*Application Report*

# *SimpleLink™ Wi-Fi® Enabled Electronic Smart Lock*

*Benjamin Moore, SimpleLink Wi-Fi Applications Team*

## ABSTRACT

This application report describes the development of Wi-Fi® enabled electronic smart locks (e-locks). Specifically, the benefits of adding Wi-Fi to an e-lock design are examined.

Different Wi-Fi use cases are presented along with an estimate of system battery life for two main use cases. This application report demonstrates that SimpleLink™ Wi-Fi makes it possible to create a battery powered e-lock design that can be securely monitored and controlled from the cloud.

The Smart Lock Reference Design Enabling 5+ Years Battery Life on 4× AA Batteries [1] is referenced throughout this document as the *Smart Lock Reference Design*. For a list of supporting documentation and additional resources, see Section 8.

## Table of Contents

## Trademarks

SimpleLink™, MSP430™, CapTIvate™, Internet-on-a chip™, Texas Instruments™, LaunchPad™, BoosterPack™, and MSP432™ are trademarks of Texas Instruments.
Google™ is a trademark of Google Inc.
Wi-Fi® is a registered trademark of Wi-Fi Alliance.
Bluetooth® is a registered trademark of Bluetooth SIG.
All other trademarks are the property of their respective owners.

# 1 Introduction

Though traditional locks have been around for thousands of years, door locks have continuously evolved into more complex systems with integrated electronic controls and wireless interfaces. Locks control who can access homes and buildings, while acting as the first line of defense in security systems.

These new locks are commonly called *electronic smart locks* (e-locks). E-locks are changing the way we think about and interact with door locks. Badges, fobs, pin numbers, or even mobile devices can act as keys that lock or unlock a door. For many residential applications, e-locks can eliminate the need for users to carry physical keys. Furthermore, changing the form of the key used to open a door helps address one of the main problems faced by traditional locks—providing a method for quickly creating and managing access keys.

Using Wi-Fi connectivity in an e-lock system makes it easy to create and manage access keys at any time. Wi-Fi connectivity also enables new features, such as the ability to remotely monitor and control the e-lock. Additionally, integrating Wi-Fi directly into the e-lock eliminates the need to use a bridge for connecting the lock to the internet. An integrated design provides an all-in-one product that reduces overall BOM cost and enables applications that demand high throughput directly to the lock. This document discusses multiple use cases for and benefits of integrating Wi-Fi in an electronic smart lock design, as well as some of the key requirements for e-locks with Wi-Fi connectivity. Specifically, this guide describes how SimpleLink Wi-Fi enables the development of battery powered e-locks that can be securely monitored and controlled through the cloud.

# 2 Terminology

The following terminology is used throughout this document.

**Asymmetric Keys** Asymmetric key pairs are used in algorithms where one party performs a cryptographic operation with a key that is not the same as the key used to apply the reverse operation. The pairs are defined as public and private keys, and used mostly for digital signing and symmetric key distribution.

**Authenticity** Authenticity ensures that assets or entities are genuine and authorized to perform a task or used as intended. The verification process usually involves cryptographic algorithms, which check that the entities are who they claim to be. Some predefined trust mechanism is always part of an authentication scheme.

**Certificates** Certificates are standard-formatted files. They typically contain the public key of the subject, and a CA signature of the header and public key. Anyone provided with the CA public key (or sub-CA in case of certificate chain) can verify the subject's identity.

**Confidentiality** Confidentiality ensures that an asset is not made available or disclosed to unauthorized entities. In most cases, confidentiality translates into encryption, while in other cases, obfuscation techniques are used to maintain confidentiality.

**Integrity** Integrity is an attribute describing an object that remains intact, in its entirety, compared to its original version.

**Keys** Keys are used for data encryption, key establishment, and digital signatures. The key lengths and types depend on the algorithm used, their purpose, and the security level.

**Security Measures** Measures that aim to provide the intended protection of some assets against some threats.

## 3 Electronic Smart Locks (E-Locks)

E-locks can typically be classified in two categories based on where they will be used:

- Commercial locks (hotel, office, shopping center, and so on)
- Residential locks (home or apartment)

System design considerations are impacted based on whether a lock will be used to secure a residential building or a commercial building.

### 3.1 Residential

Residential locks are designed to be used on the exterior of a house and are typically located on the front door. E-locks designed for residential use typically operate on battery power and are expected to last a least one year before the batteries must be replaced. Because the distance between the door and the in-home router can vary, it is necessary to choose a Wi-Fi device with robust connectivity for residential applications. Other low-power RF technologies are typically used to support the peer-to-peer connection between a key (fob or mobile device) and a residential e-lock.

Figure 3-1 shows a diagram of the typical wireless links in a residential e-lock system.

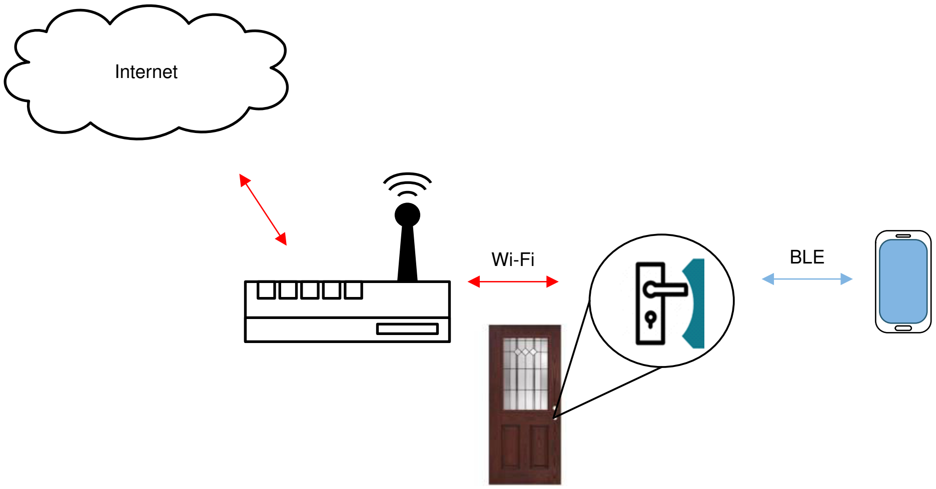


**Figure 3-1. Residential E-Lock System**

### 3.2 Commercial

Commercial locks can be placed on the exterior of a building to prevent initial entry and on the interior of the building to control access to areas restricted for use by specific personnel. Some commercial locks are designed to be line-powered, but many operate on batteries. Battery-powered, commercial locks face strict power constraints because they are often deployed in large numbers. Using a large number of battery powered locks across a building leads to a large amount of maintenance effort and cost when batteries must be replaced. Therefore, Wi-Fi solutions with extremely low-power modes and fast wake-up times are essential to commercial e-lock applications.

