SILICON LABS

works with
BY SILICON LABS

MAT-201

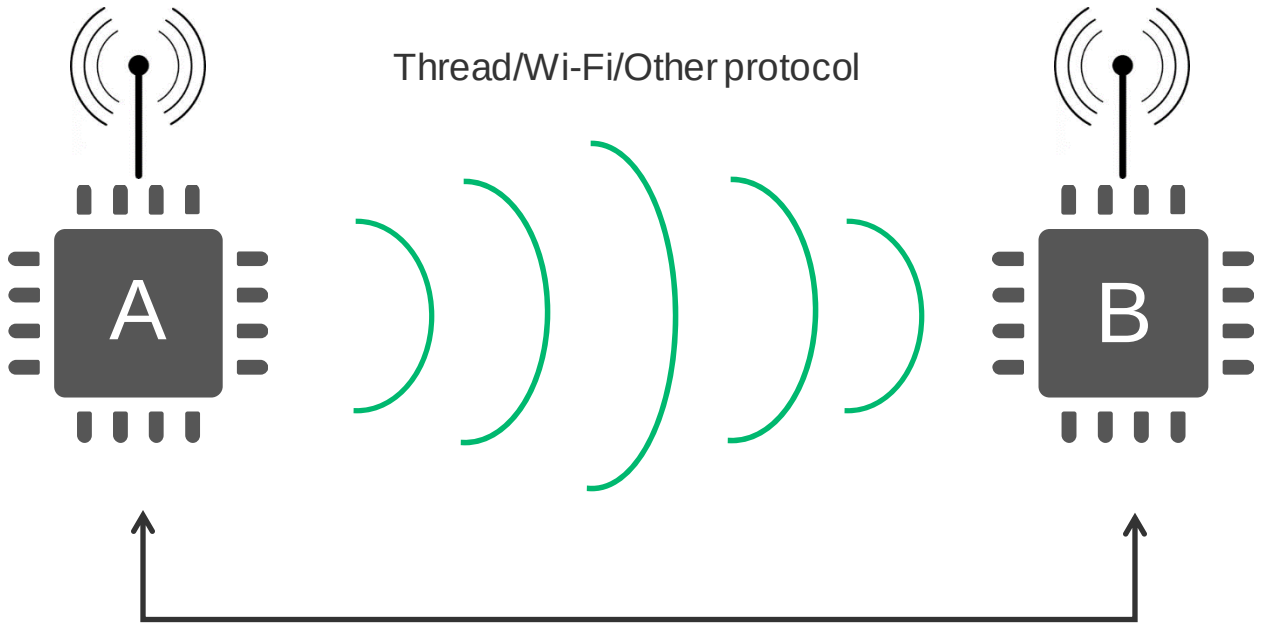
# Building a Robust and Secure Matter Device

Rohit Ravichandran | August 2023

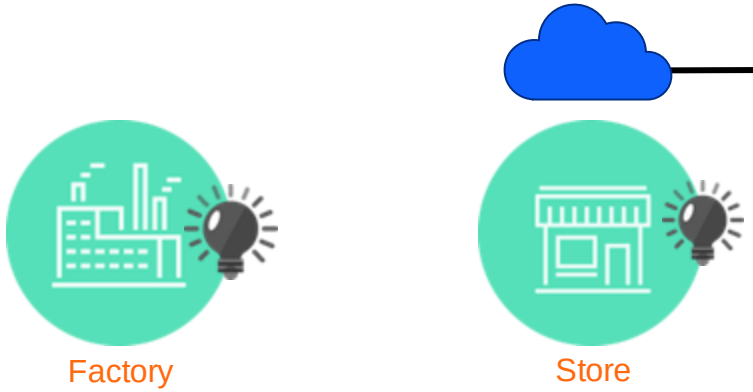
# Agenda

1. **Why Matter?**
2. **4 Important Pieces to Securing Matter Devices**
   - Matter Requirements
   - Silicon Labs Recommendations
3. **CPMS Overview and Matter Alpha Program**
4. **Key Takeaways**

