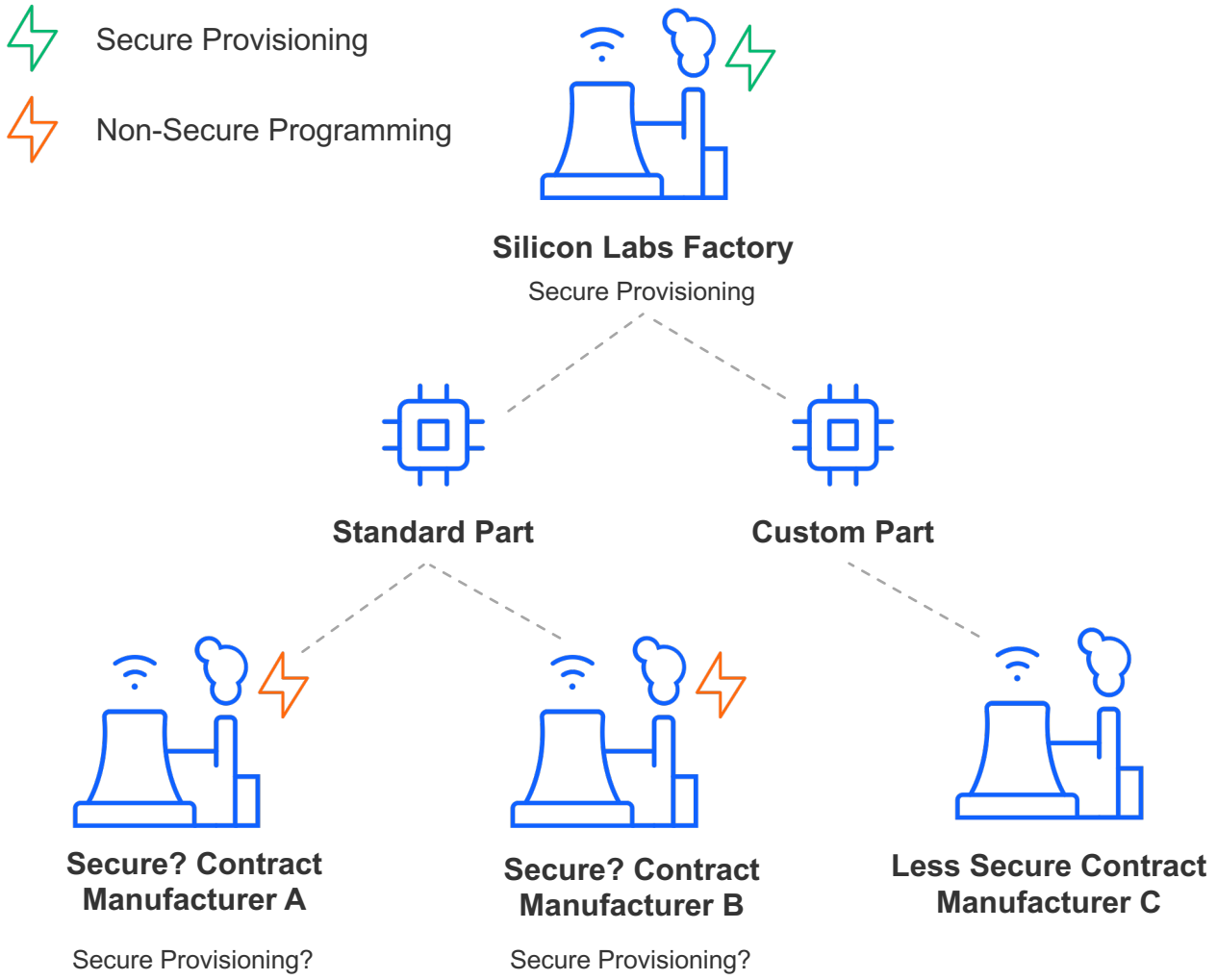
Security
- Lock Flash Pages
- Enable Secure Boot/Secure Debug (OTP)
- Set Default Tamper

Matter Provisioning
- Official Product DAC
- Other Factory Data
- Certification Declaration
- Onboarding Payload

