SILICON LABS

Matter安全特性与Silicon Labs Secure Vault解决方案

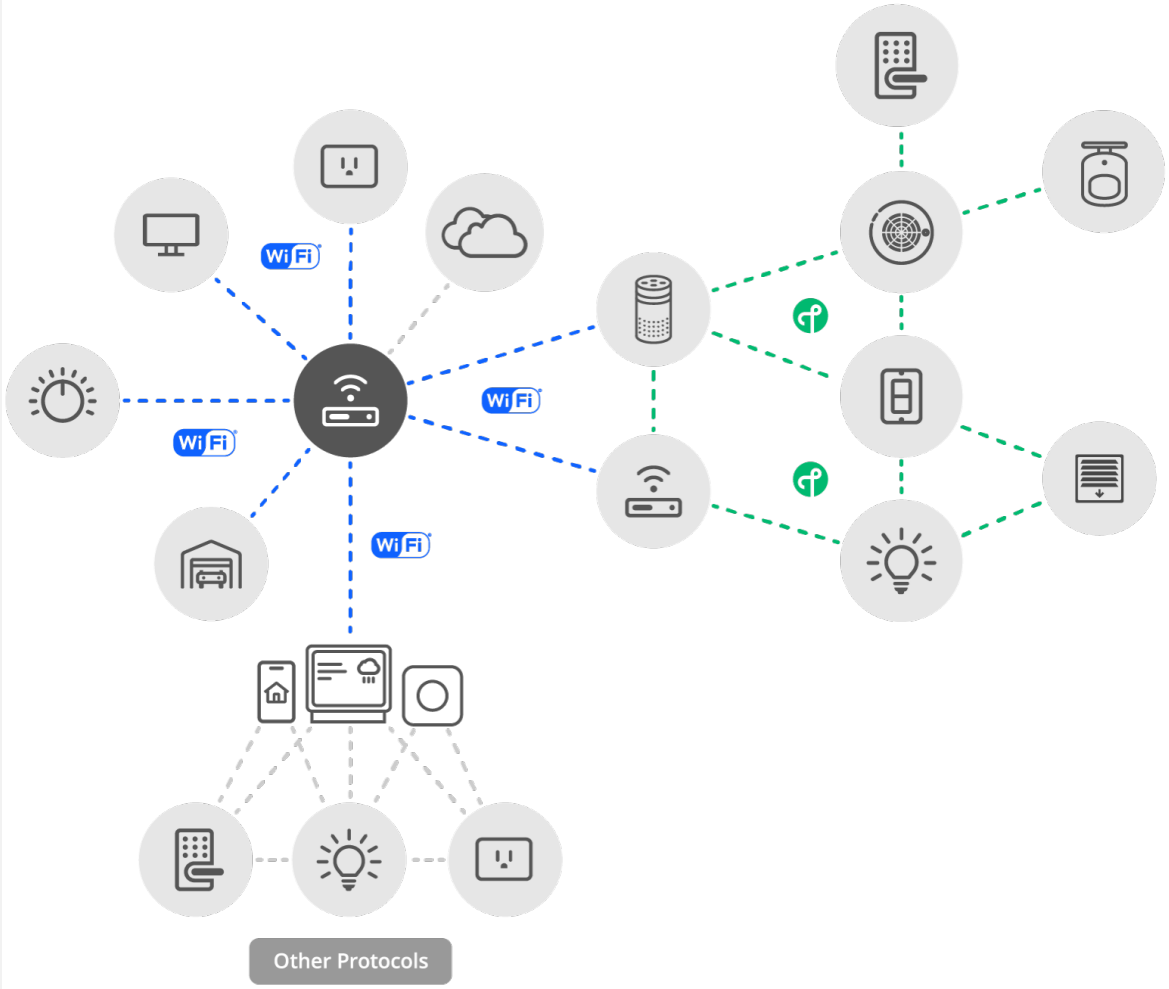
Jason Hou 侯思磊

2023年2月

大纲

- Matter安全特性概述
- Commissioning安全机制
- 访问控制 (Access Control)
- Silicon Labs Secure Vault 解决方案介绍
- Silicon Labs Secure Vault 让Matter更安全

Matter安全特性 - 概述



- 禁止匿名入网
  - 入网设备需要通过passcode证明入网的合法性
- 设备合法性认证
  - 每个设备都有唯一的标识(DAC)，由制造商进行身份验证，并且还可以通过认证声明文件(CD)验证该设备是否通过Matter认证
- 操作合法性认证
  - 通过(Operational Credentials)证明matte设备在网络(Farbic)中的合法性
- 设备安全认证完成后发送wifi或thread的网络密钥，避免泄漏给非法设备
- 通过访问控制列表(ACL)进行操作授权
- Matter是开放的标准，代码全部开源
  - 任何第三方机构可对标准和源码进行安全审查

Matter安全特性 – 加密算法

- SHA-256 is the hash algorithm
- HMAC-SHA-256 for message authentication
- NIST P-256 as public key ECC curve
- AES-CCM using 128-bit keys for message encryption

Commissioning – 基本概念

Commissioning – 基本概念

- **Commissioning: Matter设备加入Matter Fabric的过程**
  - Commissioner: 网络(Fabric)管理员
  - Commissionee: 入网设备

- **Commissioning flows**

Commissioning Flow Name	Description
标准Commissioning流程	未入网的设备上电自动广播advertising
用户介入的Commissioning流程	未入网的设备上电不会自动广播advertising，需要用户触发
用户自定义 Commissioning流程	用户自定义

Commissioning - Commissioning Flow (Part 1)

1 Initiate Matter Joining

Standard Commissioning

Just turn on device

User Directed Commissioning

Use UI to Activate Matter

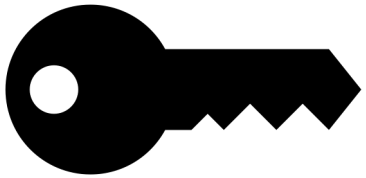
2 Scan Matter QR Code

Passcode
12345678

or enter Matter Passcode Manually

3 BLE Beaconing and connection

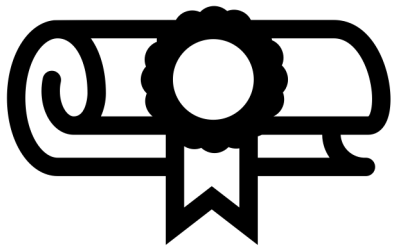
4 PASE Password Authenticated Session Establishment



Passcode verified
Encrypted Keys established

Commissioning - Commissioning Flow (Part 2)

5 Device Attestation

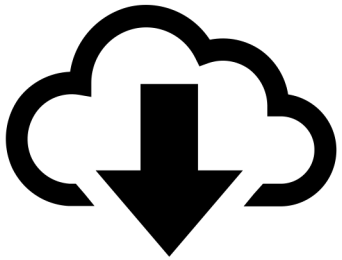


Check manufacturer certificate and device compliance

6 Add Node Operational Certificate (NOC)

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

7 Configure Operational Network

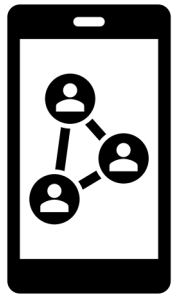


Convey WiFi or Thread network credentials using Network Commissioning Cluster

SILICON LABS

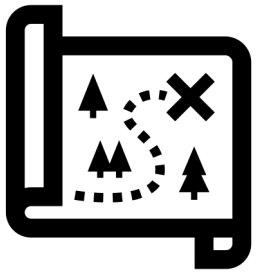
Commissioning - Commissioning Flow (Part 3)

8 Join Network



Device attaches to WiFi 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

Commissioning – Device Discovery

Commissioning – Onboarding Payload

- Commissioning入网信息(Onboarding Payload)

Onboarding Payload Element	Description
Version	Onboarding Payload的版本号
Vendor ID	CSA联盟分配的厂商ID
Product ID	厂商为产品分配的ID
Commissioning Flow	- Standard commissioning flow: 未入网的设备上电自动广播advertising - User-intent commissioning flow: 未入网的设备上电不会自动广播advertising，需要用户触发 - Custom commissioning flow: 用户自定义Commissioning流程
Discovery Capabilities Bitmask	入网设备支持的发现方式: - Soft-AP - BLE - On IP Network
Discriminator	设备鉴别码，Commissioner通过Discriminator找到想要添加的设备
Passcode	入网密码
TLV Data	(可选的) TLV (Tag-length-value) data. 支持用户自定义

