

SEC – 101: Security Regulation and How it will Drive Innovation in IoT



Silicon Labs Announces New Security Services



- **Custom Part Programming Service (CPMS) for security provisioning**
- **Long Term SDK Support Service (LTSSS)**
- **Be sure to attend SEC-102: Enforced Security Regulations will Demand a Security Warranty in IoT Devices for more details**

Regulation at the US National Level is Accelerating

IoT Cybersecurity Act of 2020

FCW The Business of Federal Technology
People IT Modernization Digital Government Security Acquisition Workforce Events Resources Subscribe


[Advertisement]

CONGRESS

SHARE... E-MAIL THIS PAGE PRINTABLE FORMAT

Senate passes IoT cybersecurity bill

By Justin Katz | Nov 18, 2020



The Senate yesterday by unanimous consent passed legislation to mandate certain security requirements for internet of things devices purchased by the federal government, moving forward legislation that had been stalled on Capitol Hill since 2017.

Cyber Shield Act

COVINGTON

HOME

AUDIOCAS

Inside Privacy

Updates on developments in data privacy and cybersecurity

FROM COVINGTON & BURLING LLP

HOME > CYBERSECURITY > "CYBER SHIELD ACT" CALLING FOR IOT DEVICE CERTIFICATION REINTRODUCED IN CONGRESS

"Cyber Shield Act" Calling for IoT Device Certification Reintroduced in Congress

By Micaela McMurrough, Jayne Ponder and Julia Oksasoglu on March 26, 2021

POSTED IN CONGRESS, CYBERSECURITY

Sen. Ed Markey (D-MA) and Rep. Ted Lieu (D-CA-33) **reintroduced** the Cyber Shield Act on March 24, 2021. The proposed legislation is not new to Congress; Sen. Markey and Rep. Lieu previously introduced the Cyber Shield Act in both **2017** and **2019**. However, the bill never made it to a vote in either the House or the Senate.

As written, the Cyber Shield Act calls for the creation of a voluntary cybersecurity certification program for Internet of Things (IoT) devices. IoT devices span a **wide**

May 2021

President Biden Executive Order on improving the Nation's Cybersecurity



BRIEFING ROOM

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

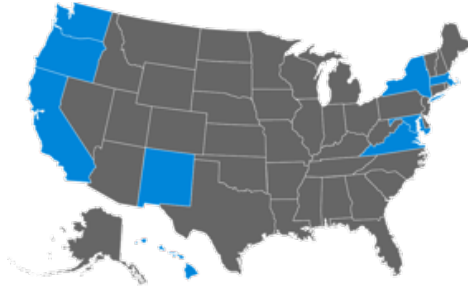
By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the

(t) Within 270 days of the date of this order, the Secretary of Commerce acting through the Director of NIST, in coordination with the Chair of the Federal Trade Commission (FTC) and representatives of other agencies as the Director of NIST deems appropriate, shall identify IoT cybersecurity criteria for a consumer labeling program, and shall consider whether such a

consumer labeling program may be operated in conjunction with or modeled after any similar existing government programs consistent with applicable law. The criteria shall reflect increasingly comprehensive levels of testing and assessment that a product may have undergone, and shall use or be compatible with existing labeling schemes that manufacturers use to inform consumers about the security of their products. The Director of NIST shall examine all relevant information, labeling, and incentive programs and employ best practices. This review shall focus on ease of use for consumers and a determination of what measures can be taken to maximize manufacturer participation.

