Secure Vault全面提升Matter物聯網設備安全性

Steven Lin, Sr FAE, Silicon Labs

May 2024

Agenda

01 Matter Overview and Update

02 Matter Secure Commissioning

03 Matter Security Requirements

04 Matter Secure Manufacturing

05 Secure Vault and Summary

Matter Overview and Update

Smart Home Dilemma – Connected Lock Example

Zigbee Z-Wave Bluetooth Wi-Fi

- **Smart Home Dilemma**
  - Multiple Ecosystems available
  - Devices often tied to one Ecosystem
  - Requires different products, apps and hubs
- **Manufacturers**
  - Manufacturers are forced to pick ecosystem(s)
  - Need to ship multiple SKUs for connectivity standards
  - Need to learn different IoT technologies and ecosystems
- **Retailers**
  - Leads to duplicate products on the shelf
  - Difficult to provide expert advice to consumer questions
  - High return rates due to interoperability or incompatibility
- **Consumers**
  - Purchasing confusion
  - Hard to mix and match the products they want
  - Difficult to change Ecosystems

Matter’s Vision

Consumers

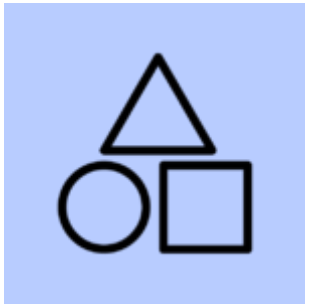
- More consistent set up experience
- Multi –Admin works across & with multiple ecosystems

