SILICON LABS

How to Design a **Smart Home Door Lock**

By: Sean Scannell, Associate Product Manager

Introduction

Access control as a technology for homes, vacation rentals and apartments is growing in demand to facilitate services, such as short-term rentals, dog walking and package delivery. With that growth comes increased concerns about safety and only granting authorized access and entry. This is complicated by different requirements across various smart applications.

This whitepaper will demonstrate how to address those challenges using a Zigbee Door Lock reference platform that is modular, allowing you to implement a dual or multi-authentication scheme using various inputs and sensors. We'll explain some of the most popular methods, including facial recognition, fingerprint ID, mobile applications, and manual keypad entry powered by the Zigbee Door Lock Reference Kit based on Silicon Labs EFR32MG21 Development Kit (Zigbee, Thread, Bluetooth).

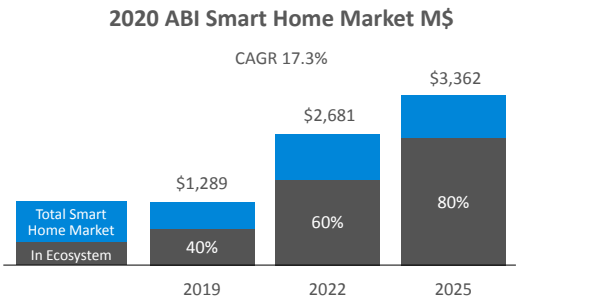
What Does a Smart Home Door Lock Offer?

When you arrive home, the first thing you do is unlock your front door. The door is one of the most used points in your house, and therefore, we want to make it smart. A smart door lock removes the need for a physical key and gives you the ability to control access without worrying about where you left your keys. You can have peace of mind knowing you can control access to your home without being physically present. Let guests inside from your smart phone and sync your smart door lock with other smart home products to provide additional utility. This makes smart door locks ideal for short-term rentals, cleaning, and maintenance services. You'll never have to worry about forgetting to lock your doors while you're away from your home. Simply lock or unlock your door from your smartphone. At Silicon Labs, we want to help our customers realize the smart home's full potential by offering innovative and easy-to-use products and detailed documentation.

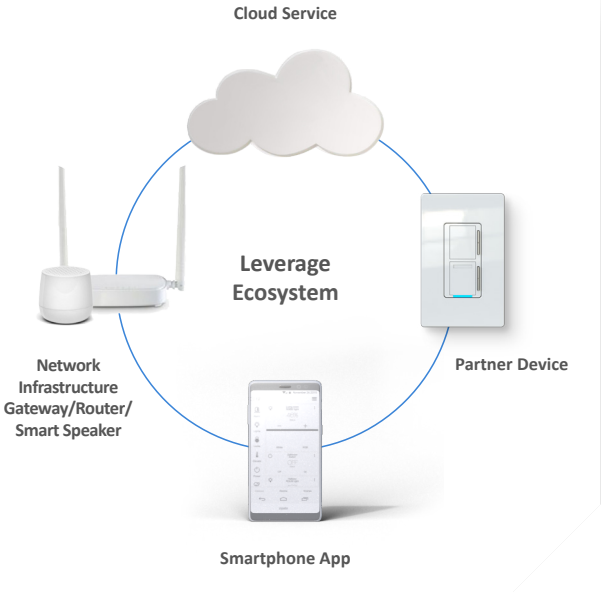
Scaling Your Smart Home Through an Ecosystem

Your smart door lock can be synced with an ecosystem of other smart devices. An ecosystem allows you to turn on the lights, ask Alexa to turn on your favorite TV show, and adjust the air conditioning from one set of controls. If you don't want to build all these elements separately, you can leverage an ecosystem Internet of Things (IoT) partner to develop a solution that fits your needs by combining your smart door lock with additional smart home devices. The 2020 ABI Smart Home Market Report predicts the IoT industry is projected to reach $3.3 billion by 2025. In this market, approximately 80 percent of products are expected to exist in at least one ecosystem.

Additionally, ecosystems are preestablished and have addressed many of the challenges associated with smart home integration, including networking and routing as well as integrating cloud services. Ecosystems also provide prebuilt smartphone profiles that reduce the need to focus on these other elements. This allows designers to focus on their specific domain expertise to deliver the best possible products, instead of spending time on non-core functionalities. Ecosystems also provide a standardized infrastructure ensuring compatibility over time and increasing the lifespan of the product. Once in an ecosystem, you can begin working with the other synched components, and the cloud becomes more accessible, allowing for a wide variety of new software features.



