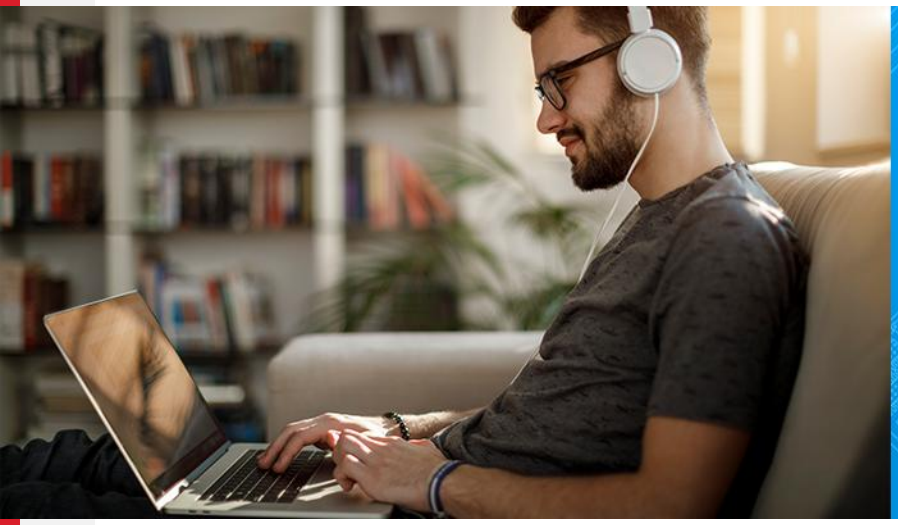
WELCOME



Silicon Labs LIVE:

Wireless Connectivity Tech Talks

APAC Tech Talks LIVE - Japanese

Topic	Date
Designing Secure Bluetooth 5.2 IoT Products with BG22	10a.m., Tuesday, June 4
Connected Home Over IP (CHIP) for Beginners	10a.m., Thursday, June 9
Device & Network Security for the IoT	10a.m., Thursday, June 11

Speaker

Akimasa Mizutani

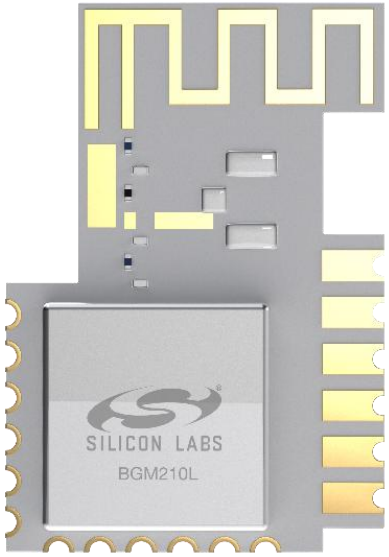
Sr. FAE & IoT Specialist, Silicon Labs Japan

Akimasa Mizutani works as Sr. FAE and IoT specialist in Silicon Labs Japan office. He serves technical support and consultation of IoT solutions by Silicon Labs.

Designing Secure Bluetooth 5.2 IoT Products with BG22

AKIMASA MIZUTANI | JUNE 2020

Silicon Labs: Advancing What's Possible in the IoT



- **Expertise**: 20+ years providing RF solutions with more than 1 billion deployed wireless nodes worldwide
- **Platform**: Simplifying IoT product design with highly-integrated devices, reusable software and advanced development tools
- **Security**: Providing enhanced security features to help developers increase consumer trust in connected products

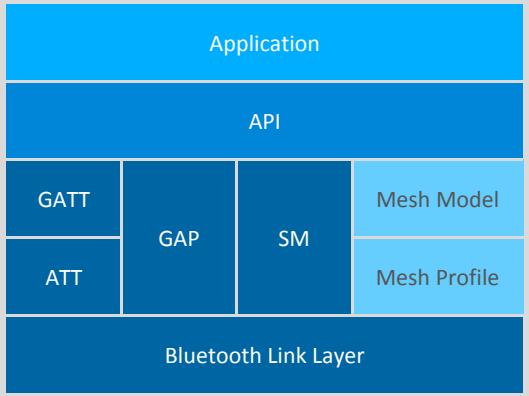
Bluetooth Proprietary THREAD Wi Fi zigbee Z-WAVE

A Complete Solution for Enabling Bluetooth Products

SoCS AND MODULES

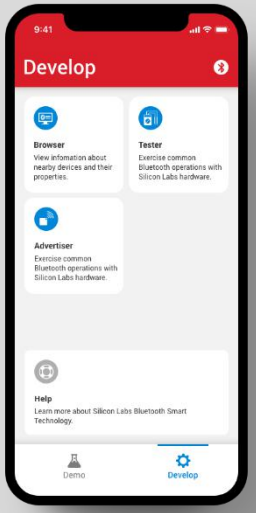
Industry leading Bluetooth 5.1 and 5.2 SoCs and pre-certified modules

STACK SOFTWARE



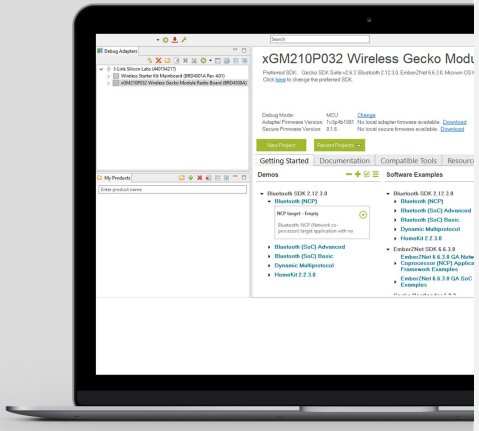
In-house developed stacks with latest Bluetooth 5.2 and mesh features

MOBILE APPLICATIONS



Reference applications and source code for iOS and Android

DEVELOPMENT TOOLS



Free-of-charge development and protocol analysis tools to boost productivity

BG22: Optimized Battery Powered Bluetooth LE

Optimized

Secure Bluetooth 5.2 SoCs for High-Volume Products

Radio
Bluetooth 5.2
TX: -27 to +6 dBm
RX: -96 to -107 dBm
1M, 2M and LE Coded PHYs
AoA & AoD

Ultra-Low Power
3.5 mA TX (radio)
2.6 mA RX (radio)
1.4 µA EM2 with 32 kB RAM
0.5 µA w/ RTC in EM4

