works with
BY SILICON LABS
VIRTUAL CONFERENCE

SILICON LABS

SEC – 102: Enforced Security Regulations will Demand a Security Warranty in IoT Devices

“Zero Trust” Model requires continuous Authentication (The Passport Example)

- **Example of authentication with a passport**
  - Start by giving the official your passport
  - Is the passport authentic (or counterfeit)?
  - Is the passport related to this you (or someone else)?

What is a Secure Identity for an IoT Device?

- **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 that a component 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

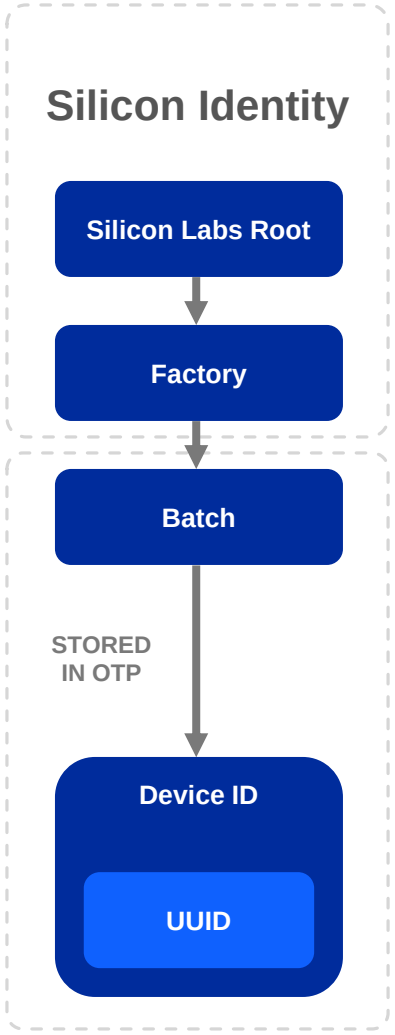
Government Regulations are Requiring Secure Identities

NISTIR 8259A

IoT Device Cybersecurity Capability Core Baseline

Concern	Federal Requirement
Device Identification **(Secure Identity)**	The IoT device can be uniquely identified logically and physically.
Device Configuration **(Secure OTA Updates)**	The IoT device's software and firmware configuration can be changed, and such changes can be performed by authorized entities only.
Data Protection	The IoT device can protect the data it stores and transmits from unauthorized access and modification.
Logical Access to Interfaces **(Secure Debug)**	The IoT device can limit logical access to its local and network interfaces to authorized entities only.
Software and Firmware Update **(Secure Boot)**	The IoT device's software and firmware can be updated by authorized entities only using a secure and configurable mechanism.
Cybersecurity Event Logging	The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.

Communication Protocols are moving to Certificate Chains to Provide Secure Identities