# 4 Wi-Fi Use Cases and Benefits

Integrating Wi-Fi into an electronic smart lock design provides clear advantages over other low-power RF technologies that do not provide a direct connection to the internet. A direct Wi-Fi connection to a home access point (AP) makes it possible to:

- Lock or unlock the door from anywhere internet connectivity is available
- Know every time the door is locked or unlocked
- Perform fast Over-the-Air (OTA) updates from anywhere
- Easily add or remove authorized users and authenticate through the cloud
- Reduce system cost and improve end-customer ease of use with a single door-lock solution connected directly to the cloud

## 4.1 Lock or Unlock From Anywhere

Connecting an electronic door lock directly to your home access AP makes it possible to access the lock from anywhere through the internet. After the lock connects to the AP, the lock can create a connection with a remote cloud server. A user can then communicate to the lock through the cloud server with another internet-connected device such as a smartphone, tablet, or PC.

Users benefit from the cloud connectivity by always knowing whether the lock is open or closed. If the lock is accidentally left open, a user can quickly check the status of the lock and then secure it from the mobile device without having to return home. Similarly, a homeowner with remote control of a lock can choose to let someone into their house at any time. Having on-demand control is especially beneficial if someone loses their key or does not need permanent access to the home (for example: repairman, postal worker, and so on).

## 4.2 Know When the Lock is Accessed

Another benefit of integrating Wi-Fi into an electronic smart lock is that a user can get a notification any time the lock is accessed. When the state of the lock is changed, the lock can publish that information to the cloud server, which can then forward a notification message on to the user.

With instant notifications, the owner of the lock has the convenience of knowing when someone is at their home. For example, a notification can be generated when children get back from school or when a housekeeper arrives to clean the home. Similarly, a notification can be sent to the owner if someone attempts to tamper with the lock or break into the lock.

## 4.3 Perform Fast OTA Updates

For internet-connected products like Wi-Fi enabled e-locks, it is necessary to have a method for updating the system files and software. Examples of files that must be replaced over time are device certificates and keys that are used by the cloud to identify and establish secure connections to the lock. Software updates may also be required to enable new features, fix existing issues, or address security flaws. Because e-locks are typically installed in doors, it is impractical for a user to remove the lock from the door and use a physical connection to perform the update. Implementing a wireless update mechanism, known as an over-the-air (OTA) update, provides a simple way to keep the system up-to-date.

OTA updates could be implemented with other low-power RF technologies, but these are often impractical. For example, using a low-power peer-to-peer technology requires a user to be physically present to enable the update. In this case, the update is delivered directly from the user's mobile device to the lock using a mobile application. Additionally, depending on the throughput provided by the technology, a user may have to wait several minutes for the update to complete.

Alternatively, an e-lock with integrated Wi-Fi and internet connectivity can be automatically updated through an AP with no need for the user to be near the lock. The user can also take advantage of higher throughput to speed up the update process. For commercial e-lock applications, Wi-Fi integration can lead to significant savings in cost and time by eliminating the need to manually update the e-lock firmware.

### 4.4 Easily Add or Remove Users

A major limitation with traditional locks is the amount of time it takes to create a new key for a user. Making a copy of a physical key requires special machinery and can take a long time. It can even be inconvenient for a user to physically access the lock to create a new pin or digital key when the lock is unlocked using a keypad or a wireless interface.

When Wi-Fi connectivity is added to an e-lock design, the lock can store authentication lists (whitelists) either locally or in the cloud. The whitelist, or list of approved users, will be used to determine whether or not to give a user access based on a digital key. Whenever the owner wants to add or remove a user, the process is simple—the owner creates a new profile with a unique key and access restrictions, then the new user information is pushed to the lock or to the cloud as an update.

### 4.5 Eliminate Extraneous Bridge Hardware

Manufacturers can add Wi-Fi based features to e-locks by creating a device that can bridge the link between a non-Wi-Fi based e-lock and the home AP. These devices, known as *network bridges*, must be designed to connect the local Wi-Fi network to the e-lock by translating packets to the protocol used directly by the e-lock, such as *Bluetooth*® low energy or Sub-1 GHz protocols.

A network bridge is not an ideal solution because it increases the complexity of the overall system design and also increases the entire system cost for the end user. Additional bridge hardware is undesirable because it usually requires a plug in the wall and takes up extra space.

In contrast to using a bridge, integrating Wi-Fi directly into the lock reduces the cost for the end user, simplifies the user experience, and makes it possible to develop new features that rely on high data throughput to the e-lock.

## 5 Wi-Fi Connectivity and Power Use Cases

There are many distinct ways that Wi-Fi connectivity can be used in electronic smart locks (e-locks). The number of features enabled and the power budget required depends on how the Wi-Fi connectivity is used. The most common Wi-Fi connectivity use cases (in order of lowest-power to highest-power consumption) are as follows:

- Wi-Fi scheduled wake-up for periodic updates
- Wi-Fi wake-up on sensor event
- Wi-Fi always connected

The lowest power use case is when the Wi-Fi is turned on only for periodic updates. This use case is generally chosen when Wi-Fi is not the interface controlling the lock because it is not always active. Typically, systems that wake up only for periodic updates will use another mechanism for receiving access credentials, such as a keypad. For example, updating the whitelist for an office building or hotel room may only need to occur once or several times a day. A wake-up that is scheduled to occur periodically can be used to turn on the Wi-Fi and check for an update. Similarly, scheduled wake-ups can be used to deliver new software to e-locks in the form of OTA updates.

Another use case is when the Wi-Fi is triggered to wake up on a sensor event (such as a button press, an interrupt generated from a passive infrared sensor, or even another connectivity device like a Bluetooth low energy network processor). A triggered wakeup can be useful to optimize power consumption while also enabling the system to respond to a user. When a user approaches a door lock that implements this scheme for Wi-Fi activity, it can use a sensor to detect the user, then connect to the cloud in order to authenticate the user or send a push notification to the owner.

The Wi-Fi solution must have a short wakeup and connection cycle to provide the best user experience with a triggered wakeup. SimpleLink™ Wi-Fi has multiple built-in mechanisms to optimize wakeup and connection times including Fast Connect, Fast DHCP Renew, and hardware acceleration of TLS/SSL handshakes. When used together, SimpleLink Wi-Fi can wake up from a 4.5-μA hibernate mode, establish a WPA2 secured connection to an AP, and create a TLS/SSL connection to a server in approximately 0.5 seconds.

