Introduction

The door access systems have evolved from simple physical keys to more sophisticated keyless entry systems. Now, we have a system that automatically unlocks the door when user carrying an access key approaches the door handle. As it does not require any user action this system is referred to as Passive Entry.

This reference design provides a passive entry door access system for hospitality and residential door access applications. It uses Atmel’s PTC based capacitive sensing and ultra-low power Bluetooth® SMART solution. This document describes the proximity sensor design, low power mode and basic BLE communication link to authenticate the user.

The associated package contains hardware design files and GCC (Atmel Studio) example projects for door handle and access key module to demonstrate passive entry access.

Features

- Small form factor design on a single PCB (includes MCU, BLE, Sensor)
- Proximity Sensing with 2cm range
- Sensor Design
- Shielding Techniques
- Fast response time (less than 1sec including authentication)
- Access control through Bluetooth Low Energy (BLE 4.1)
- Low power consumption (less than 80μA average current)
# Table of Contents

Introduction .................................................................................................................................................. 1  
Features ..................................................................................................................................................... 1  
1. Abbreviations and Definitions .............................................................................................................. 3  
2. Passive Entry System ............................................................................................................................. 4  
   2.1. System Block Diagram ........................................................................................................................ 5  
3. Access Control ....................................................................................................................................... 6  
   3.1. Proximity Sensing ............................................................................................................................... 6  
   3.2. Sensor Design .................................................................................................................................... 8  
4. Firmware .................................................................................................................................................. 11  
   4.1. Low Power Mode Proximity Sensor .................................................................................................... 12  
   4.2. Bluetooth Communication .................................................................................................................. 12  
   4.3. Source Files ..................................................................................................................................... 16  
5. Demonstration Setup ............................................................................................................................... 17  
6. Schematic ............................................................................................................................................... 18  
7. PCB Layout ............................................................................................................................................ 19  
8. References ............................................................................................................................................. 20  
9. Revision History ..................................................................................................................................... 21
1. Abbreviations and Definitions

- **Bluetooth Low Energy (BLE):** It is a wireless network technology designed and marketed by the Bluetooth Special Interest Group aimed at novel applications in the healthcare, fitness, beacons, security, and home automation. Compared to Classic Bluetooth, Bluetooth Low Energy or Bluetooth Smart is intended to provide considerably reduced power consumption and cost while maintaining a similar communication range.

- **Channel:** One of the capacitive point at which the controller can detect capacitive change.

- **Electrode:** The patch of conductive material on the substrate that forms the sensor. An electrode is usually made from copper, carbon, silver ink, Indium Tin Oxide (ITO).

- **Event System:** A system which allows for direct actions to be performed in one peripheral in response to a stimulus in another peripheral without CPU intervention.

- **Low Power Sensor:** A sensor which is periodically measured for touch detection without any CPU intervention. The CPU may be held in deep sleep mode throughout the operation, minimizing power consumption.

- **Peripheral Touch Controller (PTC):** This is a microcontroller peripheral which acquires signals to detect touch on capacitive sensors.

- **Proximity Sensor:** A sensor which is able to detect the presence of nearby conductive objects (user finger or hand) without any physical contact.

- **QTouch Library:** A software library which performs touch acquisition and post-processing. It provides interfaces to configure, calibrate, and measure touch sensors.

- **Self-capacitance Sensor:** A sensor with only one direct connection to the sensor controller. A self-capacitance sensor tends to emit electric fields in all directions.

- **Sensor:** A component that detects a touch. Sensors consists of one or more electrodes. It can be a button, slider, or wheel.
2. **Passive Entry System**

The basic requirements for a passive entry system are,

- detection of approaching user
- user authentication
- provide signal to door lock unit

**Figure 2-1 Passive Entry System**

Typically, any type of proximity sensor can be used for detecting a user approaching the door handle. When user presence is detected, the system needs to authenticate the user. This is performed by a secure communication between the door handle and access key (with user).

A typical Passive Entry System uses an access key which contains low-frequency (LF) receiver and wireless transmitter, and a door handle which contains low-frequency (LF) transmitter and wireless receiver.