Microsoft Azure

AWS IoT

amazon sidewalk

matter

Wi SUN

IBM Watson

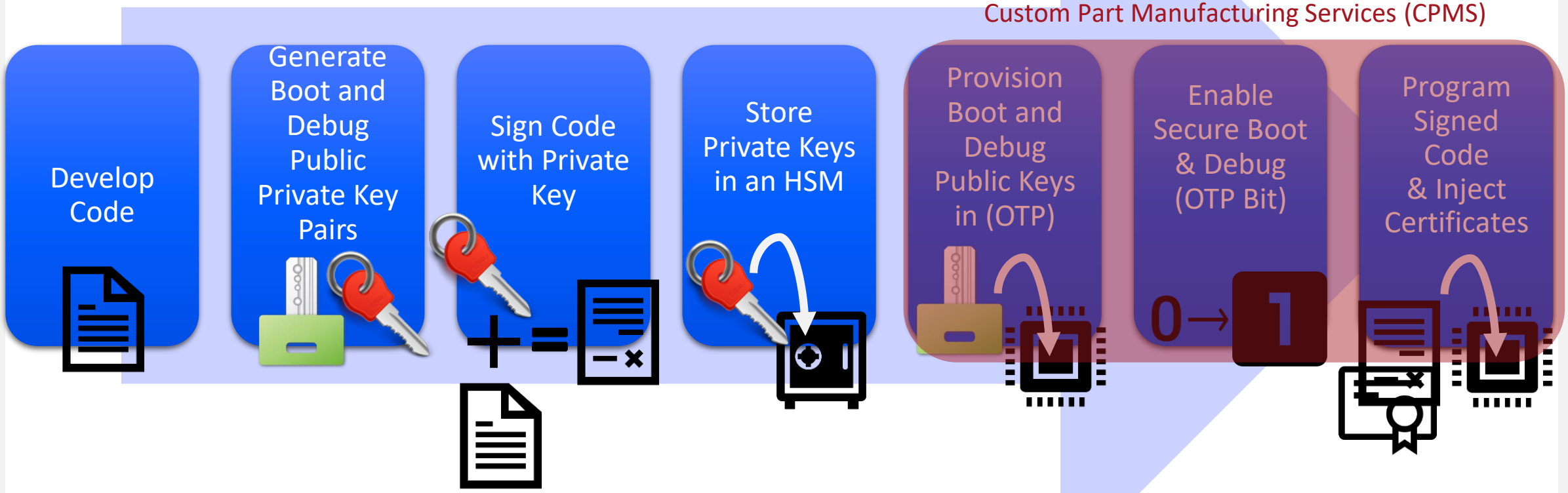
Use Case - Mutual App and Device Authentication using Public Key Certificates

- **Protects against counterfeit products and malicious apps**
- **An example of a Smartphone authenticating a Device**
  - Start by providing the certificate
  - Is the certificate authentic?