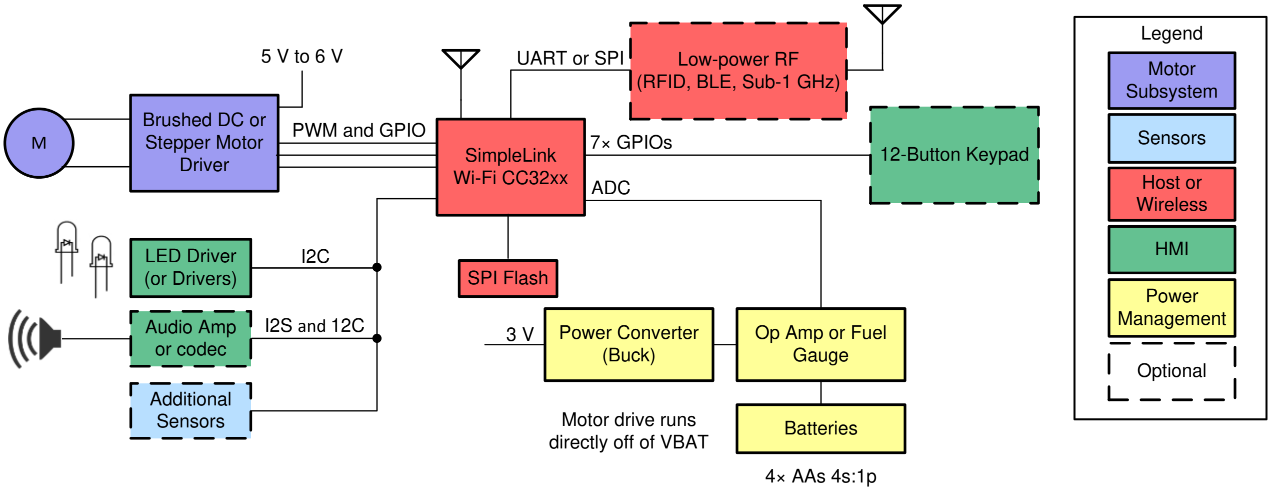
The use case for Wi-Fi that enables the widest feature set is when the Wi-Fi is always connected. Maintaining a secure connection to the cloud allows on-demand access to the lock and provides the lowest latency when sending data. In the always-connected use case, a user can quickly access the lock from anywhere, at any time. The biggest challenge for devices that implement an always-connected policy is maintaining the connection to peers through the internet while in an extremely low-power state. SimpleLink Wi-Fi solves this problem with the ability to maintain socket states even through low-power deep sleep (LPDS) cycles.

## 6 Key System Requirements

Electronic smart locks (e-locks) are usually composed of the following key functional blocks:

- Human machine interface (HMI)
- Wireless connectivity
- Host microcontroller
- Motor subsystem
- Sensors
- Power management

Figure 6-1 shows a typical block diagram for an e-lock system with Wi-Fi.



Copyright © 2017, Texas Instruments Incorporated

**Figure 6-1. Example Wi-Fi Enabled E-Lock System Block Diagram**

**HMI**

The HMI provides a method for the user to interact with the system or to view a response from the e-lock. The HMI may include a keypad, backlight, LEDs, speaker, or even a microphone. Some e-lock designs implement the HMI on a PCB that is physically separate from the rest of the system. TI's MSP430™ microcontroller (MCU) with CapTIvate™ touch technology is specifically designed for adding a dedicated HMI controller and industrial capacitive touch solution to an e-lock. Wireless connectivity enables part of the HMI functionality, such as the keypad, to be handled on a remote device (such as a smartphone or tablet).

**Wireless connectivity**

Wireless connectivity [1](such as Wi-Fi, Bluetooth low energy, Sub-1 GHz, or RFID) adds an additional data interface to the lock. This interface can be used for various purposes including wireless authentication of the user, remote control and monitoring, wireless transfer of software updates, or communication with networked sensors. In some cases, the addition of a wireless interface allows for part of the HMI functionality to be handled by a remote device (such as a smartphone or tablet).

[1] Designers must make sure coexistence requirements are met when using multiple RF transceivers in a system.

**Host controller**
The host controller is responsible for processing inputs from the user and from sensors. It also generates responses by actuating the physical locking mechanism or providing feedback through the HMI. Using the CC3220 wireless MCU, the host controller and Wi-Fi can be integrated into a single chip.

**Sensors**
Various sensors can be used in an e-lock to detect the state of the lock and door (for example, an accelerometer or inertial measurement unit (IMU) to know when a door is open or closed) or the presence of a user (for example, a passive infrared (PIR) sensor for proximity detection).

**Motor subsystem**
The motor subsystem includes both the motor driver and the motor used to actuate the locking mechanism. E-locks commonly use brushed DC or stepper motors to move the locking mechanism. These types of motors can be driven using low-voltage, single H-bridge or dual H-bridge motor drivers, such as the DRV8833, DRV8833C, DRV8837, and DRV8837C devices.

**Power**
E-locks are usually powered by four AA batteries. The various lock subsystems may operate at different voltages, which creates a need for voltage regulators in the system. A designer must carefully select the appropriate regulators to use because this choice has a direct impact on the battery life achieved by the system.

The SimpleLink CC3220 wireless MCU devices integrate multiple peripherals that support e-lock design, including a 12-bit analog-to-digital converter (ADC), general-purpose timers with a 16-bit pulse-width modulation (PWM) mode, and multiple serial interface standards. The universal asynchronous receive/transmit (UART) or Serial Peripheral Interface bus (SPI) peripherals can be leveraged to communicate with coprocessors or transceivers to support additional RF technologies in the e-lock (such as Bluetooth low energy, RFID, or Sub-1 GHz). The Inter-integrated Circuit (I2C) peripheral can be used to communicate with digital sensors and configure all audio codecs or audio amplifiers in the design. Transmission of digital audio to an audio codec or audio amplifier is possible using the Multichannel Audio Serial Port (McASP), which supports the Inter-IC Sound (I2S) bit stream format.

The SimpleLink CC3120 Network Processor can be used instead of the CC3220 device to add Wi-Fi connectivity to systems that already include an existing MCU solution. A host MCU can communicate with the CC3120 device over either UART or SPI.