Commissioning – 基于BLE的设备发现

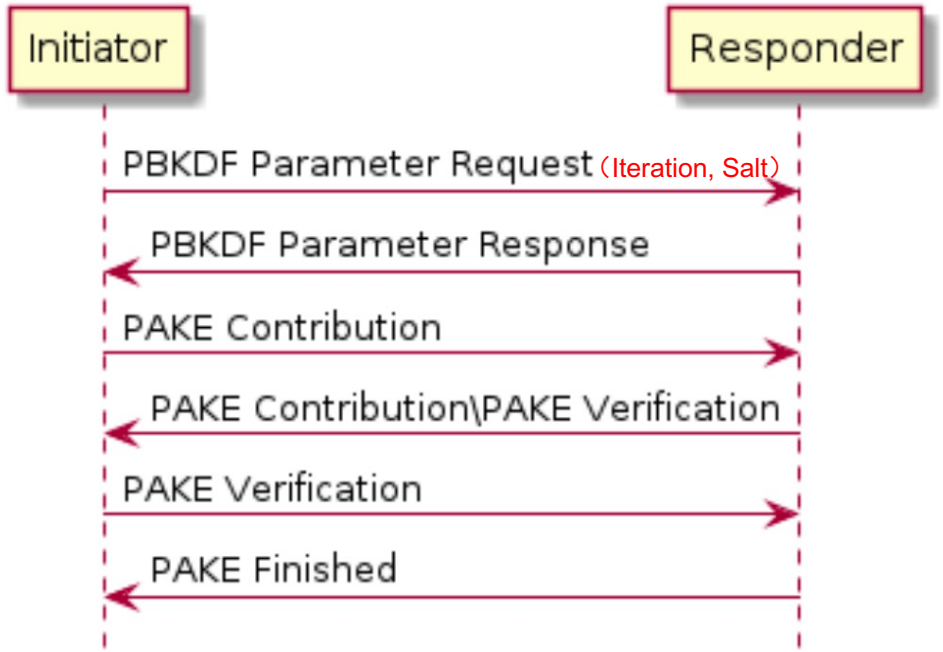
- BLE advertising data

Filed	Description	Required?
Vendor ID	CSA联盟分配的厂商ID	Optional
Product ID	厂商为产品分配的ID	Optional
Discriminator	设备鉴别码，Commissioner通过Discriminator找到想要添加的设备	Mandatory
TLV Data	(可选的) TLV (Tag-length-value) data. 支持用户自定义	Optional

- 处于 Commissioning模式的matte设备周期性的广播 Advertisement
- BLE advertising data
- Advertisement广播周期
  - 前30秒，Advertisement广播周期在20ms～60ms之间
  - 30秒后，Advertisement广播周期在150ms～1200ms之间
  - 15分钟后停止Advertisement广播
- Commissioner接收到 Advertisement后会和扫描二维码获取到的入网信息进行比对，如果VID，PID，Discriminator一致，表明已成功发现想要添加的设备。
- Commissioner与入网设备建立蓝牙连接

Commissioning – PASE

Commissioning – PASE



- SPAKE2+ Parameters Generated by Tool

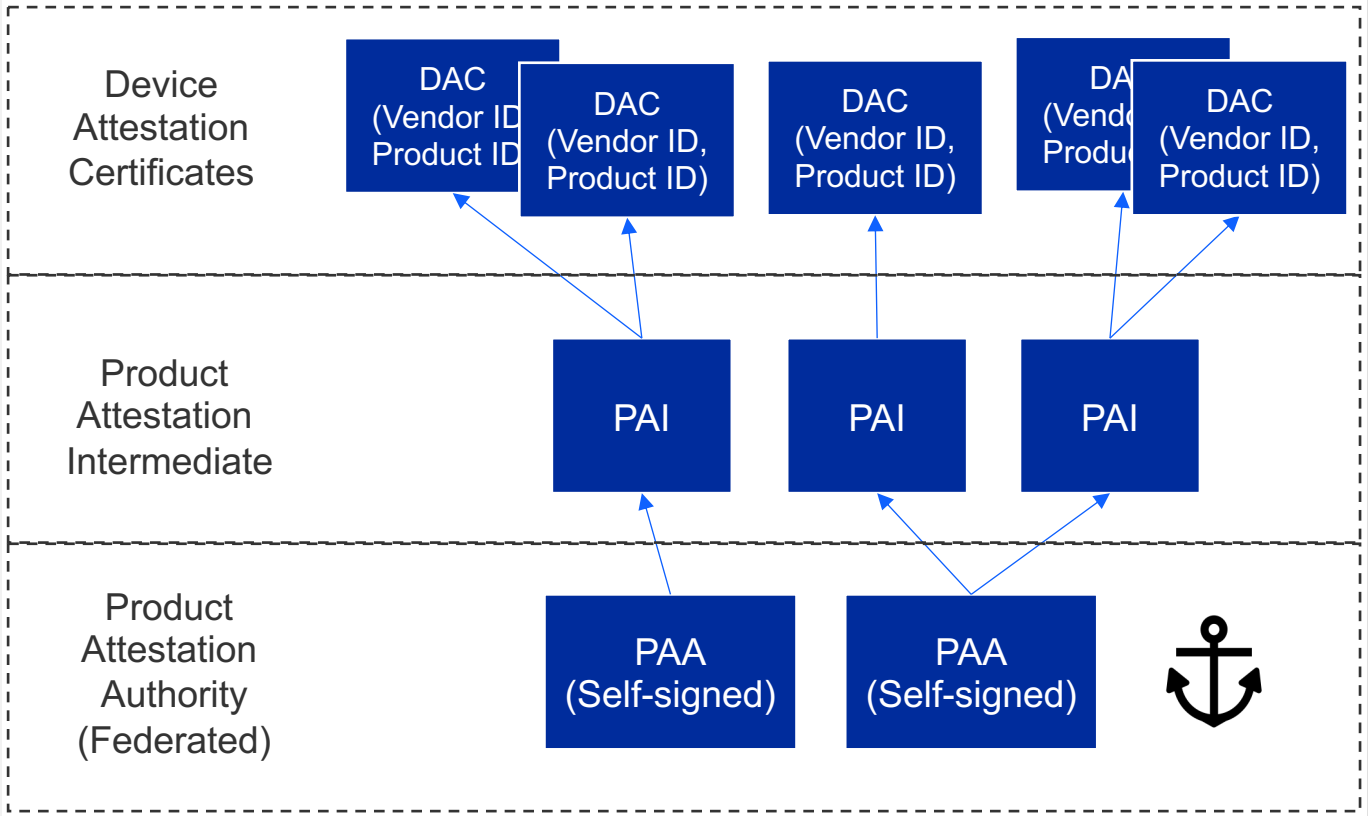
Passcode	Iteration	Salt	Verifier
62034001	15000	95834coRGvFhCB69IdmJyr5qYIzFgSirw6Ja7g5ySYA=	+0V21ZrsDkC0LSGvgqU9ZshIp0cvLLvuYIJxCmwGIZQEU0u4w/Uur9hV2EZcQtSJgA0OS2yznKYAxFruDjMm5v3jOcvXII0TE/mILeCiUGWpk4WqvJihFequs83FtAbq4Q==

- PASE: Passcode-Authenticated Session Establishment
- PASE 基于SPAKE2+协议，
  - Password Authenticated Key Exchange (PAKE) protocol
- SPAKE2+ Parameters
  - Passcode，Iteration，Salt，Verifier
- PASE完成后会协商出如下密钥：
  - I2RKey
    - 加/解密Initiator到Rsaponder的数据
  - R2IKey
    - 加/解密Rsaponder到Initiator的数据
  - AttestationChallenge
    - 设备认证时用到此参数
- PASE的目的是利用带外传输(out-of-band)的Passcode为Commissioner 和Commissionee 建立第一个安全的会话

SILICON LABS

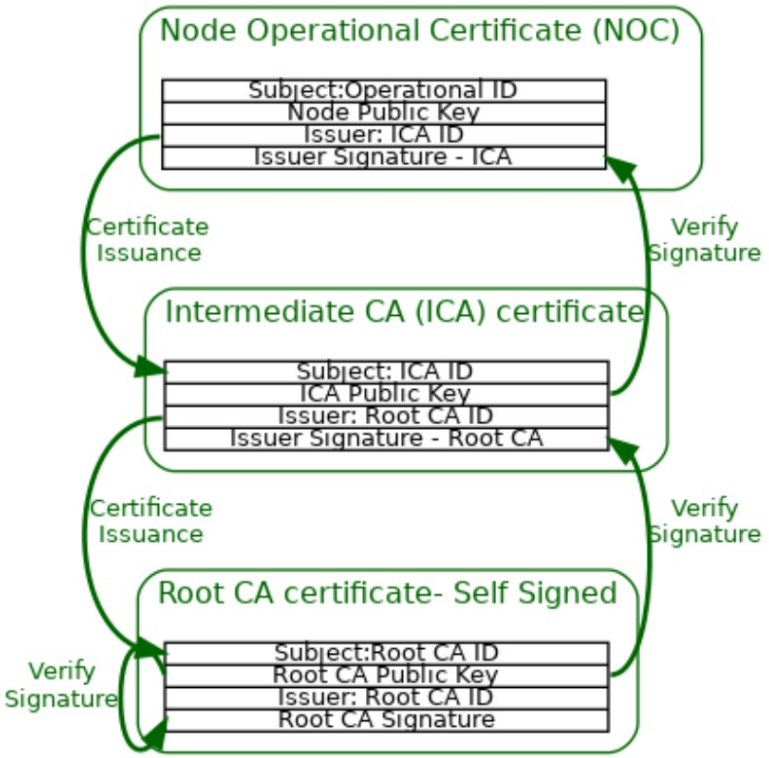
Commissioning – 设备证书（DAC）认证以及操作证书（NOC）安装