- Leverage ecosystem IoT partners to develop system solution & services
  - Cloud partners, service partners, other device partners
- Focus on your expertise and differentiate
  - Focus on core competency value creation
- Scale resources
  - Fast time to market with solution
- Scale your business
  - Working with ecosystem and other vendors expands exposure to new channels/ markets



How to Select Your Smart Home Technology

Joining an ecosystem requires being able to speak the language of the other components in that ecosystem, which means you must select a wireless technology to use. There are several established ecosystems to choose from, all of which are driven by established companies that utilize a handful of communication protocols including Wi-Fi, Bluetooth, ZigBee, Thread, and Z-Wave. Each protocol has its strengths, including providing reliable connectivity independent of Wi-Fi services which allows your smart home to continue to power on per usual even if Wi-Fi goes down.

For our smart door lock solutions, we selected the Zigbee protocol which operates on the IEEE 802.15.4-based specification. As one of the most widely adopted smart home technologies in the IoT, Zigbee utilizes the 2.4 GHz bandwidth range and has been an active protocol since 2002. It's used in the Amazon ecosystem as well as Samsung's SmartThings ecosystem. Over half a billion Zigbee chips are used worldwide, and it has along track record of proving its value in the smart home market.

Zigbee offers support on some of the largest networks, maxing out up to 65k nodes. Zigbee also has pre-designed low power support allowing for coin-cell battery operations which reduce form factor constraints. This process is fully supported by the built-in green power feature. The network is designed around security and utilizes self-forming and self-healing to ensure network integrity at all times. Additionally, Zigbee has been tested by consumers for years and comes equipped with pre-certified stacks, reference designs, and commissioning tools.

	ECOSYSTEM	
THREAD	works with the Google Assistant	Wi-Fi
	Works with Apple HomeKit	Wi-Fi Bluetooth
zigbee Bluetooth	WORKS WITH alexa	
zigbee	Friends of hue	Bluetooth
zigbee	works with XFINITY Home	Wi-Fi
zigbee Z-WAVE	Works with SmartThings	Wi-Fi
Z-WAVE	WORKS WITH ring	
Z-WAVE	WORKS WITH ALARM.COM	

Reliable and Independent of Internet Connectivity
Robust Large Networks
Battery Optimized

Interactive Options

Once you select your technology, you need to consider the remainder of the system requirements for your smart home door lock. Ask yourself, how are you going to connect your phone to the ecosystem? How will you control the deadbolt? What authentication modes will you use? Once you answer these questions you need to select your hardware based on those decisions.

Phone connectivity is the first component to consider as you'll need a smartphone with over-the-air update capabilities to ensure the door lock receives the necessary updates. Bluetooth is the obvious choice here, giving the phone local control of the door lock. It also provides over-the-air (OTA) capabilities so the device can receive updates as features and functionality progress.

Next, you need to control the deadbolt. The extension and retraction of the deadbolt represents the most basic function of a door lock and controlling this function is obviously a critical part of the lock's effectiveness. For this, we need motor control that makes it possible to extend or retract the deadbolt on command.

Finally, you'll need to select your authentication modes. There plenty of options available and for this project we've decided to use three different authentication modes: keypad code, fingerprint recognition, and facial recognition:

- **Keypad codes** are the most common option and predate the smart home aspects of door locks. They're robust and not dependent on connectivity. In addition to this reliability, keypads enable multiple software features including single-use codes and codes that expire after a certain amount of time. These are popular for short-term rental applications, where it's beneficial for a code to expire after a certain period of use.

- **Fingerprint recognition** requires the least amount of interaction with the system. The user simply presses one finger to the smart door lock once in order to gain access. This makes it appealing because it's also the fastest interaction.

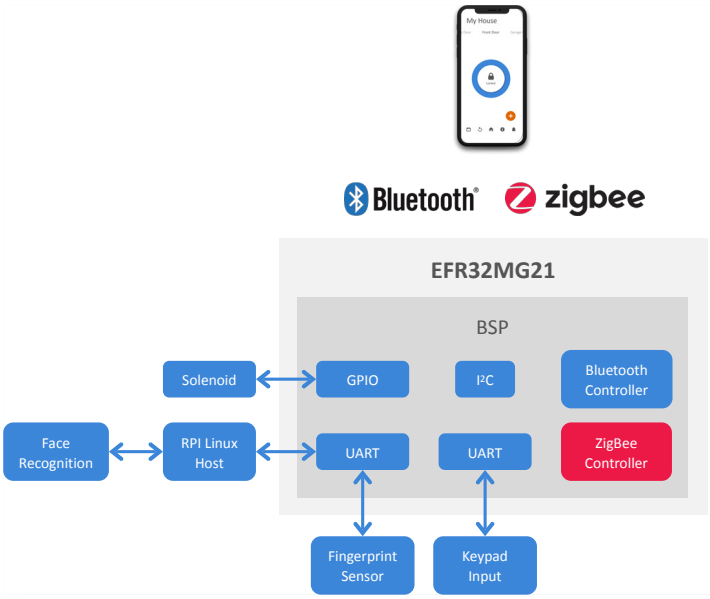
- **Facial recognition** in a high-end feature and one of the most difficult – and costly - to implement. It's also one of the most interactive options available. Smartphones have been utilizing this feature and its popularity covers a wide audience. Plus, it's just cool that your face can unlock your home.