The sequence of user detection and passive entry unlock of the doors is as follows:

1. When the user approaches the door handle, the hand is detected when it is within the range of the proximity sensor, typically 2cm.
2. The proximity sensor wakes the LF driver from sleep and LF antenna generates a magnetic field with a range of 1 to 3 meters.
3. Access key (carried by the user) transitions from a very low power listening mode to active mode in response to the field generated by LF antenna.
4. Access key wirelessly transmits a security code to wireless receiver on the door handle side.
5. If the security code is correct, the door module unlocks the door.

Usage of low-frequency (LF) communication allows the access key to remain in low-power mode until it is brought within proximity range of the door. This helps to reduce power consumption of access key and improves battery life.

In addition to this, the LF communication can be used to locate the position of access key with respect to the door and prevent unauthorized access. This provides three-dimensional data which can localize the access key as being either inside or outside of the room. If the system is able to determine the presence of the access key outside the door, it unlocks the door. If the system senses access key within the room, it denies the access.
2.1. **System Block Diagram**

The door handle module integrates a main MCU (ATSAMD21E18A), BLE (ATBTLC1000), and proximity sensor. Bluetooth Smart (BLE) technology is used for the communication between door handle and user access key. This design does not cover the usage of LF communication link. The following block diagram shows key components of the passive entry system.

**Figure 2-2 System Block Diagram**

![System Block Diagram]

The sequence of operation is as follows:

1. Access key module sends the advertising data periodically.
2. Door handle module waits for proximity sensor detection in low power mode.
3. When user hand approaches inner side of the door handle. Proximity sensor detects it and wakes up the Bluetooth wireless module from sleep.
4. Bluetooth module in the door handle starts scanning for BLE advertising data.
5. It establishes connection and pairing upon detecting a valid access key.
6. If pairing (authentication) is successful, access control module lights up a LED mounted on door handle. The LED light simulates signal from access control module to unlock the door.
3. **Access Control**

In this reference design, access control is designed using ATSAMD21J18A device. It uses input from a proximity sensor and controls the Bluetooth device (ATBTLC1000) using UART communication.

*Figure 3-1 Access Control Block Diagram*

When the proximity sensor detects a user’s presence, ATBTLC1000 performs the required communication for authentication. The door opens on successful authentication. This is indicated by lighting up an LED placed on the door handle.

**Note:** The system also requires a means for locking the door. This can be performed either by using an additional touch button for lock or a mechanical system that locks automatically when the door is closed. This solution is not covered in this reference design. The designer can design a system that is appropriate for the system.

3.1. **Proximity Sensing**

A proximity sensor is a sensor that can detect presence of an approaching conductive object or hand while it is few centimeters away from the surface of the sensor electrode. Proximity sensing does not require physical contact with the sensor electrode.

Capacitive proximity sensors measure the relative change in capacitance between a single electrode and ground (self-capacitance sensors) or between two electrodes (mutual capacitance sensors), as a conductive object / hand approaches the sensor.
Since the electrical fields spread out from the sensor electrode in all directions, self-capacitance is the preferred proximity detection method over mutual capacitance where field is largely concentrated with in the area between the transmitting(X) and receiving(Y) electrodes. Self-capacitance proximity sensor is used in this reference design.

For a passive entry door system, the key parameters that define an effective proximity sensor are:
- Proximity Range
- Shielding
- Response Time
- Power consumption
- Form Factor

### 3.1.1. Proximity Range
The user places his hand on inner side of door handle in order to pull the handle and open the door. When the hand approaches inner side of door handle, proximity sensor detects the presence of a hand. Typically, the proximity range should be 2cm.

### 3.1.2. Shielding
The shield is used as a means of preventing the sensor from being activated from any other direction except the intended sensing area. For an unintentional touch on the outer side of door handle, the door should not open. For example, a person leaning on the door with the appropriate key, proximity sensor should not report it as valid touch. Presence of a shield prevents the sensor from such unintentional touch events.

Shielding can be achieved in two ways - Active Shield and Passive Shield.

#### 3.1.2.1. Active Shield
The theory behind active shield is to apply exact same sensor signal through a buffer on an electrode on the reverse side of the sensor. This will deflect the capacitive field from the back of the sensor towards the front. Thereby, enhancing signal strength and range of the sensor on front side, while blocking any sensing on back side of the sensor.