Commissioning – 设备证书（DAC）



- 所有的Matter设备都拥有唯一的设备证书（DAC）以及与DAC证书相对应的私钥
  - DAC证明该设备为合法设备
  - 私钥证明该设备是DAC的真正拥有者
- 证书链PAA-> PAI -> DAC
  - PAA由CAS联盟认证的根证书颁发机构颁发
  - PAI由PAA签发
  - DAC由PAI签发
- DAC和PAI证书需要烧录到Matter设备上，在Commissioning 过程中Commissioner会对设备证书进行验证
  - 证书链是否有效
  - VID/PID是否与Matter设备匹配

Commissioning – 节点操作证书(NOC)

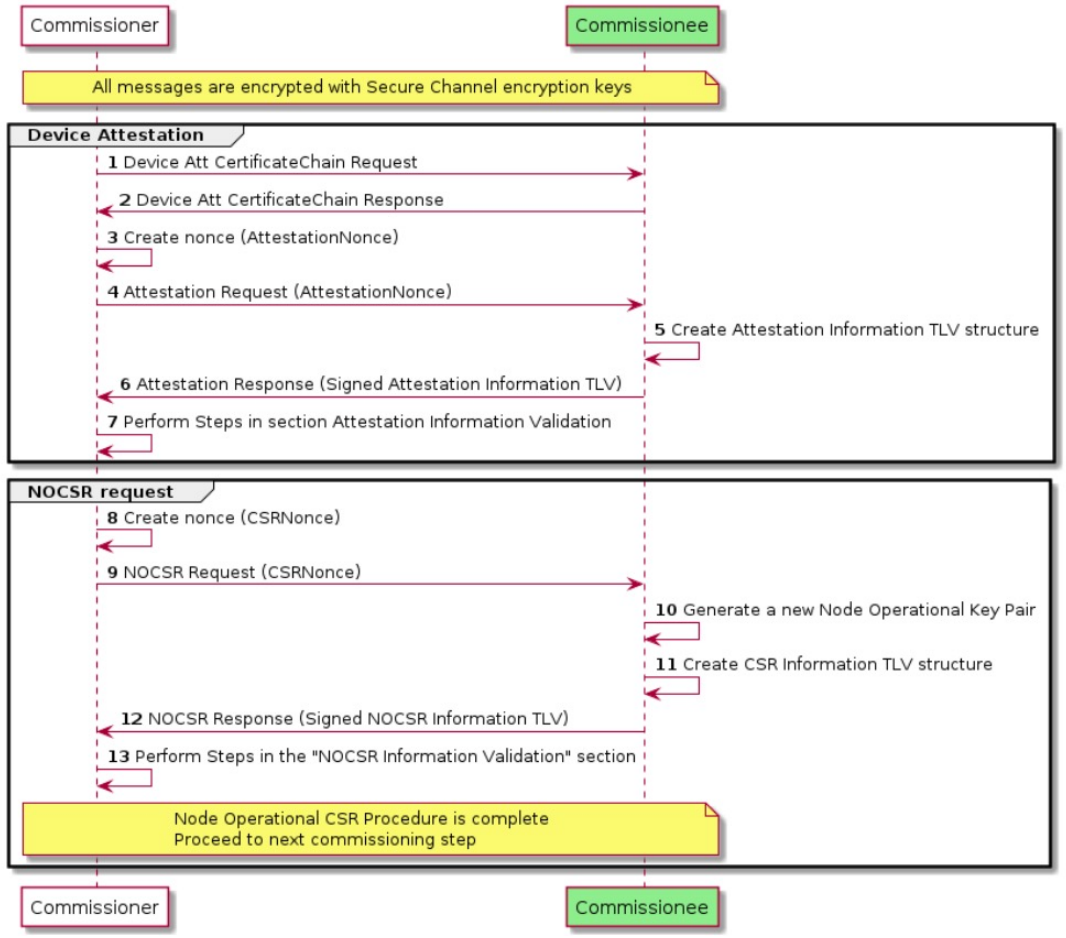


- Matter设备加入到Fabric后，Commissioner会为其颁发 Node Operational Certificate (NOC)
  - NOC证明该设备在此Fabric中的合法性
  - 设备中保存与NOC相对应的私钥
- 证书链RCAC-> ICAC -> NOC
  - RCAC由Commissioner自签名产生
  - ICAC由RCAC签发
  - NOC由ICAC签发
- NOC不需要烧录到Matter设备， Matter设备加入到Fabric后，Commissioner通过Matter协议将NOC安装到设备
- Matter设备退出Fabric后，NOC会被清除

Commissioning – 认证声明（CD）

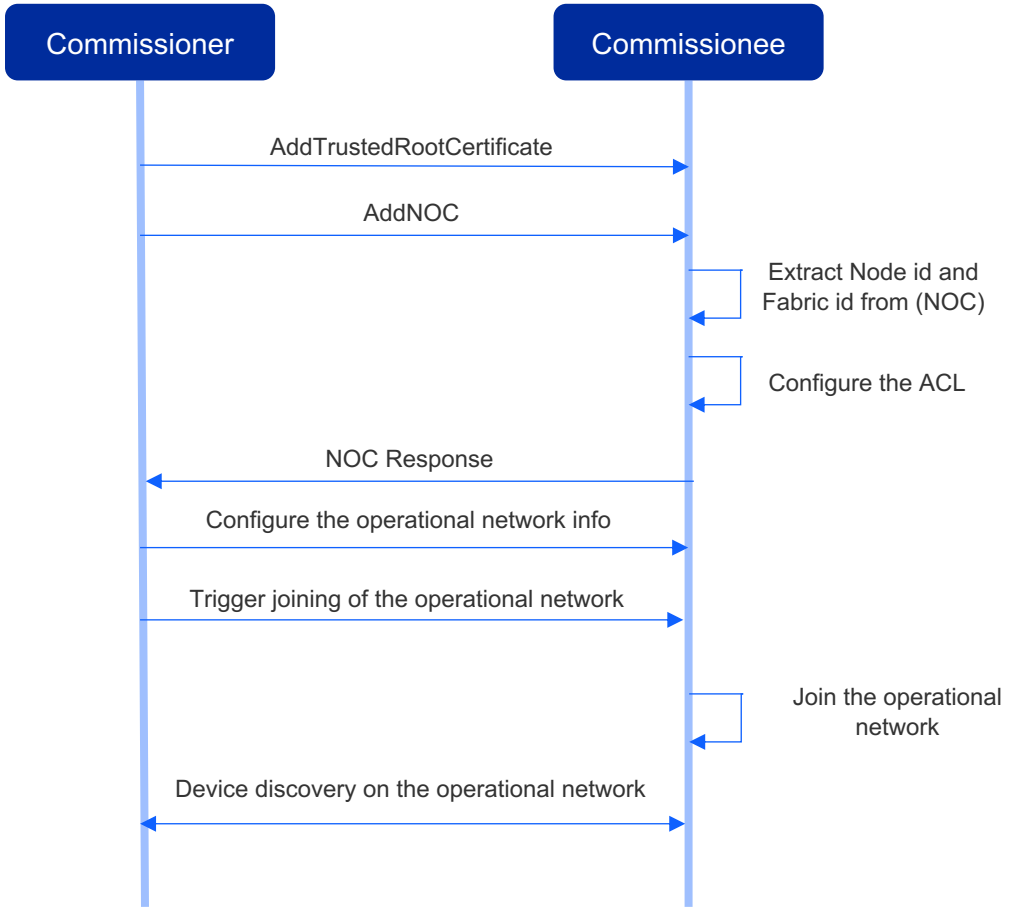
- Certification Declaration (CD)是由CSA联盟签发的产品认证声明，拥有CD的设备表明它已通过了Matter认证
- 设备通过Matter认证后，CSA联盟会为其产生一个CD文件，主要包含以下内容：
  - format_version
  - vendor_id
  - product_id_array
  - certificate_id
  - certification_type
- CD文件需要烧录到Matter设备上，在Commissioning过程中Commissioner会验证CD文件的有效性
  - 是否由CSA联盟签发
  - CD中的VID/PID是否与Matter设备匹配

