Tech Talks Schedule – Presentation will begin shortly

tech talks

Tuesday, May 31	**Matter: Securing your IoT devices**
Tuesday, June 14	Wi-Fi: Coexistence with RS9116

We will begin in: 0:00

SILICON LABS | tech talks

Welcome

Matter: Securing your IoT devices

Wendy Warne

SILICON LABS

Matter and Matter Security

Presenter: Wendy Warne

Agenda

- Why and What of Matter
- Matter Network
- Security features of Matter
- Securely commissioning a device
- How to get started with Matter

Why Matter - Unifies IoT Connectivity

IoT Devices

WORKS WITH amazon alexa

works with ring

works with XFINITY Home

Works with SmartThings

works with the Google Assistant

Friends of hue

Works with Apple HomeKit

matter

Simplicity
Interoperability
Reliability
Security

Google

SILICON LABS

Schneider Electric

COMCAST

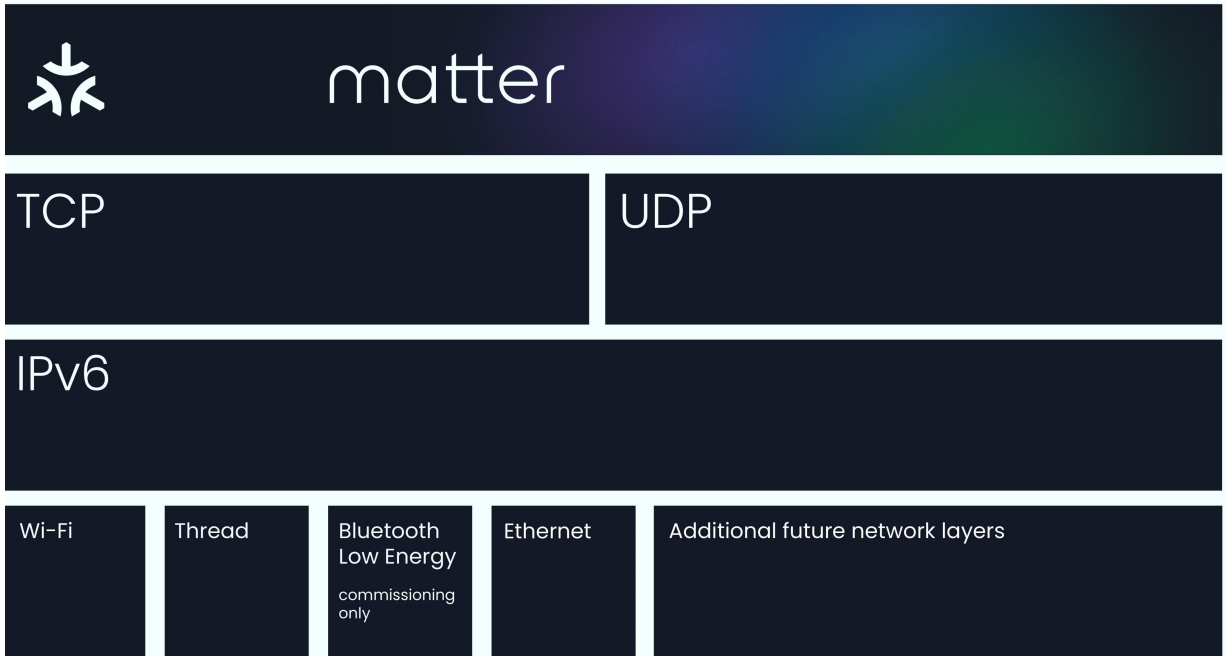
somfy

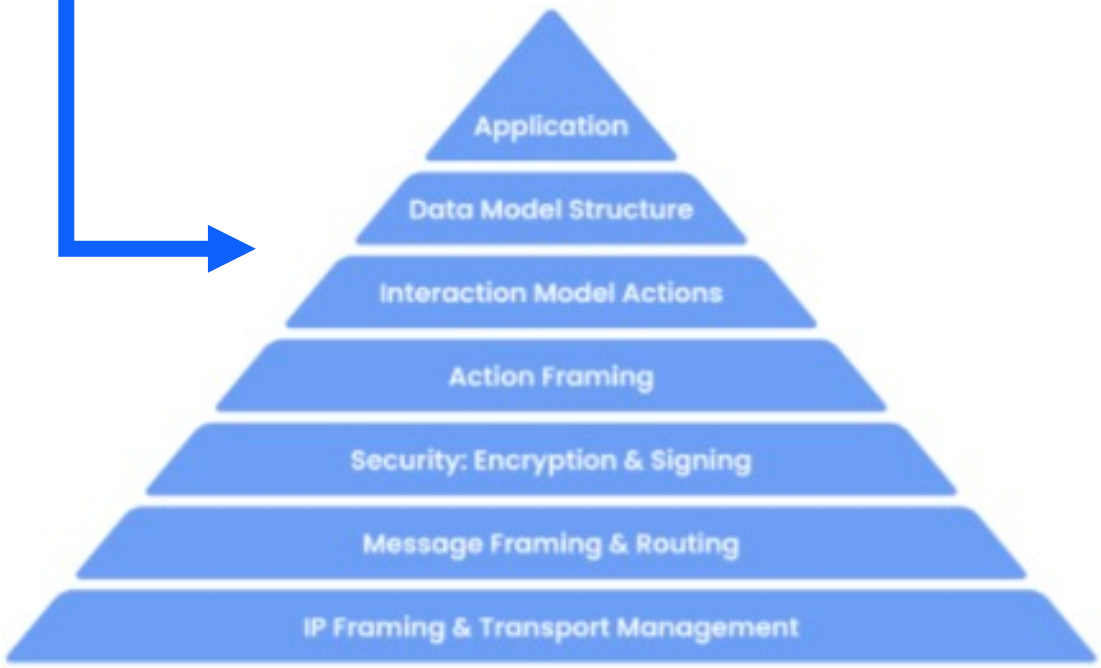
IKEA

amazon

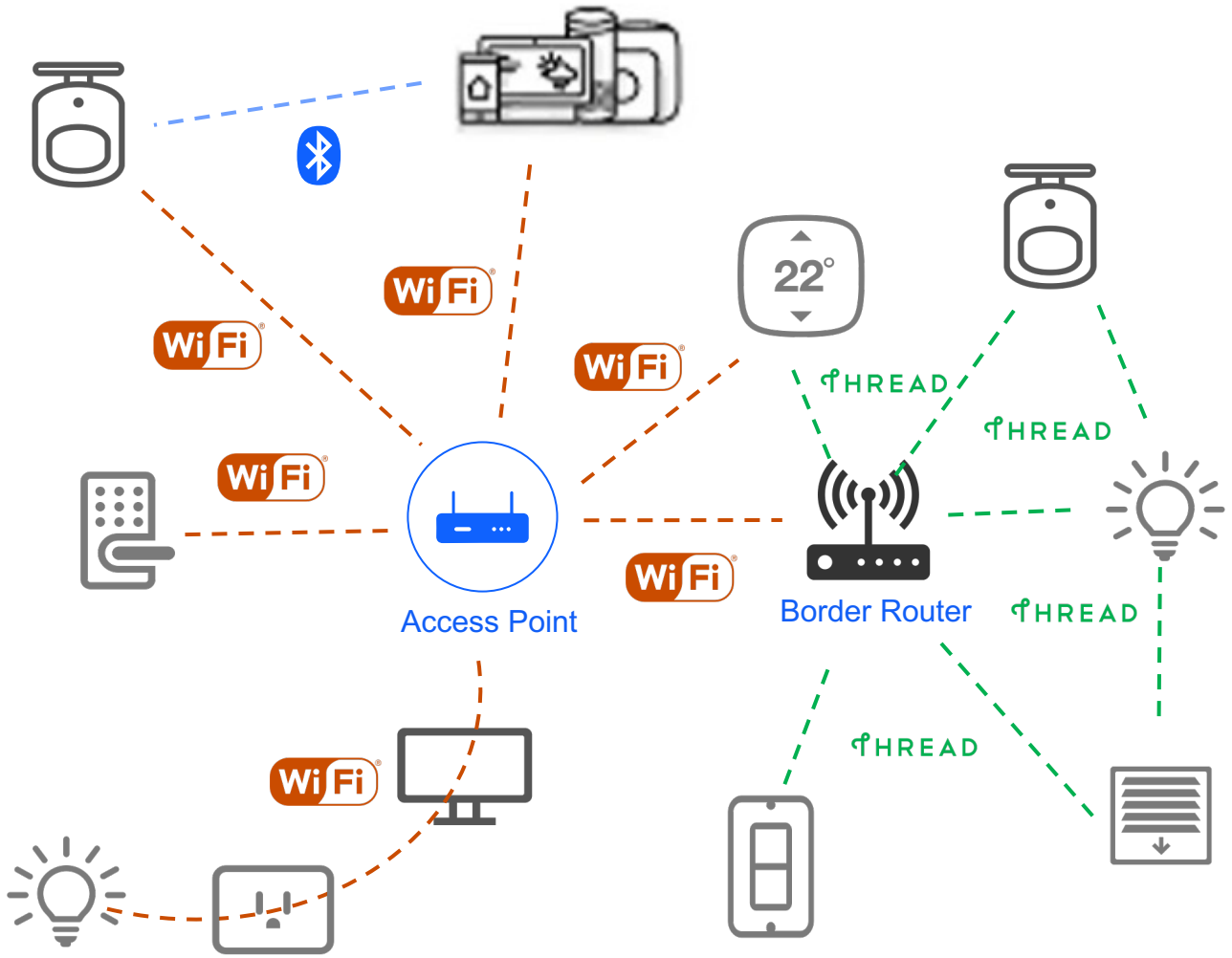