World Class Software
Bluetooth 5.2
Bluetooth mesh LPN
Direction Finding

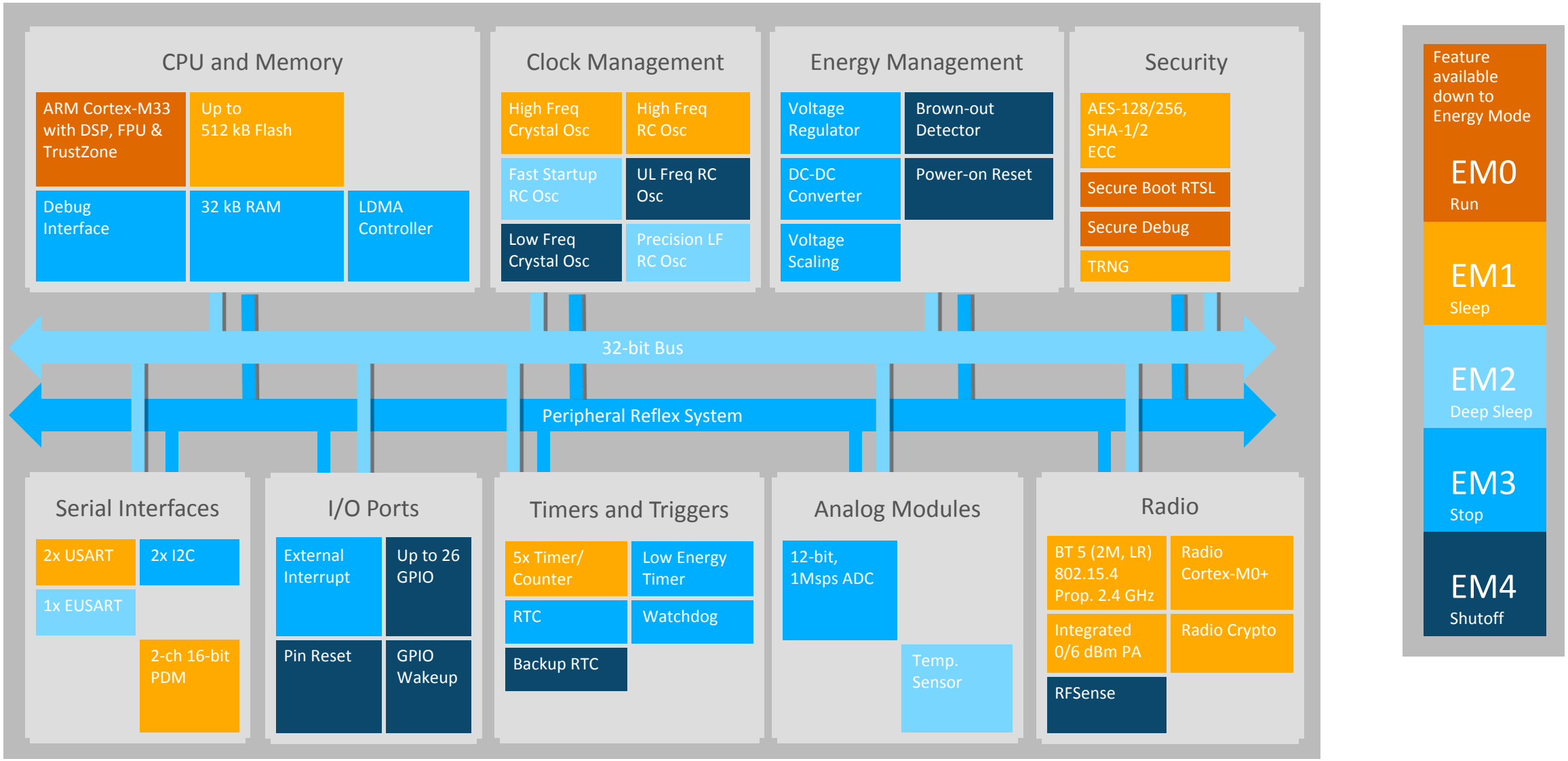
Compact Size
5x5 QFN40 (26 GPIO)
4x4 QFN32 (18 GPIO)
4x4 TQFN32 (18 GPIO)

ARM Cortex-M33 with TrustZone
38.4/76.8 MHz
352/512 kB of flash
32kB RAM

Peripherals Fit for Purpose
2x USART, 2x I2C, 2x PDM and GPIO
12-bit ADC (16 channels)
Built-in temperature sensor with +/- 1.5 °C
Built-in 32 kHz, 500ppm sleep clock

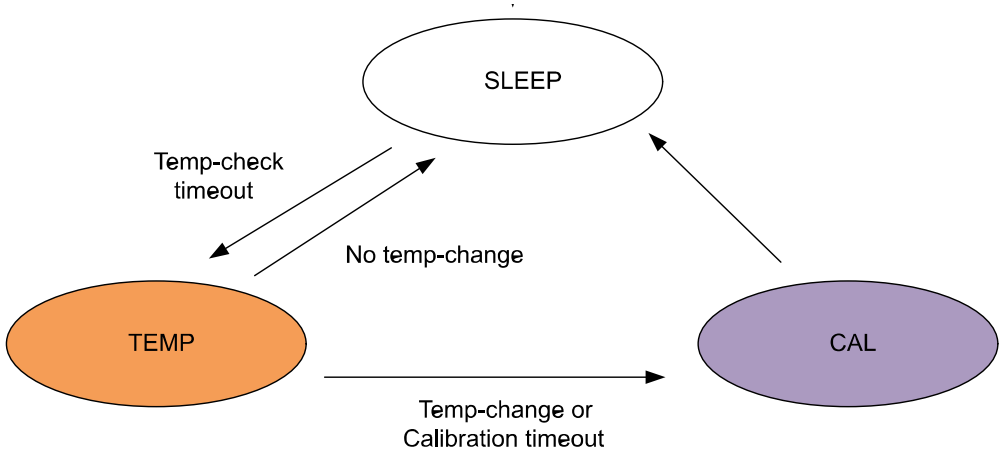
Security
AES128/256,SHA-1, SHA-2 (256-bit)
ECC (up to 256-bit), ECDSA and ECDH
True Random Number Generator (TRNG)
Secure boot with RTSL
Secure debug with lock/unlock

BG22 Block Diagram



Highlights

- **76.8MHz vs. 38.4MHz**
  - The MCU can be run at 76.8MHz or 38.4MHz
  - Lowest power is achieved when running at 38.4 MHz
  - Running at 76.8MHz should only be used when necessary
    - EM0 +1.1 mA
    - EM1 +0.6 mA
- **PLFRCO – The built-in 32kHz sleep clock**
  - 500ppm accuracy over full temperature range down to EM2
  - Can replace an external 32kHz XTAL for an optimized BoM
  - Configurable internal temperature calibration
    - Adds 0.3uA to EM2 current at stable temperatures
    - However can add +10uA in highly variable temperature conditions