Commissioning – 设备证书验证与NOCSR



- Attestation Information
  - Attestation Elements
    - Certificate Declaration
    - Timestamp
    - Attestation Nonce
    - Firmware Information (optional)
    - Vendor Specific information (optional)
  - Attestation Challenge(generated by PASE)
  - Attestation Signature(singed by Device Attestation Private Key)
- CSR(Certificate Signing Request) Information
  - NOCSR Elements
    - CSR
    - CSRNonce
    - Vendor_Reserved (optional)
  - Attestation Challenge(generated by PASE)
  - Attestation Signature(singed by Device Attestation Private Key)

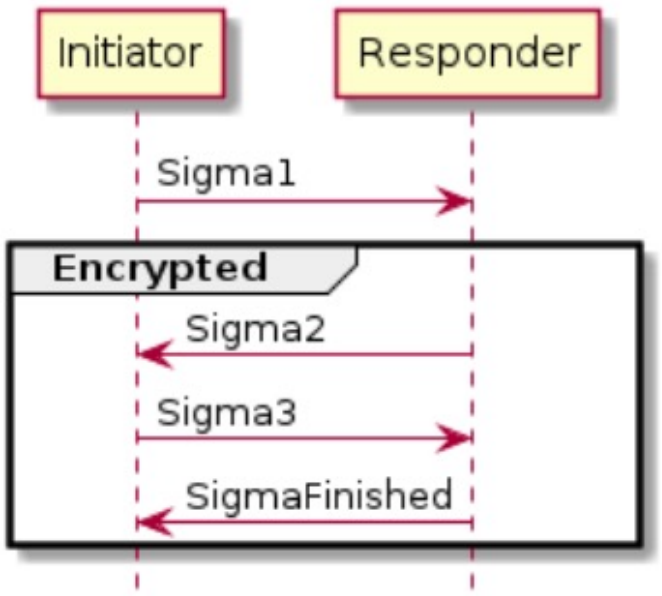
Commissioning – 安装NOC与节点信息配置



- Commissionee从NOC中获取Node id and Fabric id
- Commissionee 创建Access Control List (ACL)
  - 为Commissioner授予管理员权限
- 配置operational network information
  - Thread
    - Channel
    - Panid
    - ExtPanid
    - Network Key
  - WiFi
    - SSID
    - Password
- 基于DNS-SD的设备发现
  - DNS-SD: DNS-Based Service Discovery
  - Commissionee Host Name
    - Fabricid-Nodeid._matter._tcp

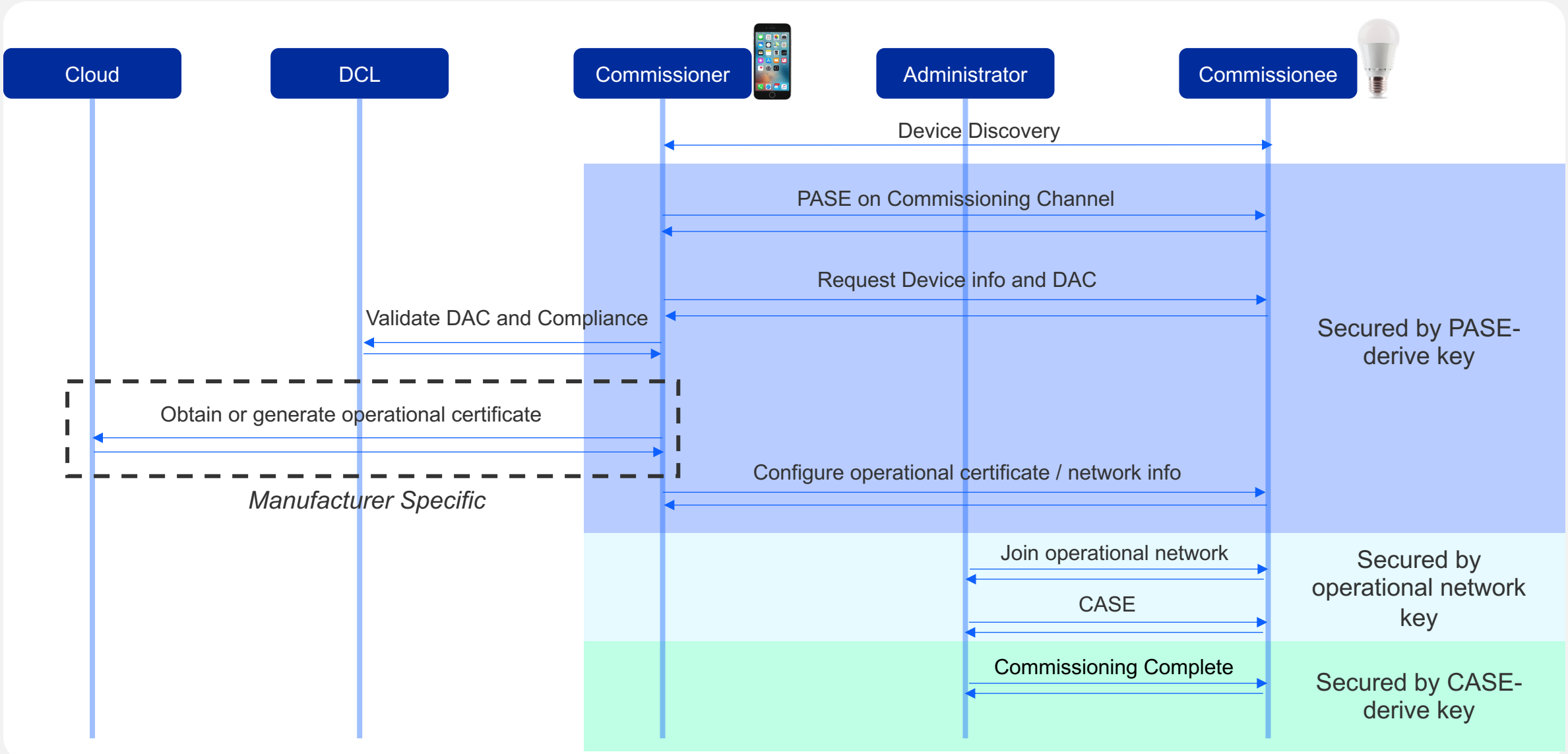
Commissioning – CASE

Commissioning – CASE



- Certificate-authenticated session establishment (CASE)
  - 基于证书认证的会话建立
- CASE的目的是为同一fabric中的2个节点建立安全的连接
- CASE基于SIGMA 协议
  1. 交换临时公钥，协商共享密钥 (Sigma1.initiatorEphPubKey and Sigma2.responderEphPubKey)
  2. 交换NOC和ICAC(Sigma2.encrypted2.responderNOC and Sigma3.encrypted3.initiatorNOC)
  3. 通过NOC所对应的私钥进行身份鉴别(sigma-2- tbsdata and sigma-3-tbsdata)
  4. 协商出I2RKey ,R2IKey 和 AttestationChallenge

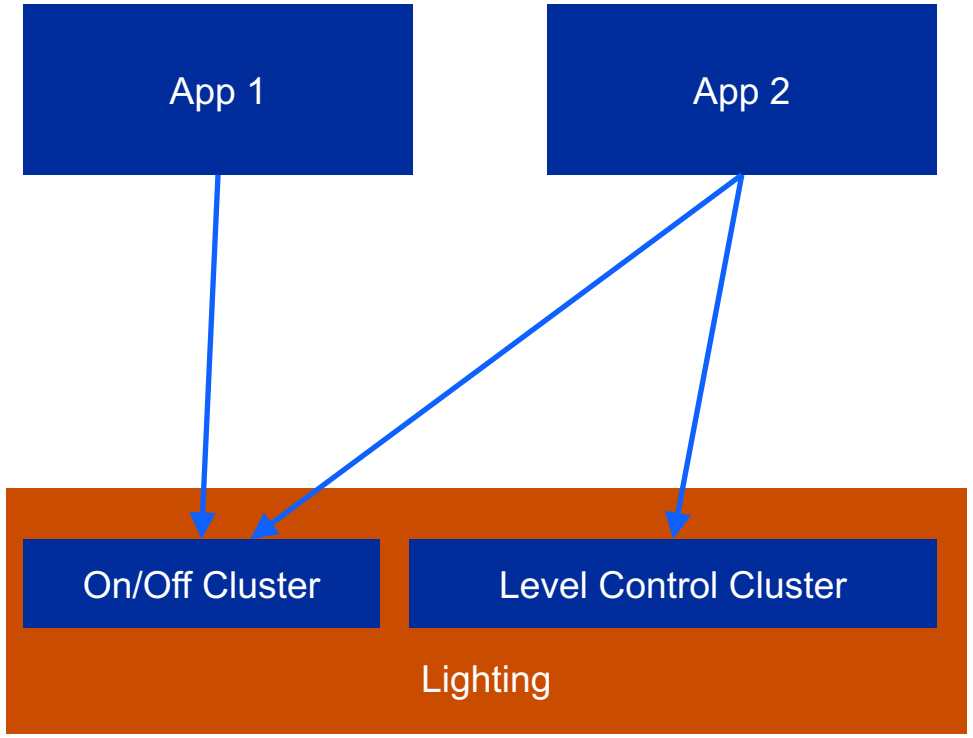
Commissioning Flow



SILICON LABS

访问控制 (Access Control)