  - Is the certificate related to this device?
- **An example of a Device authenticating a Smartphone application or user**
  - Start by providing the certificate
  - Is the certificate authentic?
  - Is the certificate related to this app or user?

IoT Device Development and Manufacturing will be Changed Forever

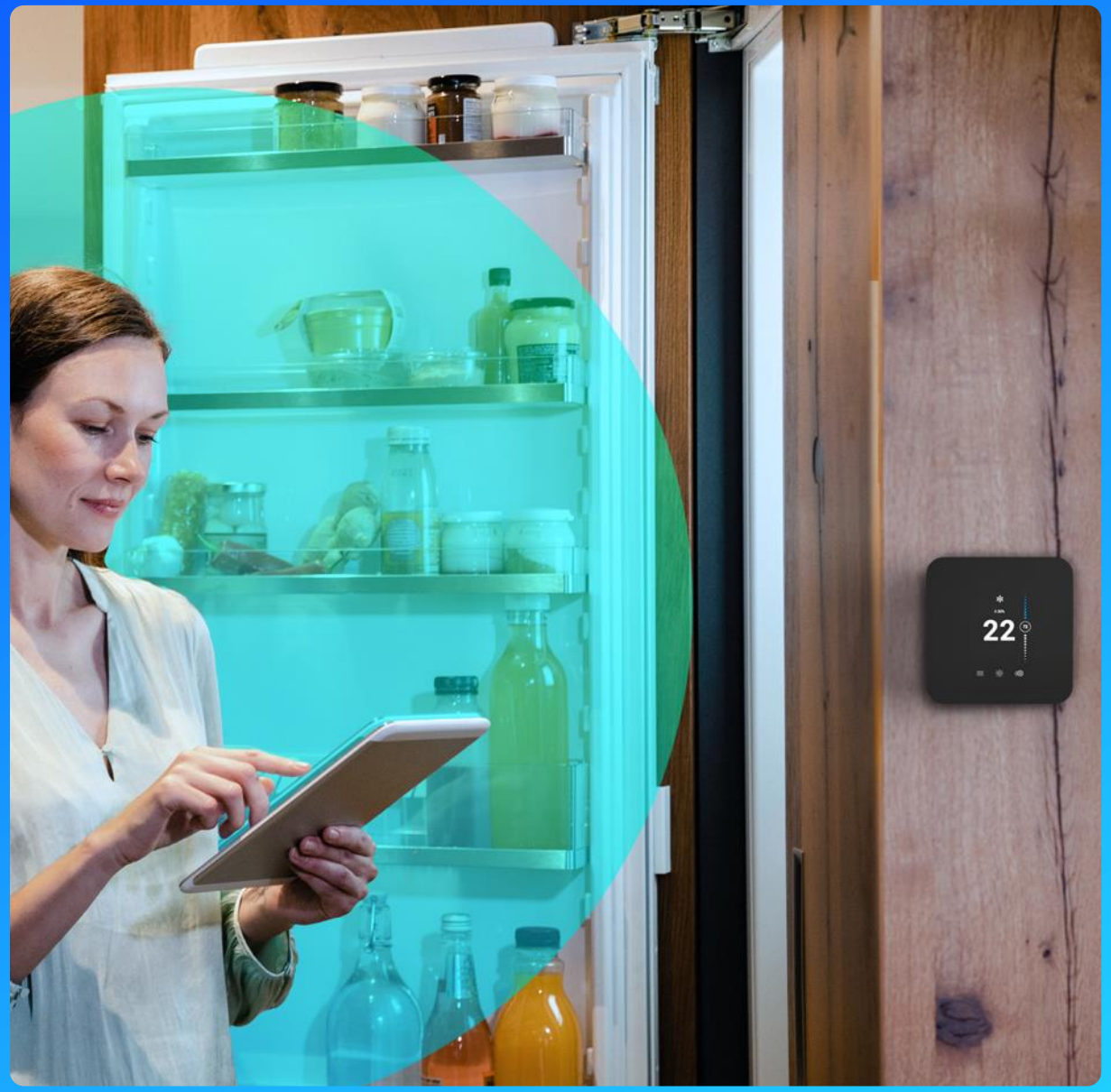
PiP Placeholder Window
(Remove Before Distribution)