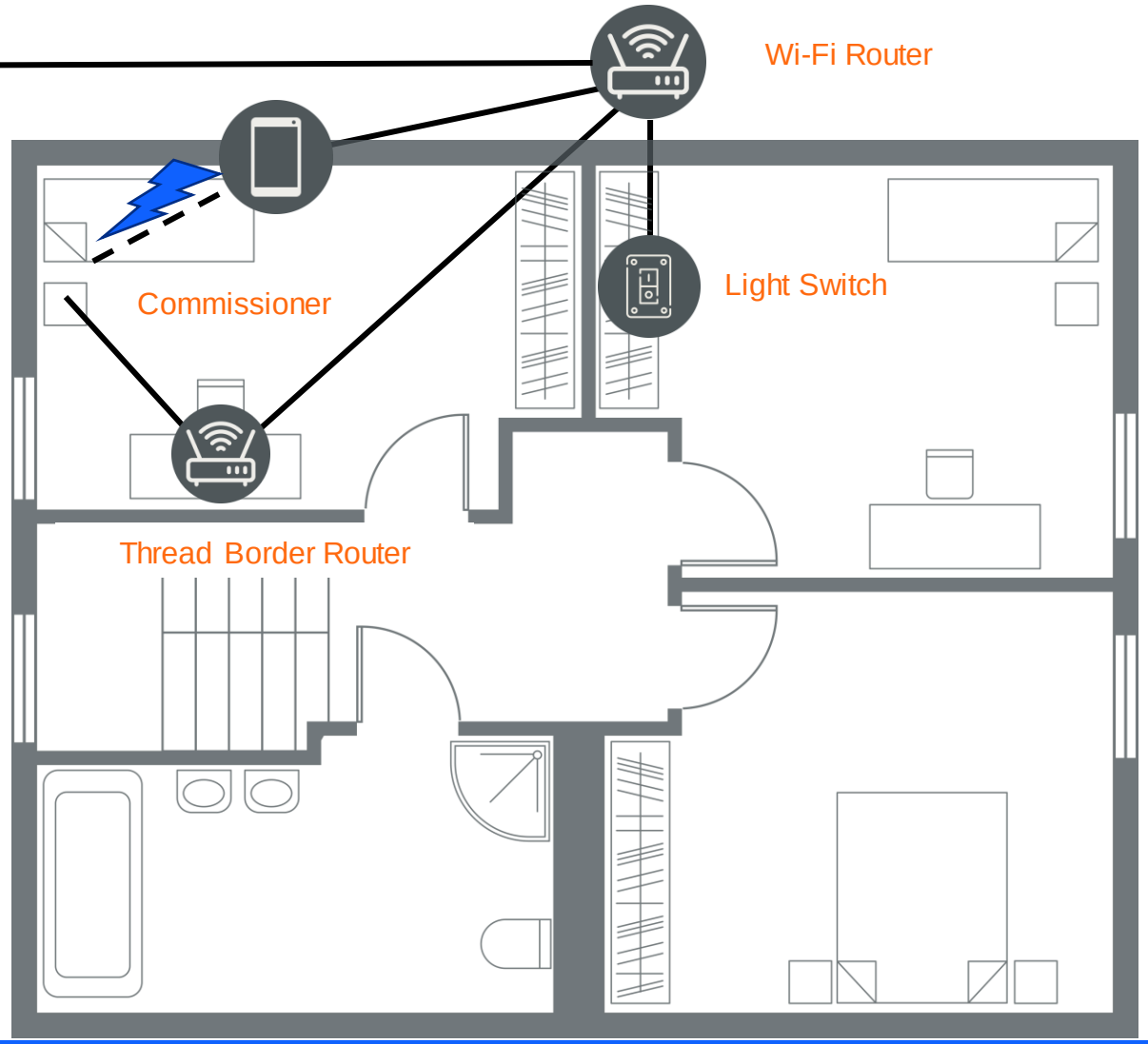
# Why Matter?



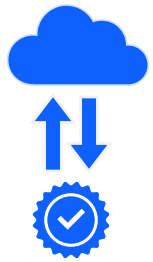
# Matter Journey




1. Device is manufactured and shipped
2. User brings Device to Smart Home
3. User intros Device to Commissioner (Tablet, Phone, Smart Speaker, etc.)
4. User initiates commissioning
5. Device is commissioned
6. Device operates smoothly in Smart Home

