

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

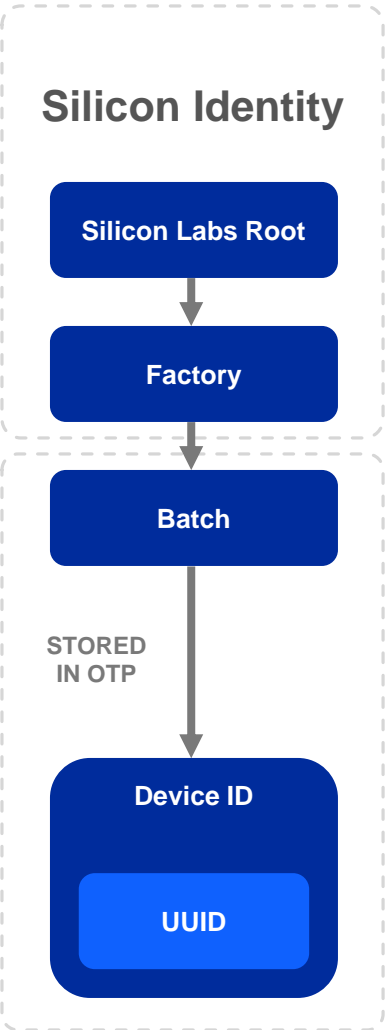


NISTIR 8259A

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



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

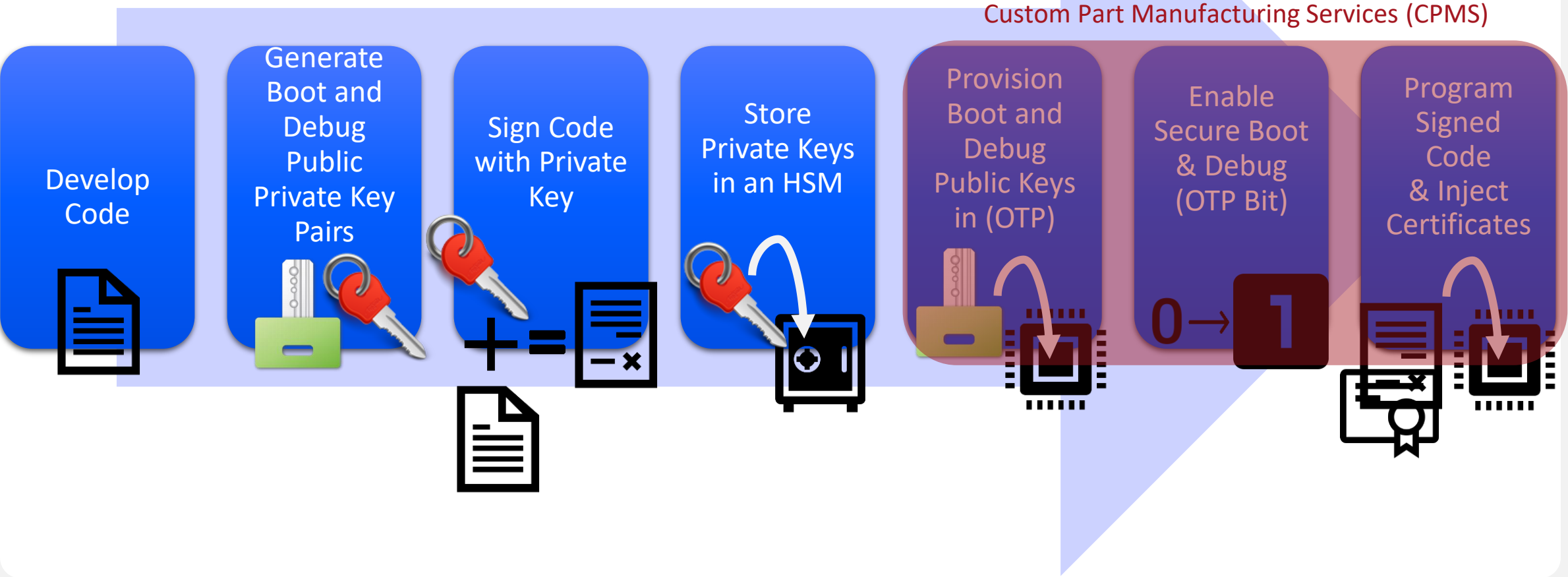


- **Protects against counterfeit products and malicious apps**
- **An example of a Smartphone authenticating a Device**