5 silabs.com/applications/home-and-life/smart-home/locks

Silicon Labs Platform Solves Key Smart Home Door Lock Needs

There's still one more decision to make – which microcontroller (MCU) to select. This might be the most important decision because the MCU is responsible for the functionality that makes the door lock smart. For this project we decided to go with the Silicon Labs EFR32 Wireless Gecko. The EFR32 is an IoT-focused wireless SoC and has been tried and tested in the industry with robust RF performance in both 2.4 and sub-GHz frequencies. It also has optimum output power and high sensitivity. Additionally, this product offers optimized power performance with both low active and sleep currents to extent battery life. Of particular importance to door locks, these MCUs offer great ecosystem interoperability and comes with built-in security features like end-to-end encryption. The built-in tamper protection ensures chip security at all times. Silicon Labs also offers modules that are pre-certified by the ecosystems, eliminating another developer pain point.

The main system controller kit includes the EFR32MG21 Development Kit which handles authentication, network, and mobile integrations. The deadbolt control demo includes an Uxcell a1409 Open Frame Actuator and enables the general solenoid door lock functionality. This communicates with our board using standard general-purpose input/output (GPIO). The Micro Robotics TTP229 4x4 Keypad Kit offers and enables code authentication. The fingerprint sensor kit is the Sunrom R307 and the face recognition kit is the Omron B5T.

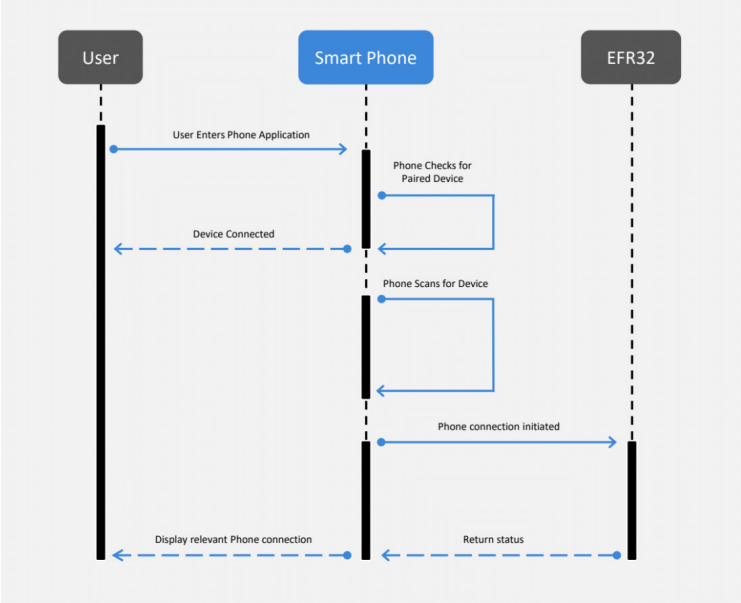


- Main System Controller Kit
  - EFR32MG21 Dev Kit
  - Handling authentication / network / mobile phone integration
- Deadbolt Control Demo for Standard Door Lock Types
  - Uxcell a1409 Open Frame Actuator
  - Enabling general solenoid door lock functionality
- Keypad Kit
  - TTP229 4x4 keypad kit
  - Enabling code authentication
- Fingerprint Sensor Kit
  - R307
  - Enabling fingerprint as authentication method
- Face Recognition Kit
  - Omron B5T face recognition
  - Enabling face recognition authentication

Building the Smart Door Lock

The reference design and code for this door lock can be found on GitHub. For authentication, the reference design provides authentication modes user interface. This makes it possible to switch between the different options we cover here. You also have the option to choose 1-step and 2-step authentications for added security. The reference design also provides general features including OTA provisioning and updates, basic driver architectures for EFR32, and power management for both sleep and active states.