The active shield is driven by an op-amp configured as a voltage follower as shown in the following circuit diagram.
The inputs to shield driver (op-amp +) and proximity sensor electrode are driven by the same capacitive sense line. The op-amp buffers input signal from the sensor and directly drives shield electrode located beneath the sensor. This method is suitable for designs where usage of an external op-amp is feasible.

3.1.2.2. Ground Shield
This method uses a ground plane on opposite side of the sensor. The ground plane suppresses all capacitive fields from back side of the sensor, preventing touch activation from back side.

The presence of ground near the sensor, loads the sensor. Such loading adds directly to sensor capacitance (Cx). Large proximity sensor with ground plane at opposite side may cause saturation of PTC channels. For reliable touch operation, it is important to ensure the sensor is not saturated and within the limit of allowable sensor capacitance per channel. This shield method is suitable for small proximity sensors.

This reference design uses ground shield method to prevent touch detection from outer side of door handle.

3.1.3. Response Time
A higher scan rate means more sensor readings are performed every second, which results in faster detection of user’s hand as it approaches the door handle. This mitigates the delay induced by communication processing and enable the doors to unlock quickly before the user could notice any lag between holding the door handle and opening it. Typical sensor scan rate (time between two successive touch measurements) for the sensor should be less than 20ms.

3.1.4. Low Power Consumption
The access control module is a battery operated system mounted on door handle. It must work for longer duration without the frequent requirement to replace battery.

Using proximity sensor, enables the control MCU to sleep until any user detection occurs. Only the proximity sensing module is active.

Further reduction in power consumption can be achieved by utilizing the low power mode in PTC QTouch Library.

3.1.5. Form Factor
The proximity sensor must fit inside a door handle. The sensor size can be designed based on door handle size and desired proximity range.

3.2. Sensor Design
The sensor for the passive entry system is designed for detecting user hand up to 2cm on one side while rejecting it on other side.
One side contains a proximity sensor electrode and the other side contains a ground shield to reject touch
detection from outer side.

**Figure 3-4 Proximity Sensor with Ground Shield**

Ground shield below the proximity sensor increases ground loading and reduces effective proximity
range. The percentage of ground added below can be reduced (using meshed ground plane) to increase
the proximity range at the cost of reduced shielding from other side. Lesser shield at back side increases
proximity detection range from back side as well.

The proximity sensor is placed inside a door handle.

**Figure 3-5 Proximity Sensor on Door Handle**
3.2.1. **Noise Performance**

Noise performance depends on the sensor design, ground shielding, power supply and the end target environment. As proximity sensors on door handle are expected to be battery powered, power supply noise should not be a major concern. However, electrostatic discharge (ESD) and other interconnected devices that have electronic activity in RF range might introduce unwanted noise into the system. Better noise performance can be achieved by complying with the general rules and recommendations for sensor designs. The *Buttons, Sliders and Wheels Sensor Design Guide* describes the general rules that can be used to create sensor patterns.

Noise robustness of the system can be improved further by adjusting the software parameters in PTC QTouch library namely Filter Level, Auto Oversampling, Prescaler, Sense Resistor, and Acquisition Frequency Mode.

Refer *SAM Peripheral Touch Controller User Guide* for more details about PTC QTouch Library and its associated parameters.

Refer *PTC Robustness Design Guide* for details on sensor tuning details in noisier environment.

3.2.2. **Limitation**

One limitation with capacitive sensor in passive entry system is that it cannot be used with metal door handles. If metal from the door handle is floating with respect to the proximity sensor, it would re-radiate the electric fields which results in erratic behavior. The sensor performance may not be reliable. Sensitivity may vary randomly. It may be over sensitive or under sensitive at times. This would cause unintentional wake ups from any passerby near the door, resulting in increased power consumption.

If the metal door handle is grounded, it affects capacitive fields and makes the sensor unusable.
4. **Firmware**

The flow of the door handle application code is depicted in the following flow diagram.

