Tech Talks LIVE Schedule – Presentation will begin shortly

tech talks

Wireless Connectivity Tech Talks

Thursday, March 25th	Unboxing the BGM220 Explorer Kit
Wednesday, April 28th	Uncover Sub-GHz and Proprietary Solution within Simplicity Studio v5
Thursday, August 19th	**Discover the Security Features of Secure Vault**

Recording and slides will be posted to:
www.silabs.com/training

We will begin in 3:00

Speaker

이경보 (Victor Lee)

Sr. FAE, Korea

SILICON LABS

tech talks

WELCOME

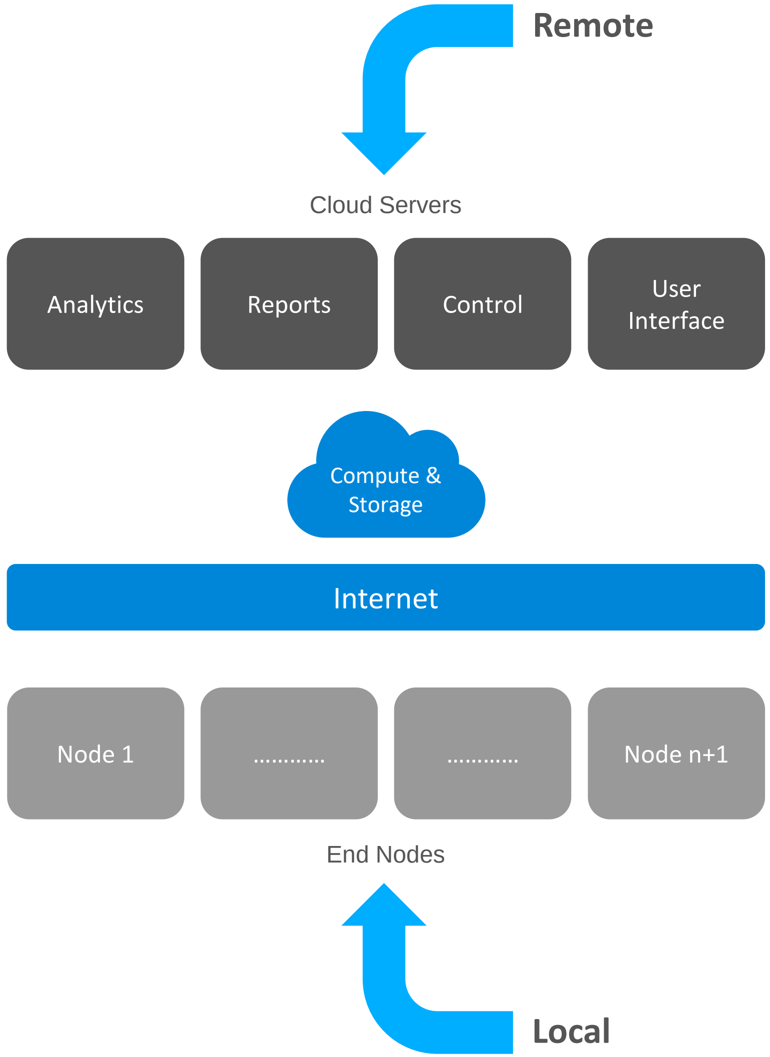
Discover the Security Features of Secure Vault

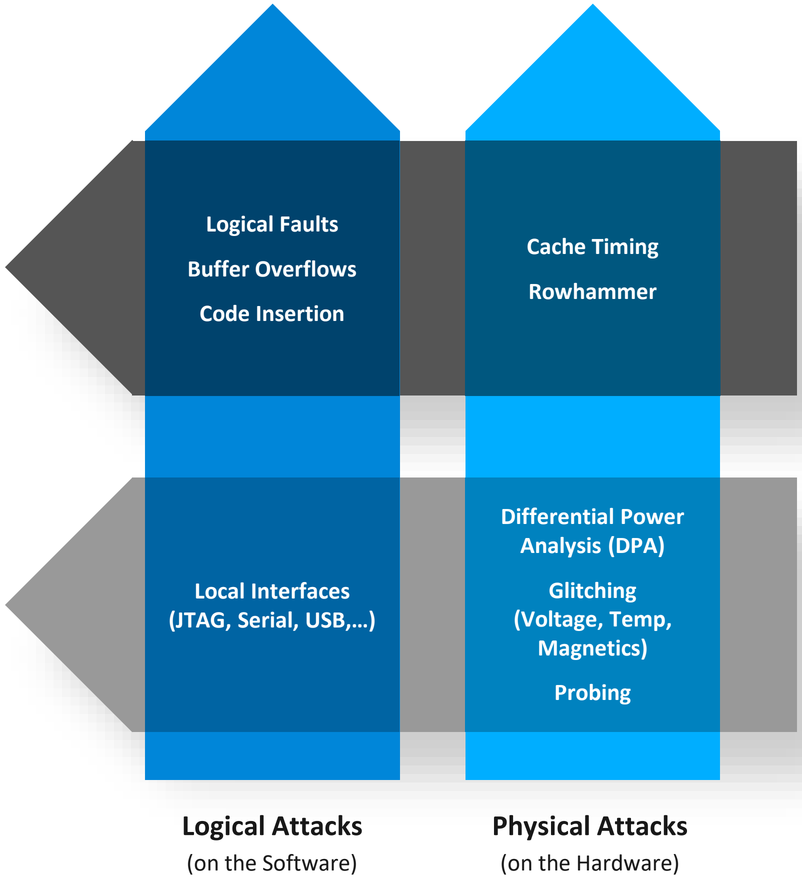
Victor Lee

Agenda

- Secure Vault Overview
- Anti-Tamper
- Secure Identity
- Secure Identity Demo
- Support Documentation

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

Threats evolve.
So should your device security.
Introducing Secure Vault.

silabs.com/security

Secure Vault – first silicon to achieve PSA Level 3 Certification

psacertified™
level three

https://www.psacertified.org/products/secure-vault/

- EETimes
- Arm Beyond The Now Podcast
- Silabs Press Release

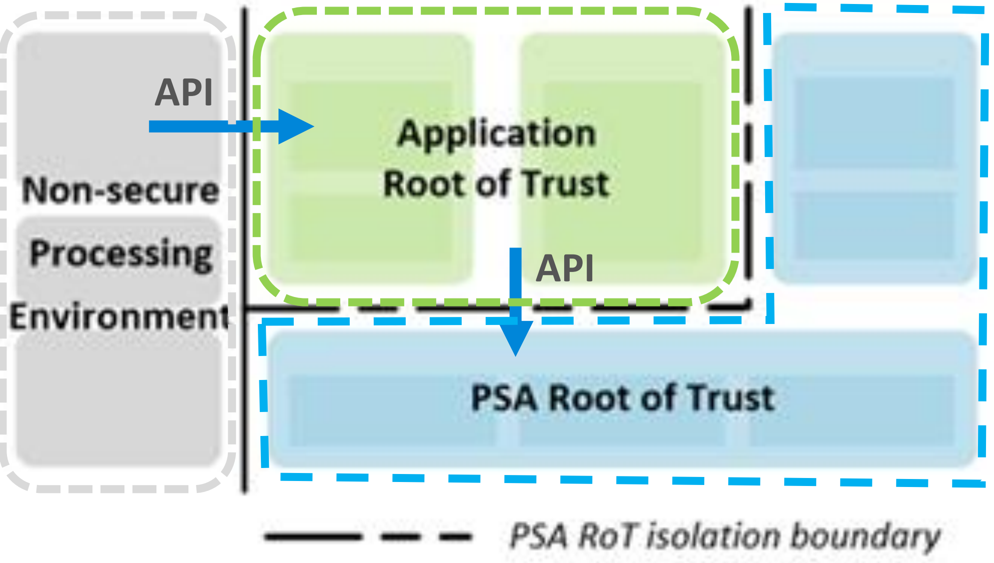
PSA Level 2&3 Requirements for Boundary Separation

Isolation level 2

Level 2 introduces an isolation boundary between the PSA Root of Trust and the Application Root of Trust.