Developers

- Develop once / deploy everywhere
- Community of support

Retailers

- Simplified purchasing experience
- Minimized returns



Simplicity

Easy to purchase and use

Interoperability

Devices from multiple brands work natively together

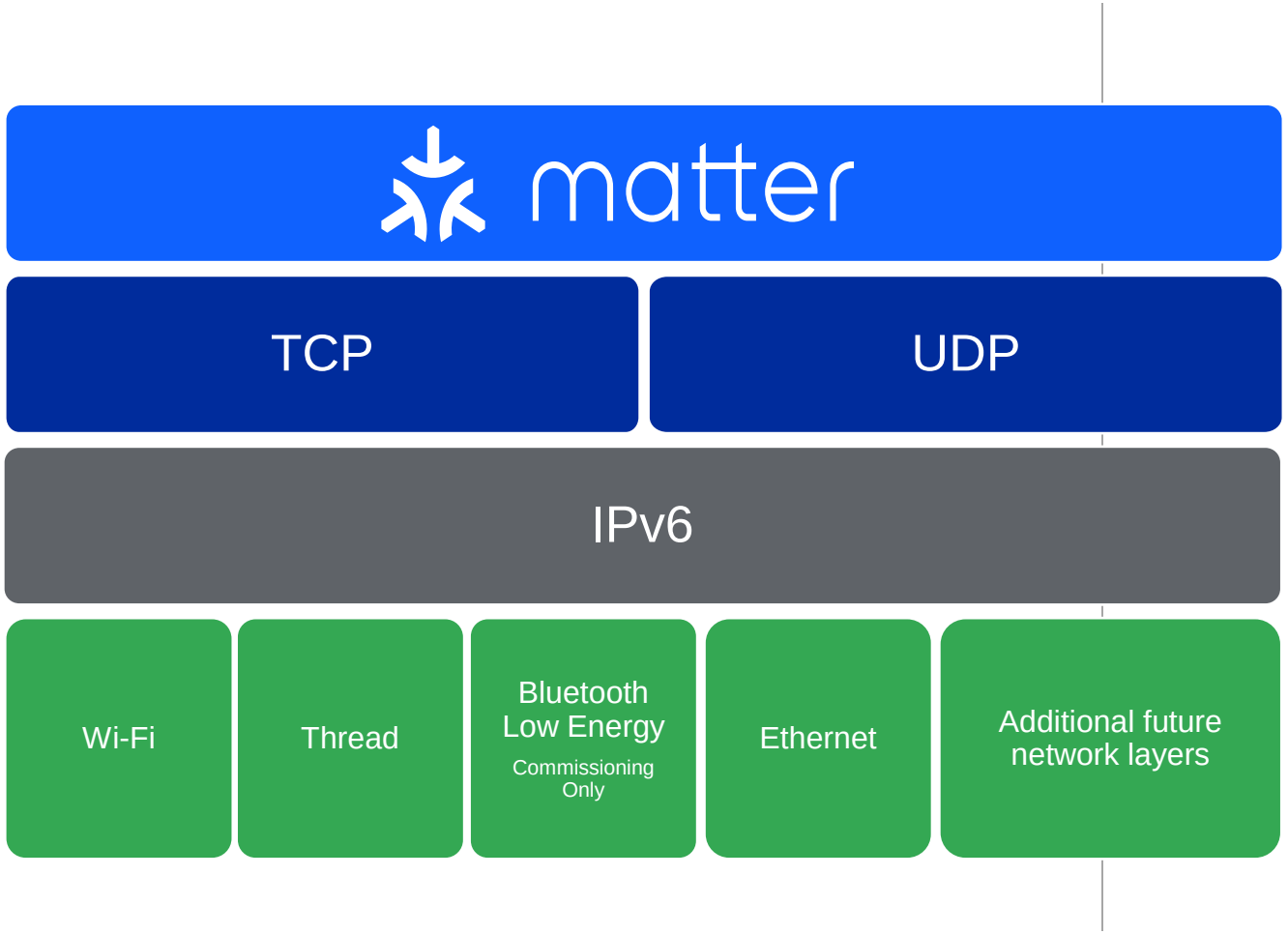
Reliability

Consistent and responsive local connectivity

Security

Robust and streamlined for developers and users

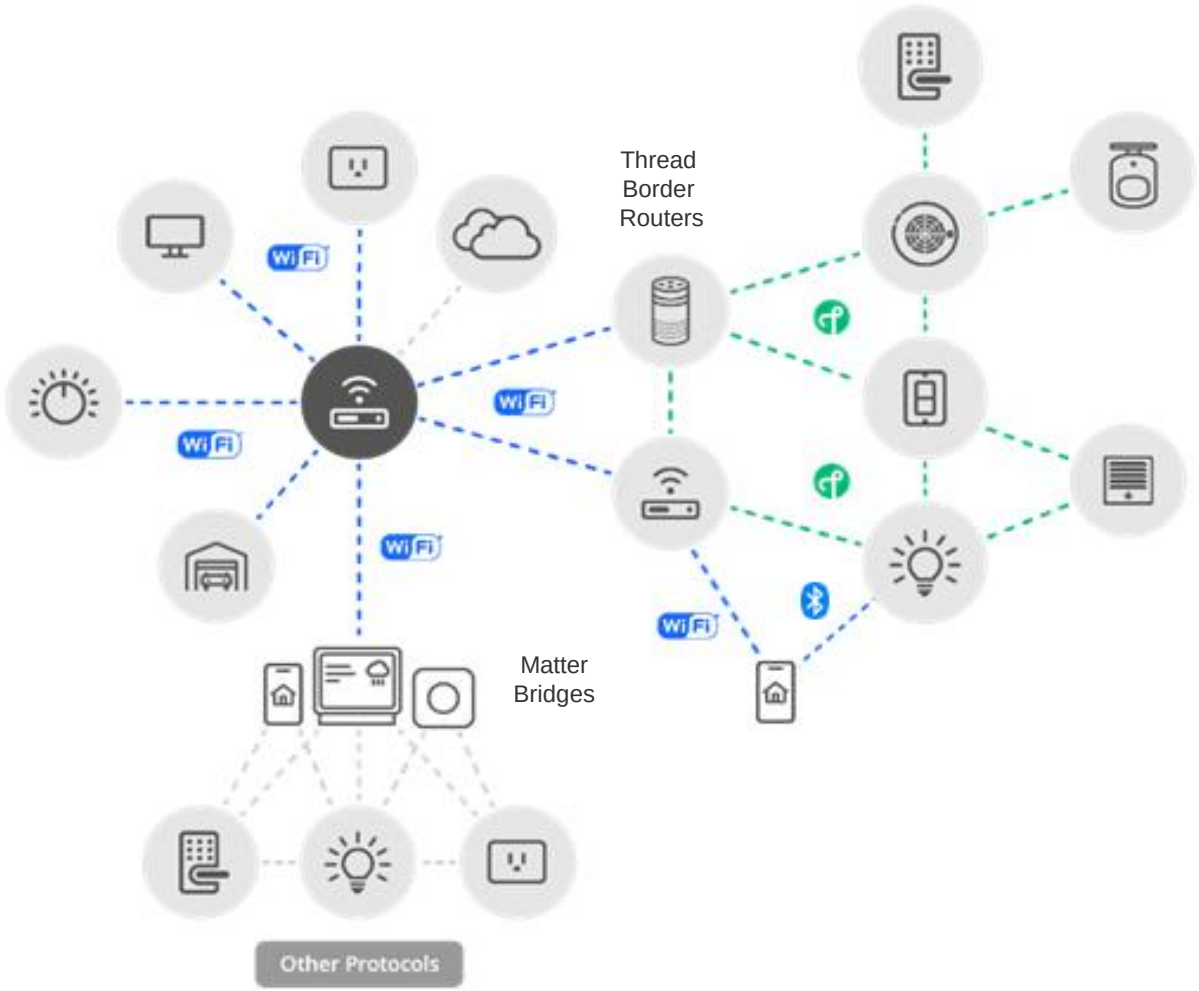
Matter High Level Components



- **Common application layer + data model**
  - Interoperability, simplified setup & control
- **IP-based**
  - Convergence layer across all compatible networks
- **Secure**
  - Requires certificates and device attestation
- **Open-source development approach**
  - Based on market-proven technologies
- **Common Protocol across device and mobile**
  - IP interface enables direct cloud connectivity as well
- **Low overhead**
  - MCU-class compute, <192KB RAM, <1MB Flash

Matter Network Topology

matter



- Native support for Wi-Fi and Thread
- Bluetooth LE is used as the commissioning channel
- Thread devices connect to other IP networks through border routers
- Bridges can link to other protocols like Zigbee and Z-Wave

Matter Device Types (November 2023)

Certifiable Today

Category	Device Types
Lights	On/Off, Dimmable Color
Actuators	On/Off Plug, Dimmable Plug, Pump
Heating/Cooling Unit	Air Conditioners, Mini-splits, Thermostats, Air Purifiers, Fan
Switches	On/Off, Dimmer, Color Dimmer
Sensors	Contact, Light, Occupancy, Temperature, Pressure Flow, Humidity, On/Off, Air Quality, Smoke & CO Alarm
Access Control	Door Locks, Window Shades
Controllers, Bridges	Gateways, Access Points, Smart Assistants, Border Routers, Mobile Phones
Video Players	TVs, Streaming Devices
Appliances	Laundry Washer, Refrigerator, Room AC, Temperature Controlled Cabinet, Dishwasher
Robotic	Robot Vacuum Cleaner

New to Matter 1.2

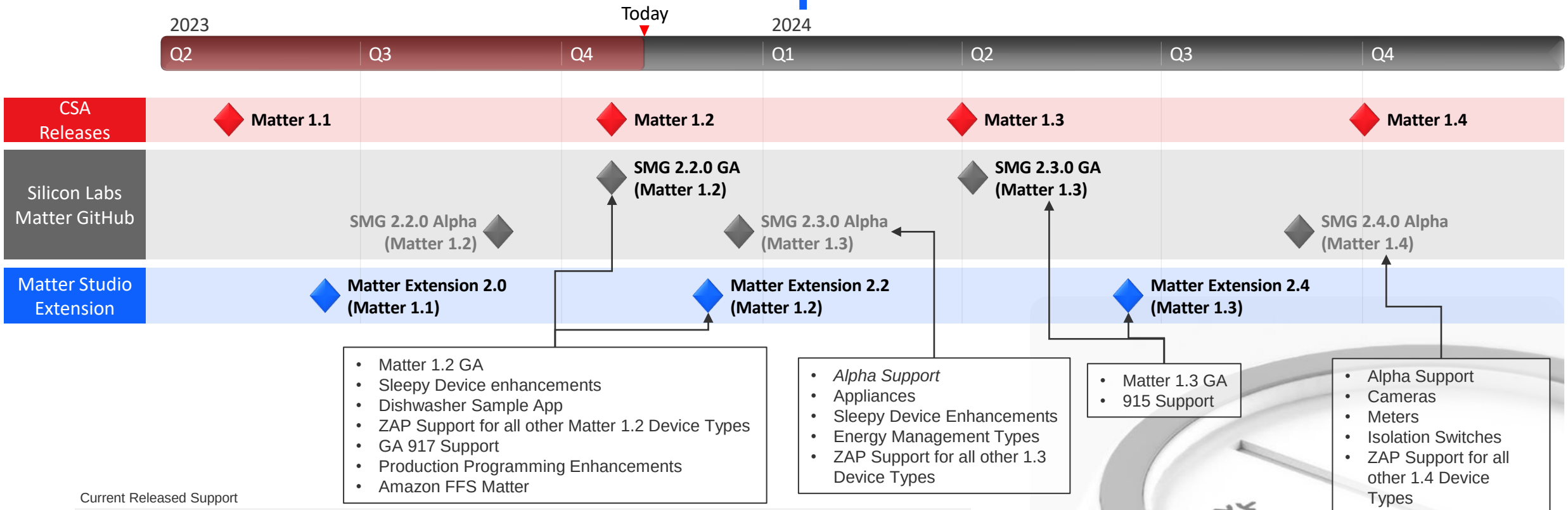
Future

Category	Device Types
Energy Management	EV, EVSE, Isolation switches, Meters
Network Infrastructure	Access Points
Additional Appliances	Dryer
Monitoring	Cameras
Presence Detection	Ambient Sensors

Industry Adoption

- **Matter 1.0 Launched on October 4, 2022**
  - Matter 1.1 Released May 2023
  - Matter 1.2 Released October 2023
  - *Matter 1.3 Targeted April 2024*
  - *Matter 1.4 Targeted October 2024*
- **As of October 16, 2023, there are 1386 certified devices across 23 device types**
- **One of the fastest standards adoptions by manufacturers ever**
- **Major ecosystems have all rolled out device support for both Thread and Wi-Fi**