访问控制



- 访问控制功能确保只有授权的节点才能访问Matter设备的某些功能(Cluster)
- 应用场景举例
  - App1只能控制灯的开关
  - App2既能控制灯开关又能调节亮度。
  - 访问控制列表(ACL)如下：

```
ACL: [
  0: {
    FabricIndex: 0,
    Privilege: operate,
    AuthMode: CASE,
    Subjects: [node ID of phone 1],
    Targets: [
      endpoint: 1,
      cluster: "on/off"
    ]
  },
  1: {
    FabricIndex: 0,
    Privilege: operate,
    AuthMode: CASE,
    Subjects: [node ID of phone 2],
    Targets: [
      endpoint: 1,
      cluster: [
        "on/off",
        "level control"
      ]
    ]
  }
],
```

SILICON LABS

Silicon Labs Secure Vault 解决方案

Silicon Labs 安全解决方案

PSA Certified™ Security Assurance Certificate

psacertified™
level three

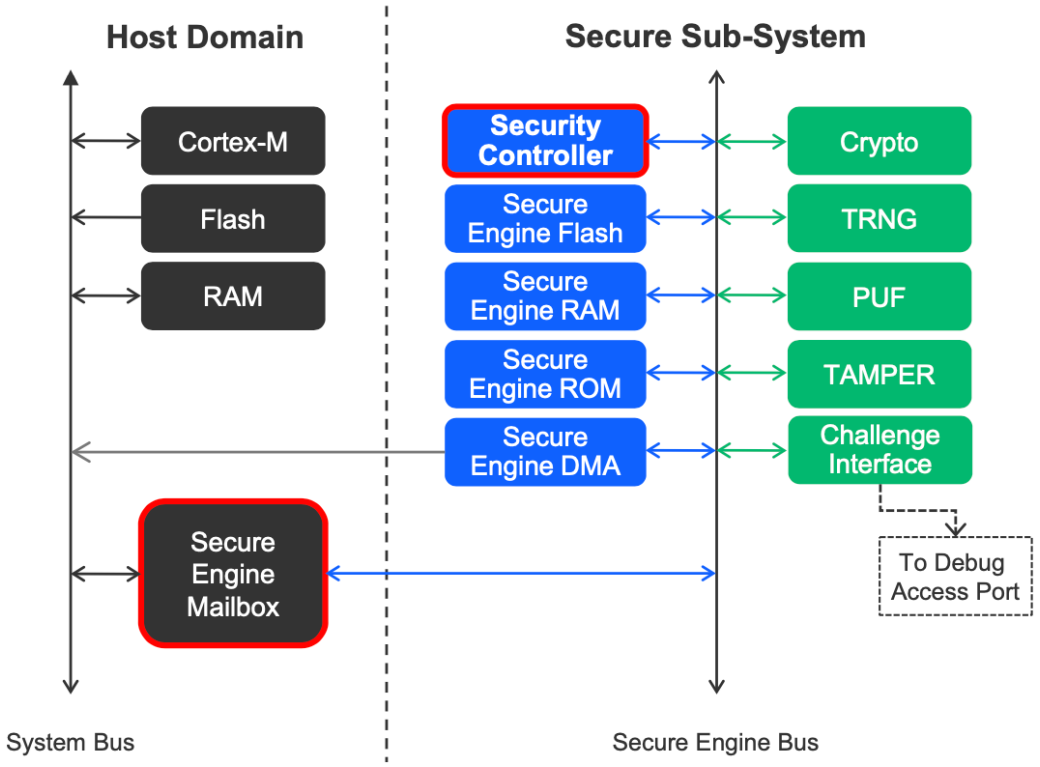
PSA Certified Level 3

- Silicon Labs的EFR32芯片是首个获得Arm PSA level2和level3认证的设备
- PSA Level 2要求
  - 芯片内部安全区域和非安全区域之间要隔离
  - 程序引导时需要检查固件的真实性与完整性
  - 保证密钥存储的安全性
  - 经过验证的加解密功能以及随机数生成功能
- PSA Level 3要求
  - 能够检测对设备的物理攻击并能做出相应的处理

Silicon Labs Secure Vault

xG1x	xG2xA	xG2xB	Feature
Base	Mid	High	
✓	✓	✓	True Random Number Generator
✓	✓	✓	Crypto Engine
✓	✓	✓	Secure Application Boot
—	VSE/HSE	HSE	Secure Engine
—	✓	✓	Secure Boot with RTSL
—	✓	✓	Secure Debug with Lock/Unlock
—	Optional	✓	DPA Countermeasures
—	—	✓	Anti-Tamper
—	—	✓	Secure Attestation
—	—	✓	Secure Key Management
—	—	✓	Advanced Crypto

安全引擎 - Secure Engine Subsystem



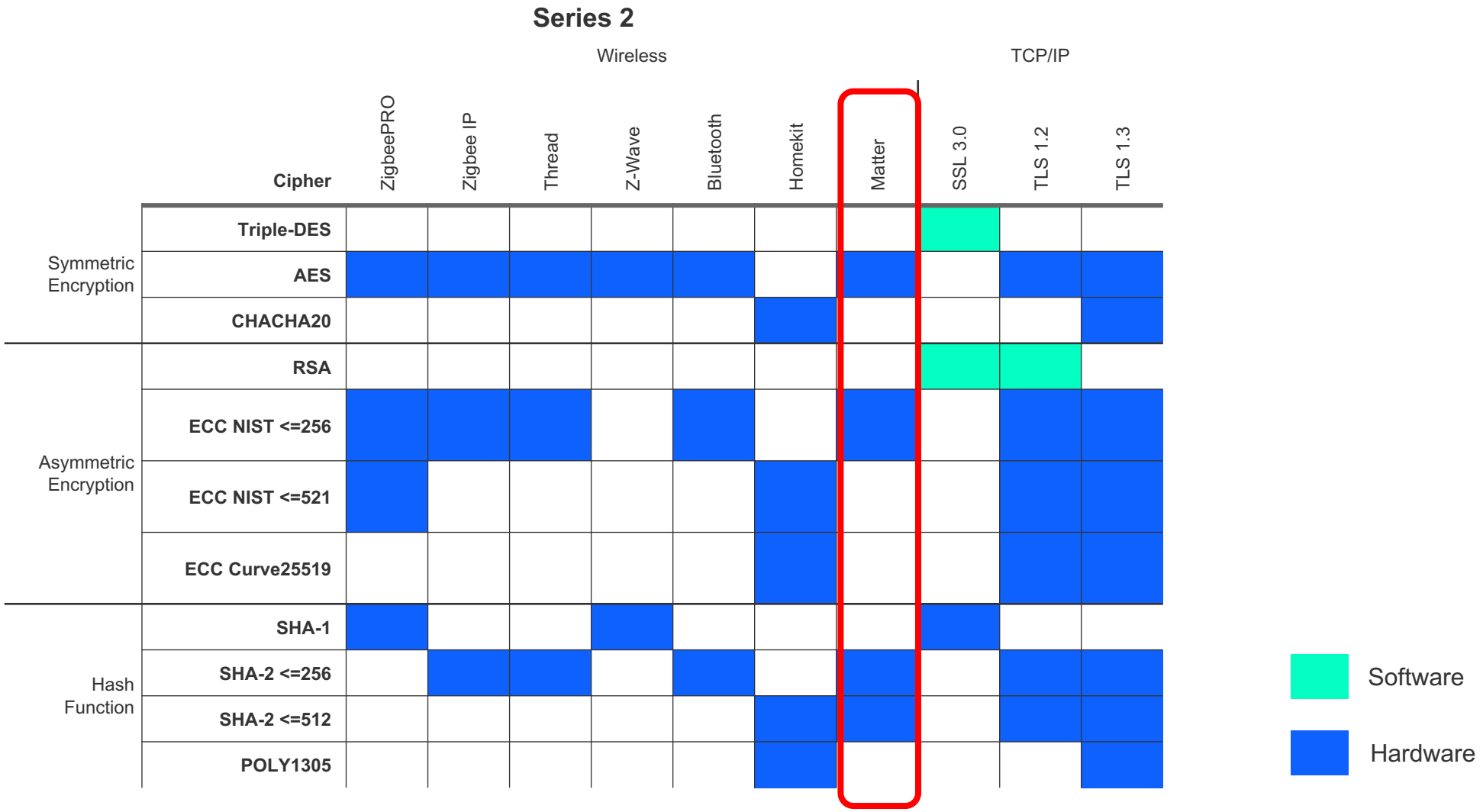
- 所有安全相关的功能都在安全引擎中实现
- 安全引擎实现方式
  - 软件 – Arm TrustZone架构
  - 硬件 – 安全处理器
- 对安全处理器访问受限
  - 主处理器通过邮箱访问安全处理器
  - 通过Debug 接口访问安全处理器 (需要完成安全验证)