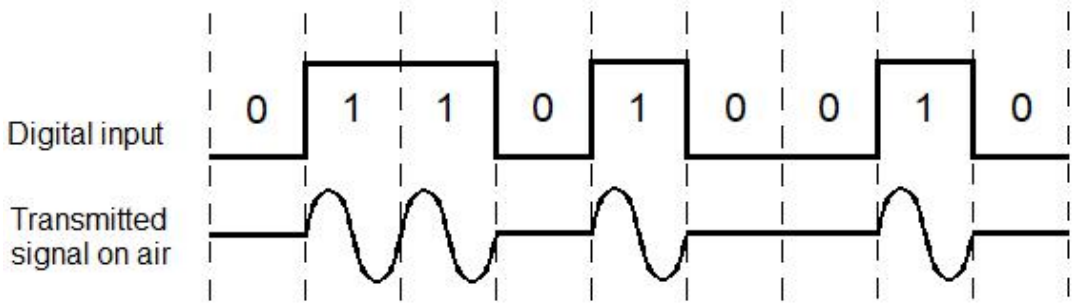


PLFRCO calibration

Highlights

- **RFSense - wake-on radio**
  - Provides wake-on radio capability from EM2, EM3 or EM4
  - Continuous wave and OOK preamble and syncword detection
  - 4/8-bit preamble and 8/16/32-bit syncword
  - Programmable RF detection threshold from -35dBm to -14dBm
  - Low power consumption at <200nA

- **EUART – Enhanced UART**
  - Separate RX/TX FIFOs with additional separate shift registers
  - Maximum Baud Rate
    - HF peripheral clock rate/16, 8, 6, or 4
    - 32kHz LF peripheral clock: 9600
  - Automatic Baud Rate Detection (only with HF peripheral clock)
  - EM2 operation with LF clock and wakeup to EM1
  - Hardware Flow Control



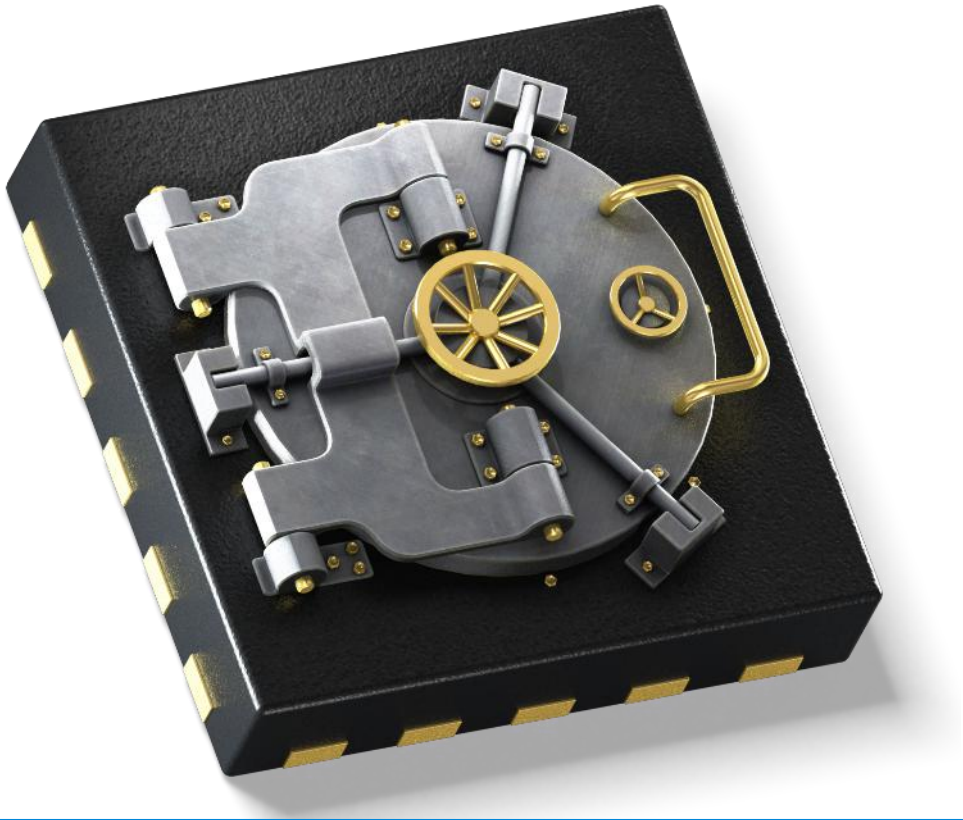
RFSense

Selecting a BG22 SoC

	BG22C112	BG22C222	BG22C224
Use cases	High-volume, consumer	Better RF, more GPIO	Advanced features, higher temp rating
Bluetooth features	1M and 2M PHYs AoA TX	1M and 2M PHYs AoA TX	1M and 2M PHYs 125k and 500k LE Coded PHYs Bluetooth mesh LPN IQ sampling for AoA
Max TX power	0 dBm	6 dBm	6 dBm
RAM	32 kB	32 kB	32 kB
Flash	352 kB	352 kB	512 kB
Max Temperature	-40 to +85°C	-40 to +85°C	-40 to +85°C (**G** OPNs) -40 to +125°C (**I** OPNs)
Max GPIO	18	26	26
Package options	4x4 QFN32	4x4 QFN32 4x4 TQFN32 5x5 QFN40	4x4 QFN32 4x4 TQFN32 5x5 QFN40

See BG22 Data Sheet for complete list of Orderable Part Numbers (OPNs)