Silicon Labs Matter Roadmap



Current Released Support

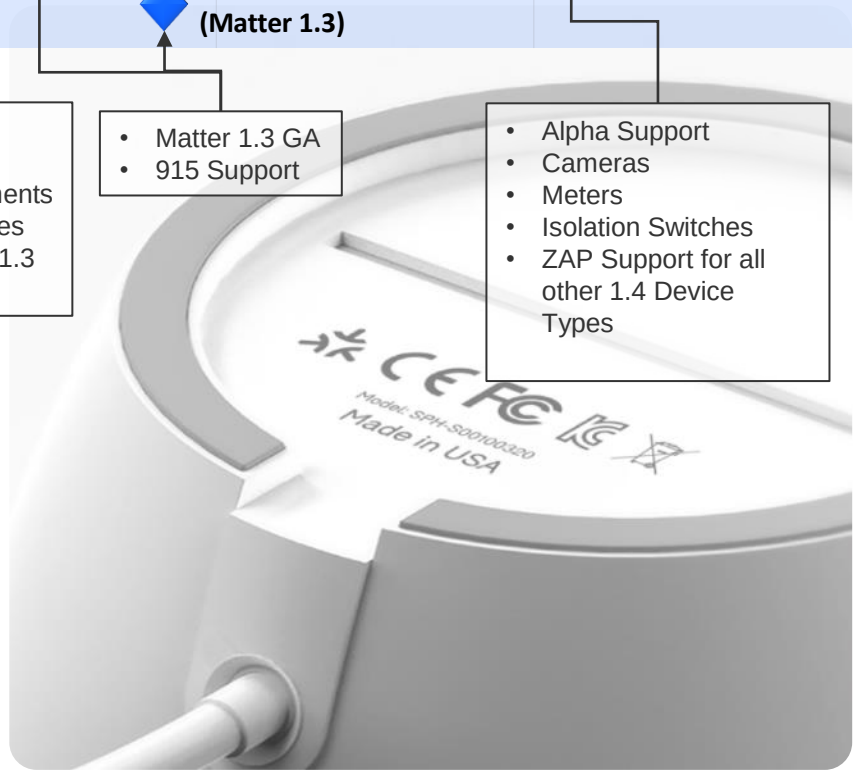
Sample Apps: Door Lock, Light Bulb, Window Shades, Switch, Thermostat, On/Off Plug, Sensor, Dishwasher

Matter over Thread Support

- 15.4 SoC: MG24
- 15.4 RCP (OTBR): MG21/24
- Delivered through GitHub and GSDK/SSv5
- Thread 1.3 certified libraries
- Multiprotocol (CMP/DMP) w/ BLE & Zigbee
- RaspberryPI Docker OTBR image

Matter over Wi-Fi Support

- Wi-Fi SoC: SiWx917 (Beta)
- Wi-Fi NCP: MG24 + WF200
- Wi-Fi NCP: MG24 + RS9116
- Wi-Fi NCP: MG24 + SiWx917 (Beta)

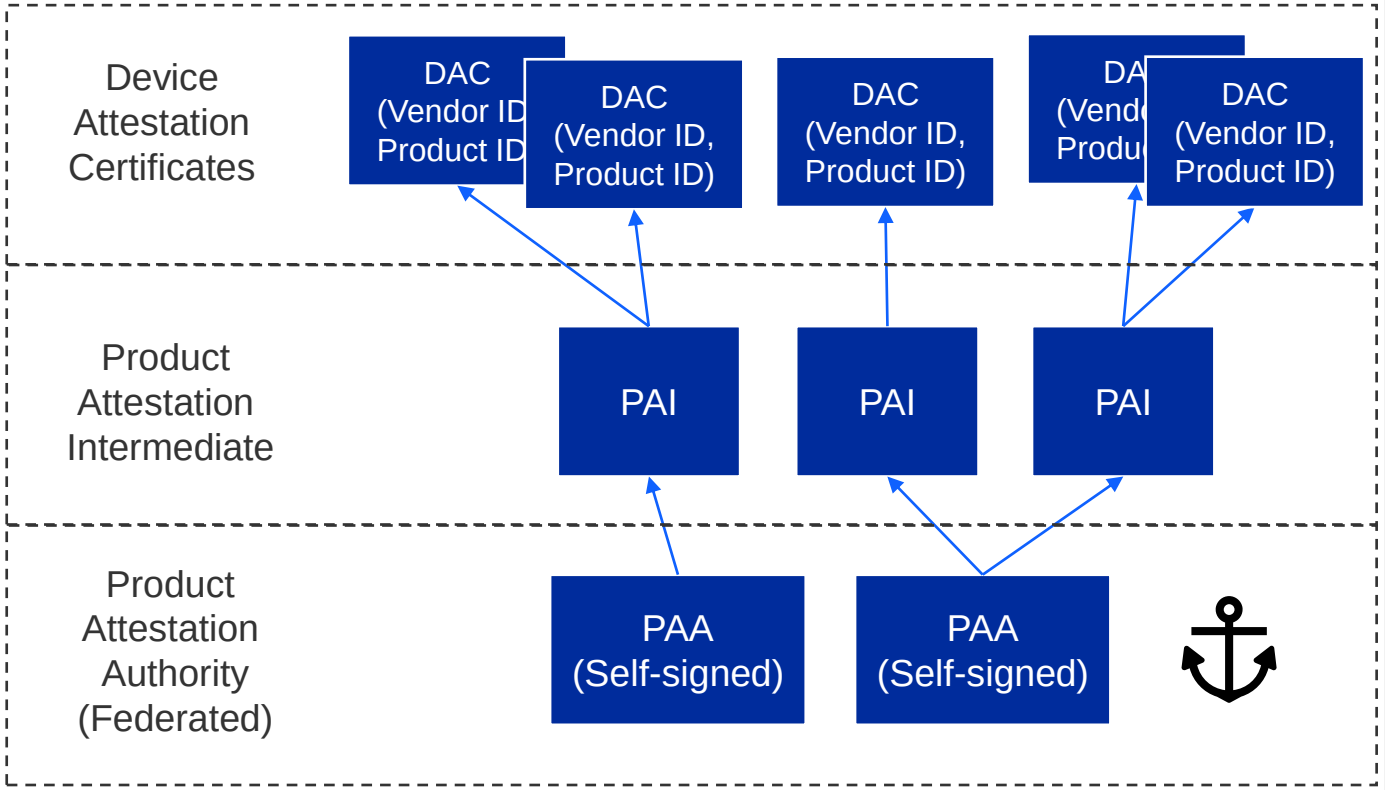


SILICON LABS

Matter Secure Commissioning

Device Attestation and Device Certificates

- Every device has a unique certificate that is signed by the manufacturer
- The hierarchy allows for a 3-level tier
- No single root CA across all devices
- During commissioning the device is challenged to prove possession of associated private key
- Certificates can be validated against the Distributed Compliance Ledger to verify device certification status