Developer Journey



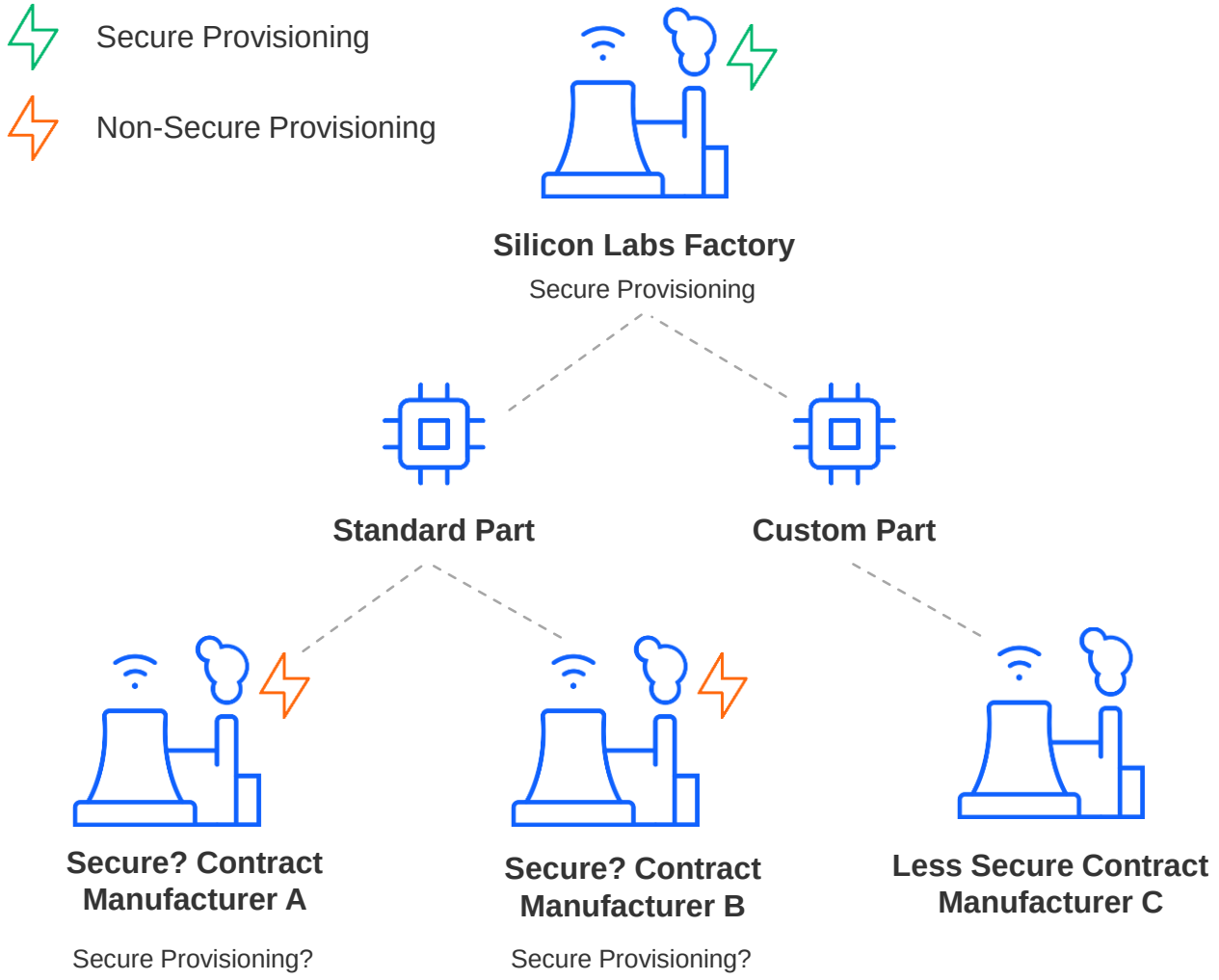
CPMS

Custom **P**art **M**anufacturing **S**ervice



Custom Part Manufacturing Service (CPMS) Secure Provisioning… not just programming!

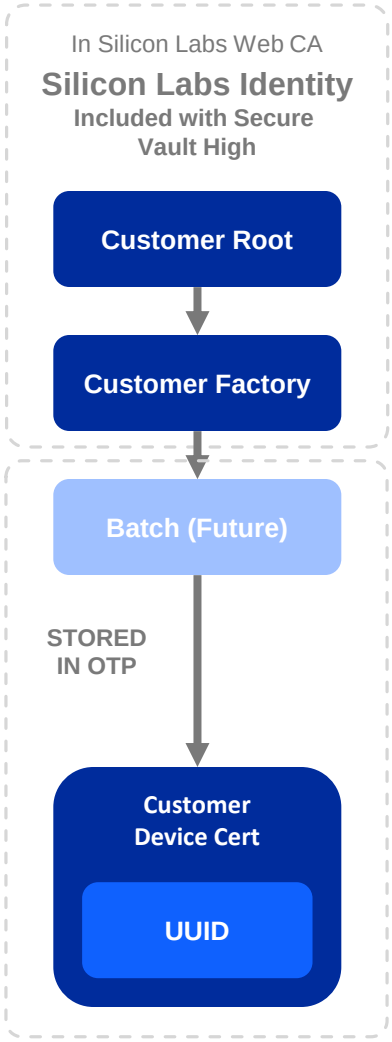
PiP Placeholder Window
(Remove Before Distribution)



- Available for Series 1 and Series 2 EFRx parts
- Easy to use web user interface
- receive 10 samples within 4 weeks for $500 flat fee
- User Private/Public Key Injection
- Security Settings:
  - Secure Debug Locked
  - Secure Boot Enable
  - Tamper Options Set
  - Anti-rollback Set
- Bootloader pre-flashed for protection of Software IP
- Secure Identity (Certificates) Injection
- Flash Programming