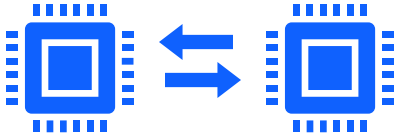


# 4 Important Pieces to Securing Matter Devices



Secure Commissioning

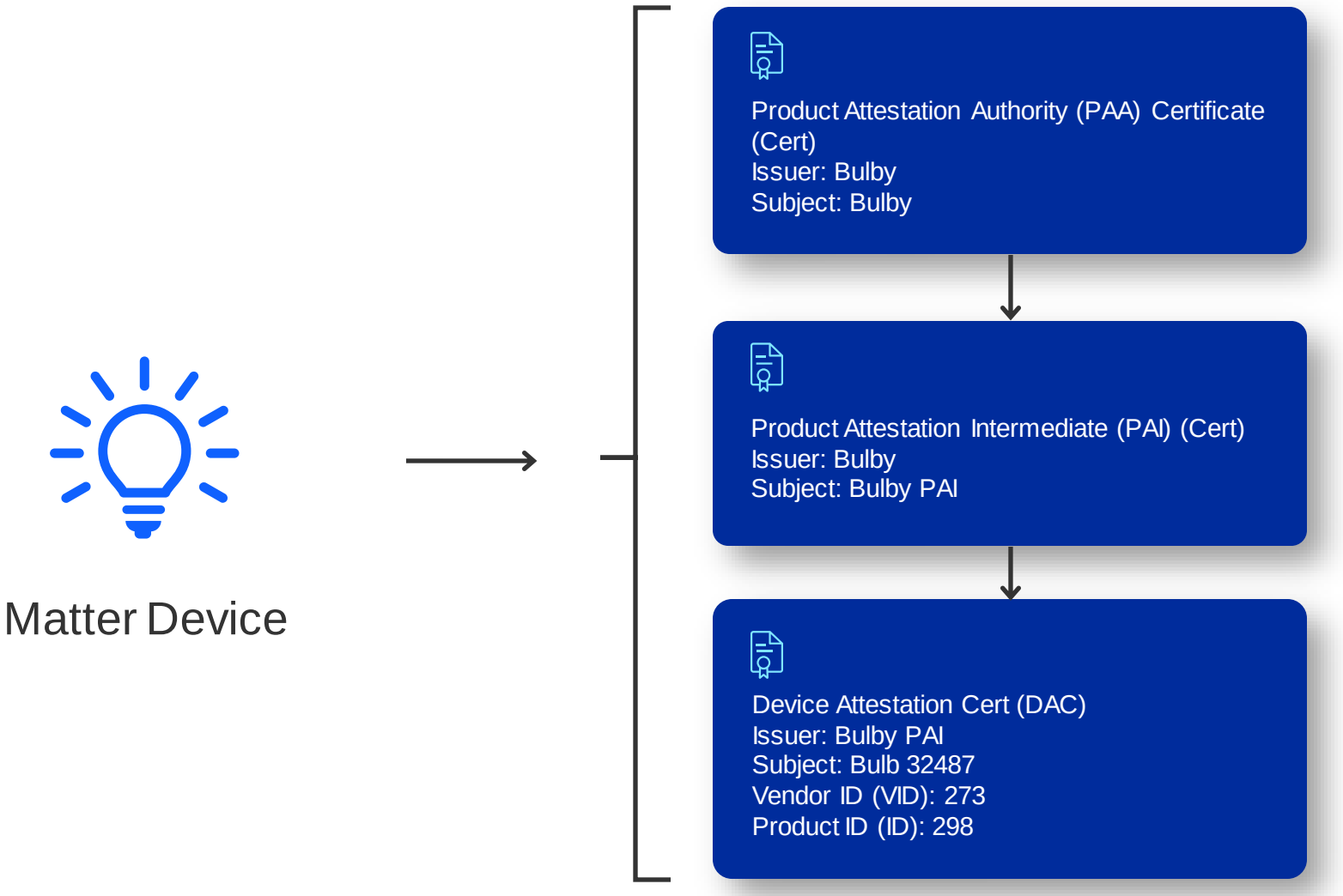
Verified Software Updates



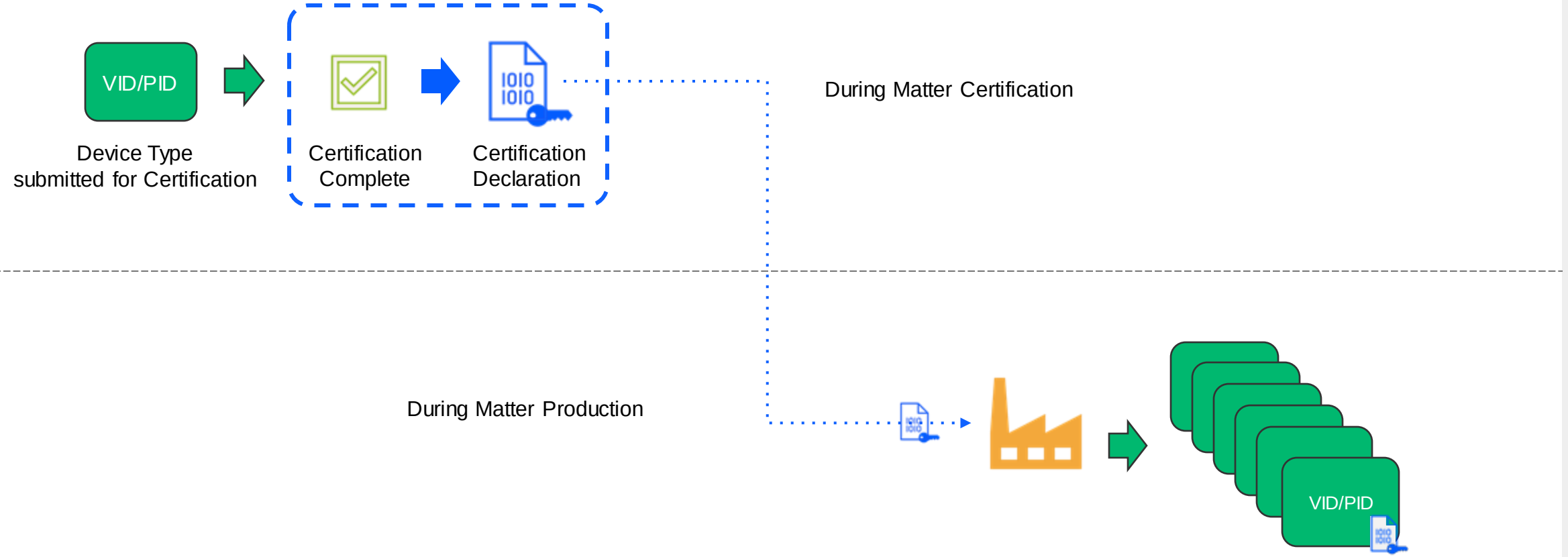
Secure Communication

Secure Manufacturing

# Matter Commissioning – Verifying the DAC



# Matter Commissioning – Verifying the Certification Declaration (CD)



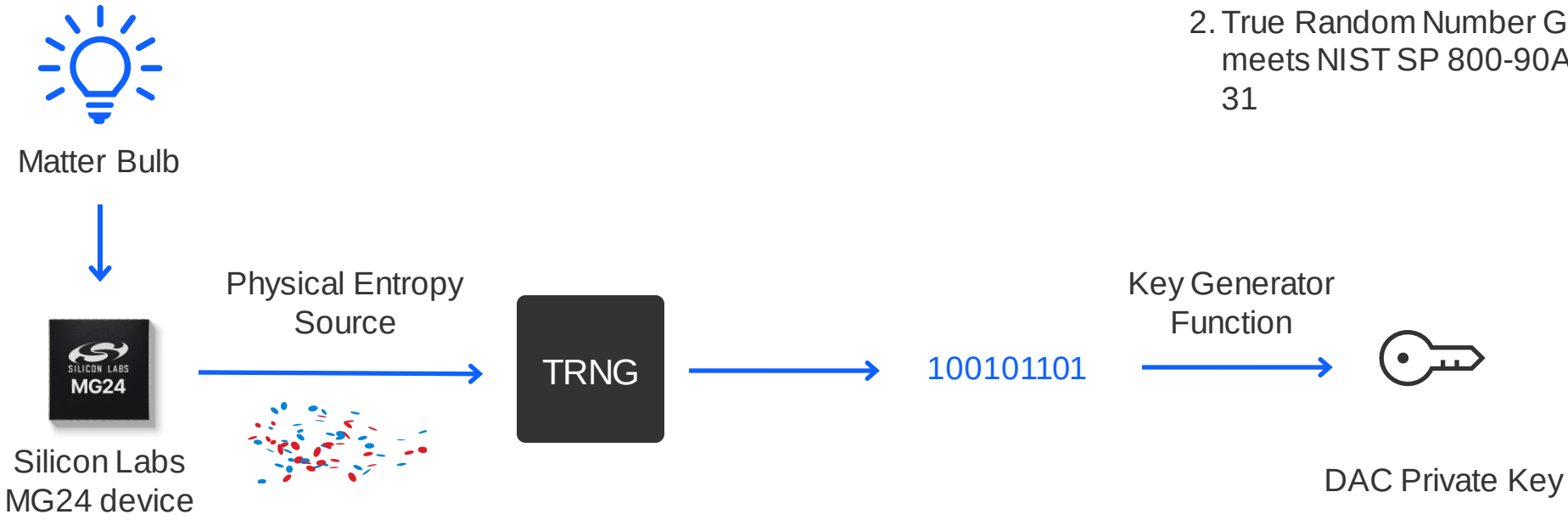
# Secure Commissioning Requirement: Unique DAC and Private Key

### 6.2.2. Device Attestation Certificate (DAC)

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-

| | |
|---|---|
| CM23 | All Devices include a Device Attestation Certificate and private key, unique to that Device. |

# True Random Number Generator (TRNG)




**Benefits**

1. Key is unique to device
2. True Random Number Generator meets NIST SP 800-90A/B/C and AIS-31

# Verified Software Updates Requirement: Image Encryption & Over-the-Air (OTA) Software Updates

#### 11.19.4.1. Image Encryption

A Vendor MAY apply at-rest encryption to Software Image bodies, excluding the Software Update Image Header, using any algorithm of its choosing.