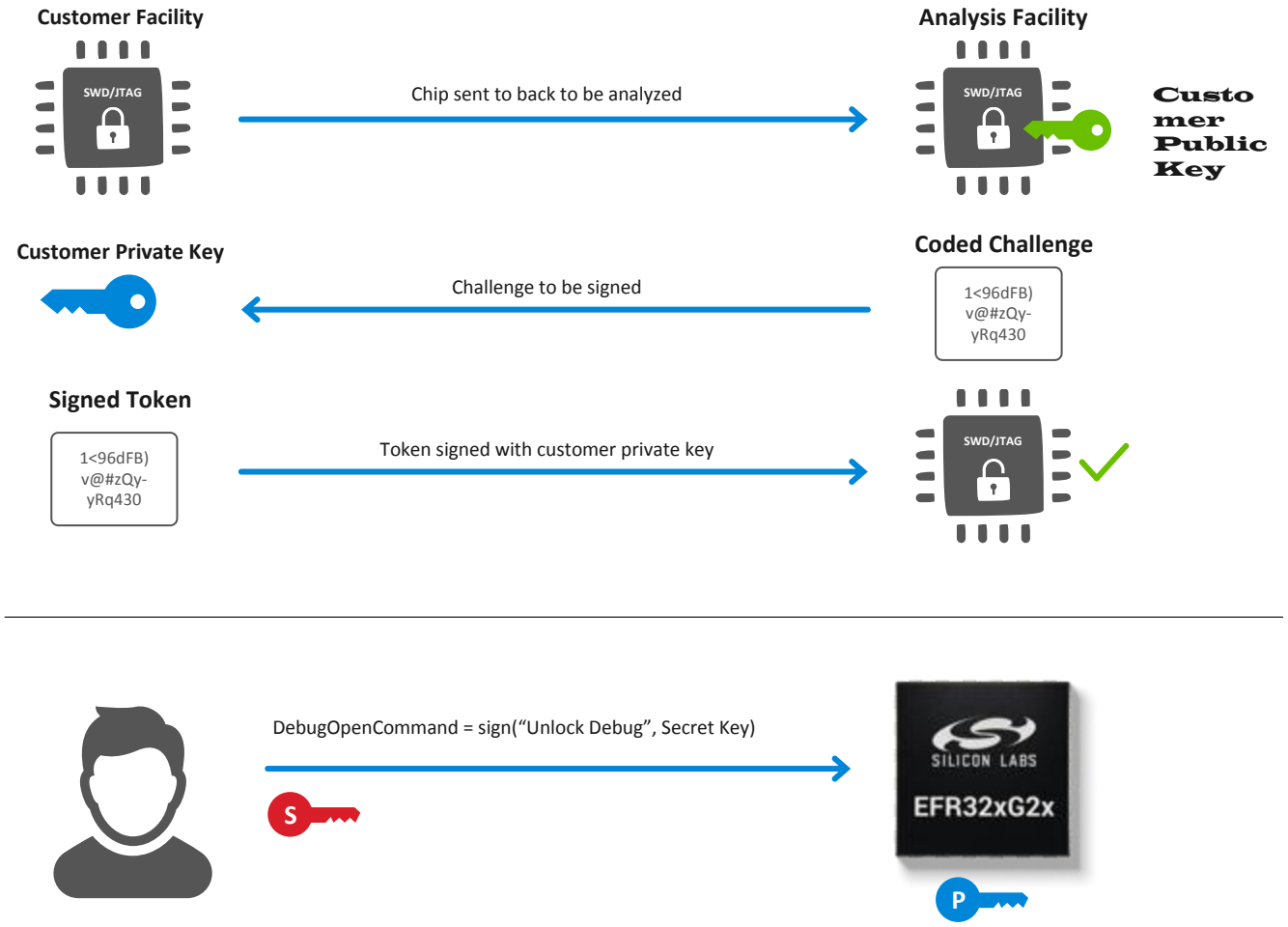
Securing Bluetooth Products with BG22



www.silabs.com/security

- **ARM Cortex M33 Core with TrustZone**
  - Provides cost effective hardware isolation
- **Hardware Accelerated Crypto**
  - Faster, more energy efficient and secure than software
- **True Random Number Generator (TRNG)**
  - Compliant with NIST SP800-90 and AIS-31
- **Secure Boot with Root of Trust and Secure Loader (RTSL)**
  - Prevents malware injection and rollback
  - Ensures authentic firmware execution and OTA updates
- **Secure Debug with Lock/Unlock**
  - Allows authenticated access for enhanced Failure Analysis (FA)

Secure Debug with Lock & Unlock



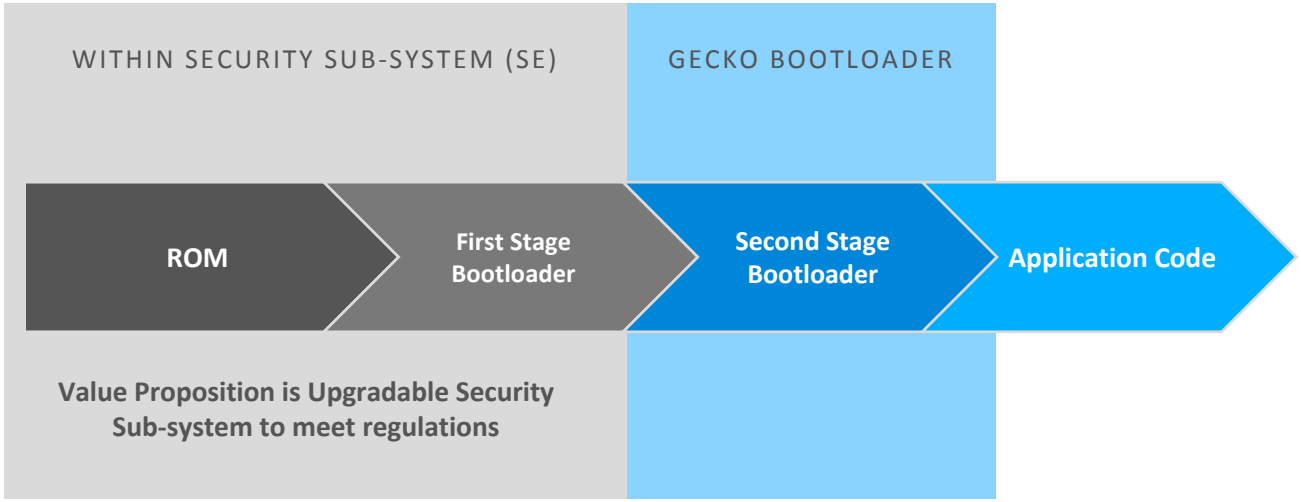
Why

- Debug / JTAG interface permits full access to code and data on a device
- The interface must be locked when deployed
- Opening debug interface often necessary for RMA or upgrades
- The debug interface is a commonly successful attack vector

Silicon Labs

- Devices support cryptographic, asymmetric authentication of debug commands
- Public 'Debug Unlock' key is provisioned during customer production
- 'Debug Unlock' token
  - is signed using a customer-provided private key and a challenge (nonce) from the device
  - can be invalidated by rolling the challenge on the device