## 6.1 Low-Power Wi-Fi E-Lock

An entire e-lock typically operates on four alkaline AA batteries used in a 4 series, 1 parallel (4s:1p) configuration. One of the biggest challenges for e-lock designs is reducing the power consumed by the motor subsystem. As discussed in the *Smart Lock Reference Design* [1], optimizing the power design in an e-lock can help reduce the power consumed by the motor subsystem and can extend the battery life to multiple years.

Currently, the amount of data that a Wi-Fi e-lock requires to transmit and receive is small in comparison to data-streaming applications. Because the radio must only be active for short bursts of data, the active power of the Wi-Fi interface does not typically impact the power consumption as much as the power consumed while the Wi-Fi device is in sleep mode. The level of low power achieved by SimpleLink Wi-Fi in sleep modes along with the optimizations to minimize the duration of active cycles by the network learning algorithm make it possible to maintain the battery life need for an e-lock.

### 6.1.1 Current Consumption and Battery Life

Using the measurements presented in the *Smart Lock Reference Design* [1], we can estimate the battery life of an e-lock designed with SimpleLink Wi-Fi for the intermittently connected and always connected use cases. An actual Wi-Fi e-lock design could dynamically switch between these use cases to achieve the necessary balance of power consumption and performance. Therefore, these estimates can serve as the estimated range in battery life of a SimpleLink Wi-Fi based e-lock.

#### 6.1.1.1 Intermittently Connected

As described in Section 5, a Wi-Fi enabled e-lock could be designed to only turn on the Wi-Fi interface when it must transmit data to or receive data from a remote server. The Wi-Fi interface could be turned on either based on a scheduled wakeup or from a sensor trigger. In this case, the system will be intermittently connected to the local network and cloud. It is assumed for the intermittently connected use case that the system will remain in hibernate mode when it is not connected to the network. In hibernate mode, the application processor and the network subsystem memory is not retained. The following steps are required for each wake-up cycle before sending data:

1. Initialize the system (load application and wake the network processor).
2. Reconnect to the local network.
3. Establish a secure socket session.
4. Transmit and receive data.
5. Return to hibernate.

In this use case, the power consumed by SimpleLink Wi-Fi can be estimated based on a measurement of the case where the device is woken by a trigger and then sends data over Wi-Fi each time the door is locked or unlocked.

For the estimate, we assume an average of 24 lock and unlock events per day, as discussed in the *Smart Lock Reference Design* [1]. We also assume that the IP address of the remote server is cached by the application so that it does not have to be looked up using DNS every time the device wakes up and reconnects to the network.

Figure 6-2 shows the average power consumption and total time required to perform one cycle of steps 1 through 5 with a CC3220S device when connecting to a local server with TLS 1.2 and the TLS_RSA_WITH_AES_256_CBC_SHA cipher suite. Figure 6-2 shows that the average current consumed is roughly 46.3 mA over a period of 0.510 seconds.

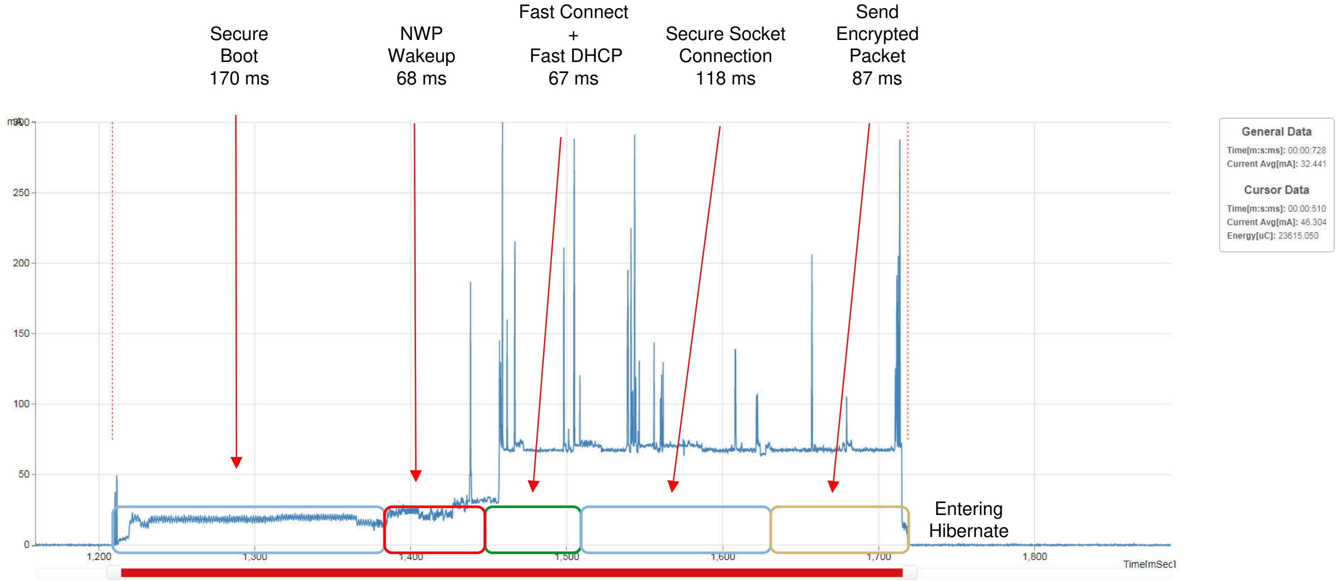


**Figure 6-2. Power Consumption of CC3220S From Hibernate to TLS Connection to Local Server**

The average power consumed by the Wi-Fi subsystem can therefore be calculated with Equation 1.

$$
\begin{aligned}
P_{total} &= \left(V_{on} \times D_{on} \times I_{on} + V_{off} \times D_{off} \times I_{off}\right)\\
P_{total} &= 3\,V \times \left(\frac{24 \times 0.510\,s}{86400\,s} \times 46.3\,mA + \frac{86400\,s - (24 \times 0.510\,s)}{86400\,s} \times 0.0045\,mA\right)\\
P_{total} &= 3\,V \times (0.00014 \times 46.3\,mA + 0.9998 \times 0.0045\,mA)\\
P_{total} &= 0.0329\ mW\,(\approx 33\,\mu W)
\end{aligned} \tag{1}
$$

Adding the average power from Equation 1 to the total system power calculated in the *Smart Lock Reference Design* [1], we can estimate that the overall average power that is consumed by the entire Bluetooth low energy plus Wi-Fi lock system would be 0.523 mW. Using the theoretical total energy capacity of the 4× AA batteries, we find the estimated battery life of the e-lock as calculated by Equation 2.

$$
\begin{aligned}
\text{Battery Life}_{yrs} &= \frac{\text{Energy Capacity of Batteries (mWh)}}{\text{Average System Power (mW)}} \times \frac{1\text{ day}}{24\text{ hrs}} \times \frac{1\text{ year}}{365\text{ days}}\\
\text{Battery Life}_{yrs} &= \frac{18000\text{ mWh}}{0.523\text{ mW}} \times \frac{1\text{ day}}{24\text{ hrs}} \times \frac{1\text{ year}}{365\text{ days}}\\
\text{Battery Life}_{yrs} &\approx 3.9\text{ years (3 years, 11 months)}
\end{aligned} \tag{2}
$$

Figure 6-3 shows the average power consumption and total time required to perform one cycle of step 1 through step 5 with a CC3220S device using *www.google.com* as the server.