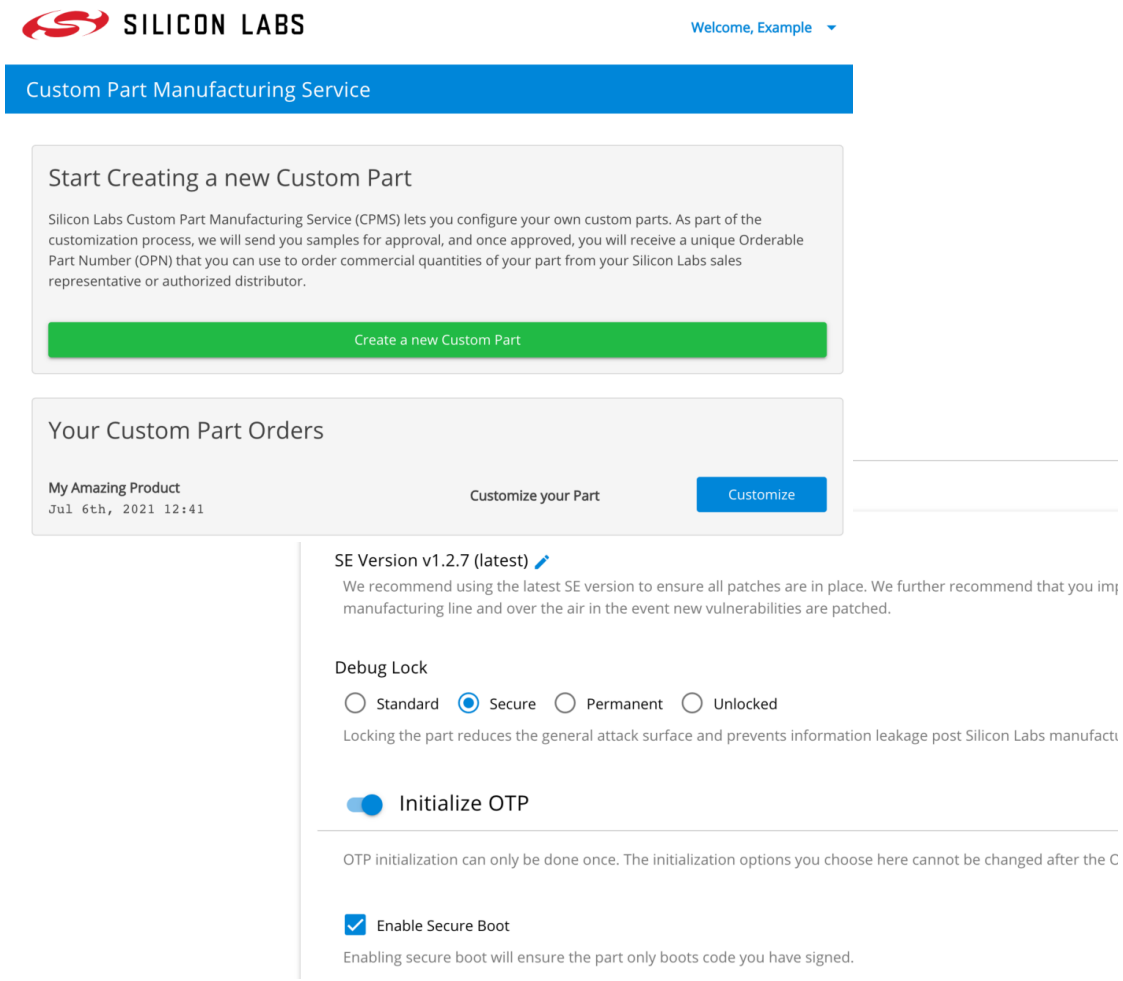
Value Add of Secure Provisioning from Silicon Labs

PiP Placeholder Window
(Remove Before Distribution)



- **Easier/Simpler – This is Security Provisioning not just programming flash**
  - You already are doing business with us
  - We know how to set the security selections and have FAEs that can help set them properly (otherwise you must learn and then teach a third part)
- **More cost effective as we are already programming the chip**
- **More secure and flexible supply chain**
  - Custom part shipments can be tracked to CM (prevents over production)
  - Can use lower cost CMs with less security infrastructure
  - Easily allows second or third source CMs
- **Dynamic content like certificates are hard to do**
  - Must be secure
  - Must be cost effective
  - Not likely a standard programming house will be able to execute
- **We welcome customization of certificates**
  - Standard certs on Vault High devices
  - Customize certificate content
  - Customize certificate root