Flashing
- Customer Application
- Bootloader

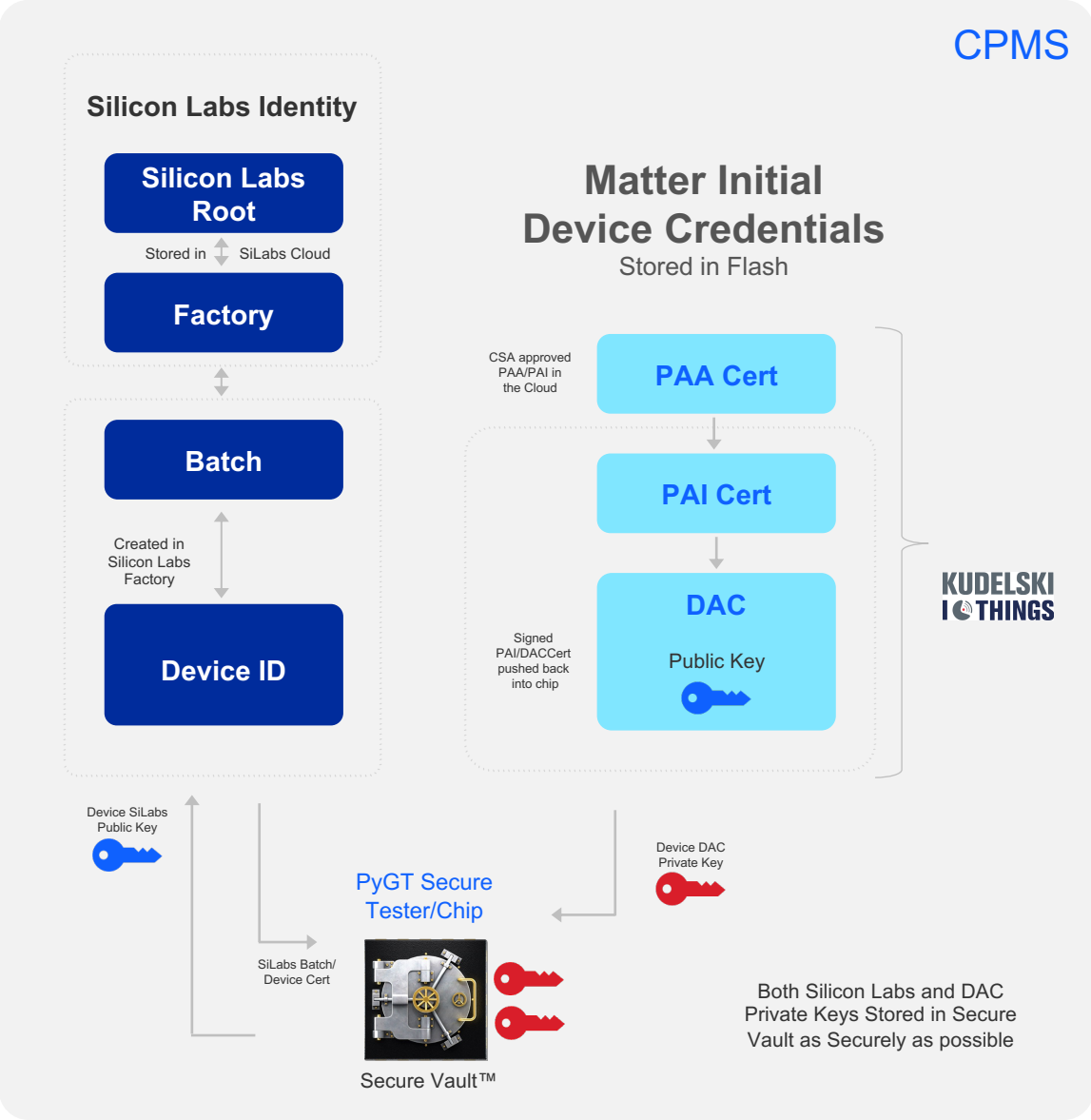


CPMS for Matter is Secure Provisioning – Alpha Program launching June 1st !



- **Available for EFRMG24A/B 15.4 Thread parts and coming soon for Si915/917 Wi-Fi parts**
- **Easy to use web user interface**
- **Receive 10 samples within 4-6 weeks for $500 flat fee (free for Alpha customers)**
- **Matter Security Credential Injection:**
  - DAC and PAI
  - Certification Declaration
  - Onboarding Payload
  - Secure Boot and Debug Public Keys
  - OTA Decryption Key
- **Secure Debug Locked**
- **Secure Boot Enable**
- **Tamper Options Set**
- **Anti-rollback Set**
- **Bootloader pre-flashed for protection of Software IP**
- **Application Flashed**

CPMS = Automated Injection of Matter certificates along side Silicon Labs chip identity