安全处理器固件

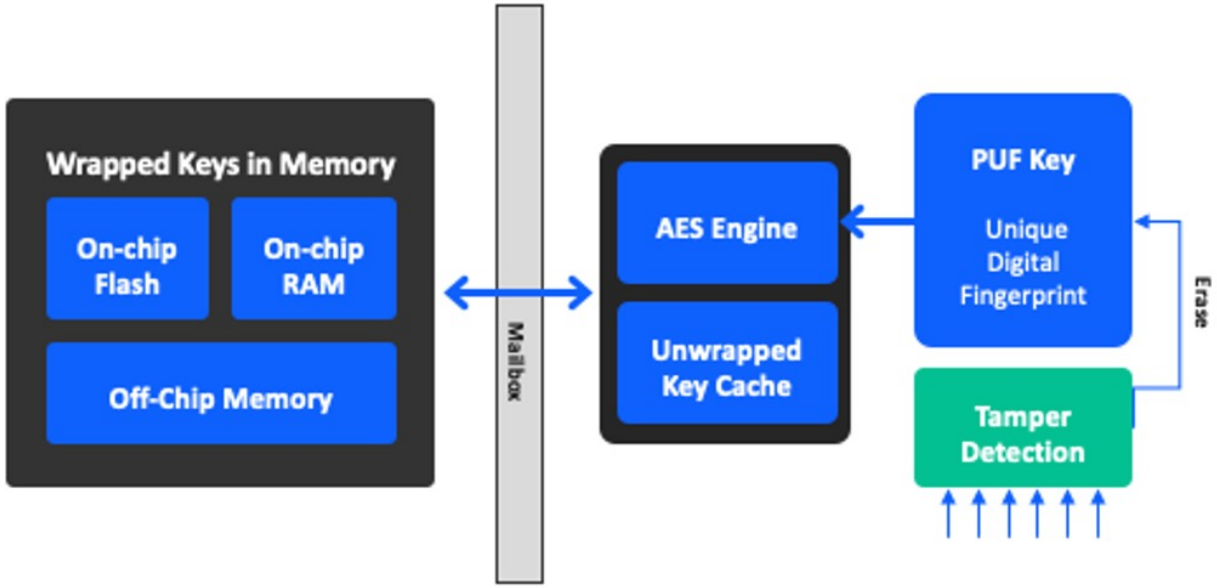
- 用户无法定制安全处理器固件，但可以升级原厂提供的固件

- 增加安全处理器的好处
  - 提高安全性
  - 主处理器专注于其他任务的处理，效率更高

加密引擎



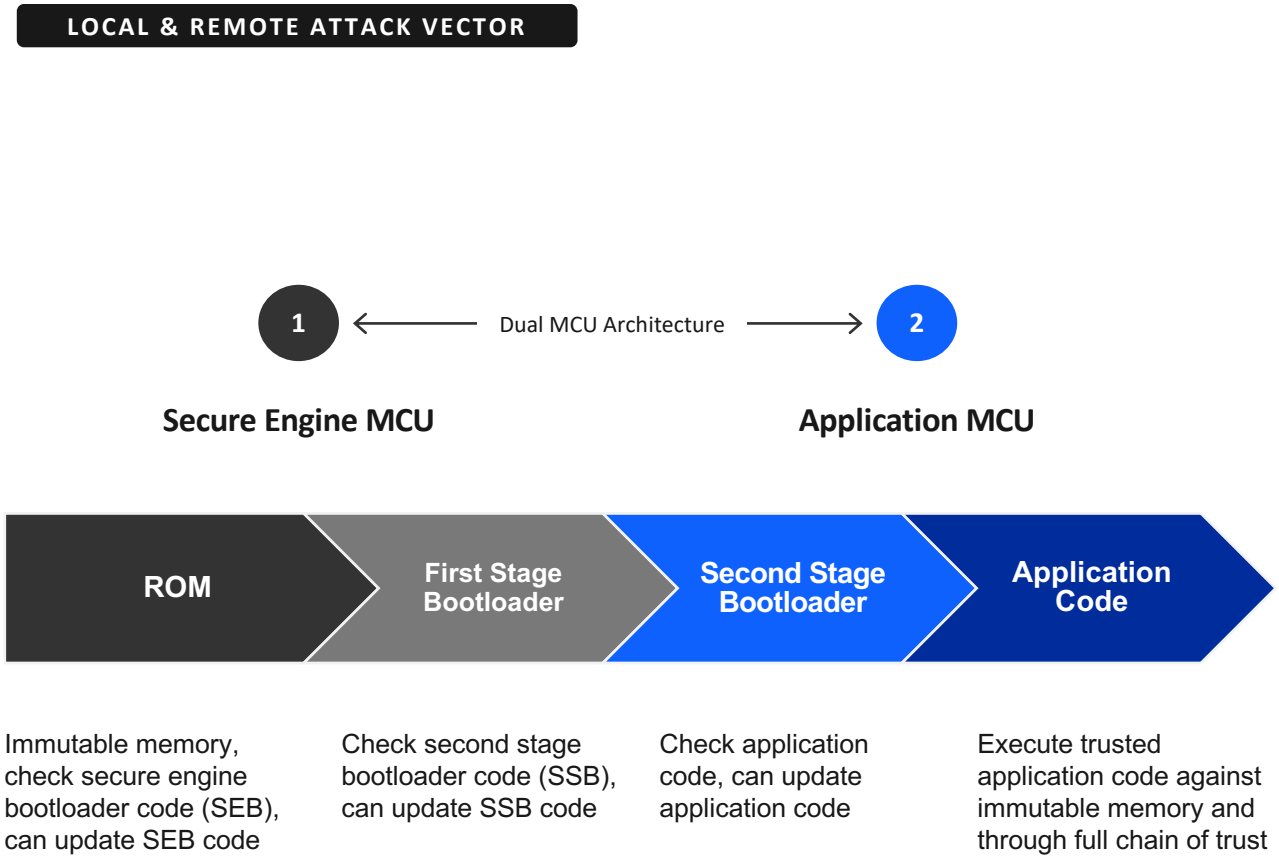
安全密钥管理功能



AN1271: Secure Key Storage

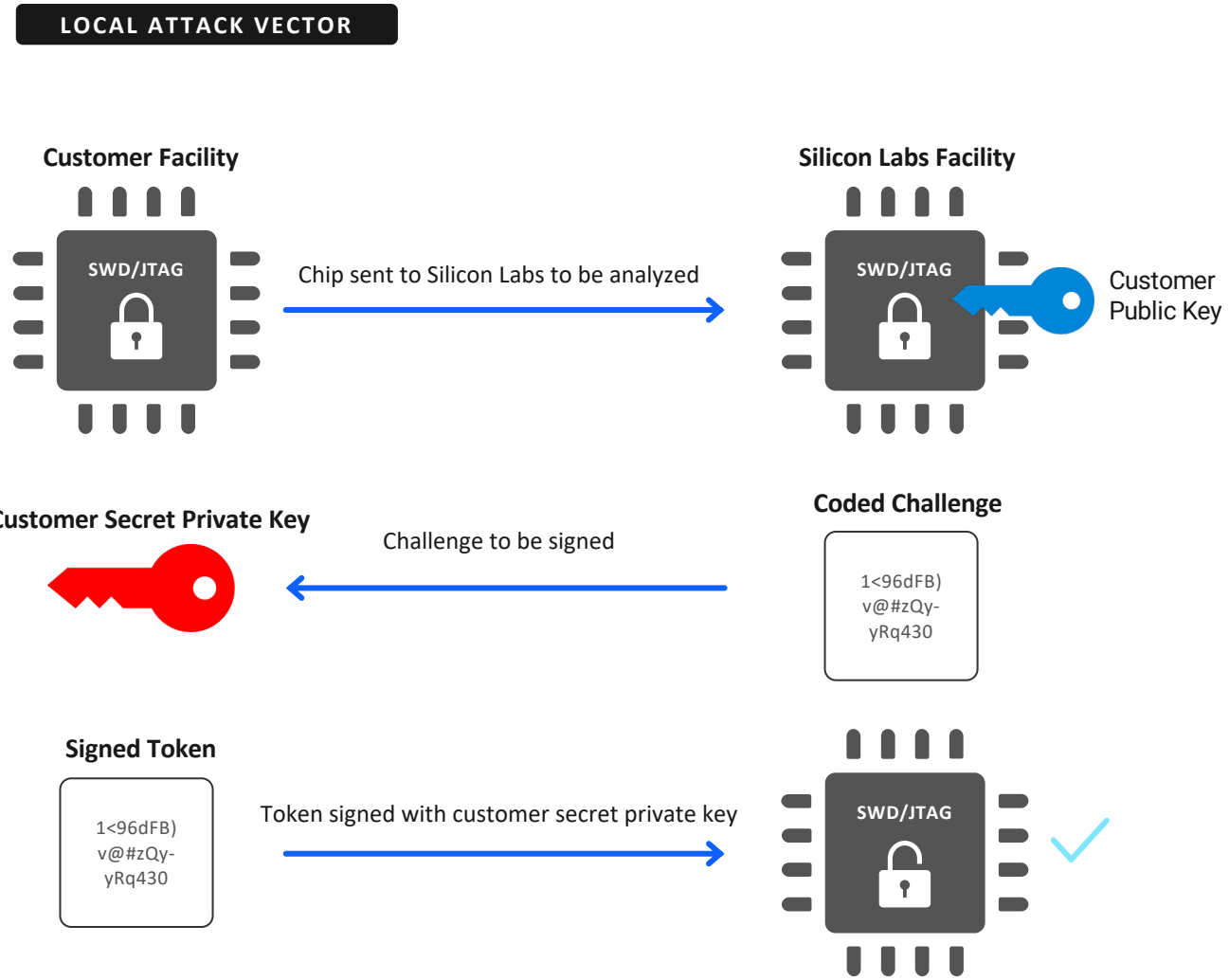
- PUF(Physically Unclonable Function)
  - 芯片每次上电时产生相同的数据作为PUF-Key
  - PUF-Key断电不保存
  - PUF-Key只有Secure Engine能够访问
  - PUF-Key用于密钥加密
- Secure Engine产生并保存密钥明文
  - RAM
- PUF-Key加密后的密钥保存在主MUC中
  - RAM
  - 内部FLASH
  - 外部FLASH
- 主MCU做加解密时，将数据和加密的密钥传给Secure Engine， Secure Engine运算完成后将结果返回给主MCU
- 密钥安全性保证
  - 密钥由Secure Engine产生并保存
  - 密钥从未离开Secure Engine
  - 只有Secure Engine能够访问PUF-Key