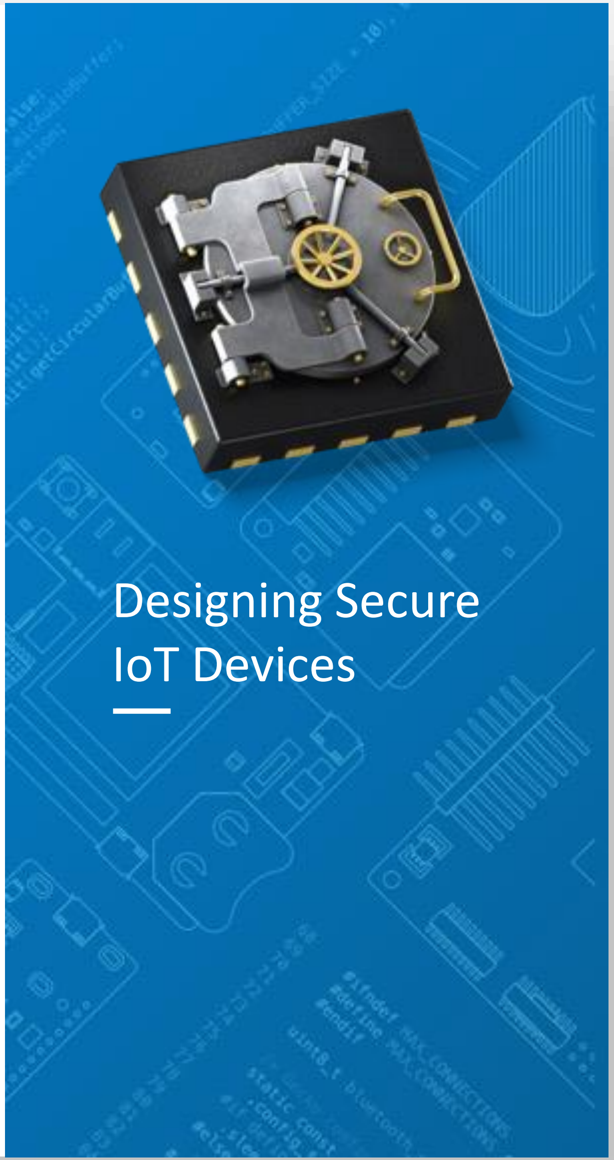
The protection domains and the required protection for isolation level 2 are as follows:

Protection domain	Needs protection from
NSPE	-
Application Root of Trust	NSPE
PSA Root of Trust	NSPE Application Root of Trust

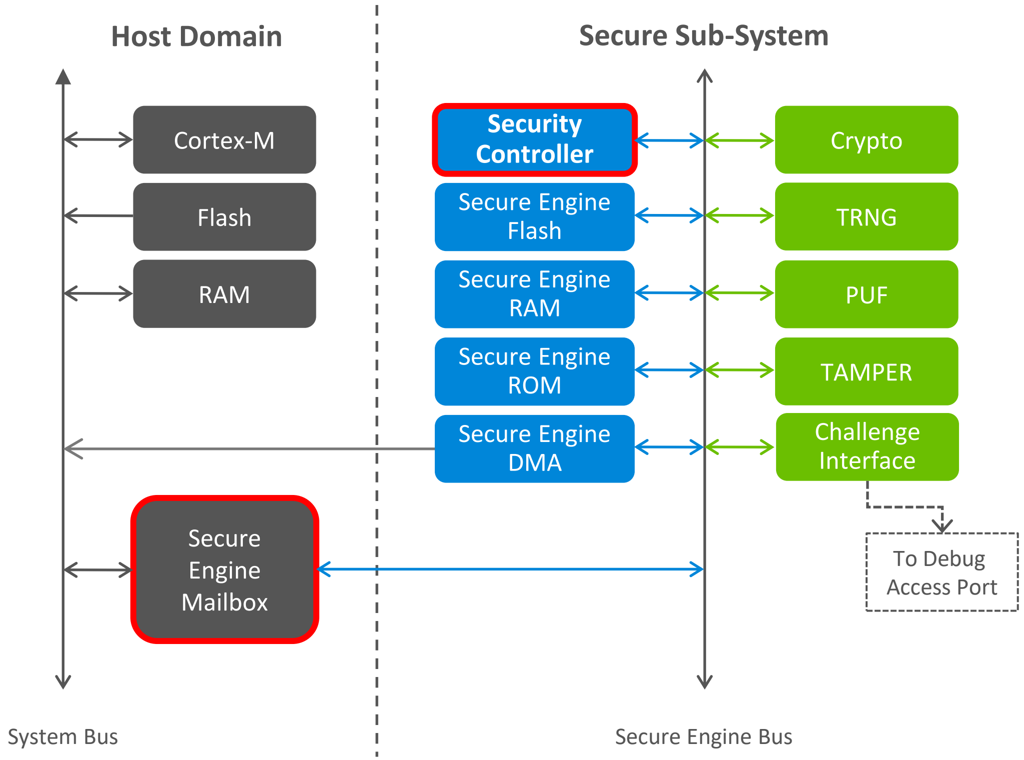


SecureVault™

Base	Mid	High (xG2xB)	Feature
✓	✓	✓	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



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

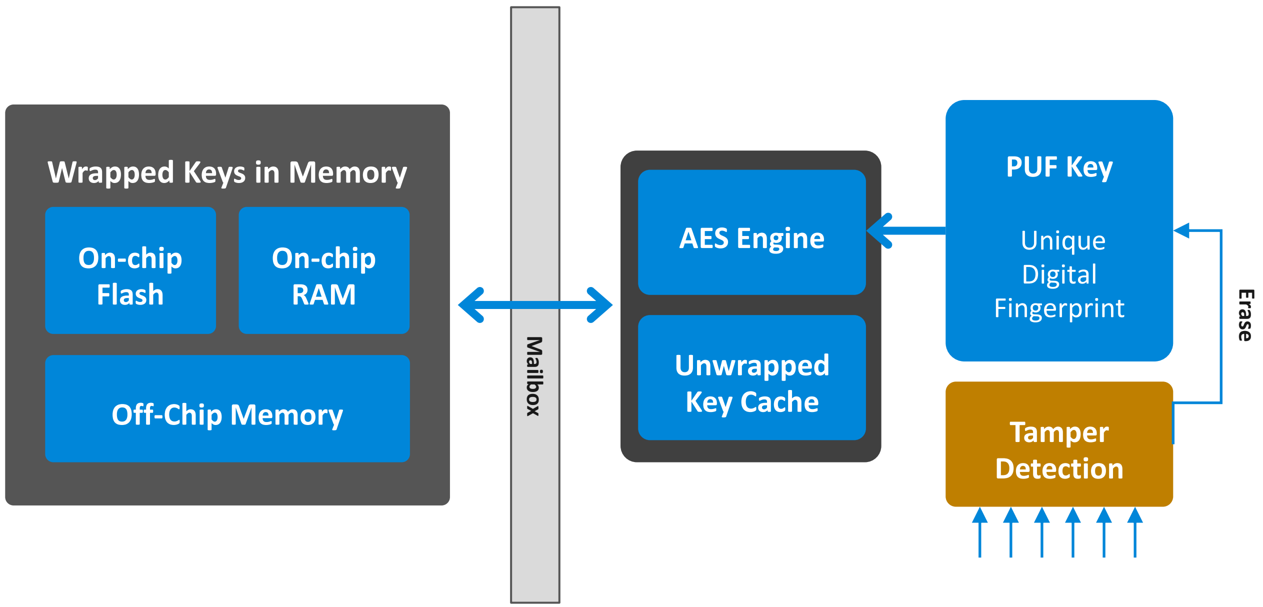
Limited accessibility to crypto-coprocessor
- Via a Host mailbox interface
- Debug pins (with Debug Challenge Interface, or DCI)