Secure Boot with Root of Trust



Checks for a staged 'First Stage Bootloader' update and apply it if available

Check for 'First Stage Bootloader' Code Authenticity

MCU in Reset

Check for FSB Update and Stage it if available

Check Secure Boot Enabled Bit

Check for SSB Update and Apply it if available

Check SSB Code Authenticity

SE Releases MCU from Reset

Check for Application Code Update and Apply it if available

Check Application Code Authenticity

Execute Code

Vulnerabilities

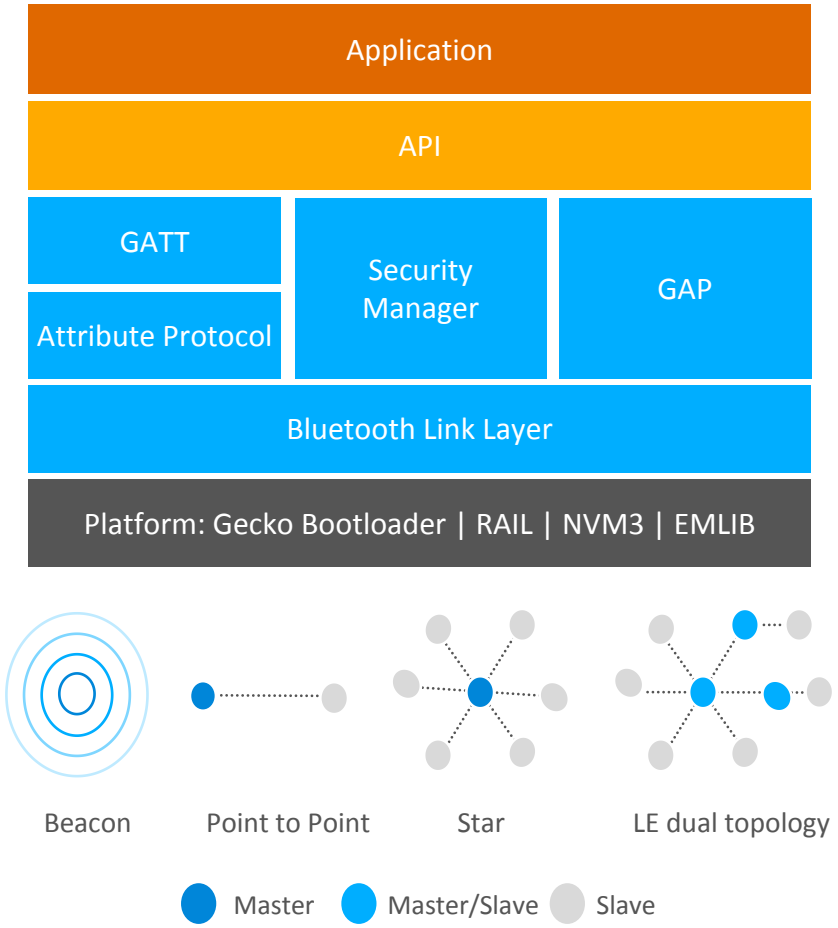
- Replacing code with 'look-alike code' makes a product appear normal. Hackers use it to copy/re-direct data to alternate servers.

Secure Boot with RTSL

(Root-of-Trust & Secure Loader)

- Use and execute only trusted application code against immutable memory and through a full chain of trust

Bluetooth LE Software



A Bluetooth 5.2 compliant Bluetooth stack, with:

- Bluetooth 5.2 Dynamic TX power control
- Bluetooth 5.1 Direction Finding
- Bluetooth 5.0 standard features
- Relevant Bluetooth 4.x features

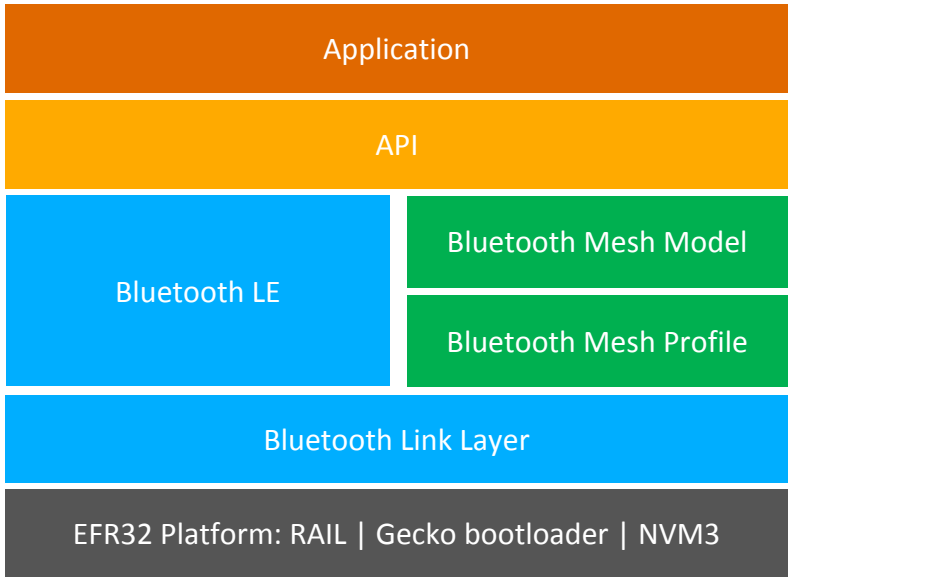
Packed with advanced functionality

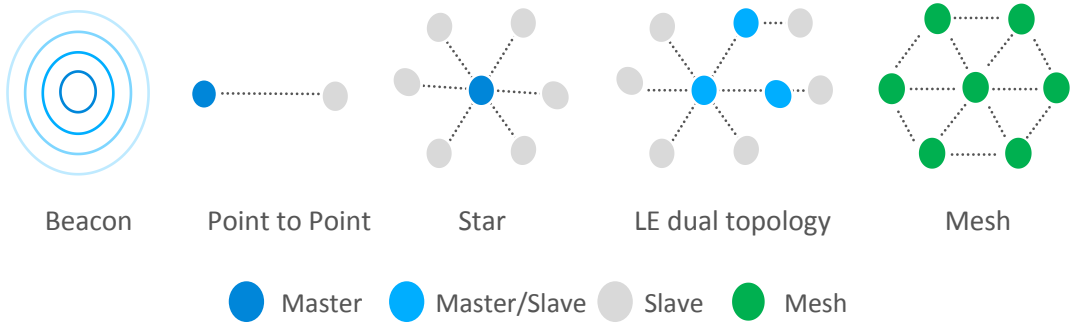
- Multiple connections and advertisers
- Concurrent advertising, scanning and LE connections
- Optimized throughput and power consumption