Commissioning - Establishing Initial Security

1 Initiate Matter Joining

Standard Commissioning

Just turn on device

User Intent Commissioning

Use UI to Activate Matter

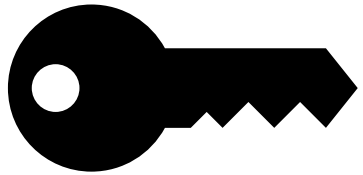
2 Scan Matter QR Code

Passcode
12345678

or enter Matter Passcode Manually

3 Discovery on existing network, or Bluetooth LE Beaconing and connection

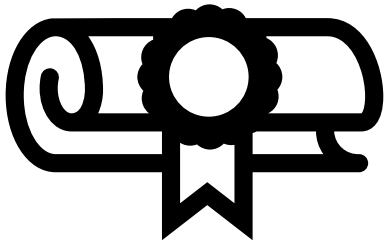
4 PASE Password Authenticated Session Establishment



Passcode verified
Encrypted Keys established

Commissioning - Installing Matter Fabric Security Credentials

5 Device Attestation

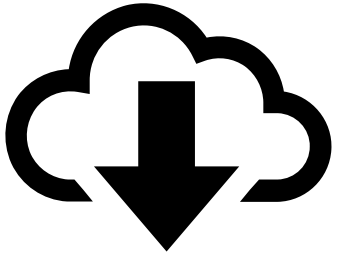


Check manufacturer certificate and device compliance

6 Install Operational Security

Install a commissioner root certificate, an operational certificate for device, and an ACL with list of administrators.

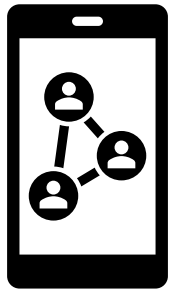
7 Configure Operational Network



Convey Wi-Fi or Thread network credentials using Network Commissioning Cluster

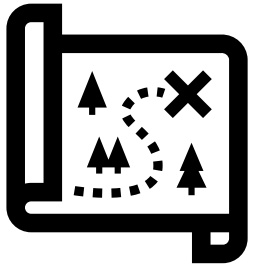
Commissioning - Final Steps

8 Join Network



Device attaches to Wi-Fi or Thread network

9 Discover Device on IP network



Controller discovers device using DNS and establishes a CASE session using newly configured security material.

10 Finalize

Inform Device Commissioning is complete
Performs any other application configuration

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)**

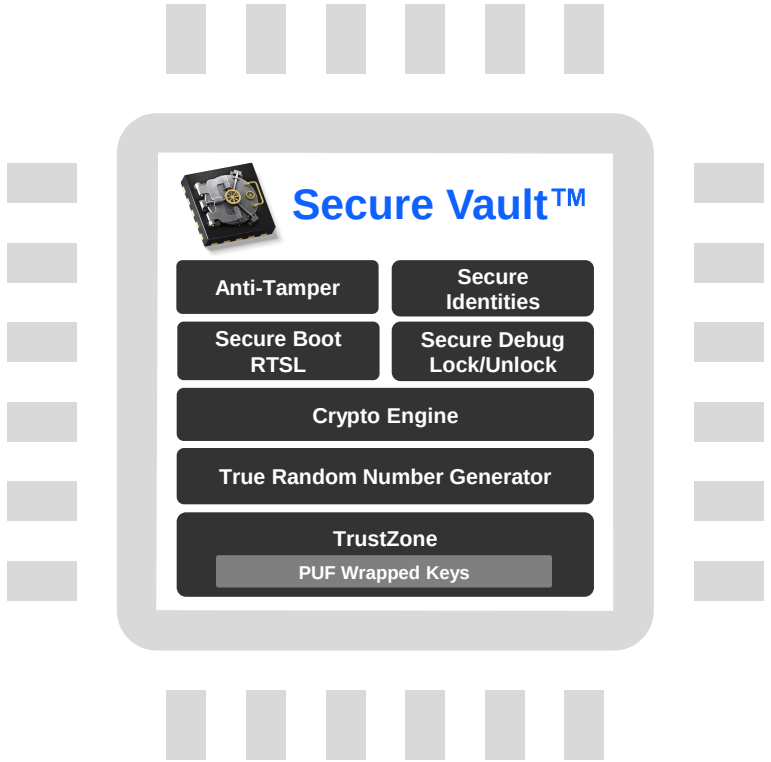
OTHER SECURITY SPECIFICATIONS

- 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

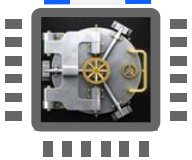
Programming…. Secure?

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

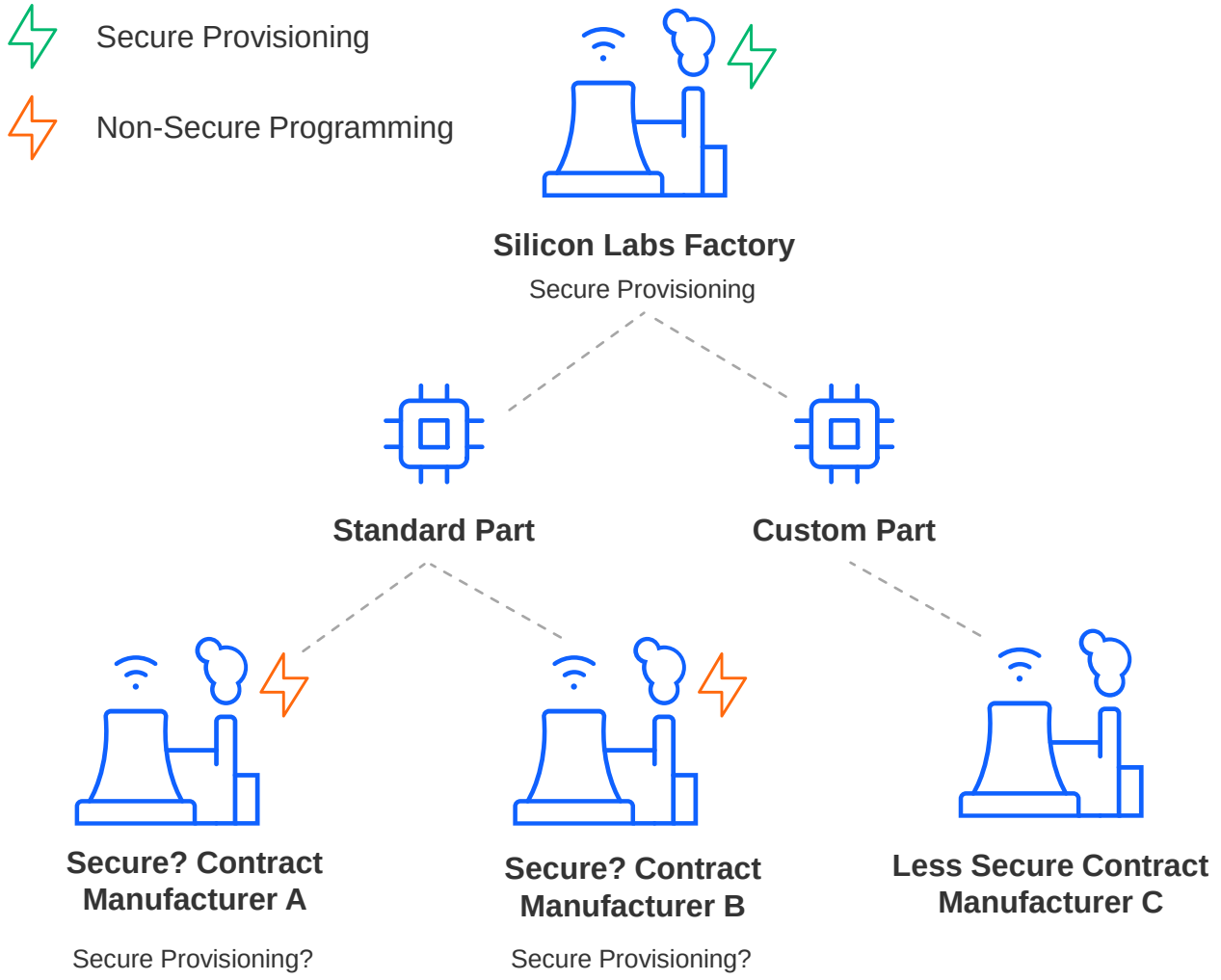
Security
- Lock Flash Pages
- Enable Secure Boot/Secure Debug (OTP)
- Set Default Tamper