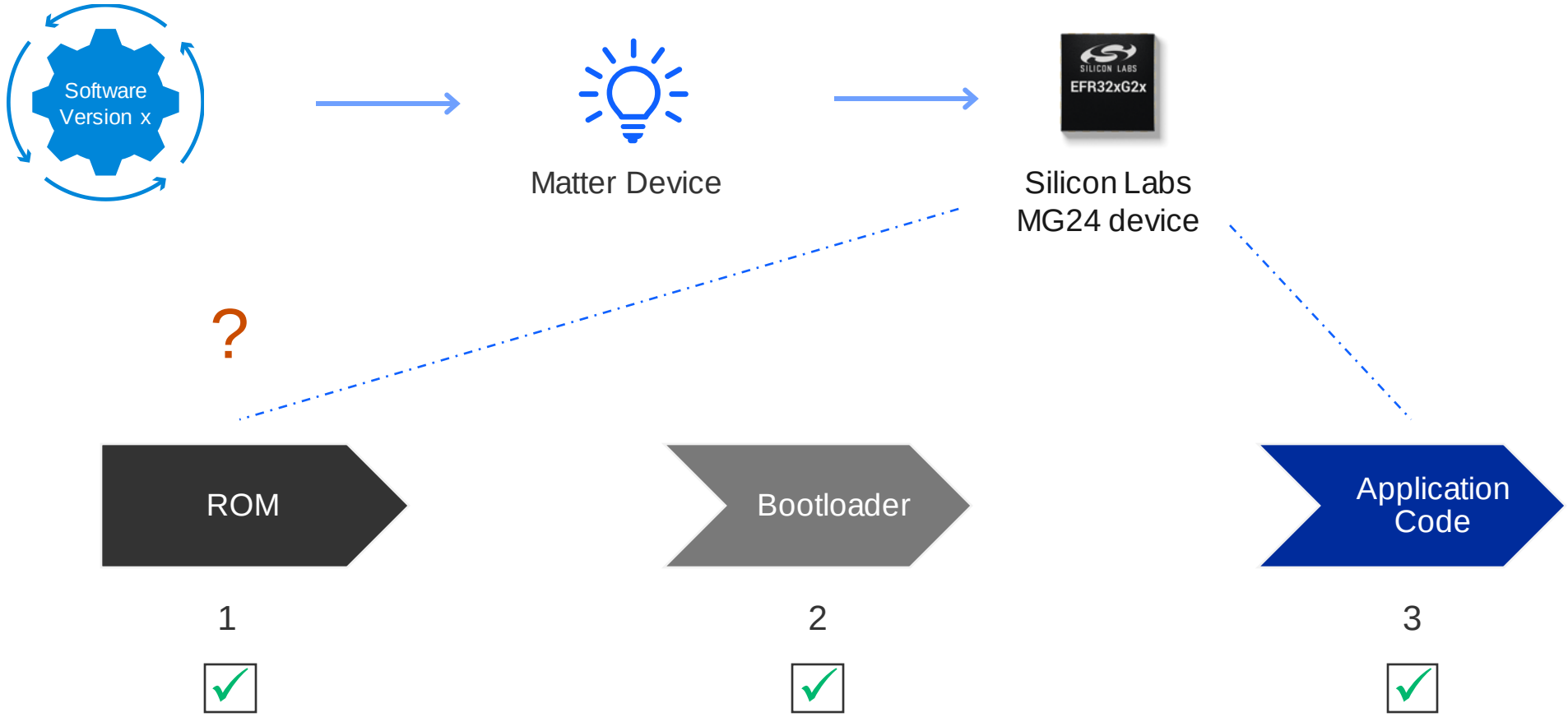
## 13.5. Firmware

a. Nodes SHALL support OTA firmware updates, either using Matter-provided means (see Section 11.19, “Over-the-Air (OTA) Software Update”) or proprietary means. [CM58 for T59]

b. Nodes SHALL validate the authenticity and integrity of the firmware prior to installation, such as through cryptographic means (see Section 11.19.4.2, “Image Verification”). [CM58 for T59]

b. Devices SHOULD have a verified boot based in an immutable root of trust to verify the authenticity of firmware. Commissioners SHOULD only be loaded on a computing platform that has such a verified boot. If devices cannot support verified boot, devices SHOULD perform verification on any firmware update before applying the new firmware. [CM22 for T16, T20]

# Secure Boot and OTA Firmware Updates



# Secure Communication Requirement: Secure Key Storage

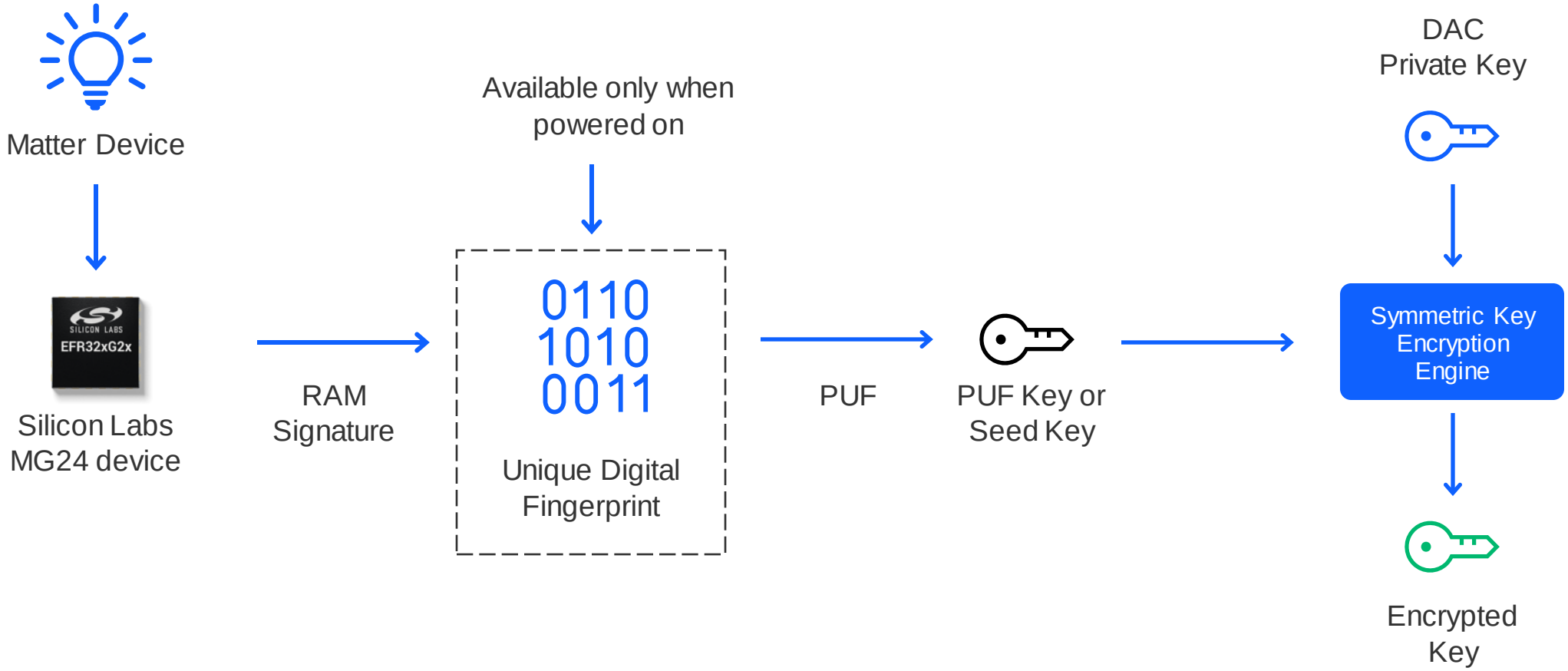
### 13.6.1. Cryptography

a. Devices and Nodes SHOULD include protection (if it exists) against known remote attacks that can be used to extract or infer cryptographic key material. [CM107 for T94]