**Figure 4-1 Door Handle Application Flow Diagram**

After initializing system clock, touch and BLE device, the application waits for proximity sensor detection in low power mode. After the sensor is detected, it initiates BLE communication and authentication check. If connection is established with access key device and authentication is successful, it is indicated by lighting up a LED. Then, it waits for the proximity sensor to go out of detect (user to take hand away from the handle) to start another cycle.
4.1. **Low Power Mode Proximity Sensor**

Atmel QTouch Peripheral Touch Controller (PTC) is used to perform capacitive touch measurements on the proximity sensor. PTC offers built-in hardware for autonomous capacitive touch measurement independently without the use of CPU. CPU is used to configure the PTC and to perform post processing on the acquired signal data. This allows the CPU to perform other application tasks or remain in sleep during the time of PTC touch acquisition.

PTC offers an additional feature called *Low Power Mode*, which further offloads the CPU. With the low power mode, CPU is not required to periodically wake up and initiate touch measurement. In this mode, a single sensor can be configured as a *Low Power Sensor* and the CPU put to sleep. This feature utilizes the Event System and allows the CPU to be in sleep throughout the operation, thereby minimizing power consumption significantly. The low power sensor is autonomously measured by the PTC and an interrupt is issued to wake up the CPU only when a valid touch event is detected on the low power sensor. In this reference design, the proximity sensor is configured as the Low Power Sensor. Refer *Low Power Sensor Design with PTC* for more details about Low Power Sensor measurement.

Figure 4-2  Proximity Sensor Measurement

4.2. **Bluetooth Communication**

The Atmel Bluetooth Low Energy (BLE) or Bluetooth Smart solution is a family of self-contained, low-power, and certified modules bringing Bluetooth Low Energy connectivity to any embedded design. These integrated modules offer the ideal solutions for designers seeking to develop Bluetooth communication without any Bluetooth Low Energy (Bluetooth Smart), IP Stack, or RF experience.

Atmel BLE devices are highly integrated SoC’s, requiring few external components and embedding the entire BLE 4.1 link and host stack enabling wireless connectivity for a variety of applications to be quickly implemented without any requirement of the wireless expertise.

This design incorporates Atmel’s Bluetooth SMART (BLE) technology using ATBTL1000 BluSDK.
4.2.1. Device Authentication
The Security Manager Protocol (SMP) running over Bluetooth Low Energy stack provides the service of device authentication. Security manager defines the procedures for pairing, authentication, and encryption between BLE devices. Encryption in BLE uses AES-CCM cryptography. Like BR/EDR, the BLE Controller will perform the encryption function.

Basic flow of authentication is as follows:
1. Access key advertises
2. Door handle scans, sees advertisement packets
3. Door handle initiates connection
4. Connection established
5. Access key requests for security
6. Door handle initiates pairing
7. Exchange keys
8. Pairing done
9. Store keys for future connections at both sides.
10. Encrypt the communication link using keys

When the device connects second time, pairing is not required. It can directly encrypt the communication link using stored keys during pairing. When communication link is encrypted successfully, peer device is authenticated.

4.2.2. Application Flow
Application flow for BLE communication is as follows.

Figure 4-3 Application Flow

During initialization, UART host interface and ATB TLC1000 chip are initialized. The device configuration includes setting up the device address, device name, and device advertising data.

Each activity (like establishing connection, pairing, encryption etc.) may trigger one or more event messages to be returned to the application. These event messages are handled in the event handler.
4.2.2.1. Establishing Connection

After initialization, peripheral device (access key) starts advertising data (send broadcast data on air to be discovered by other devices). Before advertising, advertising data is set using `at_ble_adv_data_set()`.

Central device (door handle) starts scanning for advertising data using `at_ble_scan_start()` API. Before starting scan, it adds peer device addresses to be connected. When the access key with desired device address is found, connection process is initiated.

**Figure 4-4 Connection Sequence**

4.2.2.2. Pairing

Pairing mechanism is the process where devices involved in the communication exchange, their identity information to set up trust and receive the encryption keys ready for future data exchange. The communication link key is created and exchanged during pairing procedure and is stored by both Bluetooth devices (access key and door handle), to be used during further connections to avoid repeating pairing procedure. The slave device (access key) requests the master device (door handle) to initiate security procedures. The demo firmware, Level 2 security mode is used where communication link is authenticated using pairing with encryption.
4.2.2.3. Encryption
The encryption procedure is used to encrypt the communication link using a previously bonded Long Term Key (LTK). This procedure is initiated by master (Door handle) of the connection.