Built on top of the common EFR32 software platform

- Gecko bootloader
- EMLIB for MCU peripherals and drivers
- NVM3 key/value pair data storage with wear leveling
- RAIL radio driver

Bluetooth Mesh Software





A feature complete Bluetooth mesh profile, supporting:

- Proxy, relaying and friend nodes
- Bluetooth mesh low power nodes (LPN)
- Low latency communications down to 10ms per hop
- Large network support up to 4096 nodes

A comprehensive Mesh Model application layer, with:

- Lighting models for residential and commercial applications
- Generic, sensor and vendor models

Android and iOS Application Development Kits (ADKs)

- Network setup and configuration
- Device configuration and control
- Network database import and export

Bluetooth LE support includes

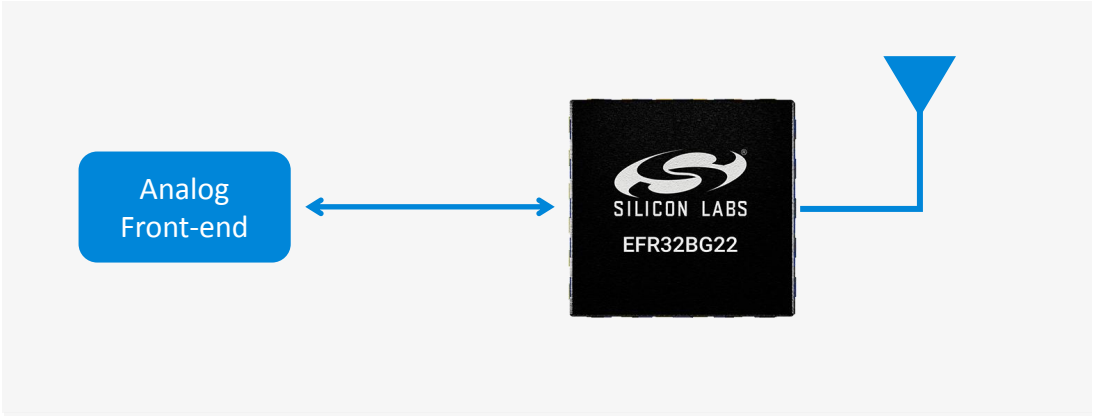
- Beaconing for indoor positioning systems
- Scanning for asset tracking
- Phone connectivity
- EnOcean light switches

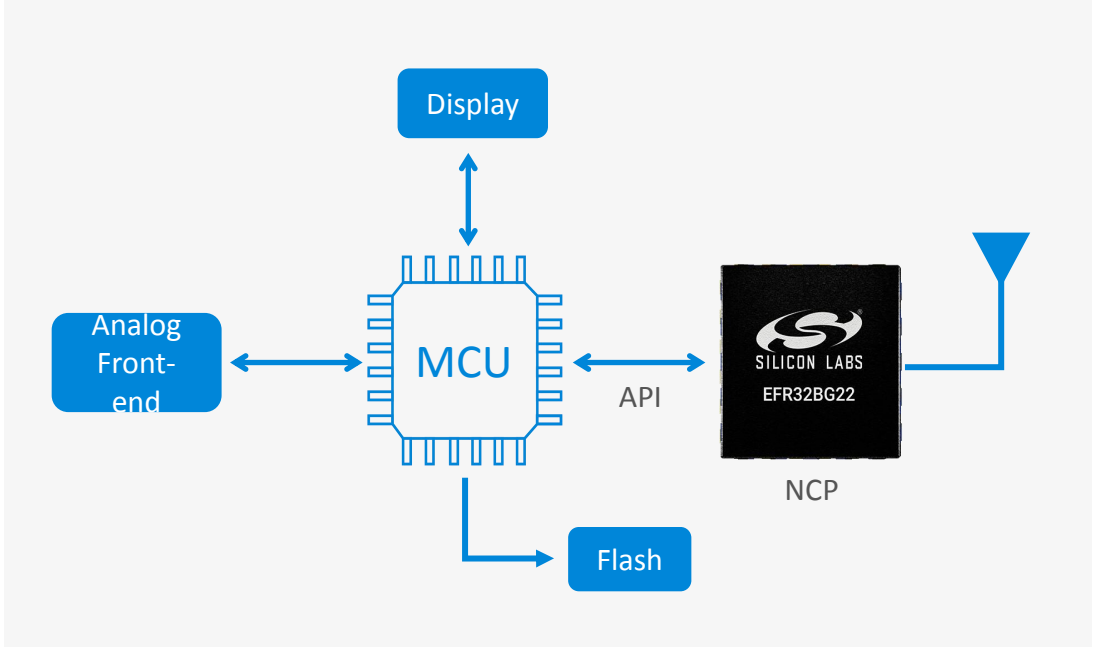
BG22 Extends Battery Life in Bluetooth Applications

Data Transfer	Location Services
Connected to a phone at 2000ms interval	Advertising 10 bytes every 1000ms
Using 2M PHY and transmitting 10 Byte / packet	TX at 0dBm and using 1 channel
Average current: 4.0 µA	**Average current: 3.7 µA**