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 Key Management

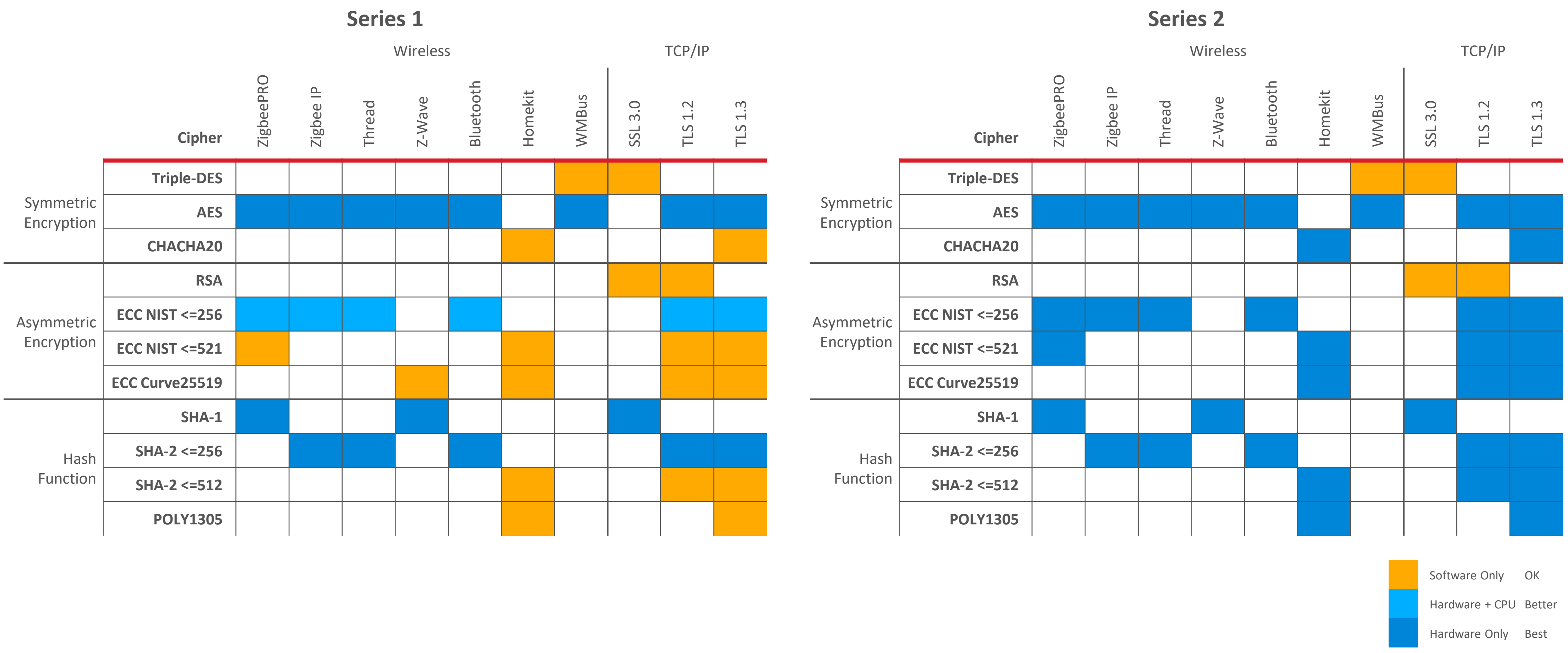
LOCAL & REMOTE ATTACK VECTOR



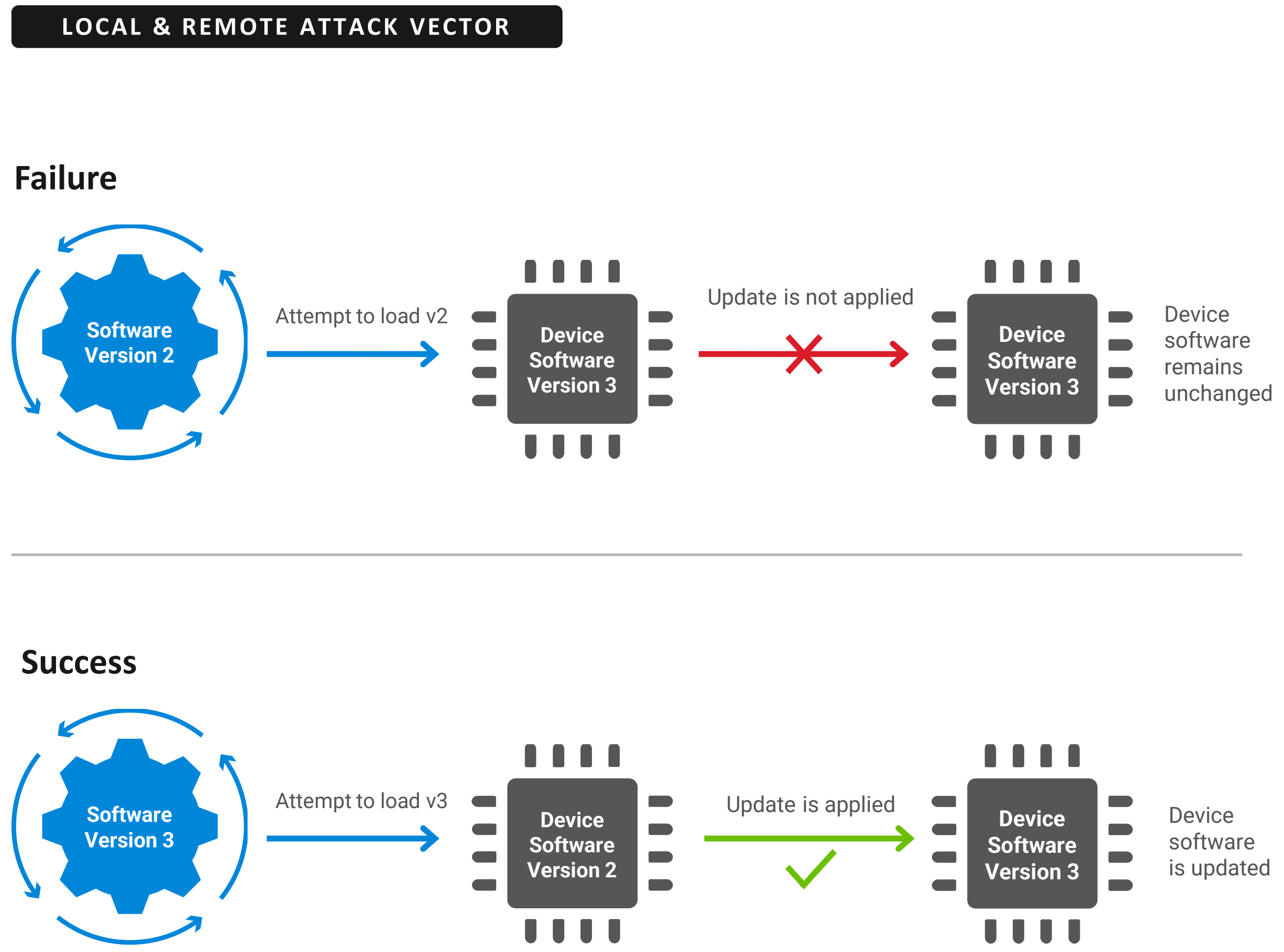
- Vulnerabilities
  - When an attacker learns how to extract keys or content from a device, they use the same attack vector to attack other devices
- Secure Key Management
  - A Physically Unclonable Function creates a secret, random, & unique key, from individual device imperfections
  - The PUF-key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

Cryptography Engine

Protocol Usage & Support



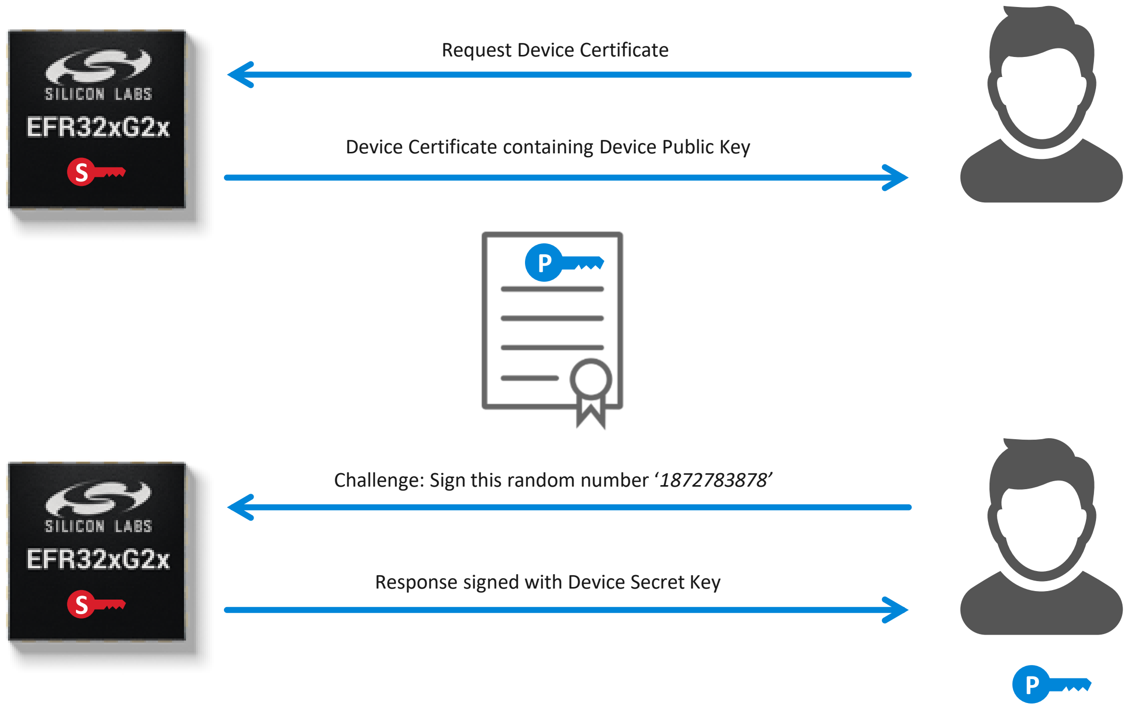
Anti-Rollback Prevention



- Vulnerabilities
  - Adversaries may have knowledge of a security flaw present in older firmware
- Anti-Rollback Prevention
  - Prevents older digitally signed firmware from being re-loaded into a device to re-expose patched flaws