**Note**

The measurement shows that the amount of time it takes to establish a secure connection to the Google™ server is roughly 1 second because an elliptic curve cipher is selected. Elliptic-curve Diffie–Hellman Exchange (ECDHE) and Elliptic Curve Digital Signature Algorithm (ECDSA) are not accelerated with the hardware encryption engine.

Figure 6-3 shows that the average current consumed is roughly 38.1 mA over a period of 1.353 seconds.

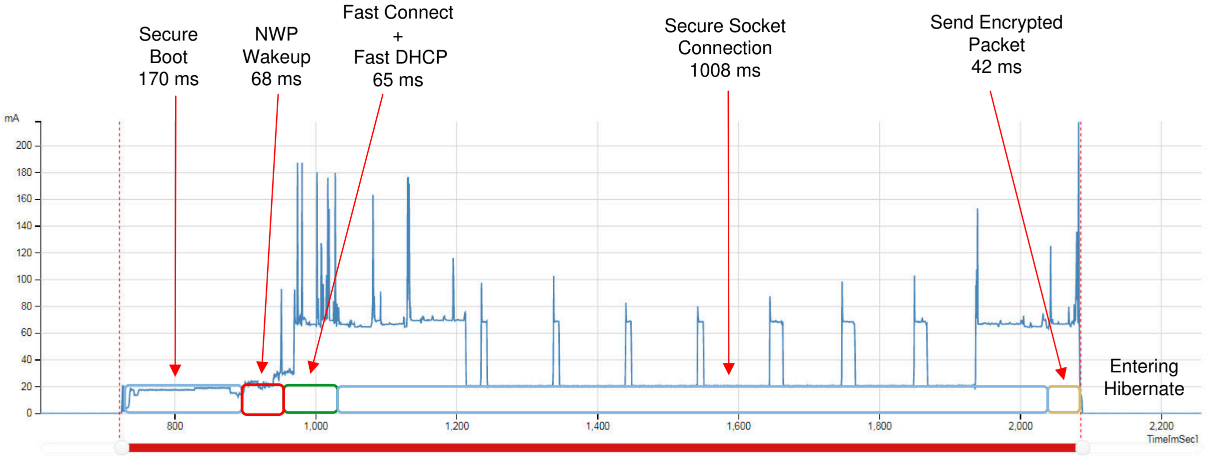


**Figure 6-3. Power Consumption of CC3220S From Hibernate to TLS Connection to www.google.com**

Using Equation 1, the average power consumed by the Wi-Fi subsystem when connecting to www.google.com can therefore be calculated as 0.0569 mW (approximately 57 µW).

Adding the average power from Equation 1 to the average system power calculated in the *Smart Lock Reference Design* [1], we find that the overall average power consumed by the entire Bluetooth low energy plus Wi-Fi lock system is 0.547 mW. Using the theoretical total energy capacity of the 4× AA batteries, we find the estimated battery life of the e-lock is approximately 3.8 years (3 years, 9 months).

#### 6.1.1.2 Always Connected

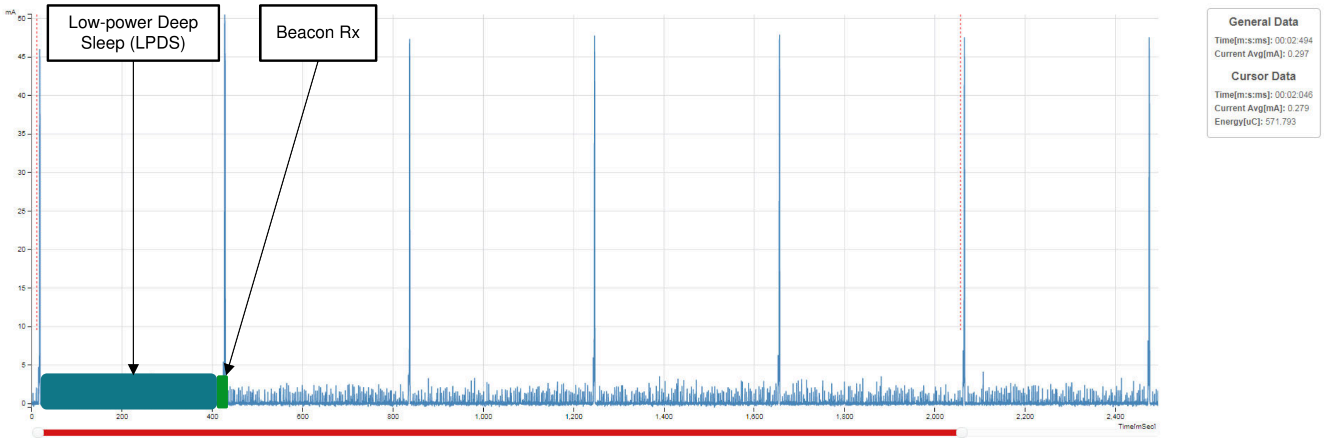
In addition to the intermittently connected use case discussed in Section 6.1.1.1, an e-lock can be designed to always remain connected to the AP, which provides on-demand access to the user. In this case, the system enters LPDS mode and maintains at all times the secure socket connection to the remote server. The system can still wake-up on a sensor trigger to send data, and can also wake up periodically to receive beacons from the AP. Receiving beacons allows the system to maintain a connection to the AP and retrieve any data the AP has buffered for the system.

SimpleLink Wi-Fi implements and extension of the 802.11 power save mode where a certain number of beacons can be skipped to allow the device to sleep longer and reduce the overall idle power. While the SimpleLink device is sleeping, the AP will buffer data destined for the device to prevent data from being lost. The number of beacons skipped is set by the duration of time that the device is configured to remain in LPDS, which is called long sleep interval (LSI). SimpleLink Wi-Fi further reduces power consumption when using an LSI with a network-learning algorithm that optimizes the amount of time the device is awake to receive each beacon. For this analysis, we will assume an LSI of 500 milliseconds.