 - Start by providing the certificate
 - Is the certificate authentic?
 - Is the certificate related to this device?
- **An example of a Device authenticating a Smartphone application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

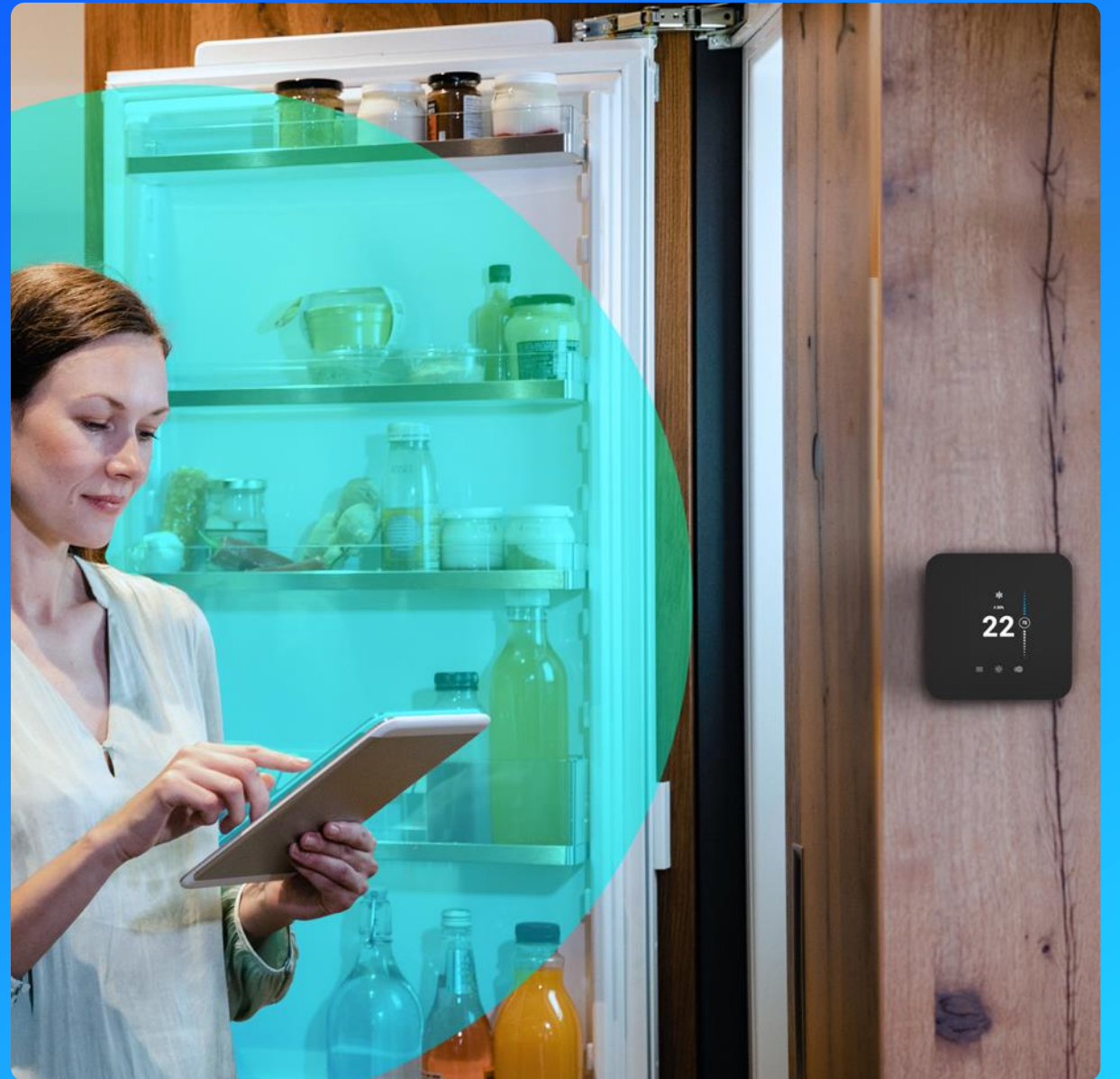
PiP Placeholder
Window
*(Remove Before
Distribution)*