Secure Boot With RTSL



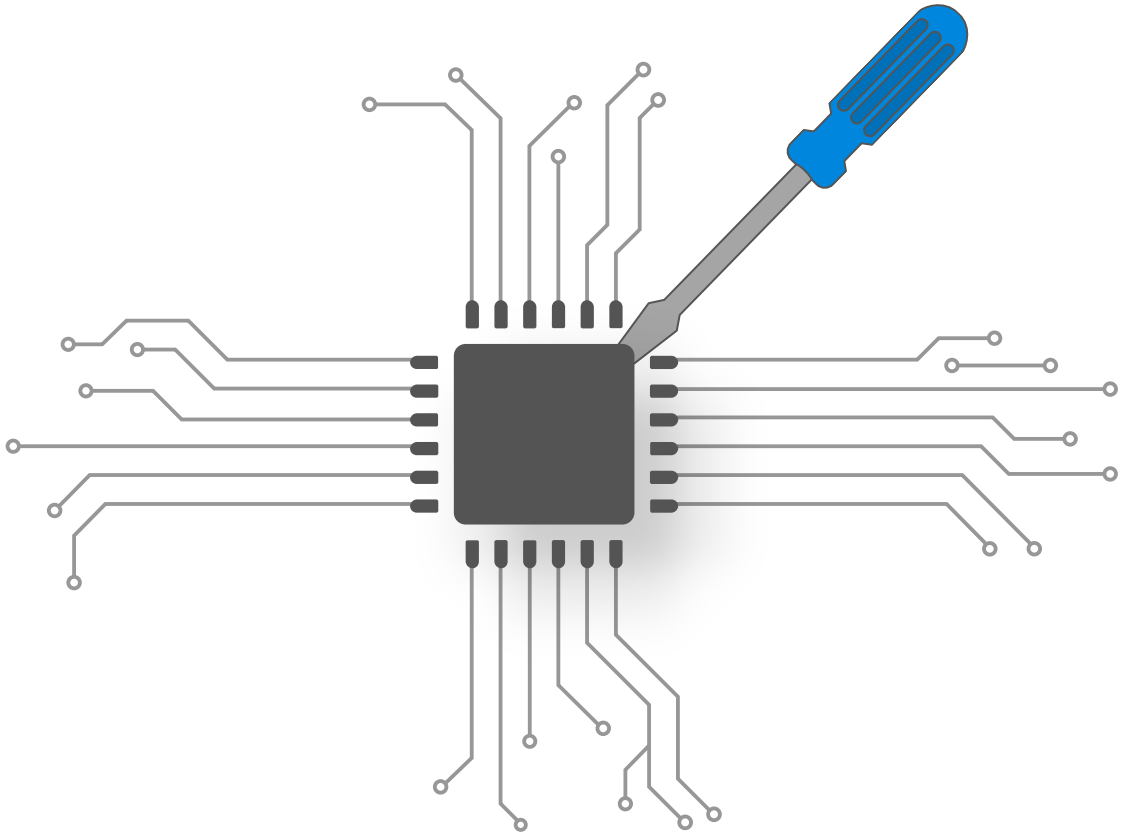
- 安全风险
  - 黑客可能通过篡改固件的方式获取设备的私密信息
- Secure Boot with RTSL
  (Root-of-Trust & Secure Loader)
  - 通过完整的信任链保证芯片上运行的固件都是经过签名验证的
  - ROM区代码无法被擦除或修改，被称为Root-of-Trust
- 应用文档
  - AN1218: Series 2 Secure Boot with RTSL

Secure Debug



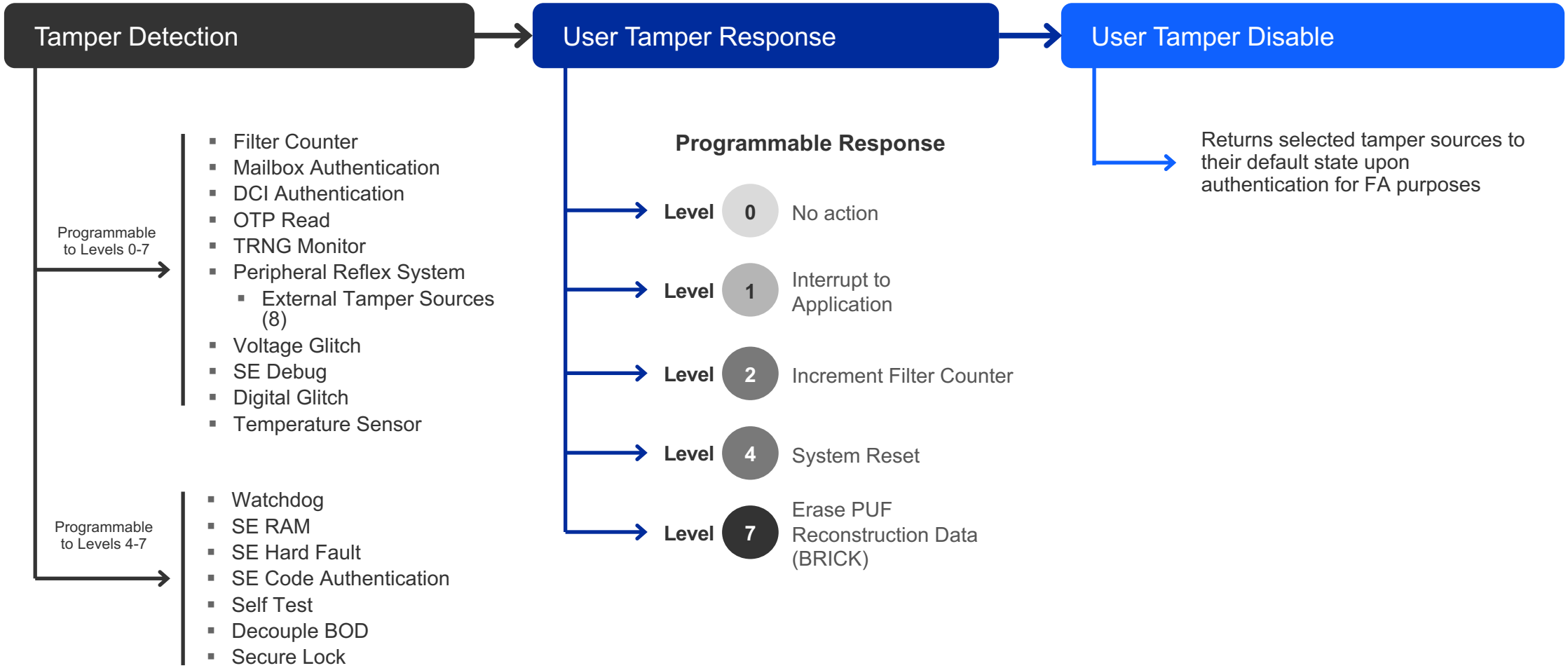
- 安全风险
  - 未上锁的Debug接口是严重的安全风险
  - 常规的Debug Lock功能在解锁时固件会被擦除，无法做失效分析
- Secure Debug
  - 使能Secure Debug Lock的设备可以通过加密令牌来解锁
  - 解锁不会擦除固件
  - 芯片复位后Debug接口会被重新上锁
- 应用文档
  - AN1190: Series 2 Secure Debug