Secure Attestation

LOCAL ATTACK VECTOR



- Vulnerabilities
  - Many systems use a UID to identify devices, but the UID is public (can be copied)
  - Developers are concerned with the authenticity of their devices
  - Most successful companies suffer counterfeit products and "ghost shifts"
- Secure Attestation
  - Secure Vault devices generate a unique device ECC keypair on-chip and securely stores the secret private key
  - The device secret private key never leaves the chip
  - During production
    - Test program reads the device public key
    - Placed in certificate & signed with an HSM secret key
    - Re-stored back in chip's OTP memory
  - External service can request the certificate chain from the device and CA web server which retrieves the unique device public key.
  - External service can perform a "Challenge Response" to the chip at any time during the life of the product to Authenticate the chip is genuine

DPA Countermeasures

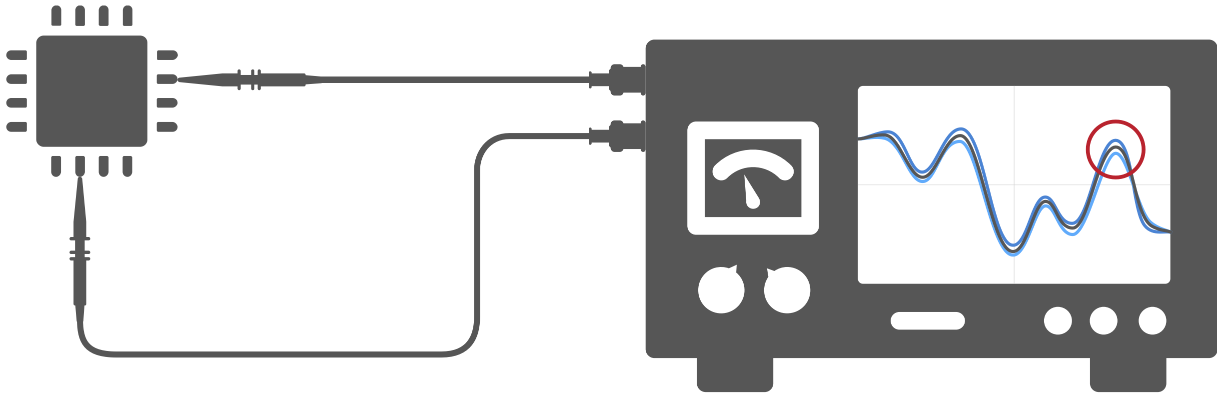
LOCAL ATTACK VECTOR

1

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

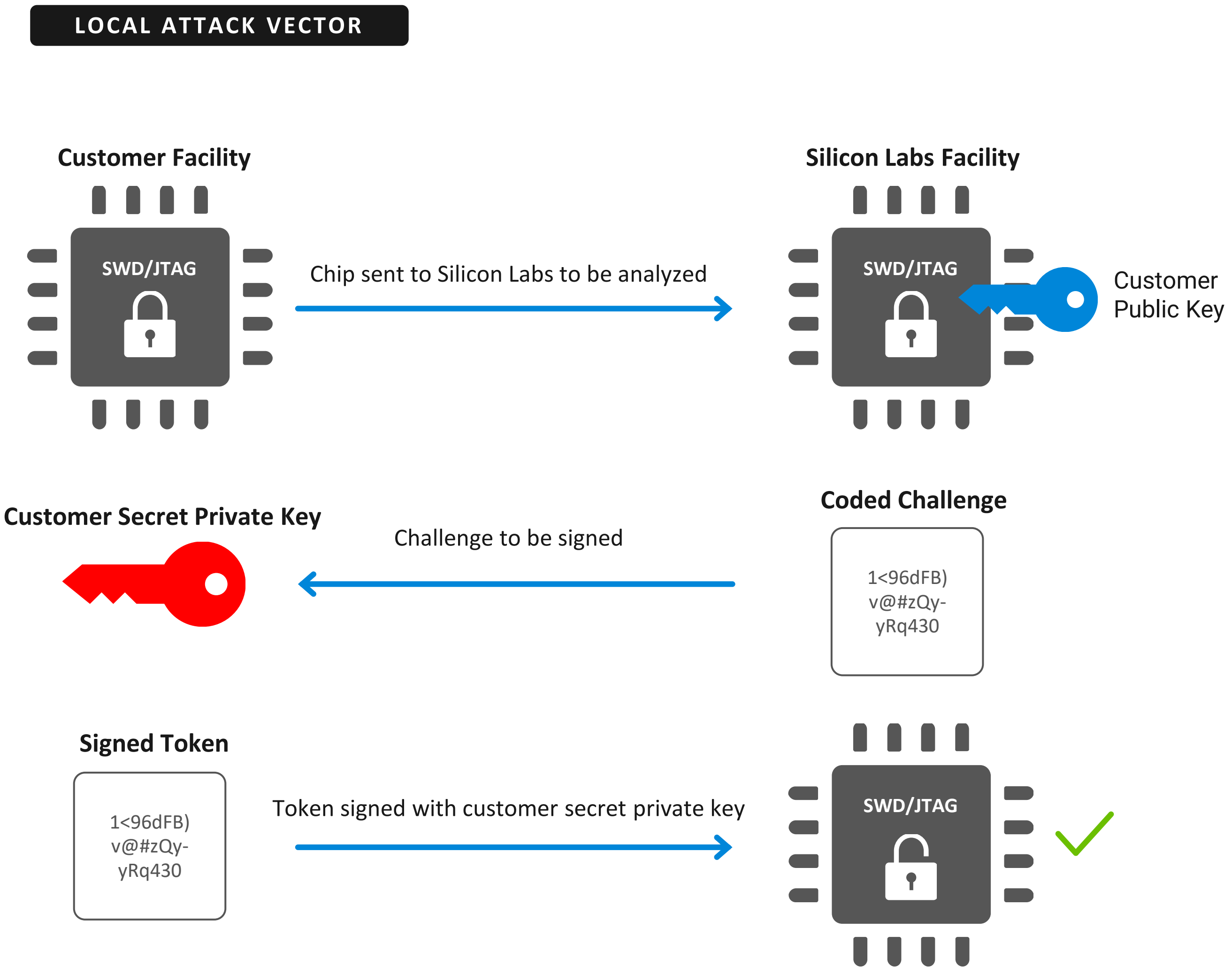
2

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



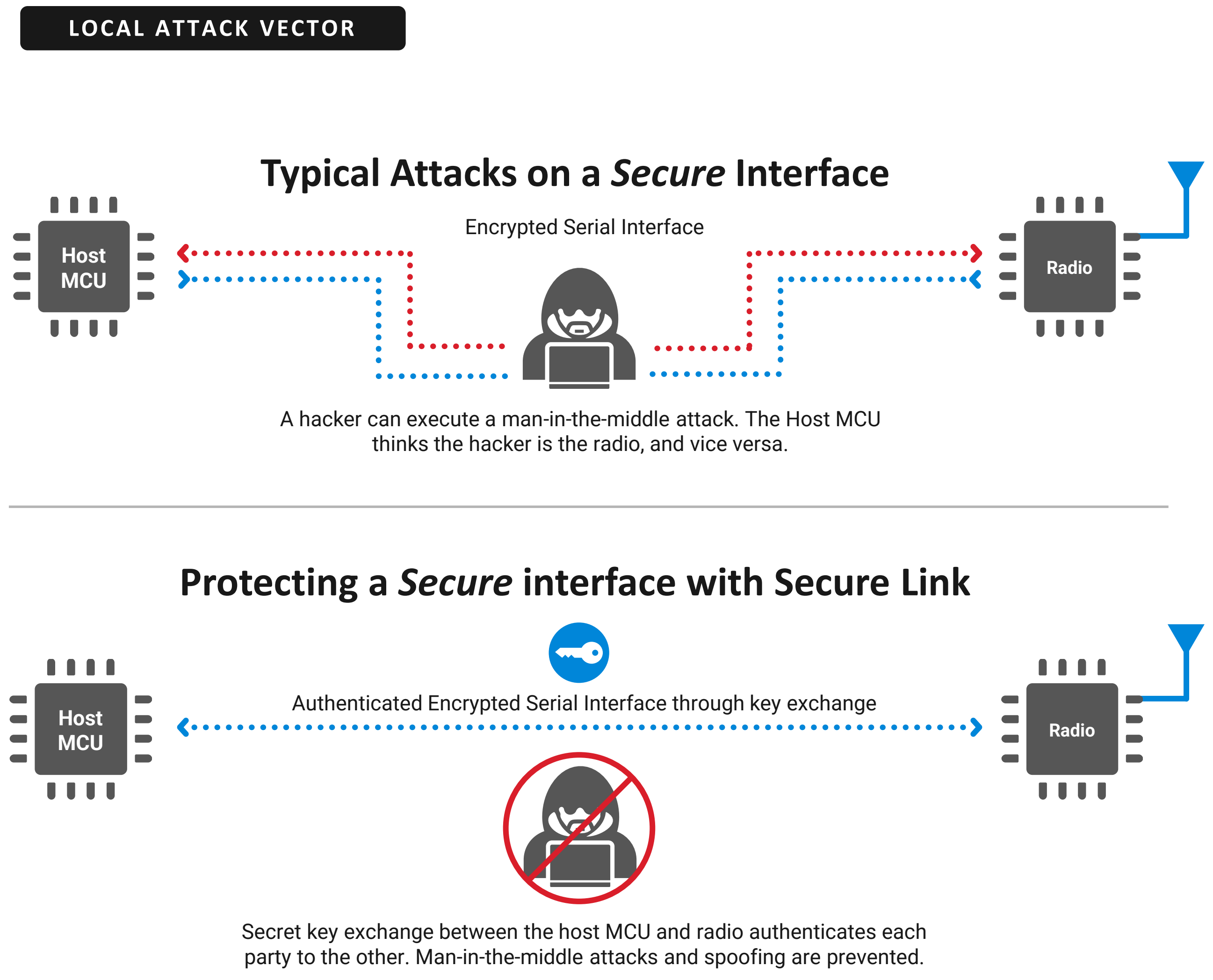
- Vulnerabilities
  - Observing subtle signal differences during given internal operations can provide insight into cryptographic functions
- DPA Countermeasures
  - Countermeasures add masks and random timings to internal operations and distorts DPA snooping

Secure Debug



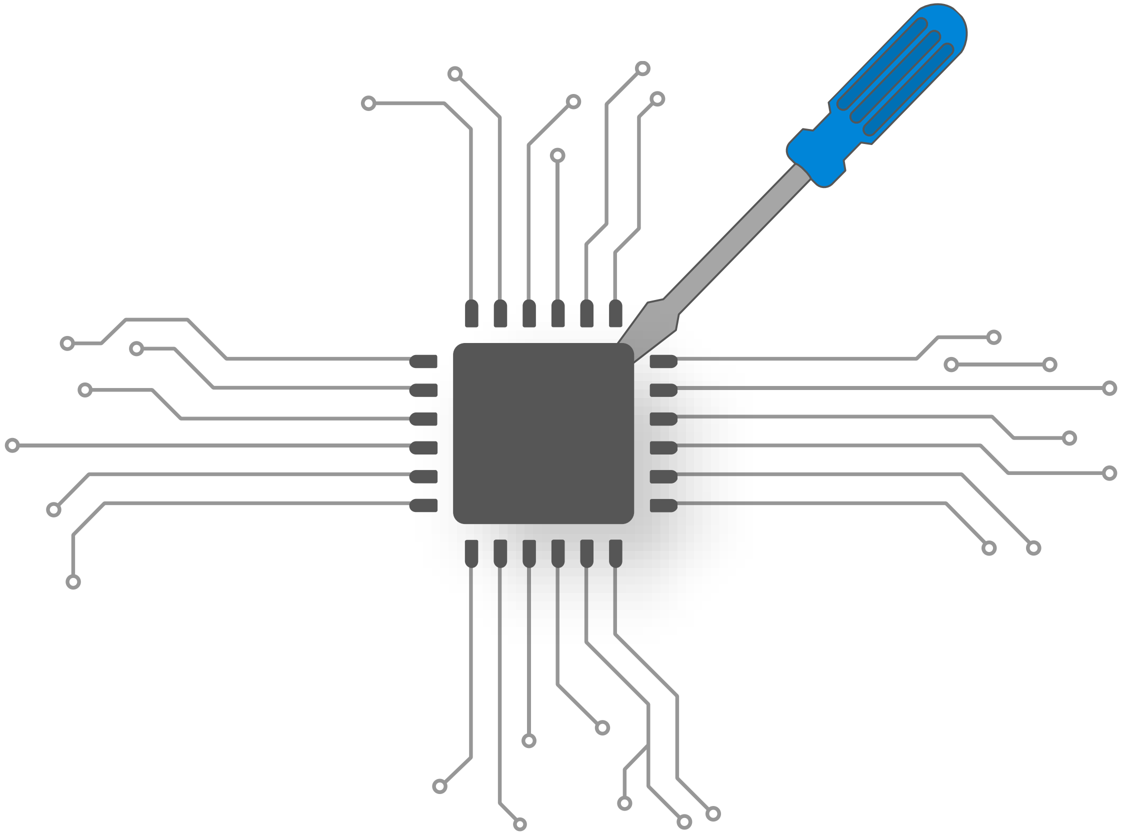
- Vulnerabilities
  - Unlocked ports are a significant security vulnerability
  - Unlocking debug ports typically wipes the memory to protect IP but this limits device failure analysis capabilities
- Secure Debug