5+ years on CR2032
10+ years on a CR2354

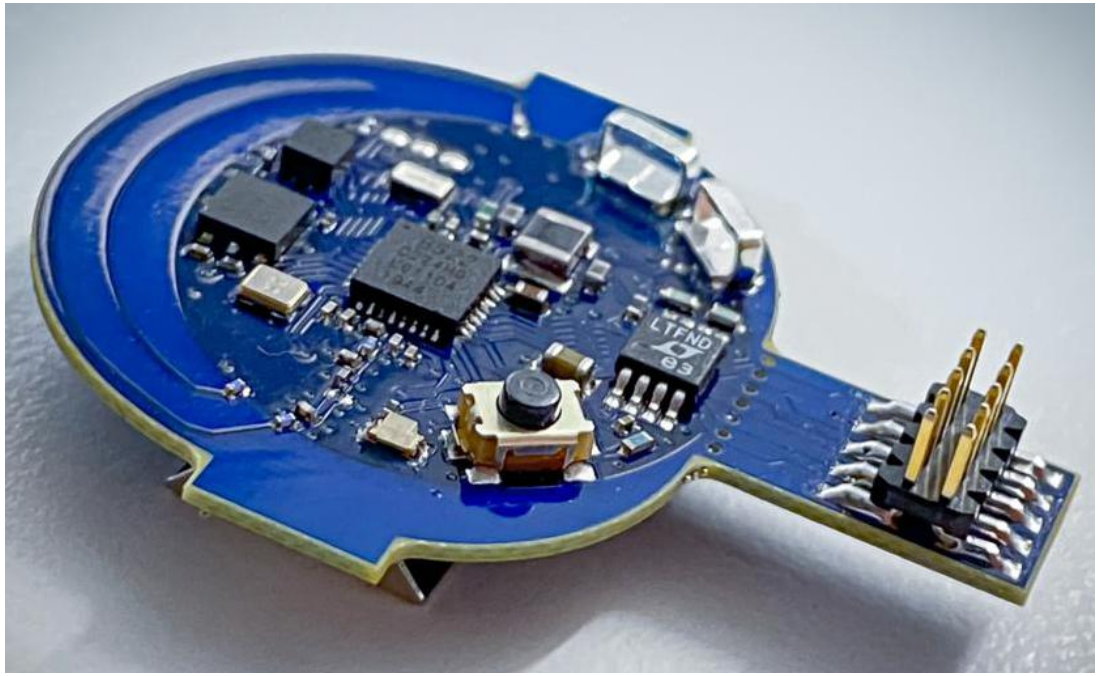
Portable Medical Devices





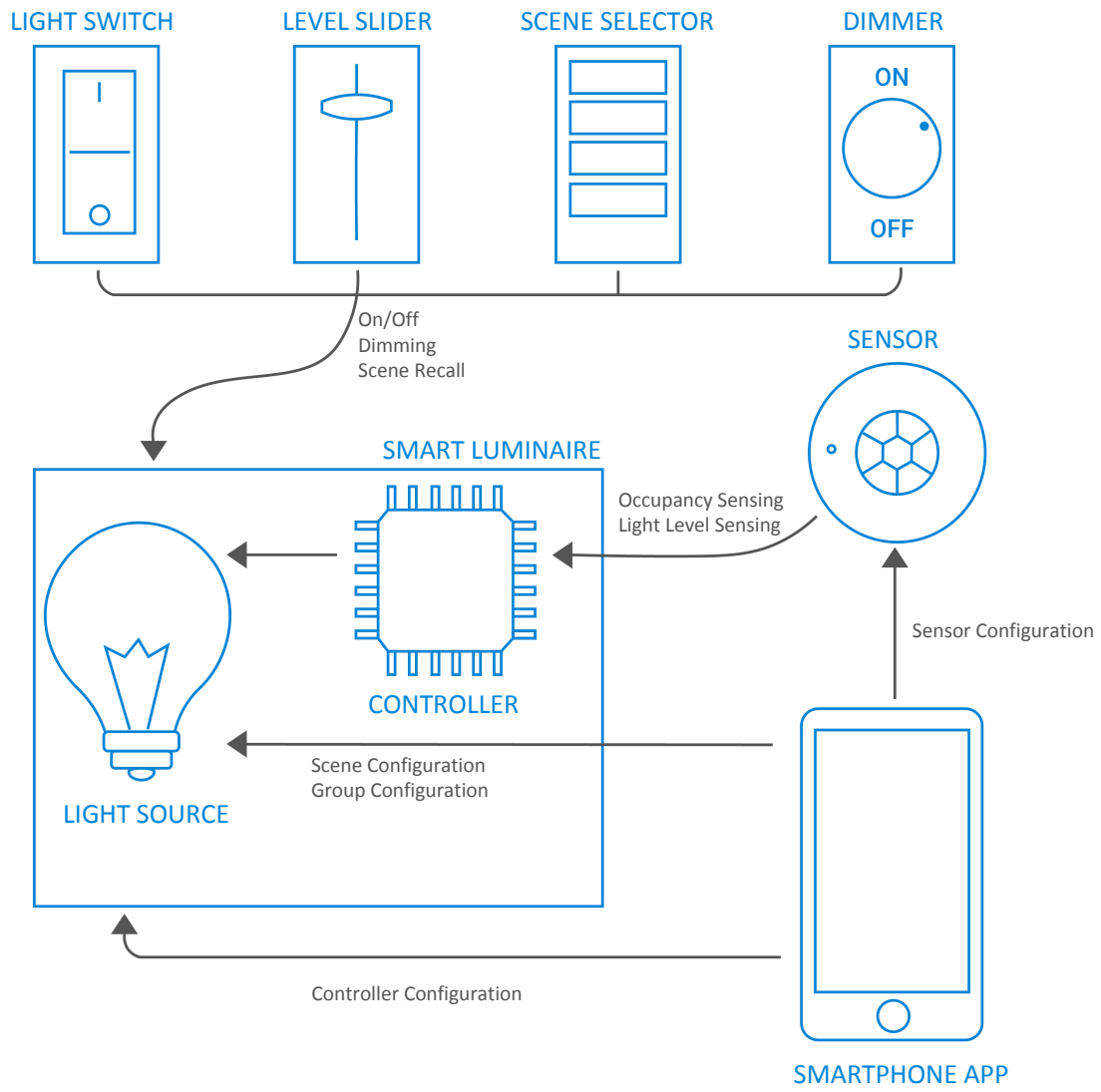
- BG22 can run as a radio and MCU for simple devices like continuous glucose monitoring patches
  - BG22 provides Bluetooth connectivity to a phone
  - Low power features help reach required lifetime
  - Interface to AFEs or sensors
  - Small size packages like 4x4 TQFN32 help minimize size
- For more complex devices with an external MCU, BG22 can be used as a low power Network Co-Processor
- BG22 supports DTSec security requirements
  - https://www.diabetestechnology.org/dtsec.shtml

Highly Accurate Indoor Location Services



- 5-10 years on a coin cell
- Support for AoA, AoD or Quuppa
- Low power peripherals
  - IO interrupts in EM4 – accelerometer can wake-up BG22
  - RTC in EM4 for timed wake-ups
- RFSense for wake-on radio
  - Can be for example used to wake-up tags for commissioning
- Optimized size and BoM
  - Possibility to use 1x HX XTAL
  - Built-in sensor for basic temperature monitoring
  - Small size packages like 4x4 TQFN32 help minimize size
  - RFSense

BG22 Enables Bluetooth Mesh Low Power Nodes



What do mesh network usually consist of?