Easy to Use Web Interface

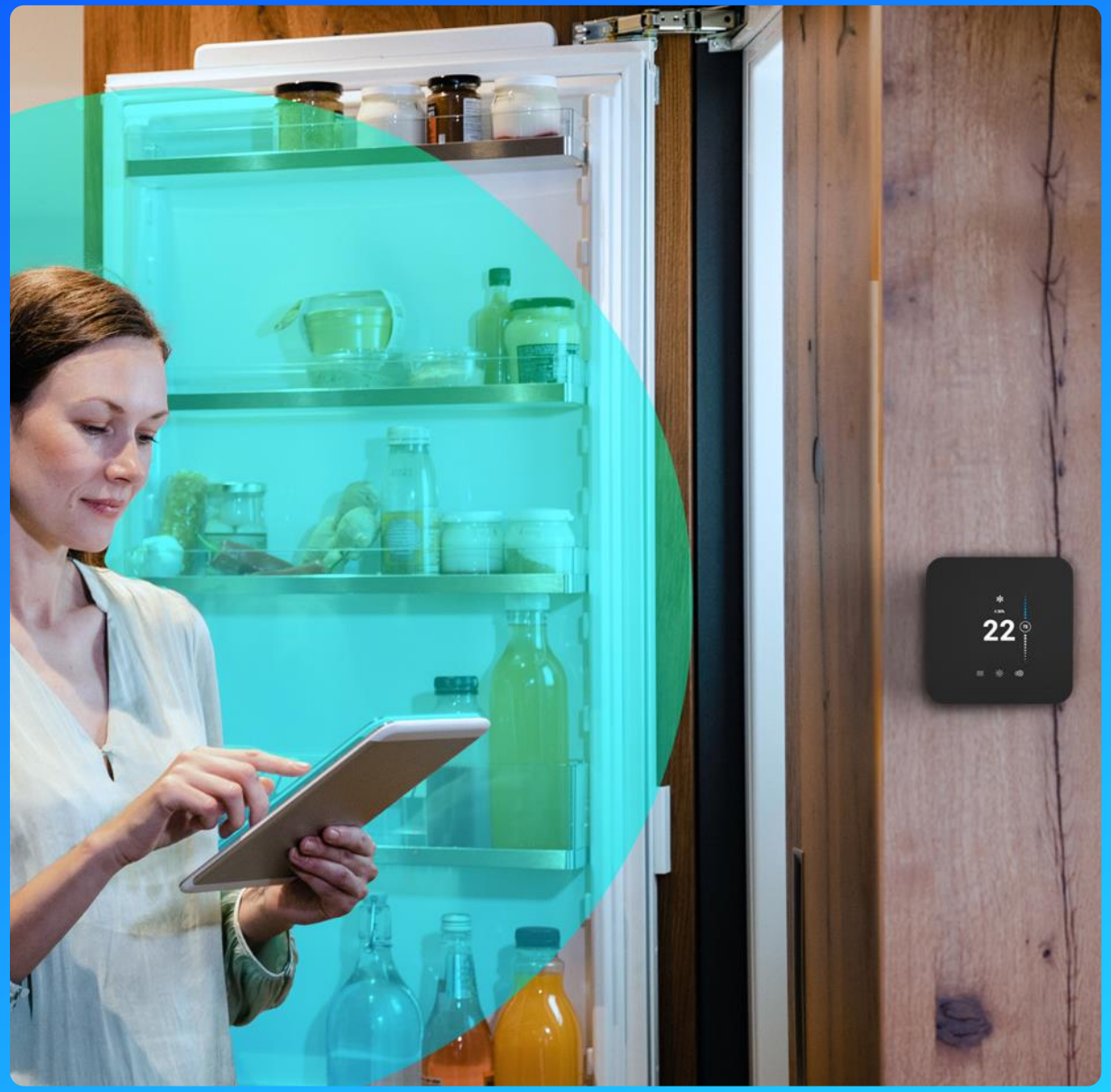


STEPS

1. Pick base part
2. Select Secure Engine Firmware Version
3. Select Debug Configuration
4. Enable Secure Boot, Anti-rollback, Flash Page Locking
5. Set Tamper Response
6. Enter Keys: Secure Boot and Debug Public Keys, OTA Decryption Key, and Customer specific keys
7. Download Flash Image
8. Optionally Request Customization of Certificates or Markings