  - Lock the emulation port and use optional cryptographic tokens to unlock it allowing memory to remain intact

Secure Link



- Vulnerabilities
  - PCB's can be easily probed potentially exposing keys, passwords and data
- Secure Link
  - Encrypts selected bus messages using a Diffie-Hellman key exchange
  - Keys are uniquely created on a 'per session/per device' basis.
  - No fleet-wide keys & new keys on each power-cycle

Anti-Tamper (1/2)



Why

- Many attacks force a device outside its standard operating range(s)
  - temperature, voltage, clock-inputs, magnetic noise
  - Debuggers running at a high rate, reboots at a high rate
- Cost of these attacks is now low enough for both large scale and hobbyists

Silicon Labs

- Implemented an ability to detect when these attacks happen
  - Voltage, clock, temperature and magnetic tamper detectors in our devices
  - Secure boot, secure debug use counters to flag abnormal behavior
  - External triggers from broken enclosures via buttons and traces
- Implemented an ability to respond to these attacks
  - Programmable tamper response
    - Includes an ability to perform rapid deletion of Secure Key Storage (forced bricking)

Anti-Tamper (2/2)

Tamper Detection

Programmable to Levels 0-7

- Filter Counter
- Mailbox Authentication
- DCI Authentication
- OTP Read
- TRNG Monitor
- Peripheral Reflex System
  - External Tamper Sources (8)
- Voltage Glitch
- SE Debug
- Digital Glitch
- Temperature Sensor

Programmable to Levels 4-7

- Watchdog
- SE RAM
- SE Hard Fault
- SE Code Authentication
- Self Test
- Decouple BOD
- Secure Lock

User Tamper Response

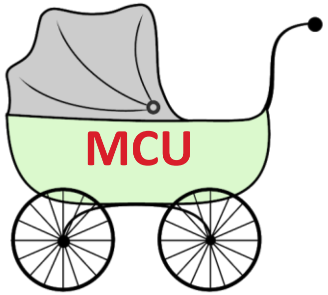
Programmable Response

- **Level 0** No action
- **Level 1** Interrupt to Application
- **Level 4** System Reset
- **Level 7** Erase PUF Reconstruction Data (BRICK)