**Note**

APs do not buffer data for connected stations indefinitely; therefore, selecting a large amount of time for the LSI can impact the compatibility of the system with APs. The developer is responsible for choosing an appropriate LSI for their product.

Because the amount of data transferred by an e-lock for each lock or unlock cycle is relatively small (estimated as <1000 bytes), the Wi-Fi radio is only active for a short amount of time each day. As a result, the average power consumption of the Wi-Fi subsystem in always connected mode can be estimated as the power consumed while the device is not sending data. Figure 6-4 shows the average power consumption of the SimpleLink Wi-Fi CC3220S device while the device is idle (not sending data) with a LSI of 500 milliseconds.



General Data

Time[m:s:ms]: 00:02:494

Current Avg[mA]: 0.297

Cursor Data

Time[m:s:ms]: 00:02:046

Current Avg[mA]: 0.279

Energy[uC]: 571.793

**Figure 6-4. Always Connected Idle Current With LSI = 500 milliseconds**

Figure 6-4 shows that the average current is roughly 279 μA while the device is idle. Based on this measurement, we can estimate the average power of the Wi-Fi in always connected mode with Equation 3.

$$P_{\text{always\_connected}} \cong V_{\text{idle}} \times I_{\text{idle}} = 3\text{ V} \times 279\text{ μA} = 0.837\text{ mW } (837\text{ μW}) \tag{3}$$

Adding the average power from Equation 3 to the average system power calculated in the *Smart Lock Reference Design* [1], we find that the overall average power consumed by the entire Bluetooth low energy plus Wi-Fi lock system is approximately 1.33 mW. By following the same calculations from Section 6.1.1.1, we find that in this case, the estimated battery life of the system is 1.54 years (approximately 1 year, 6 months).

## 6.2 Wi-Fi E-Lock Security

Because e-locks are a key component in security systems, they must be designed with security in mind. E-locks provide privileged access to an asset by locking out unauthorized users while remaining available for all authorized users. For example, a lock may provide privileged access to structures like houses, office buildings, or hotel rooms.

At a high level, privileged access is established through the use of access credentials and whitelists. In the case of a mechanical lock, the access credential is a physical key, and the whitelist is the set of users with the physical keys.

Similar to protecting a physical key, an e-lock system must protect pin numbers, digital IDs, digital keys (the access credential), and any databases of authorized users (the whitelist). In addition to these assets, a Wi-Fi e-lock must also address other security challenges, such as:

- Securing end-user private data
- Protecting against malicious or invalid OTA updates
- Protecting intellectual property (IP)
- Ensuring only authorized devices link to cloud services

Secure end-user private data—any data that enables a Wi-Fi e-lock to be controlled by specific, authorized users must be kept private. This end-user data must be secured during transfer over the Wi-Fi interface, transfer through the internet, and any time it is stored in non-volatile memory on the lock. Private end-user data could include access credentials, whitelists, or any other data that associates the lock with a specific user account.

Protect against malicious or invalid OTA updates—it is important to ensure that a Wi-Fi e-lock is functional so it will operate when accessed by an authorized user. The e-lock is rendered unuseful if it becomes locked out by having its software changed by an attacker or by performing an update to a new version with a bug. Ensure the e-lock operates when needed by protecting the system integrity through guarding against malicious or invalid updates.

Protect IP—it is also important to protect the confidentiality of the intellectual property (IP) on the system, such as the e-lock software. Keeping the IP protected helps ensure that attackers are unable to copy the lock design or learn how the system works in order to exploit potential flaws.

Ensure only authorized devices link to cloud services—building a secure system requires more than just implementing security to protect the e-lock. Developers must take steps to protect other assets, such as application servers and cloud services, by adding a mechanism to verify the identity of every e-lock that connects to an application server.

SimpleLink Wi-Fi is designed with a wide range of security features built in to help e-lock developers address these security challenges. Figure 6-5 shows several security enablers in SimpleLink Wi-Fi and how they match up with the security challenges. Section 6.2.1 through Section 6.2.7 explain the enablers that appear in red text in Figure 6-5 and how they simplify designing an e-lock.

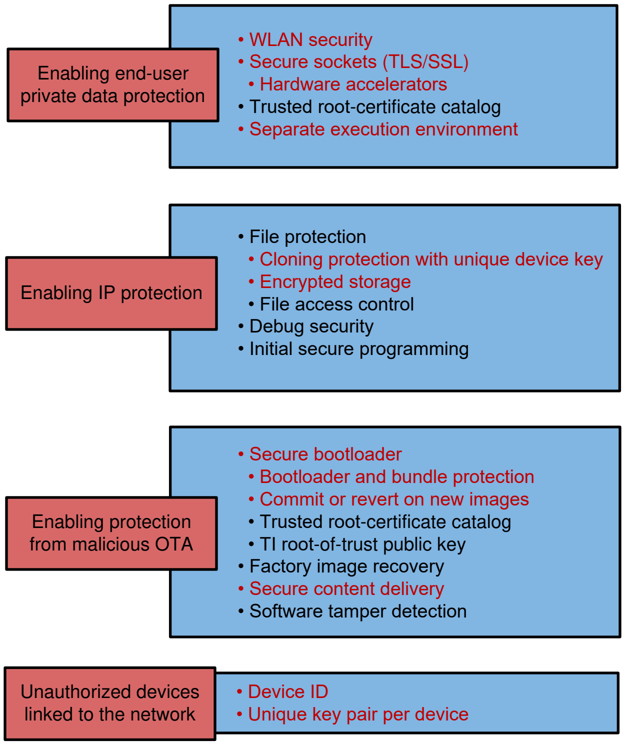

Enabling end-user private data protection
• WLAN security
• Secure sockets (TLS/SSL)
• Hardware accelerators
• Trusted root-certificate catalog
• Separate execution environment
Enabling IP protection
• File protection
• Cloning protection with unique device key
• Encrypted storage
• File access control
• Debug security
• Initial secure programming
Enabling protection from malicious OTA
• Secure bootloader
• Bootloader and bundle protection
• Commit or revert on new images
• Trusted root-certificate catalog
• TI root-of-trust public key
• Factory image recovery
• Secure content delivery
• Software tamper detection
Unauthorized devices linked to the network
• Device ID
• Unique key pair per device

**Figure 6-5. E-Lock Security Challenges and SimpleLink™ Wi-Fi Security Enablers**

To read about the complete set of security features offered in the SimpleLink Wi-Fi device family, see the *SimpleLink™ CC3120, CC3220 Wi-Fi® Internet-on-a chip™ Solution Built-In Security Features Application Report*.