We've also developed a mobile app based on our existing EFR Connect app, and the Bluetooth connection between the phone and the board is also provided, as is Zigbee network integration. The Zigbee implementation begins with powering on both devices and outing AEM on the WSTK board. Then, on the door lock device, the user presses PB1 which forms the Zigbee network. Once that has happened, the user presses PB1 on the switch device to join the Zigbee network. After the Pan ID is displayed, Press PB1 on the switch device again to discover and bind to the lock device. Pressing PB1 again closes the network. Now, PB0 on the switch device will toggle the DMP door lock.

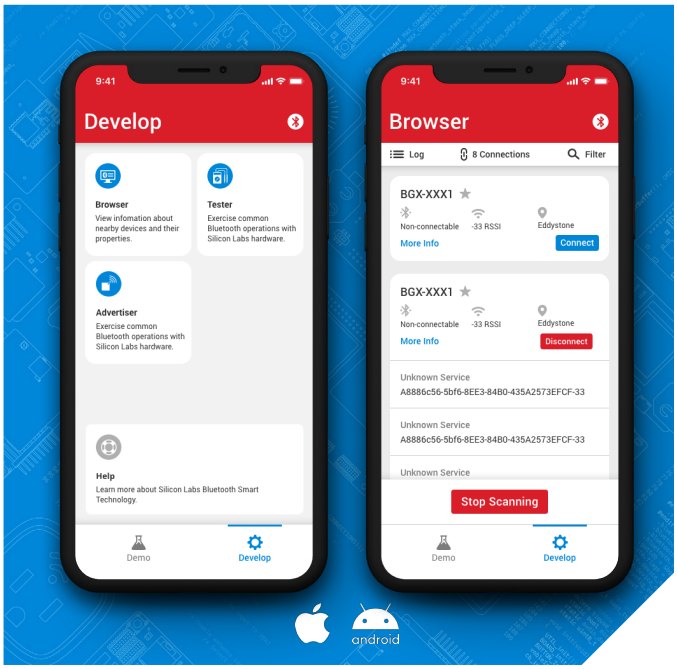


Zigbee Implementation

- Zigbee Connection
  - User powers on both devices
  - User presses PB1 to on device 1 to form a Zigbee network
  - User Presses PB1 on device 2 to join a Zigbee network
  - After Pan ID is displayed, press PB1 on Device 2 to discover and bind to the Door Lock Device
  - User Presses PB1 on the Door Lock device to close the network
  - PB0 on device 2 will now toggle the DMP Door Lock

Smart Door Lock App

We mentioned our EFR Connect app earlier, and it's a developer app that is built around simplicity. The UI is designed to forefront key Bluetooth Low Energy (BLE) metrics and includes developer-focused features, including simultaneous connections for broader visibility, log and export BLE activity, powerful filtering options to ID devices. You can access the source code on GitHub.



Enhanced Development with EFR Connect

- Developer app built around simplicity
  - UI designed to forefront key BLE device metrics
  - App-delivered tools support BLE code development
- Developer-focused features
  - Simultaneous connections for broader visibility
  - Log and export BLE activity
  - Powerful filtering options to identify devices
  - Save custom UUID to better organize a GATT
- Try it today
  - Replaces Silicon Labs Blue Gecko mobile app
  - Available on iOS and Android
  - Source code available on GitHub

Our template provides device discovery, door lock control, event history, and passcode security protection.

To implement the Bluetooth connection, open the Silicon Labs application from your smart device. Hit "Start Scanning" and check to see if there is a paired device and connect. If the paired device is not connected, keep scanning for the device, and connect. You can narrow your search by filtering out RSSI to -48 dm. The DMP4428 is the door lock device you should select and connect. You'll receive a status update of the lock. Enter your password into the app and watch the door lock status change. To see video demonstrations of the application discussed in this whitepaper, visit the Works With session page featuring this project.

Conclusion

As with any IoT application, there are a number of non-technical considerations to keep in mind. First, determine what the market opportunity might be. The smart door lock market is not likely to be overly saturated; in fact, it is quite the opposite. The fact that start-ups are popping up in this area all the time suggests that the market is healthy enough to support plenty of further innovation. Another question to consider is the segment you want to target. Do you want to develop low-cost, easy-entry smart door locks or high-end locks with sophisticated features? Once you have a design, you'll need to determine cost and what's required to make a profit. Finally, how will you sell your lock? What channels will you employ?

There are a lot of great reasons to build smart door locks and taking the time to work through these steps can make a big difference in how quickly you get to market and the quality of your end product. For more information about Silicon Labs offerings in this area, visit https://www.silabs.com/applications/home-and-life/smart-home/locks.