User Tamper Disable

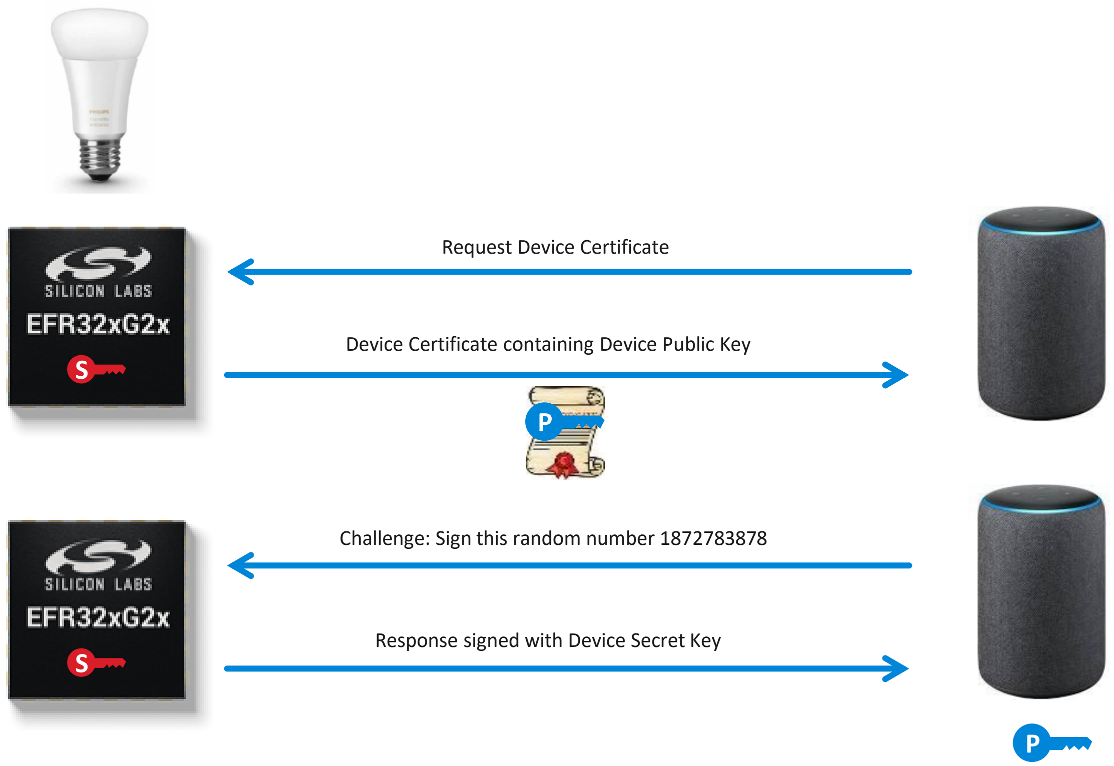
Returns selected tamper sources to their default state upon authentication for FA purposes

What is a Secure Identity?



- A Secure Identity is like a “birth certificate” for a device or a product
- A Secure Identity allows you to –
  - Trust that a device is authentic, and
  - Trust that a device is the specific device it claims to be
- Common uses for a Secure Identity
  - Ensure the device is authentic (secure the supply chain)
  - Ensure that the product is authentic (anti-counterfeit)
  - Support remote authentication of a communication link
  - Support commissioning to a wireless network
  - Satisfy regulatory requirements

Authentication Using a Device Certificate



Is the certificate authentic?

1. Request Device Certificate
2. Receive Device Certificate and verify its authenticity with the certificate chain

Is the certificate related to this device?

3. Send random challenge for the device to sign (using the device's private key)
4. Verify the signed challenge using the device's public key from the Device Certificate

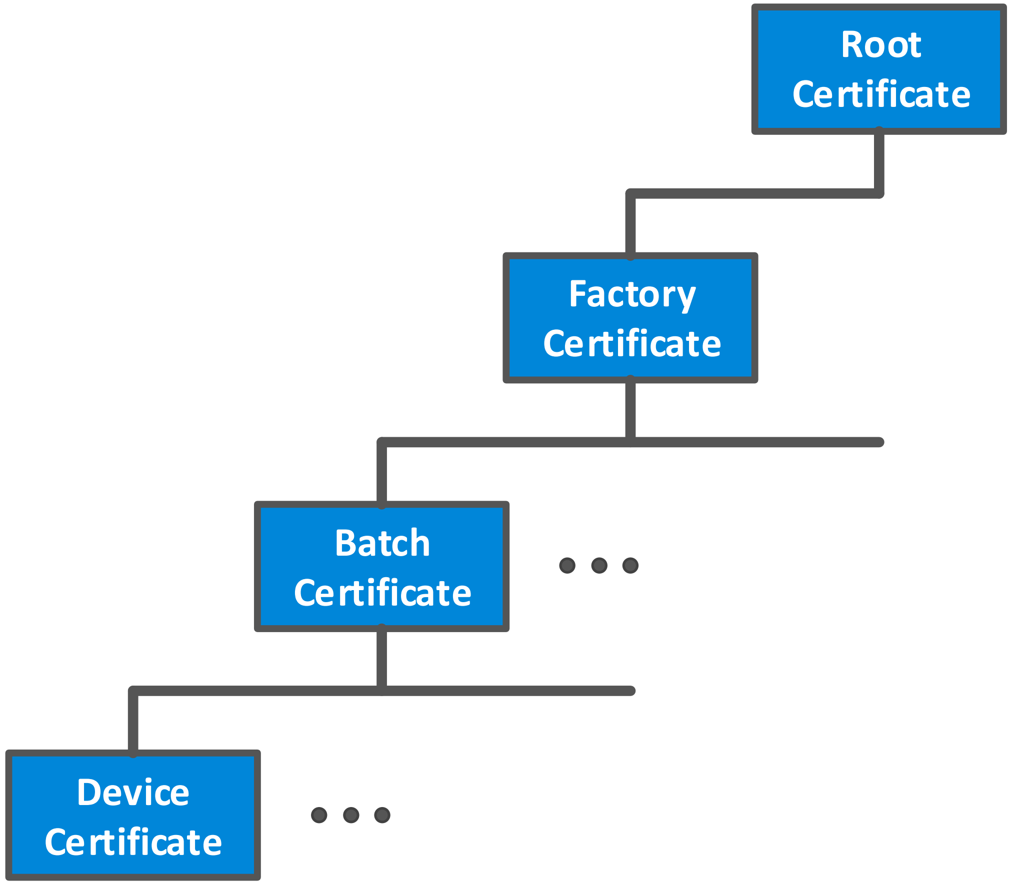
Example Secure Vault Device Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            49:2e:fd:a2:68:42:be:d4:ce:4b:ba:0b:11:60:a3:e4:e1:e0:49:90
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: O = Silicon Labs, CN = Batch 7069870
        Validity
            Not Before: Aug 16 17:55:19 2019 GMT
            Not After : Jul 23 17:55:19 2119 GMT
        Subject: C = US, O = Silicon Labs Inc., CN = EUI:000b57fffe181c9a OMS:08266E5611
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:f1:7e:ab:36:33:d2:b5:d6:bf:4c:b6:e1:82:47:
                    55:91:fa:ba:d3:12:44:5c:80:71:c7:83:e8:5a:2d:
                    85:4d:25:31:e3:21:fd:f2:2c:54:c1:8d:e8:0a:42:
                    0f:84:9c:e3:cd:9b:48:30:2b:74:1d:c9:dc:70:49:
                    31:7a:5e:e9:9c
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Subject Key Identifier:
                78:F9:C0:4A:44:7D:28:51:C3:68:63:CE:39:9F:DD:6F:55:D9:09:E1
            X509v3 Authority Key Identifier:
                keyid:2C:1D:BB:0D:10:F8:3E:DB:AA:F3:90:41:1F:A0:74:EA:78:37:0C:04