### 6.2.1 Wireless LAN and Internet Security

During everyday use of an e-lock, data such as access keys, user profile information, and software can be transferred between the e-lock and an AP, then sent on to a remote application server. For protection on the local area network, the system must use a secure Wi-Fi connection to the AP. SimpleLink Wi-Fi supports all common Wi-Fi security modes for personal and enterprise networks, including WEP, WPA/WPA2 PSK, WPA2 Enterprise (802.1x), WPA2 + PMF, and WPA3. Wi-Fi security provides a mechanism for a local network to authenticate the lock and establish encryption of the data transferred over the local link.

Because data will be transferred through the internet, steps must be taken to secure the communication link between the device and the application servers. A key step in protecting data that is transferred through the internet is using secure sockets (TLS/SSL). Use of a secure socket makes it possible for both the server and the client to verify identity and negotiate a cryptographic protocol to use for securing the transferred data.

**Note**

> The throughput achieved with secure sockets is lower than the maximum throughput of a TCP socket due to the additional headers applied to the data and the cipher applied to the data before transfer.

The CC3120 and CC3220 devices support up to six simultaneous secure sockets out of the 16 total sockets that are available. To have the best protection, an e-lock must transfer any identified assets with the highest level of security supported by the application server. For the full list of supported cipher suites, see the *CC3120, CC3220 SimpleLink™ Wi-Fi® and Internet of Things Network Processor Programmer's Guide*.

### 6.2.2 Secure Storage

Securely storing all the key assets listed in Section 6 is a top priority for e-locks because it helps keep the assets from being accessed by malicious users. Secure storage helps protect against both direct and indirect attempts to read nonvolatile memory. Even though direct (or physical) attacks may be less scalable, it is still important to protect against attackers cloning the e-lock system, or thieves reading and stealing personal information from the nonvolatile memory in a stolen e-lock.

The SimpleLink CC3120 and CC3220 devices use an external nonvolatile memory in the form of a serial flash. The content stored on the serial flash is organized by the network processor into a file system. Many features are built into the file system that can be used to protect assets during storage, including the abilities to:

- Encrypt data—use AES-128 to keep data confidential.
- Check data integrity—apply a signature to the file when changed and verify the content when opened for read.
- Control access to data—use file tokens to set access permissions.
- Alert the system about tampering—detect invalid and potentially malicious attempts to access to files.

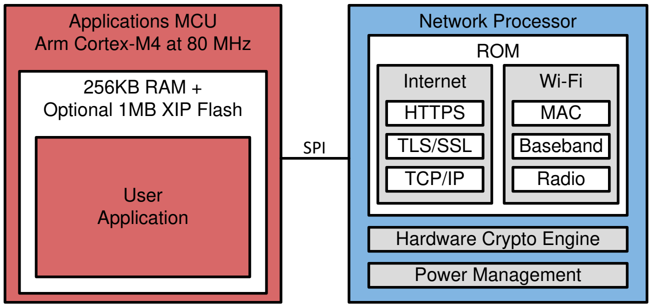
Files that are custom for the e-lock application can be created with different levels of protection using file creation flags and file tokens, based on the application requirements. However, there are forced creation flags for certain system files that must be stored securely. These files and their associated creation flags are listed in Table 6-1.

**Table 6-1. Secured System Files**

| Filename | CC3120, CC3220S, CC3220SF | CC3220R | Remark |
|---|---|---|---|
| /sys/servicepack.ucf<br>/sys/certstore.lst | Secure signed by TI<br>+ public write<br>+ Fail-safe | Secure signed by TI | • These files are delivered by TI.<br>• The service pack contains fixes to the device code; the trusted root-certificate catalog contains the root CAs supported by TI and a revoked certificate list.<br>• TI might deliver a new version for those files when required.<br>• TI highly recommends designing the host to support future updates of these files. |
| /sys/mcuimg.bin //CC3220R/ CC3220S<br>/sys/mcuflashimg.bin // CC3220SF | Secure signed | Not secure | The file contains the host program. |
| /sys/cert/private.key<br>/sys/cert/client.der<br>/sys/cert/ca.der | Secure | Secure, blocked for read | The files contain the key and certificate for SSL connection. |

### 6.2.3 Separate Execution Environments

The CC3220 device architecture is based on separate execution environments for the application MCU and the network processor. Figure 6-6 shows a simplified diagram of the CC3220 device architecture.



Copyright © 2017, Texas Instruments Incorporated

**Figure 6-6. Separate Execution Environments**

Separating the application and networking execution environments can be advantageous because this separation allows the network processor to offload the host MCU. The application can continue to run timecritical tasks while the network processor runs the networking stack and performs computationally intensive work, such as handling cryptographic algorithms.

Another benefit of using separate execution environments is that it can reduce the exposure of the application to attacks performed through the network interface. Separate execution environments also reduces the exposure of certificates and private keys. Certificates and private keys only need to be accessed by the network processor when setting up a secure socket connection, which means these files can be stored as secured files that are blocked for read access. The host controller can write the files to update them, but the host controller cannot read the files into its memory where they would be exposed as plaintext.

### 6.2.4 Secure Content Delivery

The CC3120 and CC3220 devices introduce a feature called *secure content delivery*, which is a mechanism that can be used by the developer to add additional protection to data transfers, independent of the transport layer security. Secure content delivery is built on the ability of the SimpleLink Wi-Fi Network Processor to generate temporary ECC key-pairs. A remote server can use the public key that is generated by the device to derive a shared secret and then encrypt the content.

Therefore, the content can only be decrypted by the network processor because the private key is never exposed to the host. The network processor performs decryption when the host performs a file write to a secure file. Secure content delivery is useful for protecting files (such as certificates and private keys) that are already blocked for read access by the host, but may need to be written through the host or updated over time.

### 6.2.5 Secure Boot

A ROM bootloader is built into the SimpleLink Wi-Fi CC3220S and CC3220SF devices. This ROM bootloader includes a step to validate the integrity and authenticity of the runtime binary (application image). The validation step is possible because the image must be programmed as a secure-signed file.

When the bootloader runs, it validates the signature that the developer applies to the image using a certificate supplied by the developer. The certificate is then validated against the entire chain-of-trust from which it was derived.