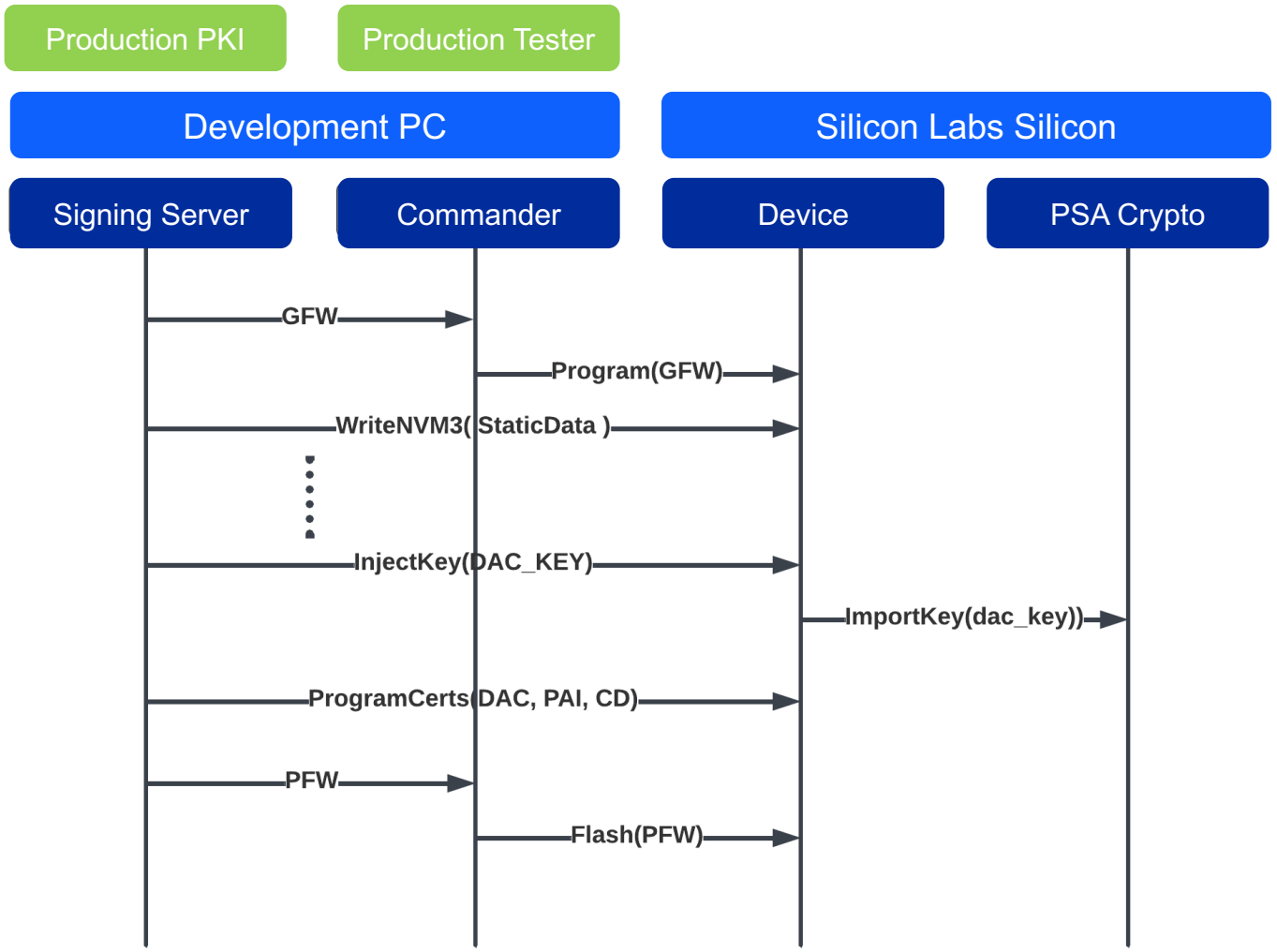
- **Silicon Labs Identity injected in our factory for Secure Vault™ Parts (optional on Secure Vault™ Mid Parts)**
  - Private and Public Keys generated in the silicon and public key pushed to our manufacturing infrastructure
  - Device and Batch Certificates created in manufacturing infrastructure and pushed back into the silicon and stored in OTP fuses

- **Matter Identity Chain delivered by Kudelski in Just-in-Time mode**
  - PAI and DAC Certificates stored in Silicon's flash
  - DAC Private Key stored as securely as chip will allow:
    - For Secure Vault™ High – Private DAC Key is PUF wrapped which protects it against Remote Logical attacks and Local Physical attacks)
    - For Secure Vault™ Mid – Private DAC Key is in Flash behind a Trusted Execution Environment (TEE) which protects it from Remote Logical attacks