            X509v3 Key Usage: critical
                Digital Signature, Non Repudiation, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Client Authentication
    Signature Algorithm: ecdsa-with-SHA256
         30:46:02:21:00:9f:7f:32:7e:73:fd:e9:2b:42:7b:03:01:7c:
         7f:35:0f:f6:0c:fd:04:e0:7e:da:79:17:75:f3:b6:58:fd:ba:
         eb:02:21:00:ed:98:d6:aa:cf:a8:1b:1d:c2:88:8f:c8:f5:05:
         f1:91:61:4e:f8:fb:bf:2d:35:bb:91:2b:62:bd:90:4b:75:52
```

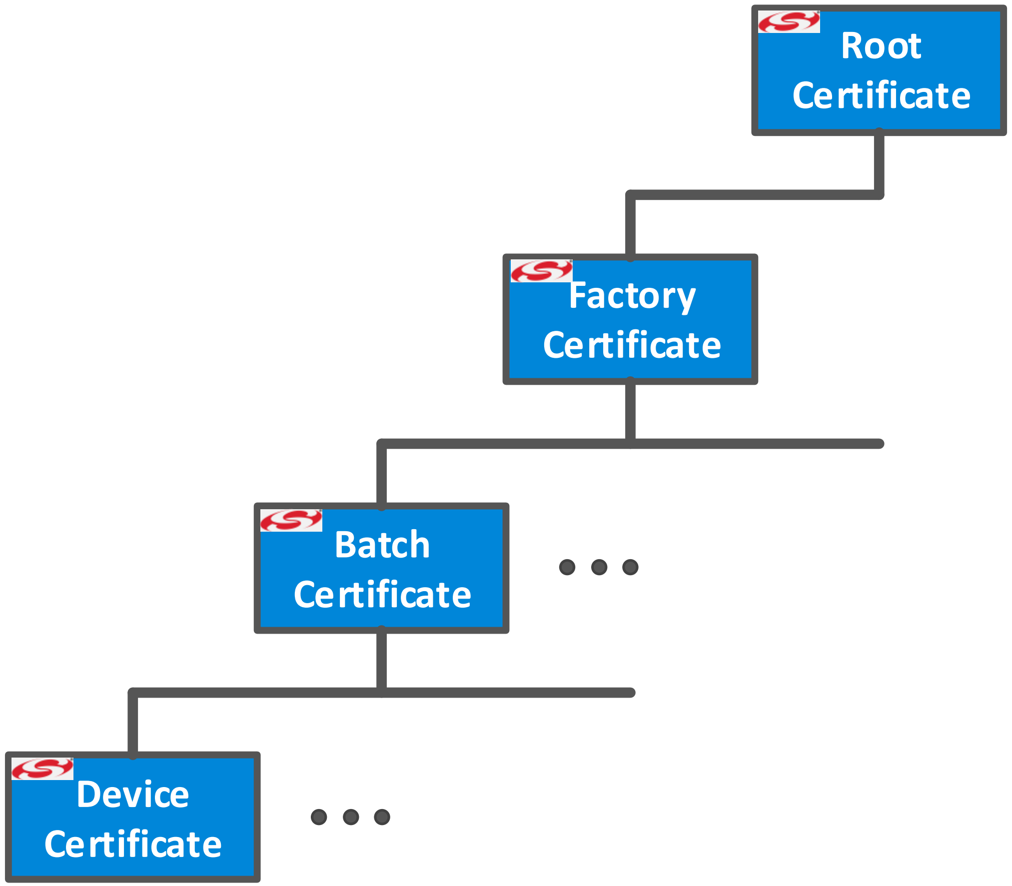
- The Device Certificate is unique to each device
- Device Certificate is stored in OTP
  - Cannot be modified once programmed
- Device Certificate is X.509 (DER-encoded binary)
  - Compatible with established internet protocols and appliances
- Common Name field contains the 64-bit EUI
  - Same as EUI64 in DEVINFO page
- Device-specific Public Key
  - Private key is generated by and securely stored in the HSE
- Validity period is 100 years from device manufacture date
- The Device Certificate can be accessed from the serial wire debug interface or from software

Device Certificate Chain



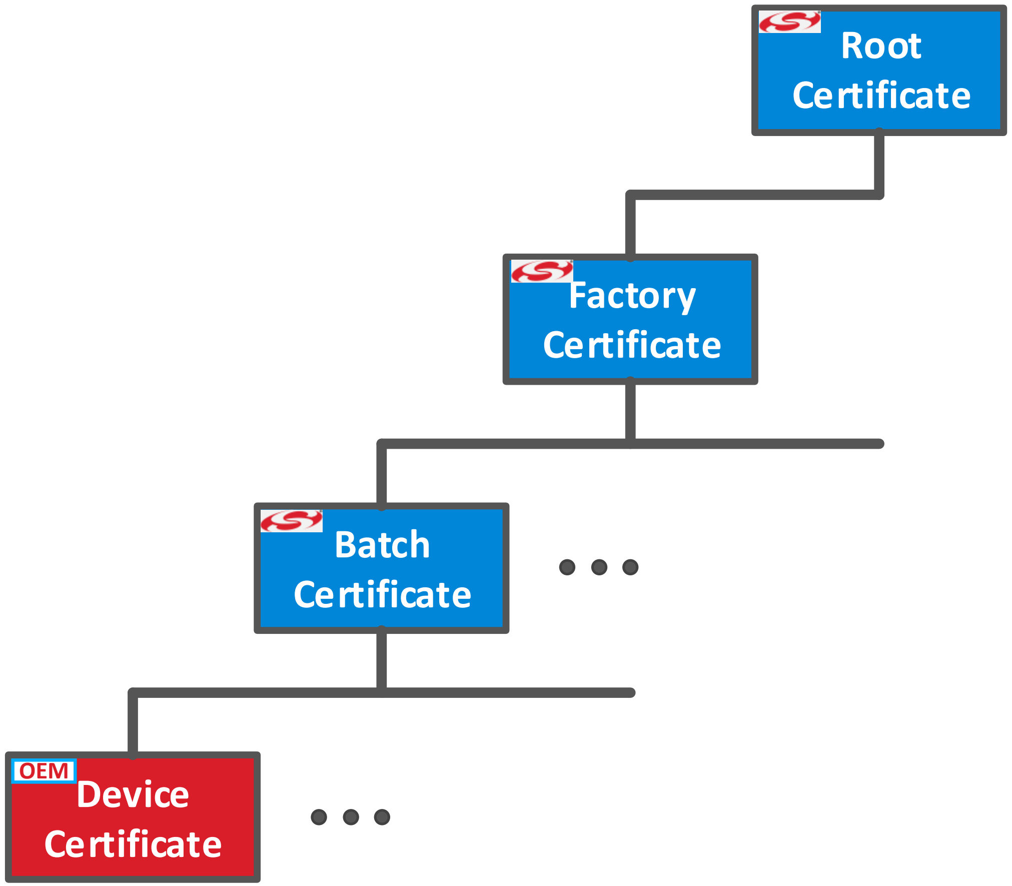
- A certificate chain is a hierarchy
  - Each certificate in the chain is signed by the certificate above it
  - Each certificate in the chain has a pointer to the certificate above it
- Silicon Labs is a Certificate Authority
  - All private keys are Silicon Labs private keys that are held in our secure Public Key Infrastructure or are securely stored in the devices themselves
  - https://ca.silabs.com
    - Contains Factory Certificate, Root Certificate, and Certificate Revocation Lists
- All certificates are X.509, signed with NIST secp256r1 elliptic curve private keys
  - Fully compatible with standard endpoint authentication methods used in internet communications

Standard Secure Vault Device Certificates



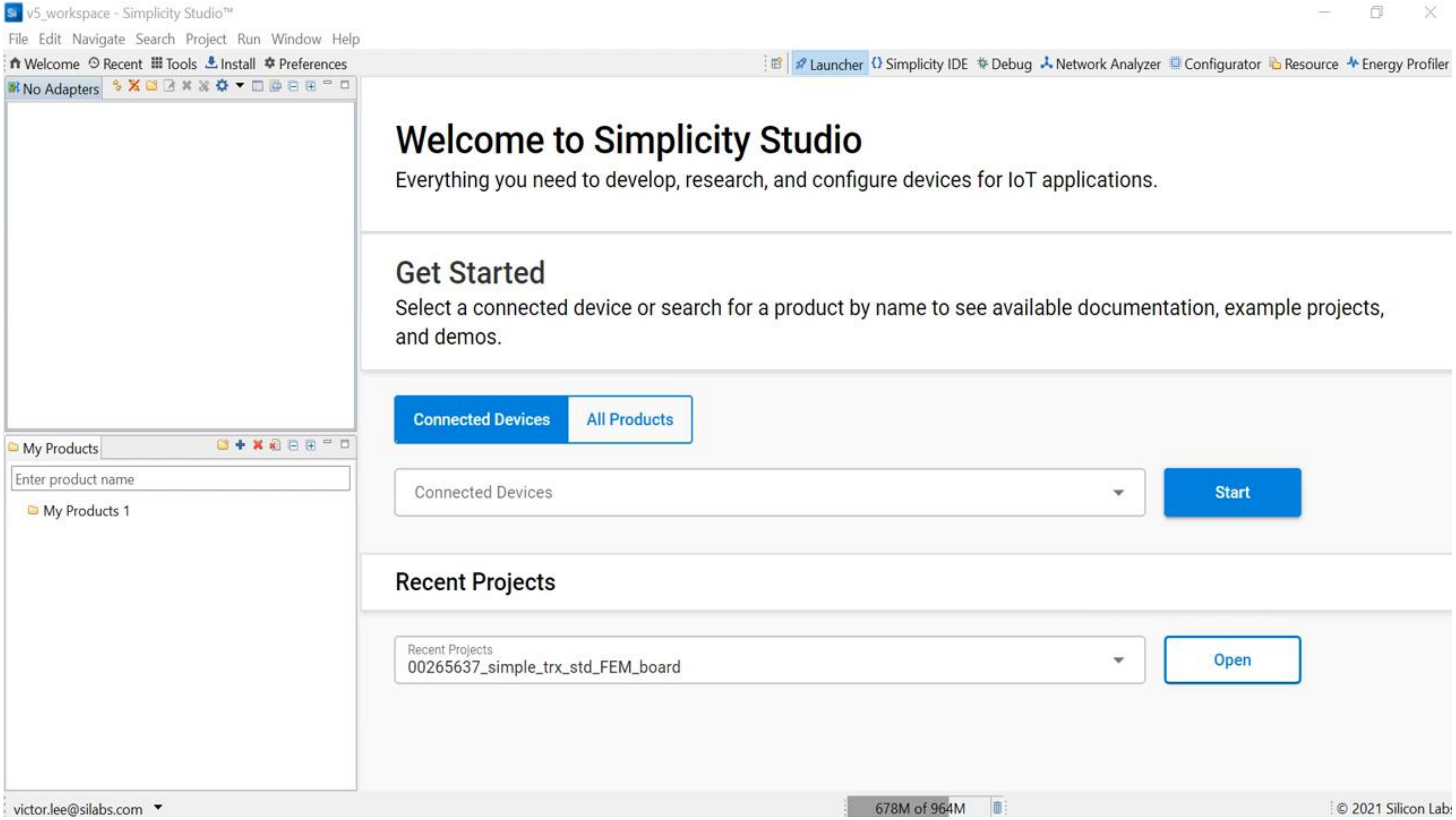
- Standard Device Certificates
  - Included with Secure Vault products
  - Can be added to non-Vault products with a customization charge
  - Cryptographically proves the device is an authentic Silicon Labs device (**prevents counterfeit devices**)