**Note**

To validate the certificate, the entire chain of trust must be programmed to the external flash. The Root CA of the chain of trust must be one of the Root CAs included in the SimpleLink Wi-Fi trusted-root-certificate catalog. The Root CA list can be found in the SDK in *tools/cc32xx_tools/certificate-catalog/readme.html*. The catalog is provided by TI and is used to verify that the chain of trust is derived from a known and trusted source.

Validating the runtime binary as part of the bootloader is intended to help inhibit the execution of an image from an unknown vendor, such as in the case of a malicious OTA update. For more information on the secure boot feature, see *SimpleLink™ CC3120, CC3220 Wi-Fi® Internet-on-a chip™ Solution Built-In Security Features*.

### 6.2.6 Failsafe Files and Bundle Protection

Use of OTA updates in e-locks creates a need for measures to protect the integrity of the system that is performing the update. Delivery of an incomplete or invalid update to the system can cause the system to stop functioning and become unusable. The developer of an e-lock must design the system to protect against failed updates to ensure the lock will function at all times.

SimpleLink Wi-Fi introduces two mechanisms in the file system that assist in protecting the integrity of the system during an update. The features are known as *failsafe files* and *bundle protection*. Failsafe files allow developers to store a duplicate copy of updated files and test the new copies before they are committed to the file system. Bundled files are all committed at the same time to prevent partial updates. Placing bundled files in a pending commit state allows the system to restart the application with all the new files and run a user-defined test before the files are actually committed to the file system for use (when they become active). This additional step of verifying the new content from the OTA update helps ensure the e-lock will work properly when the update completes.

### 6.2.7 Unique Device Identity

When a product like an e-lock connects to a cloud server, the server should verify the identity of the device to ensure it is a valid product and has permission to access the available services. Without identity verification, malicious devices could connect to the cloud services and potentially increase server utilization and costs. One solution to this problem is to create and program unique device certificates and keys to each lock. However, creating, programming, and managing a large number of devices with unique files can take a long time and be costly.

To simplify the process of establishing unique device identities, each SimpleLink CC3120 and CC3220 device has an unmodifiable 128-bit number and a unique ECC key pair built into the device during production. The 128-bit number can serve as a unique device identifier (UDID) and the unique ECC key-pair can be used to sign data. The UDID and the unique key-pair can be used together to verify the identity of each SimpleLink Wi-Fi device. For an e-lock design, this mechanism is advantageous because it saves the developer time and can help the developer make sure that only known devices access associated cloud services.

## 6.3 Interoperability

When designing a Wi-Fi enabled e-lock, it is necessary to choose a Wi-Fi solution that is interoperable with a wide range of APs. Interoperability includes establishing and maintaining a connection with an AP, and also delivering consistent low-power operation without compromising the robustness of the solution.

SimpleLink Wi-Fi is tested against over 200 APs to ensure quality of the solution, enabling designs to be deployed in regions across the world. Texas Instruments™ has also obtained Wi-Fi Alliance certification for the CC3120 and CC3220 devices and modules.

The high level of interoperability provided by the SimpleLink Wi-Fi solution ensures that battery powered e-locks have consistent performance in various deployment scenarios; including different types of homes and buildings. To learn more about the WLAN radio performance of the SimpleLink CC3220 device, see *CC3220 SimpleLink™ Wi-Fi® Wireless and Internet-of-Things Solution, a Single-Chip Wireless MCU*.

# 7 Summary

E-locks with wireless connectivity simplify access control in commercial buildings and homes. Wi-Fi connectivity provides key benefits over other RF technologies in e-locks by providing a direct method to remotely monitor and control the lock. Wi-Fi also improves the user experience by enabling automatic delivery of software updates and expediting the update process.

The SimpleLink Wi-Fi CC3120 Network Processor and CC3220 Wireless MCU make it possible to integrate Wi-Fi connectivity directly into the e-lock design without compromising battery life. SimpleLink Wi-Fi also provides the key security features and the high level of interoperability necessary for a robust e-lock design.

## 8 References and Related Documentation

### Product Pages on TI.com

[1] Smart Lock Reference Design Enabling 5+ Years Battery Life on 4× AA Batteries

[2] CC3120 SimpleLink™ Wi-Fi® Network Processor, Internet-of-Things Solution for MCU Applications

[3] SimpleLink™ Wi-Fi® and IoT, Single-Chip Wireless MCU Solution (CC3220R, CC3220S, CC3220SF)

[4] SimpleLink™ Wi-Fi® CC3220S Wireless Microcontroller LaunchPad™ Development Kit or SimpleLink™ Wi-Fi® CC3220SF Wireless Microcontroller LaunchPad™ Development Kit

[5] SimpleLink™ Wi-Fi® CC3120 Wireless Network Processor BoosterPack™ Plug-in Module with the SimpleLink™ MSP432P401R LaunchPad™ Development Kit

[6] SimpleLink™ Wi-Fi® CC3220 Software Development Kit (SDK)

[7] SimpleLink™ MSP432™ Software Development Kit (SDK)

[8] DRV8833 2-A Low-Voltage Dual Brushed DC or Single Bipolar Stepper Motor Driver (PWM Ctrl)

[9] DRV8833C 1-A Low-Voltage Stepper or Single/Dual Brushed DC Motor Driver (PWM Ctrl)

[10] DRV8837 1.8-A Low-Voltage Brushed DC Motor Driver (PWM Ctrl)

[11] DRV8837C 1-A Low-Voltage H-Bridge Driver

### Blog

[12] Texas instruments, *Smart Wi-Fi® locks will soon open many doors*

### User's Guides

[13] Texas instruments, *IP smart door locks: Power optimized and added security features for cloud connectivity with SimpleLink™ Wi-Fi®*

[14] Texas instruments, *CC3120, CC3220 SimpleLink™ Wi-Fi® and Internet-of-Things Network Processor Programmer's Guide*

### Application Reports

[15] Texas instruments, *SimpleLink™ CC3120, CC3220 Wi-Fi® Internet-on-a chip™ Solution Built-In Security Features*

[16] Texas instruments, *SimpleLink™ CC3120, CC3220 Wi-Fi® Internet-on-a chip™ Networking Subsystem Power Management*

## 9 Revision History

NOTE: Page numbers for previous revisions may differ from page numbers in the current version.

| Changes from Revision * (December 2017) to Revision A (September 2020) | Page |
|---|---|
| • Updated the numbering format for tables, figures, and cross-references throughout the document.................. | 2 |
| • Added WPA2 + PMF and WPA3 in Section 6.2.1, *Wireless LAN and Internet Security* .................................. | 12 |

## IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, or other requirements. These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale (www.ti.com/legal/termsofsale.html) or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265