SAMSUNG SmartThings

What is Matter





Matter Network



- Focus on Ethernet / WiFi / Thread
- BLE is used as the commissioning channel
- Thread devices connect to other IP networks through border routers
- Bridges can link to other protocols like Zigbee and Z-Wave

Matter’s Security Principles

- No anonymous joining
- Device identity and authentication is verified though Device Attestation
- Unique operational credentials are generated for each Matter device on each Fabric
- Network credentials are given only ***after*** device authentication
- Open standard and open-source software

Matter Security Cryptography

Cryptographic Primitives

- 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

Cryptographic Functionality

- **Verification of Device Certificate**
- **Generation of Operational Certificate via CSR (Certificate Signing Request)**
- **PASE -** Password Authenticated Session Establishment
- **CASE -** Certificate Authenticated Session Establishment

Sample Commissioning Flow (Part 1)

1 Initiate Matter Joining

Standard Commissioning

Just turn on device

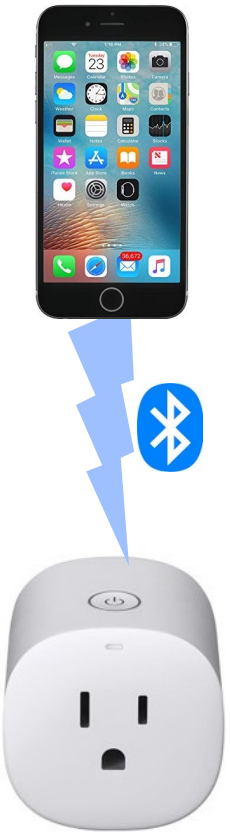
User Directed Commissioning

Use UI to Activate Matter

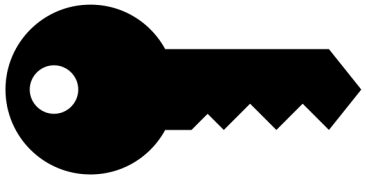
2 Scan Matter QR Code

…or enter Matter Passcode Manually

3 BLE Beaconing and connection



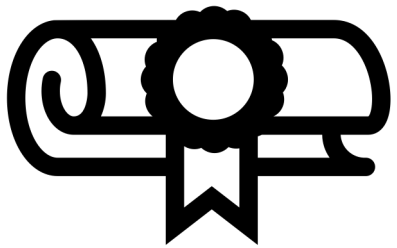
4 PASE Password Authenticated Session Establishment



Passcode verified
Encrypted Keys established

Sample Commissioning Flow (Part 2)

5 Device Attestation

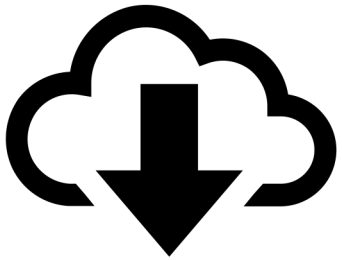


Check manufacturer certificate and device compliance

6 Install Operational Security

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

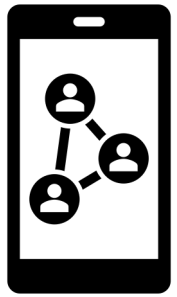
7 Configure Operational Network



Convey WiFi or Thread network credentials using Network Commissioning Cluster

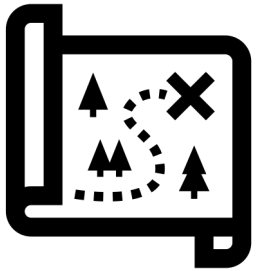
Sample Commissioning Flow (Part 3)