General Provisioning Flow for Development and Production or CPMS

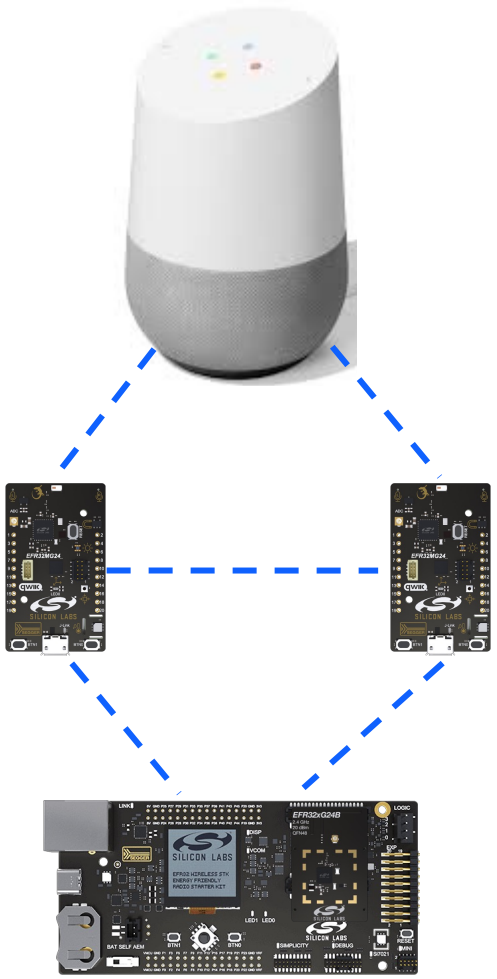
- **Generating Firmware (GFW):** This is a small program than runs in the device and talks to the Signing Server to receive the Onboarding Payload, the DACw/Private Key and the PAI.
- **Provisioning script (provision.py):** Main script driving the provisioning process. Is in charge of flashing the firmwares into the target device, interacting with the GFW, and the Signing Server
- **Signing Server Script:** During development, this script abstracts the role of the Certificate Authority. It delivers to the GFW the Onboarding Payload, the DACw/Private Key and PAI when asked. And delivers to the Provisioning Script the signed Production Firmware when requested.
- **Production Firmware (PFW):** Software that will run in production, replacing the GFW at the end of the provisioning process
- **Initial script (initialize.py):** This script runs once, setting the environment for all the boards in the line.

1. An initialization script (initialize.py) runs, preparing the environment. This is done once.
2. A provisioning script (provision.py) is run for each board in the line. This script performs the following actions:
    1. Flashes the GFW
    2. Flashes the Static Data
    3. Inject the DAC Private Key
    4. MCU Saves the Private Key with PSA Crypto
    5. Flashes the DAC, PAI, and CD
    6. Flash the PFW

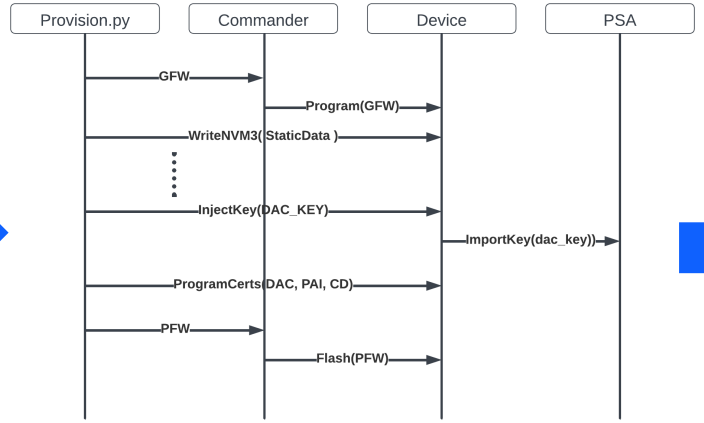


Evaluation ➡ Development ➡ Production… Made Easy

Evaluation



Development



Production

Or… CPMS
Production Volume
Linked to Customers VID/PID

SILICON LABS

Summary

Summary

matter

- Matter raises the bar on security to a new level beyond simply guaranteeing the communication pipe is secure… now the end device must be proven to be authentic
- The Matter Node Security will likely raise over time… as threats evolve the SHOULDs will become SHALLs
- Creating Secure Identities and injecting them securely in your manufacturing process is not trivial and can be costly
- Silicon Labs has the hardware, software, and services to get your secure Matter products to market quickly and cost effectively

Q&A

MATTER SERIES

That’s a wrap!

All sessions are available on-demand.

tech talks ON-DEMAND SESSIONS

FEB 9TH	Matter: Evaluation to Certification
MAR 9TH	Certifying a Matter Device: Thread and Wi-Fi
APR 6TH	Getting Started: Matter Over Wi-Fi
MAY 4TH	Start Your Matter Development Journey
JUN 1ST	Future-Proofing Matter Security with Secure Vault

2023 tech talks
WEBINAR SERIES

Thank You

Watch ON DEMAND

silabs.com/training