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

Flashing
- Customer Application
- Bootloader



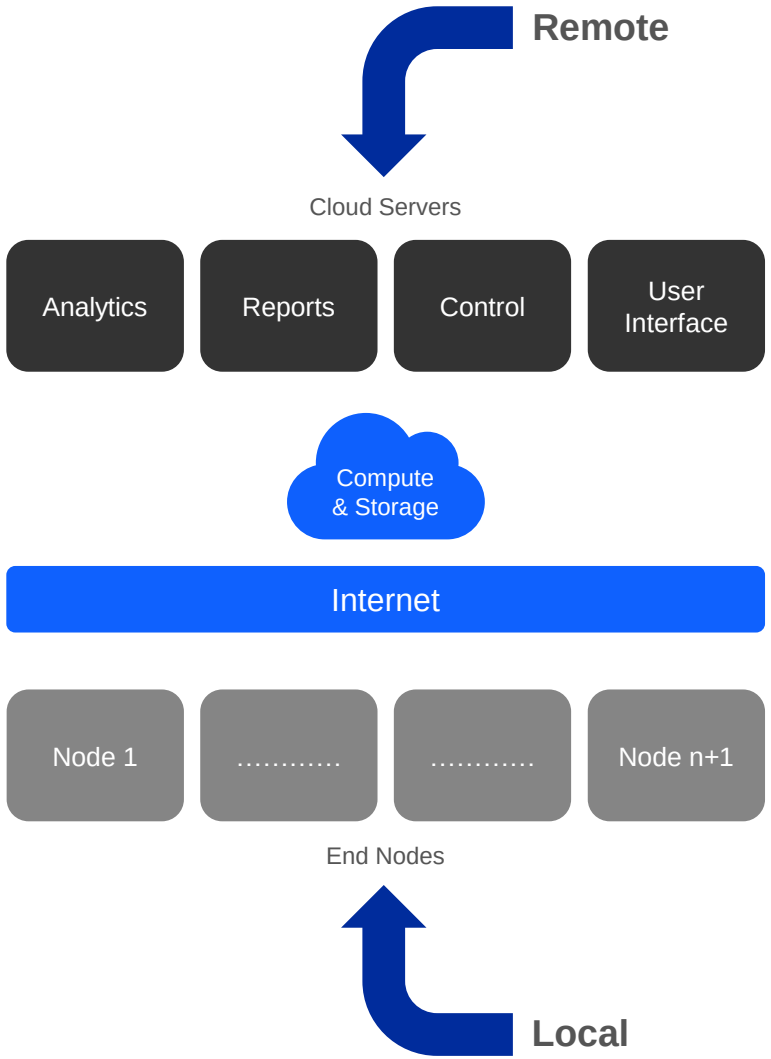
CPMS for Matter is Secure Provisioning – Alpha Program Launching June 1st !

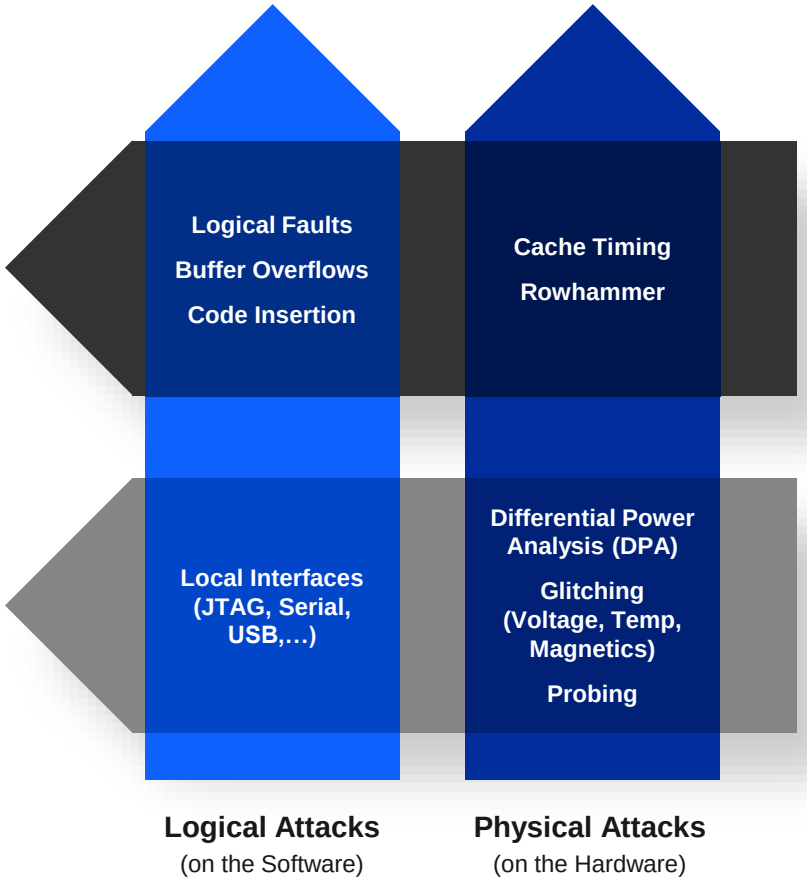


- **Available for EFRMG24A/B 15.4 Thread parts and coming soon for Si915/917 Wi-Fi parts**
- **Easy to use web user interface**
- **Receive 10 samples within 4-6 weeks for $500 flat fee (free for Alpha customers)**
- **Matter Security Credential Injection:**
  - DAC and PAI
  - Certification Declaration
  - 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**

Secure Vault and Summary

IoT Attack Vectors are Shifting from Remote to Local





Remote Attacks
(through the Internet)

Historically hackers attacked only from the cloud and focused on solely on data servers.

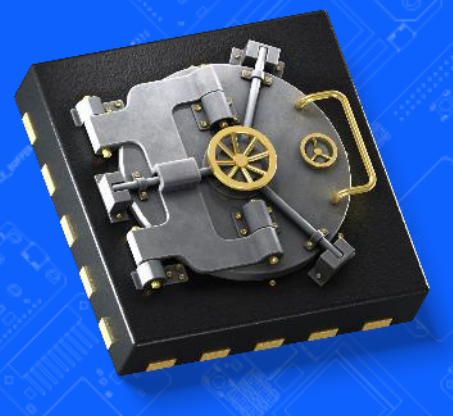
Local Attacks
(Hands-On Access)

'Pivot Attacks' are a growing attack vector against IoT.