Figure 4-6 Encryption Sequence
### 4.3. Source Files

Following tables list the main source files of the associated example projects for door handle and access key.

#### Table 4-1 Access Key Module

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>main.c</td>
<td>It consists of <code>main()</code> function and body of the example program.</td>
</tr>
<tr>
<td>access_key.c</td>
<td>It consists advertisement packet construction and sending.</td>
</tr>
<tr>
<td>access_key.h</td>
<td>Header file that defines macros required for advertisement interval, timeout.</td>
</tr>
<tr>
<td>ble_manager.c</td>
<td>It initializes ATBTLC1000 chip (set address, name) and provides function required to handle events for connection, pairing and encryption.</td>
</tr>
<tr>
<td>ble_manager.h</td>
<td>Header file that defines required macros and function declarations needed for <code>ble_manager.c</code>.</td>
</tr>
</tbody>
</table>

#### Table 4-2 Door Handle Module

<table>
<thead>
<tr>
<th>File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>main.c</td>
<td>It consists of the <code>main()</code> function and body of the example program.</td>
</tr>
<tr>
<td>touch.c</td>
<td>Main source file for proximity sensor measurement. This file contains the QTouch library initialization, sensor configuration, and measurement routines.</td>
</tr>
<tr>
<td>touch.h</td>
<td>This file contains QTouch library pin, register and sensors configuration options for Capacitive Touch acquisition using the PTC module.</td>
</tr>
<tr>
<td>peg_door_handle.c</td>
<td>It consists of functions required for scanning and handling scan events. It stores bond (key) information into NVM.</td>
</tr>
<tr>
<td>peg_door_handle.h</td>
<td>Header file that defines macros required for scan interval, connection interval, timeout needed for of <code>peg_door_handle.c</code>.</td>
</tr>
<tr>
<td>ble_manager.c</td>
<td>It initializes ATBTLC1000 chip (set address, name) and provides function required to handle events for connection, pairing, and encryption.</td>
</tr>
<tr>
<td>ble_manager.h</td>
<td>Header file that defines required macros and function declarations needed for <code>ble_manager.c</code>.</td>
</tr>
</tbody>
</table>
5. **Demonstration Setup**

The setup includes a door handle model as well as an access key. Door handle unit comprises of ATSAMD21 MCU, ATBTLC1000 and proximity sensor on a single PCB. An LED is available on the PCB to indicate successful door access authentication. The PCB is placed inside a door handle model and it is powered by a 3.3V coin cell battery. SAM D21 Xplained Pro along with BTLC1000 Xplained Pro is used as the access key. The access key is powered via USB cable.

The demonstration sequence is as follows:

1. Build the access key and door handle example projects, and program the binaries to respective modules.
2. Approach the door handle.
3. Upon proximity sensor detection, door handle unit checks user authentication (using BLE communication between access key and door handle unit).
4. If authentication is successful, the LED on door handle is illuminated.

**Note:** The door handle example project can be ported to operate on a SAM D21 Xplained pro with minimal changes. BLE interface lines and PTC lines need to be configured accordingly, along with changing device to SAMD21J18A. Using this, the demonstration can be carried out with two sets of SAM D21 Xplained Pro and BTLC1000 Xplained Pro. In such case, an external proximity sensor needs to be connected to the SAM D21 Xplained Pro that is acting as door handle.
6. Schematic

MCU and PWR

BLE

Atmel AT12649: Passive Entry Door System with Proximity Sensor [APPLICATION NOTE]
7. **PCB Layout**

Figure 7-1 Door Sensor Top Layer

Figure 7-2 Door Sensor Bottom Layer
8. References


## Revision History

<table>
<thead>
<tr>
<th>Doc Rev.</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>42582A</td>
<td>11/2015</td>
<td>Initial document release</td>
</tr>
</tbody>
</table>