Developer Journey



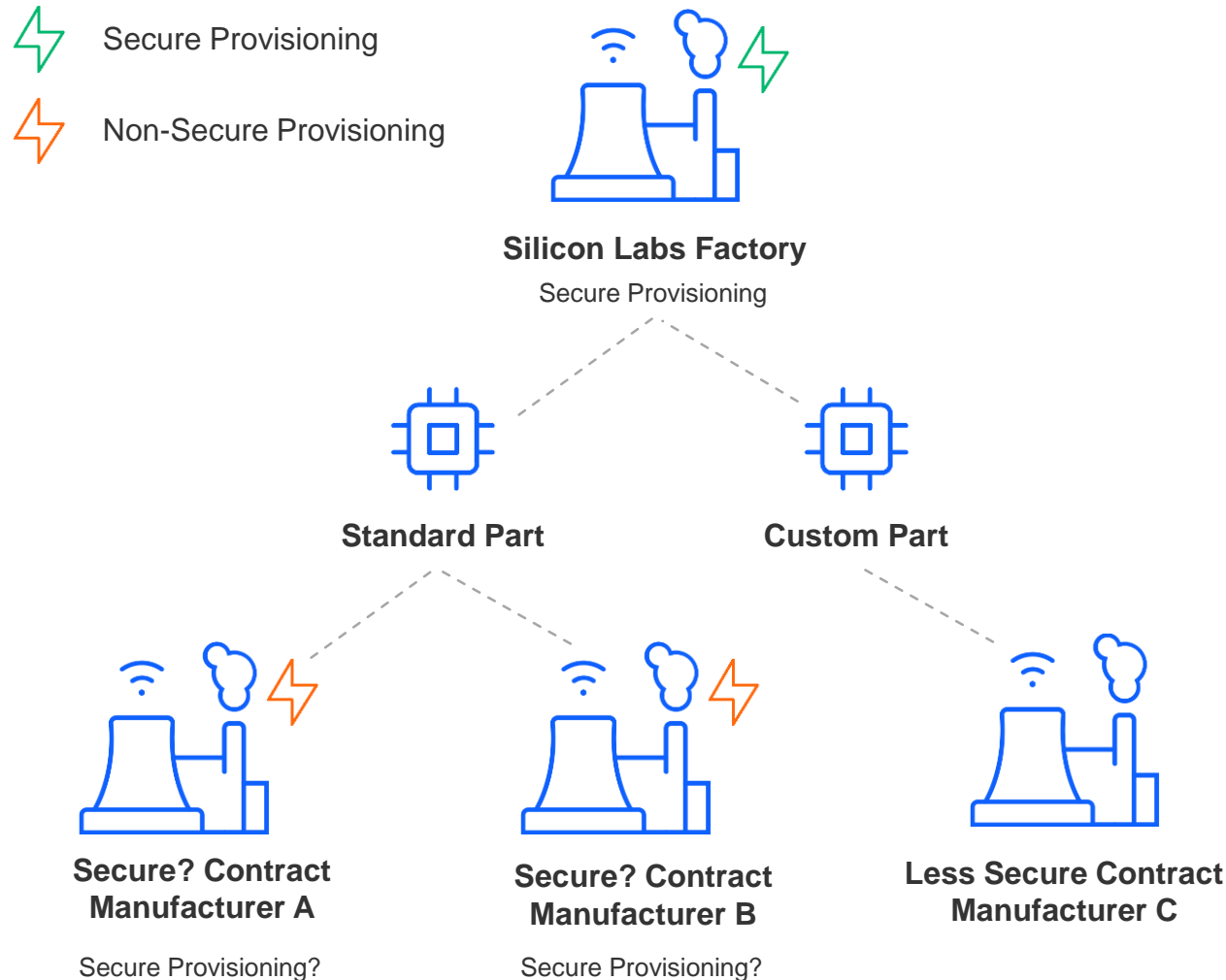
CPMS

Custom Part Manufacturing Service



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

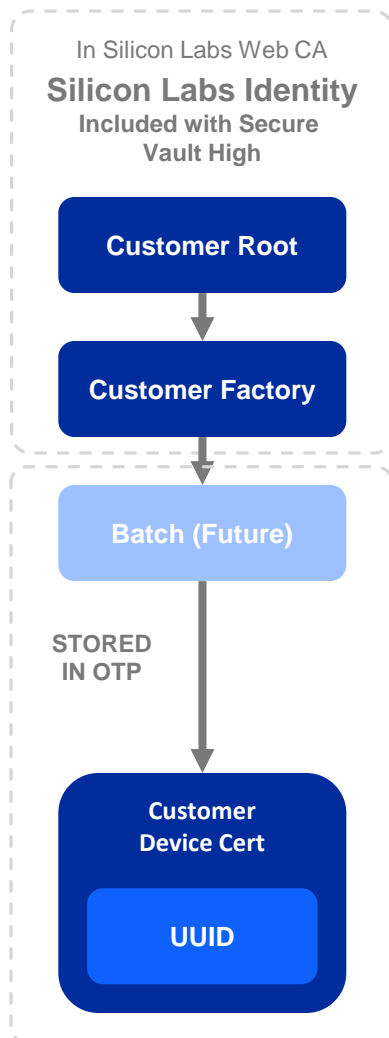
PiP Placeholder
Window
(Remove Before
Distribution)



- 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

The screenshot shows the Silicon Labs Custom Part Manufacturing Service (CPMS) web interface. At the top, the Silicon Labs logo is on the left, and a user greeting 'Welcome, Example' is on the right. Below the logo is a blue header bar with the text 'Custom Part Manufacturing Service'. The main content area is divided into two sections. The first section, 'Start Creating a new Custom Part', contains a paragraph explaining the CPMS process and a green button labeled 'Create a new Custom Part'. The second section, 'Your Custom Part Orders', shows a table with one order: 'My Amazing Product' with a timestamp 'Jul 6th, 2021 12:41'. To the right of the table is a 'Customize your Part' button. Below the table, there are configuration options: 'SE Version v1.2.7 (latest)' with a link icon, a recommendation paragraph, 'Debug Lock' with radio buttons for 'Standard', 'Secure' (selected), 'Permanent', and 'Unlocked', and a paragraph explaining the lock. Below that is a toggle switch for 'Initialize OTP' which is turned on, followed by a paragraph explaining that OTP initialization is a one-time process. At the bottom, there is a checked checkbox for 'Enable Secure Boot' and a paragraph explaining its function.

SILICON LABS Welcome, Example

Custom Part Manufacturing Service

Start Creating a new Custom Part

Silicon Labs Custom Part Manufacturing Service (CPMS) lets you configure your own custom parts. As part of the customization process, we will send you samples for approval, and once approved, you will receive a unique Orderable Part Number (OPN) that you can use to order commercial quantities of your part from your Silicon Labs sales representative or authorized distributor.