End nodes are attacked locally and then used to attack higher level servers for their more valuable data.

Secure Vault™ Support in BG24 and MG24

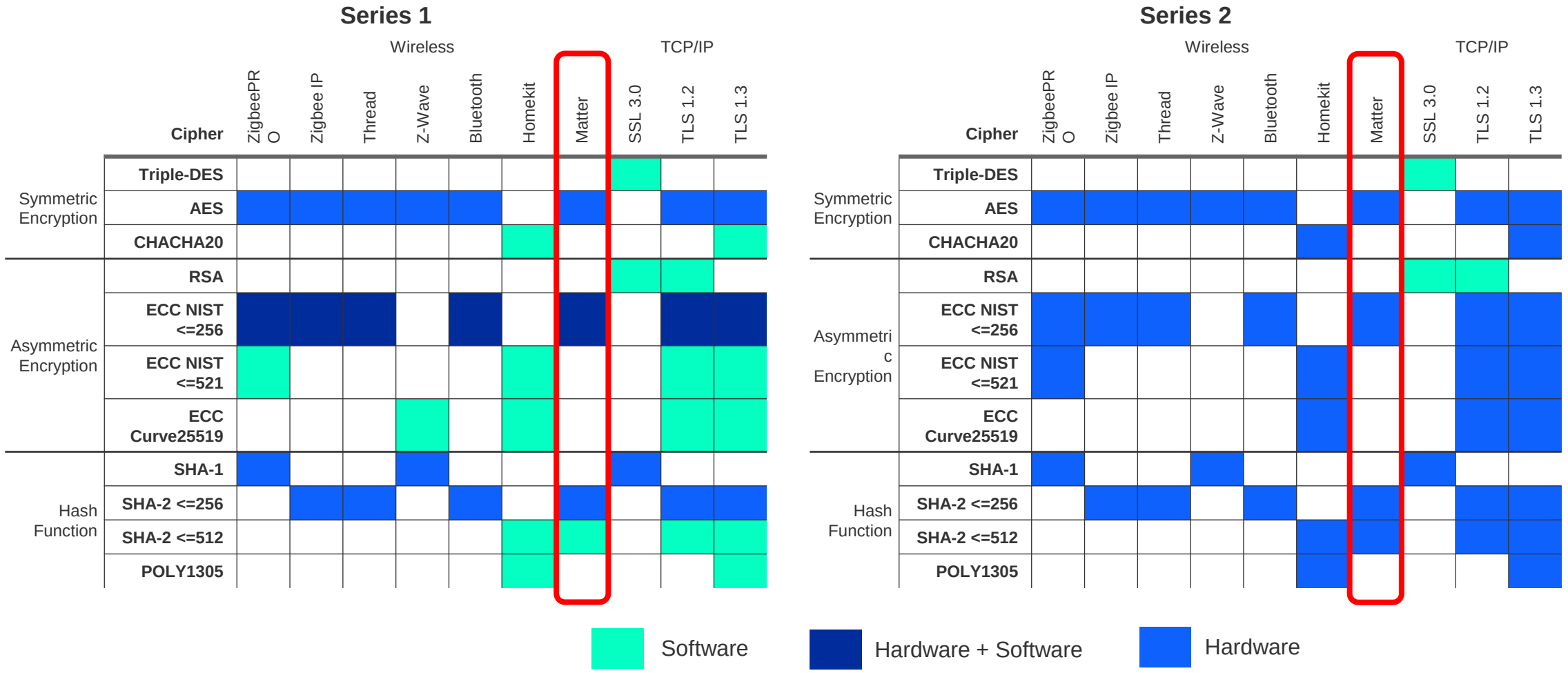
Base	Mid	High	Feature
✓	✓	✓	True Random Number Generator
✓	✓	✓	Crypto Engine
✓	✓	✓	Secure Application Boot
—	HSE	HSE	Secure Engine
—	✓	✓	Secure Boot with RTSL
—	✓	✓	Secure Debug with Lock/Unlock
—	✓	✓	DPA Countermeasures
—	—	✓	Anti-Tamper
—	—	✓	Secure Attestation
—	—	✓	Secure Key Management
—	—	✓	Advanced Crypto
	EFR32BG24 EFR32MG24		



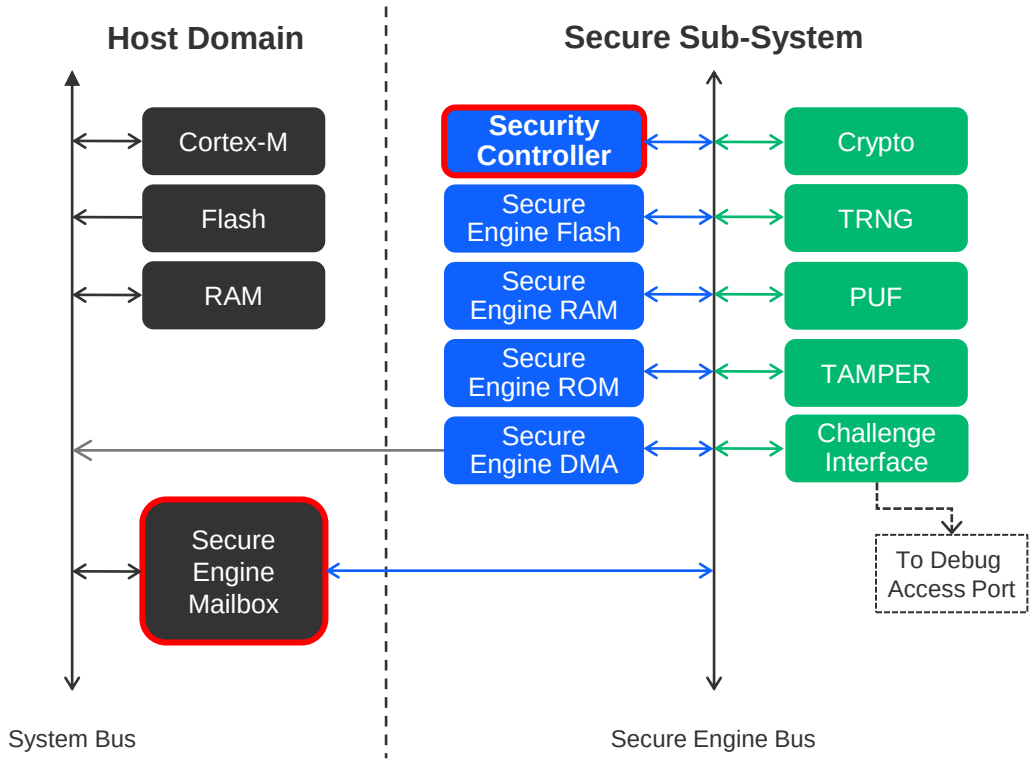
Industry Leading IoT Security

Cryptography Engine

Protocol Usage & Support



Secure Engine Subsystem



All cryptographic functions use a dedicated crypto-coprocessor

- Random number generation
- Symmetric encryption/decryption
- Hashing
- Keypair generation
- Key storage
- Signing / Verifying signatures