LTSSS

Long **T**erm **S**DK **S**upport **S**ervice



Government Regulations are Requiring Continuous Security Updates for Life of the Product

PiP Placeholder Window
(Remove Before Distribution)

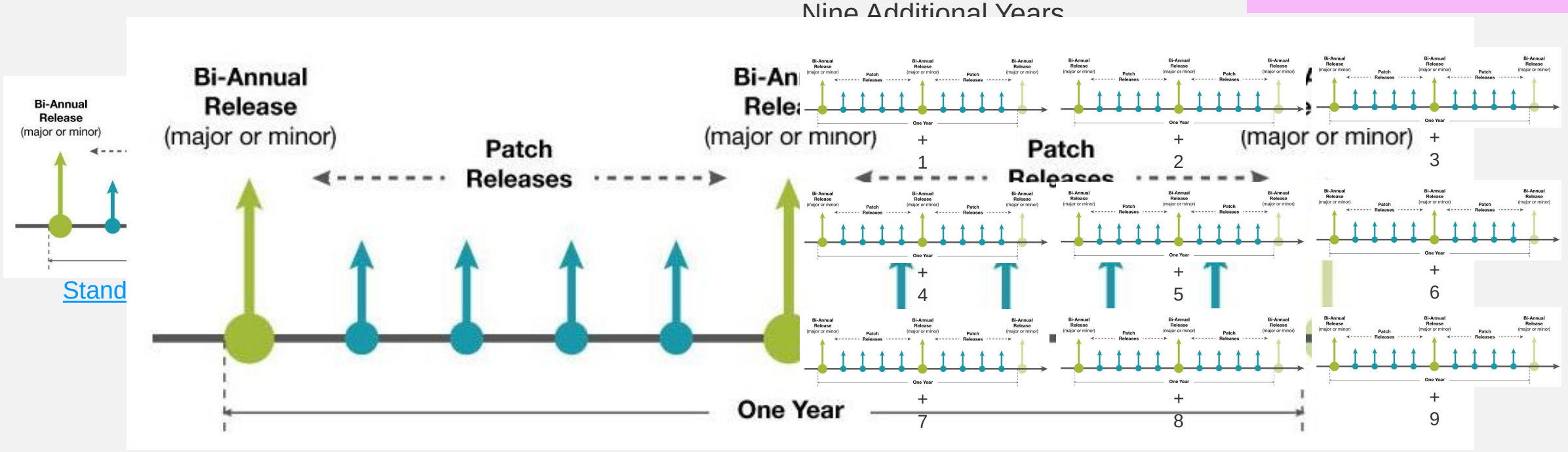
NISTIR 8259A

IoT Device Cybersecurity Capability Core Baseline

Concern	Federal Requirement
Device Identification **(Secure Identity)**	The IoT device can be uniquely identified logically and physically.
Device Configuration **(Secure OTA Updates)**	The IoT device's software and firmware configuration can be changed, and such changes can be performed by authorized entities only.
Data Protection	The IoT device can protect the data it stores and transmits from unauthorized access and modification.
Logical Access to Interfaces **(Secure Debug)**	The IoT device can limit logical access to its local and network interfaces to authorized entities only.
Software and Firmware Update **(Secure Boot)**	The IoT device's software and firmware can be updated by authorized entities only using a secure and configurable mechanism.
Cybersecurity Event Logging	The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.

Long Term SDK Support Service (LTSSS)

PiP Placeholder Window
(Remove Before Distribution)



Stand

- **10-year guaranteed support for SDK branch under contract[1]**
- **Only security patches and major bug fixes[2] to preserve investment in certifications**
- **Discount price for multiple SDKs supported**