IoT Security Legislation... States are the first movers



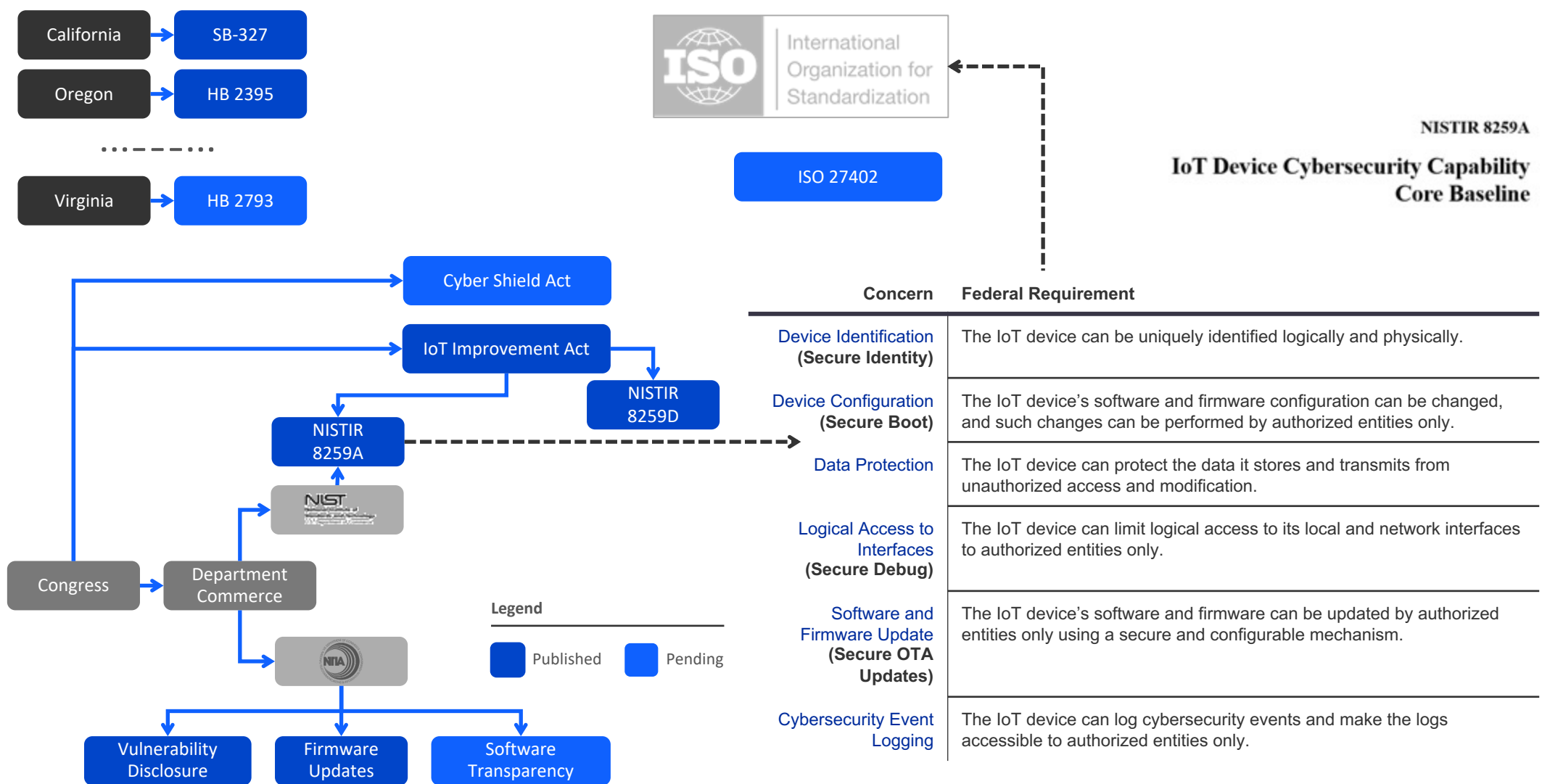
Multiple states have already introduced bills that resemble California's CCPA example

Virginia	(HB 2793)
Oregon	(HB 2395)
Hawaii	(SB 418)
Maryland	(SB 0613)
Massachusetts	(SD 341)
New Mexico	(SB 176)
New York	(S00224)
Rhode Island	(SB 234)
Washington	(SB 5376)