Limited accessibility to crypto-coprocessor

- Via a Host mailbox interface
- Debug pins (with Debug Challenge Interface, or DCI)

Crypto-coprocessor is not customer programmable

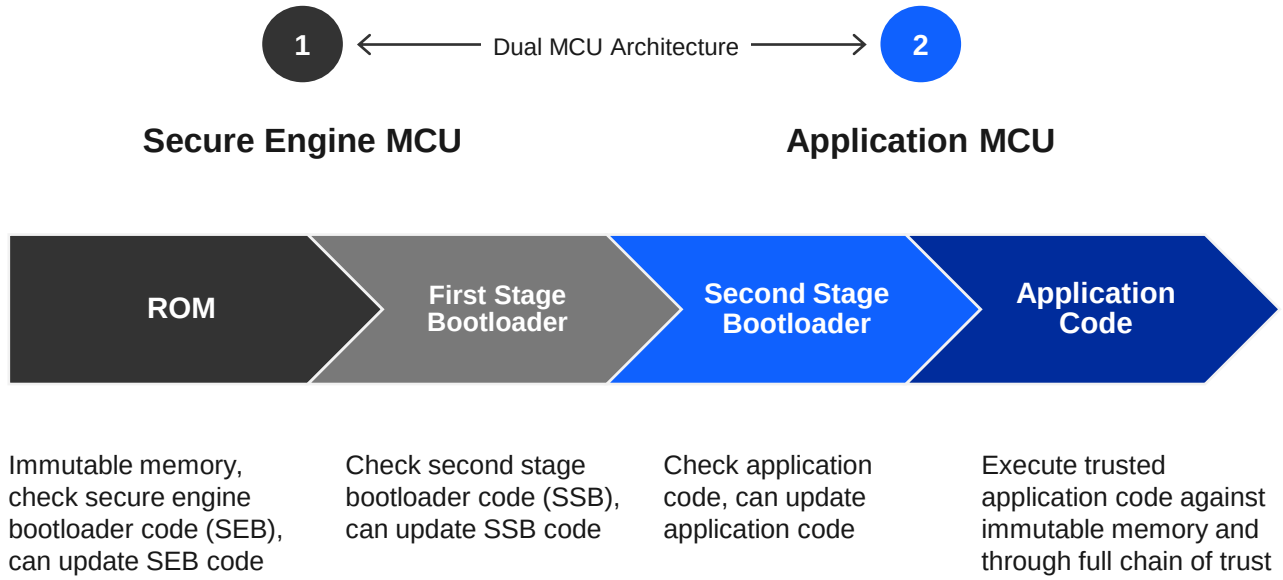
- (but can be securely updated)

Crypto-coprocessor benefits

- Increases security: access to crypto functions is tightly controlled, supports key isolation, supports Secure Boot
- Frees the Host Processor for other tasks

Secure Boot

LOCAL & REMOTE ATTACK VECTOR



- **Vulnerabilities**
  - Replacing code with ‘look-alike code’ makes a product appear normal. Hackers use it to copy/re-direct data to alternate servers.
- **Secure Boot with RTSL**
  (Root-of-Trust & Secure Loader)
  - Use and execute only trusted application code against immutable memory and through a full chain of trust

DPA Countermeasures

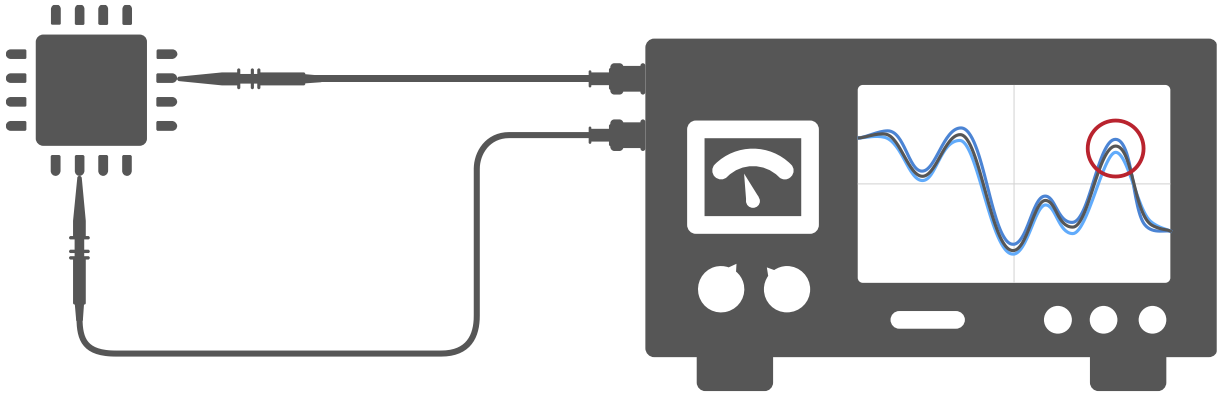
LOCAL ATTACK VECTOR

1

A Differential Power Analysis (DPA) attack requires hands-on access to the device.

2

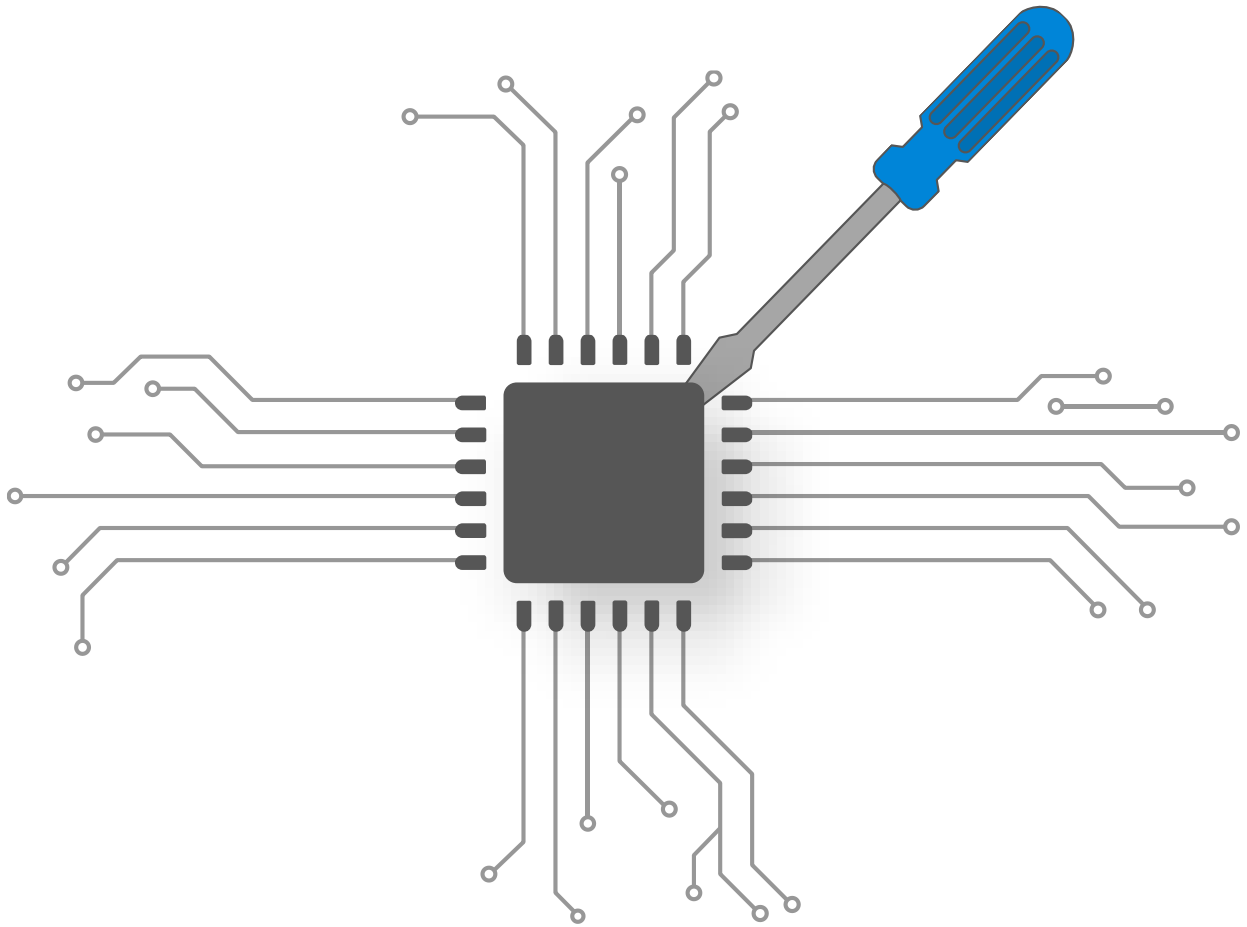
Monitoring electromagnetic radiation and fluctuations in power consumption during crypto operations may reveal security keys and other data.