  - **Does not** protect against overproduction or counterfeit products that are built with authentic Silicon Labs devices
  - Signed to a Silicon Labs Certificate Authority

Customized Secure Vault Device Certificates



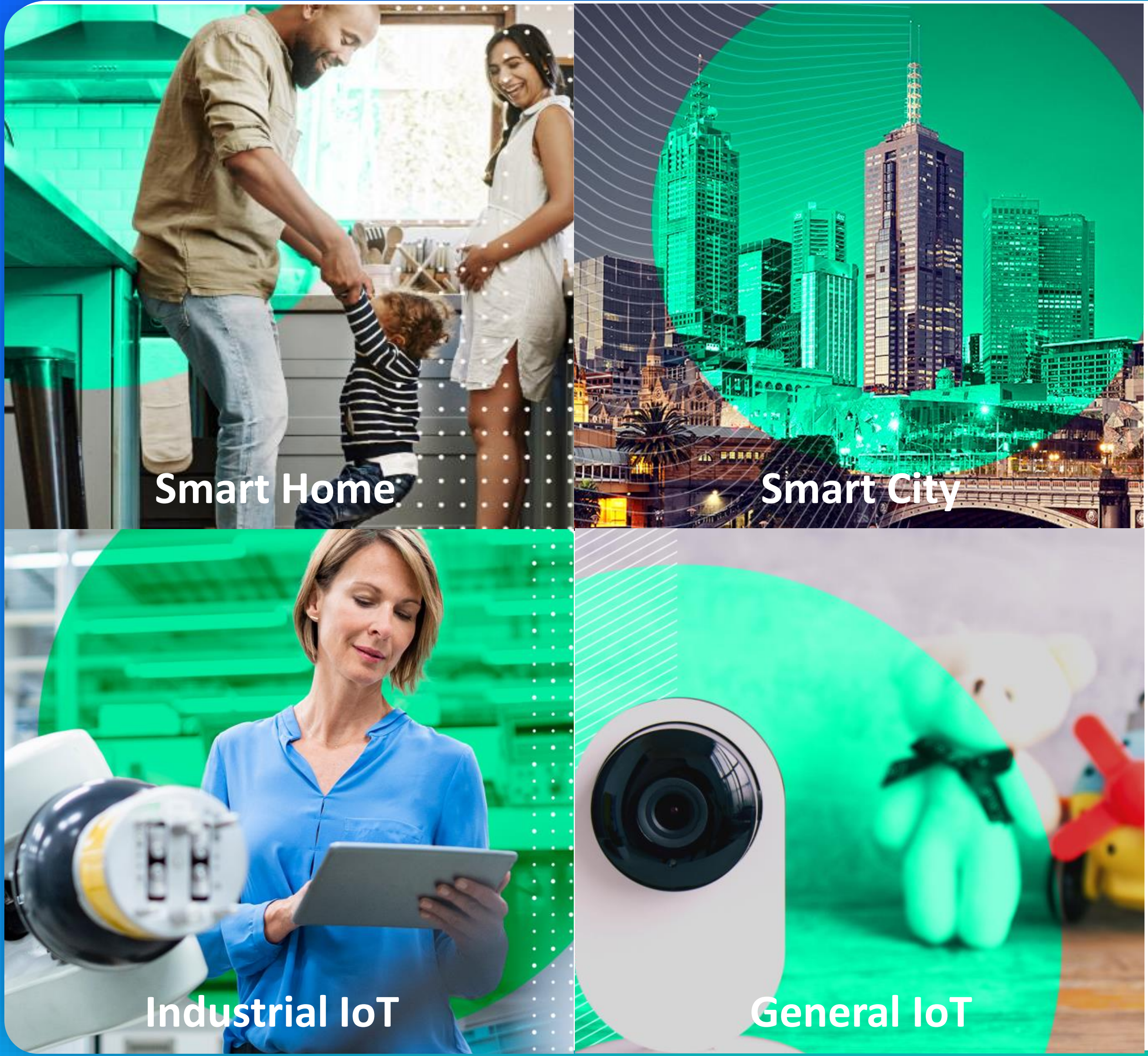
- Customized Device Certificates
  - Available via Custom Part Manufacturing Service (CPMS)
  - Protects against **overproduction** by CM
  - Protects against **counterfeit products**
  - Cryptographically proves the device is an authentic Silicon Labs device that was produced for the OEM
  - Device Certificate X.509 fields can be specified, with restrictions
  - Signed to Silicon Labs Certificate Authority

Secure Identity Demo


v5_workspace - Simplicity Studio™
File Edit Navigate Search Project Run Window Help
Welcome Recent Tools Install Preferences
Launcher Simplicity IDE Debug Network Analyzer Configurator Resource Energy Profiler
No Adapters
My Products
Enter product name
My Products 1
Welcome to Simplicity Studio
Everything you need to develop, research, and configure devices for IoT applications.
Get Started
Select a connected device or search for a product by name to see available documentation, example projects, and demos.
Connected Devices
All Products
Connected Devices
Start
Recent Projects
Recent Projects
00265637_simple_trx_std_FEM_board
Open
victor.lee@silabs.com
678M of 964M
© 2021 Silicon Labs

Support Documentation

- AN1190: Series 2 Secure Debug
- AN1218: Series 2 Secure Boot with RTSL
- AN1247: Anti-Tamper Protection Configuration and Use
- AN1271: Secure Key Storage
- AN1268: Authenticating Silicon Labs Devices Using Device Certificates
- AN1222: Production Programming of Series 2 Devices
- UG162: Simplicity Commander Reference Guide
- UG266: Silicon Labs Gecko Bootloader User’s Guide



works with
BY SILICON LABS

VIRTUAL CONFERENCE

September 14–15, 2021 (CDT)

Works With 2021 Virtual Conference

workswith.silabs.com

Q&A

Facebook	Twitter	Community

SILICON LABS

tech talks

THANK YOU

Recording and slides will be posted to:
www.silabs.com/training