Anti-Tamper (1/2)



- 安全风险
  - 安装在户外的IOT设备更容易收到物理攻击
    - 温度，电压，时钟输入，磁噪声
    - 调试器以高速率运行
    - 频繁复位
- Anti-Tamper
  - Anti-Tamper能够检测出多种物理攻击
  - Anti-Tamper能够对检测出的异常行为做出可编程的处理
- 应用文档
  - AN1247: Anti-Tamper Protection Configuration and Use

Anti-Tamper (2/2)



DPA Countermeasures

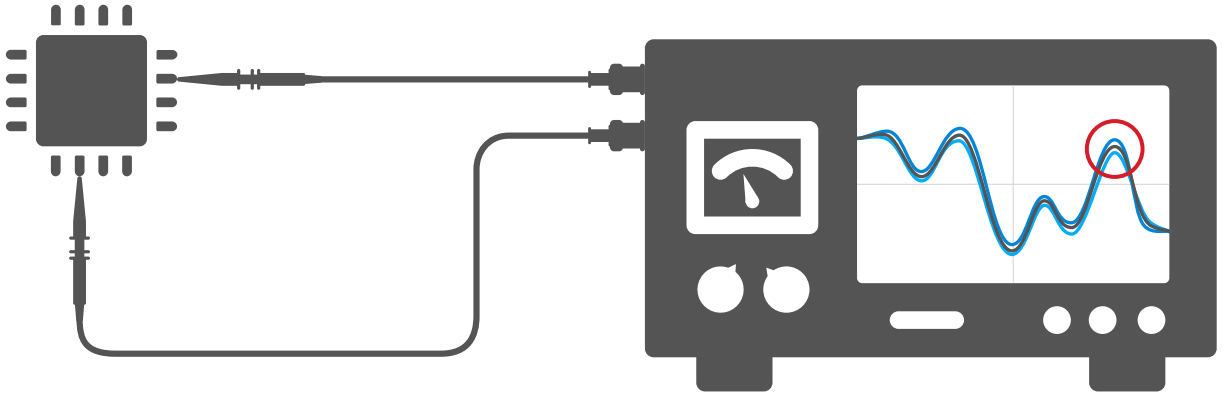
LOCAL ATTACK VECTOR

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.

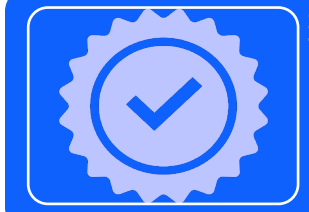
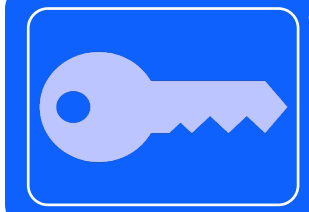
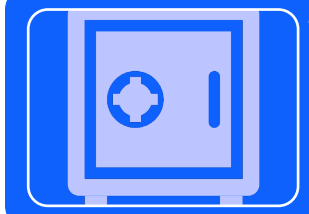


- 安全风险
  - DPA(Differential Power Analysis) 工具能通过功耗测量知道芯片何时在做加解密操作，进而分析出密钥
- DPA Countermeasures
  - 对加解密操作进行随机，使得功耗与加解密操作无规律性

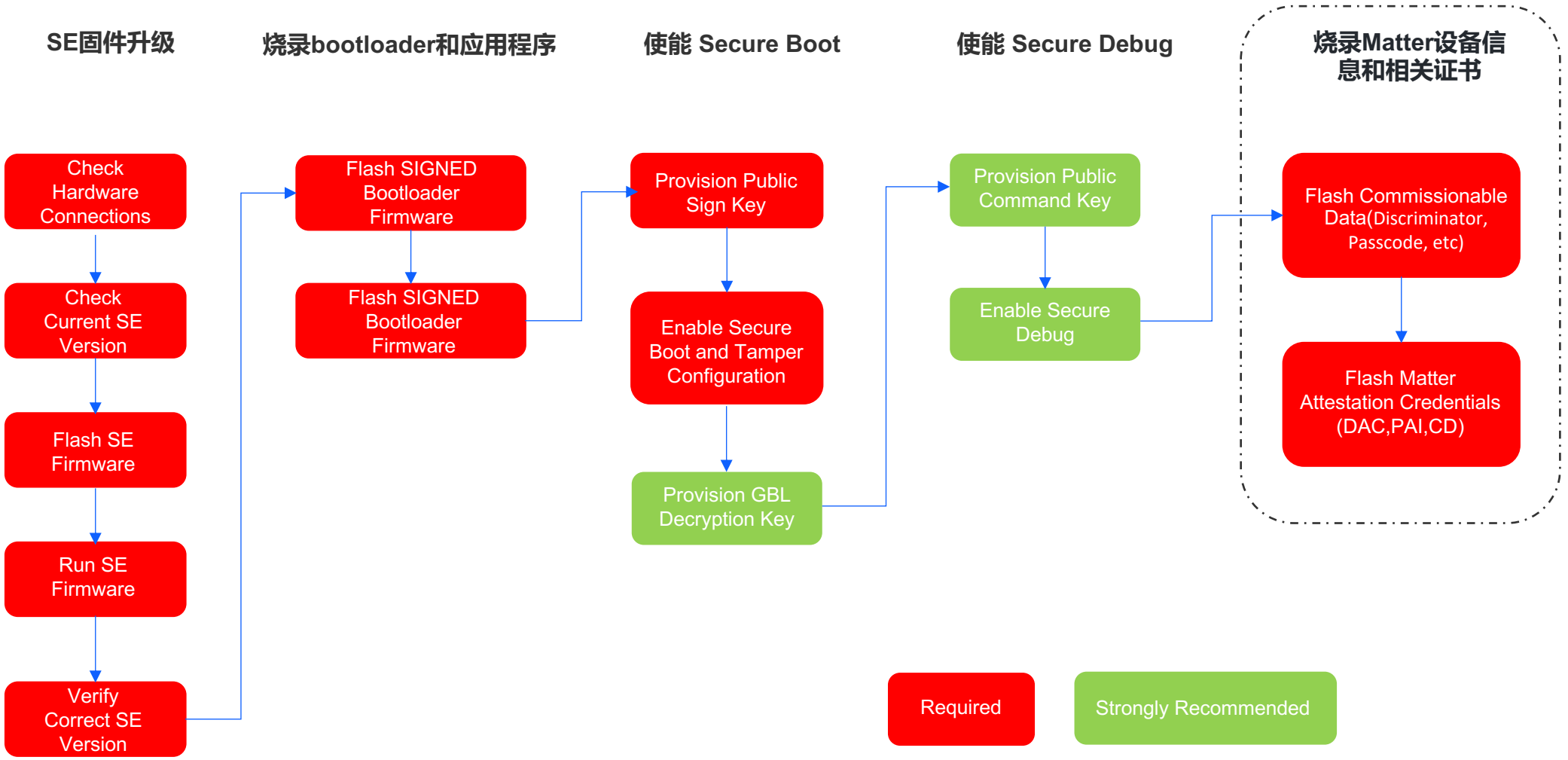
SILICON LABS

Silicon Labs Secure Vault 让Matter更安全

Silicon Labs Secure Vault 让Matter更安全

Matter安全元素	Silicon Labs保护措施	制造商获益
 **设备认证证书(DAC)** •制造商在工厂生产的时候安装证书 •证明设备的身份是真实的 •证明设备是经过Matter认证的	设备认证私钥存由Secure Vault保护，并且不可导出	防止攻击者克隆您的设备和窃取您的品牌
 **操作证书(Operational Certificate)** •在加入Matter Fabric时生成的证书 •用于Matter Fabric中的节点的身份认证	操作私钥存由Secure Vault保护，并且不可导出	防止攻击者在Matter Fabric中仿冒Matter节点
 **证书认证会话建立(CASE)** •用于两个Matter设备之间生成对称秘钥 •利用操作证书 •在CASE会话建立期间生成临时的公钥和私钥对	CASE会话建立过程中的临时私钥在Secure Vault中生成，并且不可导出	防止攻击者获取到CASE生成的对称密钥
 **安全启动(Secure Boot)** •经过制造商认证的软件固件 •经过加密的软件升级 •可升级的bootloader以防止未来的攻击	通过完整的信任链保证芯片上运行的固件都是经过签名验证的	攻击者无法侵入固件并永久控制你的设备

Secure Boot Matter Device生产烧录流程



[AN1222: Production Programming of Series 2 Devices]

SILICON LABS

谢谢！

Silicon Labs 官方网站	Silicon Labs 微信公众号	Silicon Labs 在线社区