8 Join Network



Device attaches to WiFi or Thread network

9 Discover Device on IP network

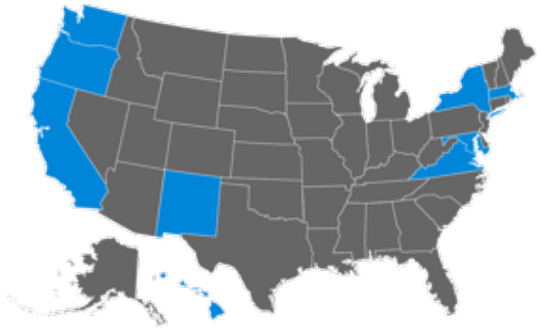


Controller discovers device using DNS and establishes a CASE session using newly configured security material.

10 Finalize

Inform Device Commissioning is complete
Performs any other application configuration

IoT Security Legislation is Happening



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

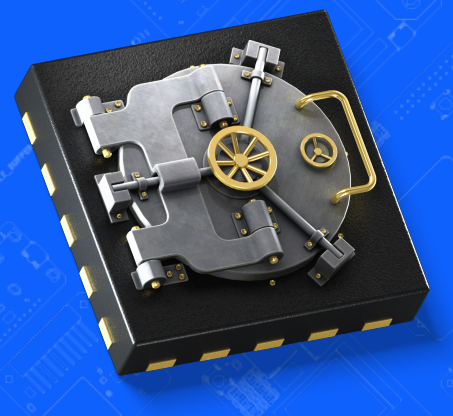
Virginia	(HB 2793)
Oregon	(HB 2395)
Hawaii	(SB 418)
Maryland	(SB 0613)
Massachusetts	(SD 341)
New Mexico	(SB 176)
New York	(S00224)
Rhode Island	(SB 234)
Washington	(SB 5376)