- Main powered relaying/routing nodes like lights
  - Always of RX and sporadic TX
- Battery powered nodes like sensors or controls
  - Sleeping most the time and TX only when necessary

BG22 is ideal for Bluetooth mesh Low Power Nodes

- 32kB RAM and 512kB flash enough for LPN
- Ultra-low TX, RX and sleep currents
- Direct operation from coin cell batteries

BG21 is better suited for mains powered relaying nodes

- 96kB RAM and 1024kB flash support relaying/routing
- BG21 does not have DC-DC, which is not needed
- TX power up to +10/20 dBm

BGM220 Bluetooth Modules

BGM220S - SIP Modules

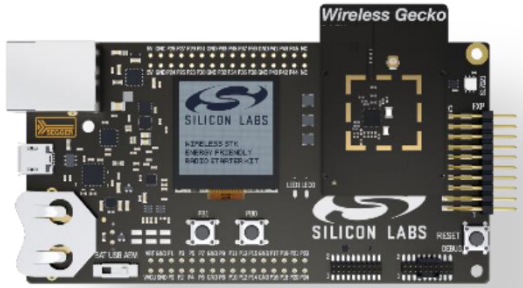
- Up to +6dBm TX
- 6 x 6 mm
- Up to 25x GPIO
- Built-in antenna and RF Pin
- With or without RF shield
- Up to 105°C
- CE, FCC/ISED, MIC and Telec

BGM220P - PCB Modules

- Up to +8dBm TX
- 13 x 15mm
- Up to 25x GPIO
- Built-in antenna
- With or without built-in LFXO
- Up to 105°C
- CE, FCC/ISED, MIC and Telec

- BGM220 modules provide additional benefits
  - Built-in antennas and integrated XTALs and passives
  - Worldwide certifications
  - Simpler design and faster time-to-market
- 10 year lifetime commitment
- BGM220 modules are sampling NOW
  - Contact your local Silicon Labs sales office
  - https://www.silabs.com/about-us/contact-us
- Full Production starts in Q3 2020

Getting Started with BG22 SoCs



BG22 SoC Starter Kit
SLWSTK6021A

Thunderboard BG22
SLTB010A

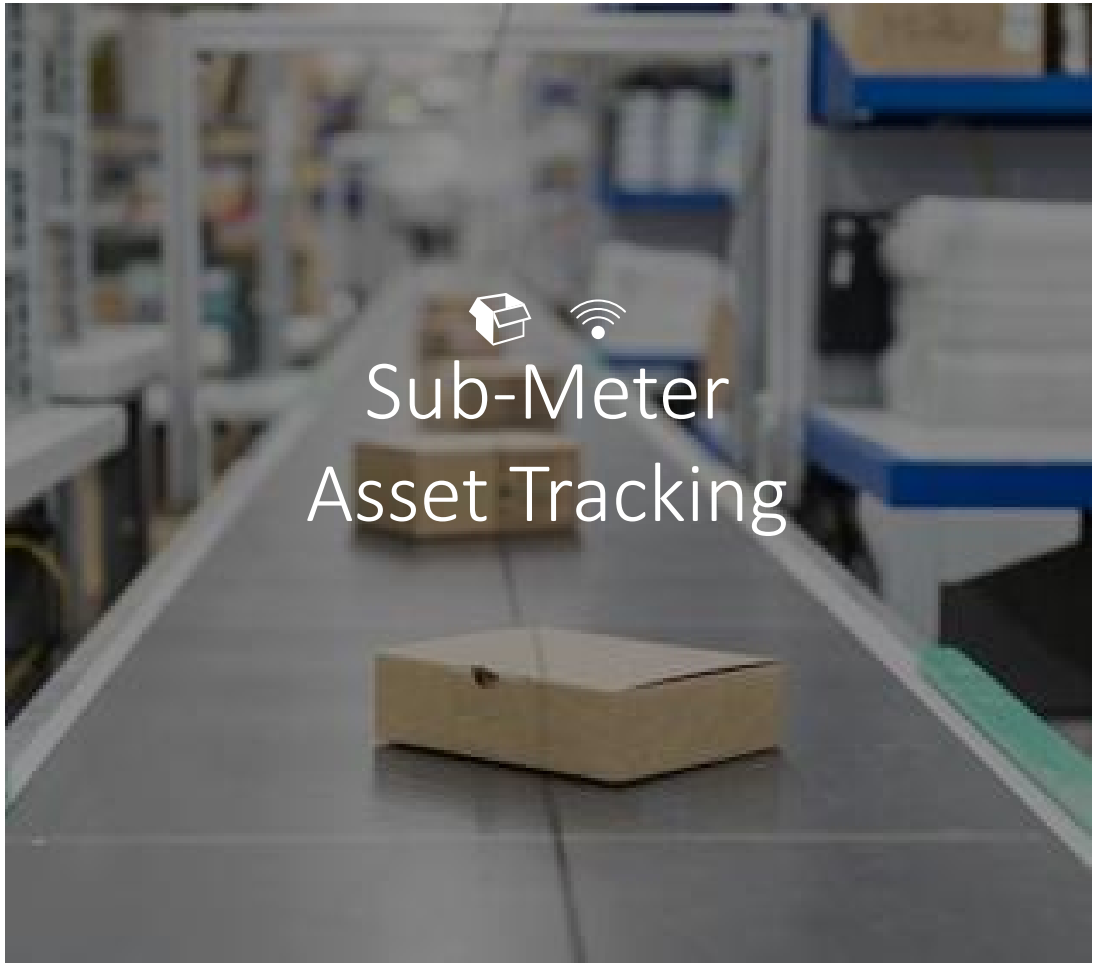
SLWSTK6021A	1x WSTK main boards 1x SLWRB4182A radio boards (QFN40) 1x SLWRB4183A radio boards (QFN32)
SLWRB4182A	BG22 +6 dBm radio board (QFN40)
SLWRB4183A	BG22 +6 dBm radio board (QFN32)
SLTB010A	Thunderboard BG22 kit

Thank You | Questions

Any query, please contact us or email to David.Fukada@silabs.com

Topic	Date
Designing Secure Bluetooth 5.2 IoT Products with BG22	10a.m., Tuesday, June 4
Connected Home Over IP (CHIP) for Beginners	10a.m., Thursday, June 9
Device & Network Security for the IoT	10a.m., Thursday, June 11

Highly Accurate Indoor Location Services



- Silicon Labs and Quuppa (www.quuppa.com) partnered to deliver accurate Bluetooth indoor locations services

Silicon Labs

- BG22 based tags can deliver 5-10 year life time on a coin cell batteries
- The BoM of a BG22 based Bluetooth tags can be reach <$1 in high volume, enabling affordable large scale asset tracking

Quuppa

- Bluetooth AoA based infrastructure for indoor and outdoor asset tracking
- A positioning engine providing X,Y and Z coordinates of assets via REST API as well two-way IoT data
- https://quuppa.com/technology/products/