- **Vulnerabilities**
  - Observing subtle signal differences during given internal operations can provide insight into cryptographic functions
- **DPA Countermeasures**
  - Countermeasures add masks and random timings to internal operations and distorts DPA snooping

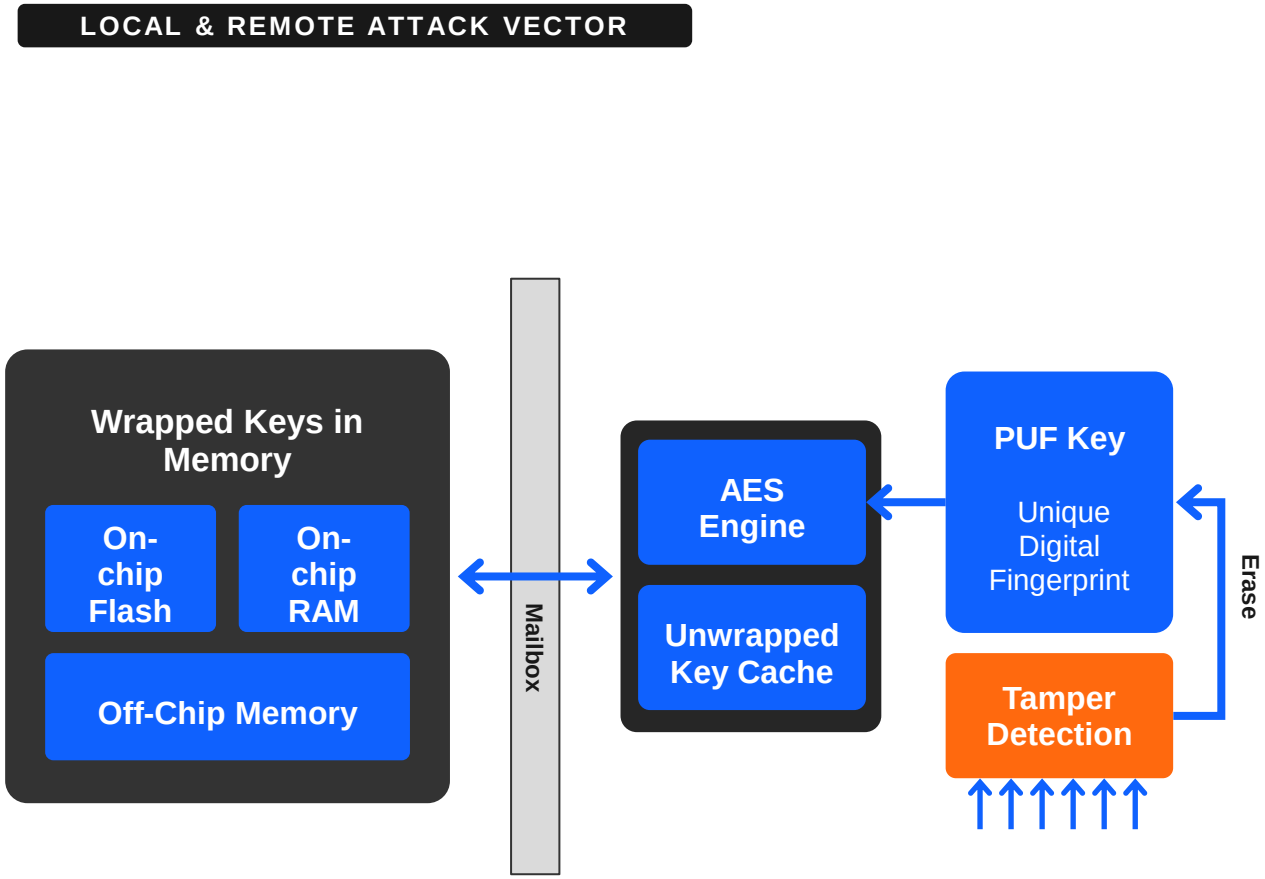
Anti-Tamper

LOCAL ATTACK VECTOR



- **Vulnerabilities**
  - Tamper attacks come from single or multiple vectors.
  - Common attacks include voltage glitching, magnetic interference and forced temperature adjustment
- **Tamper detection and rapid response**
  - Anti-tamper requires both an attack detection and suitable rapid response which may include key deletion.

Secure Key Management



- **Vulnerabilities**
  - When an attacker learns how to extract keys or content from a device, they use the same attack vector to attack other devices
- **Secure Key Management**
  - A Physically Unclonable Function creates a secret, random, & unique key, from individual device imperfections
  - The PUF-key encrypts all keys in the secure key storage. It is generated at startup and is not stored in flash

Secure Vault™ – Formally Recognized by Industry Leaders

- **ARM PSA Level 2 and 3**
  - First SoC to achieve Level 3 certification
  - Assures a proven hardware root of trust
- **SESIP Level 3**
  - First SoC to achieve a SESIP Level 3 certification
  - Common Criteria Lite
- **ISA/IEC 62443**
  - Maximum level of security for a silicon product
- **Independent Security Evaluation by Riscure**
  - Comprehensive analysis report from Riscure can be shared with customers under NDA

Summary

- 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

2024 tech talks

BY SILICON LABS

APAC Tech Talks: Wireless Technology Training

Register Now

SILICON LABS

Thank you!

Silicon Labs 官方網站	Silicon Labs 線上社群