Create a new Custom Part

Your Custom Part Orders

My Amazing Product Jul 6th, 2021 12:41	Customize your Part	Customize
---	---------------------	-----------

SE Version v1.2.7 (latest) [🔗](#)

We recommend using the latest SE version to ensure all patches are in place. We further recommend that you im[...]
manufacturing line and over the air in the event new vulnerabilities are patched.

Debug Lock

☐ Standard ☒ Secure ☐ Permanent ☐ Unlocked

Locking the part reduces the general attack surface and prevents information leakage post Silicon Labs manufactu[...]

☒ Initialize OTP

OTP initialization can only be done once. The initialization options you choose here cannot be changed after the C[...]

☒ Enable Secure Boot

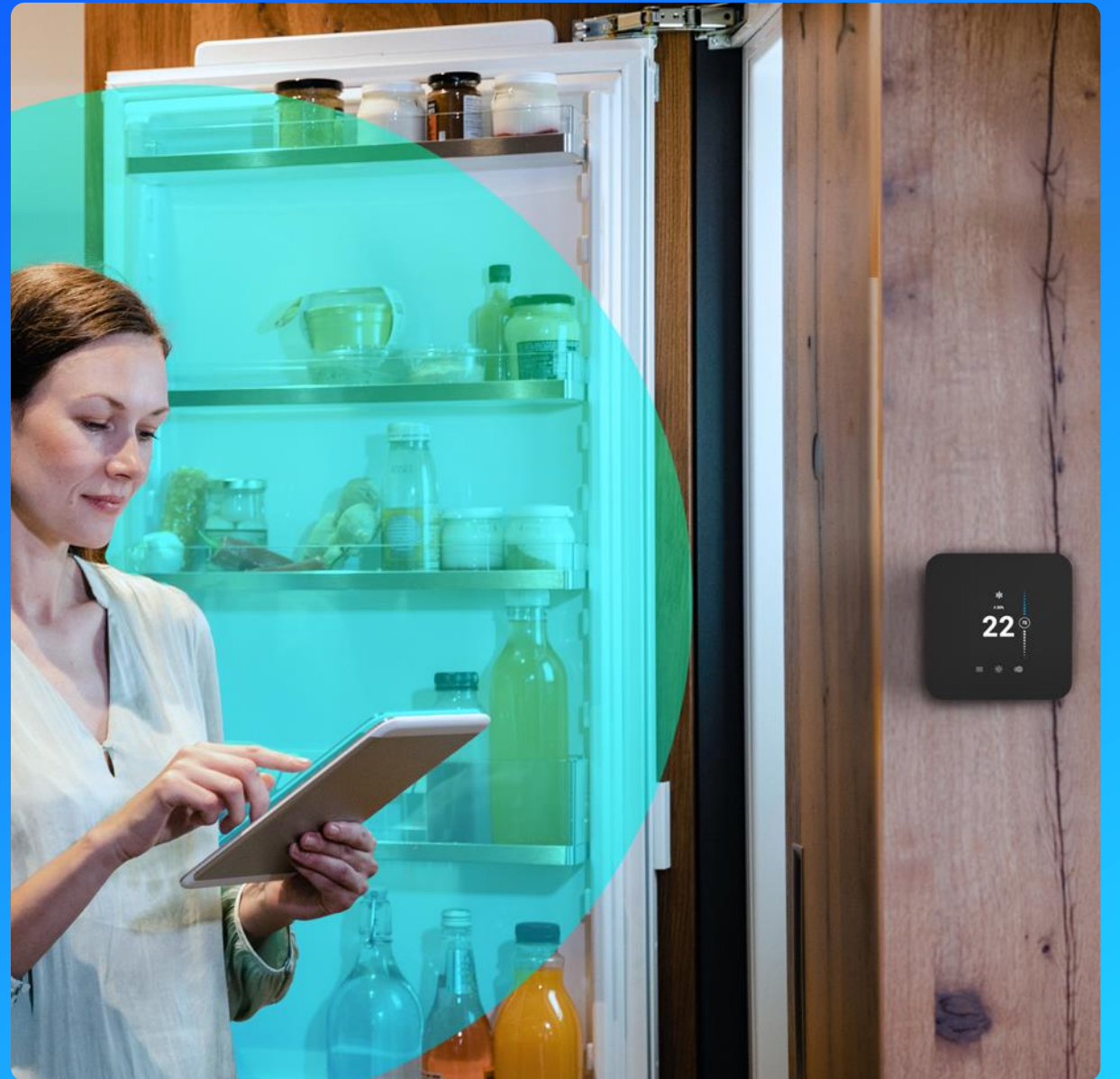
Enabling secure boot will ensure the part only boots code you have signed.