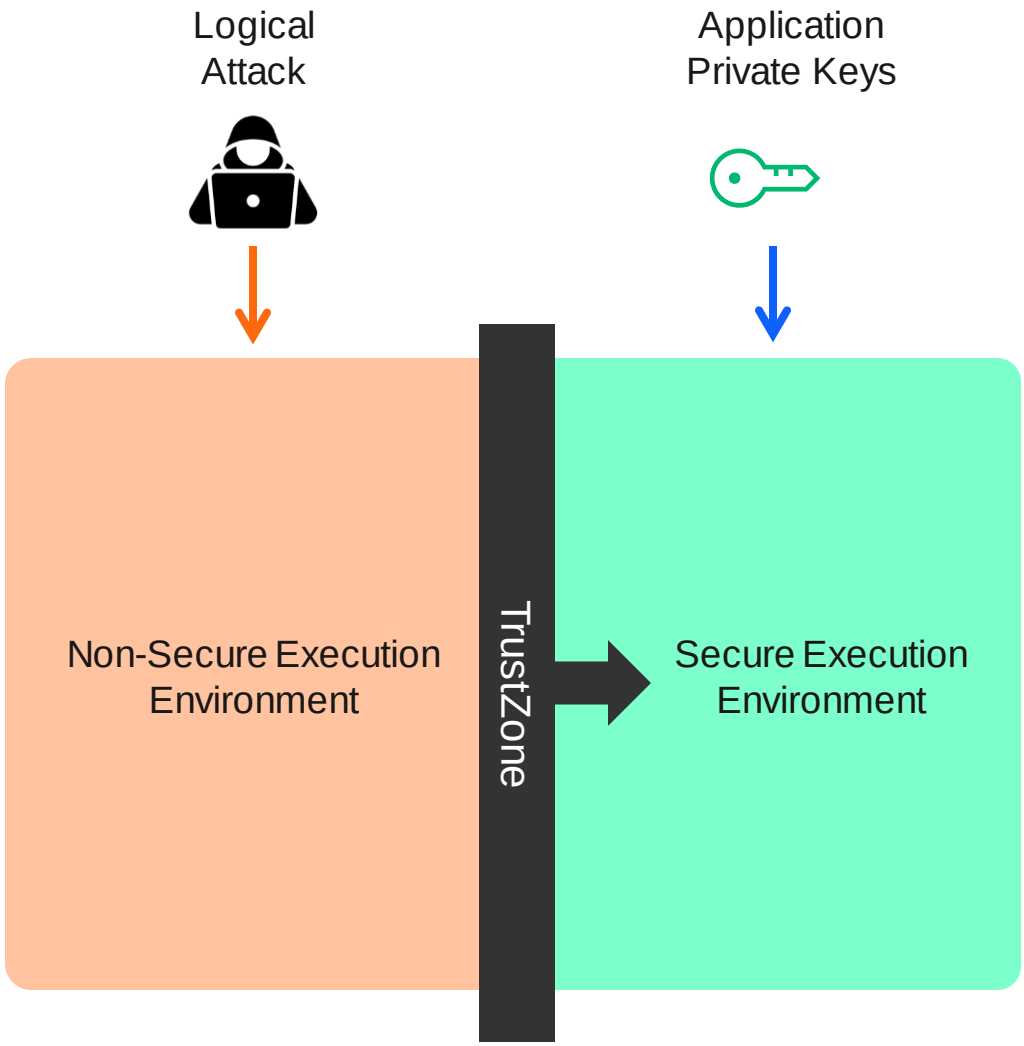
b. Devices SHOULD protect the confidentiality of attestation (DAC) private keys. The level and nature of protection for these keys may vary depending on the nature of the Device. [CM77 for T22]

c. 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. [CM87 for T87, T110, T120]