- **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

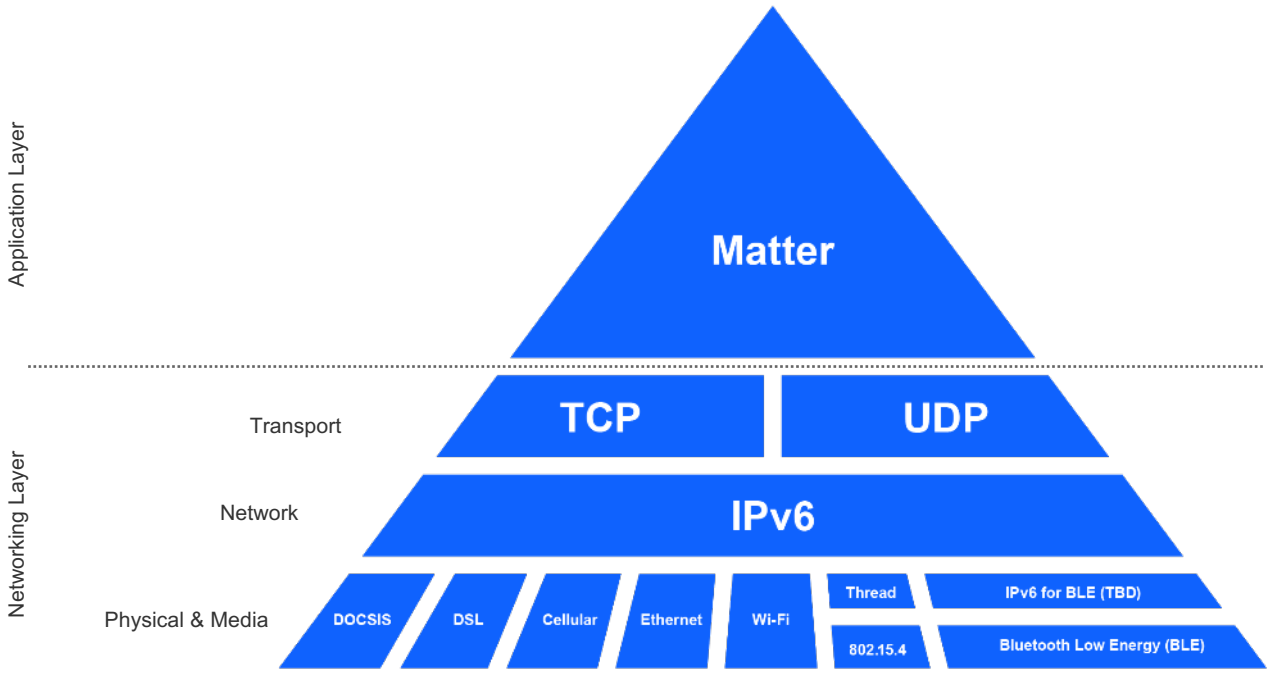
Secure Vault™

Base	Mid	High	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



Designing Secure IoT Devices

The EFR32MG24 is built for Matter



zigbee Zigbee Cluster Library

WEAVE Google Weave

Apple HomeKit

Amazon Alexa's Smart Home

GitHub

The MG24 is ideally suited for Matter thanks to its security offering, increased memory, low power consumption and improved RF performance

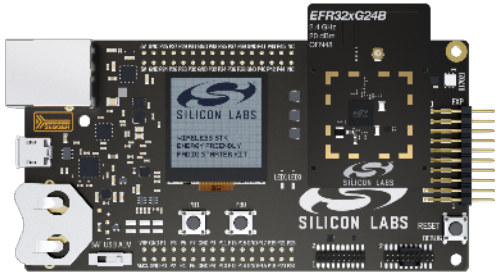
amazon Google zigbee alliance NXP resideo SmartThings Schneider Electric IKEA legrand LEEDARSON MMB NETWORKS signify SILICON LABS somfy Wulian

Getting Started with EFR32MG24 SoCs

- **Dev Board**
  - Low-cost development board
  - On-board debugger
  - Signal breakouts
  - On-board sensors
  - 20-bit ADC
  - AI/ML hardware accelerator
- **Contents**
  - 1x dev board

Part Number	Description
xG24-DK2601B	EFR32xG24 2.4 GHz +10 dev board

- **Pro kits**
  - Modular development platform
  - Advanced development
  - RF measurements
  - Energy profiling
  - External device debug
  - Ethernet for large network test
- **Contents**
  - 1 x WSTK main board
  - 1 x radio board

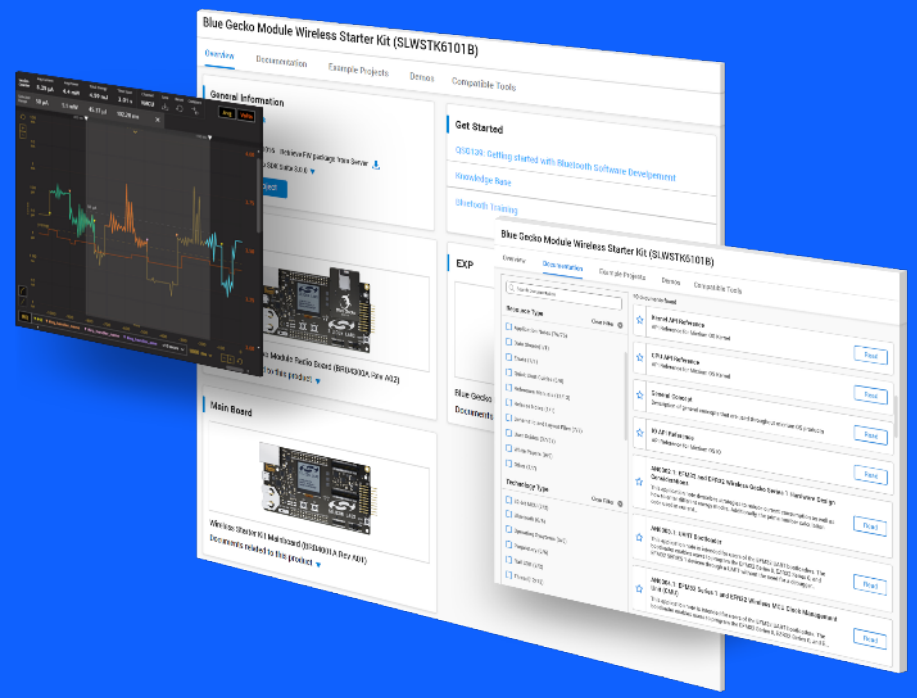


Part Number	Description
xG24-PK6009A	EFR32xG24 2.4 GHz +10 dBm Pro Kit
xG24-PK6010A	EFR32xG24 2.4 GHz +20 dBm Pro Kit