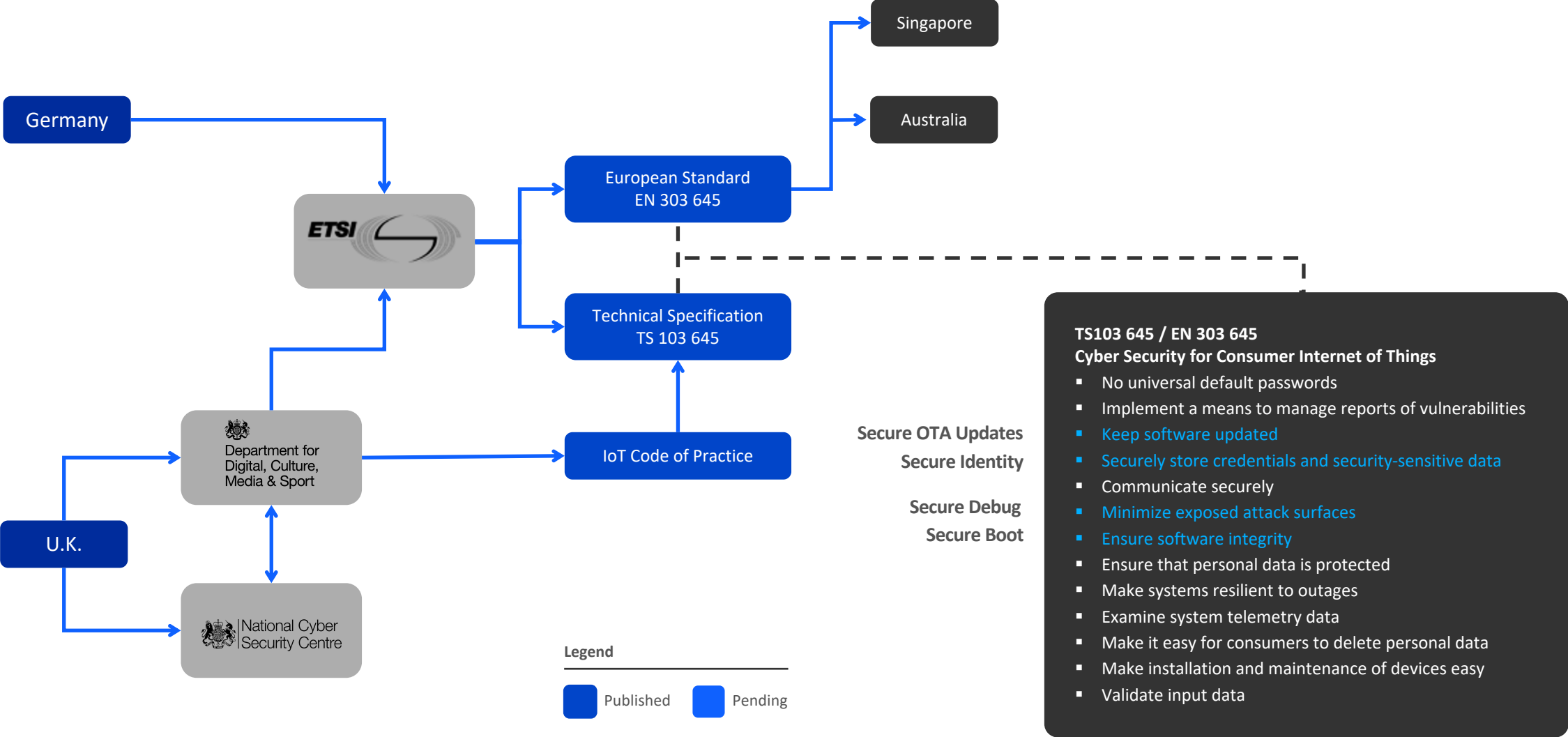
- **California Consumer Privacy Act (§ SB-327)**
 - Introduced Feb 13, 2017
 - Approved Sept 28, 2018
 - **Effective Jan 1, 2020 (<3yrs)**
- **Requires 'reasonable security features'**
 - appropriate to the nature and function of the device
 - appropriate to the information it may collect, contain, or transmit
 - **designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure**
 - Pre-programmed passwords are unique in each device manufactured

Already accounts for ~30% US population

Governmental Regulatory Landscape – United States



Governmental Regulatory Landscape – Europe



Challenging Landscape for Our Customers



LAWS

What is required legally?