# Physically Unclonable Function (PUF)



# ARM TrustZone

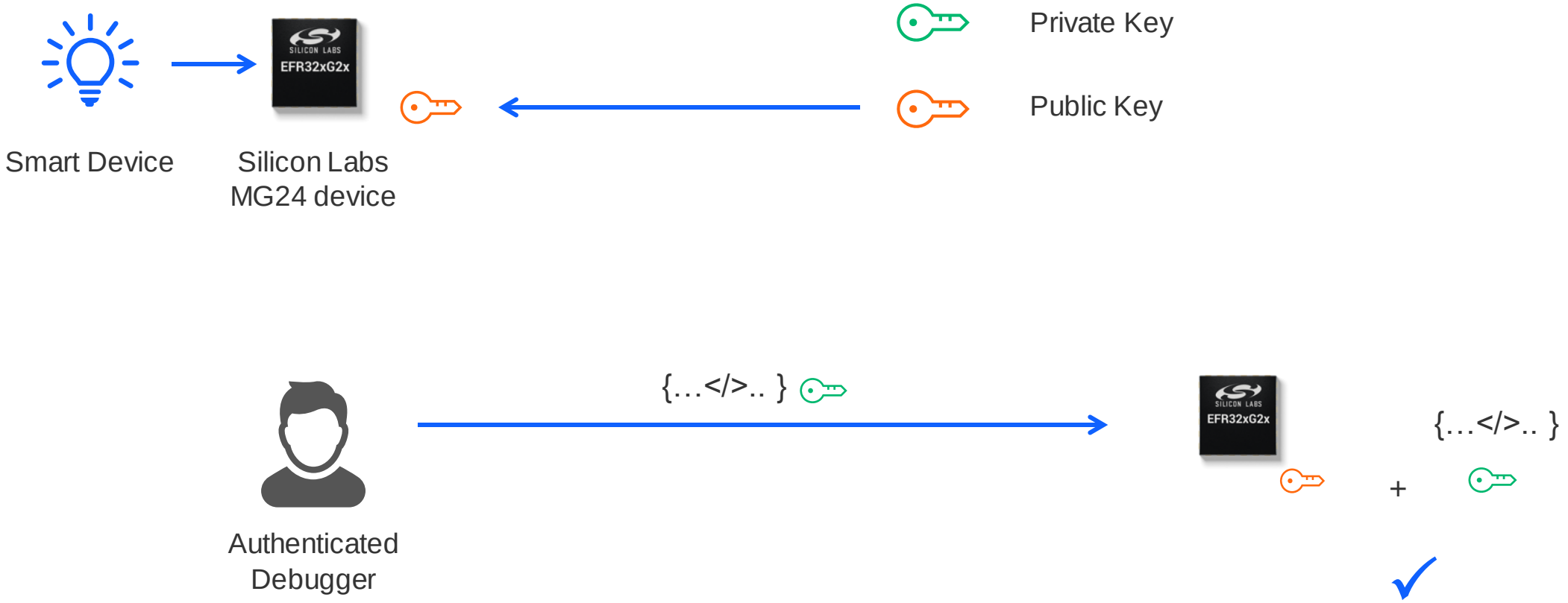


# Manufacturing Requirements: Device Fusing

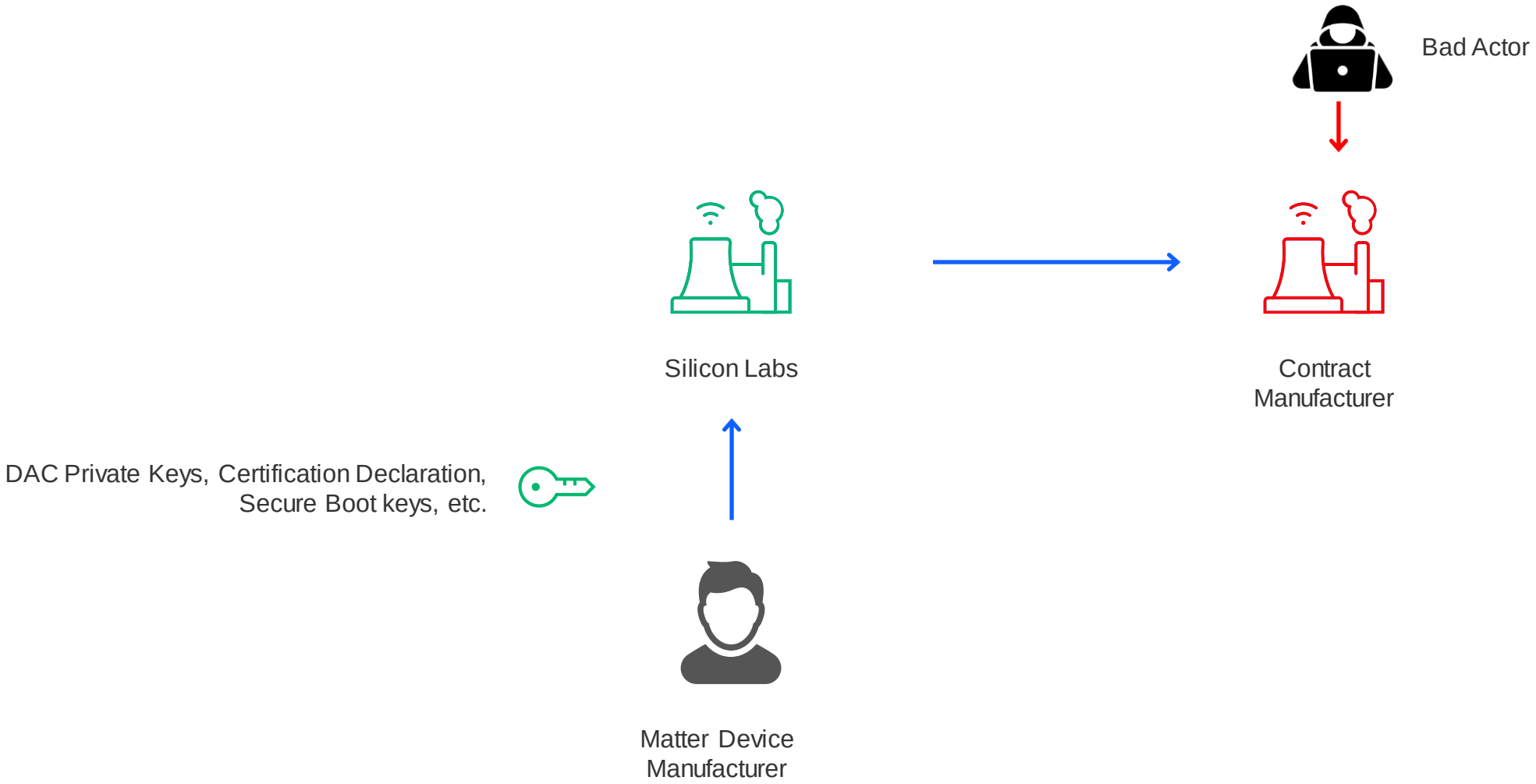
### 13.6.4. Manufacturing

a. Fusing of Devices in production SHOULD be done to limit unintended access to hardware components. For example, vendors may disable debug interfaces, and program trust anchors for secure boot. There are multiple options to secure fusing on the factory floor (e.g., physically securing the fusing station, pre-fusing the silicon, etc). [CM113 for T117]