Standard Complimentary Software Longevity Policy

1 - approximately two SDK releases will be available for contract per year
2 – as determined by Silicon Labs processes

works with | SILICON LABS

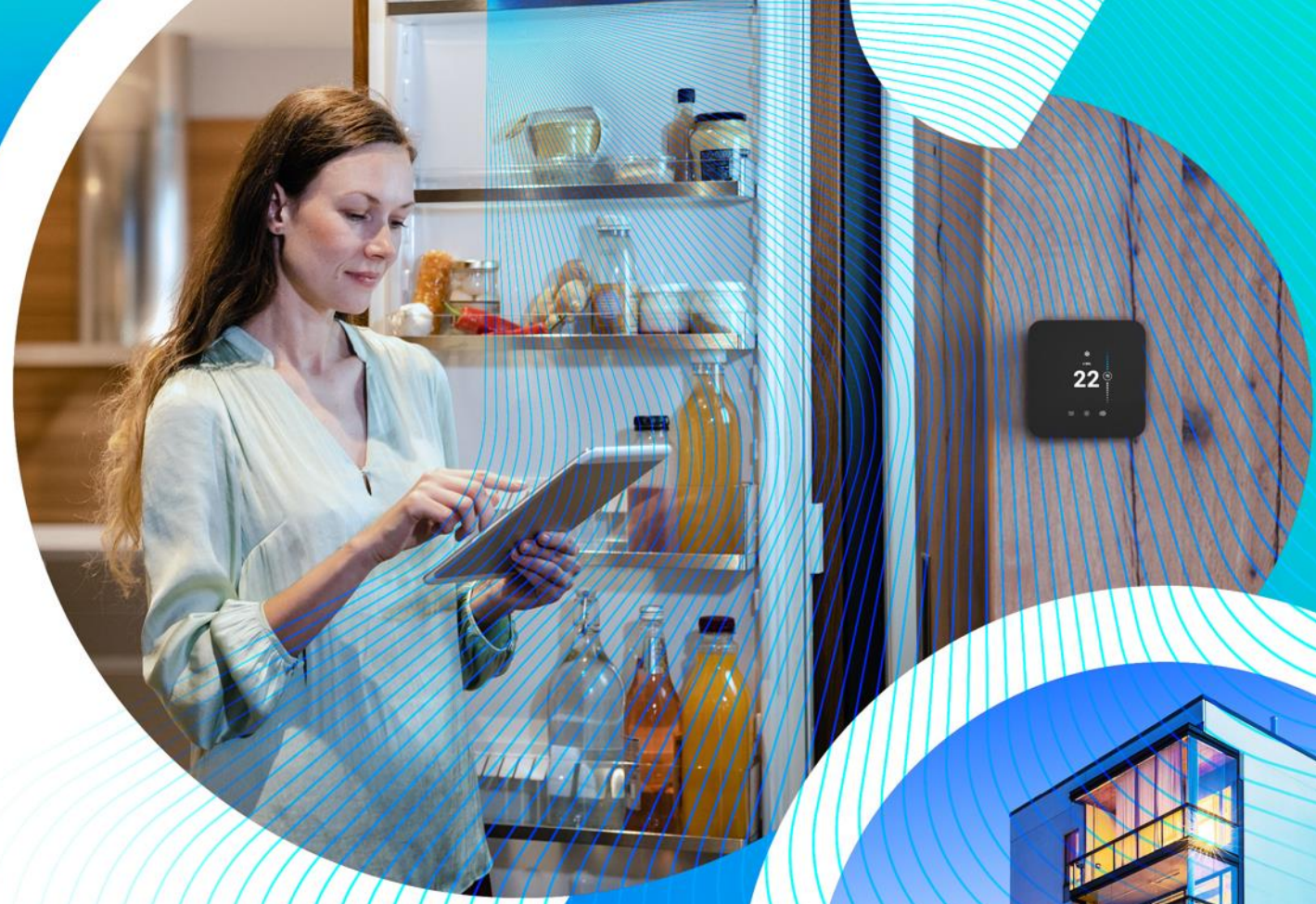
Related Security Focused Works With Sessions

PiP Placeholder Window
(Remove Before Distribution)

- **Works With Sessions**
  - SEC-101: Security Regulation and How it will Drive Innovation in IoT
  - SEC-201: Applying Security to Verify Deployed Products are Authentic
  - SEC-301: Hands on Security
  - SEC-PNL: Smart Home Security and the User Experience

works with
BY SILICON LABS

VIRTUAL CONFERENCE



SILICON LABS