GOVERNMENTS

NIST



STANDARDS

What is required functionally per market?

GOVERNMENTS



DEVICE PROFILES

What is required functionally per device type?

COMPANIES



psacertified™



SESIIP



CERTIFICATION SCHEMES

How do you standardize labs and testing of devices?

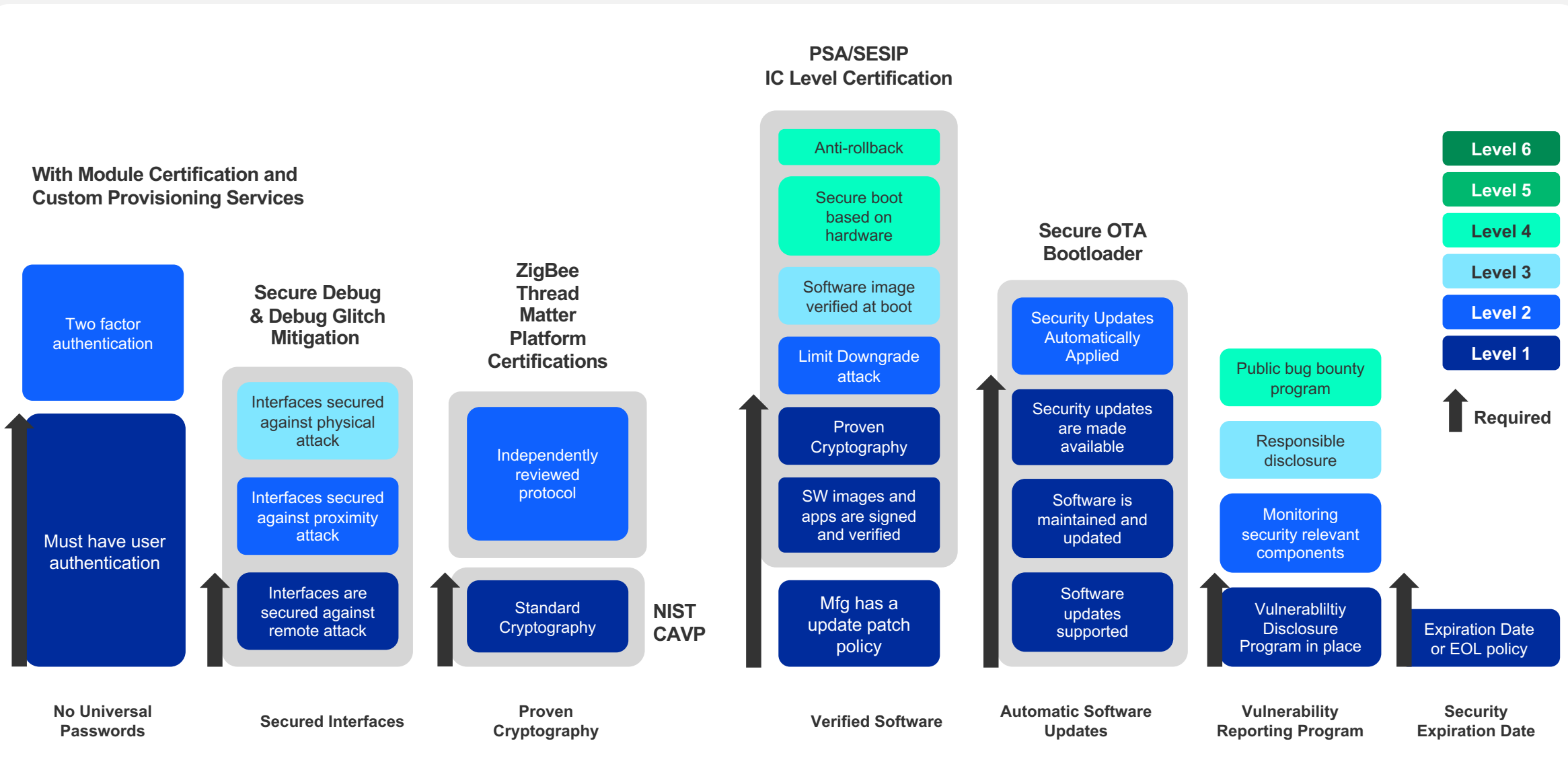
GOVERNMENTS

ioXt Alliance is Tackling Device Security Profiles and

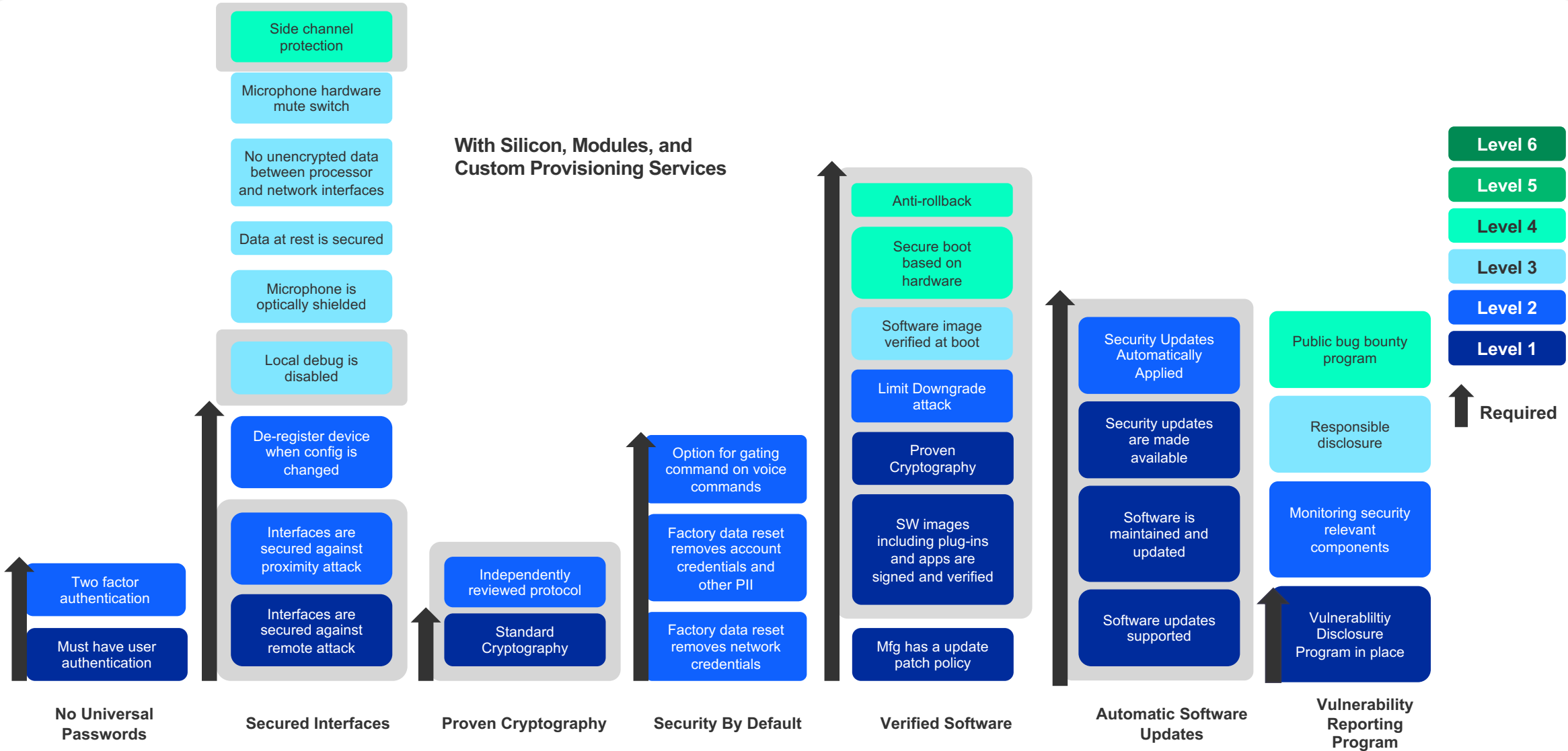
450+ MEMBER COMPANIES
35+ COUNTRIES



Example of an ioXt Base Device Security Profile



Smart Speaker Profile



QR Code – Picture of Device Appears with Certification

ioXt



Pixel 4a
Google

QD4A.200805.003

ioXt

CERTIFIED

Meet Pixel 4a, the helpful Google phone at a helpful price. It comes packed with the things you want most in a phone. You can take great photos, even if the lighting isn't right. It can even capture the Milky Way. (Yes, that Milky Way.) It has an Adaptive Battery that lasts up to 