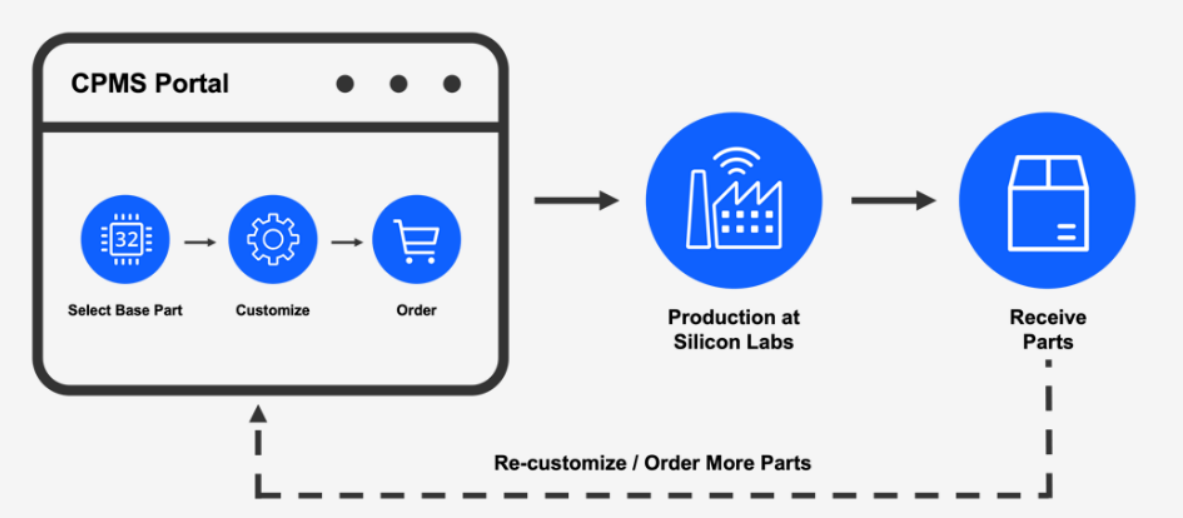
# Secure Debug



# Secure Programming with CPMS



# CPMS is Secure Provisioning… not just programming!




- **Available for Series 1 and Series 2 EFRx parts**
  - Matter DAC injection available for EFR32MG24A/B parts
- **Easy to use web user interface**
- **Flash Programming**
- **Matter DACs/Secure Identity (Certificates) Injection**
- **User Private/Public Key Injection**
- **Security Settings:**
  - Lock the debug port
  - Enable Secure Boot and Secure OTA
  - Set Anti-Tamper bits
  - Set Anti-rollback config
- **Bootloader pre-flashed for protection of Software IP**
- **Receive 10 samples within 4-6 weeks**

# CPMS Matter Alpha Program Live Now!

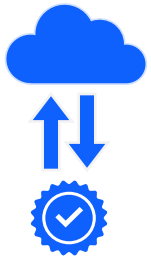
- Simplify the DAC injection process for your Matter devices with our Custom Part Manufacturing Service.
- Scan the QR code and join the CPMS Matter Alpha Program today!
- As part of the alpha program:
  - Matter samples are free of cost!
  - One hour of free consultation to walk you through the UI/security configurations, etc.

# Device Manufacturer POV

## 1
Secure Manufacturing

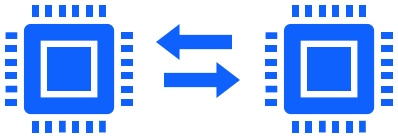
- CPMS for injection of Matter DACs, Certification Declaration
- Injection of keys for Secure Boot, OTA, Secure Debug, etc.

## 2
Secure Commissioning



- TRNG (True Random Number Generator)

## 3
Secure Communication



- Physically Unclonable Function (PUF)
- ARM TrustZone

## 4
Verified Software Updates

- Secure Boot
- Secure OTA updates

# Key Takeaways

| Sno. | Matter Security Piece | Matter Requirement | Recommended Silicon Labs Solution |
|---|---|---|---|
| 1 | Secure Commissioning | Unique DAC and Private Key | True Random Number Generator (TRNG) |
| 2 | Verified Software Updates | Image Encryption & Over – the – Air (OTA) Software Updates | Secure Boot and OTA Firmware Updates |
| 3 | Secure Communication | Protected Key Storage | PUF key as Root encryption key |
| 4 | | | Trusted Execution Environment |
| 5 | Secure Manufacturing | Device Fusing | Secure Debug |
| 6 | | | Secure Provisioning with CPMS |

SILICON LABS

works with
BY SILICON LABS

# Thank you!