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 Term SDK Support Service



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

PiP Placeholder
Window
(Remove Before
Distribution)



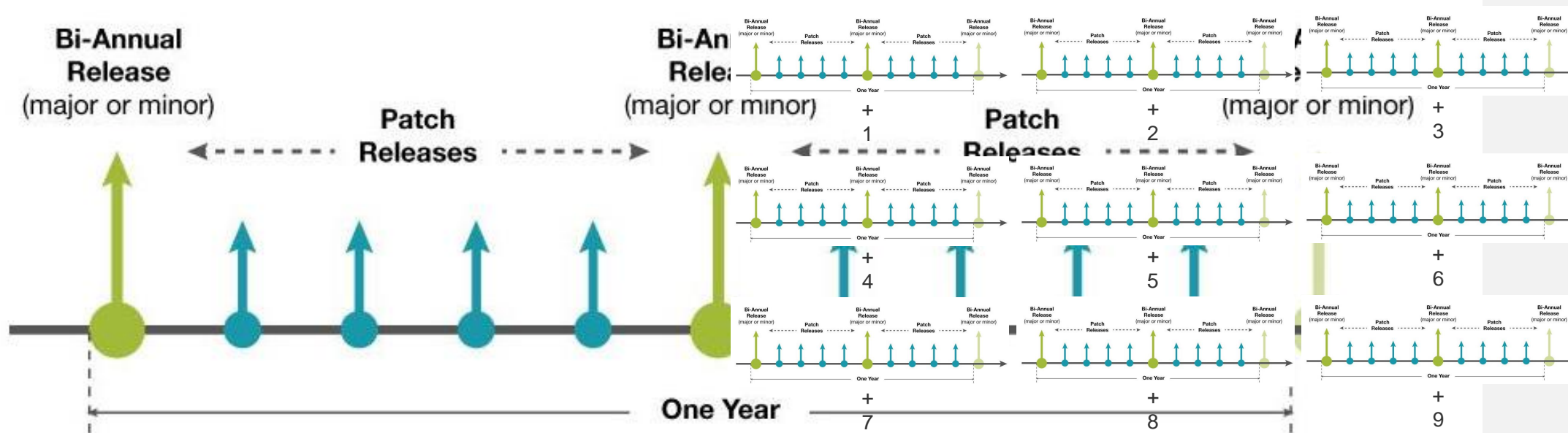
NISTIR 8259A
IoT Device Cybersecurity Capability
Core Baseline

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.

Bi-Annual Release
(major or minor)

The diagram shows a horizontal line with two vertical dashed lines indicating time intervals. A large green circle is positioned on the line, with a large green arrow pointing upwards from it. A smaller blue circle is positioned further to the right on the line, with a smaller blue arrow pointing upwards from it. A horizontal arrow points from the right towards the green circle.

Stand



- **10-year guaranteed support for SDK branch under contract¹**
[Standard Complimentary Software Longevity Policy](#)
- **Only security patches and major bug fixes² to preserve investment in certifications**
- **Discount price for multiple SDKs supported**

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

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