24 hours. And with the new Google Assistant, you get the help you need, fast. Pixel 4a comes with all this and more, for a lot less than you'd expect.

[Visit Pixel 4a web page](#)

[Dispute Certification](#)

[Report Vulnerability](#)

Scalable Crowd Sourced Certification Policed by Certification Bounties



Manufacturer Certifies Device

Method 1 - Self Assessment
Manufacturer Submits Security Information

Method 2 - Lab Assessment
Manufacturer Chooses Lab for Security Analysis



Researchers
Independent researchers submit security issues for any certified product (either self- or lab-certified) on the ioXt site and are rewarded for all verified flaws.



Inheritance through Silicon Labs ioXt Certified Components



[About ioXt](#) [News & Articles](#) [Certified Products](#) [Certification Program](#) [Board of Directors](#)

[Member Portal](#)



BLE Lightbulb

Firmware Version: # 1.0

Certification Profile: ioXt 2020

[Submit a Question](#)

Security Inheritance






Select an ioXt Certified Component provider from the drop-down below, then select the specific component that your product contains.

Click Next to skip.

ioXt Certified Provider:

Silicon Labs

ioXt Certified Components:

Product Name	SKU	Firmware Ver.	Links	Selection
 MGM210PA	MGM210PA	Bluetooth 3.1.2.0	Certification Details	Select
 MGM210PB	MGM210PB	Bluetooth 3.1.2.0	Certification Details	Select
 BGM210PA	BGM210PA	Bluetooth 3.1.2.0	Certification Details	Select
 BGM210PB	BGM210PB	Bluetooth 3.1.2.0	Certification Details	Select
 MGM220P	MGM220P	Zigbee EmberZNet Version 6.9.2.0	Certification Details	Select

[Previous](#)

[Exit wizard](#)

[Next](#)

1. Customer Selects Silicon Labs
2. Silicon Labs Certified Modules Presented
3. A mouse hover over the module gives a module description and link to Silicon Labs Website
4. Select a module
 - Auto-completes security survey