- **Radio Board kits**
  - Uses existing WSTK boards
  - Uses existing software tools
- **Contents**
  - 1x radio board

Part Number	Description
xG24-RB4186C	EFR32xG24 2.4 GHz +10 dBm Radio Board
xG24-RB4187C	EFR32xG24 2.4 GHz +20 dBm Radio Board
xG24-RB4188A	EFR32xG24 +20 dBm Antenna Diversity Board

Simplified Developer Experience



Simplicity Studio 5

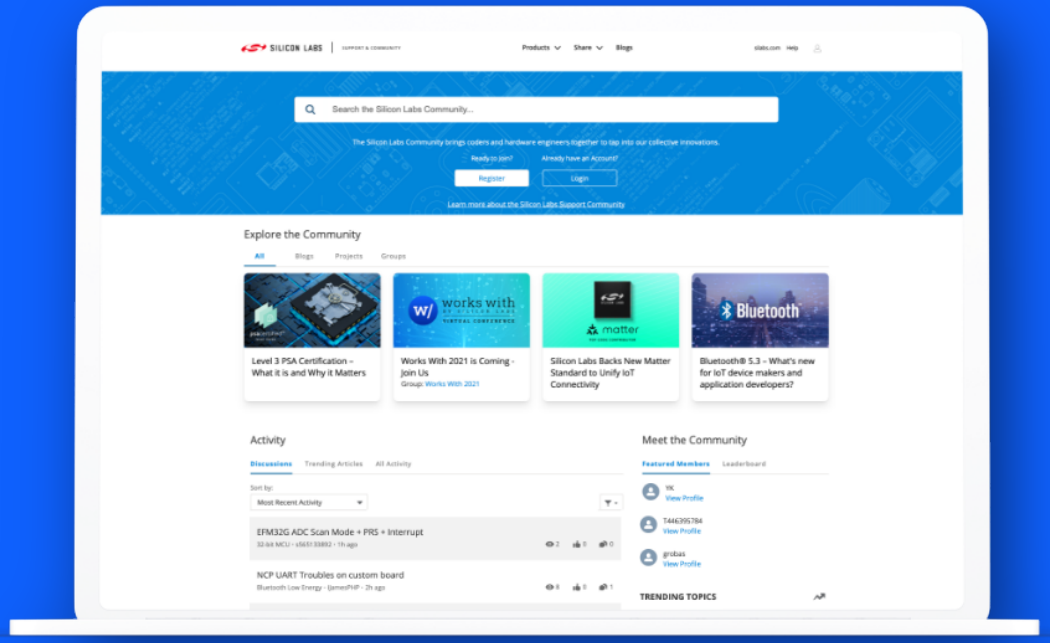
Simplicity Studio 5

- **Interface**
  - Fresh, new & simplified
  - Intuitive out-of-the-box experience
  - Fast access to developer resources
  - Linux, Mac & Windows
- **Tools**
  - Configuration utilities
  - Compiler
  - Error & validation
  - IDE & command line support
  - Graphical hardware configurator
  - Energy Profiler – visual energy analysis
  - Network Analyzer – packet capture & decode


SILICON LABS
tech talks
Thank You


SILICON LABS
tech talks
Q&A

Continue Discussion in Our Community!



How to Navigate:

- “Products” to troubleshooting forums
- “Applications” to discuss IoT
- “Share” to view example projects and existing groups
- “Blogs” to view and discuss thoughts from our specialists

community.silabs.com

tech talks

WEBINAR

Wi-Fi: Coexistence with RS9116

JUNE 14 | 10:00 CDT/CET

SILICON LABS

works with
BY SILICON LABS

VIRTUAL CONFERENCE | SEPTEMBER 13 - 15TH

REGISTRATION NOW OPEN

9 Workshops

70+ Sessions

3 Full Days

Scan to Register