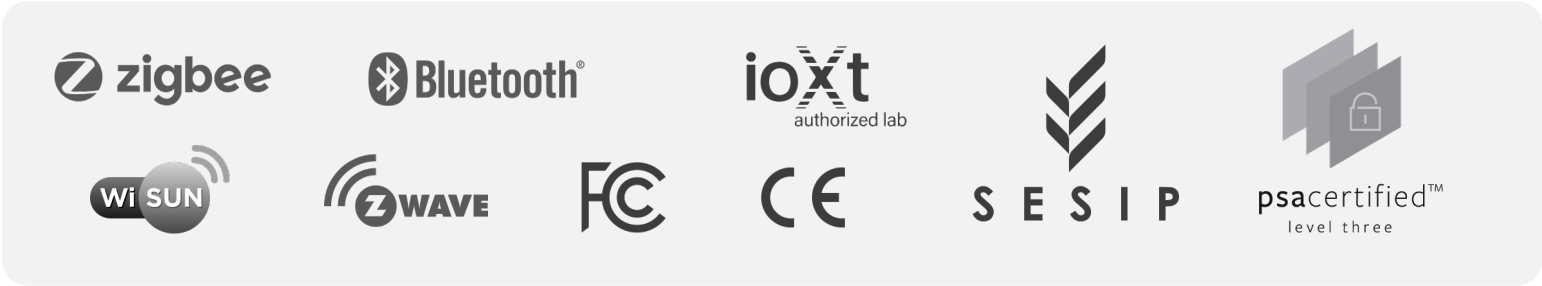
Insert Video here

- Play video of certified platform demo from Brad Ree at ioXt Alliance

Silicon Labs Makes It Easy to Protect the IoT Ecosystem



Silicon Labs ioXt Certifications can be inherited by 3rd Party Device Manufacturer



Works With Device
3rd Party Device Manufacturer only needs to do a delta certification against the specific Ecosystem Security Profile



Silicon Labs Security Certifications Inherited by 3rd Party Ecosystem Device Manufacturers

A Paradigm Shift in the Security Philosophy to “Zero Trust”

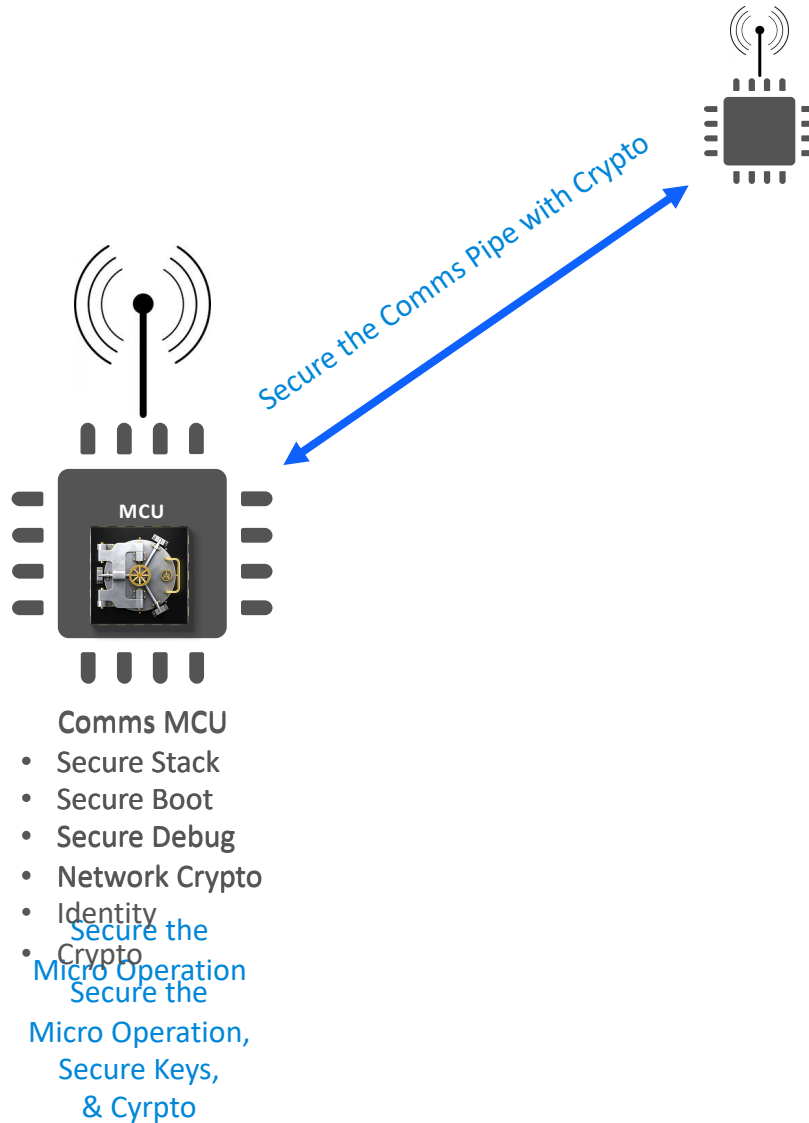
Yesterday

- Everything behind the gateway is trusted
- And assume devices are trusted perpetually

Today

- Nothing on the subnet can be trusted
- Authenticate **device identity** before allowing it to join and continuously re-authenticate

Keeping a Secure Identity Secret in the End Node is now in Scope



NewAE Technology Inc. **\$3800 USD**



HOME ABOUT PURCHASE HARDWARE EDUCATION NEWS CONTACT SUPPORT

ChipWhisperer-Pro Kit

MSRP: \$3800 US



The ChipWhisperer-Pro features a time pattern matching in the analog algorithms, and more. It keeps the seamless to switch between ChipWh

NewAE Technology Inc. **\$3300 USD**



HOME ABOUT PURCHASE **HARDWARE** EDUCATION NEWS CONTACT SUPPORT

ChipSHOUTER®

MSRP: \$3300 USD



Electromagnetic fault injection allows attacks and testing done in-situ, without the need to use special development boards or to modify the target board. It is a powerful attack method that requires careful consideration of how it might apply to your products.

The diagram illustrates the Silicon Labs Secure Identity flow for IoT devices. It shows the process from a Certificate Authority (CA) to an Ecosystem Cloud Provider (ECP) via an ODM/OEM/CM (Original Design Manufacturer/Original Equipment Manufacturer/Contract Manufacturer).



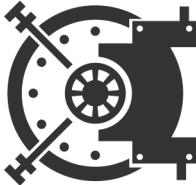
Key Components and Flow:

- Certificate Authority (CA):** Represented by a key icon, it interacts with the Silicon Labs system via a **Certificate Signing Request (CSR)**.
- Approved by Ecosystem:** A label indicating the CA's approval.
- SILICON LABS:** The central entity that manages the secure identity process.
- Secure Identity:** A blue box representing the secure identity module, which is downloaded to the device.
- ODM/OEM/CM:** The manufacturer responsible for producing the IoT devices.
- IoT Devices:** The final products, including a light bulb, a smart home device, and a smartphone, which are pre-registered in bulk.
- Ecosystem Cloud Provider (ECP):** The cloud service that manages the IoT devices.

Security and Pre-registration:

- The diagram shows a **Pre-register Devices in bulk** step, where devices are pre-registered before being shipped.
- Two devices are shown with a red 'X' over them, labeled **Fake**, indicating that only authentic devices are allowed to connect to the ECP.

Secure Vault™ Right Level of Security to Protect Identities

	Protect Identity from Remote Attacks	Protect Identity from Local Attacks	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	



Designing Secure IoT Devices

Related Security Focused Works With Sessions

- **Works With Sessions**

- SEC-102: Enforced Security Regulations will Demand a Security Warranty in IoT Devices
- SEC-201: Applying Security to Verify Deployed Products are Authentic
- SEC-301: Hands on Security
- SEC-PNL: Smart Home Security and the User Experience

- **Join ioXt Alliance and get ahead of the regulations www.ioxtalliance.org**



works with

BY SILICON LABS

VIRTUAL CONFERENCE

